FIREEYE TECHNISCHE DOKUMENTATION

ENDPOINT SECURITY

SERVER BEDIENUNGSANLEITUNG

VERSION 5.2

Bitte entschuldigen Sie unser Erscheinungsbild, da wir von FireEye zu Trellix wechseln.

Endpoint Security Server Bedienungsanleitung

Software Ausgabe 5.2.0

Revision 5

FireEye Kontaktinformation:

Website: www.fireeye.com

Technischer Support: https://csportal.fireeye.com

Telefon (USA):

1.408.321.6300

1.877.FIREEYE

Inhalt

TEIL I: Überblick

KAPITEL 1: Die Endpoint Security Plattform

FireEye Endpoint Security Produkte enthalten einen oder mehrere Endpoint Security Server, die mit Endpoint Security Agents arbeiten, die auf jedem Gerät oder Host in Ihrem Unternehmen installiert sind. Gemeinsam überwachen diese Produkte jedes Endpunktgerät oder Host und identifiziert Bedrohungsaktivitäten und Nachweise darauf.

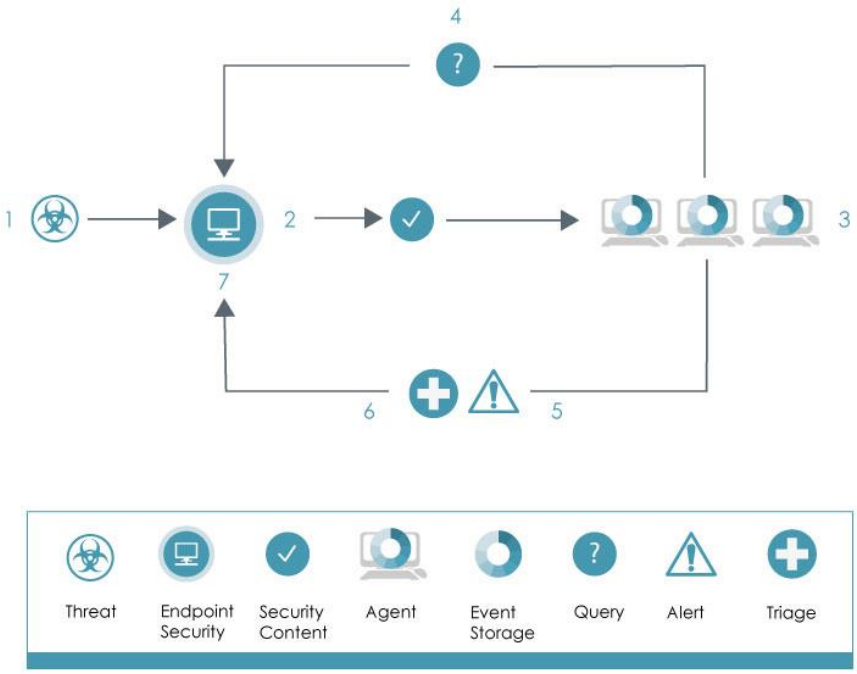
- Adaptive Sicherheit erfordert Echtzeitüberwachung aller Bedrohungsvektoren, einschließlich schnelle und genaue Bewertungen von möglichen Cyberangriffen, die auf Endpunktaktivität zurückzuführen sind. Der Endpoint Security Agent ermöglicht Ihnen, Cyberangriffe und Zero-Day Exploits auf dem Endpunkt zu erkennen, analysieren und darauf zu reagieren.
- In Windows Umgebungen können die Endpoint Security Produkte Exploit Guard auf Seite 24 verwenden, um Exploits und andere online Angriffe zu erkennen und zu verhindern, die während der Verwendung von Adobe Produkten wie z.B. Reader und Flash, Java, Browsern wie Microsoft Edge, Google Chrome und Mozilla Firefox sowie Microsoft Office Produkten wie Excel, Outlook, Powerpoint und Word auftraten.
- In Windows Umgebungen können die Endpoint Security Produkte Commodity Malware auf Ihren Host-Endpunkten erkennen und verhindern. Malware umfasst Viren, Tojaner, Würmer, Spyware, Adware, Keylogger, Rootkits, Phishing und andere potenziell unerwünschte Programme (PUP).

Der Endpoint Security Server verarbeitet Alarme von Indicators of Compromise (IOC), Exploit Guard (EXG), Anti-Virus (AV) und MalwareGuard (MG). Mit dieser Intelligenz ausgerüstet überwacht Endpoint Security Agent Aktivitäten auf jedem Endpunkt-Host, sammelt Echtzeit-, Exploit- und Malware-Daten von Ereignissen auf dem Endpunkt und identifiziert Aktivitäten, die mit den Echtzeit-Indikatorregeln und FireEyes Exploit und Malware Intelligenz übereinstimmen. Übereinstimmungen werden an den Endpoint Security als ein Alarm für den betroffenen Host-Endpunkt gemeldet. Der Server kompiliert die Daten, die von den Agents im gesamten Unternehmen empfangen werden, und bietet eine ganzheitliche Ansicht der Daten in der Endpoint Security Web-UI. Wenn eine potenzielle Bedrohung erkannt wird, können Analysten und Administratoren die Endpoint

Security Software verwenden, um die Situation schnell zu beurteilen und, wenn nötig, Hosts einzudämmen und die Bedrohung unternehmensweit zu neutralisieren. Sie können auch den Endpoint Security Server verwenden, um detaillierte Daten von dem Agent zu erfassen und zu untersuchen. Wenn die Bedrohung schwerwiegend genug ist, können Sie den Server verwenden, um den Agent einzudämmen.

Im Allgemeinen werden alle Endpoint Security-Aufgaben in der Reihenfolge der eingehenden Aufgaben verarbeitet. Der Server und der Agent können Aufgaben parallel verarbeiten, allerdings werden alle Aufgaben für einen individuellen Agent nicht unbedingt der Reihe nach bearbeitet. Eindämmungsaufgaben werden allerdings ausdrücklich als Aufgaben mit hoher Priorität markiert und kommen allen Datenerfassungsaufgaben, wie z.B. Enterprise Search und Datenerfassungsanfragen zuvor.

Das folgende Diagramm zeigt den Informationsfluss zwischen Server und Agent:



1. Dynamic Threat Intelligence (DTI) bietet Sicherheitsinhalte für den Endpoint Security Server.
2. Der Server verteilt diesen Sicherheitsinhalt an die Agents.
3. Der Agent vergleicht den Sicherheitsinhalt mit der Aktivität im Ereignisspeicher.
4. Der Agent prüft regelmäßig nach neuen Sicherheitsinhalten mit dem Endpoint Security Server.
5. Wenn ein Agent einen Vorfall erkennt, benachrichtigt der Agent den Server.

6. Der Agent bereite eine Triagesammlung vor und meldet sich beim Server sowohl mit dem neuen Alarm als auch der automatisch generierten Triagesammlung zurück.
7. Der Server empfängt und verarbeitet die Triagesammlung.

Endpoint Security und Agent Endpoint Security Kompatibilität

Einige Endpoint Security Funktionen erfordern bestimmte Mindestversionen des FireEye Endpoint Security Agent. Diese Mindestversionen sind in der Dokumentation für jede Funktion im *Endpoint Security Agent Administrationshandbuch* und in diesem Handbuch beschrieben.

Endpoint Security Versionen 3.2 und später liefern keine FireEye Intelligenzdaten an Endpoint Security Agents vor Version 11.

FireEye Endpoint Security Agents können mit on-Premises, virtueller oder Cloud Endpoint Security bereitgestellt werden. Weitere Informationen über diese unterschiedlichen Endpoint Security Formfaktoren finden Sie im *Endpoint Security Server Deploymenthandbuch*.

In der folgenden Kompatibilitätstabelle werden die Mindestversionen der Endpoint Security Software angezeigt, die von Endpoint Security Agent Softwareversionen benötigt werden und auf hoher Ebene die Betriebssystem-Umgebungen identifiziert, die von jeder Agentversion unterstützt werden.

Agent Version	Mindestversion der Endpoint Security	Betriebssystem-Umgebungen		
		Windows	macOS	Linux
30	5.2	Ja	Yes	Ja

HINWEIS: FireEye empfiehlt, dass Sie Ihre Endpoint Security Software aufrüsten und bereitstellen, bevor Sie Ihre Endpoint Security Agent Software aufrüsten und bereitstellen.

Endpoint Security Funktionssupport nach Plattform

In der folgenden Tabelle zeigt den Betriebssystemsupport für die wichtigsten Endpoint Security Softwarefunktionen.

Funktion	Unterstützung der Betriebssystemplattform		
	Windows	macOS	Linux
Echtzeit-Indikatorerkennung	Ja	Ja	Ja
Benutzerdefinierte Indikatorerstellung	Ja	Ja	Ja[1]
Echtzeit-Indikatorerkennungsrichtlinie	Ja	Ja	Ja
Exploit Guard	Ja	Nein	Nein
Malware Schutz	Ja	Ja	Nein
Enterprise Suche	Ja	Ja	Ja[2]
Datenerfassung auf Seite 29	Ja	Ja	Ja
Dateierfassungen auf Seite 29	Ja	Ja	Ja
Triagen	Ja	Ja	Nein
Endpunkteindämmung	Ja	Ja	Ja[3]
Schutz vor Entfernung des Agent	Ja	Nein	Nein
Agent Proxy Unterstützung	Ja	Ja	Ja

[1]Endpoint Security Version 4.8 oder später unterstützt die Erstellung von benutzerdefinierten Indikatorregeln für Linux Bedingungen (nur Netzwerkereignisse).

[2]Endpoint Security Version 5.2 oder später und Agent Version 34 oder später unterstützt Enterprise Search für Linux Host-Endpunkte.

[3]Endpoint Security Version 5.2 oder später und Agent Version 34 oder später unterstützt Enterprise Search für Linux Host-Endpunkte.

Echtzeit-Indikatorerkennung

Intelligenz über Bedrohungsaktivitäten wird von FireEye gesammelt und den Endpoint Security Produkten als Indicator of Compromise (IOC) Regeln (auch Indikatorregeln oder IOC Regeln) über die FireEye Dynamic Threat Intelligence (DTI) Cloud zur Verfügung gestellt.

Überwachung von Echtzeit-Indikatoren verwendet FireEye Indikatorregeln, um viele verdächtige Aktivitäten zu erkennen, einschließlich der folgenden:

- Nicht-autorisierte Verwendung von gültigen Konten
- Verfolgung von Beweisen und Teildateien

- Command and Control Aktivität
- Bekannte und unbekannte Malware
- Verdächtiger Netzwerkverkehr
- Gültige Programme, die für bösartige Zwecke verwendet werden
- Nicht-autorisierter Dateizugriff

FireEye Indikatorregeln werden für Windows, macOS und Linux Endpunkte bereitgestellt.

Weitere Informationen finden Sie unter Intelligenz (Regel) Überblick auf Seite 215.

Eine Liste spezifischer Berechtigungen, die von Echtzeit-Indikatorerkennung überwacht wird, finden Sie unter "Legale Token und Typen" im *Endpoint Security REST API-Handbuch*.

Custom Indicator Creation (Benutzerdefinierte Indikatorerstellung)

Sie können benutzerdefinierte Indikatorregeln erstellen, die Bedrohungen identifizieren, die Sie in Ihrer eigenen Umgebung identifiziert haben, z. B. die Einrichtung bestimmter Netzwerkverbindungen, DNS Suchen und die Erstellung oder Änderung von bestimmten Dateien. Die Kombination aus FireEye Indikatorregeln und Ihren benutzerdefinierten Indikatorregeln bildet den vollständigen Satz von Echtzeit-Indikatorregeln, die von Endpoint Security Agents für Echtzeit-Indikatorüberwachung verwendet werden.

WICHTIG: Endpoint Security Version 4.8 oder später unterstützt die Erstellung von benutzerdefinierten Indikatorregeln für Linux Bedingungen (nur Netzwerkereignisse).

Weitere Informationen finden Sie unter IOC Regeln verwalten auf Seite 221.

Echtzeit-Indikatorrichtlinie

Sie können die Endpoint Security verwenden, um eine benutzerdefinierte Richtlinie zu erstellen, die Agent Standardrichtlinie zu bearbeiten oder bestimmte Dateien und Ordner aufzulisten, die von der Echtzeit-Indikatorerkennung ausgeschlossen sein sollen. Wenn diese Richtlinie aktiviert ist, sind die angegebenen Dateien und Ordner von Echtzeit Indikatorerkennung ausgeschlossen.

HINWEIS: Sie können einem Hostsatz eine benutzerdefinierte Richtlinie zuweisen. Die Standardrichtlinie des Agent gilt für alle Hosts. Weitere Informationen über Richtlinien finden Sie im *Endpoint Security Agent Administrationshandbuch*.

FireEye Indikatorregeln werden für Windows, macOS und Linux Endpunkte bereitgestellt.

Exploit Guard

FireEye Endpoint Security kann Ihre Host-Endpunkte nach zuvor nicht erkannten Exploits und anderen online-Angriffen mit Hilfe einer Funktion mit dem Namen *Expoit Guard* überwachen, die sowohl Expoit Erkennung als auch Prävention bietet.

Exploit *Erkennung* deckt Exploit Verhalten auf Ihren Host-Endpunkten auf, das während der Verwendung von Adobe Reader, Adobe Flash, Microsoft Edge, Firefox, Chrome, Java, und Microsoft Office Anwendungen wie Word, Excel und PowerPoint auftritt. Nachfolgend finden Sie Beispiele der Exploit Typen, die in dieser Anwendung erkannt werden können.

- Return Oriented Programming (ROP) Angriffe
- Reverse Shell Versuche in Windows Umgebungen
- Heap Spray Angriffe
- Durch Exploits verursachte Anwendungsabstürze
- Structured Exception Handling Overflow Protection (SEHOP) Beschädigung
- Drive-by Downloads von Programmen
- Nullseiten-Exploits
- Microsoft Office Makro-basierte Exploits
- Java Exploits
- Erkennung der Eskalation von Privilegien für Zugriffstoken
- First Stage Shellcode Erkennung

Exploit *Prävention* kann überwachte Anwendungen, die von einem Exploit betroffen sind, blockieren, beenden und sogar unter Quarantäne stellen. Endbenutzer können benachrichtigt werden, wenn ein Exploit verhindert wird. Standardmäßig ist Exploit Erkennung aktiviert und Exploit Prävention ist nicht aktiviert.

Exploit Guard speichert seine Intelligenz in einer Regeldatei und verwendet eine Ausschlussdatei, um allgemeine Dateien zu identifizieren, die von Exploit Guard Verarbeitung ausgeschlossen sein sollen. Diese Dateien werden nur von FireEye bereitgestellt und verwaltet. Die neuesten Dateien können von der DTI Cloud heruntergeladen werden.

WICHTIG: Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

Exploit Erkennung wird für Windows Endpunkte unterstützt, die FireEye Endpoint Security Agent Version 21 oder später ausführen. Exploit Prävention wird für Windows Endpunkte unterstützt, die FireEye Endpoint Security Agent Version 22 oder später ausführen.

Sie können die Endpoint Security verwenden, um Richtlinien zu erstellen, die Exploit Guard Verhalten festlegen und die Richtlinien auf Hostsätze anwenden. Zusätzliche Informationen über Exploit Guard Verarbeitung und Einstellung dieser Richtlinien finden Sie im *Endpoint Security Agent Administrationshandbuch*.

Malware Schutz

Malware Schutz schützt Ihre Host-Endpunkte vor Viren, Trojanern, Würmern, Spyware, Adware, Keyloggern, Rootkits, Phishing-Software und anderen potentiell unerwünschten Programmen (PUP).

HINWEIS: Standardmäßig sind Signature and Heuristic Detection (Beseitigung und Quarantäne) sowie MalwareGuard deaktiviert. Wenn diese Funktionen deaktiviert sind, tritt kein Malware Schutz auf. MalwareGuard kann unabhängig von Signature and Heuristic Detection aktiviert werden. Allerdings muss Signature and Heuristic Dectection aktiviert sein, bevor Malware Schutz und geplante Malware Scans stattfinden können.

Malware Schutz erkennt und verhindert Malware automatisch in jeder Datei in Ihrer Umgebung in Echtzeit für alle Dateitypen mit Hilfe von zwei Erkennungsengines.

- Signature and Heuristic Detection (AV) Engine—Die AV Engine scannt Dateien beim Eintreffen auf Ihrem Endpunkt. Wenn Malware entdeckt wird, wird der Scanvorgang auf der Datei abgebrochen und wenn Quarantäne aktiviert ist werden Schutzaktionen ausgeführt.
- MalwareGuard—Wenn die AV Engine keine Malware entdeckt wird die Datei an MalwareGuard für einen Scan eingereicht, wenn dies aktiviert ist. Wenn Malware entdeckt wird, wird der Scanvorgang auf der Datei abgebrochen und wenn Quarantäne für MalwareGuard aktiviert ist werden Schutzaktionen ausgeführt.

Unterstützte Malware Scantypen

Sowohl On-Access als auch On-Demand (geplante) Malware Scans werden unterstützt.

- On-Access Malware Scans treten auf, wenn Dateien erstellt, ausgeführt oder geöffnet werden. Zu den erstellten Dateien gehören Dateien, die von einem Internet Browser heruntergeladen wurden, neue, auf dem Host durch einen beliebigen Prozess erstellte Dateien, aus Archiven extrahierte Dateien und Dateien, die durch Kopieren und Einfügen erstellt wurden. Ausgeführte Dateien sind Dateien, die einen Prozess starten. Geöffnete Dateien umfassen vorhandene Dateien, die in einem Browser von Medien wie z.B. einem USB- oder CD / DVD-Laufwerk und von Netzwerkordnern geöffnet wurden.

- On-Demand Malware Scans (geplant) können nach Zeit oder Ereignis geplant werden. Vollständige Scans, Kurzscans und Speicherscans (die laufende Prozesse scannen) können angefordert werden. Neue Scans werden nicht ausgeführt, wenn ein zuvor geplanter Scan noch läuft. Je nachdem, wie Sie die Einstellungen Ihrer Malware Scans konfigurieren, können Endbenutzer einen laufenden, geplanten Scan anhalten oder abbrechen.

Geplantes Scanverhalten

Die folgende Tabelle zeigt, wie geplante Scans auf bestimmte festgelegte Ereignisse auf der Host Maschine reagieren.

Ereignisse	Scan Status	Scan Verhalten
Herunterfahren	Geplant	Diesen Scan überspringen
Herunterfahren	In Bearbeitung	Diesen Scan überspringen
Ruhezustand	Geplant	Scan beginnt, wenn das System wieder läuft
Ruhezustand	In Bearbeitung	Scan beginnt, wenn das System wieder läuft
Energiesparmodus	Geplant	Scan beginnt, wenn das System wieder läuft
Energiesparmodus	In Bearbeitung	Scan beginnt, wenn das System wieder läuft
Die lokale Uhrzeit des Host ändern	Geplant	Geplanter Scan berücksichtigt die aktuelle Zeiteinstellung. Wenn diese Zeit so geändert wird, dass die Startzeit nach dem geplanten Scan liegt, wird der Scan übersprungen. Ansonsten läuft der Scan zur geplanten Zeit.
Die lokale Uhrzeit des Host ändern	In Bearbeitung	Scan fährt ununterbrochen fort.

Beschränkungen für Dateigröße

In der folgenden Tabelle sind die standardmäßigen Beschränkungen für Dateigröße für das Scannen aufgeführt. Sie können die maximale Dateigröße über die API anpassen.

Scan Type	AV Engine	MalwareGuard Engine
On-Access Scan	2 GB	5 MB
Geplanter Scan	2 GB	100 MB

Malware Beseitigungsaktionen

Wenn Malware erkannt wird, wird eine Malware Warnung generiert, die in der Endpoint Security Web-UI sichtbar ist. Je nach den Einstellungen Ihres konfigurierbaren Malware Schutzes können Sie anfordern, dass die folgenden Korrekturmaßnahmen durchgeführt werden.

- Die infizierte Datei wird automatisch in einen Quarantänebereich unter Quarantäne gestellt, wenn Sie Maßnahmen zur Fehlerbehebung (Quarantäne) aktivieren. Quarantänedateien werden in einem Quarantänebereich gespeichert und nach einer konfigurierbaren Alterungszeit gelöscht. Dateien, die unter Quarantäne gestellt werden, sind isoliert, so dass sie bösartigen Code nicht an andere Dateien oder Anwendungen auf den Endpunkten in Ihrer Umgebung weiterleiten können. Sie können Dateien auch aus der Quarantäne zur Analyse abrufen.
- Wenn die Infektion infizierten Code an Benutzerdateien angehängt hat, wird versucht, die Infektion aus den Dateien zu entfernen. Wenn der Versuch, die Dateien zu bereinigen fehlschlägt, bleiben die Dateien auf dem Endpunkt. Diese Dateien können zur Analyse erfasst werden.
- Wenn die Infektion neue Dateien auf den Endpunkt eingebracht hat, wird versucht, sie zu löschen Wenn die infizierten Dateien gesperrt sind und nicht ohne Neustart des Endpunktes gelöscht werden können, wird eine Benachrichtigung auf dem Endpunkt angezeigt.
- Die FireEye Malware Schutz Engine kann Artefakte entfernen, die von der Malware erstellt wurden und Änderungen zurücksetzen, die Malware auf anderen Dateien oder Verzeichniseinträgen vorgenommen hat. Dies wird als Entfernen von Malware Spuren bezeichnet.
- Benachrichtigungen auf dem Endpunkt informieren Sie darüber, wenn Korrekturmaßnahmen stattfinden.

Die vom Endpoint Security verwendeten Quell-Malware Definitionen werden von FireEye Servern heruntergeladen, die eine direkte Internetverbindung benötigen. Sie sind nicht in der Dynamic Threat Intelligence (DTI) Cloud von FireEye verfügbar.

- Aktualisierungen der Malware Definition benötigen eine direkte Internetverbindung mit den FireEye Malware Definitionsservern. Für Updates für Host-Endpunkte, die offline oder im lokalen Modus ausgeführt werden, können Sie die Quell-Definition auf einen lokalen Speicherort speichern und dann die Custom Source Download-

Option verwenden.

- Aktualisierungen der Malware Definition über den Proxyserver werden in FireEye Endpoint Security Agent Version 25 oder später unterstützt.
- Updates für Malware Definitionen werden nicht ausgeführt, wenn die CONTENT_ UPDATES Lizenz für Ihren Endpoint Security abgelaufen ist.
- Malware Erkennung wird nur für Host Endpunkte mit installierter FireEye Endpoint Security Agent Version 24 oder später bereitgestellt. Malware Beseitigung wird nur für Host-Endpunkte mit installierter FireEye Endpoint Security Agent Version 26 oder später bereitgestellt

:**HINWEIS** Malware Erkennung wird für Endpoint Security Agents unterstützt, die Version 24 oder später in spezifischen Windows Umgebungen ausführen, sowie Version 32 oder später in .macOS Umgebungen und Version 34 für Linux Umgebungen

Malware Beseitigung (Quarantäne) wird für FireEye Endpoint Security Agents unterstützt, die Version 26 oder später in bestimmten Windows Umgebungen ausführen.

MalwareGuard wird für FireEye Endpoint Security Agents unterstützt, die Version 27 oder später ausführen.

In regelmäßigen Zeitabständen werden jetzt falsch positiv Informationen über Malware Bedingungen automatisch von der FireEye Dynamic Threat Intelligence (DTI) Cloud auf den Endpoint Security heruntergeladen. Wenn FireEye Endpoint Security Agents den Server abfragen, werden die falsch positiv Daten automatisch auf die Endpunkte angewendet. Vorhandene Alarme auf dem Endpoint Security, die mit den falsch positiv Bedingungen übereinstimmen, werden als falsch positiv markiert.

WICHTIG: Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

Sie können für Ihre Organisation spezifische Richtlinien und Einstellungen für den Malware Schutz definieren. Weitere Informationen finden Sie im *Endpoint Security Agent Administrationshandbuch*.

FireEye Endpoint Security Agent Version 26 oder später sind für den Beitritt zur Microsoft Virus Initiative (MVI) zertifiziert und mit dem Windows Security Center (WSC) integriert. Dies bedeutet, dass FireEye Endpoint Security ein zertifiziertes und unterstütztes Antiviren- und Anti-Spywareprodukt für bestimmte Windows Betriebssysteme ist.

Die FireEye Malware Schutz-Engine wird nur im WSC angezeigt, wenn die Malware Erkennung, Dateiquarantäne und On-Access Malware Scans aktiviert sind. Die **Turn on**

now Schaltfläche im WSC ist, wenn sie angezeigt wird, nicht für die FireEye Malware Schutz-Engine funktionsfähig, weil Malware Schutz vom Endpoint Security Administrator für alle Ihre Host-Endpunkte oder für ausgewählte Hostsätze mit Hilfe der Endpoint Security Web-UI oder API aktiviert wurde.

Enterprise Search

Mit Hilfe der Enterprise Searches in der Endpoint Security können Sie nach Bedrohungen oder Bedrohungsindikatorregeln auf Ihren Windows und macOS Host-Endpunkten suchen, wenn sie FireEyeEndpoint Security AgentVersion 20 oder später ausführen und Linux Host-Endpunkten, die Endpoint Security Agent Version 34 oder später ausführen. Die in Ihrer Umgebung gezeigte Funktionalität ist je nach der Rolle verschieden, die Ihrem Benutzerkonto zugewiesen wurde und basiert auf den FireEye Lizenzen, die Sie installiert haben.

Weitere Informationen finden Sie unter Ihr Unternehmen durchsuchen auf Seite 253.

Datenerfassung

Mit Datenerfassungen können Sie benötigte Daten von einem einzigen laufenden Endpunkt erfassen. Daten werden über Datenerfassungsscripts angefordert, die mit Hilfe der Endpoint Security Web-UI verwaltet werden. Wenn eine Datenerfassungsanfrage getätigt wird, sammelt der Agent auf dem ausgewählten Host Endpunkt die von dem Datenerfassungsscript angeforderten forensischen Daten.

Datenerfassungen können für Windows-, macOS- und Linux-Endpunkte angefordert werden. Die für die Anforderung verfügbaren Daten sind je nach Plattform unterschiedlich.

Weitere Informationen finden Sie unter Eine Datenerfassung anfordern auf Seite 321.

Dateierfassungen

Um potenzielle Kompromittierungen zu überprüfen und schnell darauf zu reagieren, können Sie Dateien direkt von einem Host Endpunkt erhalten. Dateierfassungen werden für statische oder dynamische Analyse von potentiellen oder bestätigten Kompromittierungen verwendet, sowie für die Aufbewahrung von Beweisen bei Insider Bedrohungsermittlungen. Verwenden Sie Dateierfassungsanfragen, um einen Agent anzuweisen, eine Datei von ihrem Host Endpunkt abzurufen.

Dateierfassungen können von Windows, macOS und Linux Endpunkten angefordert werden.

Weitere Informationen finden Sie unter Dateierfassungen anfordern auf Seite 315.

Triagen

Sie können Triage-Sammlungen von Hosts mit Hilfe der Endpoint Security Web-UI erfassen. Triage-Sammlungen bieten eine Momentaufnahme der Ereignisse, die auf einem Host-Endpunkt zum Zeitpunkt einer Warnung aufgetreten sind.

Mehrere Triagen können gleichzeitig von einem Host angefordert werden. Zusätzlich können Sie mehrere Hosts auswählen und Triage-Sammlungen von ihnen anfordern.

Sie können Triagen für Ihre Windows, macOS und Linux Endpunkte ausführen.

HINWEIS: Triagen können für Linux Endpunkte durchgeführt werden, die Endpoint Security Agent Version 30 oder später ausführen.

Weitere Informationen finden Sie unter Triageerfassungen anfordern auf Seite 319.

Endpunkteindämmung

Die Endpunkteindämmung ist eine leistungsstarke Waffe, um weitere Kompromittierungen durch einen Endpunkt zu verhindern. Eingedämmte Endpunkte werden von der Kommunikation mit anderen Host-Endpunkten in Ihrem Unternehmen blockiert und können nur mit dem Endpoint Security und DMZ-Server kommunizieren, der sie verwaltet und allen anderen Hosts, die Sie in der Containment-Whiteliste definiert haben. Sie können die Eindämmungsfunktion mit Hilfe der Endpoint Security Web-UI abrufen und steuern.

Informationen über die Konfigurierung von Endpunkt-Eindämmung durch die Endpoint Security Web-UI finden Sie unter Eindämmung konfigurieren auf Seite 155 und Überblick über Eindämmung auf Seite 421.

Endpoint Security Agent Entfernungsschutz

Sie können verhindern, dass Ihre FireEye Endpoint Security Agents von Ihren Host-Endpunkten gelöscht werden, indem Sie ein Passwort für die Löschung fordern. Sie können Agent Löschschutz aktivieren und deaktivieren, Ihr Passwort für die Agent Löschung festlegen und Hostsätze identifizieren, für die das Passwort für Agent Löschung nicht erforderlich ist. Diese Einstellung kann für alle Ihre Host-Endpunkte oder für ausgewählte Hostsätze mit Hilfe der Endpoint Security Web-UI oder API festgelegt werden.

Agent Entfernungsschutz wird nur für FireEye Endpoint Security Agents unterstützt, die auf Windows Endpunkten ausgeführt werden. Linux oder macOS Endpunkte werden nicht unterstützt.

Weitere Informationen finden Sie im *Endpoint Security Agent Administrationshandbuch*.

Verwendung des Endpoint Security Agent Proxy

Der Endpoint Security Agent kann für die Verwendung eines HTTPS Proxyserver für den Zugriff auf den Endpoint Security oder das Internet konfiguriert werden. Sie können die Verwendung eines Proxys aktivieren oder deaktivieren und angeben, wo die Proxy Einstellungen abgerufen werden sollen, oder die Proxy Einstellungswerte manuell festlegen.

Proxy-Einstellungen werden nur für FireEye Endpoint Security Agents unterstützt, die Version 25 oder später ausführen. Sie können für alle Ihre Host-Endpunkte oder für ausgewählte Hostsätze mit Hilfe der Endpoint Security Web-UI oder API festgelegt werden.

Wenn Ihr Unternehmen einen HTTPS Proxyserver verwendet, konfigurieren Sie seine Einstellungen, bevor Sie die Endpoint Security Agent Software auf Ihren Host-Endpunkten installieren.

HINWEIS: Endpoint Security Agent Versionen 30 oder später bieten Host-Eindämmung über Proxy-Support für Windows und macOS Endpunkte.

Der Web-Datenverkehr wird nicht für Endpoint Security Agent Versionen 27 oder früher blockiert, die auf eingedämmten Windows-Endpunkten ausgeführt werden, die einen Proxyserver für die Kommunikation mit dem Endpoint Security verwenden.

Host-Eindämmung funktioniert nur auf der IP-Protokoll Ebene. Wenn Ihre Windows oder macOS Host Endpunkte, die Endpoint Security Agent Versionen 27 oder früher ausführen, einen Proxy-Server verwenden, der zur Containment-Whiteliste hinzugefügt wurde, kann ein eingedämmter Windows oder macOS Host immer noch Web-Datenverkehr und anderen Verkehr senden und empfangen. Wenn Sie ein Agent Proxy verwenden und kompromittierte Hosts eindämmen wollen, müssen Sie den Proxyserver mit einer separaten IP-Adresse einstellen, die nur zum Erreichen des Endpoint Security verwendet werden kann. Verwenden Sie die Endpoint Security Web-UI, um die IP-Adresse des Proxyservers zu den Allowed IP-Adresses auf der **Containment Settings** Seite hinzuzufügen.

Weitere Informationen finden Sie im *Endpoint Security Agent-Deploymenthandbuch* und *Endpoint Security Agent Administrationshandbuch*.

KAPITEL 2: Die Endpoint Security Web-UI

Die Endpoint Security Web-UI benutzt HTTPS, um eine sichere Verbindung für die Konfiguration des Servers zu liefern. Die Web-UI Funktionen, auf die Sie Zugriff haben, hängen von den Ihrer Rolle zugestandenen Berechtigungen ab.

Sie greifen auf die Web-UI zu, indem ein Browser mithilfe von HTTPS an die IP-Adresse oder den Hostnamen des Management-Ports geleitet wird. Die IP-Adresse und der Hostname werden während der Erstkonfiguration des Servers festgelegt. Der Hostname muss von einem DNS-Server aufgelöst werden, wenn Sie ihn für den Zugriff auf die Web-UI verwenden.

Wenn Sie sich auf der Helix Plattform befinden, deutet die Web-UI auch an, ob Helix Modus aktiviert ist und es sich bei Warnungen um Helix-Warnungen handelt. Details finden Sie im *Helix Administrationshandbuch*.

Browser Support

Verwenden Sie eine aktuelle Version der folgenden Webbrowser für den Zugriff auf die Web-UI:

- Microsoft Edge auf unterstützten Windows Versionen (Exploit Guard Verarbeitung wird auf Microsoft Edge nicht unterstützt.
- Google Chrome auf unterstützten Versionen von Windows und Macintosh
- Safari (macOS) wird nicht unterstützt.

Erfordernisse für Bildschirmauflösung

Die Endpoint Security Web-UI unterstützt die folgenden Bildschirmauflösungen:

1152 x 864 Pixel	1440 x 900 Pixel
1280 x 800 Pixel	1600 x 900 Pixel
1280 x 1024 Pixel	1680 x 1050 Pixel
1360 x 768 Pixel	1920 x 1080 Pixel
1366 x 768 Pixel	1920 x 1200 Pixel

Auf der Web-UI anmelden

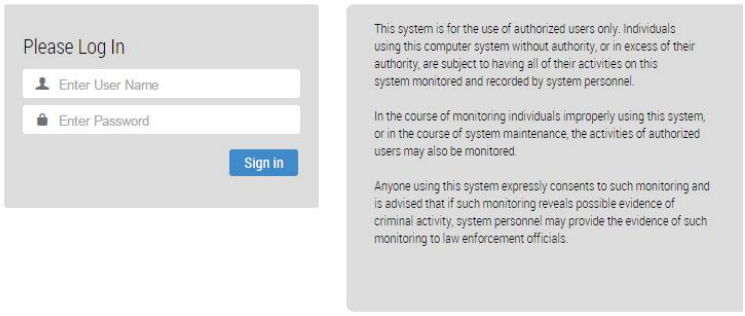
Um sich auf der Endpoint Security Web-UI anzumelden, benötigen Sie die Server IP-Adresse oder den Hostnamen sowie den Usernamen und das Passwort, dass der Server-Administrator für Sie erstellt hat.

Voraussetzungen

- Um auf die HX Web-UI zuzugreifen, müssen Sie Port 3000 verwenden.
- Bevor sich der Standard Admin User auf der Endpoint Security Web-UI anmelden und andere Benutzerkonten erstellen kann, muss das Standard-Passwort des Herstellers (`admin`) auf ein neues Passwort geändert werden, das 8 bis 32 Zeichen lang ist. Dieser Schritt ist in "Erstkonfiguration" im *System-Administrationshandbuch* enthalten.
- Wenn Sie Single Sign-On verwenden, finden Sie in Ihrer Begrüßungsmail Anweisungen zur Anmeldung bei Ihrer Cloud IAM-Instanz.

Um sich auf der Endpoint Security Web-UI anzumelden:

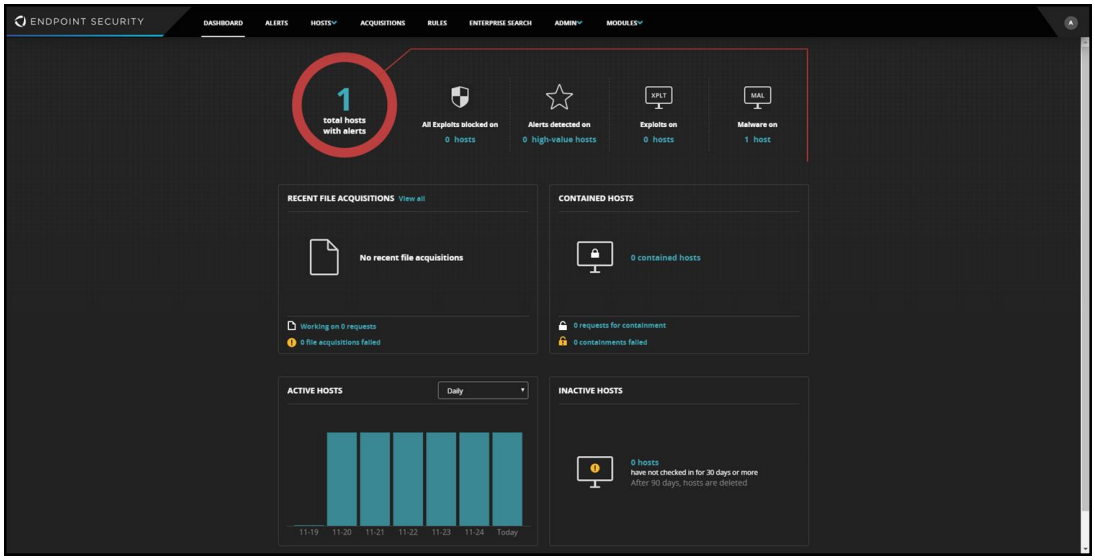
1. Öffnen Sie einen Webbrowser und geben Sie **`https://<server>`** in der Adressenzeile ein, wobei `server` die IP-Adresse oder der Hostname des Servers ist. Wenn die konfigurierte IP-Adresse des Servers zum Beispiel 10.1.0.1 ist, geben Sie **`https://10.1.0.1`** ein.
2. Geben Sie den von Ihrem Administrator bereitgestellten Usernamen und das Passwort für diesen Server auf der Web-UI Anmeldeseite ein.



Auf einem Endpoint Security mit aktiviertem single Sign-on werden Sie möglicherweise auf die Cloud IAM Anmeldeseite weitergeleitet. Ihre Anmeldeerfahrung hängt von dem für den Server eingestellten Authentifizierungsmodus ab. Weitere Informationen finden Sie unter "Single Sign-On-Authentifizierung" im *System Security Handbuch*.

Info über Endpoint Security Web-UI

Die Endpoint Security Web-UI enthält die Tools, die Sie für die Verwaltung von Netzwerkbedrohungen benötigen.

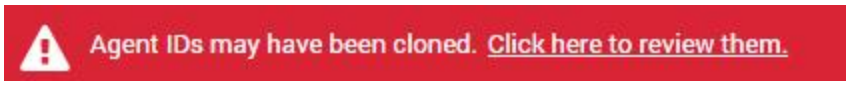


In diesem Abschnitt werden wichtige Aspekte der Web-UI beschrieben.

- Richtlinieneinstellungen auf Seite 85
- Agent Upgrade Seite auf Seite 86
- Containment Settings Seite auf Seite 86
- Acquisition Settings Seite auf Seite 88
- Data Acquisition Scripts Seite auf Seite 90
- Disk Utilization Limits Seite auf Seite 91
- Aging Settings Seite auf Seite 92
- Appliance Settings Seite auf Seite 94
- Modules Menü auf Seite 96

HINWEIS: Die in Ihrer Web-UI Umgebung gezeigte Funktionalität ist je nach der Rolle verschieden, die Ihrem Benutzerkonto zugewiesen wurde und basiert auf den FireEye Lizenzen, die Sie installiert haben.

Wenn die folgende Nachricht am oberen Rand der Web-UI Seite erscheint, sehen Sie Geklonte Agents auflösen für weitere Informationen.



Pivot Menü

Wenn Sie einen Endpoint Security mit aktiviertem single sign-on (SSO) verwenden, werden Pivot Optionen auf dem Dropdown-Menü unter Ihrem Usernamen angezeigt. Die verfügbaren Optionen hängen von der Konfiguration Ihrer Organisation ab. Über dieses Menü können Sie zu anderen Cloud Produkten wechseln, für die Ihnen Zugriff gewährt wurde.

Die folgende Tabelle enthält eine Liste möglicher Pivot-Menüoptionen.

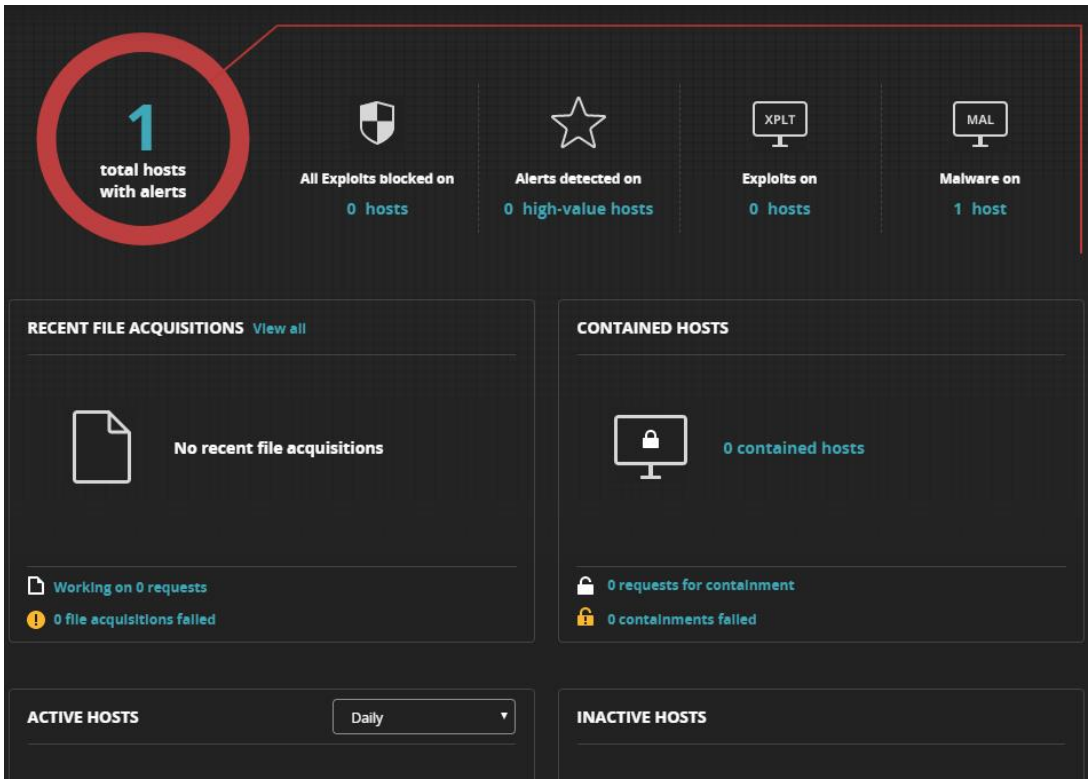
Menüoption	Beschreibung
Identity Access Management	Links auf die Cloud Identity Access Management (IAM) Web-UI. Von hier können Sie Ihr eigenes Konto verwalten (z.B. um Ihr Passwort oder Ihr Profilimage zu ändern. Wenn Sie ein Administrator für Ihre Cloud Organisation sind, können Sie Organisationseinstellungen verwalten und Benutzermanagement ausführen.
Helix	(Optional) Links auf Ihre Helix Instanz. Diese Option wird nur angezeigt, wenn Ihr Endpoint Security mit der Helix Plattform integriert ist.
Log Out	Meldet Sie von allen verbundenen Instanzen ab, für die Ihre IAM Anmeldung Ihnen Berechtigungen gewähren.

Weitere Informationen zu Single Sign-On mit Cloud IAM finden Sie im *System-Sicherheitshandbuch*.

Dashboard

Wenn Sie sich zum ersten Mal auf dem Endpoint Security anmelden wird das Dashboard angezeigt. Sie können auch auf das Dashboard navigieren, indem Sie Dashboard vom Menü am overen Rand der Seite auswählen, oder indem Sie auf das FireEye Logo am Anfang der Seite klicken.

Das Dashboard zeigt wichtige Messwerte und Links an, um Ihnen den schnellen Zugriff auf Informationen über bedrohungsbezogene Aktivitäten auf Ihren Hosts zu erleichtern.



Das Dashboard enthält eine Anzahl verschiedener Abschnitte. Die Zahlen in Blau können ausgewählt werden. Weitere Informationen zu Benutzerrollen und Authentifizierung finden Sie im *Endpoint Security Server-System-Administrationshandbuch*.

Voraussetzungen

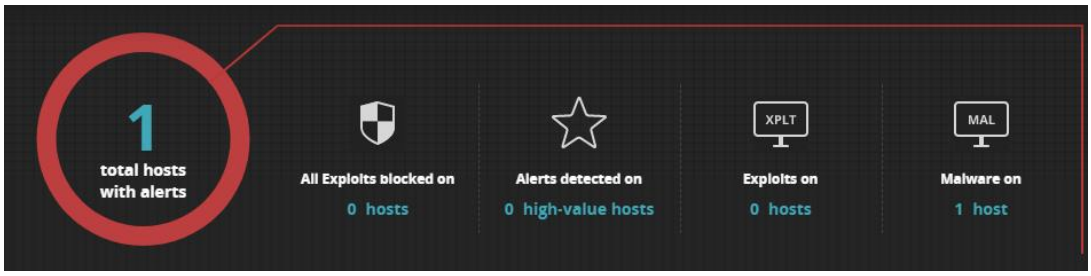
- Admin, Analyst, Senior Analyst oder Investigator Privilegien (vollständiger Zugriff)
- Operator Privilegien (nur Lesezugriff)

Die Seite aufrufen

Um das Dashboard aufzurufen, klicken Sie auf das FireEye Logo am Anfang der Seite.

Alerts

Der Alerts Abschnitt ist der oberste Abschnitt des Dashboards und zeigt Informationen über Warnungen an, die auf Ihrem Netzwerk ausgelöst wurden.



Der Alerts Abschnitt zeigt die Informationen in der folgenden Tabelle an. Klicken Sie auf eine der Zahlen in diesen Feldern, um auf die Hosts Seite zu springen, nach Ihrer Auswahl gefiltert.

Symbol	Feld	Beschreibung
---	Total hosts with alerts	Die Gesamtzahl der Hosts mit Warnungen.
	Exploit blocks on	Die Anzahl der Hosts, auf denen Exploits verhindert (blockiert) wurden.
	Alerts detected on	Die Anzahl der hochwertigen Hosts mit Warnungen.
	Exploits on	Die Anzahl der Hosts, auf denen Exploits erkannt wurden. Beachten Sie, dass die Anzahl der Exploits, die verhindert (blockiert) wurden, in den Exploit Alert Zählungen enthalten ist.
	Malware on	Die Anzahl der Hosts, auf denen Alarme für Malware Erkennungs ausgelöst wurden.

Die Auswahlen für Exploit (und) und Malware ( ) Warnungszählung werden auf dem Dashboard angezeigt, selbst wenn Exploit Guard oder Malware Erkennung ausgeschaltet sind.

Recent File Acquisitions

Der **Recent File Acquisitions** Abschnitt bietet Informationen über die neuesten Dateierfassungen, einschließlich die Anzahl der laufenden Erfassungsanfragen und die Anzahl der fehlgeschlagenen Erfassungsanfragen. Klicken Sie auf eine beliebige Zahl in diesem Abschnitt, um auf die nach Ihrer Auswahl gefilterte Acquisitions Seite auf Seite 73 Seite zu springen.

Wenn eine aktuelle Erfassung angezeigt wird, klicken Sie auf **Download** um die Erfassung auf Ihren Computer herunterzuladen. Sie auch auf **View Details** klicken, um kurze Details über die Erfassung zu sehen.

Klicken Sie auf **View All**, um alle Dateierfassungen zu sehen. Triage Erfassungen sind in dieser Liste nicht enthalten. Um alle Erfassungen, einschließlich Triage Erfassungen anzuzeigen, wählen Sie **Acquisitions** vom FireEye Menü.

Contained Hosts

Der **Contained Hosts** Abschnitt zeigt die Anzahl der eingedämmten Hosts, einschließlich der Anzahl von Eindämmungsanfragen und die Anzahl von fehlgeschlagenen Eindämmungsanfragen. Klicken Sie auf die Zahlen in diesem Abschnitt, um auf die nach Ihrer Auswahl gefilterte Hosts Seite zu springen.

Active Hosts

Der **Active Hosts** Abschnitt zeigt die Anzahl der Hosts auf dem Netzwerk über einen anpassbaren Zeitraum hinweg an. Mit Hilfe dieses Abschnitts können Sie einen unerwarteten Abfall in der Konnektivität zwischen Hosts und dem Endpoint Security erkennen.

Inactive Hosts

Der **Inaktive Hosts** Abschnitt zeigt die Anzahl der überwachten Hosts in Ihrem Netzwerk an, die seit mindestens 30 Tagen nicht mehr eingecheckt haben.

Mobile Devices

Der Mobile Devices Abschnitt zeigt die Anzahl der mobilen Geräte in Ihrem Netzwerk und die Anzahl der Geräte an, die nicht mit Ihrer Netzwerkrichtlinie übereinstimmen.

Der Mobile Device Abschnitt ist nur verfügbar, wenn der Mobile Threat Protection (MTP) Service in Ihrem Netzwerk aktiv ist und mit Ihrer Endpoint Security Software verbunden ist. Für weitere Informationen über den MTP Service wenden Sie sich an Ihren FireEye Vertriebsmitarbeiter.

Hosts Menü

Die Hosts Seite ermöglicht Ihnen, alle vom Endpoint Security überwachten Endpunkt-Hosts anzuzeigen und alle Hosts mit Alarmen schnell zu identifizieren. Im Hosts Menü können Sie alle Informationen über alle Hosts oder nur die Hosts mit Alarmen anzeigen. Wenn Sie das Host Management Modul installiert und aktiviert haben, können Sie auch den Integritätsstatus aller Agents auf Ihrem Netzwerk anzeigen. Sie können dieses Menü als den zentralen Punkt Ihres hostbasierten Workflows verwenden.

Dieses Menü enthält die folgenden Seiten:

- Die **Host Management** Seite wird nur angezeigt, wenn Sie das Host Management Modul installiert und aktiviert haben. Diese Seite bietet detaillierte Informationen über den aktuellen Zustand Ihrer Agents.
- Die **Hosts with Alerts** Seite führt alle Host-Endpunkte mit Alarmen auf. Eine Warnung ist eine Übereinstimmung zwischen einer Indikatorbedingung oder Malware Infektion und dem Nachweis potentiell bösartiger Aktivitäten auf dem Host.
- Die **All Hosts** Seite führt alle Host-Endpunkte auf, die vom Endpoint Security überwacht werden. Die Anzahl der unter Quarantäne stehenden und bereinigten Dateien auf den Endpunkten wird ebenfalls angezeigt.

Bei einem Host-Endpunkt handelt es sich um einen Computer, Server oder andere verwandte Unternehmenskomponente, auf der die FireEye Endpoint Security Agent Software installiert ist.

Dieser Abschnitt beschreibt die Komponenten und Verwendung des Hosts Menüs:

- Zugriff auf die Hosts Seiten unten
- Host Management Seite unten
- All Hosts Seite auf Seite 51
- Hosts with Alerts Seite auf Seite 45
- Scan-Zusammenfassung auf Seite 63
- Host Details auf Seite 65

Voraussetzungen

- Admin, Analyst, Senior Analyst oder Investigator Privilegien (vollständiger Zugriff)
- Operator Privilegien (nur Lesezugriff)

Zugriff auf die Hosts Seiten

Um auf die Hosts Seiten zuzugreifen, wählen Sie **Hosts** am Anfang der Seite und klicken Sie auf **Host Management**, **Hosts with Alerts** oder **All Hosts**.

Host Management Seite

Die Host Management Seite wird nur im Hosts Menü angezeigt, wenn Sie das Host Management Modul installiert und aktiviert haben. Sie können die Host Managment Seite verwenden, um die Integrität Ihre Host-Endpunkte, die Endpoint Security Agent Software ausführen, anzuzeigen und zu verwalten. Sie können die Host Management Seite auch verwenden, um Filtersätze auf Ihren Host-Endpunkten zu erstellen und zu verwalten.

Weitere Informationen über Filtersätze finden Sie unter Einen Standardsatz mit Hilfe von Filtern erstellen auf Seite 192.

Die Host Management Seite zeigt den aktuellen Status verschiedener Agent Komponenten an, so dass Sie feststellen können, ob ein Agent fehlerfrei oder fehlerhaft ist. Die Host Management Seite enthält ein Details Tab und ein Raw Sysinfo Tab, die Informationen über ausgewählte Host-Endpunkte bieten.

Die folgende Tabelle führt alle Informationsspalten für die Host Management Seite auf. Einige der in der folgenden Tabelle aufgeführten Spalten werden standardmäßig nicht angezeigt. Allerdings können Sie das Columns Tool verwenden, das sich in der oberen rechten Ecke der Web-UI befindet, um zusätzliche Spalten zum Host Management Raster hinzuzufügen.

Spaltenname	Beschreibung
Endpoint Agent ID	Einzigartige System-generierte Kennung für den Host-Endpunkt.
Server Time	Das aktuelle Datum und Uhrzeit auf dem Serverstandort.
Hostname	Der Hostname des Host-Endpunkts.
Online Status	Der aktuelle Status des Agent. Gültige Werte sind Online, Offline und All.
Operating System	Der vollständige Name des Betriebssystems, der auf dem Host ausgeführt wird.
Patch	Der neueste Patch, der auf das auf dem Host installierte Betriebssystem angewendet wurde.
Build	Die Build-Nummer des auf dem Host installierten Betriebssystems.
Logged on User	Die Usernamen der derzeit auf dem Host eingeloggten User.
Timezone	Die Zeitzone in der das Hostsystem installiert ist.
Last Check-in	Das Datum und die Uhrzeit, zu der der Agent seinen Status zuletzt gemeldet hat.
Agent Version	Die Version der Agent Software, die auf dem Host-Endpunkt ausgeführt wird.
Containment Status	Der Eindämmungsstatus des Host-Endpunkts.
Real Time	Der aktuelle Status von Real-Time Indicator Detection auf dem Host-Endpunkt. Gültige Werte sind Disabled, Degraded und OK.
Content Version	Die Version des Real-Time Indicator Detection Inhalts auf dem Host-Endpunkt.

Spaltenname	Beschreibung
Real Time Content Updated	Das Datum und die Uhrzeit, zu der Real-Time Indicator Detection Inhalt zuletzt aktualisiert wurde.
Exploit Guard	Der aktuelle Status von Exploit Guard auf dem Host-Endpunkt. Gültige Werte sind n/a, Enabled, Disabled, Running und Uninstalled.
EXD Content Version	Die Version von Exploit Guard Inhalt auf dem Host-Endpunkt.
EXD Engine Version	Die Versionsnummer der Exploit Guard Engine, die derzeit auf dem Host-Endpunkt installiert ist.
Malware Guard	Der aktuelle Status von Malware Guard auf dem Host-Endpunkt. Gültige Werte sind Enabled, Disabled, Running und Uninstalled.
Malware Guard Quarantine	Der aktuelle Status von Malware Guard Quarantine auf dem Host-Endpunkt.
Malware Guard Model	Die Modellnummer des derzeit auf dem Host-Endpunkt installierten Malware Guard.
Malware Guard Model Last Updated	Das Datum und die Uhrzeit der letzten Aktualisierung des Malware Guard Modells.
Malware Guard Engine Version	Die Versionsnummer der Malware Guard Engine, die derzeit auf dem Host-Endpunkt installiert ist.
Malware Guard Core Engine Version	Die Versionsnummer der derzeit auf dem Host-Endpunkt installierten Malware Guard Core Engine.
Malware Schutz	Der aktuelle Status von Malware Protection auf dem Host-Endpunkt. Gültige Werte sind Enabled, Disabled, Running und Uninstalled.
Signature and Heuristic Detection	Der aktuelle Status von Signature and Heuristic Detection auf dem Host-Endpunkt.
Sig and Heuristic Det Quarantine	Der aktuelle Status von Signature and Heuristic Detection Quarantine auf dem Host-Endpunkt.
Signature and Heuristic Version	Die Versionsnummer der derzeit auf dem Host-Endpunkt installierten Signature and Heuristic Detection.

Spaltenname	Beschreibung
AV Content Last Updated	Das Datum und die Uhrzeit der letzten Aktualisierung des Antiviren-Inhalts.
AV Engine Version	Die Versionsnummer des derzeit auf dem Host-Endpunkt installierten Antivirus.
Quarantine Actions	Die Quarantäneaktion, die für Malware auf dem Host-Endpunkt ergriffen wird.
FIPS	Der aktuelle FIPS Status auf dem Host-Endpunkt.
ProRemSvcStatus	Der aktuelle ProRemSvc Status auf dem Host-Endpunkt.
kernelServicesStatus	Der aktuelle kernelServices Status auf dem Host-Endpunkt.
Machine Name	Der Gerätenamen des Host Endpunkts.
Uptime	Die Zeitspanne in Tagen, Stunden, Minuten und Sekunden, die der Host-Endpunkt ausgeführt wurde.
Registered Org	Der Firmenname (falls vorhanden), der für den Host-Endpunkt registriert ist.
Registered Owner	Der registrierte Besitzer des Host-Endpunkts.
Platform	Der Plattformtyp des Host-Endpunkts. Gültige Werte sind Winm, Osx, Linux und All.
vmGuest	Zeigt an, ob vmGuest auf dem Host-Endpunkt gestattet ist oder nicht.
virtual	Der aktuelle Status von Virtuell auf dem Host-Endpunkt.
GMT Offset	Die GMC Zeitverschiebung des Host-Endpunkts.
Domain	Der Name der Domain, auf dem sich der Host-Endpunkt befindet.
Primary IPv4 Address	Die primäre IPv4 Adresse des Host-Endpunkts.
Primary IPv6 Address	Die primäre IPv6 Adresse des Host-Endpunkts.
Primary IP Address	Die primäre IP-Adresse des Host-Endpunkts.
MAC	Die Media Access Control (MAC) Adresse des Netzwerkadapters für den Host-Endpunkt.

Spaltenname	Beschreibung
Total Storage (GB)	Die Gesamtspeichermenge auf dem Host-Endpunkt.
Available Storage (GB)	Die Größe des auf dem Host-Endpunkt verfügbaren Speichers.
Process Tracker Status	Der aktuelle Status von Process Tracker auf dem Host-Endpunkt.
Process Tracker Version	Die Versionsnummer des derzeit auf dem Host-Endpunkt installierten Process Tracker.
Cloud Provider	Cloud Anbieter, auf dem Endpunkte gehostet werden.
Instance ID	Instance ID des Endpunkt-Systems.

Hosts with Alerts Seite

Die Hosts with Alerts Seite führt alle Host Endpunkte in Ihrem Unternehmen mit Alarmen auf. Eine Warnung ist eine Übereinstimmung zwischen einer Indikatorbedingung, einer Exploit Bedingung oder einer Malware Definition und dem Nachweis potentiell bösartiger Aktivität auf dem Endpunkt.

Filter By Dropdown Felder

Sie können die Daten in dem Raster auf dieser Seite mit Hilfe der Filter By Dropdown Felder filtern.

Mit Hilfe dieser Felder können Sie die Daten in dem Raster filtern.

- Verwenden Sie das **Alert type** Dropdown-Menü, um die Daten nach Warnungstyp zu filtern (All, XPLT, PRS, EXC oder MAL). Wenn ein Warnungstyp ausgewählt ist, wird der Hostraster nach Hosts mit *mindestens einem* des ausgewählten Warnungstyps gefiltert.

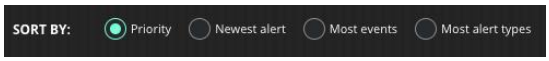
- Verwenden Sie das **Protection & Remediation** Dropdown-Menü, um die Daten nach dem Schutz- und Wiederherstellungsstatus zu filtern (All, Blocked, Quarantined, Cleaned, oder Not Blocked). Wenn **Blocked** ausgewählt ist, wird der Host Raster nach Hosts gefiltert, für die *alle* Warnungsbedingungen blockiert oder verhindert werden. Alternativ zeigt der **Not Blocked** Filter Hosts an, für die mindestens eine Warnungsbedingung nicht blockiert ist.

  Wenn **Quarantined** ausgewählt ist, wird das Host Raster nach Hosts gefiltert, für die alle Dateien, die Malware enthalten, isoliert wurden.

  Wenn **Cleaned** ausgewählt ist, wird das Host Raster nach Hosts gefiltert, für die *alle* Dateien, die Malware enthalten, bereinigt wurden. *Cleaning* bedeutet, dass das System versucht, Malware von einer Datei zu entfernen (z.B. eine bösartige Datei von einem .zip Archiv mit 10 Dateien entfernen). Wenn die bösartige Datei entfernt werden kann, wird der Rest der Eingaben nicht isoliert.
- Verwenden Sie das **Disposition** Dropdown-Menü, um die Daten nach Falsch Positiv Disposition zu filtern (all, False Positive oder Not False Positive). Wenn **False Positive** ausgewählt ist, ist ein Host in dem Raster eingeschlossen, wenn *alle* seine Warnungen (IOC, Exploit und Malware Warnungen) für eine Falsch Positiv Bedingung sind. Weitere Informationen darüber, wie Hosts nach Disposition gefiltert werden, finden Sie unter Info über Falsch Positiv Badges auf Seite 405.
- Verwenden Sie das **Host set** Dropdown-Menü, um die Daten nach Hostsatznamen oder hochwertigen Hosts zu filtern. Das Dropdown-Menü führt alle Hostsätze auf, die Sie definiert haben und eine Option für **High-value hosts**.
- Verwenden Sie das **Containment state** Dropdown-Menü, um die Daten nach Eindämmungsstatus zu filtern (All, Contained, Containment requested, Containment failed oder Containment ineligible - Alle, Eingedämmt, Eindämmung angefordert, Eindämmung fehlgeschlagen oder Eindämmung unzulässig).
- Verwenden Sie das **Agent** Dropdown-Menü, um die Daten nach der Agent Versionsnummer zu filtern.

Sort By Optionen

Sie können die Hosts in dem Raster auf dieser Seite mit Hilfe der Sort By Optionen sortieren.



Wählen Sie eine Option, um die Hosts in dem Raster nach den Alarmoptionen zu sortieren. Wählen Sie **Priority** (der Standardwert), um die Hosts mit den Alarmen mit der höchsten Priorität zuerst zu sortieren. Wählen Sie **Newest alert**, um die Hosts mit den jüngsten Warnungszeiten zuerst zu sortieren. Wählen Sie **Most events**, um die Host mit der höchsten Anzahl von Alarmmeldungen zuerst zu sortieren. Wählen Sie **Most alert**

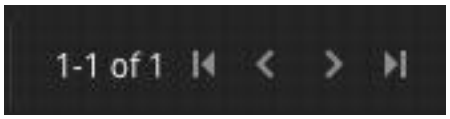
types, um die Hosts mit der höchsten Anzahl verschiedener Warnungstypen zuerst zu sortieren.

Standardmäßig werden Hosts nach der höchsten Priorität sortiert. Hosts mit IOC oder Exploit Alarmen werden mit höherer Priorität in der Liste sortiert als Hosts mit Malware Alarmen. Als sekundäre Sortierung innerhalb der Prioritässortierung werden Hosts in umgekehrter Reihenfolge nach ihren letzten Warnungsdaten sortiert.

Diese Optionen schließen sich gegenseitig aus.

Paginierungsbereich

Der Paginierungsbereich deutet die auf dieser Seite des Rasters angezeigte Spanne von Host Endpunkten und die Gesamtzahl von Host-Endpunkten an, die mit dem Endpoint Security Server bereitgestellt wurden.



Actions Bereich

Der Actions Bereich ermöglicht Ihnen, Aktionen auf jedem Host Endpunkt in der Liste auszuführen.

Das Auswahlfeld ( ) links neben dem Actions Dropdown-Feld ermöglicht Ihnen, ***jeden*** Host Endpunkt in dem Raster auszuwählen. Verwenden Sie dies mit Vorsicht. Die Anzahl der für eine Aktion ausgewählten Hosts wird rechts neben der **Go** Schaltfläche im Actions Bereich aufgeführt.

Das Actions Dropdown-Menü ermöglicht Ihnen, eine Aktion für die Host Endpunkte zu wählen, die Sie in dem Raster ausgewählt haben. Die Liste der auswählbaren Aktionen hängt von den Betriebssystemen der ausgewählten Host Endpunkte ab. Sie können:

- Host-Endpunkte löschen
- Alarme löschen
- Host Endpunkte eindämmen
- Einen Malware Scan auf Host-Endpunkten ausführen

WICHTIG: Der Run a Malware Scan Vorgang wird nur auf macOS und Linux unterstützt.

- Eine Datei-, Daten- oder Triageerfassung für Host-Endpunkte anfordern. Die im Actions Menü aufgeführten Datenerfassungsscripts unterscheiden sich je nach Plattform und enthalten alle von Ihnen erstellte benutzerdefinierte Datenerfassungsscripts, die auf die ausgewählten Endpunkte zutreffen

  Informationen über die Erstellung von benutzerdefinierten Datenerfassungsscripts finden Sie unter Datenerfassungsscripts verwalten auf Seite 121. Informationen über die gelieferten Datenerfassungsscripts finden Sie unter Bereitgestellte Datenerfassungsscripts auf Seite 459.

Wenn keine Hosts ausgewählt wurden, können keine Aktionen im Actions Dropdown-Menü gewählt werden.

Nach Auswahl einer Aktion im Actions Dropdown klicken Sie auf **Go**, um die ausgewählte Aktion zu starten.

Download Option

Um eine CSV-Datei von allen Host Endpunkten im Raster herunterzuladen (auf allen Seiten), klicken Sie auf die Download () Schaltfläche.

Die CSV-Datei enthält die folgenden Felder:

- Agent ID—Die System-generierte ID für den Host- Endpunkt.
- Hostname—Der Hostname des Host-Endpunkts.
- IP Address—Die IP-Adresse des Host-Systems.
- Operating System (OS)—Das Betriebssystem des Host-Systems.
- Timezone—Die Zeitzone, in der das Host-System installiert ist.
- Domain—Die Netzwerkdomain des Host-Systems.
- User—Das-Host-Userkonto, das den Agent ausführt.
- Agent Version—Die Version der Agent Software, die auf dem Host-Endpunkt ausgeführt wird.
- Malware Content Version—Die Version des Signature and Heuristic Detection Inhalts auf dem Host-Endpunkt.
- MalwareGuard Content Version—Die Version des MalwareGuard Inhalts auf dem Host-Endpunkt.
- Last System Audit—Der Zeitstempel des letzten System-Audits auf dem Host-Endpunkt.
- High Value Host—Gibt an, ob der Host-Endpunkt als Host mit hohem Wert definiert ist.
- Containment Status—Gibt den Eindämmungsstatus des Host-Endpunkts an.
- Alert Count—Die Gesamtzahl der Warnungen auf dem Host-Endpunkt.

- Newest Alert—Der Zeitstempel der neuesten Warnung auf dem Host-Endpunkt.
- Alert Types—Eine Liste aller Warnungstypen für den Host-Endpunkt in einer durch Semikolon getrennten Liste.
- Blocked Count—Die Anzahl der Exploits, die blockiert wurden.
- Newest Block—Der Zeitstempel des neuesten Exploit-Blocks.
- Block—Der Blockstatus für den Host-Endpunkt.
- Quarantine Count—Die Anzahl der unter Quarantäne stehenden Dateien auf dem Host Endpunkt.

Hosts Raster

Das Hosts Raster führt alle Host-Endpunkte auf, für die eine Warnung erstellt wurde.

Für jeden Host werden Informationen bereitgestellt. Von links nach rechts werden die folgenden Informationen in den Spalten geliefert:

Spalte	Beschreibung
	Wählen Sie einen Host Endpunkt, für den Sie eine Aktion ausführen wollen.
	Erweitern Sie einen Host Endpunkt, um zusätzliche Details über die Warnungen und Akquisitionen für den Host zu sehen und zusätzliche Details über den Host Endpunkt abzurufen. Siehe Scan-Zusammenfassung auf Seite 63 und Host Details auf Seite 65.
(Containment Status)	Symbole identifizieren den Eindämmungsstatus des Host-Endpunkts: angefordert (), genehmigt (), eingedämmt (), Abbruch läuft (), gescheitert () und nicht für Eindämmung qualifiziert (). Siehe Überblick über Eindämmung auf Seite 421.
(Host Type)	Der Gerätetyp: Windows (), OS X (), Linux () oder Server ().
Agent ID and IP address	Die Agent ID des Host-Endpunkts. Seine IP-Adresse wird unter der Agent-ID aufgeführt.
Operating System and Timezone	Das Betriebssystem und Zeitzone des Host Endpunkts.
Workgroup	Die Arbeitsgruppe des Host Endpunkts.

Spalte	Beschreibung
Agent Version and Sysinfo Time	Die Versionsnummer des auf dem Host-Endpunkt installierten Agent und der letzte Zeitpunkt, zu dem Systeminformationen (sysinfo task) vom Endpunkt des Endpoint Security angefordert wurde. Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.
Alerts	Die Anzahl der Warnungen, die auf dem Host Endpunkt aufgetreten sind und die Zeit (Minuten, Stunden, Tage), seit den letzten Warnungen. Wenn Sie den Mauszeiger über die Anzahl der Warnungen in dieser Spalte ziehen, werden eine Aufschlüsselung der Gesamtzahl der Warnungen und mögliche Falsch Positive für den Host angezeigt. • EXC identifiziert die Anzahl der ausgeführten Warnungen. • MAL identifiziert die Anzahl der Malware Warnungen • PRS identifiziert die Anzahl der Präsenz Warnungen • XPLT identifiziert die Anzahl der Exploit Warnungen Wenn die Gesamtzahl einzigartiger IOC (Indikator), Exploit und Malware Warnungen mit der Gesamtzahl einzigartiger falsch positiv Bedingungen für einen Host übereinstimmt, wird die falsch positiv Markierung (FP) über dem Warnungszähler angezeigt.
Remediation Actions	Die Spalte am weitesten rechts im Raster gibt an, wie viele der folgenden Abhilfemaßnahmen für eine Bedrohung aufgetreten sind, die durch eine Warnung auf dem Endpunkt Host identifiziert wurde. Diese Spalte kann Folgendes anzeigen: • Die Anzahl der blockierten Exploits. • Die Anzahl der unter Quarantäne gestellten Malware Infektionen • Die Anzahl der Malware Infektionen, die bereinigt wurden, einschließlich der bereinigten Bootsektoren. Die Zählung blockierter Exploits wird nur angezeigt, wenn die Exploit Präventionskomponente von Exploit Guard aktiviert ist. Weitere Informationen finden Sie in der Beschreibung von Exploit Guard Richtlinien im *Endpoint Security Agent Administrationshandbuch*. Die Zählungen von Quarantäne und Bereinigung werden nur angezeigt, wenn Exploit Erkennung und Quarantäne aktiviert sind. Weitere Informationen finden Sie in der Beschreibung von Malware Schutz Richtlinien im *Endpoint Security Agent Administrationshandbuch*.

All Hosts Seite

Die All Hosts Seite führt alle vom Endpoint Security Server überwachten Host-Endpunkte auf. Bei einem Host-Endpunkt handelt es sich um einen Computer, Server oder andere verwandte Unternehmenskomponente, auf der die FireEye Endpoint Security Agent Software installiert ist.

Filter By Dropdown Felder

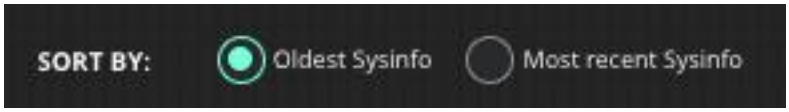
Sie können die Daten in dem Raster auf dieser Seite mit Hilfe der Filter By Dropdown Felder filtern.

Mit Hilfe dieser Felder können Sie die Daten in dem Raster filtern.

- Verwenden Sie das Alert type Dropdown-Menü, um die Daten nach dem Warnungstyp zu filtern. Optionen umfassen **All** (alle Alarme), **XPLT** (Exploit), **PRS** (Präsenz), **EXC** (Ausführung), **MAL** (Malware) und **Others**.
- Verwenden Sie das Protection & Remediation Dropdown-Menü, um die Daten nach einer bestimmten Schutz- oder Korrekturmaßnahme zu filtern. Optionen umfassen **All**, **Blocked**, **Quarantined**, **Cleaned** und **Not Blocked**.
- Verwenden Sie das Disposition Dropdown-Menü, um Daten nach dem Falsch positiv Attribute zu filtern. Optionen umfassen **All**, **False Positive** und **Not False Positive**.
- Verwenden Sie das **Host set** Dropdown-Menü, um die Daten nach Hostsatz Namen, aktiven Hosts, inaktiven Hosts oder hochwertigen Hosts zu filtern. Das Dropdown-Menü führt alle von Ihnen definierten Hostsätze auf sowie Optionen für **High-value hosts**, **Active hosts** und **Inactive hosts**.
- Verwenden Sie das **Containment state** Dropdown-Menü, um die Daten nach Eindämmungsstatus zu filtern (All, Contained, Containment requested, Containment failed oder Containment ineligible - Alle, Eingedämmt, Eindämmung angefordert, Eindämmung fehlgeschlagen oder Eindämmung unzulässig).
- Verwenden Sie das **Agent** Dropdown-Menü, um die Daten nach der Agent Versionsnummer zu filtern.

Sort By Optionen

Sie können die Hosts in dem Raster auf dieser Seite mit Hilfe der Sort By Optionen sortieren.

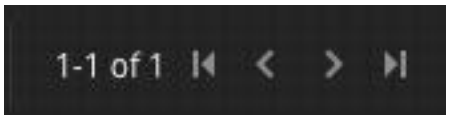


Wählen Sie eine Option, um die Hosts in dem Raster nach der Anzahl zu sortieren, wie oft die letzte Systeminformationsaufgabe (sysinfo) für die Agents auf den Host-Endpunkten ausgeführt wurde. Wählen Sie **Oldes Sysinfo**, um die Hosts mit den ältesten sysinfo Aufgabenzeiten zuerst zu sortieren. Wählen Sie **Most recent Sysinfo**, um die Host mit den neuesten sysinfo Aufgabenzeiten zuerst zu sortieren.

Diese Optionen schließen sich gegenseitig aus.

Paginierungsbereich

Der Paginierungsbereich deutet die auf dieser Seite des Rasters angezeigte Spanne von Host Endpunkten und die Gesamtzahl von Host-Endpunkten an, die mit dem Endpoint Security Server bereitgestellt wurden.



Actions Bereich

Der Actions Bereich ermöglicht Ihnen, Aktionen auf jedem Host Endpunkt in der Liste auszuführen.

Das Auswahlfeld ( ) links neben dem Actions Dropdown-Feld ermöglicht Ihnen, ***jeden*** Host Endpunkt in dem Raster auszuwählen. Verwenden Sie dies mit Vorsicht. Die Anzahl der für eine Aktion ausgewählten Hosts wird rechts neben der **Go** Schaltfläche im Actions Bereich aufgeführt.

Das Actions Dropdown-Menü ermöglicht Ihnen, eine Aktion für die Host Endpunkte zu wählen, die Sie in dem Raster ausgewählt haben. Die Liste der auswählbaren Aktionen hängt von den Betriebssystemen der ausgewählten Host Endpunkte ab. Sie können:

- Host-Endpunkte löschen
- Host Endpunkte eindämmen
- Einen Malware Scan auf Host-Endpunkten ausführen

WICHTIG: Der Run a Malware Scan Vorgang wird nur auf macOS und Linux unterstützt.

- Eine Datei-, Daten- oder Triageerfassung für Host-Endpunkte anfordern. Die im Actions Menü aufgeführten Datenerfassungsscripts unterscheiden sich je nach Plattform und enthalten alle von Ihnen erstellte benutzerdefinierte Datenerfassungsscripts, die auf die ausgewählten Endpunkte zutreffen.

  Informationen über die Erstellung von benutzerdefinierten Datenerfassungsscripts finden Sie unter Datenerfassungsscripts verwalten auf Seite 121. Informationen über die gelieferten Datenerfassungsscripts finden Sie unter Bereitgestellte Datenerfassungsscripts auf Seite 459.

Wenn keine Hosts ausgewählt wurden, können keine Aktionen im Actions Dropdown-Menü gewählt werden.

Nach Auswahl einer Aktion im Actions Dropdown klicken Sie auf **Go**, um die ausgewählte Aktion zu starten.

Download Option

Um eine CSV-Datei herunterzuladen, damit alle Details für alle Host-Endpunkte auf dem Raster (auf allen Seiten) anzuzeigen, klicken Sie auf die Download ( ) Schaltfläche.

Die CSV-Datei enthält die folgenden Felder:

- Agent ID—Die System-generierte ID für den Host-Endpunkt.
- Hostname—Der Hostname des Host-Endpunkts.
- IP Address—Die IP-Adresse des Host-Systems.
- Operating System (OS)—Das Betriebssystem des Host-Systems.
- Timezone—Die Zeitzone, in der das Host-System installiert ist.
- Domain—Die Netzwerkdomain des Host-Systems.
- User—Das-Host-Benutzerkonto, das den Agent ausführt.
- Agent Version—Die Version der Agent Software, die auf dem Host-Endpunkt ausgeführt wird.
- Malware Content Version—Die Version des Signature and Heuristic Detection Inhalts auf dem Host-Endpunkt.
- MalwareGuard Content Version—Die Version des MalwareGuard Inhalts auf dem Host-Endpunkt.
- Last System Audit—Der Zeitstempel des letzten System-Audits auf dem Host-Endpunkt.
- High Value Host—Gibt an, ob der Host-Endpunkt als Host mit hohem Wert definiert ist.
- Containment Status—Gibt den Eindämmungsstatus des Host-Endpunkts an.
- Alert Count—Die Gesamtzahl der Alarme auf dem Host-Endpunkt.

- Newest Alert—Der Zeitstempel des neuesten Alarms auf dem Host-Endpunkt.
- Alert Types—Eine Liste aller Warnungstypen für den Host-Endpunkt in einer durch Semikolon getrennten Liste.
- Blocked Count—Die Anzahl der Exploits, die blockiert wurden.
- Newest Block—Der Zeitstempel des neuesten Exploit-Blocks.
- Block—Der Blockstatus für den Host-Endpunkt.
- Quarantine Count—Die Anzahl der unter Quarantäne stehenden Dateien auf dem Host Endpunkt.

Hosts Grid

Das Hosts Raster führt alle Host-Endpunkte auf, die mit Ihrem Server bereitgestellt wurden.

Für jeden Host werden Informationen bereitgestellt. Von links nach rechts werden die folgenden Informationen in den Spalten geliefert:

Spalte	Beschreibung
	Wählen Sie einen Host-Endpunkt, für den Sie eine Aktion ausführen wollen.
	Erweitern Sie einen Host Endpunkt, um zusätzliche Details über die Alarme und Akquisitionen für den Host zu sehen und zusätzliche Details über den Host Endpunkt abzurufen.
(Containment Status)	Symbole definierten den Eindämmungsstatus des Host Endpunkt: angefordert ( ), genehmigt ( ), eingedämmt ( ), Abbruch läuft ( ), gescheitert ( ) und Eindämmung unzulässig ( ). Siehe Überblick über Eindämmung auf Seite 421.
(Host Type)	Der Gerätetyp: Windows ( ), macOS ( ), Linux ( ) oder Server ( ).
Agent ID and IP address	Die Agent-ID des Host-Endpunkts. Seine IP-Adresse wird unter der Agent ID aufgeführt.
Operating System and Timezone	Das Betriebssystem und Zeitzone des Host-Endpunkts.
Workgroup	Die Arbeitsgruppe des Host-Endpunkts.

Spalte	Beschreibung
Agent Version and Sysinfo Time	Die Versionsnummer des auf dem Host-Endpunkt installierten Agent und der letzte Zeitpunkt, zu dem Systeminformationen (sysinfo task) vom Endpunkt des Endpoint Security angefordert wurde. Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.
Alerts	Die Anzahl der Alarme, die auf dem Host Endpunkt aufgetreten sind und die Zeit (Minuten, Stunden, Tage), seit den letzten Warnungen. Wenn Sie den Mauszeiger über die Anzahl der Warnungen in dieser Spalte bewegen, wird eine Aufschlüsselung der Gesamtzahl der Alarme für den Host angezeigt. • EXC identifiziert die Anzahl der ausgeführten Warnungen • MAL identifiziert die Anzahl der Malware Warnungen • PRS identifiziert die Anzahl der Präsenz Warnungen • XPLT identifiziert die Anzahl der Exploit Warnungen
Maßnahmen zur Fehlerbehebung	Die Spalte am weitesten rechts im Raster gibt an, wie viele der folgenden Abhilfemaßnahmen für eine Bedrohung aufgetreten sind, die durch eine Warnung auf dem Endpunkt Host identifiziert wurde. Diese Spalte kann Folgendes anzeigen: • Die Anzahl der blockierten Exploits • Die Anzahl der unter Quarantäne gestellten Malware Infektionen • Die Anzahl der bereinigten Malware Infektionen. Die Zählung blockierter Exploits wird nur angezeigt, wenn die Exploit Präventionskomponente von Exploit Guard aktiviert ist. Weitere Informationen finden Sie in der Beschreibung von Exploit Guard Richtlinien im *Endpoint Security Agent Administrationshandbuch*. Die Zählungen von Quarantäne und Bereinigung werden nur angezeigt, wenn Exploit-Erkennung und -Quarantäne aktiviert sind. Weitere Informationen finden Sie in der Beschreibung von Malware Schutz Richtlinien im *Endpoint Security Agent Administrationshandbuch*.

Host Alert Details

Host Alert Details enthalten detaillierte Informationen über die Alarme für einen Host und die Daten, Datei und Triage Akquisitionen, die für den Host getätigt wurden.

Voraussetzungen

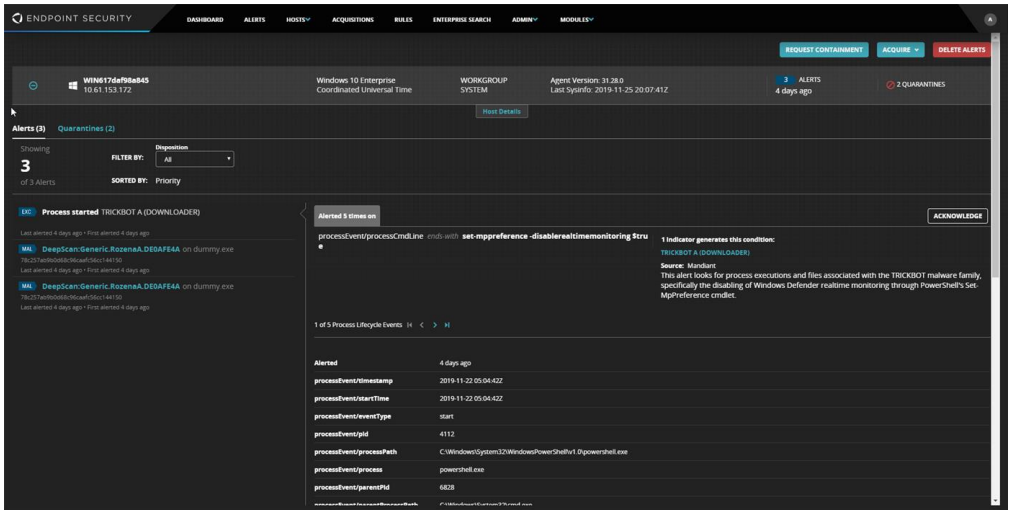
- Admin, Analyst, Senior Analyst oder Investigator Privilegien (vollständiger Zugriff)

Die Seite aufrufen

Zum Host Alert Details aufzurufen:

1. Wählen Sie **Hosts** am Anfang der Seite.
2. Klicken Sie auf **Hosts with Alerts** und dann auf das Erweitern Symbol (⊕) neben dem Host, für den Sie die Alarmdetail-Informationen benötigen.

   Um auf die Hosts with Alerts Seite zurückzukehren, klicken Sie auf das Komprimieren Symbol (⊖) in der oberen linken Ecke der Seite oder wählen Sie **Hosts with Alerts** vom Hosts Menü am Anfang der Seite.



Die folgenden Optionen sind am Anfang der Seite verfügbar.

- **Request Containment**—Sie können Eindämmung des Host-Endpunkts steuern. Je nach dem aktuellen Eindämmungsstatus des Hosts und Ihrer Endpoint Security Web-UI Userrolle können Sie Eindämmung des Host anfordern, Eindämmung des Host genehmigen oder Eindämmung des Host abbrechen oder stoppen. Die Containment Schaltfläche am oberen Rand der Seite ändert sich je nach dem Eindämmungsstatus für den Host-Endpunkt. Siehe Der Eindämmungsprozess auf Seite 425.
- **Acquire**—In diesem Menü können Sie eine Option für die Erfassung einer Datei, Triage, Standard oder umfassende Ermittlungsdaten, eine Quick File Liste oder Agent Diagnostik für den ausgewählten Endpunkt auswählen. Die Liste der Elemente, die erfasst werden können, hängt vom Betriebssystem des Host Endpunktes ab.
- **Delete Alerts**—Sie können alle Alarme für den Host löschen.

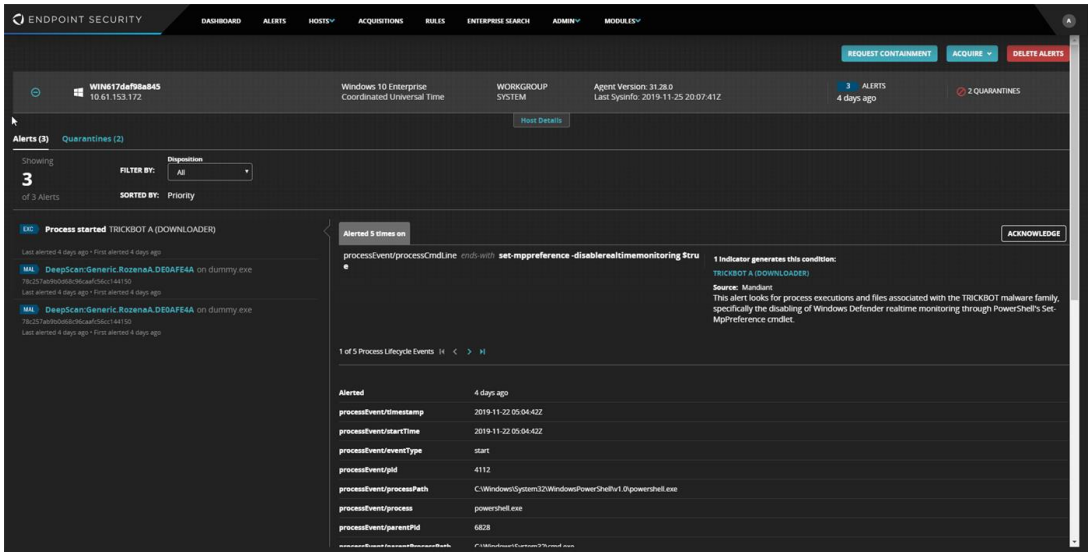
Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.

Unter den Host-Informationen befinden sich Details zu den Warnungen und den unter Quarantäne gestellten Dateien.

Die Host Alert Details Seite enthält zwei Tabs: den **Alerts** und den **Quarantines** Tab. Eine Liste der Erfassungen wird am unteren Rand der Seite angezeigt.

Alerts Tab

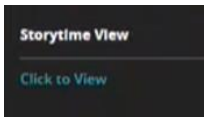
Der Alerts Tab ist der erste Datentab, der auf der Host Alert Details Seite der Endpoint Security Web-UI angezeigt wird. Die Warnungen in diesem Abschnitt sind nach bestimmten Kriterien gruppiert, die in Warnungsgruppen verstehen auf Seite 386 erläutert werden. Wenn Sie gruppiert sind, wird ein einziger Alarm mit mehreren Instanzen angezeigt. Alarme in diesem Bereich werden nach Priorität sortiert, wobei sich Alarme mit der höchsten Priorität am Anfang der Liste befinden. Wenn ein Alarm eine falsch positiv Bedingung enthält, wird der Alarm mit der falsch positiv Markierung (FP) gekennzeichnet.



In der folgenden Tabelle sind einige der Aktionen aufgeführt, die Sie auf der Alarm Details Seite ausführen können.

Aktion	Anleitung	Beschreibung
Warnungsdetails anzeigen	Eine Warnung in der Liste auf der linken Seite auswählen, um ihre Details auf der rechten Seite anzuzeigen.	Details für einen Alarm hängen von dem Warnungstyp ab, den Sie ausgewählt haben.

Aktion	Anleitung	Beschreibung
Alarme nach Disposition filtern	Das **Disposition** Dropdown-Menü verwenden, um die Daten nach falsch positiv Disposition zu filtern.	Mit Hilfe von Disposition können Sie All, False Positive oder Not False Positive Alarme anzeigen. Weitere Informationen darüber, wie Hosts nach Disposition gefiltert werden, finden Sie unter Info über Falsch Positiv Badges auf Seite 405.
Eine Warnung bestätigen oder nicht anerkennen	Klicken Sie auf **Acknowledge**, um eine Warnung zu bestätigen oder auf **Unacknowledge**, um eine bestätigte Warnung nicht anzuerkennen.	Mit Hilfe von Bestätigung können Sie andeuten, dass Sie die Warnung überprüft haben. Bestätigte Warnungen werden nicht länger als neue, überprüfungsbedürftige Warnungen markiert, sondern sie verbleiben im System zur weiteren Untersuchung oder Bezugnahme.
Datei erfassen	Klicken Sie auf**Acquire File** in den Warnungsdetails.	Verwenden Sie Aquire File, um eine infizierte Datei von ihrem originalen Speicherort zu erfassen. Die Dateierfassung wird im Acquisitions Abschnitt am Ende der Seite und auf der Acquisitions Seite in der Web-UI angezeigt.
Prozessdetails für eine Exploit-Warnung erfassen	Klicken Sie auf **Acquire process details**.	Die Prozessdetailerfassung wird im Acquisitions Abschnitt der Seite und auf der Acquisitions Seite in der Web-UI angezeigt. Beachten Sie, dass der ursprünglich ausgenutzte Prozess in den Warnungsdetails aufgeführt ist. Wenn das Exploit blockiert wurde, werden die ausgeführten Blockieraktionen angezeigt.

Aktion	Anleitung	Beschreibung
Zeigen Sie Storytime-Visualisierung an. Damit der Link angezeigt wird, muss es sich bei der Warnung um eine IOC- oder EXG-Warnung handeln, die über ein Auto-Triage-Paket verfügt.	Wählen Sie eine Warnung auf der linken Seite aus, um deren Details auf der rechten Seite anzuzeigen. Wenn die Warnung viele Ereignisse enthält, blättern Sie durch die einzelnen Ereignisse, bis Sie im unteren Teil des Alert-Detailfensters einen Storytime View Abschnitt finden. Klicken Sie auf den **Click to View** Link. 	Die Storytime Visualisation zeigt den Ablauf der Ereignisse, die zur Entdeckung führten. Die grafische Darstellung zeigt den kritischen Pfad auf den Ereignisknoten, der die Erkennung ausgelöst hat.

Anwesenheit und ausgeführte Alarme

Wenn Sie auf das **Alerted on** oder **Alerted*nnn* times on** Feld klicken, wird eine Option angezeigt, die Ihnen ermöglicht, den Alarm als ein *Falsch Positiv* zu markieren.

Die Anzahl der Indikatorregeln, die diese Bedingung generiert haben, wird angezeigt.

Diese Anzahl ist nicht plattformspezifisch, sondern repräsentiert die Gesamtzahl der Indikatorregeln, die die Bedingung enthält, die die Warnung, unabhängig von der Betriebssystemplattform ausgelöst hat. Dieselbe Bedingung kann in mehreren Indiatorregeln enthalten sein.

Sie können die Indikatorregeln überprüfen, die die Warnung generiert haben, indem Sie einen Indikator Regelnamen auswählen. Die Indikatorregeln werden auf der Rules Seite angezeigt.

Klicken Sie auf die **Acquire File** Schaltfläche in den Alert Details, um die infizierte Datei von ihrem ursprünglichen Speicherort abzurufen. Die Dateierfassung wird im Acquisitions Abschnitt der Seite und auf der Acquisitions Seite angezeigt. Wenn die Dateierfassung abgeschlossen ist, laden Sie die Dateierfassung von jedem Speicherort herunter.

Exploit Warnungen

Der anfänglich ausgenutzte Prozess wird in den Alert Details aufgeführt. Wenn das Exploit blockiert wurde, werden die verwendeten Blockieraktionen angezeigt.

Klicken Sie auf die **Acquire process details** Schaltfläche in den Alert Details, um Prozessdetails über die Exploit Warnung zu erhalten. Die Erfassung der Prozessdetails wird im Acquisitions Abschnitt der Seite und auf der Acquisitions Seite angezeigt. Wenn die Erfassung der Prozessdetails abgeschlossen ist, laden Sie die Prozessdetails von beiden Speicherorten herunter.

Info über Malware Alarme

Für Malware Ereignisse wird ein Konfidenzniveau von *signature* ( ) oder *heuristic* ( ) in den Alert Details angezeigt.

- Eine Warnung mit einem Konfidenzniveau von *signature* ( ) deutet auf bestätigte Malware, die mit einer FireEye Malware Definition übereinstimmt.
- Eine Warnung mit einem Konfidenzniveau von *heuristic* ( ) deutet auf vermutete Malware, die durch heuristische Methoden identifiziert wurde. Die Bedingung, die die Warnung ausgelöst hat, weist Charakteristiken bekannter Malware auf, aber stimmt mit keiner FireEye Malware Definition überein.

Die folgende Tabelle beschreibt die möglichen Detailinformationen für eine Malware Warnung auf dem Alerts Register. Einige Daten sind für verschiedene Arten von gescannten Objekten nicht verfügbar.

Abschnitt	Feld	Beschreibung
Event Details	Alerted	Die seit der Meldung der Malware Warnung verstrichene Zeit Endpoint Security.
	Detection time	Der Zeitpunkt, zu dem die Malware-Warnung von Endpoint Security Agent entdeckt wurde.

Abschnitt	Feld	Beschreibung
Scan Details	Scan type	Die Art des Scans deutet an, ob der Scan beim Zugriff auf eine Ressource (z.B. eine Datei) oder als ein geplanter Scan stattgefunden hat. Mögliche Werte sind **On-access** oder **On-demand**.
	Scanned object	Der Typ des gescannten Objekts. Mögliche Werte sind **Bootsector**, **File**, oder **Registry**.
Malware Details	Malware name	Der Name der erkannten Malware.
	Malware type	Der Malwaretyp.
File Details	Status	Die eingeleiteten Maßnahmen auf der Datei. Mögliche Werte sind **Alert**, **Cleaned** oder **Quarantined**. **Alert** wird angezeigt, wenn Quarantäne nicht in Ihrer Umgebung aktiviert ist oder wenn der FireEye Endpoint Security Agent die infizierte Datei nicht bereinigen kann. **Cleaned** wird angezeigt, wenn eine infizierte Datei gelöscht wird, aber der Rest der Eingabe nicht isoliert ist. **Quarantined** wird angezeigt, wenn eine von Malware eingeführte Datei automatisch vom System gelöscht wurde (sich jedoch im Quarantänebereich befindet).
	File path	Der vollständig qualifizierte Dateipfad.
	MD5	Das MD5 Hash der Datei.
	SHA1	Das SHA1 der Datei.
	File size	Die Größe der Datei.
	File compressed	Deutet an, ob die Datei komprimiert wurde.
	File created	Der Zeitstempel, als die Datei erstellt wurde.
	File modified	Der Zeitstempel, als die Datei zuletzt verändert wurde.
	File last accessed	Der Zeitstempel, als die Datei zuletzt aufgerufen wurde.

Abschnitt	Feld	Beschreibung
Process Details	Process path	Der vollständig qualifizierte Pfad auf den Prozess
	PID	Die Prozess ID
	Username	Der User, der den Prozess aufgerufen hat.
Registry Details	Key	Der Name des Verzeichnisschlüssels.
	Wert	Wert des Verzeichnisschlüssels.
System Details	Content version	Die Inhaltsversion.

Quarantines Tab

Der Quarantines Tab zeigt die infizierten Dateien an, die Malware Schutz für den Host unter Quarantäne gestellt hat. Wenn Aktionen zur Korrektur von Malware Aktionen (Quarantäne) aktiviert sind, werden infizierte Dateien automatisch auf einen Quarantänebereich kopiert, wo sie von Ihren Systemanalysten überprüft werden können. Sie werden in dem Quarantänebereich gespeichert, bis die Alterungsperiode der Quarantäne abgelaufen ist. Die Alterungsperiode der Quarantäne kann auf dem Quarantined Files Aging Tab konfiguriert werden. Der Standardwert ist 90 Tage.

Sie können die Quarantäneliste filtern, indem Sie auf eine Spaltenüberschrift klicken und die Filterkriterien eingeben. Wenn Sie fertig sind, klicken Sie auf **Filter**. Sie können Alarme auch je nach dem MD5 Hash in auf- oder absteigender Reihenfolge sortieren.

Die folgenden Optionen sind für Dateien verfügbar, die im Raster für das Quarantines Register aufgeführt sind. Klicken Sie auf die Schaltfläche, um eine Option auszuwählen.

- Wählen Sie **Acquire File**, um die infizierte Datei vom Quarantänebereich zur weiteren Untersuchung abzurufen.
- Wählen Sie **Restore File**, um die infizierte Datei vom Quarantänebereich auf seinen normalen Speicherort auf dem Endpunkt wiederherzustellen.
- Wählen Sie **Delete File from Quarantine**, um die Datei aus dem Quarantänebereich zu löschen.

Malware Scans

Der Malware Scans Tab zeigt den Status aller angeforderten, ausgeführten und abgeschlossenen Malware Scans auf Ihrem Host-Endpunkt an. Dies wird auch als Scan-Zusammenfassung bezeichnet.

Scan-Zusammenfassung

Klicken Sie auf das Erweiternsymbol (⊕) neben dem Host, für den Sie einen vollständigen Bericht oder eine Scan-Zusammenfassung von Malware Scans auf diesem Host-Endpunkt anzeigen wollen.

In der folgenden Tabelle werden die in der Scan-Zusammenfassung beschriebenen Details für einen Endpunkt beschrieben. Einige Daten werden für verschiedene Typen gescannter Objekte nicht bereitgestellt.

Feld	Beschreibung
Scan Name	Der Name, der dem Malware Scan in Malware Schutz für Linux aktivieren auf Seite 176 zugewiesen wurde oder der Name, der dem on-Demand Malware Scan in Malware Schutz konfigurieren auf Seite 247 zugewiesen wurde. Sie können nach diesem Feld suchen und filtern.
Scan Type	Die Tiefe der auf dem Endpunkt ausgeführten Malware Scans: Full (Vollständig), Custom (Benutzerdefiniert), Memory (Speicher) oder Quick (Schnell). Sie können nach diesem Feld filtern.
Status	Der aktuelle Status des auf dem Endpunkt durchgeführten Malware Scans: Requested (Angefordert), Completed (Abgeschlossen), Failed (Fehlgeschlagen), Timed out (Abgelaufen) oder Stopped (Gestoppt). Sie können nach diesem Feld filtern.
# Files Scanned	Die Gesamtzahl der gescannten Dateien.
# of Malware	Die Anzahl der auf dem Host-Endpunkt gefundenen Malware Alarme. Wenn dieser Wert größer als 0 ist, kann dieser Wert angeklickt werden, um Details zu allen Alarmen in diesem Scan anzuzeigen. Die resultierende Seite ist Malware Scan Results auf der nächsten Seite.
File/Folder Paths	Der Standardort auf dem Host-Endpunkt, auf dem der Malware Scan ausgeführt wurde, wie in der **Custom Scan** Option in Nach Malware scannen auf Seite 175 festgelegt.
Start Time	Die Startzeit des Malware Scans.
End Time	Das Ende des Malware Scans.
Duration	Die Dauer des Malware Scans.
Initiator	Die Benutzer-ID, die den Malware Scan initiiert hat. Sie können nach diesem Feld suchen und filtern.

Um ein Scan-Ergebnis zu löschen, wählen Sie das Kontrollkästchen links neben dem Scan Namen:

1. Öffnen Sie den **Malware Scans** Tab.
2. Wählen Sie das Kontrollkästchen links neben dem Malware Scan, den Sie löschen wollen.
3. Klicken Sie auf der **Actions** Liste auf **Delete scan** und dann auf **Go**.

Malware Scan Results

Durch Anklicken eines Wertes in der **# of Malware** Spalte wird die **Malware Scan Results** Seite geöffnet. Auf dieser Seite werden Details über die auf dem Host-Endpunkt entdeckte Malware angezeigt. Sie können Malware Scan Ergebnisse als eine .csv-Datei herunterladen, indem Sie auf das Download () Symbol in der rechten Ecke der Seite klicken.

In der folgenden Tabelle werden die in **Malware Scan Results** angezeigten Details beschrieben. Einige Daten werden für einige Arten von Malware nicht bereitgestellt.

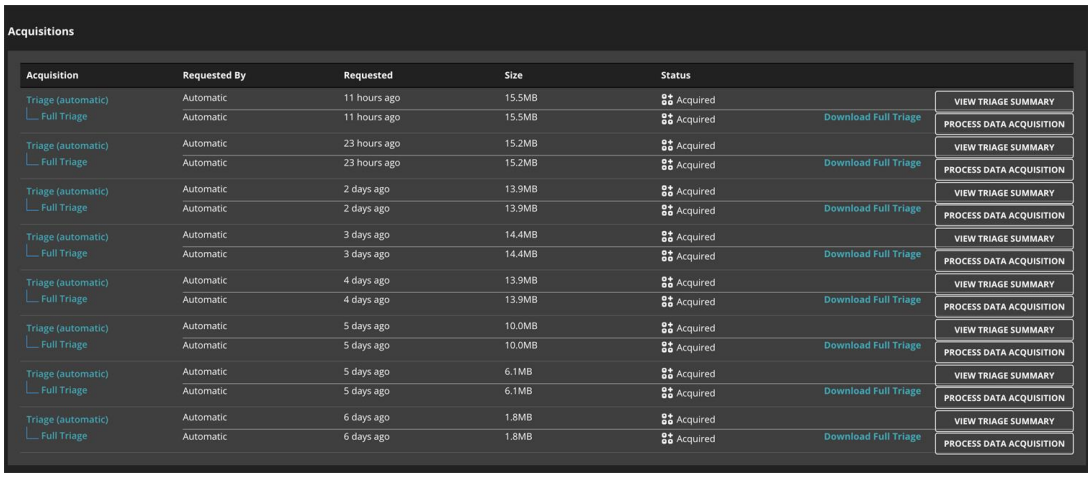
Feld	Beschreibung
Malware Name	Der Name der Malware Bedrohung, die durch den Scan auf Ihrem Host-Endpunkt entdeckt wurde. Sie können nach diesem Feld suchen und filtern.
Infection Type	Der Typ der Malware Infektion: Malware, Adware, PUP oder Spyware. Sie können nach diesem Feld suchen und filtern.
Object Scanned	Der Typ des gescannten Objekts: Datei Sie können nach diesem Feld suchen und filtern.
Path	Der Dateispeicherort auf dem Host, auf dem die Bedrohung gefunden wurde.
MD5	Die MD5 Prüfsumme für die entdeckte Bedrohung.
Action Taken	Die für die Infektion ausgeführte Maßnahme: Alert (Alarm), Clean Bereinigung) oder Quarantine Quarantäne). Sie können nach diesem Feld filtern.

Die **Malware Scan Results** Seite enthält auch Details über die Malware Engine und AV Engine, die den Scan ausführen.

Der ***n* threats detected** Wert in der linken Ecke der **Malware Scan Results** Seite kann sich von der tatsächlichen Anzahls der auf dem Host entdeckten Bedrohungen unterscheiden. Dies ist ein bekanntes Problem, das durch Faktoren wie Warnungs-Deduping auf dem Host oder Warnungs-Ratenbegrenzung verursacht wird.

Acquisitions

Erfassungen für den Host werden am Ende der Seite aufgeführt.



Klicken Sie auf die Erfassung, um die Acquisitions Detailseite anzuzeigen und eine Maßnahme für diese Erfassung zu treffen.

- Wählen Sie **Download Full Triage**, um eine Triage Acquisition Datei herunterzuladen.
- Wählen Sie **Triage Summary**, um eine Triage in Triage Summary zu öffnen.
- Wählen Sie **View Data Acquisition**, um die erfassten Daten im Audit Viewer zu überprüfen.
- Wählen Sie **Process Data Acquisition**, um Prozessdaten für den Host Endpunkt zu erhalten.
- Wählen Sie **Download**, um eine erfasste Datei herunterzuladen.

Host Details

Host Details liefern detaillierte Informationen über Ihren Host-Endpunkt. Je nach Betriebssystem des Endpunktes können geringfügige Unterschiede im Display auftreten.

Sie können die folgenden Aufgaben auf dieser Seite ausführen:

- Eindämmung des Host-Endpunkts steuern. Je nach dem aktuellen Eindämmungsstatus des Hosts und Ihrer Endpoint Security Web-UI Userrolle können Sie Eindämmung des Host anfordern, Eindämmung des Host genehmigen oder Eindämmung des Host abbrechen oder stoppen. Die Containment Schaltfläche am oberen Rand der Seite ändert sich je nach dem Eindämmungsstatus für den Host-Endpunkt. Siehe Der Eindämmungsprozess auf Seite 425.
- Datei-, Tirage- oder Datenerfassungen vom Host Endpunkt erfassen. Wählen Sie eine Option vom **Acquire** Menü. Die Liste der Elemente, die erfasst werden können, hängt vom Betriebssystem des Host Endpunktes ab.
- Alle Warnungen für den Host löschen. Klicken Sie auf **Delete alerts**.
- Eine Warnung auf Ihrem Host-Endpunkt bestätigen und verwerfen.
- Eine Warnung als Falsch positiv markieren.
- Host-Warnungsdetails anzeigen.

Der Rest der Host Details Seite führt Informationen über die Host Endpunkt Umgebung auf. Informationen zu einem Endpunkt sind auf dieser Seite in den folgenden Abschnitten organisiert: General, Malware Protection, Operating System, BIOS (nur Windows), Physical Memory (RAM), User und Network Adapters.

HINWEIS: Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.

Voraussetzungen

- Admin, Analyst, Senior Analyst oder Investigator Privilegien (vollständiger Zugriff)
- Operator Privilegien (nur Lesezugriff)

Die Seite aufrufen

Um Host Details abzurufen:

1. Wählen Sie **Hosts** am Anfang der Seite.
2. Klicken Sie auf **All Hosts**.
3. Klicken Sie in der Liste auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie die Host Detail Informationen anzeigen wollen.
    - Um auf die All Hosts Seitenliste zurückzukehren, klicken Sie auf das Komprimieren Symbol (⊖) in der oberen linken Ecke der Seite oder wählen Sie **All Hosts** vom Hosts Menü am Anfang der Seite.

General (Allgemeiner) Abschnitt

Dieser Abschnitt auf der Host Details Seite liefert allgemeine Informationen über den Host Endpunkt.

Feld	Beschreibung
Active Directory: Domain Components	Eine Liste aller dem Host zugewiesenen Domänen.
Active Directory: Organizational Units	Eine Liste aller dem Host zugewiesenen Organisationseinheiten.
Active Directory: Common Names	Dem Host zugewiesene allgemeine Namen.
Agent ID	Die eindeutige Agent ID, die dem Host Endpunkt zugewiesen wurde.
Agent Version	Die Version des auf dem Host Endpunkt installierten Agent.
Bit Level	Die Bitanzahl des Host Endpunkts.
Domain	Die Domain des Host Endpunkts.
GMT Offset	Die GMC-Zeitverschiebung des Host-Endpunkts.
IP Address	Die IP-Adresse des Host Endpunkts.
Initial Agent Connection	Der UTC-Zeitstempel, der identifiziert, wann der Endpunkt ursprünglich mit dem Endpoint Security bereitgestellt wurde.
Kernel (nur Linux)	Die Linux Kernelversion, die auf dem Endpunkt ausgeführt wird.
KernelServices Status	Der Status der Linux-KernelServices auf dem Endpunkt.
Last Sysinfo	Der UTC Zeitstempel, der angibt, wann die letzte Systeminformationsaufgabe (sysinfo) Ergebnisse von dem Agent auf dem Host Endpunkt gemeldet hat. Als nächstes sehen Sie den Vergleich dieser Zeit mit der Last Sysinfo (skewed) Zeit.
Agent Last Poll	Der UTC-Zeitstempel, der den Zeitpunkt der letzten Agentabfrage für Auditjobs identifiziert.

Feld	Beschreibung
Last Sysinfo (skewed)	Ein versetzter UTC Zeitstempel, der angibt, wann die letzte sysinfo Aufgabe Ergebnisses von dem Agent auf dem Host Endpunkt gemeldet hat. Dieser Wert ist versetzt, um den berechneten Unterschied zwischen der tatsächlichen Uhrzeit auf dem Host-Endpunkt und der Uhrzeit auf dem Endpoint Security einzuschließen. Diese Uhrzeiten können unterschiedlich sein, weil jedes Gerät von verschiedenen Faktoren betroffen sein kann, wie Taktverzögerungen, Netzwerkverzögerungen und der für die Zeitsynchronisierung verwendete Service. Für den Wert in diesem Feld behandelt Endpoint Security die Serverzeit als die tatsächliche Uhrzeit und versetzt die Zeit mit dem berechneten Unterschied zwischen den Server- und Endpunkt-Zeiten. Die versetzte Zeit sollte so ähnlich, wenn nicht identisch mit der nicht-versetzten Last Sysinfo Zeit sein, aber wenn sie unterschiedlich sind, sollte die versetzte Zeit die tatsächliche Agentzeit genauer widerspiegeln, zu der die letzte sysinfo Aufgabe Ergebnisse an den Server gemeldet hat.
OS	Das auf dem Host Endpunkt installierte Betriebssystem.
Patch	Die Patch-Ebene des auf dem Host Endpunkt installierten Betriebssystems.
Timezone	Die UTC-Zeitzone des Host Endpunkts.

Malware Protection Section

Host Details liefern Informationen zum Schutz vor Malware für den Host-Endpunkt, die in Signature and Heuristic Detection und MalwareGuard Detection unterteilt sind.

Feld	Beschreibung
Malware Engine Version	Die für den Malware Schutz verwendete Version der Malware Engine.
Malware Content Version	Die Version des Signature and Heuristic Detection Inhalts auf dem Host-Endpunkt. Die Versionsnummer der Definitionen von Malware Schutz auf dem Host Endpunkt.
Last Updated	Der Zeitpunkt, an dem die Definitionen von Malware Schutz zuletzt auf dem Host Endpunkt aktualisiert wurden.

Feld	Beschreibung
MalwareGuard Engine Version	Die für den Malware Schutz verwendete Version der MalwareGuard Engine.
MalwareGuard Content Version	Die Version von MalwareGuardInhalten auf dem Host-Endpunkt.
Last Updated	Der Zeitpunkt, zu dem MalwareGuard Inhalte zuletzt auf dem Host-Endpoint aktualisiert wurden.

Security Content Abschnitt

Feld	Beschreibung
Intel Version	Die Versionsnummer des zuletzt installierten Sicherheitsinhalts
Intel Last Updated	Die UTC-Zeit, zu der der Sicherheitsinhalt zuletzt aktualisiert wurde.

Operating System Abschnitt

Feld	Beschreibung
OS, Build & Patch	Das Betriebssystem, Version und auf dem Host Endpunkt installiertes Patch.
Install Date	Der Zeitstempel, der angibt, wann das Betriebssystem auf dem Host Endpunkt installiert wurde.
Product ID	Die Produkt-ID des Host Endpunkts.
Processor	Der für den Host Endpunkt installierte Prozessortreiber.
Processor Type	Der Prozessortyp des Host Endpunkts.
System Timestamp	Die System UTC-Zeit des Host Endpunkts.
Machine Name	Der Gerätenamen des Host Endpunkts.
System Directory	Der Speicherort des Systemverzeichnisses auf dem Host Endpunkt.

Feld	Beschreibung
Up Time	Die Anzahl der Sekunden, die der Host Endpunkt ausgeführt wurde.

BIOS Abschnitt (nur Windows)

Feld	Beschreibung
Release Date	Das Datum des Basic Input/Output System (BIOS) auf dem Host Endpunkt.
Version	Die Version des BIOS auf dem Host Endpunkt.

Physical Memory Abschnitt

Feld	Beschreibung
Total	Der Gesamtspeicher des Host Endpunkts.
Available	Die Größe des auf dem Host Endpunkt verfügbaren Speichers.

User Abschnitt

Feld	Beschreibung
Primary User	Der primäre User des Host Endpunkts.
Registered Org (Nur Windows)	Die registrierte Organisation des Host Endpunkts.
Registered Owner (Nur Windows)	Der registrierte Besitzer des Host-Endpunkts.

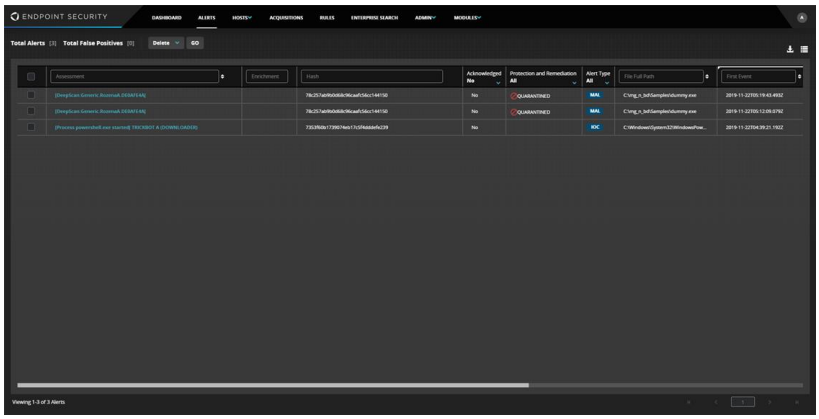
Network Adapters Abschnitt

Feld	Beschreibung
DHCP Address	(Nur Windows) Das Dynamic Host Configuration Protokoll (DHCP) des Netzwerkadapters auf dem Host Endpunkt.
IP Address	Die IP-Adresse des Netzwerkadapters auf dem Host Endpunkt.
IP Gateway Address	Die IP Gateway Adresse des Netzwerkadapters auf dem Host Endpunkt.

Feld	Beschreibung
Lease Expiry Date	Das Datum, an dem das Lease für den Netzwerkadapter abläuft.
Lease Obtained Date	Das Datum, an dem das Lease für den Netzwerkadapter erteilt wurde.
MAC	Die Media Access Control (MAC) Adresse des Netzwerkadapters.
Name	Der Name des Netzwerkadapters auf dem Host Endpunkt.
Subnet Mask	Die Subnetzmaske des Netzwerkadapters auf dem Host Endpunkt.

Alerts Seite

Die Alerts Seite bietet eine Möglichkeit für Sie, alle Warnungen für Ihre Endpoint Security Umgebung an einer Stelle anzuzeigen. Anders wie auf der Hosts with Alerts Seite umfassen diese Warnungen alle Hosts in Ihrer Umgebung. Sie können Alarme in dem Raster filtern und sortieren, um Ihre sichtbaren Ergebnisse einzugrenzen. Sie können Warnungen auch löschen oder eine Warnung auf dem Options Menü als falsch positiv markieren.



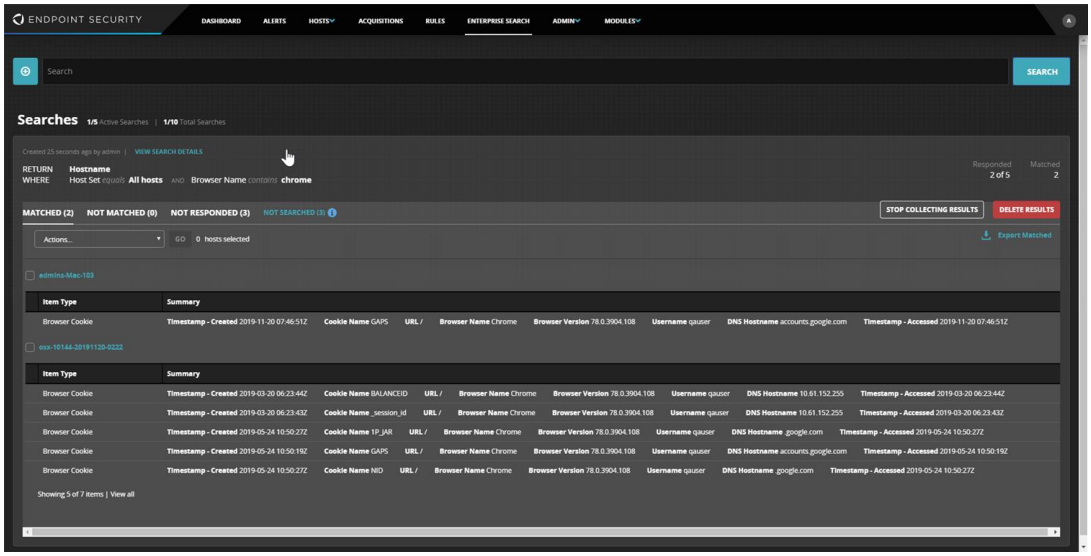
Voraussetzungen

- Administrator, Analyst, Senior Analyst oder Investigator Zugriff.

Weitere Informationen über die Verwendung der Alerts Seite finden Sie unter Warnungen anzeigen und verwalten auf Seite 367.

Enterprise Search Seite

Die Enterprise Search Seite ermöglicht Ihnen, nach Bedrohungen oder Bedrohungsindikatorregeln auf Ihren Windows und macOS Host-Endpunkten zu suchen, wenn sie FireEye Endpoint Security Agent Version 25 oder später und Linux Host-Endpunkte, dieEndpoint Security Agent Version 34 ausführen. Die in Ihrer Umgebung gezeigte Funktionalität ist je nach der Rolle verschieden, die Ihrem Benutzerkonto zugewiesen wurde und basiert auf den FireEye Lizenzen, die Sie installiert haben. Um auf die Enterprise Search Seite zuzugreifen, wählen Sie **Enterprise Search** am Anfang der Seite.



Die Enterprise Search Seite besteht aus einem einzelnen Suchfeld und Ergebnissen aus allen definierten Suchvorgängen. Die Anzahl der aktiven Suchen und die Gesamtzahl der Suchen werden unter dem Suchfeld angezeigt.

In den Suchergebnissen werden eine Reihe von Registern angezeigt.

- Das **Matched** Register führt die Host Endpunkte auf, die den Suchkriterien und den übereinstimmenden Daten entsprechen.
- Das **Not Matched** Register listet die Host Endpunkte auf, die nicht den Suchkriterien entsprechen.
- Das **Not Reponded** Register listet die Host Endpunkte auf, für die die Verarbeitung der Enterprise Search nicht abgeschlossen wurde.

- Das **Not Searched** Register listet die Host Endpunkte auf, für die die Suche nicht gültig war und daher nicht durchgeführt wurde. Eine Suche könnte für einen Endpunkt nicht gültig sein, weil die auf dem Endpunkt installierte FireEye Endpoint Security Version nicht von der Suchanfrage unterstützt wird oder auf dem Endpunkt eine nicht kompatible Betriebssystemplattform installiert ist.
- Das **Errors** Register listet Fehler auf, die während der Suche aufgetreten sind.

Die in den Registernamen angezeigten Werte ändern sich während der Verarbeitung der Enterprise Search.

HINWEIS: Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.

Verwenden Sie die **Stop collecting results** Schaltfläche, um die Enterprise Suche zu stoppen. Verwenden Sie die **Delete results** Schaltfläche, um die Ergebnisses einer Enterprise Search zu löschen. Klicken Sie auf die Export Option auf einem Register, um die auf diesem Register aufgeführte Liste von Host Endpunkten (und ggf. Daten) auf eine CSV-Datei herunterzuladen.

Informationen über die Verwendung dieser Seite finden Sie unter Ihr Unternehmen durchsuchen auf Seite 253.

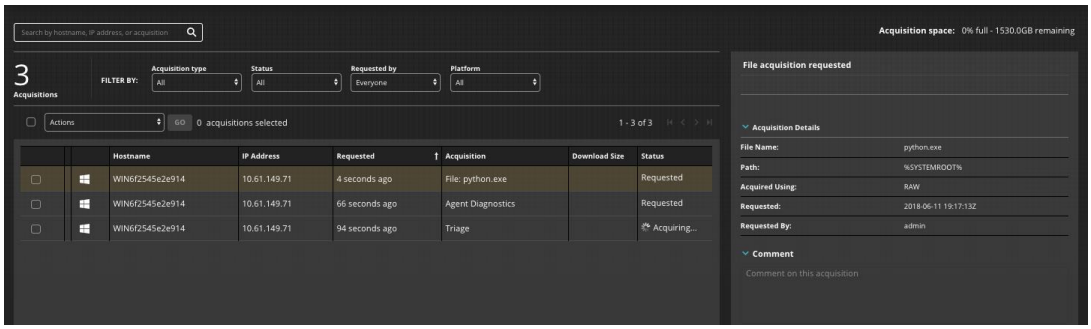
Voraussetzungen

- Administrator, Analyst, Senior Analyst oder Investigator Privilegien (vollständiger Zugriff)
- Umfassende Suchfunktionalität für Enterprise Suchen erfordert eine Endpoint Security Power Lizenz.

Acquisitions Seite

Um potentielle Kompromittierungen schnell zu überprüfen und darauf zu reagieren, können Sie Dateien und Triage Sammlungen direkt von Hosts erfassen. Die Acquisitions Seite ermöglicht Ihnen, die Details jeder Erfassung anzuzeigen. Um die Acquisitions Seite aufzurufen, wählen Sie **Acquisitions** am Anfang der Seite.

Informationen über die Benutzung dieser Seite finden Sie unter Forensische Daten analysieren auf Seite 309.



Die Acquisitions Seite ist in einen Acquisitions Raster und einen Acquisitions Detail Bereich unterteilt. Am Anfang der Seite können Sie nach einer bestimmten Erfassung nach Hostname oder IP-Adresse suchen.

Voraussetzungen

- Administrator, Analyst, Senior Analyst oder Investigator Privilegien (vollständiger Zugriff)

Filter Dropdown Felder

Sie können die Daten in dem Raster mit Hilfe der Filter Dropdown Felder filtern.

Mit Hilfe dieser Felder können Sie die Daten in dem Raster nach Erfassungstyp, Status, wer die Erfassung angefordert hat und dem Betriebssystem, auf dem die Erfassung angefordert wurde, filtern.

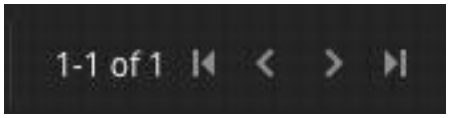
Acquisition Space Abschnitt

Die Acquisitions Seite zeigt an, wie viel Speicherplatz für Erfassungen noch verfügbar ist.

Sehen Sie Datenträgerauslastungslimits für Erfassungen festlegen auf Seite 102, um den gesamten Speicherplatz festzulegen, der für Erfassungen verwendet werden kann.

Paginierungsbereich

Der Paginierungsbereich zeigt den Umfang der auf dieser Seite des Rasters gezeigten Erfassungen und die Gesamtzahl der gespeicherten Erfassungen.



Die Schaltflächen im Paginierungsbereich ermöglicht Ihnen, durch die Liste der Erfassungen auf dem Raster zu blättern.

Schaltfläche	Beschreibung
	Zeigt die erste Seite der Erfassungen im Raster an.
	Blättert auf die vorherige Seite der Erfassungen im Raster.
	Blättert auf die nächste Seite der Erfassungen im Raster.
	Zeigt die letzte Seite der Erfassungen im Raster an.

Actions Bereich

Der Actions Bereich ermöglicht Ihnen, Aktionen auf jeder Erfassung in der Liste auszuführen.

Das Auswahlfeld ( ) links neben dem Actions Dropdown Feld ermöglicht Ihnen, ***jede*** Erfassung im Raster auszuwählen. Die Anzahl der für eine Aktion ausgewählte Erfassungen ist rechts neben der **Go** Schaltfläche im Actions Bereich aufgeführt.

Das Actions Dropdown Menü führt Erfassungen auf, die Sie für die im Raster ausgewählten Erfassungen ausführen können. Wenn keine Erfassungen ausgewählt sind, können keine Aktionen im Actions Dropdown Menü gewählt werden.

Nach Auswahl einer Aktion im Actions Dropdown klicken Sie auf **Go**, um die ausgewählte Aktion zu starten.

Acquisitions Raster

Das Acquisitions Raster führt die erfassten Dateien und Triage Sammlungen auf.

Klicken Sie einmal auf einen Spaltennamen im Acquisitions Raster, um die Rasterdaten in aufsteigender alphanumerischer Reihenfolge je nach den Spaltendaten zu sortieren. Klicken Sie erneut auf den Spaltennamen, um die Rasterdaten in absteigender alphanumerischer Reihenfolge je nach den Spaltendaten zu sortieren. Ein Pfeil rechts neben dem Spaltennamen zeigt an, wie die Rasterdaten sortiert sind.

Feld	Beschreibung
	Wählen Sie eine Erfassung aus, für die Sie Maßnahmen ergreifen möchten.

Feld	Beschreibung
(containment state)	Symbole identifizieren den Eindämmungsstatus des Hostendpunkts, der mit der Erfassung verknüpft ist: angefordert (), genehmigt (), enthalten (), Abbruch läuft (), gescheitert () und nicht zur Eindämmung geeignet (). Siehe Überblick über Eindämmung auf Seite 421.
(Host Type)	Der mit der Erfassung assoziierte Hostmaschinentyp: Windows (), Mac OS X (), Linux () oder Server ().
Hostname	Der Hostname des Host, von dem die Datei erfasst wurde.
IP Address	Die IP-Adresse des Host, von dem die Datei erfasst wurde.
Requested	Die Zeitspanne seit der Anforderung der Erfassung.
Acquisition	Die Art der Akquisition: Datei oder Triage.
Download Size	Die Größe der Erfassung.
Status	Der Erfassungsstatus: Acquired—Die Erfassung war erfolgreich. Acquiring—Die Erfassung ist in Bearbeitung. Failed—Die Erfassung war nicht erfolgreich. Processing—Eine Erfassungsaktion wird ausgeführt. Requested—Eine Erfassung wurde angefordert. Update Required—Eine Erfassung muss aktualisiert werden. Waiting for processing—Die Erfassungsaktion wartet auf Verarbeitung.

Acquisition Detail Bereich

Der Acquisition Details Bereich zeigt detaillierte Informationen für die ausgewählte Erfassungsanfrage an.

Wählen Sie **Download Full Triage**, um eine `.mans` Datei mit den Erfassungsdaten herunterzuladen. Sie können diese Daten in Redline überprüfen.

Wählen Sie **PROCESS DATA ACQUISITION**, um die Datenerfassung zu verarbeiten und die Daten im Audit Viewer anzuzeigen.

Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.

Rules Seite

Die Rules Seite führt FireEye Indicator of Compromise (IOC) und falsch positiv Regeln auf, die auf Ihrem Netzwerk ausgelöst werden könnten. Die Liste enthält einige benutzerdefinierte Indikatorregeln, die Sie für Ihre Umgebung erstellt haben, selbst wenn diese Indikatorregeln nicht ausgelöst werden. Verwenden Sie die Rules Seite, um Regeln zu überprüfen und Bedingungen in ihnen als falsch positiv oder true positiv zu markieren. Sie können die Rules Seite auch verwenden, um benutzerdefinierte Indikatorregeln zu erstellen und zu löschen. Um die Rules Seite aufzurufen, wählen Sie **Rules** am Anfang der Seite.

FireEye Regeln sind zumeist ausgeblendet und in werden in der Dynamic Threat Intelligence (DTI) Cloud gespeichert. Sie werden nur auf dieser Seite angezeigt, wenn ihre Existenz eine Warnung auslöst, wenn die Regel von einer anderen FireEye Appliance bereitgestellt wird oder die Regel für einen uneingeschränkten FireEye Indikator gilt. In einer FireEye Regel enthaltene Bedingungen sind nur sichtbar, wenn die Bedingung eine Warnung auslöst. Wenn alle mit einer Regel verknüpften Alarme entfernt werden, werden die Regel und die dazugehörigen Bedingungen wieder ausgeblendet. Dies vereinfacht Ihre forensische Analyse von Alarmen, weil nur die relevanten Regeln und Bedingungen angezeigt werden.

Am Anfang der Rules Seite können Sie nach einer bestimmten Regel anhand ihres Namens, ihres Erstellers oder ihrer Signatur suchen. Sie können auch nach Bedingungswert suchen (z.B. eine bestimmte `md5` Datei oder DNS).

Klicken Sie auf **Create Indicator**, um einen benutzerdefinierten Indikator zu erstellen. Weitere Informationen finden Sie unter IOC Regeln verwalten auf Seite 221.

Die Version der von der Dynamic Threat Intelligence (DTI) Cloud heruntergeladenen Intelligenz und die Uhrzeit des letzten Downloads wird am Anfang der Seite angezeigt.

WICHTIG: Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

Die Rules Seite enthält zwei Tabs: ein Indicators Tab und ein False Positives Tab. Jeder Tab verfügt über einen zugehörigen Detail Bereich. Der Detail Bereich zeigt Details über den Indikator oder das Falsch Positiv an, das Sie auf dem Raster ausgewählt haben.

Voraussetzungen

- Admin, Analyst, Senior Analyst oder Investigator Privilegien (vollständiger Zugriff)

Indicators Tab

Der Indicators Tab führt die ausgelösten FireEye Regeln und benutzerdefinierten Indikatorregeln an, die in Ihrer Umgebung verwendet werden. Auf diesem Register können Sie benutzerdefinierte Indikatorregeln bearbeiten und löschen. Siehe Intelligenz (Regel) Überblick auf Seite 215.

Klicken Sie auf einen Spaltennamen im Indicators Raster, um die Daten in dem Raster in aufsteigender alphanumerischer Reihenfolge auf den Spaltendaten basierend zu sortieren. Klicken Sie erneut auf den Spaltennamen, um die Rasterdaten in absteigender alphanumerischer Reihenfolge je nach den Spaltendaten zu sortieren. Ein Pfeil links neben dem Spaltennamen zeigt an, wie die Rasterdaten sortiert sind.

Feld	Beschreibung
☐	Wählen Sie einen Indikator aus, für die Sie Maßnahmen ergreifen möchten. Wenn Sie keinen Indikator auswählen, sind keine Maßnahmen möglich.
OS	Die Betriebssystemumgebungen, für die der Indikator gilt: Windows ( ), Mac OS X ( ), Linux ( ) oder All (wenn ein Indikator auf alle unterstützten Betriebssysteme zutrifft).
Name	Der Indikatorname Normalerweise werden diese Namen von FireEye erstellt und können nicht geändert werden. Sie können den Namen eines benutzerdefinierten Indikators ändern.
Active Since	Das Datum und die Uhrzeit, zu der der Indikator das erste Mal auf dem Netzwerk (FireEye) entdeckt wurde oder zu dem System hinzugefügt wurde (benutzerdefinierte Indikatorregeln). Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.
Created By	Die Appliance, Organisation oder Person, die den Indikator erstellt hat.
Category	Die Indikatorkategorie. Die folgenden Kategorien sind möglich: • **Custom**: Indikatorregeln, die Sie erstellt haben • **Imported**: Indikatorregeln, die von SIEM importiert wurden • **FireEye**: Von anderen FireEye Appliances (z.B. NX Serie oder EX Serie), aber nicht von der CM Serie importierte Indikatorregeln • **FireEye-CMS**: von CM Serie importierte Indikatorregeln • **Mandiant Intel**: von DTI importierte Indikatorregeln • **Mandiant Unrestricted intel**: Unbeschränkte FireEye Indikatorregeln, wie z.B. der **FireEye End2End Test** Indikator.

Feld	Beschreibung
Signature	Der Typ der erkannten Bedrohung. Er trifft nur auf FireEye Alarme zu. Typen umfassen **Web infection**, **Infection match**, **Malware object**, **Malware callback** und **Domain match**.
Active Conditions	Die Anzahl der mit diesem Indikator verbundenen Bedingungen. Diese Anzahl schließt die Bedingungen aus, die als falsch positive markiert wurden.
Hosts With Alerts	Die Anzahl von Hosts, die einen oder mehrere Alarme einschließen, die mit dem Indicator of Compromise verbunden sind. Klicken Sie auf die Zahl in diesem Feld, um die nach dem bestimmten Indikator gefilterten Hosts Seite zu öffnen. Dies ermöglicht Ihnen, die Alarme für die bestimmten Hosts zu überprüfen, die von dem Indikator betroffen sind.
Source Alerts	Die Anzahl der mit diesem Indikator verbundenen Quellenwarnunge.

Indicator Tab Detail Abschnitt

Der Detail Abschnitt für den Indicator Tab enthält zwei Tabs, die detaillierte Informationen über den auf dem Indicator Register ausgewählten Indikator anzeigen. Verwenden Sie den Detail Abschnitt, um eine Alarmbedingung als falsch positiv zu markieren. Wählen Sie eine Bedingung im Detail Abschnitt und klicken Sie auf **Mark as false positive**.

Tab	Beschreibung
Indicator Details	Die spezifischen Bedingungen für den ausgewählten Indikator, einschließlich die Typen von Alarmbedingungen in dem Indikator und Informationen über die für die Alarmbedingungen generierten Alarme.
Source Alerts	Die mit dem ausgewählten Indikator verbundenen Informationen über Quellenwarnunge. Wenn viele Quellenwarnunge vorhanden sind, könnte dieser Tab hinter dem Detail Tab umbrechen und scheint zu verschwinden. Wenn dies der Fall ist, verkleinern oder vergrößern Sie die Breite des Browserfensters. Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.

False Positives Tab

Falsch positiv Bedingungen werden auf dem False Positives Tab angezeigt. Siehe Falsch Positiv Regeln verwalten auf Seite 401.

Feld	Beschreibung
Marked By	Der Benutzername der Person, die die Bedingung als falsch positiv markiert hat. Von FireEye als falsch positiv markierte Bedingungen werden in diesem Feld als **FireEye** identifiziert.
Marked	Die Zeit, seit die Bedingung als falsch positiv markiert wurde. Die Einheiten in diesem Feld hängen davon ab, wann die Bedingung als falsch positiv markiert wurde.
Rule Type	Der Regeltyp, der als falsch positiv markiert wurde. Gültige Werte enthalten: IOC (Indicator of Compromise), EXD (Exploit Detection) oder MAL (Malware)
Condition Type	Der Bedingungstyp.

False Positive Tab Detail Abschnitt

Der Detail Abschnitt für den False Positive Tab zeigt detaillierte Informationen über alle falsch positiv IOC, Exploit oder Malware, die auf dem False Positives Tab ausgewählt wurde. Für falsch positiv Malware, die auf dem False Positives Tab ausgewählt wurde, wird kein Detail Fenster angezeigt.

Verwenden Sie das Detail Fenster, um eine falsch positiv Bedingung zurück in eine echte (nicht falsch positiv) Bedingung zu ändern. Wählen Sie eine falsch positiv Bedingung im Detail Abschnitt aus und klicken Sie auf **Undo false positive**.

Feld	Beschreibung
Indicator	Die mit diesem Falsch Positiv verbundenen Indikatordetails. Diese Informationen umfassen den Indikatornamen, den Benutzer, der den Indikator erstellt hat und die Signatur.
False Positive	Die als falsch positiv markierte Bedingung.

Admin Menü

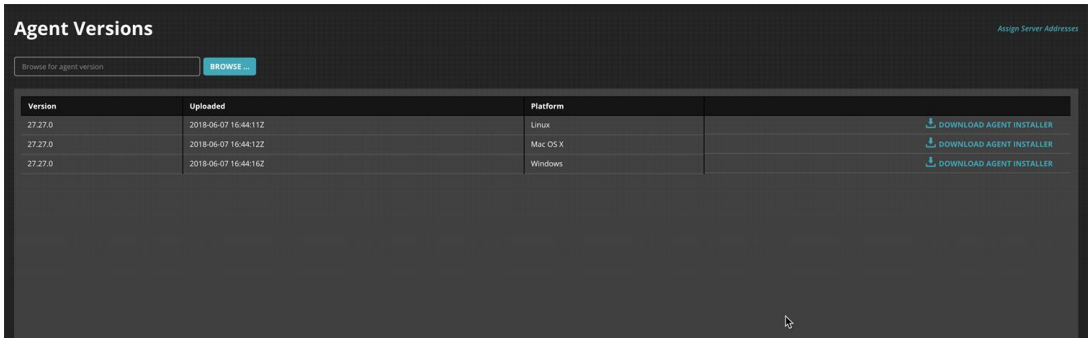
Das Admin Menü enthält die folgenden Optionen. Die in Ihrer Umgebung gezeigte Funktionalität ist je nach der Rolle verschieden, die Ihrem Benutzerkonto zugewiesen wurde und basiert auf den FireEye Lizenzen, die Sie installiert haben.

Option	Beschreibung
Host Sets	Zeigt die Host Sets Seite an, auf der Sie Gruppen oder Sätze von Hosts erstellen können. Sie können beispielsweise einen Hostsatz verwenden, um Hosts zu gruppieren, die als hochwertige Hosts gelten. Siehe Host Sets Seite auf Seite 83.
High-Value Hosts	Zeigt die High-Value Hosts Seite an, auf der Sie Hostsätze auswählen können, die Host enthalten, die für Ihre Organisation von hohem Wert sind. Siehe High-Value Hosts Seite auf Seite 85.
Policies	Zeigt die Policies Seite an, auf der Sie die Endpoint Security Funktionalität dynamisch konfigurieren können.Agent Siehe Richtlinieneinstellungen auf Seite 85.
Agent Versions	Zeigt verfügbare Agent Versionen an und bietet einen Link für den Download des Agent Installers. Siehe Agent Versions Tab auf der nächsten Seite.
Agent Upgrade	Zeigt die Agent Upgrade Seite an, die Ihnen ermöglicht, Aktualisierungsaufgaben für Endpoint Security Software zu erstellen und zu verwalten.Agent Siehe Agent Upgrade Seite auf Seite 86.
Containment Settings	Zeigt die Containment Settings Seite an, die Ihnen ermöglicht, die Endpoint Security Eindämmungsfunktion zu steuern. Siehe Containment Settings Seite auf Seite 86.
Acquisition Settings	Zeigt die Acquisitions Settings Seite an, die Ihnen ermöglicht, die Endpoint Security Erfassungsfunktion zu steuern. Siehe Acquisition Settings Seite auf Seite 88.
Data Acquisition Scripts	Zeigt die Data Acquisition Scripts Seite an, die Ihnen ermöglicht, Datenerfassungsanforderungen zu erstellen und zu verwalten. Siehe Data Acquisition Scripts Seite auf Seite 90.
Disk Utilization Limits	Zeigt die Disk Utilization Limits Seite an, die Ihnen ermöglicht, einen festgelegten Speicherplatz für Triage Sammlungen, Dateierfassungen und Datenerfassungen zuzuweisen. Siehe Disk Utilization Limits Seite auf Seite 91.
Aging Settings	Zeigt die Aging Settings Seite an, die Ihnen ermöglicht, Indikator-, Warnungs- und Hostalterungseinstellungen festzulegen. Siehe Aging Settings Seite auf Seite 92.

Option	Beschreibung
Appliance Settings	Zeigt die Appliance Settings Seite an, die Ihnen ermöglicht, Appliance Einstellungen zu verwalten. Dazu gehören Datum und Uhrzeit der Appliance, Userkonten, DTI-Informationen, Benachrichtigungen, Netzwerkeinstellungen, Zertifikate, Schlüssel, Sicherung/Wiederherstellung, Lizenzen und das Anmeldebanner. Siehe Appliance Settings Seite auf Seite 94.
Alert Settings	Zeigt die Alert Settings Seite an, die Ihnen ermöglicht, die Höchstzahl der Alarmmeldungen festzulegen, die für einen einzelnen Infektionsnamen für einen bestimmten Zeitintervall für einen beliebigen Warnungstypen auf der Seite empfangen werden. Siehe Alert Settings Seite auf Seite 95.
Triage Settings	Zeigt die Automatic Triage Settings Seite an, die Ihnen ermöglicht, Einstellungen für automatische Triage-Erfassungen für Alarme zu konfigurieren sowie die Zeitspanne vor und nach dem Ereignis-Zeitstempel, in dem Registrierungsaudit und URL-Ereignissammlung erfasst wird. Siehe Automatic Triage Settings Seite auf Seite 96.

Agent Versions Tab

Agent Images werden auf dem Agent Version Tab aufgeführt. Um auf den Agent Versions Tab zuzugreifen, wählen Sie **Agent Versions** auf dem **Admin** Menü. Auf diesem Tab können Sie die verfügbaren Agent Images anzeigen und herunterladen, ein Agent Image hochladen oder auf die Agent Default Policy Seite gehen, um Serveradressen zuzuweisen.



Um ein FireEye Agent Image herunterzuladen:

1. Finden Sie die Zeile, die das Agent Image für die Endpoint Security Agent Version und Plattform von Interesse enthält.
2. Klicken Sie auf Download Agent Installer**.**

   Die komprimierte Datei wird heruntergeladen.

Um ein FireEye Agent Image hochzuladen:

1. Klicken Sie auf **Browse**.
2. Finden und wählen Sie die Agent Image-Datei in der Dateiauswahl.
3. Klicken Sie auf **Open**.

Um eine Server-Adresse zuzuweisen:

1. Klicken Sie in der oberen rechten Ecke auf **Assign Server Addresses**.

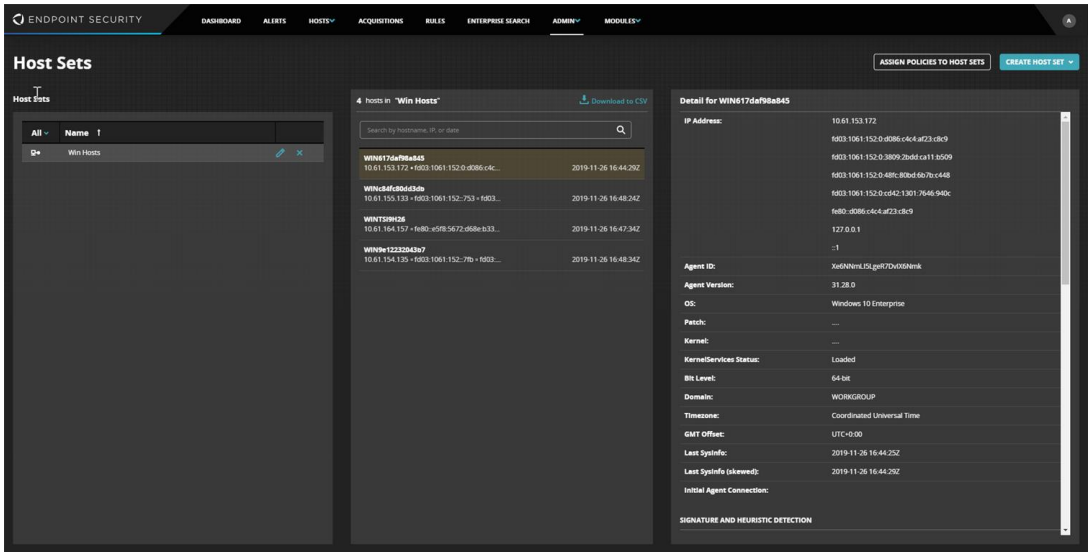
   Sie werden auf die Edit Policy Seite für die Agent Default Richtlinie umgeleitet.
2. Klicken Sie auf den **Server Address** Tab.
3. Verwalten Sie Server, wie im "Policy" Abschnitt des *Endpoint Security Agent Administrationshandbuch* beschrieben.

Weitere Informationen finden Sie im *Endpoint Security Agent Administrationshandbuch*.

Host Sets Seite

Sie können Informationen über bestimmte Gruppen von Hosts anzeigen und melden, indem Sie Hostsätze erstellen. Sie können beispielsweise einen Hostsatz verwenden, um Hosts zu gruppieren, die als hochwertige Hosts gelten. Um auf die Host Sets Seite zuzugreifen, wählen Sie **Host Sets** auf dem **Admin** Menü.

Die Host Sets Seite der Endpoint Security ermöglicht Ihnen, Hostsätze zu erstellen und zu verwalten. Sie können Hostsätze, die jeweils zugehörigen Hosts und die Details für jeden Host in dem Satz auch überprüfen. Von dieser Seite aus können Sie auch Richtlinien an einen ausgewählten Hostsatz zuweisen.



Die Host Sets Seite besteht aus drei Teilen: einer Liste vorhandener Hosts, einer Liste der Hosts in einem Hostsatz und einem Host Detail Fenster. Klicken Sie auf **Create Host set**, um einen neuen Hostsatz mit Hilfe des Standard Hostsatz Builders oder statischen Satzlisten zu erstellen. Weitere Informationen über die Einstellung von Hostsätzen finden Sie unter Hostsätze konfigurieren auf Seite 185.

Klicken Sie auf **Assign Policies to Host Sets**, um Richtlinien einem Hostsatz zuzuweisen. Weitere Informationen über die Zuweisung von Richtlinien an Hostsätze finden Sie unter Einem Hostsatz eine Richtlinie zuweisen auf Seite 198.

Voraussetzungen

- Admin oder Operator Zugriff (Vollzugriff)
- Analyst, Senior Analyst oder Investigator Zugriff (schreibgeschützter Zugriff)

Host Sets Liste

Die Host Sets Liste zeigt die Hostsätze an, die derzeit auf dem Netzwerk eingestellt sind.

Feld	Beschreibung
All	Der Typ des Hostsatzes.  Standard Satz - Dynamischer Hostsatz, der auf einer Hostdefinition basiert. Die Hostdefinition ist im Set-Builder auf der Endpoint Security Web-UI definiert.  Statischer Satz - Statischer Host Satz, der in der statischen Hostliste definiert ist.
Name	Der Name jedes Hostsatzes.
	Klicken Sie auf das Bearbeiten Symbol, um Änderungen an dem Hostsatz vorzunehmen.
	Klicken Sie auf das Löschen Symbol, um den Hostsatz zu löschen.

Hosts Liste

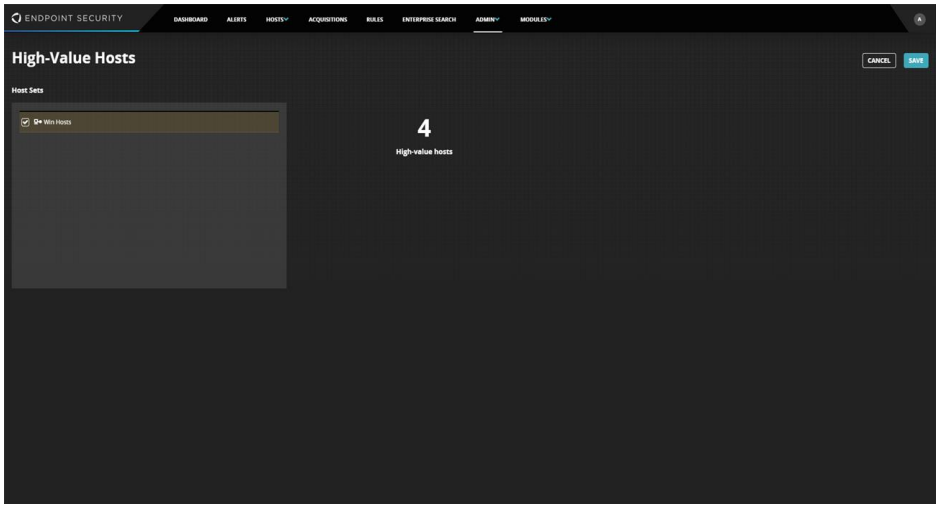
In diesem Abschnitt werden alle Hosts aufgeführt, die dem ausgewählten Hostsatz zugeordnet sind.

Host Detail Fenster

Das Host Detail Fenster zeigt Details für den in der Hosts Liste ausgewählten Host an. Informationen über die Daten in diesem Fenster finden Sie unter Host Details auf Seite 65.

High-Value Hosts Seite

Die High Value Hosts Seite ermöglicht Ihnen, Hostsätze auszuwählen, die wichtige Hosts für Ihre Organisation enthalten. Mindestens ein Hostsatz muss definiert sein. Um auf die High-Value Hosts Seite zuzugreifen, wählen Sie **High-Value Host** auf dem **Admin** Menü.



Wählen Sie das Kontrollkästchen neben einem Hostsatz im linken Bereich, um die Anzahl der hochwertigen Hosts, die im rechten Abschnitt angezeigt werden, zu erhöhen. Weitere Informationen finden Sie unter Hochwertige Hosts identifizieren.

Voraussetzungen

- Admin Zugriff

Richtlinieneinstellungen

Die Policies Seite ermöglicht Ihnen, Agent-Funktionalität dynamisch zu konfigurieren, indem Sie Richtlinien definieren, die Sie auf Hosts und Hostsätze anwenden können. Um auf die Policies Seite zuzugreifen, wählen Sie **Policies** auf dem **Admin** Menü. Endpoint Security wird mit der Agent Defauls Richtlinie geliefert und kann zusätzliche Richtlinien konfigurieren. Weitere Informationen über Richtlinien finden Sie im Endpoint Security Agent Administrationshandbuch.

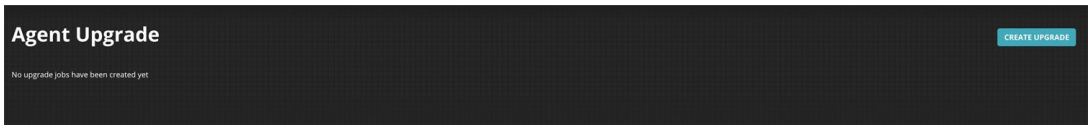
Um Richtlinien auf Hostsätze anzuwenden, sehen Sie Einem Hostsatz eine Richtlinie zuweisen auf Seite 198.

Voraussetzungen

- Admin Zugriff

Agent Upgrade Seite

Endpoint Security Agent Softwareaktualisierungen können mit Hilfe von Upgrade-Aufgaben ausgeführt werden. Die Agent Upgrade Seite ermöglicht Ihnen, Upgrade-Aufgaben zu erstellen und zu verwalten. Weitere Informationen über die Verwaltung von Ugrade-Aufgaben finden Sie unter "Agent Software aufrüsten" im *Endpoint Security Agent Administrationshandbuch*.



Um auf die Agent Upgrade Seite zuzugreifen, wählen Sie **Agent Upgrade** auf dem **Admin** Menü.

Klicken Sie auf die **Create upgrade** Schaltfläche, um eine Aktualisierungsaufgabe zu erstellen.

Voraussetzungen

- Admin oder Operator Zugriff

Containment Settings Seite

Verwenden Sie die Containment Settings Seite, um die Endpoint Security Eindämmungsfunktion zu steuern:

- Die Eindämmungsfunktion ein- oder ausschalten.
- Hostsätze identifizieren, die von der Eindämmung ausgeschlossen werden sollen
- Eine Whiteliste von IP-Adressen erstellen, mit denen eingedämmte Host-Endpunkte weiterhin kommunizieren können

  WICHTIG: Whitelisting funktioniert nur, wenn eine direkte Verbindung zwischen Ihrem Host-Endpunkt und einem verbundenen System besteht. Wenn Ihr eingedämmter Host mit anderen System über den Proxy-Server verbunden ist, können Sie die eingedämmte Host IP-Adresse nicht whitelisten.

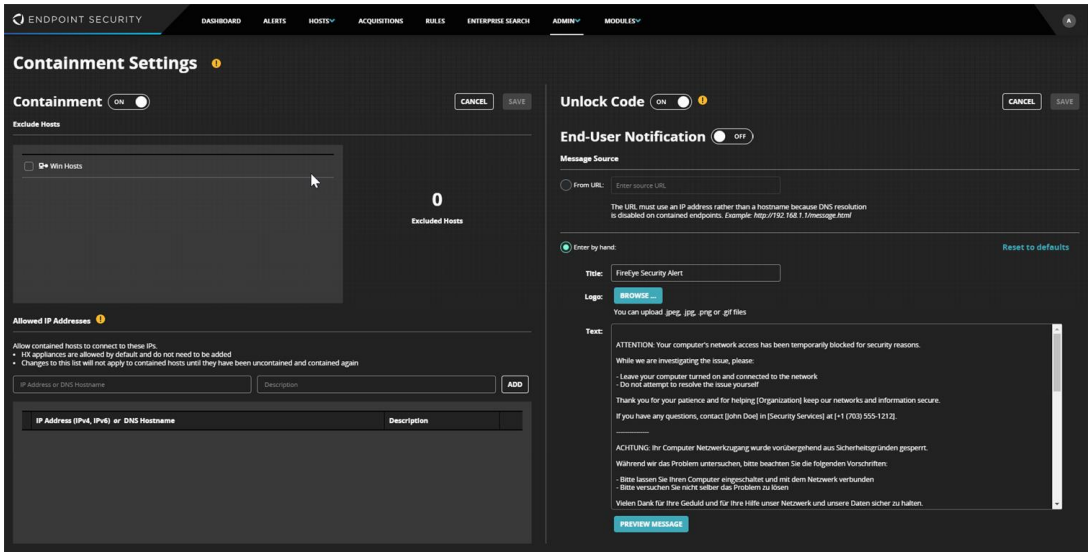
- Schalten Sie die Containment Freischaltcode Funktion ein oder aus.

WICHTIG: Der Containment Freigabecode wird nur für Windows Agents Version 28 oder später unterstützt. Er wird nicht für Endpunkte unterstützt, die Windows XP ausführen.

Der Eindämmungs-Freischaltcode wird nur für macOS Agents mit Version 30 oder später unterstützt

- Eine automatische Benachrichtigung über die Eindämmung eines Host Endpunkts einrichten, entweder mit Hilfe einer direkten Nachricht oder einer Webseitenumleitung.

Vollständige Informationen finden Sie unter Eindämmung konfigurieren.



Um auf die Containment Settings Seite zuzugreifen, wählen Sie **Containment Settings** auf dem **Admin** Menü.

Voraussetzungen

- Admin Zugriff

Containment Schalter

Verwenden Sie den **Containment** Schalter am Anfang der Seite, um die Fähigkeit, Hosts einzudämmen, ein- und auszuschalten.

HINWEIS: Wenn Eindämmung deaktiviert ist (in der Endpoint Security Web-UI wird DISABLED angezeigt), können Sie es nicht ein- oder ausschalten. Sie müssen Eindämmung zunächst mit Hilfe der CLI aktivieren. Siehe Zugriff auf Eindämmung blockieren und freigeben auf Seite 155 und Eindämmung ein- und ausschalten auf Seite 156.

Exclude Hosts Liste

Die Exclude Hosts Liste zeigt die Hostsätze an, die derzeit auf Ihrer Appliance definiert sind. Wählen Sie einen Hostsatz, der von der Eindämmung ausgeschlossen werden soll. Weitere Informationen finden Sie unter Hostsätze von Eindämmung ausschließen auf Seite 158.

Allowed IP Addresses Liste

Die Allowed IP Addesses Liste zeigt die IP-Adressen an, mit denen eingedämmte Hosts kommunizieren können. Sie können IP-Adressen von dieser Liste hinzufügen oder entfernen. Weitere Informationen finden Sie unter Die Whitelist für eingedämmte Hosts verwalten auf Seite 161.

Unlock Code Switch

Mit dem Containment **Unlock Code** Switch können Sie die Option ein- und ausschalten, einen Freischaltcode für die Auslösung eines Host-Endpunktes aus der Eindämmung von der Endpoint Security Web-UI anzufordern.

End-User Notification Abschnitt

Verwenden Sie den **End-User Notification** Schalter am Anfang der Seite, um Benachrichtigungen über Eindämmung ein- und auszuschalten. Sie können eine URL festlegen, auf die Host umgeleitet werden, wenn sie eingedämmt sind, oder eine direkte Nachricht festlegen, die an Hosts gesendet wird, wenn sie eingedämmt werden. Weitere Informationen finden Sie unter Endbenutzer über Host-Eindämmung benachrichtigen auf Seite 166.

Acquisition Settings Seite

Verwenden Sie die Acquisition Settings Seite, um die Endpoint Security Server Erfassungsfunktion zu steuern.

- Datei- und Datenerfassungen ein- oder ausschalten
- Automatische Triage Erfassungen ein- oder ausschalten
- Zeitspannen für Registrierungsaudit und URL Ereignissammlung in Tragen definieren

Vollständige Informationen finden Sie unter Forensische Daten analysieren.

Um auf die Acquisition Settings Seite zuzugreifen, wählen Sie **Acquisition Settings** auf dem **Admin** Menü

Voraussetzungen

- Admin Zugriff

File & Data Acquisition Schalter

Der **File & Data Acquisition** Schalter am Anfang der Seite gibt Ihnen die Fähigkeit, die Ausführung von Datei- und Datenerfassungen (ON) ein- und (OFF) auszuschalten.

Automatic Triage Schalter

Der **Automatic Triage** Schalter gibt Ihnen die Fähigkeit, die Ausführung von automatischen Triage Erfassungen (ON) ein- und (OFF) auszuschalten. Automatische Triage wird auf Windows, macOS und Linux Endpunkten unterstützt.

HINWEIS: Triagen können für Linux Endpunkte durchgeführt werden, die Endpoint Security Agent Version 30 oder später ausführen.

WICHTIG: Malware Alarme in Windows Umgebungen lösen unabhängig von dieser Einstellung keine automatische Triage aus.

Timestamp Triage Settings

Die Timestamp Triage Einstellungen ermöglichen Ihnen, die Zeitspanne um den Zeitstempel einer Triage festzulegen, in dem Registrierungsaudit- und URL-Ereigness gesammelt werden.

Feld	Beschreibung
seconds before timestamp	Die Anzahl der Sekunden *vor* der Zeitstempel, in dem Registrierungsaudit- und URL-Ereignisse für Triage Anforderungen gesammelt werden sollen.

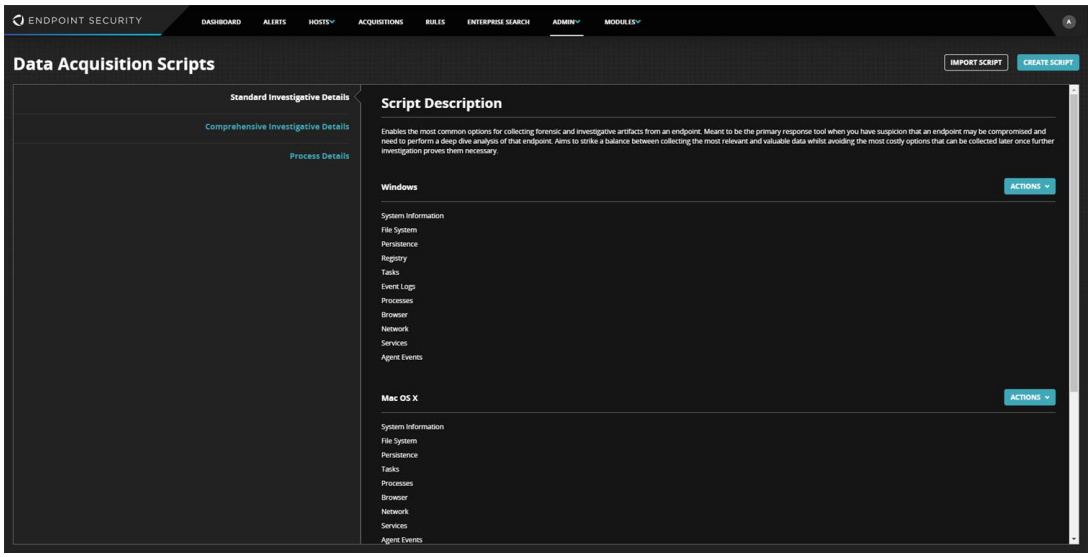
Feld	Beschreibung
seconds after timestamp	Die Anzahl der Sekunden *nach* der Zeitstempel, in dem Registrierungsaudit- und URL-Ereignisse für Triage Anforderungen gesammelt werden sollen.

Data Acquisition Scripts Seite

Verwenden Sie die Data Acquisition Scripts Seite, um Datenerfassungsscripte zu erstellen und zu verwalten, die bei Datenerfassungsanforderungen von Ihren Host Endpunkten verwendet werden. Datenerfassungsanforderungen ermöglichen Ihnen, alle benötigten Daten von einem einzigen laufenden Endpunkt zu erfassen.

Mehrere Scripte werden von FireEye bereitgestellt . Sie können diese Scripts nicht löschen, obwohl Sie sie bearbeiten oder kopieren und als Grundlage für Ihr eigenes Script verwenden können. Wenn Sie sie bearbeitet haben, können Sie sie auch auf ihre werksseitig verteilte Form zurücksetzen.

Vollständige Informationen finden Sie unter Datenerfassungsscripts verwalten auf Seite 121 und Eine Datenerfassung anfordern auf Seite 321.



Um auf die Data Acquisition Scripts Seite zuzugreifen, wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü.

Voraussetzungen

- Admin, Analyst, Senior Analyst oder Investigator Zugriff
- Einige Funktionen erfordern die Endpoint Security Power Lizenz.

Create Script Schaltfläche

Klicken Sie auf die **Create Script** Schaltfläche, um den Prozess zum Erstellen eines neuen Scripts zu starten.

Import Script Schaltfläche

Klicken Sie auf die **Import Script** Schaltfläche, um mit dem Import eines neuen Scripts zu beginnen.

Scriptliste

Die Scriptliste links auf der Seite führt bekannte Scripts auf. Wenn Sie ein Script auswählen, wird seine Definition im Scriptdetail Bereich angezeigt und ein **Actions** Dropdown Menü wird über den Scriptdetails angezeigt. Sie können:

- Das Script löschen
- Den Titel und die Beschreibung des Scripts ändern
- Datenerfassungsanforderungen für ein anderes Betriebssystem hinzufügen
- Ein Datenerfassungsscript für ein anderes Betriebssystem importieren

Achten Sie darauf, auf **Save** zu klicken, um Ihre Einstellungen zu speichern, wenn Sie Änderungen am Script vorgenommen haben.

Scriptdetail Bereich

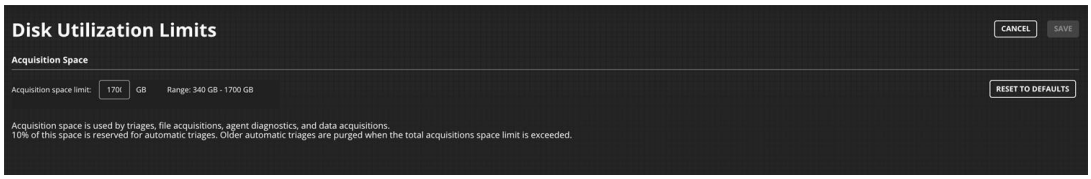
Der Scriptdetail Bereich zeigt die Definition eines ausgewählten Scripts an. Das Script für jede Plattform enthält ein Actions Dropdown Menü. Die Aktionen, die Sie für das Script für ein einzelnes Betriebssystem auswählen können, umfassen:

- Löschen des Scripts für dieses Betriebssystem
- Bearbeiten des Scripts für dieses Betriebssystem
- Exportieren des Scripts für dieses Betriebssystem

Disk Utilization Limits Seite

Verwenden Sie die Disk Utilization Limits Seite, um die Speichermenge zu steuern, die von der HX Appliance für die Speicherung aller Akquisitionen (Datei, Daten und Triage) verwendet wird. Zehn Prozent des Speicherplatzes sind für automatische Triage Erfassungen reserviert. Wenn der gesamte Erfassungsbereich überschritten ist, werden die ältesten automatischen Triagen gelöscht.

Vollständige Informationen finden Sie unter Datenträgerauslastungslimits für Erfassungen festlegen auf Seite 102.



Um auf die Disk Utilization Limits Seite zuzugreifen, wählen Sie **Disk Utilization Limits** auf dem **Admin** Menü.

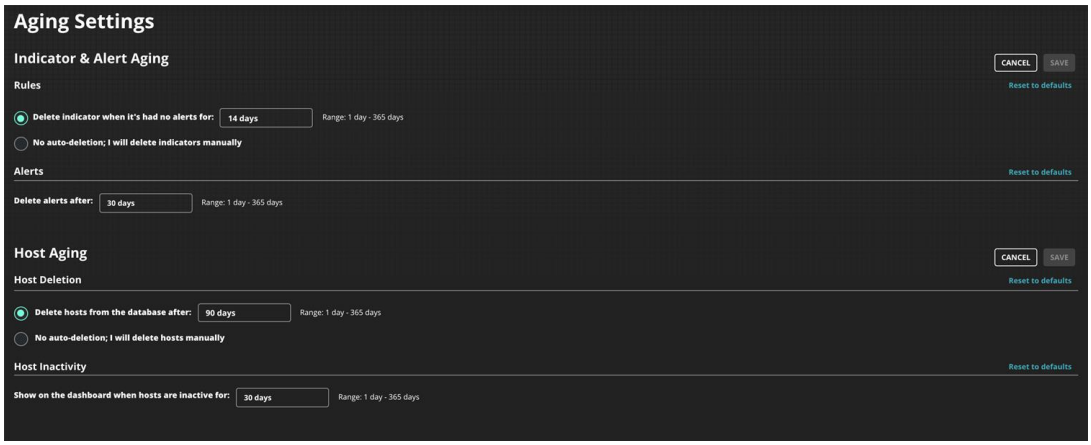
Voraussetzungen

- Admin Zugriff

Aging Settings Seite

Verwenden Sie die Aging Settings Seite, um zu steuern, wie lange der Endpoint Security Indikatorregeln, Alarme und Host-Endpunkte speichert.

Vollständige Informationen finden Sie unter Alterung von Indikatorregeln auf Seite 235 und Host Alterungsintervalle festlegen auf Seite 177.



Die Aging Settings Seite hat zwei Teile: einen Indicator & Alert Aging Abschnitt und einen Host Aging Abschnitt.

Um auf die Aging Settings Seite zuzugreifen, wählen Sie **Aging Settings** auf dem **Admin** Menü.

Voraussetzungen

- Admin Zugriff

Indicator & Alert Aging Einstellungen

Die Indicator & Alert Aging Einstellungen ermöglichen Ihnen festzulegen, wie oft Indikatorregeln und Alarme, die von FireEye Appliances stammen, vom System gelöscht werden. (Benutzerdefinierte Indikatorregeln sind von diesen Einstellungen nicht betroffen.)

Feld	Betrifft	Beschreibung
Delete indicator rule when it's had no alerts for...	Indikatorregeln	Stellt die Anzahl der Tage ein, nach denen ein Indikator, der keine Alarme ausgelöst hat, automatisch gelöscht wird. Gültige Werte liegen zwischen 1 Tag und 365 Tagen. Wenn Sie diese Einstellung auswählen, können Sie die **No auto-deletion** Einstellung nicht auswählen.
No auto-deletion; I will delete indicator rules manually	Indikatorregeln	Gibt an, dass Indikatorregeln niemals automatisch gelöscht werden sollen. Wenn Sie diese Einstellung auswählen, können Sie die **Delete indicator when...** Einstellung nicht auswählen.
Delete alerts after	Alarme	Legt die Anzahl der Tage fest, nach denen Alarme gelöscht werden. Gültige Werte liegen zwischen 1 Tag und 365 Tagen.

Klicken Sie für jede dieser Einstellungen auf **Reset to defaults**, um zu den Standardwerten zurückzukehren.

Host Aging Einstellungen

Mit den Host Aging Einstellungen können Sie angeben, wie oft Hosts vom System gelöscht werden und ob inaktive Hosts in Dashboard Statistiken enthalten sind.

Feld	Beschreibung
Delete hosts from the database after ...	Setzt die Anzahl von Tagen fest, nach denen ein Host automatisch gelöscht wird. Gültige Werte liegen zwischen 1 Tag und 365 Tagen. Wenn Sie diese Einstellung auswählen, können Sie die **No auto-deletion** nicht auswählen.

Feld	Beschreibung
No auto-deletion; I will delete hosts manually	Zeigt an, dass Hosts niemals automatisch gelöscht werden sollen. Wenn Sie diese Einstellung auswählen, können Sie die **Delete hosts from the database...** Einstellung nicht auswählen.
Show on the dashboard when hosts are inactive for	Setzt die Anzahl der Tage fest, für die ein Host inaktiv sein muss, bevor er in die inaktive Hosts Tabelle des Dashboards aufgenommen wird. Gültige Werte liegen zwischen 1 Tag und 365 Tagen.

Klicken Sie für jede dieser Einstellungen auf **Reset to defaults**, um zu den Standardwerten zurückzukehren.

Appliance Settings Seite

Die Appliance Settings Seite der Endpoint Security ermöglicht Ihnen, Endpoint Security Einstellungen beizubehalten und enthält die folgenden Optionen. Die in Ihrer Umgebung angezeigten Funktionalität kann je nach der Ihrem Benutzerkonto zugewiesenen Rolle variieren.

Option	Beschreibung
Date and Time	Zeigt die Date and Time Settings Seite an. Verwenden Sie diese Seite, um das Datum, die Uhrzeit und die Zeitzone Ihres Servers einzustellen. Sehen Sie "Datum und Uhrzeiteinstellungen einstellen" im *Endpoint Security Server-System-Administrationshandbuch*.
User Accounts	Zeigt die User Accout Settings Seite an. Verwenden Sie diese Seite, um User hinzuzufügen oder zu entfernen oder ihre Konto-Passwörter zurückzusetzen. Sehen Sie "Authentifizierung" und "Autorisierung" im *FireEye System-Sicherheitshandbuch*.
DTI Network	Zeigt die DTI Network Settings Seite an. Verwenden Sie diese Seite, um die Integration zwischen der FireEyeDynamic Threat Intelligence (DTI) Cloud und Ihrem Endpoint Security zu verwalten. Sehen Sie das "Das DTI Netzwerk" im *Endpoint Security Server-System-Administrationshandbuch*.
Benachrichtigungen	Zeigt die Notifications Settings Seite an. Verwenden Sie diese Seite, um Alarmmeldungen für den Endpoint Security zu konfigurieren. Sehen Sie Ereignisbenachrichtigungen" im *Endpoint Security Server-System-Administrationshandbuch*.

Option	Beschreibung
Network	Zeigt die Network Settings Seite an. Verwenden Sie diese Seite, um die Netzwerkintegration Ihres Endpoint Security zu verwalten. Sehen Sie "Netzwerkverwaltung" im *Endpoint Security Server-System-Administrationshandbuch*.
Certificates/Keys	Zeigt die Certificate Managment Seite an. Verwenden Sie diese Seite, um Zertifikate und Schlüssel für Ihren Endpoint Security zu verwalten. Sehen Sie "Zertifikate" im *FireEye System-Sicherheitshandbuch*.
Appliance Backup & Restore	Zeigt die Backup and Restore Seite an. Verwenden Sie diese Seite, um den für eine Serversicherung erforderlichen Speicherraum zu schätzen, Ihren Server zu sichern, eine Sicherungsdatei hochzuladen und den Server von einer früheren Sicherung wiederherzustellen. Sehen "Datenbank sichern und wiederherstellen" im *Endpoint Security Server-System-Administrationshandbuch*.
Appliance Licenses	Zeigt die Appliance License Settings Seite an. Verwenden Sie diese Seite, um Ihre Endpoint Security Lizenzen zu verwalten. Sehen Sie "Lizenzschlüssel" im *Endpoint Security Server-System-Administrationshandbuch*.
Login Banner	Zeigt die Login Banner Seite an. Verwenden Sie diese Seite, um den Bannertext für Ihren Server zu ändern. Dieser Bannertext wird auf den Endpoint Security Web-UI und SSH Anmeldeseiten angezeigt. Sehen Sie "Anmeldebanner und Nachrichten anpassen" im *Endpoint Security Server-System-Administrationshandbuch*.

Alert Settings Seite

Verwenden Sie die Alert Settings Seite, um die Höchstzahl der Alarmmeldungen festzulegen, die Sie für einen einzelnen Infektionsnamen innerhalb der definierten Zeitspanne für jeden der auf der Seite aufgeführten Warnungstypen empfangen können. Die Warnungstypen sind Real Time Indicator Detection (IOC), Malware Detection (MAL) und Process Guard (PRO), wenn Sie das Process Guard Modul installiert und aktiviert haben. Um auf die Alert Settings Seite zuzugreifen, klicken Sie auf dem Admin Menü auf **Alert Settings**.

Informationen über die Benutzung dieser Seite finden Sie unter Einstellungen der Grenzwerte für die Warnungsrate festlegen.

Automatic Triage Settings Seite

Verwenden Sie die Automatic Triage Settings Seite, um die Anzahl der Triage-Anfragen zu steuern, so dass Ihre Agents nicht überlastet werden. Sie können die Triage Settings Seite verwenden, um die Erfassung von Triage-Paketen je nach Warnungstypen zu steuern. Die Automatic Triage Settings Seite enthält Tabs für Automatic Triages und Timestamp Settings. Diese Konfigurationseinstellungen bestimmen, ob eine Triage ausgelöst werden sollte. Wenn das konfigurierte Ratenlimit für die Triage nicht überschritten wurde, wird die Triage für den Alarm ausgelöst.

Sie können auch den Timestamp Settings Tab auf der Automatic Triage Settings Seite verwenden, um den Zeitraum vor und nach dem Ereignis-Zeitstempel festzulegen, für den Daten gesammelt werden.

Automatische Triage-Einstellungen sind standardmäßig aktiviert, was bedeutet, dass auto-Triage für alle unterstützten Warnungstypen aktiviert ist. Administratoren können die Konfigurationseinstellungen verwenden, um Auto-Triage vollständig zu deaktivieren oder automatische Triage für bestimmte Warnungstypen zu deaktivieren.

Die Triage Settings Seite unterstützt sowohl ältere als auch neue Alarme, einschließlich die folgenden Warnungstypen:

- IOC
- ExD
- PRO (Dieser ist nur verfügbar, wenn Sie das Process Tracker Modul in Verbindung mit dem Enricher Modul verwenden und Sie diese Module zum Generieren von PRO Alarmen konfiguriert haben.

HINWEIS: Wenn automatische Triage ausgeschaltet ist, können Sie weiterhin manuell Triage-Sammlungen anfordern.

Modules Menü

Das Modules Menü führt alle in Ihrer Endpoint Security Web-UI installierten und aktivierten Module auf, sowie die Module, die zum Download verfügbar sind. Bei Modulen handelt es sich um Funktionssätze oder Erweiterungen, die Sie zur Endpoint Security Web-UI hinzufügen können und direkt an einen zugewiesenen Hostsatz Ihrer Wahl senden können.

Einige Module, die *System Modules* genannt werden, sind im Endpoint Security Produkt enthalten und diese Module sind standardmäßig aktiviert. Sie können zusätzliche Module direkt aus dem FireEye Market installieren oder über den Additional Modules Tab von der DTI herunterladen. Informationen über Systemmodule sind in der *Endpoint Security Server-Bedienungsanleitung* enthalten. Informationen über die zusätzlich installierten User Module und deren Konfiguration finden Sie in einer individuellen Bedienungsanleitung für jedes

Modul. Sie können diese individuellen Bedienungsanleitungen für die Modulseiten vom FireEye Market herunterladen.

Nachdem Sie ein Modul installiert und aktiviert haben, wird es im Modules Menü auf Ihrer Endpoint Security Web-UI angezeigt.

Endpoint Module Administration

Endpoint Module Administration bietet eine Benutzerschnittstelle (UI), auf der Sie alle Aspekte Ihres Endpoint Security Modules verwalten können. Die Modules Seite enthält separate Tabs für System Modules, Installed Modules und Available Modules. Auf dem System Modules Tab werden alle Module angezeigt, die in Endpoint Security enthalten sind. Der Installed Modules Tab zeigt alle Module an, die Sie auf Ihrer Endpoint Security Instanz installiert haben. Der Available Modules Tab führt alle Module auf, die Sie herunterladen und installieren können. Diese Module können von FireEye Market oder von der DTI heruntergeladen werden.

Sie können die Modules Seite der Endpoint Module Administration zum Anzeigen einer Liste aller auf Ihrer Endpoint Security Web-UI installierten Module verwenden, bestätigen, welche Module System Modules und welche Installed Modules sind, eine Liste von Modulen überprüfen, die zum Herunterladen verfügbar sind, Module aktivieren und deaktivieren und die Konfiguration und Web-UI Seiten für individuelle auf der Seite aufgeführte Module abrufen.

TEIL II: Konfiguration

KAPITEL 3: Erfassungseinstellungen konfigurieren

Erfassungseinstellungen steuern, wie Ihre Agents Informationen über Triage-, Daten und Dateierfassungen vom Endpunkt Host sammeln und melden. Triage-, Daten- und Dateierfassungen fordern Daten vom Agent über verdächtige Dateien und Aktivitäten auf dem Host Endpunkt zum Zeitpunkt einer Warnung an. Informationen über Triageerfassungen werden in einer `.mans` Datei gesammelt; Informationen über Dateierfassen werden in einer `.zip` Datei gesammelt.

Triage Informationen werden auf der Endpoint Security Web-UI bereitgestellt. Wenn eine Triage angefordert wurde und die Endpoint Security Appliance feststellt, dass die Daten signifikant sind, kann eine hochwertige Zusammenfassung der Triagedaten auf der Triage Summary Seite angezeigt werden. Die vollständige Triage `.mans` Datei kann jederzeit mit Hilfe von Redline heruntergeladen und überprüft werden. Siehe Forensische Daten erfassen.

Die Standard Erfassungseinstellungen liefern optimale Informationen über die meisten Unternehmen. Administratoren können die folgenden Einstellungen ändern:

- Einstellungen für Dateierfassung konfigurieren auf Seite 108
- Alterungseinstellungen für Erfassungen konfigurieren auf Seite 104
- Beschränkungen für ausstehende Erfassungsaufgaben einstellen auf Seite 103
- Datenträgerauslastungslimits für Erfassungen festlegen auf der nächsten Seite
- Automatische Triage-Einstellungen konfigurieren auf Seite 111
- Einstellungen für automatische Triage Drosselung konfigurieren auf Seite 113
- Zeitstempel-Einstellungen konfigurieren auf Seite 118

Datenträgerauslastungslimits für Erfassungen festlegen

Triagen, Dateiakquisitionen und Datenerfassungen können sich im Laufe der Zeit ansammeln und eine wachsende Menge an Speicherplatz belegen. Um die zu steuern, können Sie einen festgelegten Speicherraum für sie bestimmen.

Zehn Prozent des von Ihnen festgelegten Speicherplatzes sind für automatische Triage-Erfassungen reserviert. Wenn der gesamte zugewiesene Erfassungsbereich überschritten wird, werden die ältesten automatischen Triagen gelöscht.

Wenn die Gesamtgröße des Datenträgers für abgeschlossene Erfassungen ein festgelegtes Limit überschreitet, löscht die Endpoint Security Appliances die ältesten abgeschlossenen Akquisitionen, bis genügender Speicherplatz geschaffen ist, um den Gesamtwert unter das festgelegte Limit zu bringen. Erfassungen, die noch nicht abgeschlossen sind, sind nicht betroffen.

Die Endpoint Security Appliance löscht Erfassungen automatisch, wenn ein Administrator, Analyst oder Investigator die Endpoint Security Web-UI verwendet, um den zugehörigen Agent manuell zu löschen.

Voraussetzungen

- Admin Zugriff

Datenträgerausnutzungslimits mit Hilfe der Web-UI festlegen

Um Auslastungslimits von Datenträgern für abgeschlossene Erfassungen mit Hilfe der Web-UI festzulegen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Disk Utilization Limits** vom **Admin** Menü.
3. Im **Acquisition space limit** Bereich legen Sie den maximal verfügbaren Speicherplatz (in GB) fest, der für die Speicherung von Triage-, Datei- und Datenerfassungen verwendet werden kann. Gültige Werte und Standard sind je nach Ihrem Endpoint Security Appliance Modell unterschiedlich. Die für Ihr Modell geeigneten Werte werden auf der Disk Utilization Limits Seite angezeigt.
4. Klicken Sie auf **Save**.

Datenträgerausnutzungslimits mit Hilfe der CLI festlegen

Um die Datenträgerausnutzungslimits für abgeschlossene Erfassungen mit Hilfe der CLI zu ändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Ändern Sie das Speicherplatzlimit für abgeschlossene Erfassungen:

   ```
   hostname (config) # hx server acquisition aging disk-limit <MB>
   ```

   Geben Sie für <MB> die maximale Speicherplatzgröße (in MB) an, die zum Speichern von Triage-, Datei- und Datenerfassungen verwendet werden kann. Gültige Werte und Standard sind je nach Ihrem Endpoint Security Appliance Modell unterschiedlich. Die für Ihr Modell geeigneten Werte werden in der Hilfe für diesen Befehl angezeigt (geben Sie `hx server acquisition aging disk-limit ?` ein).).

   Um das Standard Speicherplatzlimit für abgeschlossene Erfassungen wiederherzustellen:

   ```
   hostname (config) # no hx server acquisition aging disk-limit
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Beschränkungen für ausstehende Erfassungsaufgaben einstellen

Die Endpoint Security Appliance beschränkt die Anzahl der Erfassungsaufgaben, die für die Wartung von Erfassungsanfragen verfügbar sind. Wenn mehr Anfragen als die konfigurierte Höchstmenge vorliegen, werden diese ausgesetzt (ausstehend) Wenn eine Erfassungsaufgabe abgeschlossen wird, erstellt Endpoint Security neue Aufgaben (bis zu der konfigurierten Höchstzahl), bis alle Anfragen in der Warteschleife bearbeitet sind. Sie können die Höchstzahl ausstehender Aufgaben für die Appliance mit Hilfe des `hx server triage task-limit` CLI-Befehls konfigurieren.

Ausstehende Aufgaben werden automatisch gelöscht, wenn sie die festgelegten Alterungslimits für ausstehende Akquisitionen überschreiten. Um diese Einstellung zu steuern, sehen Sie Die Alterungsperiode für ausstehende Erfassungen mit Hilfe der CLI festlegen auf Seite 107

Die Endpoint Security Appliance löscht Erfassungen automatisch, wenn ein Administrator, Analyst oder Investigator die Endpoint Security Web-UI verwendet, um den zugehörigen Agent manuell zu löschen.

Voraussetzungen

- Admin Zugriff

Um die Höchstzahl ausstehender Erfassungsaufgaben mit Hilfe der CLI zu ändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Ändern Sie die Höchstzahl ausstehender Erfassungsaufgaben:

   ```
   hostname (config) # hx server triage task-limit number
   ```

   Die Standard Höchstzahl ausstehender Erfassungsaufgaben ist **100**. Der Bereich für diese Einstellung ist 0-65535. Wenn Sie das Maximum auf 0 setzen, wird das Limit deaktiviert.

   Um die Standard Höchstzahl ausstehender Erfassungsaufgaben wiederherzustellen:

   ```
   hostname (config) # no hx server triage task-limit
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Alterungseinstellungen für Erfassungen konfigurieren

Sie können steuern, wie lange Triage-, Daten- und Dateiakquisitionsanfragen und -ergebnisse beibehalten werden. Sie können diese Einstellungen mit Hilfe von CLI Befehlen konfigurieren; diese Funktionalität ist nicht über die Endpoint Security Web-UI verfügbar. Die Endpoint Security Appliance löscht Erfassungen automatisch, wenn ein Administrator, Analyst oder Investigator die Web-UI verwendet, um den zugehörigen Agent manuell zu löschen.

Ändern Sie die Einstellungen für die Erfassungsalterung nicht, ohne vorher FireEye Customer Support zu konsultieren.

Die folgenden Erfassungsalterungsfunktionen können Sie mit Hilfe der Erfassungsalterungseinstellungen steuern:

Einstellung	Beschreibung
Alterungseinstellungen aktivieren	Sie können alle Erfassungsalterungseinstellungen aktivieren. Siehe Alle Alterungseinstellungen für Erfassungen mit Hilfe der CLI aktivieren auf der nächsten Seite.

Einstellung	Beschreibung
Alterungseinstellungen deaktivieren	Sie können alle Erfassungsalterungseinstellungen deaktivieren. Siehe Alle Alterungseinstellungen für Erfassungen mit Hilfe der CLI deaktivieren auf der nächsten Seite.
Die Alterungsperiode für abgeschlossene Erfassungen einstellen	Sie können die Alterungsdauer festlegen, nach der abgeschlossene Erfassungen gelöscht werden. Siehe Die Alterungsperiode für abgeschlossene Erfassungen mit Hilfe der CLI festlegen auf der nächsten Seite.
Die Alterungsperiode für ausstehende Erfassungen einstellen	Sie können die Alterungsdauer festlegen, nach der ausstehende Erfassungen gelöscht werden. Eine ausstehende Erfassungsanfrage ist eine Anfrage die auf Bearbeitung wartet. Siehe Die Alterungsperiode für ausstehende Erfassungen mit Hilfe der CLI festlegen auf Seite 107.
Die Alterungsperiode für fehlgeschlagene Erfassungen einstellen	Sie können die Alterungsdauer festlegen, nach der fehlgeschlagene Erfassungen gelöscht werden. Siehe Die fehlgeschlagene Alterungsperiode für Erfassungen mit Hilfe der CLI festlegen auf Seite 107.

Darüber hinaus können Sie die Erfassungsalterung steuern, indem Sie den Speicherplatz für Erfassungen ändern. Wenn die Gesamtgröße des Datenträgers für abgeschlossene Erfassungen ein festgelegtes Limit überschreitet, löscht die Endpoint Security Appliances die ältesten abgeschlossenen Erfassungen, bis genügender Speicherplatz geschaffen ist, um den Gesamtwert unter das festgelegte Limit zu bringen. Erfassungen, die noch nicht abgeschlossen sind, bleiben davon unberührt. Siehe Datenträgerauslastungslimits für Erfassungen festlegen auf Seite 102.

Voraussetzungen

- Admin Zugriff

Alle Alterungseinstellungen für Erfassungen mit Hilfe der CLI aktivieren

Um alle Alterungseinstellungen für Erfassungen mit Hilfe der CLI zu aktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie alle Alterungseinstellungen für Erfassungen vollständig:

   ```
   hostname (config) # hx server acquisition aging enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Alle Alterungseinstellungen für Erfassungen mit Hilfe der CLI deaktivieren

Um alle Alterungseinstellungen für Erfassungen mit Hilfe der CLI zu deaktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie alle Alterungseinstellungen für Erfassungen vollständig:

   ```
   hostname (config) # no hx server acquisition aging enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Die Alterungsperiode für abgeschlossene Erfassungen mit Hilfe der CLI festlegen

Um die Alterungsperiode für abgeschlossene Erfassungen mit Hilfe der CLI zu ändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Bestimmen Sie die Anzahl der Sekunden für die Alterungsperiode abgeschlossener Akquisitionen.

   ```
   hostname (config) # hx server acquisition aging completed-period
   <seconds>
   ```

   Der Standard ist **0** Sekunden (deaktiviert). Der Bereich für diese Einstellung ist 0-31536000 Sekunden (ein Jahr).

   Um die Standard Alterungsperiode für abgeschlossene Akquisitionen wiederherzustellen:

   ```
   hostname (config) # no hx server acquisition aging completed-period
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```


Die Alterungsperiode für ausstehende Erfassungen mit Hilfe der CLI festlegen

Eine ausstehende Erfassungsanfrage ist eine Erfassung, die auf Verarbeitung wartet, weil eine Erfassungsaufgabe noch nicht verfügbar ist. Informationen über die Einstellung der Alterungsperiode für ausstehende Erfassungen finden Sie unter Beschränkungen für ausstehende Erfassungsaufgaben einstellen auf Seite 103.

Um die Alterungsperiode für ausstehende Erfassungen mit Hilfe der CLI zu ändern.

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Bestimmen Sie die Anzahl der Sekunden für die Alterungsperiode ausstehender Akquisitionen.

   ```
   hostname (config) # hx server acquisition aging pending-period
   <seconds>
   ```

   Die Standard Periode für die Alterung ausstehender Erfassungsanfragen ist **1209600** Sekunden (oder 14 Tage). Der Bereich ist 0-31536000 Sekunden (ein Jahr). Wenn Sie das Limit auf 0 setzen, wird das Löschen von ausstehenden Erfassungsanforderungen deaktiviert.

   Um die Standard Alterungsperiode für ausstehende Erfassungen wiederherzustellen:

   ```
   hostname (config) # no hx server acquisition aging pending-period
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Die fehlgeschlagene Alterungsperiode für Erfassungen mit Hilfe der CLI festlegen

Um die Alterungsperiode für fehlgeschlagene Erfassungen mit Hilfe der CLI zu ändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Bestimmen Sie die Anzahl der Sekunden für die Alterungsperiode fehlgeschlagener Erfassungen.

   ```
   hostname (config) # hx server acquisition aging failed-period <seconds>
   ```

   Der Standard ist 0 Sekunden (deaktiviert). Gültige Werte liegen zwischen 0 und 31536000 Sekunden (ein Jahr).

   Um die Standard Alterungsperiode für fehlgeschlagene Erfassungen wiederherzustellen:

```
hostname (config) # no hx server acquisition aging failed-period
```

3. Speichern Sie Ihre Einstellungen.

```
hostname (config) # write mem
```

Einstellungen für Dateierfassung konfigurieren

Wenn ein Endpoint Security Benutzer eine Dateierfassungsanfrage tätigt, weist die Endpoint Security Appliance einen Agent an, eine Datei von ihrem Host Endpunkt abzurufen. Dateierfassungen werden für statische oder dynamische Analyse sowie für Aufbewahrung von Beweisen bei Insider Bedrohungsermittlungen verwendet. Informationen übe Dateierfassung wird in einer `.zip` Datei gesammelt.

Jede Erfassungsanfrage kann jeweils nur eine Datei von einem individuellen Host Endpunkt abrufen. Sie können die gleiche Datei von mehreren Host Endpunkten mit Hilfe von Host Sätzen anfordern. Sie können andere Dateien von dem gleichen Host Endpunkt anfordern, indem Sie zusätzliche Anfragen tätigen. Die einzigen Beschränkungen für die Gesamtzahl der Erfassungsanfragen, die Sie für jeden Host Endpunkt tätigen können, beziehen sich auf die Einstellungen für Akquisitionsalterung.

Sie können die folgenden Dateierfassungsfunktionen mit Hilfe von Dateiakquisitionseinstellungen steuern.

Funktion	Beschreibung
Enable file acquisitions	Aktiviert Dateierfassungen. Dateierfassungen sind standardmäßig aktiviert. Siehe Dateierfassungen mit Hilfe der Web-UI aktivieren auf der nächsten Seite und Dateierfassungen mit Hilfe der CLI aktivieren auf der nächsten Seite.
Disable file acquisitions	Deaktiviert Dateierfassungen. Siehe Dateierfassungen mit Hilfe der Web-UI deaktivieren auf der nächsten Seite und Dateierfassungen mit Hilfe der CLI deaktivieren auf Seite 110.
Specify the file acquisition passphrase	Identifiziert die Passphrase, die zum Verschlüsseln der Dateierfassung verwendet wird. Siehe Die Passphrase für die Dateierfassung mit Hilfe der CLI ändern auf Seite 110.

Voraussetzungen

- Admin Zugriff

Dateierfassungen mit Hilfe der Web-UI aktivieren

Um Dateierfassungen mit Hilfe der Web-UI aktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Acquisition Settings** auf dem **Admin** Menü. Die Acquisition Settings Seite wird geöffnet.
3. Klicken Sie den **File & Data Acquisitions** Schalter auf ON.
4. Klicken Sie auf **Save**.

Dateierfassungen mit Hilfe der CLI aktivieren

Um Dateierfassungen mit Hilfe der CLI zu aktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Dateierfassungen aktivieren:

   ```
   hostname (config) # hx server acquisition enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Dateierfassungen mit Hilfe der Web-UI deaktivieren

Um Dateierfassungen mit Hilfe der Web-UI deaktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Acquisition Settings** auf dem **Admin** Menü. Die Acquisition Settings Seite wird geöffnet.
3. Klicken Sie den **File & Data Acquisitions** Schalter auf OFF.
4. Klicken Sie auf **Save**.

Dateierfassungen mit Hilfe der CLI deaktivieren

Dateierfassungen deaktivieren

Um Dateierfassungen mit Hilfe der CLI zu deaktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie Dateierfassungen:

   ```
   hostname (config) # no hx server acquisition enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Die Passphrase für die Dateierfassung mit Hilfe der CLI ändern

Dateierfassungen sind herunterladbare `.zip` Dateien. Sie werden mit Hilfe einer Passphrase verschlüsselt, die immer dann eingesetzt wird, wenn eine Akquisitionsanfrage gestellt wird. Die Standard Passphrase ist **unzip-me**.

Durch Ändern dieser Einstellung wird die Passphrase für bereits angeforderte Akquisitionen nicht geändert.

Die Sicherheit wird nicht durch Ändern der Passphrase verbessert. Die Passphrase soll verhindern, dass Antivirus Software das Paket beim Herunterladen als bösartig kennzeichnet. Erfassungspakete können bösartige Inhalte enthalten.

Um die Passphrase für Dateierfassungen mit Hilfe der CLI zu ändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Ändern Sie die Passphrase für Dateierfassungen:

   ```
   hostname (config) # hx server acquisition default-zip-passphrase
   <passphrase>
   ```

   Legen Sie eine Passphrase fest, kie 8192 Zeichen nicht übersteigt. Der Standard ist `unzip-me`.

   Um die Standard Passphrase wiederherzustellen:

   ```
   hostname (config) # no hx server acquisition default-zip-passphrase
   ```

3. Speichern Sie Ihre Einstellungen.

```
hostname (config) # write mem
```

Automatische Triage-Einstellungen konfigurieren

Die automatische Triage-Erfassungsfunktion ermöglicht Agents, Informationen rund um den Zeitpunkt einer Warnung mit Hilfe von Parametern automatisch zu sammeln, die Leistung und Untersuchungswerte optimieren. Siehe Triage Sammlungen auf Seite 312. In Endpoint Security Version 4.9 und später können Sie automatische Triage nach Warnungstyp festlegen.

HINWEIS: Der Anfragetyp für automatische Triage ist "Around timestamp". Der Zeitstempel ist die Zeit, zu der das Ereignis stattfand, das die Warnung generiert hat. Around Timestamp fordert Informationen an, die während eines spezifischen Zeitraums vor dem Zeitstempel bis zu einem bestimmten Zeitraum nach dem Zeitstempel gesammelt wurden.

Administratoren können diese Funktion mit Hilfe der Endpoint Security Web-UI deaktivieren. Der Standardwert für diese Einstellung ist **On**.

Wenn automatische Triage ausgeschaltet ist, können Sie weiterhin manuell Triage-Sammlungen anfordern.

HINWEIS: Malware Alarme lösen keine automatische Triage aus, wie dies bei anderen Alarmen der Fall ist.

- Automatische Triage aktivieren auf der nächsten Seite
- Automatische Triage nach Warnungstyp aktivieren auf der nächsten Seite
- Automatische Triage deaktivieren auf Seite 113
- Automatische Triage nach Warntyp deaktivieren auf Seite 113

Voraussetzungen

- Administratorzugriff
- Bevor Sie automatische Triage für Process Tracker (PRO) Alarme konfiguriert werden können, muss das Process Tracker Modul installiert und aktiviert werden.

Automatische Triage aktivieren

Sie können die Automatic Triage Settings Seite für die Aktivierung der automatischen Triage verwenden.

Um automatische Triageerfassungen von der Automatic Triage Settings Seite zu aktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Triage Settings** auf dem **Admin** Menü.
3. Auf der Automatic Triage Settings Seite schalten Sie den **Triage Settings** Schalter auf **ON**.
4. Klicken Sie auf **Save**.

Automatische Triage nach Warnungstyp aktivieren

Sie können die Automatic Triage Settings Seite verwenden, um automatische Triage für bestimmte Warntypen zu aktivieren.

Um automatische Triageerfassungen für bestimmte Warnungstypen von der Automatic Triage Settings Seite zu aktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Triage Settings** auf dem **Admin** Menü.
3. Im Alert Type Specific Settings Bereich auf der Automatic Triage Settings Seite schalten Sie den Schalter auf **ON** für den bestimmten Warnungstyp. Sie können automatische Triage für die folgenden Warnungstypen aktivieren:
    - Real-Time Detection (IOC)
    - Exploit Guard Detection (EXD)
    - Process Tracker (PRO)--Dieser Warnungstyp ist nur verfügbar, wenn Sie das Process Tracker Modul in Verbindung mit dem Enricher Modul verwenden und Sie diese Module zum Generieren von PRO Alarmen konfiguriert haben.
4. Klicken Sie auf **Save**.

Automatische Triage deaktivieren

Sie können die Automatic Triage Settings Seite für die Deaktivierung der automatischen Triage verwenden.

Um automatische Triageerfassungen von der Automatic Triage Settings Seite zu deaktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Triage Settings** auf dem Admin Menü.
3. Auf der Automatic Triage Settings Seite schalten Sie den **Triage Settings** Schalter auf **OFF**.
4. Klicken Sie auf **Save**.

Automatische Triage nach Warntyp deaktivieren

Sie können die Automatic Triage Settings Seite verwenden, um automatische Triage für bestimmte Warntypen zu deaktivieren.

Um automatische Triageerfassungen für bestimmte Alamtypen von der Automatic Triage Settings Seite zu deaktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Triage Settings** auf dem **Admin** Menü.
3. Im Alert Type Specific Settings Bereich auf der Automatic Triage Settings Seite schalten Sie den Schalter auf **OFF** für den bestimmten Warnungstyp. Sie können automatische Triage für die folgenden Warnungstypen deaktivieren:
   - Real-Time Detection (IOC)
   - Exploit Guard Detection (EXD)
   - Process Tracker (PRO)--Dieser Warnungstyp ist nur verfügbar, wenn Sie das Process Tracker Modul in Verbindung mit dem Enricher Modul verwenden und Sie diese Module zum Generieren von PRO Alarmen konfiguriert haben.
4. Klicken Sie auf **Save**.

Einstellungen für automatische Triage Drosselung konfigurieren

VORSICHT: Ändern Sie die Drosselungseinstellungen für die Triage nicht, ohne vorher FireEye Customer Support zu kontaktieren.

Mit Hilfe der Automatic Triage Settings Seite können Sie steuern, ob die Endpoint Security Appliance automatische Triage Sammlungen generiert, wenn eine weit verbreitete Kompromittierung oder ein Falsch Positiv eine übermäßige Anzahl von Triageanfragen generiert. Drosselungseinstellungen gestatten Ihnen, die Anzahl der automatischen Triage Anfragen festzulegen, die generiert werden können (Anforderungslimit) und den Zeitraum (in Sekunden), in dem sie generiert werden können.

Die folgende Tabelle führt die Einstellungen auf, die Sie auf der Automatic Triage Settings Seite konfigurieren können.

Globale Triage Einstellungen

Hochzahl von Triagen

Steuert die Höchstzahl automatischer Triage Sammlungsanfragen, die global während eines festgelegten Zeitraums erstellt werden. Gültige Zeiträume liegen zwischen 0 bis 604800 Sekunden. Gültige Anfragelimits liegen zwischen 0-65535 Anfragen.

Konfigurationseigenschaften	Standard
Limit	5000 (Anfragen)
automatische Triage(n) alle	21600 (Sekunden)

Pro individuellem Agent

Steuert die Anzahl automatischer Triage Sammlungsanfragen, die für einzigartige Agents während eines festgelegten Zeitraums erstellt werden. Gültige Zeiträume liegen zwischen 0 bis 604800 Sekunden pro Agent. Gültige Anforderungslimits liegen zwischen 0-65535 Anfragen pro Agent.

Konfigurationseigenschaften	Standard
Limit	1 (Anfragen pro Agent)
automatische Triage(n) alle	1800 (Sekunden)

Pro Agent und Bedingung

Steuert die Anzahl der automatischen Triage Sammlungsanfragen, die für einzigartige Bedingungen erstellt werden, die für einen individuellen Agent während eines festgelegten Zeitraums aufgetreten sind. Gültige Zeiträume liegen zwischen 0 bis 604800 Sekunden pro

Bedingung pro Agent. Gültige Anforderungslimits liegen zwischen 0-65535 Anfragen pro Bedingung.

Konfigurationseigenschaften	Standard
Limit	1 (Anfrage pro spezifischer Alarmbedingung)
automatische Triage(n) alle	43200 (Sekunden)

Warnungstypspezifische Einstellungen

Echtzeit-Erkennung (IOC)

Steuert die Anzahl der automatischen Triage Sammlungsanfragen, die für alle Indicator of Compromise (IOC) während eines festgelegten Zeitraums erstellt werden. Gültige Zeiträume liegen zwischen 0 bis 604800 Sekunden. Gültige Anfragelimits liegen zwischen 0-65535 Anfragen.

Konfigurationseigenschaften	Standard
Limit	75
automatische Triage(n) alle	21600
Pro Bedingung: Limit von 20	20
automatische Triage(n) alle	43200
Pro Indikator: Limit von	20
automatische Triage(n) alle	43200

Exploit Guard Erkennung (EXD)

Steuert die Anzahl der automatischen Triage Sammlungsanfragen, die für Exploit Vorfälle erstellt wurden, die von Exploit Guard während eines festgelegten Zeitraums identifiziert wurden. Gültige Zeiträume liegen zwischen 0 bis 604800 Sekunden. Gültige Anfragelimits liegen zwischen 0-65535 Anfragen.

Konfigurationseigenschaften	Standard
Limit	75 (Anfragen pro spezische Exploit Bedingung)
automatische Triage(n) alle	21600 (Sekunden)

Process Tracker* (PRO)

Steuert die Anzahl der automatischen Triage Sammlungsanfragen, die für Exploit Vorfälle erstellt wurden, die von ProcessTracker während eines festgelegten Zeitraums identifiziert wurden. Gültige Zeiträume liegen zwischen 0 bis 604800 Sekunden. Gültige Anfragelimits liegen zwischen 0-65535 Anfragen.

Konfigurationseigenschaften	Standard
Limit	75 (Anfragen pro PRO)
automatische Triage(n) alle	21600 (Sekunden)

* Dieser ist nur verfügbar, wenn Sie das Process Tracker Modul in Verbindung mit dem Enricher Modul verwenden und Sie diese Module zum Generieren von PRO Alarmen konfiguriert haben.

Voraussetzungen

- Administratorzugriff

Drosselungseinstellungen für die automatische Triage festlegen

Sie können die Automatic Triage Settings Seite verwenden, um Drosselungseinstellungen für die automatische Triage festzulegen. Sie können globale Einstellungen sowie Einstellungen für jeden Warnungstypen festlegen.

Ändern Sie die Einstellungen für die Triage Drosselung nicht, ohne vorher FireEye Customer Support zu kontaktieren.

Um Einstellungen für automatische Triage-Drosselung festzulegen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Triage Settings** auf dem **Admin** Menü.
3. Im **Global Triage Settings** Bereich der Automatic Triage Settings Seite legen Sie das Limit und den Zeitraum für Folgendes fest:
    - Maximum Triages
    - Per Individual Agent
    - Per Agent and Condition

4. Im **Alert Type Specific Settings** Bereich der Automatic Triage Settings Seite legen Sie das Limit und den Zeitraum für Folgendes fest:
    - Real-Time Detection (IOC)
    - Exploit Guard Detection (EXD)
    - Process Tracker (PRO)--Dieser ist nur verfügbar, wenn Sie das Process Tracker Modul in Verbindung mit dem Enricher Modul verwenden und Sie diese Module zum Generieren von PRO Alarme konfiguriert haben.
5. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

HINWEIS: Sie können einen Wert auf die Standardeinstellung zurückstellen, indem Sie auf **Reset to Defaults** und dann auf **Save** klicken.

Einstellungen der Grenzwerte für die Warnungsrate festlegen

Sie können die Alert Settings Seite im Admin Menü verwenden, um die Einstellungen der Grenzwerte für die Warnungsrate festzulegen.Endpoint Security

Um die Einstellungen der Grenzwerte für die Warnungsrate festzulegen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Alert Settings** auf dem **Admin** Menü.
3. Auf der **Alert Settings** Seite legen Sie die Einstellungen der Grenzwerte für die Warnungsrate für Endpoint Security fest. Sie können Einstellungen der Grenzwerte für die Warnungsrate für die folgenden Warnungstypen konfigurieren.
    - Real-Time Detection (IOC)
    - Malware Detection (MAL)
    - Process Tracker (PRO)--Dieser Warnungstyp ist nur verfügbar, wenn Sie das Process Tracker Modul in Verbindung mit dem Enricher Modul verwenden und Sie diese Module zum Generieren von PRO Warnungen konfiguriert haben.
4. Klicken Sie auf **Save**.

HINWEIS: Sie können einen Wert auf die Standardeinstellung zurückstellen, indem Sie auf **Reset to Defaults** und dann auf **Save Settings** ei

Zeitstempel-Einstellungen konfigurieren

Wenn ein Endpoint Security Benutzer eine Triage-Sammlung auf einem bestimmten Datum und Uhrzeit basierend anfordert, oder wenn eine automatische Triage-Erfassung Host-Endpunktinformationen in Bezug auf die Zeit eines Alarms sammelt, gibt der Agent Informationen für ein bestimmtes Zeitfenster vor und nach dem Alarm zurück. Die Zeitstempel-Einstellungen steuern die Länge des Fensters für die Triage-Sammlung.

Zeitstempel-Einstellungen treffen nur auf Agent URL-Ereignisse (`URL Monitor Events`) und Verzeichnisschlüssel-Ereignisse (`Reg Key Events`) zu.

Sie können den Timestamp Settings Tab verwenden, um die Zeitspanne zum Sammeln von Informationen vor und nach dem Zeitstempel festzulegen. **Zeitstempel-Einstellungen** können von 0-86400 Sekunden reichen. Der Standardwert für beide Einstellungen ist **600** Sekunden.

- Zeitstempel-Einstellungen festlegen unten

Voraussetzungen

- Administratorzugriff

Zeitstempel-Einstellungen festlegen

Sie können den Timestamp Settings Tab auf der Automatic Triage Settings Seite verwenden, um die Länge der Zeit vor und nach dem Zeitstempel festzulegen, während der Informationen gesammelt werden sollen. Der Zeitstempel ist die Zeit, zu der das Ereignis stattfand, das die Warnung ausgelöst hat.

Um Zeitstempel-Einstellungen festzulegen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Triage Settings** auf dem **Admin** Menü.
3. Auf der **Automatic Triage Settings** Seite klicken Sie auf den **Timestamp Settings** Tab.
4. Auf der **Timestamp Settings** Seite können Sie die Zeitspanne vor und nach dem Zeitstempel festlegen, während der Informationen gesammelt werden sollen.
5. Im oberen Feld auf der **Timestamp Settings** Seite geben Sie die Anzahl der Sekunden vor dem festgelegten Zeitstempel ein, für die Informationen gesammelt werden sollen.
6. Im unteren Feld der **Timestamp Settings** Seite geben Sie die Anzahl der Sekunden nach dem Zeitstempel ein, für die Informationen gesammelt werden sollen.
7. Klicken Sie auf **Save**, um Ihre Einstellungen zu speichern.

HINWEIS: Sie können alle Werte auf der Seite auf die Standardeinstellungen zurücksetzen, indem Sie auf **Reset to Defaults** und dann **Save** klicken.

KAPITEL 4: Datenerfassungsscripts verwalten

Datenerfassungsanfragen (manchmal auch *Live Response (Live-Antwort) Anfragen* genannt) ermöglichen Ihnen, Daten, die Sie benötigen, von einem einzelnen laufenden Endpunkt zu erfassen. Mit Hilfe der Data Acquisition Scripts Seite können Sie die für Datenerfassunganfragen verwendeten Datenerfassungsscripts erstellen, bearbeiten, kopieren und löschen.

Mehrere Scripts werden von FireEye bereitgestellt. Sie können diese Scripts nicht löschen, obwohl Sie sie bearbeiten oder kopieren und als Grundlage für Ihr eigenes Script verwenden können. Wenn Sie sie bearbeitet haben, können Sie sie auch auf ihre werksseitig verteilte Form zurücksetzen. Weitere Informationen über die bereitgestellten Scripts finden Sie unter Bereitgestellte Datenerfassungsscripts auf Seite 459.

HINWEIS: Erfassungstypen, die in Datenerfassungsscript enthalten sein können, fordern die meisten der durch MIR-Audits gesammelten Daten an. Zusätzlich können Sie Ihre eigenen MIR Scripts importieren.

Voraussetzungen

- Admin, Analyst, Senior Analyst oder Investigator Zugriff
- Eine aktive installierte Endpoint Security Power Lizenz. Sehen Sie "Lizenzverwaltung" im *Endpoint Security Server System-Administrationshandbuch*.

  Wenn Ihre Lizenz abläuft, nachdem Sie Ihre eigenen Scripts erstellt habe oder die gelieferten Scripts bearbeitet haben, können Sie diese Scripts auf der Data Acquisition Scripts Seite sehen, aber Sie können sie nicht bearbeiten oder zum Erfassen von Daten verwenden. Sie können sie exportieren.

Die Data Acquisition Scripts Seite abrufen

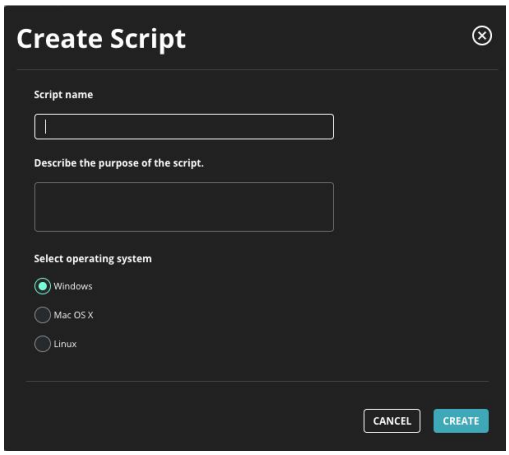
Um die Data Acquisition Scripts Seite abzurufen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü.

Ein Script erstellen

Um ein Datenerfassungsscript zu erstellen:

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. Klicken Sie auf **Create Script**.



3. Im Script Name Feld geben Sie einen Namen für das neue Script ein.

4. Optional können Sie eine Beschreibung für das Script eingeben.
5. Wählen Sie das Betriebssystem, auf das das Script angewendet werden soll. Sie können nur ein einziges Betriebssystem auf dem Create Script Dialog auswählen. Wenn ein Script allerdings auf mehr als ein Betriebssystem zutrifft, können Sie Betriebssysteme hinzufügen, nachdem das Script erstellt ist. Siehe Script Betriebssysteme ändern auf Seite 126.
6. Klicken Sie auf **Create**, um die Scriptdefinition zu starten.
7. Wählen Sie einen Erfassungsdatentyp im **Add an acquisition type** Dropdown-Feld und klicken Sie auf **Add**. Siehe Verweis auf Erfassungsdatentyp auf Seite 135.

   Optionen für den von Ihnen angeforderten Erfassungstyp werden rechts neben der Scriptliste angezeigt.
8. Geben Sie Werte für die Erfassungstypoptionen ein oder verwenden Sie die Standardwerte, die bereits ausgewählt wurden.

   Die Web-UI warnt Sie nicht, oder entfernt Register, Leerzeichen oder ungewollte Zeichen (wie z.B. \n) in Ihren Spezifikationen.
9. Wiederholen Sie letzten beiden Schritte, um zusätzliche Daten für das Datenerfassungsscript anzufordern.

   Einige Erfassungsdatentypen sind nur einmal für ein Script verfügbar, während andere mehr als einmal festgelegt werden können. Nach Hinzufügen eines Erfassungstyps zu einem Script wird die Liste der verfügbaren Erfassungstypen im **Add an acquisition type** Dropdown Feld entsprechen angepasst.
10. Um einen Erfassungsdatentyp von dem Script zu entfernen, klicken Sie auf das x Symbol () auf dem Acquisition Tab links auf der Seite.
11. Wenn alle Erfassungsdatentypen und Optionen festgelegt sind, klicken Sie auf **Create**.

    Das neue Script wird erstellt.

Wenn Fehler im Script vorliegen, weist das Register ein Warnsymbol für den Erfassungsdatentyp mit den Fehlern auf.

Ein Script kopieren

Um ein Datenerfassungsscript zu kopieren:

1. Exportieren Sie das Script, das Sie kopieren wollen. Siehe Ein Script exportieren auf Seite 129.
2. Importieren Sie das Script unter einem neuen Namen. Siehe Ein Script importieren auf Seite 129.

Ein Script bearbeiten

Sie können die Endpoint Security Verwenden, um den Titel und die Beschreibung eines Datenerfassungsscripts zu bearbeiten, sowie die Erfassungstypen und Betriebssysteme für das Script auszuwählen.

- Scripttitel und -beschreibungen ändern unten
- Script Erfassungsdatentypen anpassen auf der nächsten Seite
- Script Betriebssysteme ändern auf Seite 126

Wenn Sie ein Script zur Bearbeitung auswählen, werden die unterschiedlichen Versionen des Scripts für jedes unterstützte Betriebssystem angezeigt. Stellen Sie sicher, dass Sie die Änderungen an den korrekten Betriebssystemversionen eines Scripts vornehmen.

Scripttitel und -beschreibungen ändern

Sie können die Endpoint Security Web-UI verwenden, um den Titel und die Beschreibung eines Datenerfassungsscripts zu verändern.

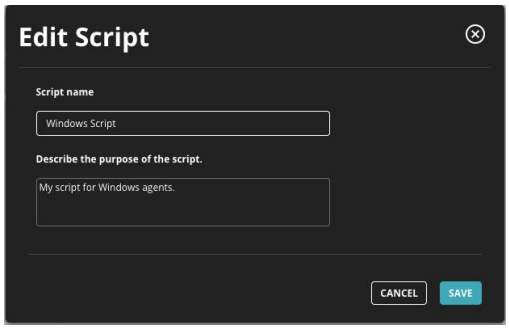
Um den Titel oder die Beschreibung eines Datenerfassungsscripts zu ändern:

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. In der Liste der Scripts wählen Sie das Script, das Sie ändern möchten, links auf der Data Acquisition Scripts Seite aus.

   Details über das Script werden rechts auf der Seite angezeigt, einschließlich getrennte Abschnitte für jedes von dem Script unterstützte Betriebssystem.

3. Mindestens zwei **Actions** Menüs werden für benutzerdefinierte Scripts angezeigt. Ein Menü wird im Überschriftenbereich angezeigt und eins für jedes Betriebssystem, das das Script unterstützt. (Die mitgelieferten Standard Investigative Details, Comprehensive Investigative Details und Process Details Scripts verfügen nicht über ein **Actions** Menü im Überschriftenbereich.)

   Wählen Sie **Edit Title and Description** im Actions Menü im Überschriftenbereich der Scriptdefinition. Der Edit Script Dialog wird angezeigt.



4. Ändern Sie den Scriptnamen und -beschreibung nach Bedarf.
5. Klicken Sie auf **Save**.

Script Erfassungsdatentypen anpassen

Die für das Script ausgewählten Erfassungsdatentypen können bearbeitet werden.

Um die für ein Datenerfassungsscript ausgewählten Erfassungstypen zu ändern:

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. In der Liste der Scripts wählen Sie das Script, das Sie ändern möchten, links auf der Data Acquisition Scripts Seite aus.

   Details über das Script werden rechts auf der Seite angezeigt, einschließlich getrennte Abschnitte für jedes von dem Script unterstützte Betriebssystem. Stellen Sie sicher, dass Sie den richtigen Betriebssystem Abschnitt bearbeiten.

3. Mindestens zwei **Actions** Menüs werden für benutzerdefinierte Scripts angezeigt. Ein Menü wird im Überschriftenbereich angezeigt und eins für jedes Betriebssystem, das das Script unterstützt. (Die mitgelieferten Standard Investigative Details, Comprehensive Investigative Details und Process Details Scripts verfügen nicht über ein **Actions** Menü im Überschriftenbereich.)

   Wählen Sie **Edit** im **Actions** Menü, das im Betriebssystem Abschnitt des Scripts angezeigt wird, das Sie ändern wollen.

   Die Data Acquisition Seite wird angepasst, so dass nur der Script Abschnitt, der zu dem ausgewählten Betriebssystem gehört, angezeigt wird. Sie können das Betriebssystem durch das auf der linken Seite des Scriptnamens angezeigte Symbol identifizieren: Windows (), MacOS () oder Linux ().

4. Wählen Sie einen Akquisitionsdatentyp in dem Script oder fügen Sie einen neuen hinzu, indem Sie einen im **Add an acquisition type** Dropdown-Feld auswählen und auf **Add** klicken. Siehe Verweis auf Erfassungsdatentyp auf Seite 135.

   Optionen für den von Ihnen angeforderten Akquisitionsdatentyp finden Sie auf der rechten Seite der Scriptliste.

5. Geben Sie Werte für die Optionen für den Erfassungsdatentyp ein oder verwenden Sie die Standardwerte, die bereits ausgewählt wurden.

   HINWEIS: Die Web-UI warnt Sie nicht und entfernt keine Register, Leerzeichen oder ungewollte Zeichen (wie z.B. \n) in Ihren Spezifikationen.

6. Wiederholen Sie letzten beiden Schritte, um zusätzliche Daten für das Datenerfassungsscript anzufordern.

   Einige Erfassungsdatentypen sind nur einmal für ein Script verfügbar, während andere mehr als einmal festgelegt werden können. Nach Hinzufügen eines Erfassungstyps zu einem Script wird die Liste der verfügbaren Erfassungstypen im **Add an acquisition type** Dropdown Feld entsprechen angepasst.

7. Um einen Erfassungsdatentyp von dem Script zu entfernen, klicken Sie auf das x Symbol () auf dem Acquisition Tab links auf der Seite.

8. Wenn alle Erfassungsdatentypen und Optionen festgelegt sind, klicken Sie auf **Save**.

   Das Script ist aktualisiert.

Script Betriebssysteme ändern

Sie können Betriebssysteme in einem Datenerfassungsscript mit Hilfe der Endpoint Security Web-UI hinzufügen oder entfernen.

Ein Betriebssystem hinzufügen

Um ein Betriebssystem zu einem Datenerfassungsscript hinzuzufügen:

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. In der Liste der Scripts wählen Sie das Script, das Sie ändern möchten, links auf der Data Acquisition Scripts Seite aus.

   Details über das Script werden rechts auf der Seite angezeigt, einschließlich getrennte Abschnitte für jedes von dem Script unterstützte Betriebssystem.
3. Mindestens zwei **Actions** Menüs werden für benutzerdefinierte Scripts angezeigt. Ein Menü wird im Überschriftenbereich angezeigt und eins für jedes Betriebssystem, das das Script unterstützt. (Die mitgelieferten Standard Investigative Details, Comprehensive Investigative Details und Process Details Scripts verfügen nicht über ein **Actions** Menü im Überschriftenbereich.)

   Nach Bedarf wählen Sie **Add Windows version**, **Add OS X version** oder **Add Linux version** im **Actions** Menü im Überschriftenbereich.

   Die Data Acquisition Seite wird angepasst, so dass nur der Script Abschnitt, der zu dem ausgewählten Betriebssystem gehört, angezeigt wird. Sie können das Betriebssystem durch das auf der linken Seite des Scriptnamens angezeigte Symbol identifizieren: Windows (), Mac OS X () oder Linux ().
4. Wählen Sie einen Erfassungstyp im **Add an acquisition type** Dropdown Feld und klicken Sie auf **Add**. Siehe Verweis auf Erfassungsdatentyp auf Seite 135.

   Optionen für den von Ihnen angeforderten Erfassungstyp werden rechts neben der Scriptliste angezeigt.
5. Geben Sie Werte für die Erfassungstypoptionen ein oder verwenden Sie die Standardwerte, die bereits ausgewählt wurden.

   HINWEIS: Die Web-UI warnt Sie nicht und entfernt keine Register, Leerzeichen oder ungewollte Zeichen (wie z.B. \n) in Ihren Spezifikationen.
6. Wiederholen Sie letzten beiden Schritte, um zusätzliche Daten für das Datenerfassungsscript anzufordern.

   Einige Erfassungstypen sind nur einmal für ein Script verfügbar, während andere mehr als einmal festgelegt werden können. Nach Hinzufügen eines Erfassungstyps zu einem Script wird die Liste der verfügbaren Erfassungstypen im **Add an acquisition type** Dropdown Feld entsprechen angepasst.
7. Um einen Erfassungstyp von dem Script zu entfernen, klicken Sie auf das x Symbol () auf dem Acquisition Tab links auf der Seite.

8. Wenn alle Erfassungstypen und Optionen festgelegt sind, klicken Sie auf **Save**.

   Das Script wird für das neue Betriebssystem aktualisiert.

Eine Betriebssystemversion entfernen

Um eine Betriebssystemversion von einem Datenerfassungsscript zu entfernen:

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. In der Liste der Scripts wählen Sie das Script, das Sie ändern möchten, links auf der Data Acquisition Scripts Seite aus.

   Details über das Script werden rechts auf der Seite angezeigt, einschließlich getrennte Abschnitte für jedes von dem Script unterstützte Betriebssystem.
3. Mindestens zwei **Actions** Menüs werden für ein Script angezeigt. Ein Menü wird im Überschriftenbereich angezeigt und eins für jedes Betriebssystem, das das Script unterstützt.

   Wählen Sie **Delete** im **Actions** Menü, das in dem Betriebssystem Abschnitt angezeigt wird, das Sie entfernen wollen.

   Ein Dialog wird angezeigt, und fordert Sie auf, die Löschung zu bestätigen.
4. Klicken Sie auf dem Dialog auf Delete**.**

   Das Datenerfassungsscript wird angepasst und auf der Data Acquisition Scripts Seite gespeichert.

Ein Script löschen

Um ein Datenerfassungsscript zu löschen

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. Wählen Sie das Script, das Sie löschen möchten links auf der Seite aus.

3. Mindestens zwei **Actions** Menüs werden für benutzerdefinierte Scripts angezeigt. Ein Menü wird im Überschriftenbereich angezeigt und eins für jedes Betriebssystem, das das Script unterstützt. (Die mitgelieferten Standard Investigative Details, Comprehensive Investigative Details und Process Details Scripts verfügen nicht über ein **Actions** Menü im Überschriftenbereich.)

   Wählen Sie **Delete** in dem zutreffenden **Actions** Menü. Durch Auswahl von **Delete** im **Actions** Menü im Überschriftenbereich wird das gesamte Script gelöscht. Durch Auswahl von **Delete** im **Actions** Menü in einer einzelnen Betriebssystemversion des Script wird das Script für dieses Betriebssystem gelöscht.

   Ein Dialog wird angezeigt, und fordert Sie auf, die Löschung zu bestätigen.

4. Klicken Sie auf dem Dialog auf **Delete**.

   Das Datenerfassungsscript wird gelöscht.

Ein Script exportieren

Sie können einen Betriebssystemabschnitt eines Datenerfassungsscripts auf eine JSON Datei exportieren.

Um ein Datenerfassungsscript zu exportieren:

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. Wählen Sie das Script, das Sie exportieren möchten links auf der Seite aus.
3. Mindestens zwei **Actions** Menüs werden für benutzerdefinierte Scripts angezeigt. Ein Menü wird im Überschriftenbereich angezeigt und eins für jedes Betriebssystem, das das Script unterstützt. (Die mitgelieferten Standard Investigative Details, Comprehensive Investigative Details und Process Details Scripts verfügen nicht über ein **Actions** Menü im Überschriftenbereich.)

   Wählen Sie ggf. **Export script** im **Actions** Menü des Betriebssystem Abschnitts des Scripts, das Sie importieren wollen.

   Eine JSON Datei für das ausgewählte Betriebssystem wird auf Ihren Computer heruntergeladen. Der Name der JSON Datei enthält das Betriebssystem, so dass Sie einfach feststellen können, welche Scripts für welches Betriebssystem gedacht ist.

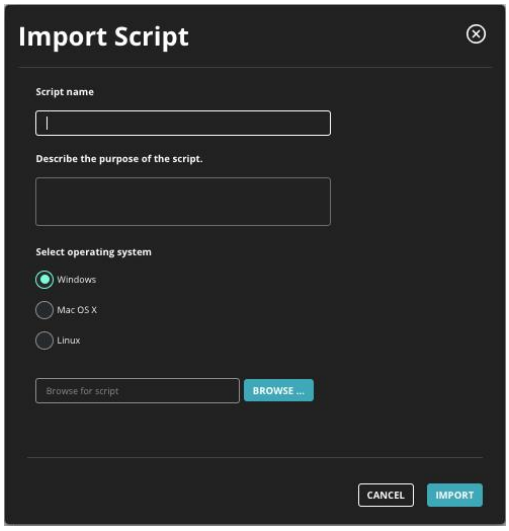
Ein Script importieren

Sie können ein MIR Script oder ein anderes Datenerfassungsscript in ein neues Datenerfassungsscript oder in ein vorhandenes Script importieren.

Ein Script in ein neues Script importieren

Um ein Script in ein neues Datenerfassungsscript zu importieren:

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. Klicken Sie auf **Import Script**. Der Import Script Dialog wird angezeigt.



3. Im Script Name Feld geben Sie einen Namen für das neue Script ein.
4. Optional können Sie eine Beschreibung für das Script eingeben.
5. Wählen Sie das Betriebssystem des Scripts, das Sie importieren wollen. Sie können nur ein einziges Betriebssystem auf dem Import Script Dialog auswählen. Wenn ein Script allerdings auf mehr als ein Betriebssystem zutrifft, können Sie Betriebssysteme hinzufügen, nachdem das Script erstellt ist. Siehe Script Betriebssysteme ändern auf Seite 126.
6. Klicken Sie auf **Browse**, um das Script zu finden, das Sie importieren wollen.

7. Wählen Sie das Script, das Sie importieren wollen, und klicken Sie auf **Open**. Das Script wird zu Import Script Dialog hinzugefügt.

   Sie können das Script vom Import Script Dialog entfernen, indem Sie auf das Symbol neben seinem Namen klicken. Dies kann beispielsweise erforderlich sein, wenn Sie versehentlich das falsche Script zum Importieren ausgewählt haben.

   Wenn keins der Audits im ausgewählten Script von dem ausgewählten Betriebssystem unterstützt wird, wird der Fehler "The selected file contains only unsupported audits" (Die ausgewählte Datei enthält nur nicht unterstützte Audits) angezeigt und Sie werden aufgefordert, ein anderes Import-Script auszuwählen.

   Wenn Sie das falsche Betriebssystem des Scripts ausgewählt haben, das Sie importieren, aber einige der Audits für das ausgewählte Betriebssystem gelten, werden die Audits, die nicht importiert werden können, während des Imports aus dem Script entfernt und in einer Fehlertextdatei gemeldet .

8. Wenn das richtige Script ausgewählt wurde, klicken Sie auf **Import**, um das Script zu importieren.

   Wenn der Endpoint Security Probleme bei der Interpretation des Scripts hat oder ein Audit in dem Script nicht erkennt, wird eine Nachricht angezeigt.

   Wählen Sie Download the list of import issues**, um eine Textdatei mit einer Liste dessen herunterzuladen, was nicht importiert wurde.**

   - Wenn Sie das falsche Betriebssystem für das Script, das Sie importieren, ausgewählt haben, werden die Audits, die nicht importiert werden können, von dem Script entfernt und in der Fehlertextdatei gemeldet. Wenn keins der Audits importiert werden kann, werden Sie auf dem Import Script Dialog benachrichtigt, bevor der Import stattfindet.
   - Einige Audits in einem Script können nicht importiert werden. In diesem Fall werden die Audits, die nicht importiert werden können, aus dem Script entfernt und in der Fehlertextdatei gemeldet. Siehe Audits, die nicht importiert werden können auf Seite 133.

   Wenn der Import erfolgreich verläuft, wird die Datenerfassung angepasst, so dass nur der Scriptabschnitt angezeigt wird, der dem importierten Script zugeordnet ist. Sie können das Betriebssystem durch das auf der linken Seite des Scriptnamens angezeigte Symbol identifizieren: Windows ( ), OS X ( ) oder Linux ( ).

9. Klicken Sie auf **Create**, um das Script zu erstellen und in Endpoint Security zu speichern. Sie können ein Script mit den nicht behobenen Importproblemen erstellen.

Ein Script in ein vorhandenes Script importieren

Um ein Script in ein vorhandenes Datenerfassungsscript zu importieren:

1. Wählen Sie **Data Acquisition Scripts** auf dem **Admin** Menü auf der Endpoint Security Web-UI.
2. Wählen Sie das Script, das Sie in ein anderes Script importieren wollen, links auf der Data Acquisition Scripts Seite.

   Details über das Script werden rechts auf der Seite angezeigt, einschließlich getrennte Abschnitte für jedes von dem Script unterstützte Betriebssystem.
3. Mindestens zwei **Actions** Menüs werden für benutzerdefinierte Scripts angezeigt. Ein Menü wird im Überschriftenbereich angezeigt und eins für jedes Betriebssystem, das das Script unterstützt. (Die mitgelieferten Standard Investigative Details, Comprehensive Investigative Details und Process Details Scripts verfügen nicht über ein**Actions** Menü im Überschriftenbereich.)

   Wählen Sie ggf. **Import Windows version**, **Import macOS version** oder **Import Linux version**, im **Actions** Menü im Überschriftenbereich. Stellen Sie sicher, dass Sie die Menüoption auswählen, die mit dem Betriebssystem des Scripts übereinstimmt, das Sie importieren wollen.

   Ein Browserfenster wird angezeigt.
4. Finden Sie das Script, das Sie importieren wollen.
5. Wählen Sie das Script, das Sie importieren wollen und klicken Sie auf **Open**, um das Script zu importieren.

   Wenn der Endpoint Security Probleme bei der Interpretation des Scripts hat oder ein Audit in dem Script nicht erkennt, wird eine Nachricht angezeigt.

   Wählen Sie **Download the list of import issues**, um eine Textdatei mit einer Liste dessen herunterzuladen, was nicht importiert wurde.

   - Wenn Sie das falsche Betriebssystem für das Script, das Sie importieren, ausgewählt haben, werden die Audits, die nicht importiert werden können, von dem Script entfernt und in der Fehlertextdatei gemeldet.
   - Einige Audits in einem Script können nicht importiert werden. In diesem Fall werden die Audits, die nicht importiert werden können, aus dem Script entfernt und in der Fehlertextdatei gemeldet. Siehe Audits, die nicht importiert werden können auf der nächsten Seite.

   Wenn der Import erfolgreich verläuft, wird die Datenerfassung angepasst, so dass nur der Scriptabschnitt angezeigt wird, der dem importierten Script zugeordnet ist. Sie können das Betriebssystem durch das auf der linken Seite des Scriptnamens angezeigte Symbol identifizieren: Windows (), OS X () oder Linux ().

6. Klicken Sie auf **Save**, um das Script in Endpoint Security zu speichern. Sie können ein Script mit den nicht behobenen Importproblemen erstellen.

Audits, die nicht importiert werden können

Die folgenden Auditmodule können nicht in ein Datenerfassungsscript mit der Endpoint Security Web-UI importiert werden, weil sie eine Verarbeitung umfassen, die die Systemleistung erheblich beeinträchtigen können oder weil sie eine Funktion ausführen, die nichts mit Datenerfassung zu tun haben. Wenn versucht wird, Scripts zu importieren, die diese Audits enthalten, treten Fehler auf.

Für einige dieser Audits stellt FireEye vorkonfigurierte Datenerfassungsscripts bereit, die für einen individuellen Host von der Hosts Seite ausgeführt werden können. Zugehörige vorkonfigurierte Datenerfassungsscripts werden in der nachfolgenden Tabelle aufgeführt. Alle dieser Audits können mit Hilfe von API Massenerfassungen angefordert werden. Zusätzliche Informationen finden Sie im Endpoint Security REST API-Handbuch.

Auditmodul	Bereitgestelltes vorkonfiguriertes Script (falls vorhanden)	Legacyname
agentinfo	---	---
config	---	---
configuration	---	---
containment	---	---
diagnostic	---	---
disk-acquisition	Raw Disk Script auf Seite 472	w32disk-acquisition
dissolve	---	---
driver-memoryacquire	Driver Memory	w32driver-memoryacquire
file-acquisition-api	---	w32apifile-acquisition
file-acquisition-raw	---	w32rawfile-acquisition
intel-key	---	---
iocload	---	---
iocmatch	---	---
log-audit	---	---

Auditmodul	Bereitgestelltes vorkonfiguriertes Script (falls vorhanden)	Legacyname
memory-acquisition	Full Memory	w32memory-acquisition
multifile-acquisition-api	---	w32multifileapi-acquisition
multifile-acquisition-raw	---	w32multifileraw-acquisition
plist-acquisition	---	---
processes-memoryacquire	Process Memory	w32processes-memoryacquire
reprovision	---	---
restart	---	---
upgrade	---	---

Weitere Informationen über Auditmodule finden Sie im *Endpoint Security Audit Referenzhandbuch*.

Bereitgestellte Scripts zurücksetzen

Sie können die ursprünglichen Einstellungen in den bereitgestellten Script wiederherstellen, nachdem sie verändert wurden. Informationen über die von FireEye bereitgestellten Scripts finden Sie unter Bereitgestellte Datenerfassungsscripts auf Seite 459.

Um ein bereitgestelltes Datenerfassungsscript zurückzusetzen:

1. Wählen Sie **Data Acquisition Scripts** auf dem Admin Menü auf der Endpoint Security Web-UI.
2. Wählen Sie das Script, das Sie zurücksetzen möchten, links auf der Seite aus.
3. Mindestens zwei **Actions** Menüs werden für benutzerdefinierte Scripts angezeigt. Ein Menü wird im Überschriftenbereich angezeigt und eins für jedes Betriebssystem, das das Script unterstützt. (Die mitgelieferten Standard Investigative Details, Comprehensive Investigative Details und Process Details Scripts verfügen nicht über ein **Actions** Menü im Überschriftenbereich.)

   Wählen Sie ggf. **Reset** im **Actions** Menü des Betriebssystem Abschnitts des Scripts, das Sie auf die Standardwerte zurücksetzen wollen.

   Das bereitgestellte Datenerfassungsscript wird auf seine Werkseinstellungen zurückgesetzt.

Verweis auf Erfassungsdatentyp

Die Erfassungsdatentypen, die in einer Datenerfassungsanfrage angefordert werden können, werden hier beschrieben. Bei diesen Erfassungstypen werden viele der gleichen Daten angefordert, die durch die Agent Audits gesammelt werden. Sie können diese Datentypen anfordern, indem Sie Ihr Datenerfassungsscript mit Hilfe der Data Acquisition Scripts Seite erstellen. Siehe Ein Script erstellen auf Seite 122. Detaillierte Informationen über jedes Auditmodul finden Sie im *Endpoint Security Audit Referenzhandbuch*.

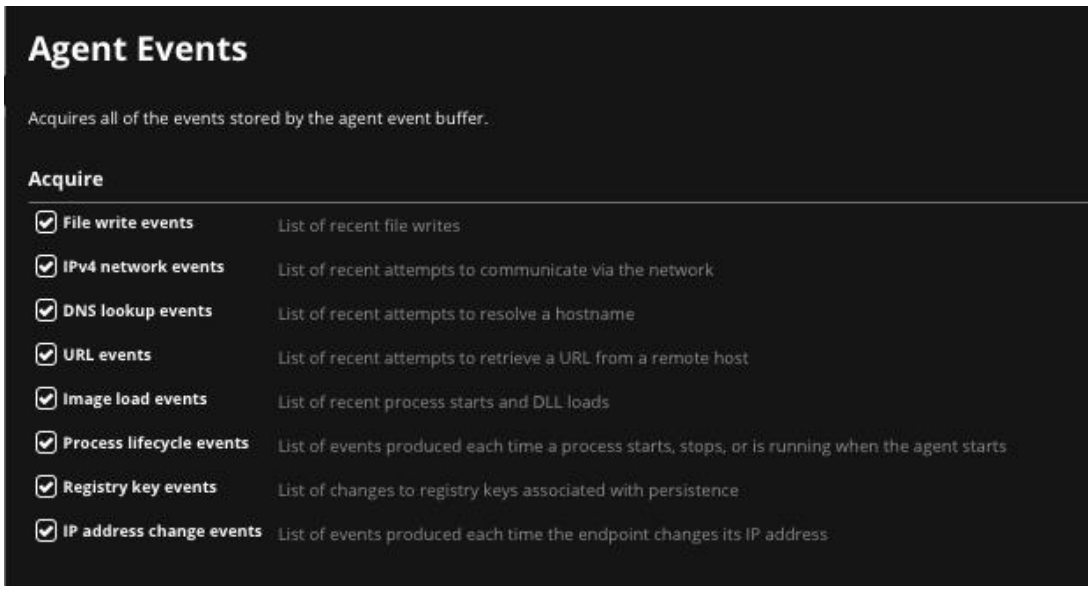
Wenn Sie Optionen über diese Register auswählen oder die Auswahl aufheben, könnte die Anzahl der für einen Erfassungstyp verfügbaren Optionen erweitert oder reduziert werden.

Erfassungsdatentyp	Endpunkt Betriebssystem Support		
	Windows	macOS	Linux
Agent Event Daten	Ja	Ja	Ja
Browser Daten	Ja	Ja	Nein
Driver Daten	Ja	Nein	Nein
Event Log Daten	Ja	Nein	Nein
File System Daten	Ja	Ja	Ja
Kernel Hook Detection Daten	Ja	Nein	Ja
Network Daten	Ja	Ja	Ja
Persistence Daten	Ja	Ja	Nein
Process Daten	Ja	Ja	Ja
Registry Daten	Ja	Nein	Nein
Service Daten	Ja	Ja	Nein
Shell History Daten	Nein	Nein	Ja
System Information Daten	Ja	Ja	Ja
System Log Daten	Nein	Ja	Nein
Task Daten	Ja	Ja	Ja

Agent Event Daten

Agent-Ereignisdaten können in Windows, macOS und Linux Umgebungen angefordert werden. Daten werden mit Hilfe des Eventbuffer-Auditmoduls gesammelt.

Wählen Sie **Agent Events** im **Add an acquisition type** Menü, um Daten zu erfassen, die im Agent Ereignispuffer (Ringpuffer) gespeichert sind. Das **Agent Events** Register wird angezeigt. Die Optionen auf diesem Tab hängen von dem Betriebssystem ab, das für das Datenerfassungsscript ausgewählt wurde. Das folgende Beispiel stammt von einem Windows-Script.

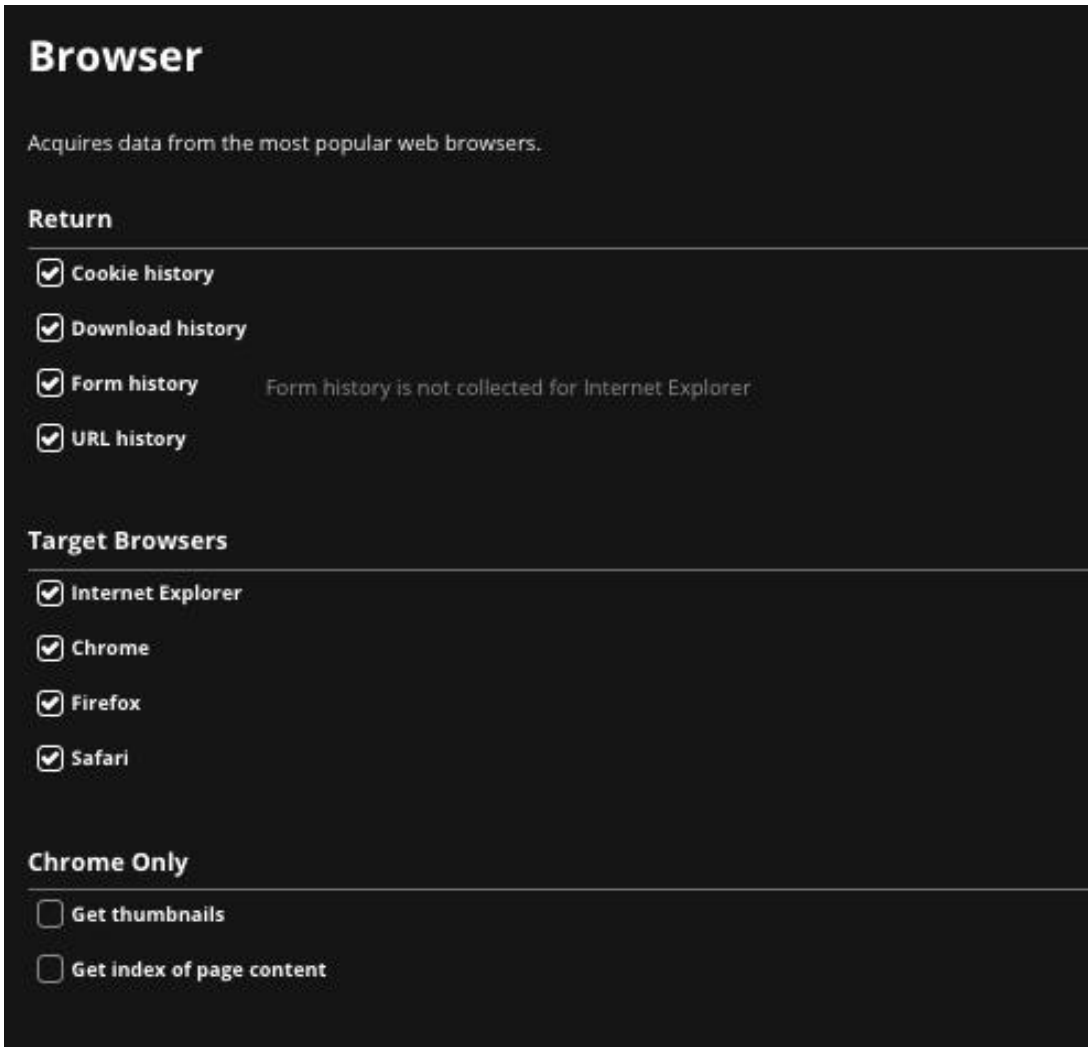


Verwenden Sie dieses Register, um die Ereignisdatentypen auszuwählen, die Sie in dieser Datenerfassungsanforderung sammeln wollen. URL-Ereignisdaten und Registrierungsschlüssel-Ereignisdaten können nicht für eine macOS Datenerfassung ausgewählt werden.

Browserdaten

Browserdaten können sowohl in Windows als auch in macOS Umgebungen angefordert werden. Daten werden mit Hilfe der cookiehistory, filedownloadhistory, formhistory, urlhistory und Quarantäne-Ereignisse (nur macOS) Auditmodule gesammelt.

Wählen Sie **Browser** im **Add an acquisition Type** Menü, um Daten aus den gängigsten Webbrowsern zu erfassen. Das **Browser** Register wird angezeigt. Die Optionen auf diesem Tab hängen von dem Betriebssystem ab, das für das Datenerfassungsscript ausgewählt wurde. Das folgende Beispiel stammt von einem Windows-Script.

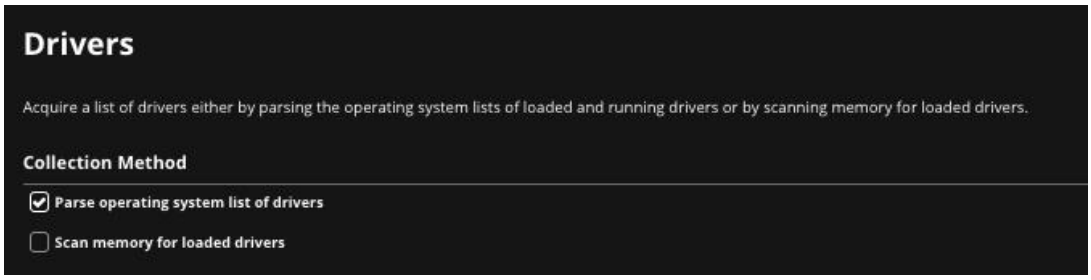


Verwenden Sie dieses Register, um die Browser auszuwählen, für die Sie Daten sammeln wollen und den Typen der Browserdaten, die Sie sammeln wollen. Quarantäne-Ereignisdaten können für macOS Endpunkte zurückgegeben werden.

Driver Daten

Treiberdaten können nur in Windows Umgebungen angefordert werden. Daten werden mit Hilfe der Treiber Modulliste und Treiber Signatur Auditmodule gesammelt.

Wählen Sie **Drivers** im **Add an acquisition type** Menü, um eine Liste von Treibern auf Ihrem Host Endpunkt zu erhalten. Das **Drivers** Register wird angezeigt.

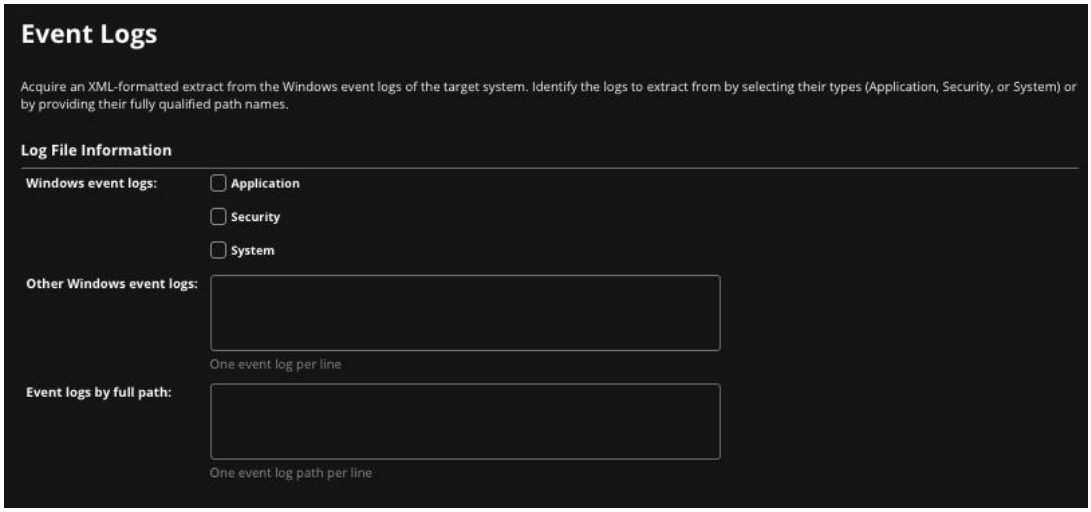


Verwenden Sie dieses Register, um anzugeben, wie die Treiberliste erfasst werden soll. Wenn Sie **Scan memory for loaded drivers** auswählen, werden weitere Optionen auf dem Drivers Register angezeigt.

Event Log Daten

Ereignisprotokolldaten können nur in Windows Umgebungen angefordert werden. Daten werden mit Hilfe des eventlogs Auditmoduls gesammelt.

Wählen Sie **Event Logs** im **Add an acquisition type** Menü, um einen Auszug der Windows Ereignisprotokolle eines Hosts im XML Format zu erfassen. Das **Event Logs** Register wird angezeigt.



Verwenden Sie dieses Register, um die Standard Ereignisprotokolle zu identifizieren, die Sie extrahieren wollen. Optional können Sie den vollständig qualifizierten Pfadnamen eines Ereignisprotokolls bereitstellen, das Sie extrahieren wollen.

Ereignisprotokolle verstehen

Bei der Arbeit mit Windows Ereignissprotokollen beachten Sie die folgenden Informationen.

- Wenn die Option *Event logs by name* benutzt wird, könnten Erfassungen mit einer Warnung in der issues.xml Datei fehlschlagen.
- Wenn die Option *Event logs by full path* benutzt wird, werden keine anderen auf der Seite konfigurierten Protokolle gesammelt. Die Verarbeitung von *Event logs by full path* wird gestoppt, wenn ein Ereignisprotokoll nicht gefunden wird und ein Fehler könnte in der issues.xml Datei angezeigt werden.
- Sie können eine Liste der Ereignisprotokolle in Ihrem System mit dem integrierten Windows `wevtutil` Dienstprogramm sehen. Zum Beispiel produziert der folgende Befehl eine Liste aller Ereignisprotokolle:

  ```
  wevtutil el
  ```

  Wenn Sie den spezifischen Pfad auf ein gegebenes Ereignisprotokoll sehen wollen, verwenden Sie die folgenden Parameter:

  ```
  wevtutil gl <event_log_name>
  ```

File System Daten

Dateisystemdaten können in Windows, macOS und Linux Umgebungen angefordert werden. Daten werden mit Hilfe der files-api und files-raw (nur Windows) Auditmodule gesammelt.

Wählen Sie **File System** im **Add an acquisition type** Menü, um eine Liste von Dateien und ihren Metadaten zu erhalten. Das File System Register wird angezeigt. Die Optionen auf diesem Tab hängen von dem Betriebssystem ab, das für das Datenerfassungsscript ausgewählt wurde.

Verwenden Sie dieses Register, um:

- Den Typ und den Speicherort der gesammelten Daten zu filtern. Sie können auch einen einzelnen Perl-kompatiblen regulären Ausdruck angeben, um den Pfad zu bestimmen, auf dem die Sammlung beginnen soll. Der eingegebene Ausdruck wird im **Regex path filter** Textfeld umgebrochen.

  Der reguläre Ausdrucksbereich der Endpoint Security Web-UI funktioniert anders als die Bearbeitung des Regex in einem Texteditor.

  - Wenn Sie einen Backslash zur Regex in der Web-UI hinzufügen, muss nur ein einzelner Backslash festgelegt werden. Wenn Endpoint Security den regex auf JSON konvertiert, werden diese einzelnen Backslashes auf doppelte Backslashes konvertiert. Daher entspricht der Regex in dem exportierten Script nicht der Version, die Sie in der Web UI sehen.
  - Bestimmen Sie `.*` in einem Script, um alle Dateien zu erfassen.
- Schließen Sie Dateien von Remotestandorten ein (nur Linux und macOS)
- Überprüfen Sie Digitale Signaturen (nur Windows und macOS)

- Schließen Sie alle Verzeichnisebenen ein
- Bestimmen Sie die Tiefe und Mindest- und Höchstdateigrößen für die Sammlung
- Aktivieren Sie Raw Modus (nur Windows)
- Wählen Sie bestimmte Dateihashes für die Sammlung aus
- Identifizieren Sie die Typen der Portable Executable (PE) Informationen, die Sie sammeln wollen (nur Windows)
- Geben Sie an, ob Sie Zeichenfolgen sammeln wollen (Nur Windows)
- Bestimmen Sie einen einzigen Perl-kompatiblen regulären Ausdruck in Windows Umgebungen , um andere Dateiinhalte zu identifizieren, die Sie sammeln wollen. Der eingegebene Ausdruck wird im **Regex** Textfeld umgebrochen.

  Der reguläre Ausdrucksbereich der Endpoint Security Web-UI funktioniert anders als die Bearbeitung des Regex in einem Texteditor. Wenn Sie einen Backslash zur Regex in der Web UI hinzufügen, muss nur ein einzelner Backslash festgelegt werden. Wenn der Endpoint Security den regex auf JSON konvertiert, werden diese einzelnen Backslashes auf doppelte Backslashes konvertiert. Daher entspricht der Regex in dem exportierten Script nicht der Version, die Sie in der Web UI sehen.

Sie können auch angeben, dass diese Daten bearbeitet werden können, wenn Sie eine Datenerfassung mit Hilfe dieses Scripts anfordern. Klicken Sie auf das **Allow edits before acquiring** Kontrollkästchen in den entsprechenden Abschnitten des Tabs, um diesen Abschnitt bei der Ausführung eines Scripts bearbeitbar zu machen.

Das Anfordern von PE-Daten oder Zeichenfolgen in der Datenerfassung des Dateisystem (nur Windows-Endpunkte) kann mehr Informationen als erwartet zurückgeben und zu Leistungs- und Speicherproblemen führen. FireEye empfiehlt, dass Sie diese Informationen nur für eine einzige Datei sammeln.

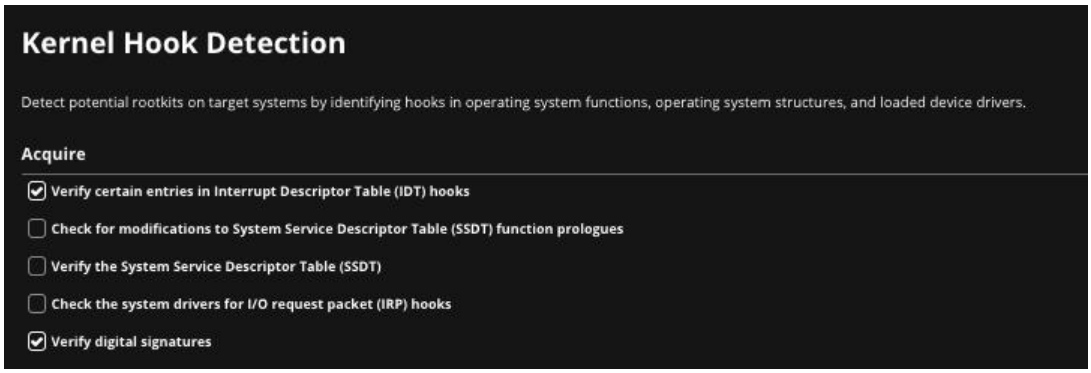
Ein schwerwiegender Fehler kann zurückgegeben werden, wenn der Raw Modus (nur Windows-Endpunkte) angefordert wird und der Dateipfad nicht gefunden werden kann.

Kernel Hook Detection Daten

Kernel-Hook Erkennungsdaten können in Windows und Linux Umgebungen angefordert werden. Daten werden mit Hilfe des kernel-hookdetection Auditmoduls gesammelt.

HINWEIS: Dieses Audit wird nicht mehr aktiv unterstützt. Es kann jedoch weiterhin mit unterstützten Windows Betriebssystemversionen vor Windows 10 1803 funktionieren.

Wählen Sie **Kernel Hook Detection** im **Add an acquisition type** Menü, um Informationen über potentielle Rootkits auf einem Host Endpunkt zu erhalten. Das **Kernel Hook Detection** Register wird angezeigt.

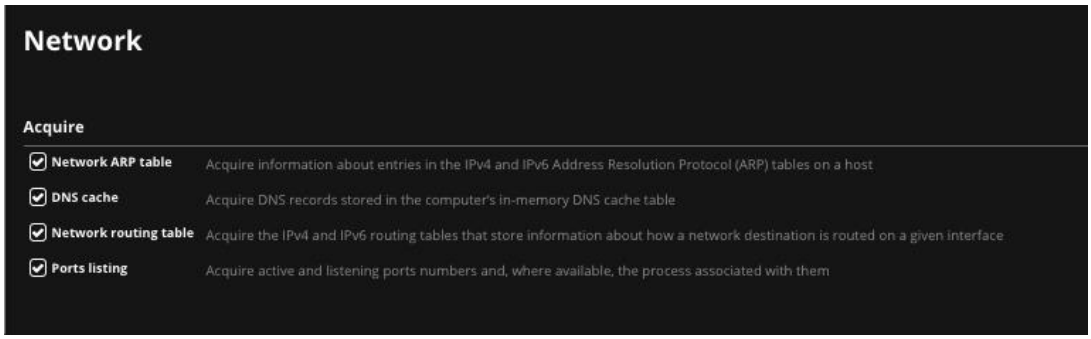


Verwenden Sie diesen Tab, um die Betriebssystemfunktionen und Strukturen und die geladenen Gerätetreiber auszuwählen, die nach Kernel Hooks durchsucht werden sollen.

Network Data

Netzwerkdaten können in Windows, macOS und Linux Umgebungen angefordert werden. Daten werden mit Hilfe der network-arp (nur Windows und macOS), network-dns (nur Windows und macOS), network-route(nur Windows und macOS) und ports Auditmodule gesammelt.

Wählen Sie **Network** im **Add an acquisition type** Menü, um die Netzwerkinformationen zu identifizieren, die Sie erfassen wollen. Der **Network** Tab wird angezeigt. Die Optionen auf diesem Tab hängen von dem Betriebssystem ab, das für das Datenerfassungsscript ausgewählt wurde. Das folgende Beispiel stammt von einem Windows-Script.

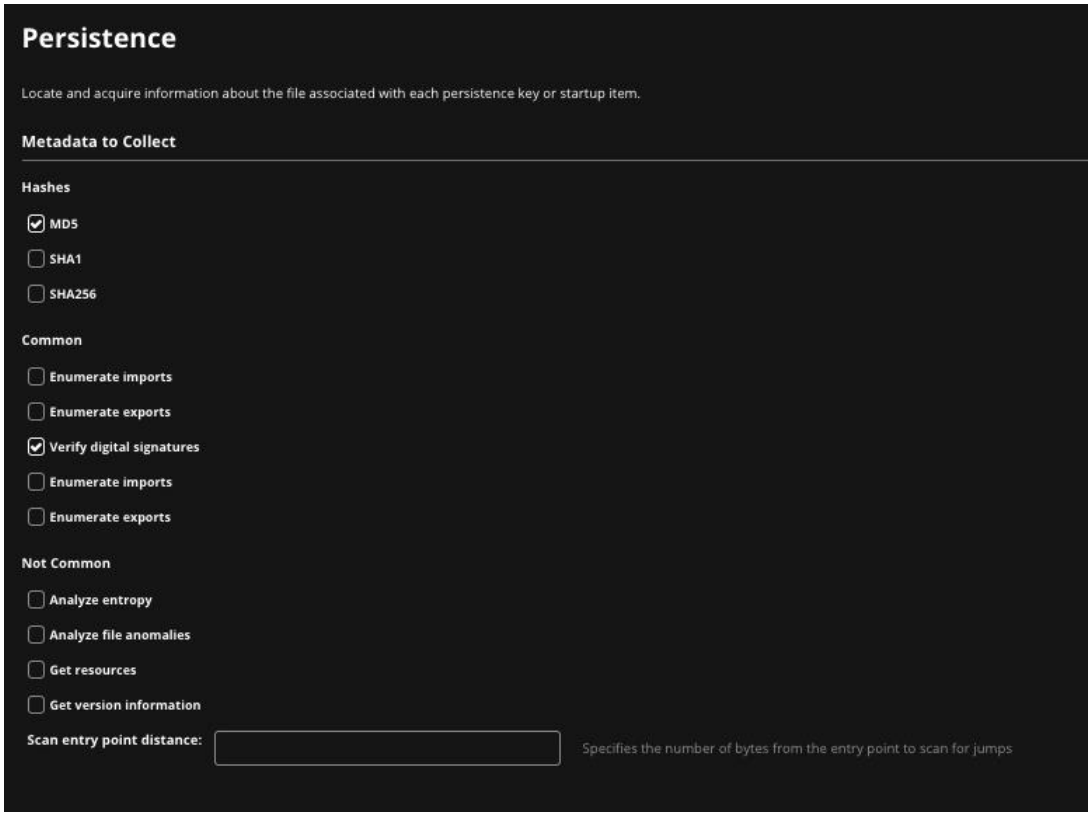


Verwenden Sie diesen Tab, um die Arten der Netzwerkinformationen zu wählen, die Sie in dieser Datenerfassungsanforderung sammeln wollen. Von Linux Endpunkten können nur Portinformationen gesammelt werden.

Persistence Daten

Persistenzdaten können sowohl in Windows als auch in macOS Umgebungen angefordert werden. Daten werden mit Hilfe des persistence Auditmoduls gesammelt.

Wählen Sie **Persistence** im **Add an acquisition type** Menü, um Daten über die Dateien zu erfassen, die mit jedem Persistenzschlüssel oder Startelement zugeordnet sind. Die Optionen auf diesem Tab hängen von dem Betriebssystem ab, das für das Datenerfassungsscript ausgewählt wurde. Das folgende Beispiel stammt von einem Windows-Script.



Verwenden Sie diesen Tab, um die Metadatentypen auszuwählen, von denen Persistenzinformationen für diese Datenerfassungsanforderung gesammelt werden sollen. Für macOS Endpunkte können Sie nur MD5, SHA1 und Hashes und digitale Signatur-Verifizierungsmetadaten anfordern.

Process Daten

Prozessdaten können in Windows, macOS und Linux Umgebungen angefordert werden. Daten werden mit Hilfe der processes-api, processes-handle (nur Windows) und processes-memory (nur Windows) Auditmodule gesammelt.

Wählen Sie **Processes** im **Add an acquisition type** Menü, um Prozessinformationen von Ihrem Host Endpunkt zu erhalten. Das **Processes** Register wird angezeigt. Die Optionen auf diesem Tab hängen von dem Betriebssystem ab, das für das Datenerfassungsscript ausgewählt wurde. Für macOS oder Linux Datenerfassungsscripts sind keine dieser Optionen verfügbar.

Für Windows Endpunkte verwenden Sie dieses Register um:

- Zu Filtern, wie die Prozessliste erfasst werden soll
- Die nach PID (Prozess ID) oder Prozessname gesammelten Prozess einzuschränken
- Die Metadaten zu identifizieren, die gesammelt werden sollen
- Raw Modus zu aktivieren
- Anzudeuten, ob Sie Zeichenfolgen sammeln wollen
- Einen einzelnen Perl-kompatiblen regulären Ausdruck anzugeben, um anderen Prozessinhalt zu identifizieren, der gesammelt werden soll. Der eingegebene Ausdruck wird im **Regex** Textfeld umgebrochen.

  Der reguläre Ausdrucksbereich der Endpoint Security Web-UI funktioniert anders als die Bearbeitung des Regex in einem Texteditor. Wenn Sie einen Backslash zur Regex in der Web UI hinzufügen, muss nur ein einzelner Backslash festgelegt werden. Wenn der Endpoint Security den regex auf JSON konvertiert, werden diese einzelnen Backslashes auf doppelte Backslashes konvertiert. Daher entspricht der Regex in dem exportierten Script nicht der Version, die Sie in der Web UI sehen.

Sie können auch angeben, dass diese Daten bearbeitet werden können, wenn Sie eine Datenerfassung mit Hilfe dieses Scripts anfordern. Klicken Sie auf das **Allow edits before acquiring** Kontrollkästchen in den entsprechenden Abschnitten des Tabs, um dieses Abschnitt bei der Ausführung eines Scripts bearbeitbar zu machen.

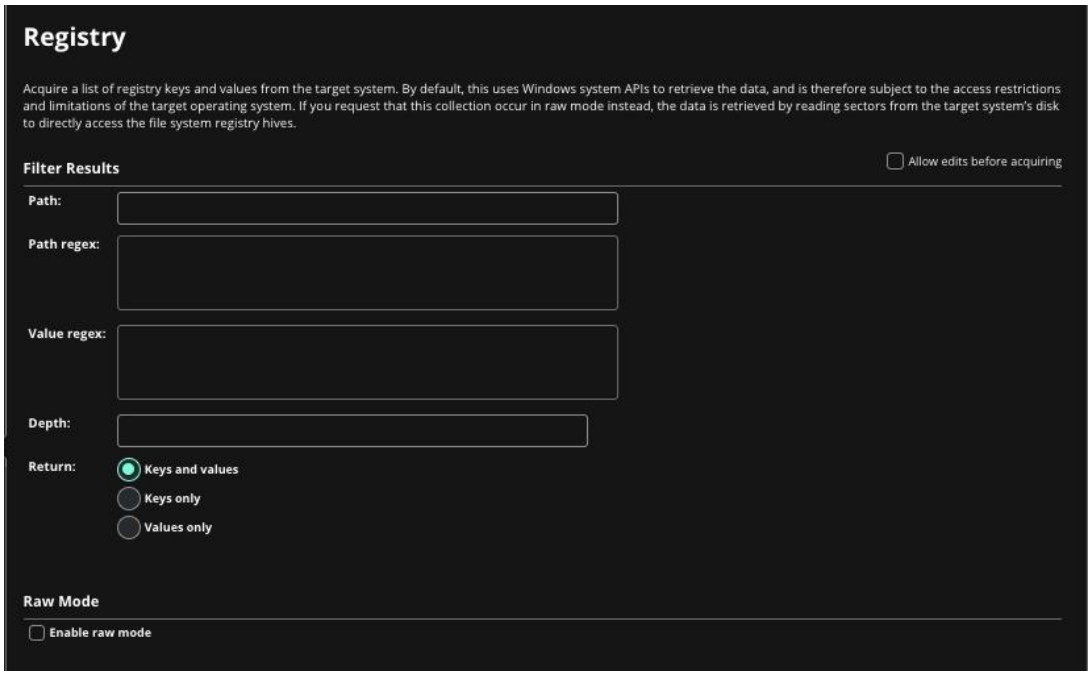
Die Details, die Sie über Prozesse sammeln können, umfassen Speicherdaten und Zeichenfolgen im Speicher für einen Prozess. Sie können die Daten im Audit Viewer überprüfen. Wenn Sie die Erfassung herunterladen, können die Daten in Redline überprüft werden.

Das Anfordern von Zeichenfolgen in Ihrer Prozessdatenerfassung kann mehr Informationen als erwartet zurückgeben und zu Leistungs- und Speicherproblemen führen, insbesondere wenn Sie Zeichenfolgen für alle Prozesse anfordern. FireEye empfiehlt, dass Sie diese Informationen nur für einen einzigen Prozess sammeln.

Registry Daten

Registrierungsdaten können nur in Windows Umgebungen angefordert werden. Daten werden mit Hilfe der registry-api und registry-raw audit Module gesammelt.

Wählen Sie **Registry** im **Add an acquisition type** Menü, um eine Liste von Registrierungsschlüsseln und Werten von einem Host Endpunkt zu erhalten. Das **Registry** Verzeichnis wird angezeigt.



Verwenden Sie dieses Register, um die Ergebnisse zu filtern, zu identifizieren, was zurückgegeben wird und Raw Modus zu aktivieren.

Reguläre Ausdrücke in Registry Scripts müssen von einem harten Zeilenumbruch gefolgt sein, damit sie gespeichert werden können.

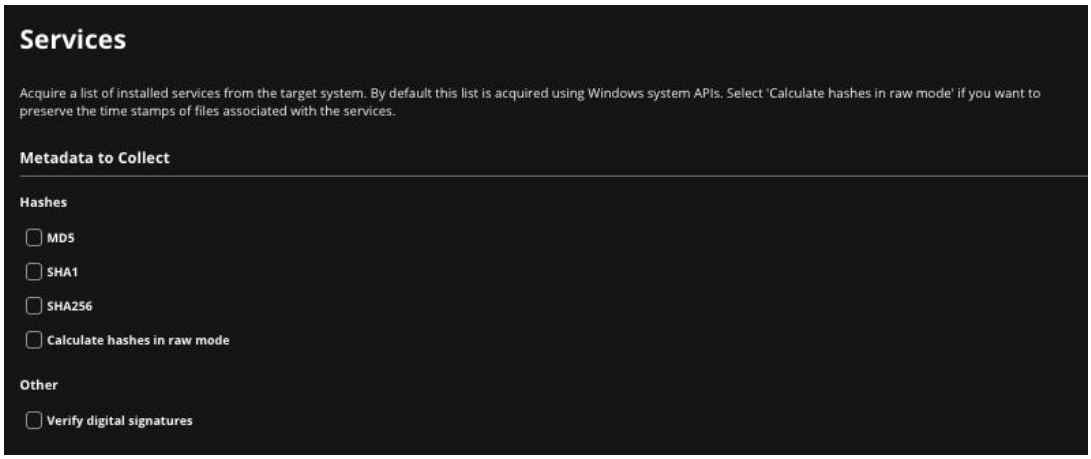
Zusätzlich müssen **Path regex** und **Value regex** Spezifikationen Perl-kompatibel sein.

Sie können auch angeben, dass diese Daten bearbeitet werden können, wenn Sie eine Datenerfassung mit Hilfe dieses Scripts anfordern. Klicken Sie auf das **Allow edits before acquiring** Kontrollkästchen in den entsprechenden Abschnitten des Tabs, um dieses Abschnitt bei der Ausführung eines Scripts bearbeitbar zu machen.

Service Daten

Servicedaten können sowohl in Windows als auch in macOS Umgebungen angefordert werden. Daten werden mit Hilfe des services Auditmoduls gesammelt.

Wählen Sie **Services** im **Add an acquisition type** Menü, um eine Liste der installierten Dienste auf einem Host Endpunkt zu erhalten. Das **Services** Register wird angezeigt. Die Optionen auf diesem Tab hängen von dem Betriebssystem ab, das für das Datenerfassungsscript ausgewählt wurde. Das folgende Beispiel stammt von einem Windows-Script.



Verwenden Sie dieses Register, um die Metadaten auszuwählen, die Sie sammeln wollen und anzugeben, ob Hashes im Raw Modus gesammelt werden sollen und ob digitale Signaturen verifiziert werden sollen. In macOS Datenerfassungsscripts können Sie Hashes im Raw Modus nicht berechnen.

Shell History Daten

Shell Verlaufsdaten können nur in Linux Umgebungen angefordert werden. Daten werden mit Hilfe des shell-history Auditmoduls gesammelt. Befehlsverläufe von den `bash`, `zsh` und `ksh93` Linux Shells werden gesammelt.

Wählen Sie **Shell History** im **Add an acquisition type** Menü, um Systemprotokolle von einem Host Endpunkt zu erfassen. Das **Shell History** Register wird angezeigt.

Verwenden Sie dieses Register, um die Ergebnisse zu filtern.

HINWEIS: Reguläre Ausdrücke in Registry Scripts müssen von einem harten Zeilenumbruch gefolgt sein, damit sie gespeichert werden können.

Zusätzlich muss die **Command regex** Spezifikation Perl-kompatibel sein.

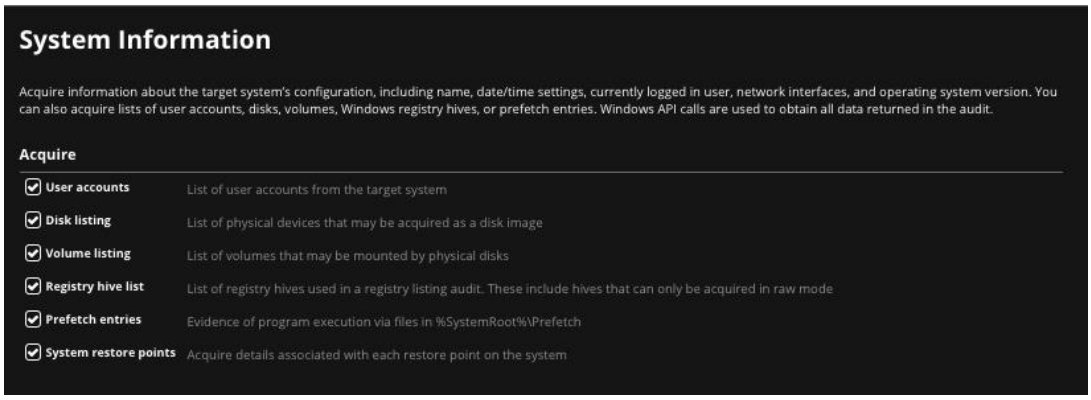
Sie können auch angeben, dass diese Daten bearbeitet werden können, wenn Sie eine Datenerfassung mit Hilfe dieses Scripts anfordern. Klicken Sie auf das **Allow edits before acquiring** Kontrollkästchen in den entsprechenden Abschnitten des Tabs, um dieses Abschnitt bei der Ausführung eines Scripts bearbeitbar zu machen.

System Information

Systeminformationen werden in jedem Datenerfassungsscript in Windows, macOS und Linux Umgebungen angefordert. Daten werden mit Hilfe der sysinfo, useraccounts (nur Windows und macOS), Gruppen (nur macOS), Disks (nur Windows und macOS),

Volumen (nur Windows und macOS), hivelist (nur Windows), prefetch (nur Windows) and systemrestore (nur Windows) Audit Module gesammelt.

Sie können die Arten von Systeminformationen auswählen, die erfasst werden. Klicken Sie auf das **System Information** Register.



Verwenden Sie diesen Tab, um die Arten von Systeminformationen auszuwählen, die erfasst werden sollen. Je nach Ihrer Auswahl werden unterschiedliche Audits (oder Teile von Audits) ausgeführt. Wenn in der nachfolgenden Tabelle (---) kein Audit aufgeführt ist, werden diese Daten nicht für das zugehörige Betriebssystem gesammelt. Vollständige Informationen über die Auditmodule finden Sie im *Endpoint Security Audit Referenzhandbuch*.

Angeforderte Daten	Windows Audit	macOS Audit	Linux Audit
Userkonten	sysinfo useraccounts	sysinfo useraccounts	sysinfo
Gruppen	---	groups	---
Laufwerkliste	disks	disks	---
Volumenliste	volumes	volumes	---
Registrungsstrukturliste	hivelist	---	---
Prefetch-Einträge	prefetch	---	---
Systemwiederherstellungspunkte	systemrestore	---	---

System Log Daten

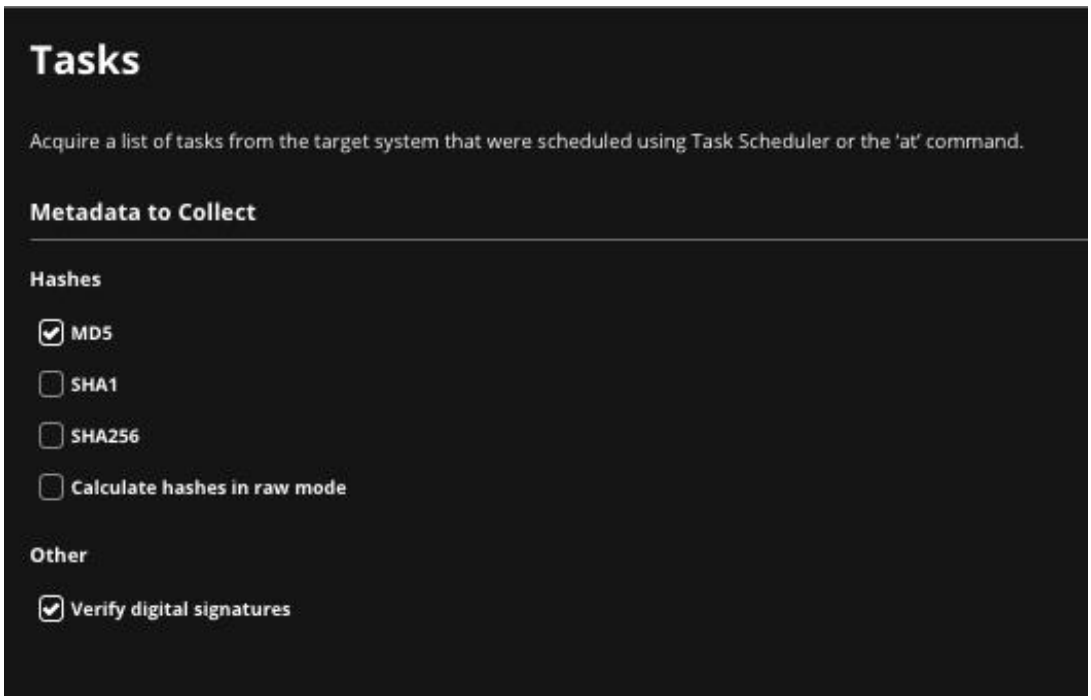
Systemprotokolldaten können nur in macOS Umgebungen angefordert werden. Daten werden mit Hilfe des syyslog Auditmoduls gesammelt.

Wählen Sie **System Logs** im **Add an acquisition type** Menü, um Systemprotokolle von einem Host Endpunkt zu erhalten. Das **System Logs** Register wird angezeigt.

Task Daten

Aufgabendaten können in Windows, macOS und Linux Umgebungen angefordert werden. Daten werden mit Hilfe des tasks Auditmoduls gesammelt.

Wählen Sie **Tasks** im **Add an acquisition type** Menü, um eine Liste von Aufgaben zu erhalten, die auf dem Host Endpunkt geplant wurden. Der **Tasks** Tab wird angezeigt. Die Optionen auf diesem Tab hängen von dem Betriebssystem ab, das für das Datenerfassungsscript ausgewählt wurde. Das folgende Beispiel stammt von einem Windows-Script.



Verwenden Sie dieses Register, um die Metadaten auszuwählen, die Sie sammeln wollen und anzugeben, ob Hashes im Raw Modus gesammelt werden sollen und ob digitale Signaturen verifiziert werden sollen. In macOS Datenerfassungsscripts können Sie Hashes nicht im Raw Modus berechnen.

KAPITEL 5: Einstellungen für Enterprise Search konfigurieren

Mit den Einstellungen für die Enterprise Search können Sie die maximale Anzahl der möglichen Suchvorgänge, die definiert werden können, die Anzahl gleichzeitig ausführbarer Suchvorgänge und die Anzahl eindeutiger Probleme für eine Enterprise Search konfigurieren, die sich auf fehlerhafte oder unerwartete Daten auf Host Endpunkten während der Suche beziehen.

Die Anzahl definierter Suchen einschränken

Sie können ein Limit für die maximale Anzahl von Suchen einstellen, die auf der Enterprise Search Seite definiert werden können. Der Standardwert ist 10 Suchvorgänge. Wenn das konfigurierte Limit erreicht ist, treten Fehler auf.

Sie können dieses Limit mit Hilfe der CLI überprüfen und verändern.

Voraussetzungen

- Admin Zugriff

Das maximale Suchlimit überprüfen

Um das maximale Suchlimit zu überprüfen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Überprüfen Sie die Problemgrenze:

   ```
   hostname (config) # show hx server search
   ```

   Die Ausgabe dieses Befehls könnte folgendermaßen aussehen:

   ```
   HX Enterprise Security Search Configurations:

   Concurrent search limit: 5
   Existing search limit: 10
   Search issues item limit: 10
   ```

Das maximale Suchlimit ändern

Um das maximale Suchlimit zu ändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Ändern Sie das Problemlimit:

   ```
   hostname (config) # hx server search existing-search-limit <number>
   ```

   wobei `<number>` die maximale Anzahl von Enterprise Searches ist, die auf der Enterprise Search Seite definiert ist. Gültige Werte liegen zwischen 0 bis 15. Der Standardwert ist 10.

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Auf das Standard maximale Suchlimit zurückkehren

Um auf das Standard maximale Suchlimit von 10 eindeutigen Problemen zurückzukehren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Kehren Sie auf den Standardwert für das Limit zurück:

   ```
   hostname (config) # no hx server search existing-search-limit
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```


Die Anzahl der gleichzeitigen Suchen einschränken

Sie können ein Limit für die Anzahl der Suchen festlegen, die gleichzeitig ausgeführt werden können. Der Standardwert ist fünf gleichzeitige Suchen. Wenn das konfigurierte Limit erreicht ist, treten Fehler auf.

Sie können das Limit für die gleichzeitige Suche mit Hilfe der CLI überprüfen und verändern.

Voraussetzungen

- Admin Zugriff

Das Limit für die gleichzeitige Suche überprüfen

Um das Limit für die gleichzeitige Suche zu überprüfen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Überprüfen Sie die Problemgrenze:

   ```
   hostname (config) # show hx server search
   ```

   Die Ausgabe dieses Befehls könnte folgendermaßen aussehen:

   ```
   HX Enterprise Security Search Configurations:

   Concurrent search limit: 5
   Existing search limit: 10
   Search issues item limit: 10
   ```

Das Limit für die gleichzeitige Suche ändern

Um das Limit für die gleichzeitige Suche zu ändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Ändern Sie das Limit für die gleichzeitige Suche:

   ```
   hostname (config) # hx server search concurrent-search-limit <number>
   ```

   wobei `<number>` die Anzahl der Enterprise Searches ist, die gleichzeitig ausgeführt werden können. Gültige Werte liegen zwischen 0 bis 15. Der Standardwert ist 5.

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Auf den Standardwert für das Limit für die gleichzeitige Suche zurückkehren

Um auf den Standardwert für das Limit von 5 einzigartigen Problemen für die gleichzeitige Suche zurückzukehren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Kehren Sie auf den Standardwert für das Limit zurück:

   ```
   hostname (config) # no hx server search concurrent-search-limit
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Falsch formatierte oder unerwartete Datenprobleme beschränken

Sie können ein Limit für die Anzahl der für eine Enterprise Seach gemeldeten einzigartigen Probleme festlegen, die sich auf falsch formatierte oder unerwartete Daten beziehen, die auf Hosts Endpunkten während der Suche gefunden wurden. Solche Suchprobleme treten häufig auf, aber könnten bedeuten, dass der Host nicht vollständig nach den Elementtypen durchsucht werden konnte, in denen die Probleme aufgetreten sind.

Der Standardwert ist 10 einzigartige Probleme. Wenn dieses Limit erreicht ist, stoppt der Endpoint Security die Aufzeichnung von Problemen für die Suche, obwohl die Enterprise Search weiterläuft.

Sie können dieses Limit mit Hilfe der CLI überprüfen und verändern.

Voraussetzungen

- Admin Zugriff

Das Problemlimit überprüfen

Um das Problemlimit zu überprüfen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Überprüfen Sie das Problemlimit:

   ```
   hostname (config) # show hx server search
   ```

   Die Ausgabe dieses Befehls könnte wie folgt aussehen:

   ```
   Search issues item limit: 20
   ```

Das Problemlimit ändern

Um das Problemlimit zu ändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Ändern Sie das Problemlimit:

   ```
   hostname (config) # hx server search issues items-limit <number>
   ```

   wobei `<number>` die Anzahl der einzigartigen Suchprobleme ist, die für eine Enterprise Search gemeldet wurde. Gültige Werte liegen zwischen 10 bis 100 Problemen. Angabe von 0 fordert an, dass mit falsch formatierten oder unerwarteten Daten auf Host Endpunkten verbundene Suchprobleme nicht für Enterprise Searches gemeldet werden sollten.

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Auf den Standardwert für Problemlimits zurückkehren

Um auf den Standardwert von 10 eindeutigen Problemen zurückzukehren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Kehren Sie auf den Standardwert für das Limit zurück:

   ```
   hostname (config) # no hx server search issues items-limit
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

KAPITEL 6: Eindämmung konfigurieren

Die Eindämmungsfunktion verhindert weitere Kompromittierung eines Host-Endpunkt Systems und Komponenten, indem sie die Kommunikationsfähigkeit des eingedämmten Hosts auf dem Netzwerk einschränkt eingeschränkt wird. Sie können die folgenden Aktionen für die Verwaltung der Eindämmungsfunktion ausführen:

- Zugriff auf Eindämmung blockieren und freigeben unten
- Eindämmung ein- und ausschalten auf der nächsten Seite
- Hostsätze von Eindämmung ausschließen auf Seite 158
- Die Whitelist für eingedämmte Hosts verwalten auf Seite 161
- Den Containment Freigabecode aktivieren und deaktivieren auf Seite 165
- Endbenutzer über Host-Eindämmung benachrichtigen auf Seite 166

Informationen über die Eindämmung eines Host Endpunkts finden Sie unter Überblick über Eindämmung auf Seite 421.

Zugriff auf Eindämmung blockieren und freigeben

Sie können den Zugriff auf die Eindämmungsfunktion auf der Endpoint Security Web-UI mit Hilfe des `block containment` CLI Befehls blockieren. Wenn die Eindämmungsfunktion blockiert ist, zeigt der Containment Switch **DISABLED** in der Web-UI an.

Wenn die Eindämmungsfunktion blockiert ist, müssen Sie Eindämmung mit Hilfe der CLI freigeben.

Voraussetzungen

- Admin Zugriff

Dieses Thema enthält die folgenden Aufgaben:

- Eindämmungszugriff mit Hilfe der CLI blockieren unten
- Eindämmungszugriff mit Hilfe der CLI entsperren unten

Eindämmungszugriff mit Hilfe der CLI blockieren

Um Eindämmungszugriff zu blockieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Blockieren Sie den Zugriff auf Eindämmung.

   ```
   hostname (config) # hx server containment block
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Eindämmungszugriff mit Hilfe der CLI entsperren

Um Eindämmungszugriff zu entsperren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Entsperren Sie den Eindämmungszugriff.

   ```
   hostname (config) # no hx server containment block
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Eindämmung ein- und ausschalten

Die Eindämmungsfunktion kann eine leistungsstarke Waffe im Sicherheitsarsenal Ihres Unternehmens sein. Sie können die Endpoint Security Eindämmungsfunktion mit Hilfe der Endpoint Security Web-UI oder der CLI ein- und ausschalten. Standardmäßig ist die Eindämmungsfunktion eingeschaltet.

HINWEIS: Wenn Eindämmung deaktiviert ist (in der Web-UI wird DISABLED angezeigt), können Sie es nicht ein- oder ausschalten. Sie müssen Eindämmung zunächst mit Hilfe der CLI aktivieren. Siehe Zugriff auf Eindämmung blockieren und freigeben auf der vorherigen Seite.

Dieser Abschnitt beschreibt:

Voraussetzungen

- Admin Zugriff

Eindämmung mit Hilfe der Web-UI einschalten

Um die Eindämmungsfunktion mit Hilfe der Web-UI einzuschalten:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Containment Settings** auf dem **Admin** Menü. Die **Containment Settings** Seite wird geöffnet.
3. Schieben Sie den **Containment** Schalter auf **On**.
4. Klicken Sie auf **Save**.

Eindämmung mit Hilfe der CLI einschalten

Um die Eindämmungsfunktion mit Hilfe der CLI einzuschalten:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Schalten Sie Eindämmung ein.

   ```
   hostname (config) # hx server containment enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Eindämmung mit Hilfe der Web-UI ausschalten

Um die Eindämmungsfunktion mit Hilfe der Web-UI auszuschalten:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Containment Settings** auf dem **Admin** Menü. Die Containment Settings Seite wird geöffnet.
3. Schieben Sie den **Containment** Schalter auf **Off**.
4. Klicken Sie auf **Save**.

Eindämmung mit Hilfe der CLI ausschalten

Um die Eindämmungsfunktion mit Hilfe der CLI auszuschalten:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Schalten Sie Eindämmung aus.

   ```
   hostname (config) # no hx server containment enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Hostsätze von Eindämmung ausschließen

Standardmäßig unterliegen alle Hosts der Eindämmung. Sie sollten möglicherweise Eindämmung für bestimmte Hosts einschränken (z.B. könnte die Eindämmung des Mailservers für Ihr Netzwerk unternehmensweite Kommunikation beeinträchtigen). Hosts können nur von der Eindämmung ausgeschlossen werden, wenn sie Mitglieder eines Hostsatzes sind.

HINWEIS: Sie können einen Hostsatz erstellen, der nur einen Host enthält.

Wenn Eindämmungsaktionen bereits durchgeführt werden, wirkt sich das Ausschließen von Host Sätzen aus der Eindämmung auf die in den Sätzen enthaltenen Hosts wie folgt aus:

- **Hosts, für die Eindämmung angefordert wird:** Der Host verbleibt auf dem **Requested** Register der **Containment** Seite. Solange sich die Agent Software des Hosts jedoch auf dem Host befindet, kann die Eindämmungssanforderung nicht genehmigt werden.

- **Hosts, die eingedämmt sind oder für die Eindämmung genehmigt wurde:**Der Host verbleibt in einem eingedämmten Zustand, bis er freigegeben wird. Nachdem der Host aus der Eindämmung freigegeben wird, kann er nicht länger eingedämmt werden.

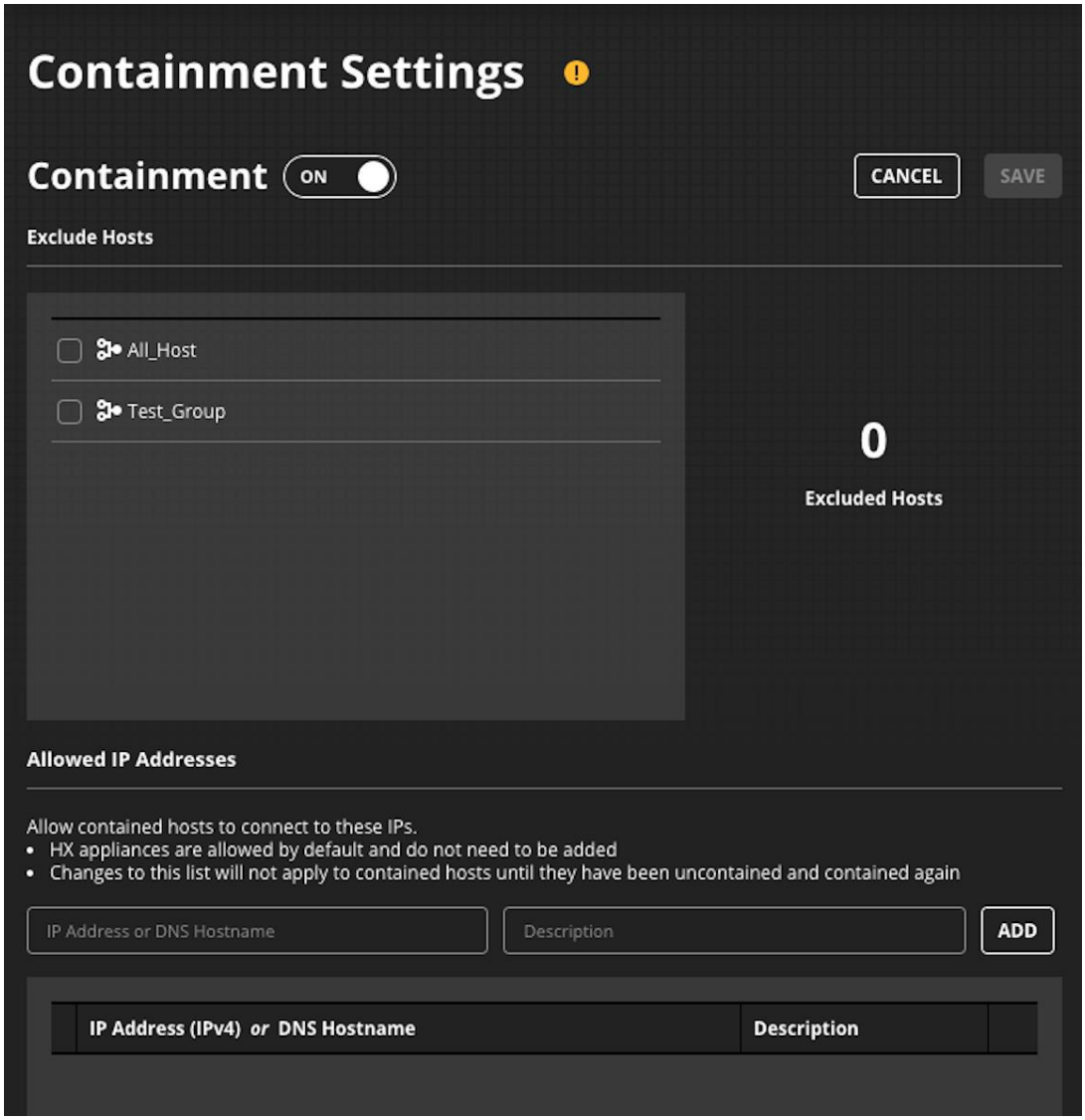
HINWEIS: Sie können Hosts nur mit Hilfe der Endpoint Security Web-UI von der Eindämmung ausschließen.

Wenn ein Host Satz von der Eindämmung ausgeschlossen ist, werden die in dem Host Satz eingeschlossenen Hosts für Eindämmung untauglich und werden auf Web-UI Seiten mit dem Untauglich Symbol ( ) angezeigt.

Voraussetzungen

- Admin Zugriff

Hostsätze von Eindämmung mit Hilfe der Web-UI ausschließen



Um Hosts auszuschließen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Containment Settings** auf dem **Admin** Menü.
3. In der **Exclude Hosts** Liste wählen Sie Host Sätze, die ausgeschlossen werden sollen.
4. Klicken Sie auf **Save**.

Die Whitelist für eingedämmte Hosts verwalten

Standardmäßig können eingedämmte Hosts nur mit dem Endpoint Security kommunizieren. Durch Erstellung einer Whitelist für eingedämmte Hosts ermöglichen Sie eingedämmten Hosts, mit bestimmten IPv4-Adressen und Hostnamen zu kommunizieren.

Whitelisting funktioniert nur, wenn eine direkte Verbindung zwischen Ihrem Host-Endpunkt und einem verbundenen System besteht. Wenn Ihr eingedämmter Host mit anderen System über den Proxy-Server verbunden ist, können Sie die eingedämmte Host IP-Adresse nicht whitelisten.

WICHTIG: Die Verwendung von DNS-Namen anstelle von IP-Adressen in Ihrer Server Whitelist kann in einigen Szenarien für einen eingedämmten Host Probleme verursachen. Stellen Sie sicher, dass Ihre Serverliste (**Admin** > **Policies** > **Agent Default policy** > **Server Address**) die IP-Adresse Ihres Endpoint Security Servers enthält.

Ein eingedämmter Host bleibt so lange eingedämmt, wie der Endpoint Security Agent installiert ist und auf dem Host-Endpunkt ausgeführt wird oder bis Sie den Host aus der Eindämmung entfernen. Wenn der Agent von einem eingedämmten Host heruntergefahren oder deinstalliert wird, ist der Host nicht länger eingedämmt.

WICHTIG: Wenn die IP-Adresse eines Host auf der Whitelist geändert wird, nachdem ein Host-Endpunkt eingedämmt wurde, kann der Endpunkt den Host auf der Whitelist nicht kontaktieren.

Um sicherzustellen, dass eingedämmte Hosts auf einer VPN-Verbindung weiterhin mit dem Endpoint Security kommunizieren, fügen Sie die IP-Adresse für Ihr VPN zu der Containment-Whiteliste hinzu. Wenn die VPN-IP-Adresse nicht auf der Whiteliste steht, könnten Endpoint Security Anfragen, einschließlich Anfragen zur Aufhebung der Eindämmung, den Host-Endpunkt nicht erreichen, weil die VPN-Verbindung nach der Eindämmung unterbrochen wird.

In diesem Abschnitt wird die Verwaltung Ihrer Contained Host Whiteliste beschrieben.

- Einen Host zu der Containment Whiteliste mit Hilfe der Web-UI hinzufügen auf der nächsten Seite
- Einen Host zur Containment Whiteliste mit Hilfe der CLI hinzufügen auf der nächsten Seite
- Die Hostbeschreibung in der Containment-Whitliste mit Hilfe der CLI verändern auf Seite 163

- Einen Hosts aus der Containment Whiteliste mithilfe der Web-UI entfernen auf Seite 164
- Einen Hosts aus der Containment Whiteliste mithilfe der CLI entfernen auf Seite 164

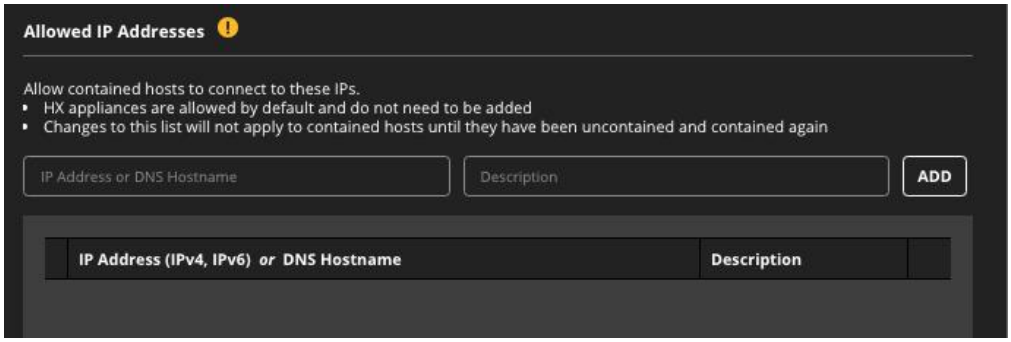
Voraussetzungen

- Admin Zugriff

Einen Host zu der Containment Whiteliste mit Hilfe der Web-UI hinzufügen

Um einen Host zu der Containment Whiteliste mit Hilfe der Web-UI hinzuzufügen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Containment Settings** auf dem **Admin** Menü.
3. Im Allowed IP Addresses Abschnitt geben Sie die IP-Adresse oder den Hostnamen ein, den Sie hinzufügen wollen.



Wenn die IP-Adresse eines Hosts auf der Whiteliste geändert wird, nachdem ein Host Endpunkt eingedämmt wurde, kann der Endpunkt keinen Kontakt mit dem Host auf der Whiteliste aufnehmen.

4. Klicken Sie auf **Add**.

Einen Host zur Containment Whiteliste mit Hilfe der CLI hinzufügen

Um einen Host zu der Containment Whitlist mit Hilfe der CLI hinzuzufügen:

1. Aktivieren Sie den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```


2. Fügen Sie die IP-Adresse oder den Hostnamen zur Containment Whiteliste hinzu.

   ```
   hostname (config) # hx server containment whitelist <IPorHostname>
   description <description>
   ```

   Wenn die IP-Adresse eines Hosts auf der Whiteliste geändert wird, nachdem ein Host Endpunkt eingedämmt wurde, kann der Endpunkt keinen Kontakt mit dem Host auf der Whiteliste aufnehmen.

   Eine Beschreibung ist optional. Schießen Sie Beschreibung, die länger als ein Wort sind, in Anführungszeichen (") ein.

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Beispiele

Im folgenden Beispiel wird eine Host IP zu der Containment Whiteliste ohne Beschreibung hinzugefügt:

```
hostname (config) # hx server containment whitelist 123.45.6.7
```

Im folgenden Beispiel wird ein Hostname zu der Containment Whiteliste mit einer ein-Wort Beschreibung hinzugefügt.

```
hostname (config) # hx server containment whitelist testserverhost
description testserver
```

Im Folgenden Beispiel wird eine Host IP zu der Containment Whiteliste mit einer Beschreibung aus mehreren Wörtern hinzugefügt.

```
hostname (config) # hx server containment whitelist 123.45.6.7 description
“The Group A Test Appliance”
```

Die Hostbeschreibung in der Containment-Whitliste mit Hilfe der CLI verändern

Sie können die Hostbeschreibung ändern, indem Sie eine neue Beschreibung für einen vorhandenen Host eingeben, der in der Whiteliste aufgeführt ist.

Um die Hostbeschreibung in der Containment-Whiteliste zu verändern:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Verändern Sie die Hostbeschreibung. Schießen Sie Beschreibung, die länger als ein Wort sind, in Anführungszeichen (") ein.

   ```
   hostname (config) # hx server containment whitelist <IPorHostname>
   description <description>
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Geben Sie diesen Befehl ein, um die derzeit auf der Whiteliste befindlichen Hosts aufzuführen:

```
hostname (config) # show hx server containment
```

Beispiele

Im folgenden Beispiel wird eine Hostbeschreibung in der Containment Whiteliste auf ein einziges Wort geändert.

```
hostname (config) # hx server containment whitelist testserverhost
description testserver
```

Im folgenden Beispiel wird eine Hostbeschreibung in der Containment Whiteliste auf eine Reihe von Wörtern geändert:

```
hostname (config) # hx server containment whitelist 123.45.6.7 description
“The Group A Test Appliance”
```

Einen Hosts aus der Containment Whiteliste mithilfe der Web-UI entfernen

Um einen Host mit Hilfe der Web-UI aus der Containment Whiteliste zu entfernen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Containment Settings** auf dem **Admin** Menü. Die Containment Settings Seite wird geöffnet.
3. Wählen Sie das Entfernensymbol neben der IP-Adresse oder dem Host, den Sie löschen wollen.

Einen Hosts aus der Containment Whiteliste mithilfe der CLI entfernen

Um einen Host mit Hilfe der CLI aus der Containment Whiteliste zu entfernen:

1. Aktivieren Sie den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Entfernen Sie die IP-Adresse oder den Hostnamen von der Containment Whiteliste.

   ```
   hostname (config) # no hx server containment whitelist <IPorHostname>
   ```

3. Speichern Sie Ihre Einstellungen.

```
hostname (config) # write mem
```

Geben Sie den folgenden Befehl ein, um die derzeit auf der Whiteliste befindlichen Hosts aufzulisten:

```
hostname (config) # show hx server containment
```

Den Containment Freigabecode aktivieren und deaktivieren

Eingedämmte Hosts können nur mit dem Endpoint Security und DMZ-Server kommunizieren, von denen sie verwaltet werden sowie andere in Ihrer Containment-Zulassungsliste definierte Hosts. In seltenen Fällen könnte Ihr eingedämmter Host die Verbindung mit dem Endpoint Security oder DMZ Server verlieren, wodurch Sie daran gehindert werden, den betroffenen Host aus der Eindämmung zu entfernen.

Der Containment Freigabecode gestattet Ihnen, einen Host von der Eindämmung zu entfernen, wenn der auf dem betroffenen Host ausgeführte Endpoint Security Agent nicht mit Endpoint Security kommunizieren kann.

WICHTIG: Der Containment Freigabecode wird nur für Windows Agents Version 28 oder später, mac OS Agents 30 oder später und Linux Agents 34 oder später unterstützt. Er wird nicht für Endpunkte unterstützt, die Windows XP ausführen.

Standardmäßig ist die Containment Freigabecode Funktion für alle Ihre Windows Endpunkte aktiviert, die Endpoint Security Version 28 oder später, macOS Agents 30 oder später und Linux Agents 34 oder später ausführen. Sie können die Containment Freigabecode-Funktion durch die Endpoint Security Web-UI oder API aktivieren und deaktivieren.

Dieser Abschnitt beschreibt:

- Den Containment Freigabecode aktivieren auf der nächsten Seite
- Den Containment Freigabecode deaktivieren auf der nächsten Seite

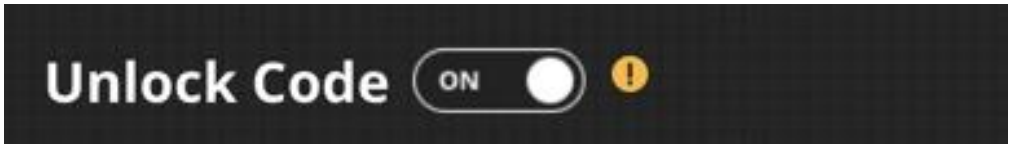
Voraussetzungen

- Admin Zugriff

Den Containment Freigabecode aktivieren

Um den Containment Freigabecode Funktion mit Hilfe der Web-UI zu aktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Containment Settings**.
3. Schalten Sie den **Unlock Code** Schalter auf **ON**.



4. Klicken Sie auf **Save**.

Den Containment Freigabecode deaktivieren

Um den Containment Freigabecode mit Hilfe der Web-UI zu deaktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Containment Settings**.
3. Schalten Sie den **Unlock Code** Schalter auf **OFF**.

4. Klicken Sie auf **Save**.

Endbenutzer über Host-Eindämmung benachrichtigen

Wenn der Netzwerkzugriff eines macOS Host Endpunkts durch Eindämmung eingeschränkt wird, wird der Endbenutzer durch eine Pop-up Nachricht informiert. Die Pop-Up Benachrichtigungen werden je nach Gerätestandort übersetzt und können in den folgenden Sprachen angezeigt werden: Chinesisch (vereinfacht oder traditionell), Englisch, Französisch, Deutsch, Italienisch, Japanisch, Koreanisch, Polnisch, Portugiesisch, Russisch und Spanisch.

Wenn der Netzwerkzugriff eines Windows oder Linux Host Endpunkts durch Eindämmung eingeschränkt ist, wissen Endbenutzer nur, dass Sie keinen Netzwerkzugriff haben. Sie könnten möglicherweise versuchen, den Netzwerkzugriff wiederherzustellen,

indem Sie den Host neu starten oder andere Aktionen ausführen. Durch diese Aktionen könnte Ihre Fähigkeit, den Vorfall zu untersuchen, beeinträchtigt werden.

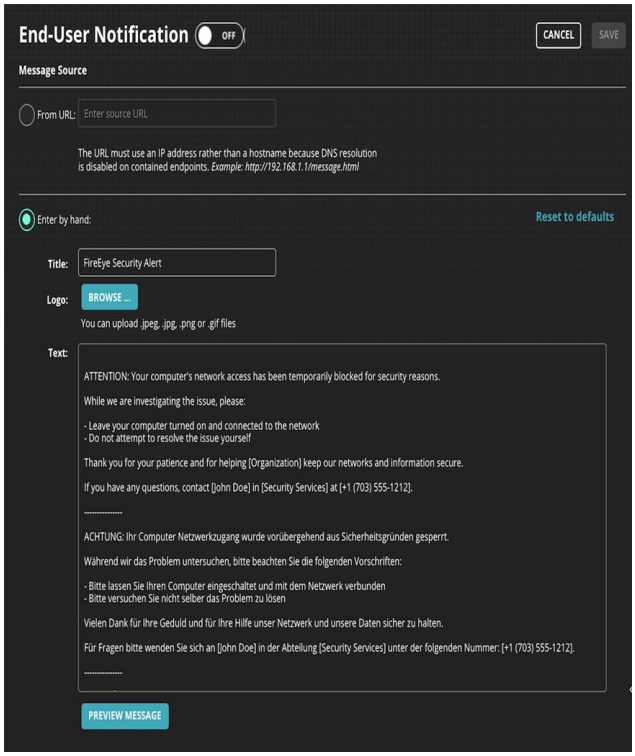
Um Benutzer davon abzuhalten, solche Maßnahmen zu ergreifen, können Sie sie auf zwei Arten darüber informieren, dass die Netzwerkeinschränkung beabsichtigt war.

- Webseitenumleitung: Der Browser des Endbenutzers wird auf eine zentrale Webseite umgeleitet, die die Benachrichtigung bereitstellt. Um diese Methode zu verwenden, müssen Sie eine Webseite, einschließlich der URL auf der Containment Settings Seite in der Endpoint Security Web-UI einrichten und den Server, der die Seite hostet, zu der Containment-Whiteliste hinzufügen. Siehe Endbenutzer über Host-Eindämmung mit Hilfe einer Webseitenumleitung benachrichtigen.
- Direkte Nachricht: Die Agent Software auf dem Host zeigt die Benachrichtigung an den Endbenutzer an. Um diese Methode zu benutzen, müssen Sie die Nachricht auf der Containment Settings Seite eingeben. Siehe Endbenutzer über Host-Eindämmung mit Hilfe einer direkten Nachricht informieren.

Voraussetzungen

- Admin Zugriff

Endbenutzer über Host-Eindämmung mit Hilfe einer Webseitenumleitung benachrichtigen



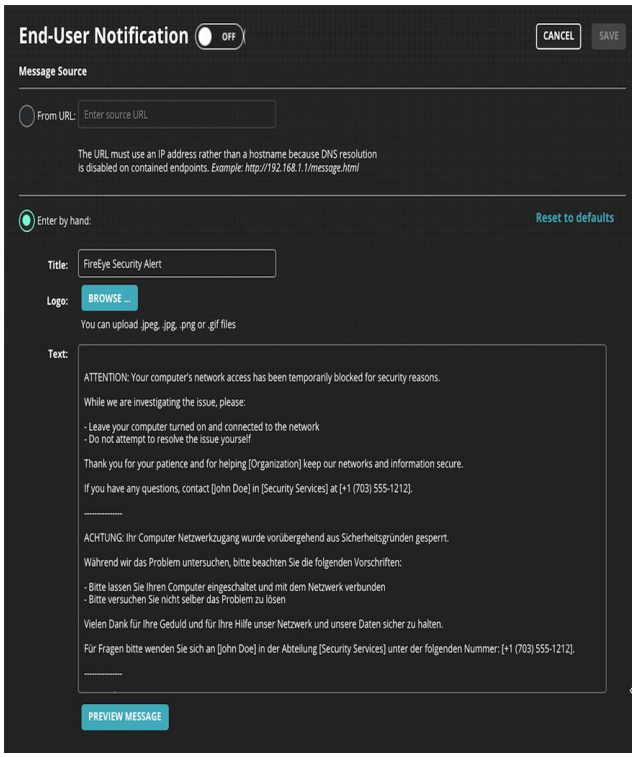
Um Benutzer mit Hilfe einer Webseitenumleitung von der Web-UI zu benachrichten:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Containment Settings** auf dem **Admin** Menü. Die Containment Settings Seite wird geöffnet.
3. Im **End-User Notification** Abschnitt schieben Sie den **End-User Notification** Schalter auf **On**.
4. Wählen Sie **From URL;** und geben Sie die URL der Benachrichtigungs-Webseite in das Textfeld ein.

   Geben Sie eine IP-Adresse und keinen Hostnamen ein. Während der Eindämmung ist DNS Auflöstung auf dem Host deaktiviert.

5. Klicken Sie auf **Save**.

Endbenutzer über Host-Eindämmung mit Hilfe einer direkten Nachricht informieren



Um Benutzer mit einer direkten Nachricht von der Web-UI zu benachrichtigen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Containment Settings** auf dem **Admin** Menü. Die Containment Settings Seite wird geöffnet.
3. Im **End-User Notification** Abschnitt schieben Sie den **End-User Notification** Schalter auf **On**.
4. Wählen Sie **Enter by hand:**
5. Bestimmen Sie einen Titel für die Benachrichtigung im **Title:** Textfeld.
6. (Optional) Fügen Sie ein Logo oder ein anderes grafisches Element zu der Nachricht hinzu. Klicken Sie auf die **Browse** Schaltfläche und wählen Sie eine `*.jpg`, `*.jpeg`, `*.png` oder `*.gif` Datei.
7. Geben Sie den gewünschten Benachrichtigungstext im **Text** Feld ein.

   Eine Standardnachricht ist im Lieferumfang der Endpoint Security Software enthalten. Wenn Sie diese Standardnachricht verwenden, müssen Sie Ihren Firmennamen und Kontaktinformationen aktualisieren. Geben Sie bei der Bereitstellung der Kontaktinformationen eine Telefonnummer oder andere Kontaktmethoden an, für die kein Netzwerkzugriff erforderlich ist.
8. Klicken Sie auf **Preview message**.
9. Klicken Sie auf **Save**.

KAPITEL 7: Host-Endpunkte verwalten

Dieser Abschnitt bietet die Informationen die Sie für die Verwaltung von Hosts und Hostsätzen benötigen.

Ein Host ist ein Computer, ein Server oder ein anderes Endpunktsystem im Netzwerk. Hosts werden auf verdächtige Aktivitäten von der Endpoint Security Software überwacht. FireEye Endpoint Security Agent Software ist auf jedem individuellen Host-Endpunkt installiert. Um die Agent Softwareinstallation auf dem Endpunkt abzuschließen, stellt der Agent eine Verbindung mit einem bereitstellenden Endpoint Security her und wird für die Überwachung bereitgestellt. Nachdem der Agent bereitgestellt wurde, kann der Host auf der Hosts Seite auf der Endpoint Security Web-UI angezeigt werden. Jedem Agent wird eine Agent ID zugewiesen, die seinen Host Endpunkt während der Endpoint Security Verarbeitung identifiziert.

Die Verwaltung von Host Endpunkten umfasst Informationen darüber, Auflösung geklonter Agents, scannen von Malware und Entfernen von Hosts (nach Bedarf) vom Endpoint Security System.

Dieser Abschnitt behandelt die folgenden Themen:

Hosts können auch in Hostsätzen gruppiert werden, um Endpoint Security Funktionalitäten, wie z.B. Containment und Agent-Upgrades anzupassen. Siehe Hostsätze konfigurieren auf Seite 185.

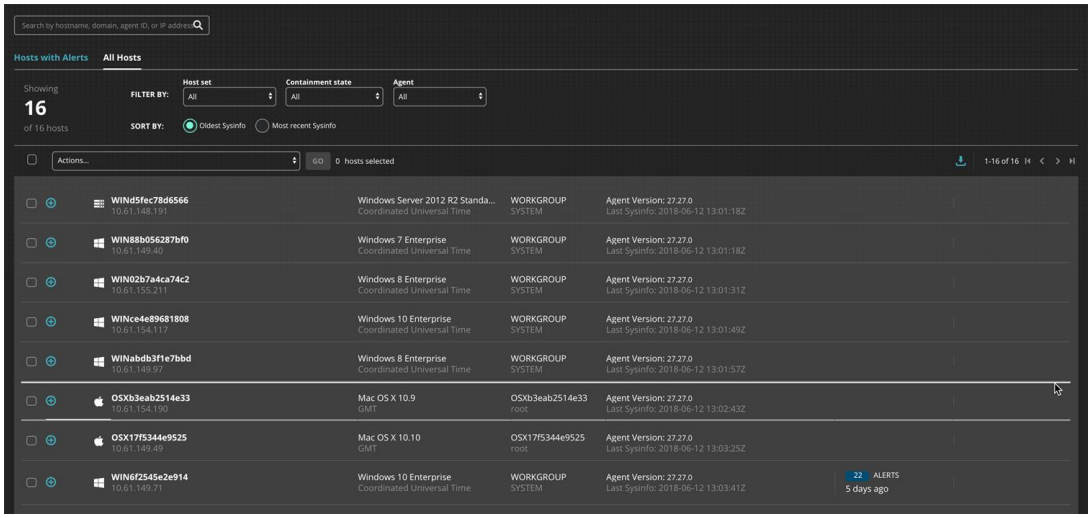
Sie können auch einen Hostsatz mit hochwertigen Hosts erstellen, was Ihnen ermöglicht, die wichtigsten Hosts in Ihrem Unternehmen schnell anzuzeigen. Siehe Hochwertige Hosts identifizieren auf Seite 203.

Hosts finden und anzeigen

Die Hosts Seite ermöglicht Ihnen, den vollständigen Bestand der überwachten Hosts auf Ihrem Netzwerk anzuzeigen und Details über jeden Host abzurufen. Wählen Sie Hosts am oberen Rand der Endpoint Security Web-UI, um auf die **Hosts** Seite zuzugreifen.

Verwenden Sie die Hosts Seite um:

- Hosts nach dem Host mit den neuesten Warnungen, den meisten Warnungen oder den meisten Warnungstypen zu sortieren.
- Die Hostsnach Hostname, Domain, IP-Adresse oder Agent ID mit Hilfe des Suchfeldes am Anfang der Seite zu durchsuchen
- Die Liste der Hosts zu filtern. Verwenden Sie den **Filter By** Abschnitt der Seite, um die Hosts nach Warnungstyp, Hostsatz oder Containment Status zu filtern.
- Verwenden Sie die Download Schaltfläche ( ), um die Liste der Hosts auf eine Durch Trennzeichen getrennte Datei (CSV) herunterzuladen.



Sie können die Hosts Seite als zentralen Punkt für eine Host-basierte Workflow verwenden, einen Host Endpunkt für ein schnelles Drilldown auswählen, und weitere Informationen über ihre Alarme und alle erhaltenen Erfassungsdaten erlangen.

Umfassende Informationen über den Zugriff und die Verwendung dieser Seite finden Sie unter Hosts Menü auf Seite 40.

Geklonte Agents auflösen

Agent IDs werden durch den Endpoint Security verwendet, um jeden Endpunkt zu identifizieren. Geklonte Agents sind FireEye Endpoint Security Agents, die mit dem Endpoint Security mit Hilfe der gleichen Agent-ID bereitgestellt wurden. Wenn geklonte

Agents nicht aufgelöst werden, wird die Kommunikation zwischen dem Endpoint Security und den Host-Endpunkten problematisch. Wenn mehrere Endpunkte die gleiche Agent-ID haben, kann der Endpoint Security einen individuellen Endpunkt nicht eindeutig identifizieren, um Daten- oder Triage-Informationen abzufragen, einzudämmen, zu erfassen oder mit diesen zu kommunizieren.

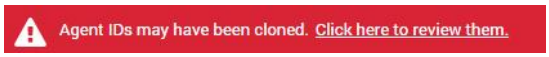
WICHTIG: Damit die Endpoint Security und FireEye Endpoint Security Agent Software ordnungsgemäß kommunizieren können, muss jedem Host-Endpunkt eine einzigartige Agent-ID zugewiesen werden.

Geklonte Agents können versehentlich erstellt werden, wenn einem Golden oder Master-Image eine Agent-ID zugeordnet wird, bevor das Image zur Bereitstellung der Endpoint Security Agent Software verwendet wird. Nach Abschluss des Deployment haben alle Host Endpunkte, auf denen das Image bereitgestellt wurde, die gleiche Agent-ID wie das Golden oder Master-Image. Um die Erstellung eines Golden oder Master-Image mit einer zugewiesenen Agent ID zu vermeiden, lesen Sie "Agents mit Hilfe eines Golden oder Master-Image installieren" im *Endpoint Security Agent Administrationshandbuch*.

Voraussetzungen

- Admin Zugriff

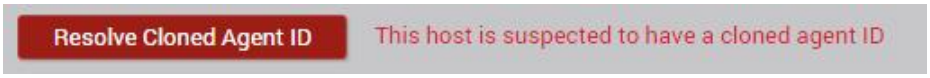
Wenn geklonte Agents vom Endpoint Security identifiziert werden, wird eine rote Nachricht am Anfang der Endpoint Security Web-UI angezeigt.



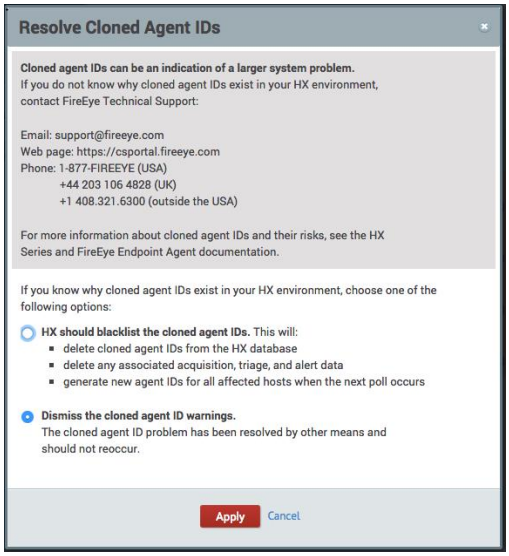
Um geklonte Agent IDs von der Web-UI zu verwalten:

1. Klicken Sie auf **Click here to review them** in der roten Nachricht am Anfang der Endpoint Security Web-UI Seite. Eine Hosts Seite wird angezeigt, die nur die Hosts mit geklonten Agent IDs zeigt.

2. Tun Sie eins der Folgenden:
   - Wählen Sie einen geklonten Host auf der Hosts Seite. Wählen Sie dann **Resolve Cloned Agent ID** im Actions Dropdown-Feld und klicken Sie auf **Go**.
   - Erweitern Sie einen Host, indem Sie auf sein Erweiterungssymbol (⊕) klicken. Der Host Details Abschnitt der Hosts Seite wird mit einer **Resolve Cloned Agent ID** Schaltfläche am Anfang der Seite angezeigt. Klicken Sie auf die **Resolve Cloned Agent ID** Schaltfläche.

   Die Resolve Cloned Agent IDs Tafel wird angezeigt.

3. Wählen Sie eine Option:
   - Die Sperrung der geklonten Agent-ID löscht den Klon von der Endpoint Security Datenbank, sowie alle mit dem Klon verknüpften Aquisitions-, Triage- oder Alarmdaten und bewirkt, dass der Endpoint Security eine neue Agent-ID für den ausgewählten Host-Endpunkt erstellt, wenn sein Endpoint Security Agent die Appliance das nächste Mal abfragt. Weitere Informationen über Agent Abfrage finden Sie unter "Einstellungen für Agent Abfrage konfigurieren" im *Endpoint Security Agent Administrationshandbuch*.
   - Verwerfen der Alarme bedeutet, dass Sie das Problem der geklonten Agents auf andere Weise gelöst haben. Sie könnten diese Option wählen, wenn Sie genau wissen, wie der geklonte Agent erstellt wurde, die geklonte Agent Software vom betroffenen Host Endpunkt entfernt haben und sicher sind, dass der Agent die geklonte Agent ID nicht erneut abfragt.
4. Klicken Sie auf **Apply**.

Wenn Sie nicht wissen, warum geklonte Agent-IDs in Ihrer Endpoint Security Umgebung vorhanden sind, oder wenn Sie zusätzliche Unterstützung benötigen, wenden Sie sich an FireEye Technical Support.

Nach Malware scannen

Benutzer mit Admin oder API Admin Authorisierung können Malware Scans auf Ihren Host-Endpunkten initiieren. Malware Scans sind entweder als Full Scan (Vollständiger Scan) oder Custom Scan (Benutzerdefinierter Scan) konfiguriert. Ein Full Scan umfasst all lokalen und eingebundenen Laufwerke, während ein Custom Scan Ihnen die Möglichkeit bietet, Ordnernamen oder Dateipfade anzugeben.

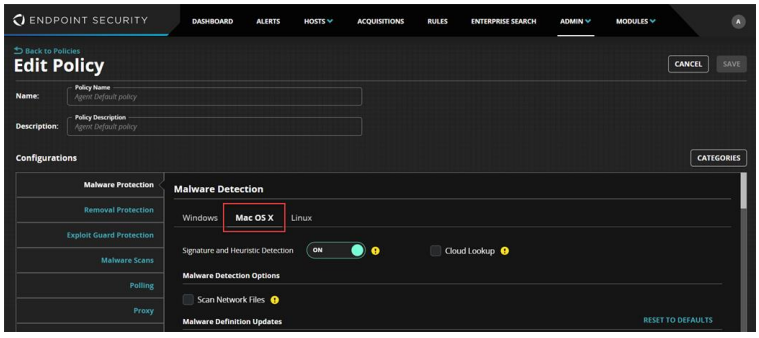
WICHTIG: Der Run a Malware Scan Vorgang wird nur auf macOS und Linux unterstützt.

WICHTIG: Malware Protection muss zuerst in der Agent Richtlinie aktiviert sein, damit diese Funktion funktioniert. Folgen Sie diesen Schritten, um Malware Schutz zu aktivieren.

Malware Schutz für Mac OS X aktivieren

Um Malware Schutz auf einer Agent Richtlinie zu aktivieren:

1. Im **Admin** Menü wählen Sie **Policies**.
2. Klicken Sie unter **Policy Name** auf die Richtlinie, die Sie bearbeiten wollen.
3. In der **Configurations** Gruppe wählen Sie **Malware Protection**.
4. Klicken Sie unter der **Malware Detection** Gruppe auf den **Mac OS X** Tab.
5. Stellen Sie Signature and Heuristic Detection auf **ON**.

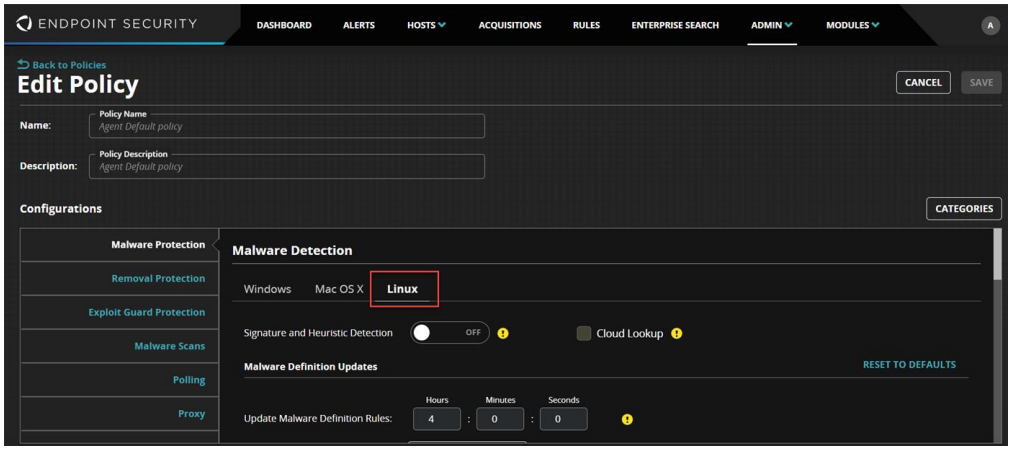


6. Klicken Sie in der oberen rechten Ecke auf **Save**.

Malware Schutz für Linux aktivieren

Um Malware Schutz auf einer Agent Richtlinie zu aktivieren:

1. Im **Admin** Menü wählen Sie **Policies**.
2. Klicken Sie unter **Policy Name** auf die Richtlinie, die Sie bearbeiten wollen.
3. In der **Configurations** Gruppe wählen Sie **Malware Protection**.
4. Klicken Sie unter der **Malware Detection** Gruppe auf den **Linux** Tab.
5. Stellen Sie Signature and Heuristic Detection auf **ON**.



6. Klicken Sie in der oberen rechten Ecke auf **Save**.

Jetzt nach Malware scannen

Um einen Host oder Hostsatz nach Malware zu scannen:

1. Wählen Sie das **Host** Menü am oberen Rand des Bildschirms.
2. Wählen Sie einen Host oder Hostsatz in der Hosts Liste.
3. Auf dem **Actions** Dropdown-Menü wählen Sie **Run a Malware Scan** und klicken Sie auf **Go**.
4. Geben Sie einen Namen für den Scan ein.
5. Wählen Sie entweder **Full Scan** oder **Custom Scan** als die Scantiefe.
6. Wenn **Custom Scan** ausgewählt wurde, legen Sie die Datei oder den Ordnerpfad fest und klicken Sie dann auf **Add**.
7. Klicken Sie auf **Scan Now**, um den Malware Scan auszuführen.

Cancel Scan Now

In Fällen, in denen ein angeforderter Scan einen Anstieg im Ressourcenverbrauch verursacht, kann die Leistung durch den Abbruch eines angeforderten Scan Now Ereignisses für einen Host wiederhergestellt werden.

HINWEIS: Nur Scan Now Ereignisse im REQUESTED Status können abgebrochen werden.

Um einen angeforderten Scan für einen Host abzubrechen:

1. Wählen Sie das **Hosts** Menü am oberen Rand des Bildschirms.
2. Klicken Sie auf das Erweitern Symbol ( ) auf dem macOS-Host, der einen angeforderten Scan hat.
3. Wählen Sie das Kontrollkästchen des angeforderten **Scan Namens**, den Sie abbrechen wollen, aus der Liste der Scan Now Ereignisse.
4. Auf dem **Actions** Dropdown-Menü wählen Sie **Cancel Scan** und klicken Sie auf **Go**.
5. Wählen Sie **Proceed**, um den Vorgang zu bestätigen.

Host Alterungsintervalle festlegen

Host Endpunkte senden keine Daten mehr oder reagieren nicht mehr auf ihren bereitstellenden Endpoint Security wenn sie inaktiv werden.

Sie können Host Alterungsperioden festlegen. Standardmäßig altert (entfernt) die Endpoint Security Software inaktive Host Endpunkte automatisch, nachdem ihre definierten Alterungsperioden abgelaufen sind.

Sie können Host Alterung aktivieren oder deaktivieren und die Host Alterungsperioden ändern. Zusätzlich können Sie Host Endpunkte jederzeit löschen. Siehe Hosts entfernen auf Seite 183.

HINWEIS: Wenn Host-Endpunkte gelöscht werden—gleichgültig ob automatisch oder manuell—, löscht die Endpoint Security Software auch automatisch alle Triagen und Datenerfassungen, die mit den gelöschten Endpunkten verbunden sind.

Host Alterungseinstellungen überprüfen

Sie können Host Alterungseinstellungen mit Hilfe der Endpoint Security Web-UI oder der CLI überprüfen.

Voraussetzungen

- Administratorzugriff

Host Alterungseinstellungen mit Hilfe der Web UI überprüfen

Um Host Alterungseinstellungen mit Hilfe der Web UI zu überprüfen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt. Die Host Alterungseinstellungen werden im Host Aging Feld auf dieser Seite angezeigt.

Host Alterungseinstellungen mit Hilfe der CLI überprüfen

Um Host Alterungseinstellungen mit Hilfe der CLI überprüfen

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Listen Sie Host Alterungseinstellungen auf:

   ```
   hostname (config) # show hx agent aging
   ```

   Nachfolgend finden Sie eine Beispielausgabe dieses Befehls:

   ```
   HX Agent Aging values:

   Enable: enabled
   Inactive Period: 90 days
   New Orphan Period: 1 day
   ```

Host Alterungseinstellungen festlegen

Die folgende Tabelle fasst die verfügbaren Host Alterungseinstellungen zusammen.

Einstellung	Beschreibung
Host Aging Enabled	Standardmäßig ist Host Alterung aktiviert. Sie können Host Alterung mit Hilfe der Endpoint Security Web-UI oder der CLI deaktivieren. Siehe Host Alterung aktivieren oder deaktivieren auf der nächsten Seite.

Einstellung	Beschreibung
Host Aging Intervall	Das Alterungsintervall von Host Endpunkten auf dem System. Host Endpunkte, die für dieses Intervall inaktiv sind, werden gelöscht. Das Host Alterungsintervall kann mit Hilfe der Web-UI oder der CLI eingestellt werden. Web-UI Bereich: 1 bis 365 Tage CLI Bereich : 86400 bis 31536000 Sekunden (1 Tag bis 365 Tage) Standard: 7776000 Sekunden (90 Tage) Siehe Das Host Alterungsintervall einstellen auf Seite 181.
Orphaned Host Aging Interval	Das Alterungsintervall, das definiert, ob ein Host Endpunkt verwaist ist. Verwaiste Host Endpunkte sind Endpunkte, die innerhalb dieses Intervalls auf anfängliche Endpoint Security System Informationsanfragen nicht reagieren. Das verwaiste Host Alterungsintervall kann nur mit Hilfe der CLI eingestellt werden. CLI Bereich: 60 bis 31536000 Sekunden (1 Minute bis 365 Tage) Standard: 1209600 Sekunden (14 Tage) Siehe Das Alterungsintervall von verwaisten Hosts einstellen auf Seite 182.
Dashboard Host Inactivity Interval	Das Intervall, nach dem inaktive Hosts in die inaktive Host Zählung auf dem Web-UI Dashboard aufgenommen werden. Diese Einstellung kann nur mit Hilfe der Web-UI festgelegt werden. Web-UI Bereich: 1 bis 365 Tage Standard: 30 Tage Siehe Das Host Inaktivitätsintervall auf dem Dashboard einstellen auf Seite 183.

Host Alterung aktivieren oder deaktivieren

Sie können Host Endpunktalterung mit Hilfe der Endpoint Security Web-UI oder der CLI aktivieren oder deaktivieren.

Voraussetzungen

- Administratorzugriff

Host Alterung mit Hilfe der Web-UI aktivieren

Um Host Alterung mit Hilfe der Web-UI zu deaktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt.
3. Im Host Aging Feld auf der Aging Settings Seite bestimmen Sie ein Alterungsintervall im **Delete hosts from the database after:** Feld. Gültige Werte liegen zwischen 1 bis 365 Tagen. Dies stellt das Alterungsintervall ein und aktiviert es.
4. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

Um Standardeinstellungen wiederherzustellen, klicken Sie auf **Reset to default** und klicken Sie dann auf **Save**. Wenn Sie auf **Cancel** klicken, gibt Endpoint Security Einstellungen auf die zuletzt gespeicherten Werte zurück.

Host Alterung mit Hilfe der CLI aktivieren

Um Host Alterung mit Hilfe der CLI zu aktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Das Host Alterungsintervall aktivieren:

   ```
   hostname (config) # hx agent aging enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Host Alterung mit Hilfe der Web-UI deaktivieren

Um Host Alterung mit Hilfe der Web-UI zu deaktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt.
3. Im Host Aging Feld auf der Aging Settings Seite wählen Sie die **No auto-deletion; I will delete hosts manually** Option.
4. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

Um Standardeinstellungen wiederherzustellen, klicken Sie auf **Reset to default** und klicken Sie dann auf **Save**. Wenn Sie auf **Cancel** klicken, gibt Endpoint Security Einstellungen auf die zuletzt gespeicherten Werte zurück.

Host Alterung mit Hilfe der CLI deaktivieren

Um Host Alterung mit Hilfe der CLI zu deaktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Das Host Alterungsintervall deaktivieren:

   ```
   hostname (config) # no hx agent aging enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Das Host Alterungsintervall einstellen

Sie können das Host Alterungsintervall mit Hilfe der Web-UI oder der CLI einstellen.

Voraussetzungen

- Administratorzugriff

Das Host Alterungsintervall mit Hilfe der Web UI einstellen

Um das Host Alterungsintervall mit Hilfe der Web UI einzustellen und zu aktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt.
3. Im Host Aging Feld auf der Aging Settings Seite bestimmen Sie ein Alterungsintervall im **Delete hosts from the database after:** Feld. Gültige Werte liegen zwischen 1 bis 365 Tagen. Dies stellt das Alterungsintervall ein und aktiviert es.
4. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

Um Standardeinstellungen wiederherzustellen, klicken Sie auf **Reset to default** und klicken Sie dann auf **Save**. Wenn Sie auf **Cancel** klicken, gibt Endpoint Security Einstellungen auf die zuletzt gespeicherten Werte zurück.

Das Host Alterungsintervall mithilfe der CLI einstellen

Um das Host Alterungsintervall mit Hilfe der CLI einzustellen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Stellen Sie das Host Alterungsintervall ein:

   ```
   hostname (config) # hx agent aging inactive-period <seconds>
   ```

   wobei <seconds> die Anzahl der Sekunden für die Alterungsperiode für Host Endpunkte ist. Der Standard ist 7776000 Sekunden (90 Tage). Gültige Werte liegen zwischen 86400 (einTag) und 31536000 Sekunden (ein Jahr).

   Um dieses Intervall auf seine Standardeinstellung zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   hostname (config) # no hx agent aging inactive-period
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Das Alterungsintervall von verwaisten Hosts einstellen

Sie können das Alterungsintervall von verwaisten Hosts mit Hilfe der CLI einstellen. Verwaiste Host Endpunkte sind Endpunkte, die innerhalb dieses Intervalls auf anfängliche Endpoint Security System Informationsanfragen nicht reagieren.

Voraussetzungen

- Administratorzugriff

Das Host Alterungsintervall mithilfe der CLI einstellen

Um das verwaiste Host Alterungsintervall mit Hilfe der CLI einzustellen.

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Stellen Sie das Host Alterungsintervall ein:

   ```
   hostname (config) # hx agent aging new-orphan-period <seconds>
   ```

   wobei <seconds> die Anzahl der Sekunden für die Alterungsperiode für verwaiste Hosts ist. Die Standardeinstellung ist 86400 Sekunden (ein Tag). Gültige Werte liegen zwischen 86400 (einTag) und 31536000 Sekunden (ein Jahr).

   Um dieses Intervall auf seine Standardeinstellung zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   hostname (config) # no hx agent aging new-orphan-period
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Das Host Inaktivitätsintervall auf dem Dashboard einstellen

Sie können die Endpoint Security Web-UI verwenden, um den Intervall einzustellen, nach dem inaktive Hosts in die Zählung inaktiver Hosts auf dem Web-UI Dashboard eingeschlossen sind.

Voraussetzungen

- Administratorzugriff

Das Dashboard Host Inaktivitätsintervall mit Hilfe der Web-UI einstellen

Um das Dashboard Host Inaktivitätsintervall mit Hilfe der Web-UI zu einstellen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt.
3. Im Host Aging Feld auf der Aging Settings Seite bestimmen Sie ein Alterungsintervall im **Show on the dashboard when hosts are inactive for:** Feld. Gültige Werte liegen zwischen 1 bis 365 Tagen.
4. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

Um Standardeinstellungen wiederherzustellen, klicken Sie auf **Reset to default** und klicken Sie dann auf **Save**. Wenn Sie auf **Cancel** klicken, gibt Endpoint Security Einstellungen auf die zuletzt gespeicherten Werte zurück.

Hosts entfernen

Wenn Ihr Unternehmen Host-Endpunkte deaktiviert, neu organisiert oder Reimaging durchführt, müssen Sie den alten Agent und Host IDs verarbeiten. Sie können spezielle Hostsätze erstellen um sie von Vorgängen auszuschließen. FireEye empfiehlt, dass Sie die alten Identitäten vollständig vom Endpoint Security System entfernen.

Administratoren und Operatoren können Hosts vollständig von der Endpoint Security Datenbank entfernen. Wenn Sie einen Host von der Datenbank entfernen, entfernen Sie auch alle zugehörigen Alarme und Akquisitionen, sowie die Zugehörigkeit des Host Endpunkts in Hostsätzen und seinen gesamten Aufrüstungs- und Eindämmungsverlauf. Wenn Sie alle Hosts von einem Hostsatz löschen, bleibt der Hostsatz bestehen, enthält jedoch keine Elemente.

Wenn Sie versehentlich einen aktiven Host-Endpunkt entfernen, wird der Endpunkt erneut im System angezeigt, wenn der Endpoint Security das nächste Mal nach Agents sucht, die

aus der Endpoint Security Web-UI entfernt wurden, aber noch immer Abfragen durchführen (normalerweise innerhalb von 15 Minuten).

Wenn ein entfernter Host in dem System wiederhergestellt wird, werden die früheren Akquisitionsdaten und Agent Aktivitätsverlauf nicht erneut angezeigt. Sie könnten Warnungen sehen, die zuvor gelöscht wurden. Dies liegt daran, dass beim Entfernen des Hosts aus dem System die Informationen darüber, welche seiner Warnungen gelöscht wurden, ebenfalls entfernt wurden.

Voraussetzungen

- Admin, Analyst, Senior Analyst oder Investigator Berechtigungen

Um Hosts mit Hilfe der Web UI zu entfernen:

1. Wählen Sie **Hosts** am oberen Rand der Endpoint Security Web-UI, um auf die Hosts Seite zuzugreifen.
2. Wählen Sie das Kontrollkästchen links neben jedem Host, den Sie entfernen wollen.
3. Auf dem Actions Menü wählen Sie **Delete host** und klicken Sie dann auf **Go**.
4. Klicken Sie auf **Delete**, um die Entfernung des Host Endpunkts vom Endpoint Security System zu bestätigen.

   Die Hosts und alle zugehörigen Akquisitionen und Alarme werden von der Endpoint Security Datenbank entfernt.

KAPITEL 8: Hostsätze konfigurieren

Mehrmals am Tag liefern Agents der Host Endpunkte Ihre Unternehmens Informationen über ihre Hosts und empfangen Aufträge von der Endpoint Security Appliance.

Sie müssen möglicherweise die Aufgaben nicht auf allen Hosts ausführen oder wollen nicht jedes Mal individuelle Hosts festlegen, wenn Sie eine Aufgabe auf mehr als einem Host ausführen müssen. Viele Endpoint Security Funktionen laufen auf persistente Gruppen von Hosts (Hostsätzen) oder schließen diese aus.

Es gibt zwei Arten von Hostsätzen:

- Statische Sätze: Dies sind stabile Gruppen von Hosts, die Sie direkt erstellen und bearbeiten. Statische Sätzen ändern, wenn Sie Hosts hinzufügen oder entfernen. Weitere Informationen finden Sie unter Statische Sätze verstehen.
- Standardsätze: Dies sind dynamische Gruppen von Hosts, die durch von Ihnen festgelegte Filterkriterien definiert sind. Standardsätze ändern sich, wenn geeignete Hosts bereitgestellt oder gelöscht werden und wenn Sie ihre Filterkriterien ändern. Weitere Informationen finden Sie unter Standardsätze verstehen.

Verwenden Sie die Host Sets Seite, um folgendes zu tun:

- Hostsätze erstellen und verwalten
- Listen von Sätzen anzeigen und sortieren, die Ihr Unternehmen bereits erstellt hat
- Die Hosts in einem Satz anzeigen
- Details über Hosts in einem Satz anzeigen
- Richtlinien auf Hostsätze anwenden
- Listen von Hosts als `*.csv` Dateien herunterladen
- Hostlisten nach einem bestimmten Host oder Hosts durchsuchen

Informationen über Agent Richtlinien finden Sie unter "Agent Richtlinienservice" im "Agent Konfiguration" Abschnitt des *Endpoint Security Agent Administrationshandbuch*.

Lesen Sie die folgenden Abschnitte, um zu lernen, mit Hostsätzen zu arbeiten:

- Verwendungen von Hostsätzen
- Hostsätze benennen
- Statische Sätze verstehen
- Standardsätze verstehen
- Statische Sätze erstellen
- Standardsätze erstellen
- Hostsätze mit Hilfe der Web-UI bearbeiten
- Hostsätze mit Hilfe der Web-UI löschen

Das Zeitlimit für die Inaktivität der Endpoint Security Web-UI wird ignoriert, wenn die Host Sets Seite im Browser geöffnet bleibt.

Wenn FireEye Endpoint Security Agents Änderungen vom Endpoint Security erfassen, erfassen sie Änderungen an Hostsätzen, bevor Sie Änderungen an Richtlinien und Konfigurationsdateien für diese Hostsätze erfassen. Änderungen an Hostsätzen werden auf einen Agent angewendet, wenn eine System Informationsabfrage (sysinfo) stattfindet. Sie können die Rate, mit der die Systemabfrage geschieht, erhöhen, indem Sie die sysinfo Abfragezeit verringern, aber mit dem Risiko, dass die Leistung Ihres Agent auf Ihren Host Computern beeinträchtigt wird. Weitere Informationen finden Sie unter "Abfrage konfigurieren" und "Leistungsaspekte" im *Endpoint Security Agent Administrationshandbuch*.

Verwendungen von Hostsätzen

Administratoren und Operatoren können Hostsätze für eine Vielzahl von Vorgängen erstellen, speichern, bearbeiten und löschen, z. B. Eindämmungseinstellungen und Agent Upgrades konfigurieren. Andere Benutzer können Gruppen von Hosts für die Recherche zusammenstellen und `*.csv` Dateien für die Berichterstattung herunterladen, obwohl diese Benutzer diese Gruppen nicht als Hostsätze erstellen, speichern, bearbeiten oder löschen können.

Mögliche Verwendungen von Hostsätzen sind:

- **Agent Upgradesätze**—Verwenden Sie Hostsätze, um eine spezifische Gruppe von Hosts aufzurüsten, während andere Hosts Systemladung oder andere organisatorischen Prioritäten unterstützen. Agent Upgrade Sätze können aus Agents auf Hosts bestehen, die sich in der gleichen geografischen Region oder spezifischer funktionellen Abteilung befinden, die dieselbe Agentversion ausführen, oder die

sensible oder kritische Geräte sind.

- **Richtlinien anwenden**—Sie können Richtlinien auf eine spezifische Gruppe von Hosts anwenden und die Reihenfolge priorisieren, in der die Richtlinien angewendet werden sollen. Weitere Informationen finden Sie unter Einem Hostsatz eine Richtlinie zuweisen auf Seite 198.
- **Ausschlusssätze**— Verwenden Sie Hostsätze, um Agents ausdrücklich von Vorgängen auszuschließen. Sie können beispielsweise Ausschlusssätze verwenden, um Domain Controller, andere Spezialserver, Executive Laptops und andere vertrauliche Hosts vor Störungen während Eindämmungsaktionen und Agent Aktualisierungen zu schützen.
- **Berichtssätze**—Kombinieren und laden Sie einen Bericht auf einem Hostsatz herunter und teilen Sie Informationen über die Hosts in dem Satz. Beispielsweise könnten Sie Host Endpunkte gruppieren, die ihren Status während eines bestimmten Zeitintervalls gemeldet haben.

Hostsätze benennen

Sie können Hostsätze jederzeit benennen und umbenennen.

Wenn Sie einen Hostsatz mit einem neuen Namen speichern, wird der Hostsatz einfach umbenannt. Alle Änderungen, die Sie vorgenommen haben, werden auf dem Hostsatz mit dem neuen Namen gespeichert.

Es ist eine gute Idee, Hostsätze nach Ihrem Zweck zu benennen. Folgen Sie diesen Namenkonventionen:

- Satznamen können Groß- und Kleinbuchstaben, Zahlen und Unterstriche enthalten, aber keine Sonderzeichen.
- Leerzeichen werden in Unterstriche konvertiert.
- Satznamen werden nach 256 Zeichen abgeschnitten.

Namen, die mit Domain- oder Filternamen identisch sind, können verwirrend sein. Vermeiden Sie Verwirrung, indem Sie spezifischere Namen wählen.

Akzeptable Namen:

- QA_Windows7_workstations
- Chicago_Office
- Executive_Laptops_Ann_Arbor

Schlechte Namen:

- QANet oder hr.lawrencedomain.com (Namen, die mit einem der Windows Domainnamen Ihrer Organisation übereinstimmen)
- Windows 7 Enterprise (ein Name, der dem eines Betriebssystems und Patch entspricht)
- Seattle R&D (ein Name, der das kaufmännische Und-Sonderzeichen enthält).

Statische Sätze verstehen

Statische Sätze sind Gruppen von Hosts, die Sie erstellen und bearbeiten, indem Sie Hosts mithilfe ihrer IP-Adressen oder Hostnamen direkt hinzufügen und entfernen.

Sie können Hosts nur dann zu einem statischen Satz hinzufügen, wenn die Hosts bereits bereitgestellt wurden.

Die Mitgliedschaft in einem statischen Satz ist stabil. Die Mitgliedschaft ändert sich nur, wenn Sie den Satz zum Hinzufügen oder Entfernen von Hosts bearbeiten.

Mit statischen Sätzen können Sie kleine Gruppen von Hosts definieren und steuern, für die Sie nicht einfach einen dynamischen (Standard-) Hostsatz erstellen können. Selbst wenn sich der Hostname oder die IP-Adresse eines Hosts ändert, bleibt der Host Endpunkt Teil des Hostsatzes bestehen.

Diese Stabilität erfordert, dass Sie diese Sätze aktiv verwalten.

- Wenn Sie einen Host Endpunkt neu abbilden und einen neuen Agent darauf installieren, denken Sie daran, die vorherige Agent ID auf die neue Agent ID in ein allen statischen Sätzen zu ändern, in denen dieser Host Mitglied war. Andernfalls wird der neu abgebildete Host möglicherweise nicht ordnungsgemäß in Vorgänge ein- oder ausgeschlossen.
- Wenn Sie eine statische Gruppe erstellen oder bearbeiten, empfiehlt FireEye, dass Sie eine `*.csv` Datei ihrer Satzmitgliedschaft herunterladen. Sie können diese `*.csv` Dateien als Referenzen verwenden um sicherzustellen, dass diese Sätze im Laufe der Zeit weiterhin die richtigen Hosts enthalten. Sie können diese `*.csv` Dateien auch referenzieren, wenn Sie verlorengegangene statische Sätze neu erstellen müssen.

  Endpoint Security bietet keine **Save As** oder **Copy** Funktion. Wenn Sie einen Hostsatz mit einem neuen Namen speichern, wird der Hostsatz einfach umbenannt.

Standardsätze verstehen

Standardsätze sind dynamisch. Sie bestehen aus Gruppen von Hosts, die durch Filterkriterien erstellt wurden. Die Beziehungen zwischen den gefilterten Gruppen in einem Standardsatz können manipuliert werden, so dass der Hostsatz weiter nach Kombinationen von Gruppen, Schnittpunkten von Gruppen oder dem relativen Komplement von Gruppen filtert. Standardsätze werden automatisch ausgefüllt, wenn Agents nach der Installation auf einem Host Endpunkt zum ersten Mal bereitgestellt werden.

Die Mitgliedschaft in einem Standardsatz ändert sich, wenn Folgendes geschieht:

- Ein neuer berechtigter Host wird bereitgestellt
- Filterkriterien werden geändert
- Mitglieder werden direkt hinzugefügt oder entfernt

Standardsätze können von Vorteil sein, wenn Sie eine der folgenden Aktionen ausführen möchten:

- Große Sets erstellen, die aktuelle und zukünftige Hosts auf von Ihnen festgelegten Kriterien basierend, automatisch einschließen und ausschließen, sodass Sie neue Hosts nicht manuell hinzufügen oder ausschließen müssen
- Mit einer großen Anzahl von Hosts arbeiten, je nach den Kriterien, die Sie anpassen.
- Gruppen von Hosts von einer größeren Gruppe von Hosts, auf zusätzlichen Kriterien basierend ausschließen (zum Beispiel können Sie Hosts mit einer früheren Agent Version ausschließen, die keine bestimmte Version des Betriebssystems ausführen)

Mit Standardsätzen können Sie komplexe Hostsammlungen erstellen und bearbeiten. Sie können Standardgruppen erstellen, um Agent Metadaten mit Hilfe unterschiedlicher Filterkriterien zu durchsuchen:

- Vorhandene Hostsätze. Dies sind statische oder Standard Hostsätze, die Sie in einem anderen Satz kombinieren. Solche Sätze werden *eingebettete Sätze* genannt. Sie könnten beispielsweise einen Satz einbetten, um eine kleinere, spezifische Gruppe von Hosts, die Sie bereits identifiziert haben, ein- oder auszuschließen.

Durch das Einbetten von Sätzen können Sie Zeit beim Erstellen und Verwalten von Gruppen sparen, die Feinabstimmung von Beziehungen zwischen Gruppen von Hosts und die Berichterstellung ermöglichen.

Behalten Sie den Überblick darüber, wo Sie Hostsätze einbetten. Die Mitgliedschaft eines Hostsatzes ändert sich, wenn Sie seine eingebetteten Hostsätze bearbeiten oder löschen.

Das Einbetten von mehr als 10 Hostsätzen kann die Systemleistung beeinträchtigen. FireEye empfiehlt, die Einbettung von mehr als 10 Sätzen in einem Hostsatz zu vermeiden.

Auf der Host Sets Seite wird ein Sternchen (*) angezeigt, nachdem der Hostsatzname eines Hostsatzes angezeigt wird, der in einem anderen Hostsatz eingebettet ist.

- Filter basierend auf Geschäftskriterien. Beispielsweise kann eine Gruppe gebildet werden, indem alle bereitgestellten Hosts nach Agent Version, Windows Domain, Betriebssystem, Patch- oder Bit-Ebene, Zeitzone, Hostname, letzte Sysinfo oder Subnetz gefiltert werden.
- Ausdrücke in Form von Suchbegriffen, die Sie entweder direkt in Regex oder in CIDR-Notation eingeben. Zum Beispiel Subnetz oder Windows Domänen.

Endpoint Security unterstützt keine **Save As** oder **Copy** Funktion. Wenn Sie einen Hostsatz mit einem neuen Namen speichern, wird der Hostsatz einfach umbenannt. Wenn der Hostsatz in einen anderen Hostsatz eingebettet wurde, spiegelt die Mitgliedschaft des anderen Hostsatzes die vorgenommenen Änderungen und den neuen Namen des Hostsatzes wieder.

Statische Sätze erstellen

Verwenden Sie die **Set Manager** Tools auf der Host Sets Seite in der Endpoint Security Web-UI, um statische Sätze zu erstellen.

Voraussetzungen

- Admin oder Operator Zugriff

Um einen statischen Satz zu erstellen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.

3. Bewegen Sie den Cursor über die **Create Host Set** Schaltfläche in der oberen rechts auf der Seite und wählen Sie **Using static list**.

   Eine Liste aller bereitgestellten Hosts füllt den All Hosts Bereich links auf der Create Host Set Static List Seite aus.

4. Geben Sie einen Namen in **Set Name** ein. Siehe Hostsätze benennen auf Seite 187
5. Suchen Sie die Hosts, die in Ihren Satz aufgenommen werden sollen, indem Sie in der All Hosts Liste nach ihnen suchen.
   - Um nach einem oder mehreren Hosts nach IP-Adresse, Subnetz, Hostname oder Datum zu suchen, geben Sie vollständige oder teilweise Informationen über den Host oder die Gruppe von Hosts ein, die Sie im **Search by hostname, IP, or date** Feld finden wollen.

     Wenn Sie beispielsweise Hosts auf dem 172.20 Netzwerk hinzufügen wollen, geben Sie 172.20 als einen Suchbegriff ein.
6. Wählen Sie den Host im linken Bereich und klicken Sie dann auf **Add** oder ziehen Sie den ausgewählten Host in den mittleren Abschnitt. Benutzen Sie **Strg-klick**, um mehr als einen Host auszuwählen.

   Sie können die Umschalttaste nicht verwenden, um einen Bereich von Hosts auszuwählen.

   Wenn Sie einen Host im zentralen Bereich auswählen, werden detaillierte Informationen über diesen Host in dem Abschnitt auf der rechten Seite angezeigt. Sehen Sie Host Details auf Seite 65 für Details.

7. Um einen Host von dem Satz zu entfernen, wählen Sie den Host im mittleren Bereich und klicken Sie dann auf **Remove**.
8. (Optional) Laden Sie eine `*.csv` Datei mit Informationen zu den Hosts in dem Satz herunter. Klicken Sie auf das **Download** Symbol am oberen Rand des zentralen Bereichs. Sie können die `*.csv` Dateien als Referenz für die Erstellung verlorengegangener Sätze verwenden.
9. Klicken Sie auf die **Create** Schaltfläche am oberen Rand der Seite, um Ihren statischen Hostsatz zu erstellen und zu speichern.

Standardsätze erstellen

Sie können Standardsätze mit Hilfe von Endpoint Security Set Builder Tools und Funktionsbereichen auf der **Create Standard Set** Seite erstellen und bearbeiten:

Im Allgemeinen erstellen Sie Hostgruppen, indem Sie die Liste der bereitgestellten Hosts mithilfe der Filter und Filterkriterien Bereiche filtern. Der Set Navigator zeigt die Anzahl

der Hosts, die Ihre Kriterien erfüllen, im blauen Kreis an. Ziehen Sie den blauen Kreis im Set Navigator auf den Result Set Kreis im Set Visualizer. Verwenden Sie schließlich den Visualizer, um Gruppen von Hosts zu kombinieren und ihre Beziehungen anzupassen.

Sie können einen Hostsatz erstellen, der nur einen Host beinhaltet. Dadurch können Sie diesen Host für spezielle Fälle verwalten (z.B. um eine benutzerdefinierte Richtlinie anzuwenden).

Weitere Informationen und Anweisungen zum Erstellen von Standardsätzen finden Sie unter:

- Einen Standardsatz mit Hilfe von Filtern erstellen
- Einen Standardsatz mit Hilfe von Filterausdrücken erstellen
- Hostsätze in eine Hostgruppe für einen Standardsatz einbetten
- Beziehungen zwischen Hostgruppen in einem Standardsatz manipulieren

Voraussetzungen

- Admin oder Operator Zugriff

Einen Standardsatz mit Hilfe von Filtern erstellen

Die folgenden Filter sind im **Filters** Bereich verfügbar:

- **SAVED HOST SETS** ermöglicht Ihnen, auf Hostsätzen zu filtern, die Sie bereits erstellt haben
- **All Hosts** ermöglicht Ihnen, nach allen Hosts zu filtern, die vom Endpoint Security verwaltet werden.
- **Agent Version** ermöglicht Ihnen, nach der Agentversion zu filtern
- **Domain** ermöglicht Ihnen, nach der Domain zu filtern
- **Active Directory: Domain Components** ermöglicht Ihnen, nach den Domänenkomponenten zu filtern, die sich derzeit in der Umgebung befinden
- **Active Directory: Organizational Units** ermöglicht Ihnen, nach den Organisationseinheiten zu filtern, die sich derzeit in der Umgebung befinden
- **Active Directory: Common Names** ermöglicht Ihnen, nach den allgemeinen Namen in der Umgebung mit Hilfe von regulären Ausdrücken zu filtern
- **OS & Patch** ermöglicht Ihnen, nach dem Betriebssystem und der Patchebene zu filtern
- **Bit level** ermöglicht Ihnen, nach der Bitanzahl (32-bit oder 64-bit) des Hosts zu filtern

- **Cloud Provider** ermöglicht es Ihnen, Cloud-Hosts nach dem Anbieter zu filtern
- **Timezone** ermöglicht Ihnen, nach der Zeitzone zu filtern
- **Subnet** ermöglicht Ihnen, nach Host Subnetzen zu filtern
- **Hostname** ermöglicht Ihnen nach Hostnamen zu filtern
- **Last Sysinfo** ermöglicht Ihnen, nach dem letzten Datum zu filtern, an dem eine sysinfo Aufgabe für den Host ausgeführt wurde. Sysinfo Aufgaben werden in regelmäßigen Abständen ausgeführt und übertragen Informationen vom Endpoint Security Agent auf Endpoint Security.

Wenn Sie einen Filter auswählen, könnten zusätzliche Filterkriterien im Filter Criteria Bereich angezeigt werden:

- Spezifische Filterkriterien für den Filter, den Sie ausgewählt haben. Wählen Sie einen oder mehrere dieser Optionen, um die in einer Hostgruppe eingeschlossenen Hosts weiter zu filtern.
- Ein Feld für die direkte Eingabe von Ausdrücken, um Subnet oder Hostname Filter zu suchen.
- Ein **Create Expression** Link, der Ihnen ermöglicht, Ausdrücke einzugeben, um die Domain, OS & Patch, Timezone, Subnet, Hostname oder Last Sysinfo Filter zu suchen.
- Suchoptionen für Hosts, die in optionalen Zeitbereichen (Last Sysinfo Filter) überprüft werden oder nicht.

Um Filter für die Erstellung eines Standardsatzes zu verwenden:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.
3. Bewegen Sie den Cursor über die **Create Host Set** Schaltfläche und wählen Sie **Using set builder**.

   Die Create Standard Set Seite wird angezeigt.
4. Im Filters Abschnitt am unteren Seitenrand wählen Sie einen Filter in der Liste auf der linken Seite.

   Kriterien für den Filter werden in der Mitte des Filter Criteria Bereichs angezeigt. Dies könnte Bereiche einschließen, in denen Sie Ausdrücke für den Filter eingeben können. Weitere Informationen finden Sie unter Einen Standardsatz mit Hilfe von Filterausdrücken erstellen.
5. Legen Sie Ihre Filterkriterien fest.

   Der Set Navigator Kreis auf der rechten Seite zeigt die Hosts an, die mit den ausgewählten Filtern übereinstimmen. Dies ist die Hostgruppe.

6. Ziehen Sie den Set Navigator Kreis auf den Result Set Kreis.

   Sie haben jetzt einen Standardsatz erstellt, der eine Hostgruppe enthält.

7. Definieren Sie Hostgruppen mit Hilfe der Filter in den Filters and Filter Criteria Abschnitten. Ziehen Sie den Set Navigator Kreis jedes Mal auf den Set Visualizer, um eine weitere Hostgruppe zu dem Standardsatz hinzuzufügen.

   Zusätzliche Informationen über Filter und Filterausdrücke finden Sie unter Hostsätze in eine Hostgruppe für einen Standardsatz einbetten und Einen Standardsatz mit Hilfe von Filterausdrücken erstellen.

8. Wenn das Hinzufügen von Hostgruppen zum Standardsatz abgeschlossen ist, geben Sie ihre Beziehungen im Set Visualizer an. Weitere Informationen finden Sie unter Beziehungen zwischen Hostgruppen in einem Standardsatz manipulieren.

9. Geben Sie einen Namen im Set Name Feld ein und klicken Sie dann auf **Create**.

   Der Standardsatz, der eine oder mehrere Hostgruppen enthält, wird erstellt.

Um einen Host von einem Standardsatz zu entfernen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.
3. Finden Sie den Hostsatz im Host Sets Abschnitt und klicken Sie auf das **Edit** Symbol.
4. In der Set Builder Ansicht **Alt+Klicken Sie** den Host, den Sie von dem Hostsatz entfernen wollen.

Einen Standardsatz mit Hilfe von Filterausdrücken erstellen

Endpoint Security ermöglicht Ihnen, Hostgruppen für einen Standardsatz, auf Ausdrücken für einige der Hostgruppenfilter basierend zu erstellen. Ausdrücke sind Suchfilter, die Ihnen gestatten, eine Hostgruppe weiter zu filtern, indem Sie unter relativ großen Metadatenwerten suchen. Sie sind nur für einige Filter verfügbar.

Sie können Hostgruppen auf Ausdrücken basierend erstellen, noch bevor Hosts bereitgestellt werden. Wenn berechtigte Hosts bereitgestellt werden, treten sie automatisch den Gruppen bei.

Verwenden Sie entweder CIDR Notation oder reguläre Ausdrücke (regex), um Gruppen auf Ausdrücken basierend zu erstellen, die nach Hosts suchen.

- Mit Hilfe von CIDR Notation können Sie Ausdrücke erstellen, die nach Subnetzen suchen.

Wenn Sie einen CIDR Notationsausdrück falsch eingeben, verarbeitet Endpoint Security, was Sie als regex eingeben, wodurch möglicherweise keine idealen Ergebnisse erzielt werden.

- Mit Hilfe von regex können Sie Ausdrücke erstellen, die das OS & Patch, Windows Domain oder Hostnamenfilter für eine Hostgruppe weiter filtern.

Um Filterausdrücke für die Erstellung eines Standardsatzes zu verwenden:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.
3. Bewegen Sie den Cursor über die **Create Host Set** Schaltfläche und wählen Sie **Using set builder**.

   Die Create Standard Set Seite wird angezeigt.
4. Im Filters Abschnitt wählen Sie einen Filter. Diese Filter ermöglichen Ihnen Ausdrücke festzulegen oder spezifische Filterkriterien einzugeben: Domain, OX & Patch, Zeitzone, Subnetz, Hostname oder Letzte Sysinfo.

   Der Filter Criteria Bereich führt Filterkriterien für den ausgewählten Filter auf, einen Link mit dem Namen **Create Expression** oder ein Feld, in dem Sie ein oder mehrere Kriterien für den Filter eingeben können.
5. Klicken Sie auf den **Create Expression** Link im Filter Criteria Bereich, um einen regulären Ausdruck für den Filter in regex oder in CIDR Notation festzulegen. Geben Sie Werte oder einen gültigen Ausdruck in regex oder in CIDR Notation im resultierenden Textfeld ein.

   Der Set Navigator Kreis zeigt die Hosts an, die den ausgewählten Filtern entsprechen.
6. Ziehen Sie den Set Navigator Kreis auf den Result Set Kreis im Set Visualizer.

   Sie haben jetzt einen Standardsatz erstellt, der eine Hostgruppe enthält.
7. Definieren Sie Hostgruppen mit Hilfe der Filter in den Filters and Filter Criteria Abschnitten. Ziehen Sie den Set Navigator Kreis jedes Mal auf den Set Visualizer, um eine weitere Hostgruppe zu dem Standardsatz hinzuzufügen.

   Zusätzliche Informationen über Filter und Filterausdrücke finden Sie unter Hostsätze in eine Hostgruppe für einen Standardsatz einbetten und Einen Standardsatz mit Hilfe von Filtern erstellen.
8. Wenn das Hinzufügen von Hostgruppen zum Standardsatz abgeschlossen ist, geben Sie ihre Beziehungen im Set Visualizer an. Weitere Informationen finden Sie unter Beziehungen zwischen Hostgruppen in einem Standardsatz manipulieren.
9. Geben Sie einen Namen im Set Name Feld ein und klicken Sie dann auf **Create**.

   Der Standardsatz, der eine oder mehrere Hostgruppen enthält, wird erstellt.

Um einen Host von einem Standardsatz zu entfernen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.
3. Finden Sie den Hostsatz im Host Sets Abschnitt und klicken Sie auf das **Edit** Symbol.
4. In der Set Builder Ansicht **Alt+Klicken Sie** den Host, den Sie von dem Hostsatz entfernen wollen.

Hostsätze in eine Hostgruppe für einen Standardsatz einbetten

Verwenden Sie die Informationen und Anleitungen in diesem Thema, um einen vorhandenen Hostsatz in eine Hostgruppe einzubetten, die in einem Standard Hostsatz enthalten ist.

Das Einbetten von mehr als 10 Hostsätzen kann die Leistung des Systems beeinträchtigen. FireEye empfiehlt, die Einbettung von mehr als 10 Sätzen in einem Hostsatz zu vermeiden.

Um einen Standardsatz zu erstellen, der einen Hostsatz in einer seiner Hostgruppen einbettet:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.
3. Bewegen Sie den Cursor über die **Create host set** Schaltfläche und wählen Sie **Using set builder**.

   Die Create Host Set: Set Builder Seite wird angezeigt.
4. Im Filters Abschnitt wählen Sie **SAVED HOST SETS**.

   Eine Liste der vorhandenen statischen und Standard Hostsätze wird in dem Bereich angezeigt.
5. Wählen Sie einen Hostsatz vom Filter Criteria Bereich.

   Der Set Navigator Kreis zeigt die Hosts an, die den von Ihren getroffenen Auswahlen entsprechen.
6. Ziehen Sie den Set Navigator Kreis auf den Result Set Kreis im Set Visualizer.

   Sie haben jetzt einen Standardsatz erstellt, der einen eingebetteten Hostsatz enthält.

7. Definieren Sie Hostgruppen mit Hilfe der Filter in den Filters and Filter Criteria Abschnitten. Sie können sogar einen anderen Hostsatz einbetten. Ziehen Sie den Set Navigator Kreis jedes Mal auf den Set Visualizer, um eine weitere Hostgruppe zu dem Standardsatz hinzuzufügen.

   Zusätzliche Informationen über Filter und Filterausdrücke finden Sie unter Einen Standardsatz mit Hilfe von Filtern erstellen und Einen Standardsatz mit Hilfe von Filterausdrücken erstellen.

8. Wenn das Hinzufügen von Hostgruppen zum Standardsatz abgeschlossen ist, geben Sie ihre Beziehungen im Set Visualizer an. Weitere Informationen finden Sie unter Beziehungen zwischen Hostgruppen in einem Standardsatz manipulieren.

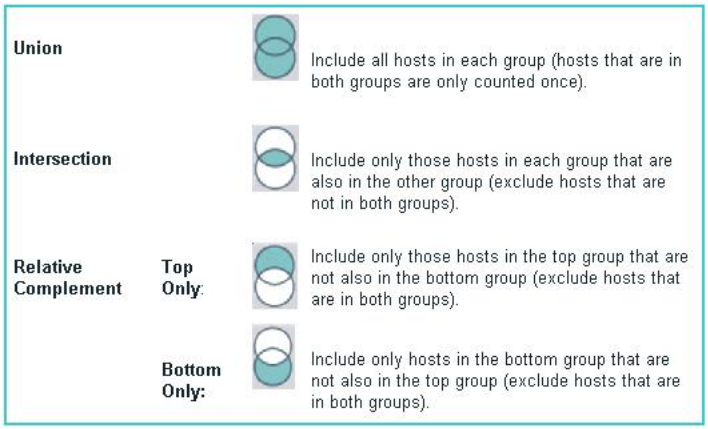
9. Geben Sie einen Namen im Set Name Feld ein und klicken Sie dann auf **Create**.

   Der Standardsatz mit einem oder mehreren eingebetteten Hostsätzen wird erstellt. Wenn ein Hostsatz in einem anderen Hostsatz eingebettet ist, wird ein Sternchen (*) nach seinem Namen auf der Host Sets Seite angezeigt.

Beziehungen zwischen Hostgruppen in einem Standardsatz manipulieren

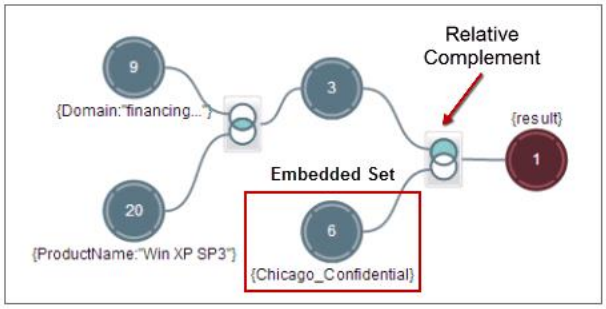
Der Set Visualizer Bereich ermöglicht Ihnen, Gruppen von Hosts zu kombinieren und Ihre Beziehungen innerhalb des endgültigen Result Set zu manipulieren.

Verwenden Sie die Venn Diagramme, die zwischen den Hostgruppen im Set Visualizer angezeigt werden, um die Beziehungen zwischen zwei Hostgruppen zu manipulieren. Wenn Sie das Venn Diagramm anklicken, durchlaufen Sie Optionen, die Ihnen ermöglichen, die Gruppen von Hosts auf unterschiedliche Art, auf Beziehungen zwischen den Gruppen basierend, zu kombinieren:**Union**, **Intersection** und **Relative Complement**:



Sie können beispielsweise einen statischen Hostsatz in einem Hostsatz mit Standard (dynamischen) Hostsätzen einbetten und dann den Hostsatz ausschließen Die folgende Abbildung zeigt einen statischen Hostsatz (Chicago_Confidential), der in eine größere

Gruppe von Hosts eingebettet ist und dann mit Hilfe einer relativen Ergängzung ausgeschlossen wird:



Um Hostgruppen vom Set Visualizer zu entfernen, drücken Sie auf die **Alt** Taste, während Sie auf den Kreis klicken, der die Hostgruppe enthält, die Sie entfernen wollen.

Wenn Sie Beziehungen zwischen Gruppen von Hosts kombinieren und anpassen, zeigt der **Result Set** die Gruppe der Hosts an, die durch Ihre Auswahlmöglichkeiten erstellt wurde. Details über den Ergebnissatz werden im **Result Set Details** Abschnitt angezeigt.

Wenn Sie eine neue Gruppe mit dem **Result Set** kombinieren, zeigt der neue **Result Set** eine Beziehung zwischen der neuen Gruppe und allen früheren Kombinationen an, die Sie erstellt haben.

Wenn Sie eine neue Gruppe mit einer der anderen Gruppenkreise im **Set Visualizer** kombinieren, zeigt ein neuer Zweig die Beziehung zwischen den Gruppen an, die Sie kombiniert haben; der **Result Set** zeigt die endgültige Kombination an.

Sie kombinieren weiterhin relevante Gruppen von Hosts und passen ihre Beziehungen an, bis Sie die gewünschten endgültigen Ergebnisse erhalten.

Einem Hostsatz eine Richtlinie zuweisen

Wenn Sie benutzerdefinierte Richtlinien auf eine Hostgruppe anwenden wollen, können Sie einen Hostsatz erstellen und die benutzerdefinierten Richtlinien in dem Satz anwenden, wie in diesem Abschnitt beschrieben.

Auf allen Host-Endpunkte wird die Agent Default Richtlinie automatisch angewendet.

In besonderen Fällen, in denen Sie benutzerdefinierte Richtlinien auf einen einzelnen Host anwenden wollen, erstellen Sie einen Hostsatz, der nur diesen Host enthält.

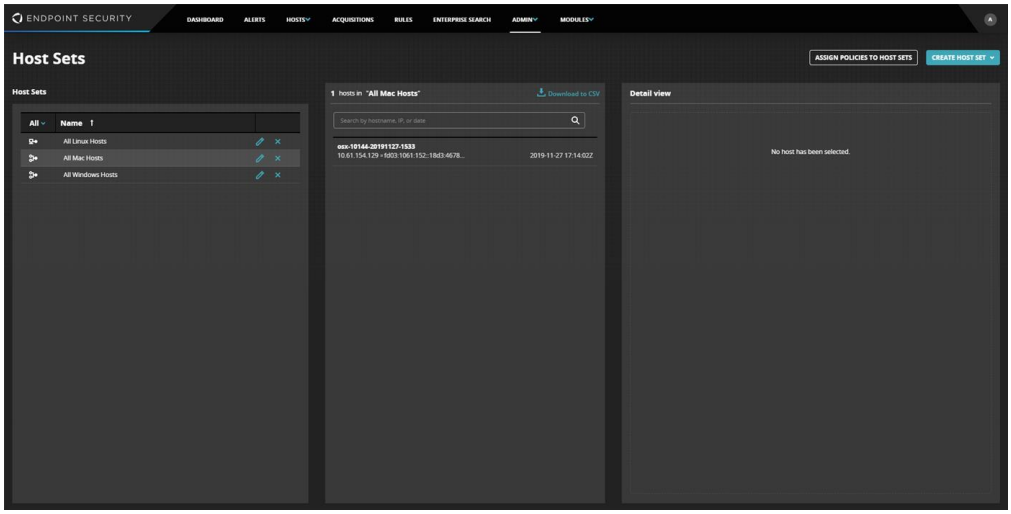
Voraussetzungen

- Administratorzugriff

Um die Richtlinie auf einen Hostsatz anzuwenden:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.
3. Klicken Sie auf die **Assign Policies to Host Sets** Schaltfläche in der oberen rechten Ecke der Seite.

   Die Assign Policies to Host Sets Seite wird angezeigt.



4. Wählen Sie einen Hostsatz von der Host Sets Spalte.
5. Wählen Sie die Richtlinien in der Policies Spalte, die Sie dem Hostsatz zuweisen wollen.
6. Überprüfen Sie die Details eines Hostsatzes oder einer Richtlinie auf dem Selected Host Set or Selected Policy Tab.
7. Klicken Sie auf **Save**.

Wenn ein Host zu einem bestehenden Hostsatz hinzugefügt wird, werden die auf diesen Hostsatz anwendbaren Richtlinien an den neu hinzugefügten Host gesendet.

Weitere Informationen über Richtlinen, einschließlich die Priorisierung der Reihenfolge, in der Richtlinien angewendet werden, finden Sie im Endpoint Security Agent Administrationshandbuch.

Eine Liste von Hosts in einem Hostsatz mit Hilfe der Web-UI herunterladen

Sie können eine Liste der Hosts in einem Hostsatz mit Hilfe der Endpoint Security Web-UI herunterladen.

Voraussetzungen

- Admin oder Operator Zugriff

Um eine Liste der Hosts in einem Hostsatz herunterzuladen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.
3. Wählen Sie den Hostsatz im linken Bereich der **Host Sets** Seite. Eine Liste der in dem Hostsatz enthaltenen Hosts werden im mittleren Abschnitt angezeigt.
4. Klicken Sie auf das **Download** Symbol am Anfang des mittleren Abschnitts. Eine CSV-Datei wird heruntergeladen, die eine Liste der Hosts in dem Hostsatz enthält.

Wenn Sie die Hostliste für einen Hostsatz herunterladen, der Zeitzonen für Länder mit nicht-lateinischen Sprachen enthält, müssen Sie Ihre Tabellenkalkulationsanwendung so konfigurieren, dass sie die Hostliste mit Hilfe des Unicode (UTF-8) Zeichenkodierungsformats importiert, die von Endpoint Secuity verwendet wird.

Hostsätze mit Hilfe der Web-UI bearbeiten

Verwenden Sie die Informationen und Anweisungen in diesem Thema, um statische und Standardsätze mit Hilfe der Web-UI zu bearbeiten.

Voraussetzungen

- Admin oder Operator Zugriff

Um einen Hostsatz zu bearbeiten:

1. Melden Sie sich auf der Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.

3. Klicken Sie auf das **Edit** Symbol auf der rechten Seite des Satzes, den Sie löschen möchten.

   Die Edit Static Set Seite (für statische Sätze) oder die Edit Standard Set Seite (für Standard Sätze) wird angezeigt.

4. Bearbeiten Sie den Satz:

   - Um Hosts oder Hostgruppen hinzuzufügen oder zu entfernen folgen Sie dem gleichen Verfahren, dass Sie zum Hinzufügen oder Entfernen von Hosts oder Hostgruppen verwendet haben, als Sie den Satz erstellt haben. Siehe:
     - Statische Sätze erstellen
     - Standardsätze erstellen
   - Um den Namen des Satzes zu ändern, geben Sie einen neuen Namen im **SET NAME** Feld ein.

     Endpoint Security bietet keine **Save As** oder **Copy** Funktion. Wenn Sie einen Hostsatz mit einem neuen Namen speichern, wird der Hostsatz einfach umbenannt.

5. Klicken Sie auf **Save**.

Hostsätze mit Hilfe der Web-UI löschen

Verwenden Sie die Informationen und Anweisungen in diesem Thema, um statische und Standardsätze mit Hilfe der Endpoint Security Web-UI zu löschen.

Eingebettete Hostsätze können nicht gelöscht werden, bis sie von den Hostsätzen entfernt werden, in die sie eingebettet sind. Weitere Informationen über eingebettete Sätze finden Sie unter Standardsätze verstehen.

Voraussetzungen

- Admin oder Operator Zugriff

Um einen Hostsatz zu löchen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Admin** Menü wählen Sie **Host Sets**.
3. Klicken Sie auf das **Delete** Symbol auf der rechten Seite des Satzes, den Sie löschen möchten.

Wenn Sie versuchen, einen eingebetteten Hostsatz zu löschen, wird eine Liste der Hostsätze, in denen er eingebettet ist, angezeigt.

4. Klicken Sie im Bestätigungsfeld auf **Delete**.

KAPITEL 9: Hochwertige Hosts identifizieren

Hochwertige Hosts sind Hosts, die für Ihre Organisation von entscheidender Bedeutung sind. Dabei kann es sich um Hosts handeln, die Ihr System stark beeinflussen.

Sie können Hostsätze identifizieren, die aus hochwertigen Hosts bestehen und sie kennzeichnen. Auf diese Weise können Sie Endpoint Security Web-UI Listen für hochwertige Hosts filtern. Sie können Alarme, Erfassungen und Eindämmungsaktionen für hochwertige Hosts schnell anzeigen und Ereignisse dafür behandeln, bevor Sie Ereignisse für andere Hosts angehen.

Wenn Ihre hochwertigen Hosts in mehreren Hostsätzen mit anderen Hosts enthalten sind, die keine hochwertigen Hosts sind, sollten Sie in Betracht ziehen, einen neuen Hostsatz zu erstellen, der nur hochwertige Hosts enthält. Weitere Informationen finden Sie unter Hostsätze konfigurieren.

Voraussetzungen

- Admin Zugriff
- Mindestens ein Hostsatz ist definiert.

Um hochwertige Hosts mit Hilfe der Web-UI zu identifizieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Navigieren Sie auf die High-Value Hosts Seite. Wählen Sie **High-Value Hosts** auf dem **Admin** Menü. Die High-Value Hosts Seite wird geöffnet. Alle definierten Hostsätze sind auf dieser Seite aufgeführt.
3. Im **Host Sets** Bereich wählen Sie die Hostsätze, die hochwertige Hosts enthalten.
4. Klicken Sie auf **Save**.

   Die Gesamtzahl der Hosts, die in den hochwertigen Hostsätzen enthalten sind, wird angezeigt.

KAPITEL 10: Warnungsschwellenwerte konfigurieren

Sie können Warnungsschwellenwerte verwenden, um die Anzahl der Warnungen zu begrenzen, die durch den Endpoint Security von FireEye Endpoint Security Agents in einem Treffersturm verarbeitet wurden (wenn übermäßige Malware Warnungen vom Endpoint Security empfangen werden).

Es können drei Warnungsschwellenwerte festgelegt werden:

- Die Gesamtzahl der Warnungsschwellenwerte steuert die Gesamtzahl der Warnmeldungen, die vom Endpoint Security verarbeitet werden können. Siehe Den gesamten Warnungsschwellenwert konfigurieren unten
- Der Malware Warnungsschwellenwert steuert die Anzahl der Malware Warnungen für die gleiche Malware Infektion, die vom Endpoint Security in einem festgelegten Intervall verarbeiten kann.
- Der IOC und Exploit Warnungsschwellenwert steuert die Anzahl der IOC und Exploit Warnungen für die gleiche Infektion, die vom Endpoint Security in einem festgelegten Intervall verarbeitet werden kann.

Den gesamten Warnungsschwellenwert konfigurieren

Sie können einen gesamten Warnungsschwellenwert verwenden, um die Gesamtzahl der Warnungen, die durch die Endpoint Security Appliance vom FireEye Endpoint Security Agents in einem Treffersturm verarbeitet werden, einzuschränken.

Wenn der gesamte Schwellenwert für Warnmeldungen zu niedrig eingestellt wird, können Warnungen verloren gehen. Wenn der Schwellenwert zu hoch eingestellt wird, kann dies zu Leistungsproblemen auf der Appliance führen, wenn ein Hit-Storm auftritt.

Diese Einstellung wird mit Hilfe der CLI konfiguriert. Sie kann nicht mit Hilfe der Endpoint Security Web-UI konfiguriert werden.

- Die Einstellung für den gesamten Warnungsschwellenwert überprüfen unten
- Das gesamte Warnungsmaximum festlegen unten

Voraussetzungen

- Admin Zugriff

Die Einstellung für den gesamten Warnungsschwellenwert überprüfen

Um die Einstellung für den gesamten Warnungsschwellenwert mit Hilfe der CLI zu überprüfen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Überprüfen Sie die Einstellung für den gesamten Warnungsschwellenwert.

   ```
   hostname (config) # show hx server detection
   ```

   Die folgende Zeile wird al Teil der Ausgabe dieses Befehls angezeigt und zeigt die Einstellung für den gesamten Warnungsschwellenwert.

   ```
   Total Alert Limit Maximum: 1000000
   ```

Das gesamte Warnungsmaximum festlegen

Um die Höchstzahl von Alarmen festzulegen, die die Endpoint Security Appliance mit Hilfe der CLI verarbeiten kann:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Legen Sie das gesamte Warnungsmaximum fest.

   ```
   hostname (config) # hx server detection alert total-limit <number>
   ```

   wobei <number> die Höchstzahl von Warnmeldungen festlegt, die von der Endpoint Security Appliance verarbeitet werden kann. Gültige Werte reichen von 0 bis 1048576. Der Standardwert ist 1000000.

   Wenn die Anzahl der Alarme diesen Schwellenwert überschreitet, werden die ältesten Alarmmeldungen verworfen.

   Um das Alarmmaximum auf den Standard zurückzusetzen, verwenden Sie die no Form dieses Befehls.

   ```
   hostname (config) # no hx server detection alert total-limit
   ```

   Um diesen Schwellenwert zu deaktivieren, stellen Sie seinen Wert auf 0 (Null) ein.

   ```
   hostname (config) # hx server detection alert total-limit 0
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

KAPITEL 11: Warnungsalterung

Alte Warnungen und Quellenalarme können für Ihr Unternehmen von begrenztem Wert sein und die Leistung Ihres Systems und Ihrer Systemanalytiker beeinträchtigen.

Standardmäßig altert (entfernt) die Endpoint Security Software automatisch alle von FireEye Appliances ausgehenden Warnungen und Quellenwarnunge, nachdem ihre definierten Alterungsperioden abgelaufen sind.

Sie können diese Alterungsperioden ändern. Zusätzlich können Sie Warnungen und Quellenalarme jederzeit manuell löschen.

HINWEIS: Wenn Indikatorregeln gelöscht sind—gleichgültig ob manuell oder automatisch—löscht die Endpoint Security Software auch alle zugehörigen Warnungen automatisch. Die Software löscht keine mit den gelöschten Indikatorregeln verbundenen Erfassungen.

Einstellungen für die Warnungsalterung überprüfen

Sie können Einstellungen für die Alterung der Warnung mit Hilfe der Endpoint Security Web-UI oder CLI überprüfen.

Voraussetzungen

- Administratorzugriff

Einstellungen für Warnungsalterung mit Hilfe der Web UI überprüfen

Sie können die Einstellungen für die Warnungsalterung auf der Alerts Settings Seite überprüfen.

Um Einstellungen für Warnungsalterung mit Hilfe der Web UI zu überprüfen

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** vom Admin Menü, um auf die Aging Settings Seite zuzugreifen. Einstellungen für die Alarm- und Indikatorregelalterung werden im Indicator & Alert Aging Feld auf dieser Seite angezeigt.

Einstellungen für Warnungsalterung mit Hilfe der CLI überprüfen

Um Einstellungen für Warnungsalterung mit Hilfe der CLI zu überprüfen

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Listen Sie Einstellungen für Warnungsalterung auf:

   ```
   hostname (config) # show hx server detection
   ```

   Nachfolgend finden Sie eine Beispielausgabe dieses Befehls:

   ```
   HX Server Detection Configuration:

   Generated Indicator Aging: enabled
   Generated Indicator Aging Period: 14 days
   Generated Condition Aging: enabled
   Generated Condition Aging Period: 30 days
   Source Alert Aging: enabled
   Source Alert Aging Period: 30 days
   Alert Aging Period: 30 days
   False Positive Alert Aging Period: 1 day

   Intel Matching: enabled

   Legacy notification listener active: no
   Malicious.URL Indicator Generation (legacy): yes
   Suspicious (noisy) Indicator Generation (legacy): no

   Inbound alert poll interval: 5 minutes
   Inbound alert minimum severity: majr
   No ignored alert types.

   Last bookmark ID: 0
   ```


Einstellungen für Warnungsalterung festlegen

Die folgende Tabelle fasst die verfügbaren Einstellungen für Warnungsalterung zusammen.

Einstellung	Beschreibung
Alert Aging Interval	Der Alterungsintervall für ausgelöste Warnungen auf dem System. Die Einstellung kann mit Hilfe der Endpoint Security Web-UI oder der CLI festgelegt werden. Eine Warnung wird automatisch vom System entfernt, wenn die Zeit seit seinem letzten Vorkommnis größer als dieser Intervall ist. Web UI Bereich: 1 Tag bis 365 Tage CLI Bereich: 60 bis 31536000 Sekunden (1 Minute bis 365 Tage) Standardwert: 2592000 Sekunden (30 Tage) Siehe Den Alterungsintervall der Warnung einstellen auf der nächsten Seite.
False Positive Alert Aging Interval	Das Alterungsintervall von Warnungen, die als Falsch Positiv Warnungen auf dem System markiert sind. Die Einstellung kann nur mit Hilfe der CLI geändert werden. CLI Bereich: 60 bis 31536000 Sekunden (1 Minute bis 365 Tage) Standardwert: 86400 Sekunden (ein Tag) Siehe Das Falsch Positiv Warnungsalterungsintervall mit Hilfe der CLI einstellen auf Seite 213.
Source Alert Aging Enabled	Aktiviert oder deaktiviert das Alterungsintervall der Warnung für die Quelle. Wenn das Alterungsintervall erreicht ist, werden Quellenwarnungen von der Datenbank entfernt. Wenn Alterung deaktiviert ist, werden Quellenwarnungen nicht automatisch entfernt. Das Warnungsalterungsintervall der Quelle kann mit Hilfe der CLI aktiviert oder deaktiviert werden. Standardwert: Aktiviert Siehe Warnungsalterung für Quellen mit Hilfe der CLI aktivieren auf Seite 213 und Warnungsalterung für Quellen mit Hilfe der CLI deaktivieren auf Seite 214.

Einstellung	Beschreibung
Source Alert Aging Interval	Das Alterungsintervall von Quellenwarnungen auf dem System. Eine Quellenwarnung wird automatisch vom System entfernt, wenn die Zeit seit ihrem letzten Vorkommnis größer als dieser Intervall ist. CLI Bereich: 60 bis 31536000 Sekunden (1 Minute bis 365 Tage) Standardwert: 2592000 Sekunden (30 Tage) Siehe Das Warnungsalterungsintervall für Quellen mit Hilfe der CLI einstellen auf Seite 214.

Den Alterungsintervall der Warnung einstellen

Sie können den Alterungsintervall der Warnung mit Hilfe der Endpoint Security Web-UI oder der CLI einstellen.

- Das Warnungsalterungsintervall mit Hilfe der Web-UI einstellen unten
- Das Warnungsalterungsintervall mit Hilfe der CLI einstellen auf der nächsten Seite

Voraussetzungen

- Administratorzugriff

Das Warnungsalterungsintervall mit Hilfe der Web-UI einstellen

Um das Warnungsalterungsintervall mit Hilfe der Web-UI einzustellen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie Aging Settings **auf dem Admin** Menü. Die Aging Settings Seite wird angezeigt.
3. Im Indicator & Alert Aging Feld auf der Aging Settings Seite geben Sie ein Alterungsintervall im **Delete alerts after:** Feld ein. Gültige Werte liegen zwischen 1 bis 365 Tagen. Dies stellt das Alterungsintervall ein und aktiviert es.
4. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

Um Standardeinstellungen wiederherzustellen, klicken Sie auf **Reset to default** und klicken Sie dann auf **Save**. Wenn Sie auf **Cancel** klicken, gibt Endpoint Security Einstellungen auf die zuletzt gespeicherten Werte zurück.

Das Warnungsalterungsintervall mit Hilfe der CLI einstellen

Um das Warnungsalterungsintervall mit Hilfe der CLI einzustellen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Das Warnungsalterungsintervall einstellen:

   ```
   hostname (config) # hx server detection aging alert period <seconds>
   ```

   wobei <seconds> die Anzahl von Sekunden für die Alterungsperiode für Warnungen ist. Der Standardwert ist 2592000 Sekunden (30 Tage). Gültige Werte liegen zwischen 0 und 31536000 Sekunden (ein Jahr).

   Um dieses Intervall auf seine Standardeinstellung zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   hostname (config) # no hx server detection aging alert period
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Das Falsch Positiv Warnungsalterungsintervall mit Hilfe der CLI einstellen

Um das Falsch Positiv Warnungsalterungsintervall mit Hilfe der CLI einzustellen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable hostname # configure terminal
   ```

2. Das Falsch Positiv Warnungsalterungsintervall einstellen:

   ```
   hostname (config) # hx server detection aging alert fp-period <seconds>
   ```

   wobei <seconds> die Anzahl von Sekunden für die Alterungsperiode für Falsch Positiv Warnungen ist. Die Standardeinstellung ist 86400 Sekunden (ein Tag). Gültige Werte liegen zwischen 0 und 31536000 Sekunden (ein Jahr).

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Warnungsalterung für Quellen mit Hilfe der CLI aktivieren

Um Warnungsalterung mit Hilfe der CLI zu aktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie das Warnungsalterungsintervall für Quellen:

   ```
   hostname (config) # hx server detection aging source-alert enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Warnungsalterung für Quellen mit Hilfe der CLI deaktivieren

Um Warnungsalterung mit Hilfe der CLI zu deaktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie das Warnungsalterungsintervall für Quellen:

   ```
   hostname (config) # no hx server detection aging source-alert enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Das Warnungsalterungsintervall für Quellen mit Hilfe der CLI einstellen

Um das Warnungsalterungsintervall für Quellen mit Hilfe der CLI einzustellen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Das Warnungsalterungsintervall für Quellen einstellen:

   ```
   hostname (config) # hx server detection aging source-alert period
   <seconds>
   ```

   wobei <seconds> die Anzahl von Sekunden für die Alterungsperiode für Quellenalarme ist. Der Standardwert ist 2592000 Sekunden (30 Tage). Gültige Werte liegen zwischen 60 und 31536000 Sekunden (ein Jahr).

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

KAPITEL 12: Intelligenz (Regel) Überblick

Die Endpoint Security Software verwendet Intelligenz aus einer Vielzahl von Quellen, um Endpunktaktivität zu überwachen. Intelligenz (Intel) wird verwendet, um verdächtiges Verhalten auf Ihrem Netzwerk zu identifizieren. Intelligenzinformationen sind in Regeln definiert.

Regeln können Indicator of Compromise Regeln sein (auch IOC Regeln oder Indikatoren genannt), Exploit Guard Regeln oder falsch positiv Regeln sein.

Regeln bestehen aus einer oder mehreren Bedingungen. Eine Bedingung ist eine spezifische Aktivität auf einem Host. Beispiele für eine Bedingung sind:

- Ein Registrierungsschlüssel Update
- Eine Dateiänderung
- Eine DNS Suche
- Eine Benutzerkontoänderung

Eine Regel ist eine Sammlung von Bedingungen, die in Kombination eine bestimmte Bedrohung für einen Endpunkt identifizieren. Wenn Regeln ausgelöst werden, generieren sie Alarme.

Da Regeln anhand der Betriebssystemplattform und der Agentenversion identifiziert werden, können FireEye Endpoint Security Agents auf Ihren Endpunkten Regeln, die für das Betriebssystem des Endpunkts und die Agentenversion geeignet sind, effizient herunterladen.

Sie können Indikator und Falsch Positiv Regeln mit Hilfe der Endpoint Security Web-UI, aber nicht mit der CLI verwalten. Zusätzlich werden Exploit Guard Regeln nur von FireEye bereitgestellt und verwaltet. Informationen über die Verwaltung von Indikatorregeln finden Sie unter IOC Regeln verwalten auf Seite 221. Informationen über die Verwaltung von falsch positiv Regeln finden Sie unter Falsch Positiv Regeln verwalten auf Seite 401.

Indikatorregeltypen

Die folgenden Typen von Indikator (IOC) Regeln werden unterstützt. Diese Typen können in der Category Spalte auf dem Indicators Register der Rules Seite in der Endpoint Security Web-UI angezeigt werden.

Type	Beschreibung
Custom	Benutzerdefinierte Indikatorregeln, die Bedingungen wie z.B. DNS Suche, Netzwerkverbindungen und der Erstellung spezifischer Malware Dateien enthalten.
Imported	Aus SIEM importierte Indikatorregeln.
FireEye	Von anderen FireEye Appliances (wie NX Serie oder EX Serie) aber nicht von der CM Serie importierte Indikatorregeln. Diese Indikatorregeln werden von Quellenalarmen erstellt. Siehe FireEye Quellenwarnungen auf Seite 415.
FireEye-CMS	Aus CM Serie importierte Indikatorregeln Diese Indikatorregeln werden von Quellenwarnungen erstellt. Siehe FireEye Quellenwarnungen auf Seite 415.
Mandiant Intel	Aus DTI importierte eingeschränkte Indikatorregeln. Eingeschränkte Indikatorregeln sind ausgeblendet, bis eine der Bedingungen in dem Indikator eine Warnung für einen Endpunkt auslöst.
Mandiant Unrestricted Intel	Uneingeschränkte Indikatorregeln. Diese Indikatorregeln werden immer in der Indikatorliste auf dem Indicators Register der Rules Seite in der Web-UI angezeigt. Sie werden von FireEye für einige interne Verarbeitung verwendet und dienen als Hinweis darauf, dass das FireEye Indikatorpaket auf Ihrer Appliance geladen und funktionsfähig ist. Zusätzlich können Sie sie als Beispiele verwenden, wenn Sie benutzerdefinierte Indikatorregeln erstellen.

Informationen über die Verwaltung von IOC Regeln finden Sie unter IOC Regeln verwalten auf Seite 221.

Eingeschränkte Indikatorregeln

FireEye Indikatorregeln sind eingeschränkt und werden in der Dynamic Threat Intelligence (DTI) Cloud gespeichert. Sie sind normalerweise in der Endpoint Security Web-UI und der API ausgeblendet. Sie sind nur sichtbar, wenn ihr Vorhandensein auf einem Endpunkt einen Alarm auslöst oder wenn der Indikator von einer anderen FireEye Appliance bereitgestellt wird. Ebenso können die mit FireEye Indikatorregeln verknüpften Bedingungen nur angezeigt werden, wenn die Bedingung eine Warnung auslöst. Wenn alle mit einem Indikator oder Bedingung verknüpften Alarme entfernt werden, wird der Indikator und die dazugehörigen Bedingungen wieder ausgeblendet. Dies vereinfacht die forensische Analyse von Alarmen, weil nur die relevanten Indikatorregeln und Bedingungen angezeigt werden. Wenn FireEye Indikatorregeln sichtbar sind, werden sie auf dem Indicators Tab der Rules Seite in der Web-UI angezeigt.

Uneingeschränkte Indikatorregeln

Einige FireEye Indikatorregeln sind uneingeschränkt. Diese Indikatorregeln werden immer in der Indikatorliste auf dem Indicators Tab der Rules Seite in der Web-UI angezeigt. Sie werden von FireEye für einige interne Verarbeitung verwendet und dienen als Hinweis darauf, dass das FireEye Indikatorpaket auf Ihrer Appliance geladen und funktionsfähig ist. Zusätzlich können Sie sie als Beispiele verwenden, wenn Sie benutzerdefinierte Indikatorregeln erstellen.

Die folgende Tabelle enthält eine kurze Beschreibung jedes uneingeschränkten FireEye Indicator of Compromise (IOC).

Indikatorname	Beschreibung
CRYPMIC RANSOMWARE (FAMILY)	Identifiziert mit der Ausführung der CRYPMIC Ransomware Familie und ihrer Varianten verknüpfte Artefakte.
FIREEYE END2END OSX TEST	Testet, dass das FireEye Indikatorpaket richtig in macOS Umgebungen geladen ist.
FIREEYE END2END TEST	Testet, dass das FireEye Indikatorpaket in Windows Umgebungen ordnungsgemäß geladen ist.
JAKU (REPORT)	Identifiziert eine Indicator of Compromise (IOC) Regel, die aus Informationen im Forcepoint JAKUE Bericht abgeleitet wird. Dies umfasst Host-basierte und netzwerkbasierte Indikatorregeln.

Indikatorname	Beschreibung
MALICIOUS SCRIPT CONTENT A (METHODOLOGY)	Sucht nach möglicherweise bösartigen Scripts, die über `mshta.exe` oder `rundll32.exe` über Persistenzmechanismen des Verzeichnisses ausgeführt werden. Der Inhalt des Scripts ist möglicherweise in den Verzeichnisdaten verfügbar oder verweist auf Dateien auf der Festplatte.
MIMIKATZ (CREDENTIAL STEALER)	Identifiziert Artefakte, die mit der Ausführung von MIMIKATZ Malware verbunden sind. MIMIKATZ ist eine frei herunterladbare Binärdatei, die zur Prozessinjektion, zum Security Account Manager (SAM) Hash-Dumping und zum Exportieren von Zertifikaten und privaten Schlüsseln des ausführenden Benutzers geeignet ist.
NEUTRINO EXPLOITKIT (EXPLOIT)	Identifiziert Dateien, die vom Neutrino Exploit-Kit gelöscht wurden. Eine verschlüsselte `jscript` Nutzlast wird verwendet, um eine `.exe` oder `.dll` Nutzlast, die auf `%TEMP%` geschrieben und dann gestartet wird, herunterzuladen und zu entschlüsseln.
SUSPICIOUS SCRIPT CREATION (METHODOLOGY)	Identifiziert die Erstellung und Ausführung von Scripts mit zufälligen Namen. Durch diese Technik können Nutzlasten in phishing E-Mail abgelegt werden.
SUSPICIOUS VBSCRIPT (METHODOLOGY)	Identifiziert die Verwendung ausdrücklicher Script Engine Deklarationen für `cscript` oder `wscript` ohne ihre normalerweise verbundenen Dateierweiterungen.
WSCRIPT LAUNCHING POWERSHELL (METHODOLOGY)	Sucht nach `wscript.exe` startenden Powershell Scripts aus einem `temp` Verzeichnis. Der CERTOR ist hierfür bekannt.

Benutzerdefinierte Indikatorregeln

Sie können benutzerdefinierte Indikatorregeln erstellen, um nach Hinweisen auf Kompromittierung zu suchen, z. B. beim Einrichten bestimmter Netzwerkverbindungen, DNS Suchen und beim Erstellen oder Ändern bestimmter Dateien. Benutzerdefinierte Warnungen treten auf, wenn eine Bedingung in einem benutzerdefinierten Indikator eine Warnung auf einem Endpunkt auslöst. Siehe Benutzerdefinierte Indikatorregeln verwalten auf Seite 223.

Falsch positiv Regeltypen

Die folgenden falsch positiv Regeltypen werden unterstützt. Diese Typen können in der Rule Type Spalte auf dem False Positiv Register der Rules Seite in der Endpoint Security Web-UI angezeigt werden.

Typ	Beschreibung
IOC	Identifiziert eine falsch positiv Regel für eine Indicator of Compromise (IOC) Bedingung.
EXD	Identifiziert eine falsch positiv Regel für eine Exploit Warnung.
MAL	Identifiziert eine falsch positiv Regel für Informationen aus einer Malware Warnung.

Informationen über die Verwaltung von falsch positiv Regeln finden Sie in Falsch Positiv Regeln verwalten auf Seite 401.

KAPITEL 13: IOC Regeln verwalten

FireEye liefert Indicators of Compromise (IOCs) für den Schutz Ihrer Umgebung. Sie werden von FireEye in der Dynamic Threat Intelligence (DTI) Cloud verwaltet. IOCs können auch von anderen FireEye Appliances generiert und der Endpoint Security Appliance zur Unterstützung Ihrer Untersuchungen bereitgestellt werden.

Zusätzlich kann Endpoint Security die eigene Intelligenz Ihrer Appliance verwenden, indem sie Ihren Benutzer hilft, benutzerdefinierte Indicator of Compromise Regeln zu erstellen, bearbeiten und löschen. Sie können Indikatorregeln erstellen und bearbeiten, indem Sie individuelle Bedingungen hinzufügen oder löschen oder Listen mit Bedingungen hochladen.

Letztendlich können Sie nach Indikatorregeln mit Hilfe der Endpoint Security Web-UI suchen und sie löschen.

Endpoint Security fügt diese Intelligenz zu Ihrer Liste von Indikatorregeln hinzu, zusammen mit Indikatorregeln von anderen Quellen.

HINWEIS: Endpoint Security Version 4.8 oder später unterstützt die Erstellung von benutzerdefinierten Indikatorregeln für Linux Bedingungen (nur Netzwerkereignisse).

WICHTIG: Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

Die Erstellung von Ausführungs-Indikatorregeln von FireEye Appliance Warnungen aktivieren

Sie können die Erstellung von Endpoint Security Appliance Indikatorregeln von NX, EX, FX und AX Appliance Warnungen aktivieren und deaktivieren, die Warnungen auf Malware Rückrufverkehr und Host Infektionen einschließen. Diese Indikatorregeln werden auch als *verrauschte Warnungsindikatorregeln* bezeichnet.

Falsch postiv Ergebnisse können auftreten, wenn Warnungsindikatorregeln aktiviert sind. Falsch positiv Ergebnisse umfassen häufig besuchte Domains, die nicht bösartig sind, falsch positiv Verzeichniseinträge und MD5 Indikatorregeln für Dateien. Aktivieren Sie die Erstellung von verrauschten Warnungsindikatorregeln, wenn Sie glauben, dass Sie mit den möglichen Fehlalarmen umgehen können. Sie sind standardmäßig deaktiviert.

- Verrauschte Warnungsindikatorregeln aktivieren unten
- Verrauschte Warnungsindikatorregeln deaktivieren auf der nächsten Seite
- Feststellen, ob verrauschte Warnungsindikatorregeln aktiviert sind auf der nächsten Seite

Voraussetzungen

- Administratorzugriff

Verrauschte Warnungsindikatorregeln aktivieren

Um die Erstellung von verrauschten Warnungsindikatorregeln zu aktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie die Erstellung von verrauschten Warnungsindikatorregeln:

   ```
   hostname (config) # hx server detection legacy noisy-indicator enable
   ```

Verrauschte Warnungsindikatorregeln deaktivieren

Um die Erstellung von verrauschten Warnungsindikatorregeln zu aktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie die Erstellung von verrauschten Warnungsindikatorregeln:

   ```
   hostname (config) # no hx server detection legacy noisy-indicator
   enable
   ```

Feststellen, ob verrauschte Warnungsindikatorregeln aktiviert sind

Um festzustellen, ob verrauschte Warnungsindikatorregeln aktiviert sind:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Führen Sie Erkennungsbezogene Einstellungen für die HX Appliance auf:

   ```
   hostname (config) # show hx server detection
   ```

   In der Ausgabe von diesem Befehl suchen Sie nach den **Noisy Alert Indicator Generation** Einstellungen. Nachfolgend wird die Beispielausgabe von diesem Befehl mit deaktivierten falschen) verrauschten Warnungsindikatorregeln gezeigt.

   ```
   HX Server Detection Configuration:
   Generated Indicator Aging: enabled
   Generated Indicator Aging Period: 14 days
   Alert Aging Period: 30 days
   False Positive Alert Aging Period: 1 day
   Malicious.URL Indicator Generation: yes
   Noisy Alert Indicator Generation: false
   ```

Benutzerdefinierte Indikatorregeln verwalten

Sie können die Endpoint Security Web-UI verwenden, um benutzerdefinierte Indikatorregeln auf eine der folgenden Arten zu erstellen:

- Sie können eine benutzerdefinierte Indikatorregel erstellen, indem Sie individuelle Bedingungen individuell hinzufügen. Diese individuellen Bedingungen können Host Endpunkte auf Aktivitäten in Bezug zu Netzwerkverbindungen, DNS Suchen und Erstellung oder Veränderung spezifischer Dateien überwachen. Siehe

Benutzerdefinierte Indikatorregeln durch manuelles Hinzufügen von Bedingungen erstellen unten.

- Sie können eine benutzerdefinierte Indikatorregel erstellen, indem Sie eine Liste von Bedingungen hochladen. Siehe Benutzerdefinierte Indikatorregeln durch Hochladen von Bedingungslisten erstellen auf Seite 228.

Benutzerdefinierte Indikatorregeln können auch bearbeitet werden, nachdem Sie erstellt wurden. Siehe Benutzerdefinierte Indikatorregeln mithilfe der Web-UI bearbeiten auf Seite 232.

Sie können benutzerdefinierte Indikatorregeln mit Hilfe der CLI erstellen oder bearbeiten.

WICHTIG: Endpoint Security Version 4.8 oder später unterstützt die Erstellung von benutzerdefinierten Indikatorregeln für Linux Bedingungen (nur Netzwerkereignisse).

Endpoint Security weist Indicators of Compromise (IOCs) ab, die nur eine einzige negierte Bedingung enthalten. Dadurch wird ein möglicher falsch positiv Sturm vermieden, der durch die außer Kraft gesetzte Bedingung hervorgerufen wird. Zum Beispiel könnte ein falsch positiv Sturm durch ein IOC hervorgerufen werden, der nur eine einzige Bedingung enthält, die eine Warnung auslöst, wenn ein MD5 Hash kein spezifischer Wert ist.

Voraussetzungen

- Admin Zugriff
- Wenn Sie beschließen, eine benutzerdefinierte Indikatorregel durch Hochladen einer Liste von Bedingungen zu erstellen, müssen eine oder mehrere ordnungsgemäß formatierte Listen von Bedingungen bereits erstellt werden.

Benutzerdefinierte Indikatorregeln durch manuelles Hinzufügen von Bedingungen erstellen

Sie können individuelle Bedingungen hinzufügen, um benutzerdefinierte Indikatorregeln zu erstellen, die Host Endpunkte für Aktivitäten in Bezug auf Netzwerkverbindungen, DNS Suchen und Erstellung oder Veränderung von bestimmten Dateien überwachen.

- Konventionen für Bedingungen auf der nächsten Seite
- Bedingungen zu einer benutzerdefinierten Indikatorregel in der Web UI hinzufügen. auf Seite 226

Reguläre Ausdrücke, die Sie in Ihren benutzerdefinierten Indikatorregeln verwenden, werden validiert, wenn der regex für eine Dateipfadbedingung ist, die den `matches`

Operator verwendet. Wenn die Regex ungültig ist, wird die folgende Nachricht am oberen Rand der Endpoint Security Web-UI angezeigt:

Konventionen für Bedingungen

Die folgenden Konventionen gelten bei der Erstellung von individuellen Bedingungen für die Verwendung in einer benutzerdefinierten Indikatorregel.

Gültige Operatoren

Diese Bedingungen suchen mit Hilfe der folgenden Operatoren nach Aktivitätswerten:

- *is*, *equal*, oder *matches* suchen nach genauen Übereinstimmungen für den Wert, den Sie für die Bedingung festgelegt haben
- *contains* sucht nach Teilübereinstimmungen mit den gegebenen Informationen
- *is greater than* sucht nach Übereinstimmungen, in denen der Bedingungswert auf dem Host größer als der Wert ist, den Sie für diese Bedingung festgelegt haben.
- *is less than* sucht nach Übereinstimmungen, in denen der Bedingungswert auf dem Host geringer als der Wert ist, den Sie für die Bedingung festgelegt haben.
- *is between* sucht nach Übereinstimmungen, in denen der Bedingungswert auf dem Host in einen Bereich von Werten fällt, den Sie festlegen.

Dateibedingungen

Wenn Sie eine Bedingung für die Überwachung einer Datei hinzufügen, sucht die daraus resultierende Indikatorregel nach dem Vorhandensein auf dem Host einer Datei, die mit den Werten übereinstimmt, die für einige oder alle der folgenden festgelegt haben:

- Dateipfad: *equal*, *contains*, oder *matches*
- MD5: *equal*
- Dateigröße (in Bytes): *equal*

Bedingungen für Netzwerkverbindung

Wenn Sie eine Bedingung für die Überwachung einer Netzwerkverbindung hinzufügen, sucht Ihre Indikatorregel nach der Ausführung von Netzwerkverbindungsaktivitäten, die mit den Werten übereinstimmen, die Sie für einige oder alle der Folgenden festgelegt haben:

- Lokale oder Remote (Ziel) IP-Adressen: *equal*
- Lokale oder Remote (Ziel) Ports: *equal, is greater than, is less than,* und *is between*

Die lokalen und remote Portspezifikationen in einer Netzwerkverbindungsbedingung können nicht Null (0) sein.

DNS Suchbedingungen

Wenn Sie eine Bedingung für die Überwachung einer DNS Suche hinzufügen, sucht die resultierende Indikatorregel nach der Ausführung eines Wertes auf dem Host, den Sie für Folgendes festgelegt haben:

- DNS Suche: *equal, contains oder matches*

Bedingungen für reguläre Ausdrücke

Endpoint Security unterstützt Übereinstimmung regulärer Ausdrücke (regex) in Indikatorregeln für aktuelle Implementationen von RE2. Sie können regex für jeden Bedingungswert eingeben, den Sie zu einer benutzerdefinierten Indikatorregel hinzufügen wollen.

Zum Beispiel:

- Um einen Dateisatz in einem Verzeichnis zu finden:

  `C:\\windows\\`*`filename1`*`|`*`filename2`*`|`*`filename3`*

- Um die gleiche Datei in einem Verzeichnissatz zu finden:

  ```
  (c:\\Windows\\|c:\\Temp\\|c:\\ Program Files)\\malwarebytes.exe)
  ```

- Um Userprofile zu durchsuchen:

  ```
  C:\\(Documents and Settings|Users)\\.*\\.*
  (Documents|Desktop|Downloads)\\malware.exe
  ```

  ```
  C:\\(Documents and Settings|Users)\\.*malware.exe
  ```

  Das erste Beispiel sucht nach der Datei `malware.exe` in jedem Userprofil innerhalb der `Documents`, `Desktop` und `Downloads` Verzeichnisse. Das zweite Beispiel sucht nach der Datei in jedem Dateipfad im `Users` Verzeichnis.

Bedingungen zu einer benutzerdefinierten Indikatorregel in der Web UI hinzufügen.

In diesem Thema erfahren Sie, wie Sie mit Hilfe der Endpoint Security Web-UI eine benutzerdefinierte Indikatorregel erstellen können, indem Sie individuelle Bedingungen hinzufügen. Die folgenden Anweisungen basieren auf den Informationen im folgenden Beispiel.

Angenommen, Sie vermuten, dass eine Datei mit dem Namen `cmd.exe` bösartig ist. Sie können eine benutzerdefinierte Indikatorregel erstellen, damit Ihre Agents die Erstellung oder Veränderung von Dateien mit diesem Namen auf Ihren Hosts überwachen können. Sie wissen, dass die Daten einen Dateipfad von `C:\Windows\system32\cmd.exe`, ein MD5 Hash von `a9a3daa780ca6c9671a19d52456705b4` und eine Größe von 256 Bytes hat.

Benutzerdefinierte Indikatorregeln werden nicht für Linux Bedingungen unterstützt.

Um eine Indikatorregel durch Hinzufügen individueller Bedingungen in der Web UI zu erstellen:

1. Wählen Sie **Rules**, um die Rules Seite aufzurufen.
2. Auf dem Indicators Register klicken Sie auf die **+ Create indicator** Schaltfläche.
3. Auf der Create Indicator Seite bestimmen Sie einen Namen für die Indikatorregel im **Indicator Name** Feld. Indikatorregelnamen können die folgenden Zeichen verwenden:
   - Groß- und Kleinbuchstaben `A` (`a`) bis `Z` (`z`)
   - Positive Zahlen `0` bis `9`
   - Leerzeichen
   - Sonderzeichen: `()-.,_[]`
4. Wählen Sie die Betriebssysteme (**Windows** oder **Mac OS X**), die mit der Indikatorregel verknüpft sind, in der **Operating System** Liste.

   Nehmen Sie das Standard Betriebssystem nicht automatisch an. Stellen Sie sicher, dass Sie ein Betriebssystem auswählen, bevor Sie Bedingungen für den Indikator hinzufügen.

5. Unter **1. Define indicator** wählen Sie den zutreffenden Typ der Bedingung für die Indikatorregel auf (Datei, Netzwerkverbindung oder DNS Suche) in der **Look for** Liste unter Add Individual Conditions und klicken Sie dann auf **Add**.

   Für das obige Beispiel würden Sie **Datei** auswählen. Wenn Sie wollen, dass Agents nach Nachweisen von Netzwerkverbindungen oder DNS Suchen suchen, würden Sie die entsprechende Option in der **Look for** Liste wählen.

6. Im **Look for** Dialogfeld wählen Sie den Typ der benutzerdefinierten Indikatorregel und geben Sie entsprechende Werte ein.

   Für das obige Beispiel würden Sie folgendes eingeben:

   - Für **File Path** wählen Sie *equal* und geben Sie dann `C:\Windows\system32\cmd.exe` ein

Reguläre Ausdrücke, die Sie in Ihren benutzerdefinierten Indikatorregeln verwenden, werden validiert, wenn die Dateipfadbedingung den `matches` Operator verwendet. Wenn die Regex ungültig ist, wird die folgende Nachricht am oberen Rand der Web UI angezeigt:

- Für **MD5** wählen Sie *equal* und geben Sie dann `a9a3daa780ca6c9671a19d52456705b4` ein
- Für **File Size** wählen Sie *equal* und geben Sie dann `256` ein

Wenn Sie fälschlicherweise nur einen Teil eines MD5 Hash oder einer IP-Adresse eingeben, könnte der Eintrag als ein Hostname in einer Bedingung angezeigt werden. Um Konflikte mit vorhandenen Hostnamen zu vermeiden, empfiehlt FireEye, dass Sie diese Bedingungen löschen.

Benutzerdefinierte Indikator-Bedingungswerte können auf maximal 255 ASCII und Escape Unicode Zeichen eingestellt werden. Endpoint Security kürzt hochgeladene Indikatorbedingungen ab, die mehr als 255 Zeichen enthalten. Wenn eine Bedingung abgekürzt wird, können Falsch Positive auftreten.

7. Klicken Sie auf **Add**.

   In dem Abschnitt auf der rechten Seite der **Create Indicator** Seite können Sie die Bedingungen vorschauen, die Sie gerade hinzugefügt haben.

8. Um eine weitere Bedingung hinzuzufügen, wiederholen Sie die vorherigen Schritte.

   Um eine Bedingung zu löschen, bewegen Sie den Mauszeiger darüber und klicken Sie dann auf das **x** Symbol in der oberen rechten Ecke.

9. (Optional) Unter **2. Describe indicator**, können Sie eine Beschreibung des Indikators eingeben.

10. Klicken Sie auf die **Create** Schaltfläche.

    Ihre Indikatorregel wird auf der **Indicators** Seite angezeigt.

Benutzerdefinierte Indikatorregeln durch Hochladen von Bedingungslisten erstellen

Das manuelle Hinzufügen individueller Bedingungen für Indikatorregeln kann unpraktisch sein, wenn Ihre Sicherheitsorganisation regelmäßig große Mengen an Informationen aufnimmt.

Sie können diese Informationen hochladen, indem Sie Listen von Bedingungen erstellen, die für die Erstellung von benutzerdefinierten Indikatorregeln verwendet werden.

- Konventionen für hochgeladene Listen von Bedingungen unten
- Listen von Bedingungen auf eine benutzerdefinierte Indikatorregel in die Web-UI hochladen auf der nächsten Seite

Konventionen für hochgeladene Listen von Bedingungen

Hier finden Sie die allgemeinen Konventionen für das Hochladen von Listen von Bedingungen.

- Erstellen Sie eine Datei für jeden Indikator.
- Jede Datei kann eine Liste von Bedingungen enthalten.
- Dateien sollten entweder im Unix- oder Windows Textformat sein (`*.txt`) Dateien (formatiert mit UTF-8 oder ASCII).
- Jede Datei darf nicht mehr als 10000 Bedingungen enthalten.
- Jede Datei kann nur einen Wert per Zeile enthalten und jede Zeile muss mit einer Zeilenumbruch enden.
- Eine Datei kann eine Mischen von MD5 Hashes, Domainnamen und IP-Adressen enthalten. Ein Domainname ist eine Sequenz alphanumerischer Zeichen und der folgenden drei Sonderzeichen.

  _ (niedrige Linie oder Unterstrich)

  - (hohe Linie oder Bindestrich)

  . (Punkt wird verwendet, um andere Zeichen in der Sequenz zu trennen)

  Wenn Sie versehentlich nur einen Teil eines MD5 Hash oder IP-Adresse eingeben, könnte die Endpoint Security Appliance den Eintrag als einen Domainnamen annehmen (der Eintrag wird als ein Hostname in einer Bedingung angezeigt).

- Verwenden Sie Kommentare im Shell-Stil, um Kommentare oder Bedingungen auszublenden. Fügen Sie ein Nummernzeichen (#) am Anfang jeder Zeile ein, die die Endpoint Security Appliance ignorieren soll.
- Vorangestelltes oder nachfolgendes Leerzeichen und Leerzeilen werden ignoriert.
- Die Endpoint Security Appliances ersetzt doppelte Einträge in einer Liste, aber fügt sie nicht hinzu.

Listen von Bedingungen auf eine benutzerdefinierte Indikatorregel in die Web-UI hochladen

In diesem Thema erfahren Sie, wie Sie mit Hilfe der Endpoint Security Web-UI eine benutzerdefinierte Indikatorregel erstellen können, indem Sie Listen von Bedingungen hochladen.

Benutzerdefinierte Indikatorregeln werden nicht für Linux Bedingungen unterstützt.

Um eine benutzerdefinierte Indikatorregel mit Hilfe hochgeladener Listen von Bedingungen in der Web UI zu erstellen:

1. Wählen Sie **Rules**, um die Rules Seite aufzurufen.
2. Auf dem **Indicators** Register klicken Sie auf die **+ Create indicator** Schaltfläche.
3. Auf der Create Indicator Seite bestimmen Sie einen Namen für die Indikatorregel im **Indicator Name** Feld. Indikatorregelnamen können die folgenden Zeichen verwenden:
   - Groß- und Kleinbuchstaben `A` (`a`) bis `Z` (`z`)
   - Positive Zahlen `0` bis `9`
   - Leerzeichen
   - Sonderzeichen: `()-.,_[]`
4. Wählen Sie die Betriebssysteme (**Windows** oder **Mac OS X**), die mit der Indikatorregel verknüpft sind, in der **Operating System** Liste.

   Nehmen Sie das Standard Betriebssystem nicht automatisch an. Stellen Sie sicher, dass Sie ein Betriebssystem auswählen, bevor Sie Bedingungen für den Indikator hinzufügen.
5. Auf der **Create Indicator** Seite unter **1. Definie indicator** gehen Sie auf **UPLOAD A LIST OF CONDITIONS**. Klicken Sie auf die Browse Schaltfläche neben dem **Browse for intel file** Feld und finden und wählen Sie eine Datei zum Hochladen.
6. Klicken Sie auf **Upload**. Eine Nachricht unter dem **Browse for intel file** Feld zeigt die Anzahl der hochgeladenen Bedingungen und Anzahl der Zeilen in der Datei an.

Wenn Ihre Liste mehr als 10000 Bedingungen enthält oder eine der Bedingungen falsch formatiert ist, wird eine Fehlernachricht angezeigt. Endpoint Security zeigt einen Link auf eine Fehlerliste an, die die Zeilennummer jeder Bedingung mit einem oder mehreren Problemen zeigt, den fehlerhaften Wert und eine Erklärung dieses Fehlers.

Zum Beispiel: *<IP-address> - indicator formatted incorrectly*
(Indikator falsch formatiert)

Die Fehlerliste zeigt auch alle leeren Zeilen und doppelten Einträge in der Datei an. Die Anzahl der hochgeladenen Bedingungen und Zeilen in der ursprünglichen Datei können abweichen, wenn Probleme oder Duplikate vorliegen.

Benutzerdefinierte Indikator-Bedingungswerte können auf maximal 255 ASCII und Escape Unicode Zeichen eingestellt werden. Endpoint Security kürzt hochgeladene Indikatorbedingungen ab, die mehr als 255 Zeichen enthalten. Wenn eine Bedingung abgekürzt wird, können Falsch Positive auftreten.

7. In dem Abschnitt auf der rechten Seite der **Create Indicator** Seite können Sie die Bedingungen vorschauen, die Sie hochgeladen haben.
8. Um zusätzliche Listen mit Bedingungen hochzuladen: wiederholen Sie die vorherigen 2 Schritte. Stellen Sie sicher, dass die **Append to indicator** Option ausgewählt ist. Um individuelle Bedingungen hinzuzufügen, folgen Sie den Anweisungen in Bedingungen zu einer benutzerdefinierten Indikatorregel in der Web UI hinzufügen. auf Seite 226.

   Wiederholen Sie dies, bis Sie alle neuen Bedingungen hinzugefügt haben, die Sie im Indikator einschließen möchten.
9. Im Vorschaufenster bewegen Sie den Mauszeiger über unnötige Bedingungen und klicken Sie auf das **x** Symbol in der oberen rechten Ecke, um sie zu löschen.
10. (Optional) Unter **2. Describe indicator**, können Sie eine Beschreibung des Indikators eingeben.

    Diese Beschreibung wird auf dem **Indicator Details** Register der **Indicators** Seite **Details** Abschnitt angezeigt.
11. Klicken Sie auf die **Create** Schaltfläche auf der rechten Seite.

    Ihre benutzerdefinierte Indikatorregel wird auf der Rules Seite angezeigt.

Benutzerdefinierte Indikatorregeln mithilfe der Web-UI bearbeiten

In diesem Thema erfahren Sie, wie Sie eine benutzerdefinierte Indikatorregel durch Hinzufügen oder Entfernen individueller Bedingungen oder durch Hochladen einer oder mehrerer Listen von Bedingungen bearbeiten können.

Nach Erstellung eines Indikators können Sie die Betriebssysteme, auf die er angewendet wird, nicht ändern. Um das Betriebssystem zu ändern, erstellen Sie eine oder mehrere neue Indikatorregeln für das individuelle Betriebssystem und löschen Sie dann gegebenenfalls den ursprünglichen Indikator.

Voraussetzungen

- Admin Zugriff

Um eine benutzerdefinierte Indikatorregel mit Hilfe der Endpoint Security Web-UI zu bearbeiten:

1. Wählen Sie **Rules**, um die Rules Seite aufzurufen.
2. Auf dem **Indicators** Register im **Indicators** Raster wählen Sie das Kontrollkästchen links neben dem **Custom Indicator**, den Sie bearbeiten wollen.
3. In der **Actions** Liste klicken Sie auf **Edit indicator** und kann auf **Go**.

   Die **Edit Indicators** Seite wird geöffnet.
4. Um individuelle Bedingungen hinzuzufügen:
   - Unter ADD INDIVIDUAL CONDITIONS in der **Look for** Liste wählen Sie die relevante Option und klicken Sie dann auf **Add**.
   - Im **Look for [option]** Dialogfeld geben Sie die zutreffenden Werte und Operatoren ein und klicken Sie dann auf **Add**.

5. Um eine oder mehrere Listen von Bedingungen hinzuzufügen:
    - Auf der **Create Indicator** Seite unter **1. Definie indicator** gehen Sie auf UPLOAD A LIST OF CONDITIONS. Klicken Sie auf die Browse Schaltfläche neben dem **Browse for intel file** Feld und finden und wählen Sie eine Datei zum Hochladen.
    - Klicken Sie auf **Upload**.
    - Wählen Sie eine der folgenden Optionen:
        - Um die Bedingungen in der neuen Liste zu dem vorhandenen Indikator hinzuzufügen, wählen Sie **Append to indicator**.
        - Um die Bedingungen in dem vorhandenen Indikator zu ersetzen, wählen Sie **Replace all conditions**.
6. Um zusätzliche Listen mit Bedingungen hochzuladen: wiederholen Sie den vorherigen Schritt. Um individuelle Bedingungen hinzuzufügen, folgen Sie den Anweisungen in Schritt 4. Stellen Sie sicher, dass die **Append to indicator** Option ausgewählt ist.

   Wiederholen Sie dies, bis Sie alle neuen Bedingungen hinzugefügt haben, die Sie im Indikator einschließen möchten.
7. Überprüfen Sie die Bedingungen im Vorschaufenster.

   Wenn Sie fälschlicherweise nur einen Teil eines MD5 Hash oder IP-Adresse eingeben, könnte der Eintrag als ein Hostname in einer Bedingung angezeigt werden. Um Konflikte mit vorhandenen Hostnamen zu vermeiden, empfiehlt FireEye, dass Sie diese Bedingungen löschen.
8. Im Vorschaufenster bewegen Sie den Mauszeiger über unnötige Bedingungen und klicken Sie auf das **x** Symbol in der oberen rechten Ecke, um sie zu löschen.
9. (Optional) Unter **2. Describe indicator**, können Sie eine Beschreibung des Indikators hinzufügen oder aktualisieren.

   Diese Beschreibung wird auf dem Indicator Details Register im Details Bereich für die Indikatorregel auf der Rules Seite angezeigt.
10. Klicken Sie auf **Save**.

    Ihre aktualisierte Indikatorregel wird auf dem Indicators Register der Rules Seite angezeigt.

Nach Indikatorregeln und Bedingungen suchen

Mit Hilfe der Endpoint Security Web-UI können Sie nach Indikatorregeln und Bedingungen suchen. Sie können nicht mit Hilfe der CLI danach suchen.

Voraussetzungen

- Administrator, Senior Analyst oder Investigator Zugriff.

Um nach Indikatorregeln und Bedingungen zu suchen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Rules**, um die Rules Seite aufzurufen.
3. Wählen Sie den **Indicators** Tab.
4. In dem **Search by name, created by, signature, or condition** Feld geben Sie einen der folgenden Werte ein:
    - Name—der Name der Indikatorregel
    - Created by— der Benutzername oder andere Identifizierung der Quelle der Indikatorregel. Von FireEye bereitgestellte Indikatorregeln haben normalerweise Quellennamen, die mit "General" beginnen.
    - Signature—ein von anderen FireEye Produkten bereitgestellter Wert.
    - Condition value—der Wert der Bedingung, z.B. der MD5 Hashwert oder Dateiname
5. Klicken Sie auf das Vergrößerungsglas auf der rechten Seite des Suchfeldes oder drücken Sie **Eingabe**.

    Die Liste der Indikatorregeln auf dem Indicator Register wird nur nach den Indikatorregeln gefiltert, die mit Ihren Suchkriterien übereinstimmen.

Indikatorregeln löschen

Indikatorregeln können auf verschiedene Arten entfernt werden:

- Benutzerdefinierte Indikatorregeln können manuell entfernt werden.
- Indikatorregeln können automatisch gelöscht (oder gealtert) werden. Siehe Alterung von Indikatorregeln auf der nächsten Seite.

Wenn eine Indikatorregel gelöscht wurde, werden alle zugehörigen Alarme automatisch gelöscht.

Dieses Thema beschreibt die manuelle Löschung von benutzerdefinierten Indikatorregeln mit Hilfe der Endpoint Security Web-UI. Die CLI kann nicht zum Löschen von Indikatorregeln benutzt werden.

Voraussetzungen

- Administrator, Senior Analyst oder Investigator Zugriff.

Um benutzerdefinierte Indikatorregeln mit Hilfe der Web UI manuell zu löschen:

1. Wählen Sie **Rules** am Anfang der Seite. Die Rules Seite wird angezeigt.
2. Auf dem **Indicators** Register im **Indicators** Raster wählen Sie das Kontrollkästchen links neben der Indicatorregel, die Sie löschen wollen.
3. In der **Actions** Liste klicken Sie auf **Delete indicator** und dann auf **Go**.

   Die benutzerdefinierte Indikatorregel wird gelöscht.

Alterung von Indikatorregeln

Alte Indikatorregeln und Bedingungen können für Ihr Unternehmen von begrenztem Wert sein und die Leitung Ihres System und Ihrer Systemanalytiker beeinträchtigen.

Standardmäßig altert (entfernt) die Endpoint Security Software Indikatorregeln automatisch, nachdem ihre definierten Alterungsperioden abgelaufen sind. Bedingungen werden nicht aus der Datenbank entfernt. Stattdessen werden sie von ihren zugehörigen integrationsgenerierten Indikatorregeln getrennt. Benutzerdefinierte Indikatorregeln sind nicht von Alterungsperioden betroffen.

Sie können diese Alterungsperioden ändern. Darüber hinaus können Sie Indikatorregeln und Bedingungen jederzeit manuell löschen.

HINWEIS: Wenn Indikatorregeln gelöscht werden—gleichgültig ob automatisch oder manuell— löscht die Endpoint Security Software automatisch auch alle zugehörigen Alarme. Die Software löscht keine mit den gelöschten Indikatorregeln verbundenen Erfassungen.

- Einstellungen für die Alterung von Indikatorregeln überprüfen auf der nächsten Seite

- Einstellungen für die Alterung von Indikatorregeln festlegen auf der nächsten Seite

Einstellungen für die Alterung von Indikatorregeln überprüfen

Sie können Einstellungen für die Alterung von Indikatorregeln mit Hilfe der Endpoint Security Web-UI oder CLI überprüfen.

- Einstellungen für die Alterung von Indikatorregeln mit Hilfe der Web-UI überprüfen unten
- Einstellungen für die Alterung von Indikatorregeln mit Hilfe der CLI überprüfen unten

Voraussetzungen

- Administratorzugriff

Einstellungen für die Alterung von Indikatorregeln mit Hilfe der Web-UI überprüfen

Um Einstellungen für die Alterung von Indikatorregeln mit Hilfe der Web-UI zu überprüfen

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt. Einstellungen für die Alarm- und Indikatorregelalterung werden im Indicator & Alert Aging Feld auf dieser Seite angezeigt.

Einstellungen für die Alterung von Indikatorregeln mit Hilfe der CLI überprüfen

Um Einstellungen für die Alterung von Indikatorregeln mit Hilfe der CLI zu überprüfen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

```
hostname > enable
hostname # configure terminal
```

2. Führen Sie die Einstellungen für die Indikatorregel und Warnungsalterung auf:

   ```
   hostname (config) # show hx server detection
   ```

   Nachfolgend finden Sie eine Beispielausgabe dieses Befehls:

   ```
   HX Server Detection Configuration:

   Generated Indicator Aging: enabled
   Generated Indicator Aging Period: 14 days
   Generated Condition Aging: enabled
   Generated Condition Aging Period: 30 days
   Source Alert Aging: enabled
   Source Alert Aging Period: 30 days
   Alert Aging Period: 30 days
   False Positive Alert Aging Period: 1 day

   Intel Matching: enabled

   Legacy notification listener active: no
   Malicious.URL Indicator Generation (legacy): yes
   Suspicious (noisy) Indicator Generation (legacy): no

   Inbound alert poll interval: 5 minutes
   Inbound alert minimum severity: majr
   No ignored alert types.

   Last bookmark ID: 0
   ```

Einstellungen für die Alterung von Indikatorregeln festlegen

Die folgende Tabelle fasst die verfügbaren Einstellungen für die Alterung von Indikatorregeln zusammen.

Einstellung	Beschreibung
Indicator Aging Enabled	Aktiviert oder deaktiviert das Alterungsintervall für Indikatorregeln. Wenn das Alterungsintervall erreicht ist, werden Indikatorregeln von der Datenbank entfernt. Wenn Alterung deaktiviert ist, werden Indikatorregeln nicht automatisch entfernt. Das Alterungsintervall für die Indikatorregel kann mit Hilfe der Endpoint Security Web-UI oder CLI aktiviert oder deaktiviert werden. Standardwert: Aktiviert Siehe Alterung von Indikatorregeln aktivieren oder deaktivieren auf Seite 239.

Einstellung	Beschreibung
Indicator Aging Interval	Das Alterungsintervall für die Indikatorregeln (IOC-Regeln) auf dem System. Die Endpoint Security Software altert (löscht) Indikatorregeln, die keine Warnungen für dieses Zeitintervall haben. Wenn Indikatorregel und Warnungsalterung deaktiviert sind, tritt keine Alterung der Indikatorregel auf. Web-UI Bereich: 1 Tag bis 365 Tage CLI Bereich: 60 bis 31536000 Sekunden (1 Minute bis 365 Tage) Standard: 1209600 Sekunden (14 Tage) Siehe Den Alterungsintervall für die Indikatorregel einstellen auf Seite 241.
Condition Aging Enabled	Aktiviert oder deaktiviert das Alterungsintervall für Bedingungen, die von Indikatorregeln aus anderen FireEye Projekten (z. B. NX Serie und der EX Serie Appliances) generiert werden. Das Alterungsintervall für Alarme kann mit Hilfe der CLI aktiviert oder deaktiviert werden. Wenn das Alterungsintervall für die Bedingung erreicht ist, werden Bedingungen nicht von der Datenbank entfernt. Sie werden nur von den zugehörigen Indikatorregeln getrennt. Wenn Alterung von Indikatorregeln und Alarme deaktiviert ist, tritt keine Alterung von Bedingungen auf. Standardwert: Aktiviert Siehe Bedingungsalterung aktivieren oder deaktivieren auf Seite 242.

Einstellung	Beschreibung
Condition Aging Interval	Das Alterungsintervall von Bedingungen auf dem System. Wenn das Alterungsintervall für die Bedingung erreicht ist, werden Bedingungen nicht von der Datenbank entfernt. Sie werden nur von den zugehörigen Indikatorregeln getrennt. Wenn Alterung von Indikatorregeln und Alarme deaktiviert ist, tritt keine Alterung von Bedingungen auf. CLI Bereich: 60 bis 31536000 Sekunden (1 Minute bis 365 Tage) Standardwert: 2592000 Sekunden (30 Tage) Siehe Den Intervall für die Bedingungsalterung mit Hilfe der CLI einstellen auf Seite 243.

Alterung von Indikatorregeln aktivieren oder deaktivieren

Sie können Alterung von Indikatorregeln mit Hilfe der Endpoint Security Web-UI oder der CLI aktivieren oder deaktivieren.

- Alterung für Indikatorregeln mit Hilfe der Web-UI aktivieren unten
- Alterung für Indikatorregeln mit Hilfe der CLI aktivieren auf der nächsten Seite
- Alterung für Indikatorregeln mit Hilfe der Web-UI deaktivieren auf der nächsten Seite
- Alterung für Indikatorregeln mit Hilfe der CLI deaktivieren auf Seite 241

Voraussetzungen

- Administratorzugriff

Alterung für Indikatorregeln mit Hilfe der Web-UI aktivieren

Um die Alterung der Indikatorregel mithilfe der Web-UI zu aktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt.

3. Im Indicator & Alert Aging Feld auf der Aging Settings Seite geben Sie ein Alterungsintervall im **Delete indicator when it's had no alerts for:** Feld ein. Gültige Werte liegen zwischen 1 bis 365 Tagen. Dies stellt das Alterungsintervall ein und aktiviert es.
4. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

Um Standardeinstellungen wiederherzustellen, klicken Sie auf **Reset to default** und klicken Sie dann auf **Save**. Wenn Sie auf **Cancel** klicken, gibt Endpoint Security Einstellungen auf die zuletzt gespeicherten Werte zurück.

Alterung für Indikatorregeln mit Hilfe der CLI aktivieren

Um die Alterung der Indikatorregel mithilfe der CLI zu aktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie das Alterungsintervall der Indikatorregel:

   ```
   hostname (config) # hx server detection aging indicator generated
   enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Alterung für Indikatorregeln mit Hilfe der Web-UI deaktivieren

Um die Alterung von Indikatorregeln mit Hilfe der Web-UI zu deaktivieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt.
3. Im Indicator & Alert Aging Feld auf der Aging Settings Seite wählen Sie die **No auto-deletion; I will delete indicator rules manually** Option.
4. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

Um Standardeinstellungen wiederherzustellen, klicken Sie auf **Reset to default** und klicken Sie dann auf **Save**. Wenn Sie auf **Cancel** klicken, gibt Endpoint Security Einstellungen auf die zuletzt gespeicherten Werte zurück.

Alterung für Indikatorregeln mit Hilfe der CLI deaktivieren

Um die Alterung der Indikatorregel mithilfe der CLI zu deaktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie das Alterungsintervall der Indikatorregel:

   ```
   hostname (config) # no hx server detection aging indicator generated
   enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Den Alterungsintervall für die Indikatorregel einstellen

Sie können das Alterungsintervall für die Indikatorregel mit Hilfe der Endpoint Security Web-UI oder der CLI einstellen.

Voraussetzungen

- Administratorzugriff

Den Alterungsintervall für die Indikatorregel mit Hilfe der Web-UI einstellen

Um den Alterungsintervall für die Indikatorregel mit Hilfe der Web-UI einzustellen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Aging Settings** auf dem **Admin** Menü. Die Aging Settings Seite wird angezeigt.
3. Im Indicator & Alert Aging Feld auf der Aging Settings Seite geben Sie ein Alterungsintervall im **Delete indicator when it's had no alerts for:** Feld ein. Gültige Werte liegen zwischen 1 bis 365 Tagen. Dies stellt das Alterungsintervall ein und aktiviert es.
4. Klicken Sie auf **Save**, um Ihre Änderungen zu speichern.

Um Standardeinstellungen wiederherzustellen, klicken Sie auf **Reset to default** und klicken Sie dann auf **Save**. Wenn Sie auf **Cancel** klicken, gibt Endpoint Security Einstellungen auf die zuletzt gespeicherten Werte zurück.

Den Alterungsintervall für die Indikatorregel mit Hilfe der CLI einstellen

Um den Alterungsintervall für die Indikatorregel mit Hilfe der CLI einzustellen:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Stellen Sie den Alterungsintervall für die Indikatorregel ein:

   ```
   hostname (config) # hx server detection aging indicator generated
   period <seconds>
   ```

   wobei <seconds> die Anzahl von Sekunden für die Alterungsperiode für Indikatorregeln ist. Der Standardwert ist 1209600 Sekunden (14 Tage). Gültige Werte liegen zwischen 60 und 31536000 Sekunden (ein Jahr).

   Um dieses Intervall auf seine Standardeinstellung zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   hostname (config) # no hx server detection aging indicator generated
   period
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Bedingungsalterung aktivieren oder deaktivieren

Sie können Bedingungsalterung mit Hilfe der CLI aktivieren oder deaktivieren.

- Bedingungsalterung mit Hilfe der CLI aktivieren unten
- Bedingungsalterung mit Hilfe der CLI deaktivieren auf der nächsten Seite

Voraussetzungen

- Administratorzugriff

Bedingungsalterung mit Hilfe der CLI aktivieren

Um Bedingungsalterung mit Hilfe der CLI zu deaktivieren

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie den Intervall für die Bedingungsalterung:

   ```
   hostname (config) # hx server detection aging condition generated
   enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Bedingungsalterung mit Hilfe der CLI deaktivieren

Um Bedingungsalterung mit Hilfe der CLI zu deaktivieren:

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie den Intervall für die Bedingungsalterung:

   ```
   hostname (config) # no hx server detection aging condition generated
   enable
   ```

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

Den Intervall für die Bedingungsalterung mit Hilfe der CLI einstellen

Um den Intervall für die Bedingungsalterung mit Hilfe der CLI einzustellen

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Legen Sie den Intervall für die Bedingungsalterung fest:

   ```
   hostname (config) # hx server detection aging condition generated
   period <seconds>
   ```

   wobei <seconds> die Anzahl der Sekunden für die Alterungsperiode für Bedingungen ist. Der Standardwert ist 2592000 Sekunden (30 Tage). Gültige Werte liegen zwischen 60 und 31536000 Sekunden (ein Jahr).

3. Speichern Sie Ihre Einstellungen.

   ```
   hostname (config) # write mem
   ```

KAPITEL 14: Exploit Guard konfigurieren

Endpoint Security Agent Software Version 21 oder später unterstützt Exploit Erkennung, eine Komponente von Exploit Guard. Endpoint Security AgentVersion 23 oder später unterstützt Exploit Prävention, eine weitere Komponente von Exploit Guard.

Exploit Guard Komponenten verwenden eine interne Regeldatei und eine Ausschlussdatei, die allgemeine Dateien aufführen, die von Exploit Cuard Verarbeitung ausgeschlossen werden sollen. Diese Dateien werden nur von FireEye bereitgestellt. Aktualisierungen für die Regeln und Ausschlussdateien werden automatisch über die FireEye Dynamic Threat Intelligence (DTI) Cloud bereitgestellt.

HINWEIS: Exploit Guard wird für Desktop-Betriebssysteme Windows XP SP3, 7, 8 und 10 sowie Windows Server-Betriebssysteme 2008, 2012 und 2016 unterstützt. Das Betriebssystem wird von dem Agent automatisch erkannt.

Exploit Guard wird nicht auf Endpunkten unterstützt, auf denen die überwachten Appliances (Adobe Reader, Adobe Flash, Microsoft Edge, Firefox, Google Chrome, Java, Microsoft Outlook, Microsoft Word, Microsoft Excel und Microsoft PowerPoint) von einem virtuellen Anwendungsserver gestreamt werden, wie z.B. App-V, Xenapp oder VMware ThinApp. Schließen Sie gestreamte Anwendungen von der Exploit Guard Verarbeitung für die betroffenen Endpunkte aus. Wenn alle Ihre Endpunkte betroffen sind, verwenden Sie eine globale Richtlinie; wenn nur ein paar Endpunkte betroffen sind, verwenden Sie Hostsätze in einer Ausnahmerichtlinie.

WICHTIG: Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

Sie können für Ihre Organisation spezifische Richtlinien für Exploit Guard einstellen. Mit Hilfe dieser Richtlinien können Sie:

- Exploit Guard für alle Host Endpunkte ein- und ausschalten.
- Eine für Ihre Installation für alle Host Endpunkte globale Richtlinie verwalten, die Ihnen ermöglicht, globale Exploit Guard Optionen festzulegen.
- Eine Ausnahmerichtlinie für ausgewählte Hostsätze verwalten

Informationen zum Definieren von Exploit Guard Richtlinien und zum Verwalten von Exploit Guard finden Sie im *Endpoint Security Agent Administrationshandbuch*.

KAPITEL 15: Malware Schutz konfigurieren

Malware Schutz schützt Ihre Endpunkte vor Viren, Trojanern, Würmern, Spyware, Adware, Keyloggern, Rootkits, Phishing-Software und anderen potentiell unerwünschten Programmen (PUP). Malware Schutz umfasst eine Signatur und heuristische Erkennungs-Engine (Antivirus) sowie MalwareGuard, ein Machine-Learning Modell, um eine zusätzliche Schutzschicht gegen portierbare ausführbare (PE) Dateien.

MalwareGuard verwendet statische Analyse für die Erkennung von Malware, einschließlich Ransomware und neue Malware Varianten, die nahezu in Echtzeit für portierbare ausführbare (PE) Dateien ausgeführt werden. (PE ist ein exe, dll, sys, drv, mui, cpl und scr Dateien sowohl in 32-Bit und 64-Bit Versionen des Windows Betriebssystem zugeordnetes Dateiformat.)

HINWEIS: Malware Erkennung wird für Endpoint Security Agents unterstützt, die Version 24 oder später in spezifischen Windows Umgebungen ausführen, sowie Version 32 oder später in macOS Umgebungen und Version 34 für Linux Umgebungen.

Malware Schutz (Quarantäne und Beseitigung) wird für Endpoint Security Agents unterstützt, die Version 26 oder später in spezifischen Windows Umgebungen ausführen.

Die Malware-Erkennung wird für die Scan-Now Funktion für Endpunkte unterstützt, die in Linux Umgebungen ausgeführt werden, aber die Malware Beseitigung wird nicht unterstützt.

Sowohl On-Access als auch On-Demand (geplante) Malware Scans werden unterstützt.

- On-Access Malware Scans treten auf, wenn Dateien erstellt, ausgeführt oder geöffnet werden. Zu den erstellten Dateien gehören Dateien, die von einem Internet Browser heruntergeladen wurden, neue, auf dem Host durch einen beliebigen Prozess erstellte Dateien, aus Archiven extrahierte Dateien und Dateien, die durch Kopieren und Einfügen erstellt wurden. Ausgeführte Dateien sind Dateien, die einen Prozess starten. Geöffnete Dateien umfassen vorhandene Dateien, die im Windows Explorer,

von Medien wie einem USB- oder CD / DVD-Laufwerk und von Netzwerkordnern geöffnet wurden.

- On-Demand Malware Scans (geplant) können nach Zeit oder Ereignis geplant werden. Vollständige Scans, Kurzscans und Speicherscans (die laufende Prozesse scannen) können angefordert werden. Neue Scans werden nicht ausgeführt, wenn ein zuvor geplanter Scan noch läuft. Je nachdem, wie Sie die Einstellungen Ihrer Malware Scans konfigurieren, können Endbenutzer einen laufenden, geplanten Scan anhalten oder abbrechen.

Malware Schutz erkennt Malware in jeder Datei in Ihrer Umgebung automatisch, je nach den unten angegebenen Beschränkungen für Dateigröße.

Scantyp	Größenbeschränkung Antivirus / MalwareGuard
On-Access	2 GB / 12 MB
On-demand	2 GB / 100 MB

VORSICHT: Obwohl Sie die Dateigrößenbeschränkung mit Hilfe der API verändern können, wirkt sich die Erhöhung der Werte für Max File Size oder Scan Timeout möglicherweise auf die Systemleistung aus.

Standardmäßig sind Malware Erkennung und Prävention (Beseitigung und Quarantäne) deaktiviert. Wenn Malware Erkennung deaktiviert ist, findet kein Malware Schutz statt.

Die von den FireEye Malware Schutz-Engines verwendeten Malware Definition Updates werden von FireEye Servern heruntergeladen, die eine direkte Internetverbindung benötigen. Sie in der Dynamic Threat Intelligence (DTI) Cloud der FireEye nicht verfügbar.

- Aktualisierungen der Malware Definition benötigen eine direkte Internetverbindung mit den FireEye Malware Definitionsservern. Für Updates für Host-Endpunkte, die offline oder im lokalen Modus ausgeführt werden, können Sie die Quell-Definition auf einen lokalen Speicherort speichern und dann die Custom Source Download-Option verwenden.
- Aktualisierungen der Malware Definition über den Proxyserver werden in FireEye Endpoint Security Agent Version 25 oder später unterstützt.
- Updates für Malware Definitionen werden nicht ausgeführt, wenn die CONTENT_ UPDATES Lizenz für Ihren Endpoint Security abgelaufen ist.
- Malware Erkennung wird nur für Host Endpunkte mit installierter FireEye Endpoint Security Agent Version 24 oder später bereitgestellt. Malware Beseitigung wird nur für Host-Endpunkte mit installierter FireEye Endpoint Security Agent Version 26 oder später bereitgestellt

Wenn der Endpoint Security ein Update beginnt, wählt er einen zufälligen Intervall für den Inhaltsdownload zwischen 0 und dem konfigurierten Abfrageintervall, der standardmäßig Sekunden (4 Stunden) betrifft.Agent Wenn das Download nicht erfolgreich ist, oder der Inhalt beschädigt ist, versucht der Endpoint Security Agent das Download in einem anderen zufälligen Intervall. Nach erfolgreichem Download wird der Aktualisierungsvorgang bis zum nächsten Malware Definition Rules Intervall angehalten.

Wählen Sie eine Methode zum Herunterladen von Malware-Definitionen:

- Internet (Standard): Aktualisierungen der Malware Definition benötigen eine direkte Internetverbindung mit den FireEye Malware Definition Servern.
- HX Only: Laden Sie Aktualisierungen der Malware-Definition über einen Proxy-Server herunter. Dies wird in FireEye Endpoint Security Agent Version 26 oder später unterstützt.
- HX Preferred:: Laden Sie Aktualisierungen der Malware-Definition über einen Proxy-Server herunter. Dies wird in FireEye Endpoint Security Agent Version 26 oder später unterstützt.
- Benutzerdefinierte Quelle: Laden Sie Updates der Malware-Definition von einem benutzerdefinierten Speicherort herunter, um die Internetnutzung zu vermeiden.

In regelmäßigen Abständen werden falsch positiv Malware Informationen automatisch von der FireEye Dynamic Threat Intelligence (DTI) Cloud auf den Endpoint Security Server heruntergeladen. Wenn FireEye Endpoint Security Agents die Appliance abfragen, werden falsch positiv Daten automatisch auf die Endpunkte angewendet. Vorhandene Warnungen auf dem Endpoint Security, die mit den falsch positiv Bedingungen übereinstimmen, werden als falsch positiv markiert.

WICHTIG: Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

Wenn Malware erkannt wird, wird eine Malware Warnung generiert, die in der Endpoint Security Web-UI sichtbar ist. Je nach den Einstellungen Ihres konfigurierbaren Malware Schutzes können Sie anfordern, dass die folgenden Korrekturmaßnahmen durchgeführt werden.

- Die infizierte Datei kann automatisch in einem Quarantänebereich unter Quarantäne gestellt werden. Wenn Sie Korrekturmaßnahmen (Quarantäne) aktivieren, geschieht dies automatisch. Quarantänedateien werden in einem Quarantänebereich gespeichert und nach einer konfigurierbaren Alterungszeit gelöscht. Durch Alterung von Dateien unter Quarantäne können Platzprobleme vermieden werden. Analysten können Quarantänedateien nach Bedarf erfassen, löschen und wiederherstellen.

- Sie können versuchen, die Infektion von der Datei zu bereinigen (entfernen). Dateien, die nicht bereinigt werden können, werden vom Endpunktsystem gelöscht. Erfolgreich bereinigte Dateien werden nicht isoliert.
- Endbenutzer können benachrichtigt werden, wenn eine infizierte Datei unter Quarantäne steht oder bereinigt wird.
- Malware Spuren (von der Malware erstellte Artefakte) können nach Bedarf entfernt oder wiederhergestellt werden.

HINWEIS: Von MalwareGuard generierte Alarme besitzen einen eindeutigen Subtyp ("mg"), um sie von durch Antivirus erkannten Warnungen (Subtyp "av") zu unterscheiden. Sie können Warnungen nach Subtyp in der /alerts API filtern.

Für Malware Regeln produzierte Warnungen werden auf die gleiche Art gealtert wie Indicator of Compromise (IOC) oder Exploit Regeln. Siehe Alterung von Indikatorregeln auf Seite 235. Malware Warnungen lösen keine automatische Triage aus, wie dies bei anderen Warnungen der Fall ist.

FireEye **empfiehlt dringend**, dass Sie Prozess- und Ordnerausschlüsse für den Malware Schutz für alle Software von Drittanbietern zu erstellen, die Sie auf Ihren Host-Endpunkten installiert haben. Dadurch wird die Leistung maximiert, die Kompatibilität mit anderer Antivirensoftware sichergestellt und die Anzahl der doppelten Alarme reduziert, die Sie von der Endpoint Security Malware Schutzfunktion und Antivirus-Software von Drittanbietern erhalten. Verwenden Sie die globale Richtlinie zum Schutz vor Malware, um diese Ausnahmen zu definieren. Lesen Sie "Globale Richtlinie für die Malware Erkennung definieren" im *Endpoint Security Agent Administrationshandbuch*.

Darüber hinaus sollten Sie die Endpoint Security Dateien in Ihrer Antivirus Software von Drittanbietern auf die Whiteliste setzen, wie unter "Agentdateien in Ihrer Antivirus-Software ausschließen" im *Endpoint Security Agent Administrationshandbuch* beschrieben.

Wenn Sie beispielsweise Symantec Endpoint Protection (SEP) ausführen, sollten Sie Ausschlüsse in SEP für Endpoint Security Prozesse und Ordner erstellen.Agent Darüber hinaus sollten Sie Ausschlüsse für SEP Prozesse und Ordner in der globalen Richtlinie für den Endpoint Security Malware Schutz erstellen.Agent

Sie können für Ihre Organisation spezifische Richtlinien und Einstellungen für den Malware Schutz definieren. Mit Hilfe dieser Richtlinien und Einstellung können Sie:

- Malware Erkennung für alle Host-Endpunkte oder für ausgewählte Hostsätze aktivieren oder deaktivieren
- Korrekturaktionen (Quarantäne) für alle Host Endpunkte oder für ausgewählte Hostsätze aktivieren oder deaktivieren

- Eine globale, für Ihre Installation auf allen Host Endpunkten spezifische Malware Richtlinie erstellen, die Ihnen ermöglicht, Optionen für globalen Malware Schutz festzulegen
- Eine Ausnahme Malware Richtlinie für ausgewählte Hostsätze erstellen
- Festlegen, wie lange Dateien unter Quarantäne im Quarantänebereich gehalten werden
- Scan bei der Installation aktivieren oder deaktivieren
- Geplante Scans aktivieren oder deaktivieren und bis zu zehn globale geplante Scans und bis zu zehn Ausnahmen für geplante Scans definieren
- Festlegen, ob geplante oder nicht geplante Scans von Endpunktbenutzern abgebrochen oder pausiert werden können und die Länge und Häufigkeit der Pausen für geplante Scans definieren

Informationen über die Definition von Malware Schutz Richtlinien und Einstellungen, sowie über die Verwaltung von Malware Schutz, einschließlich MalwareGuard finden Sie im *Endpoint Security Agent Administrationshandbuch*.

TEIL III: Ihr Unternehmen durchsuchen

Verwenden Sie die Enterprise Search Funktion, um alle Host Endpunkte in Ihrem Unternehmen nach bestimmten Bedrohungsindikatorregeln zu durchsuchen. Die Ergebnisse werden für Schnellsuchen schnell zurückgegeben, wobei Speicherorte übersprungen werden, deren Durchsuchung zeitaufwendig und kostspielig ist. Wenn die Ergebnisse der Schnellsuche jedoch nicht ausreichen, können Sie die Suche erweitern, um übersprungene Speicherorte einzuschließen (dies wird als ausführliche Suche *bezeichnet).*

Enterprise Search Abfragen können nur für Windows, macOS und Linux Host-Endpunkte durchgeführt werden, auf denen Endpoint Security Agent Version 34 oder später ausgeführt wird.

Stellen Sie sicher, dass Sie alle Enterprise Search Abfragen vor dem Durchführen eines Appliance Upgrades stoppen. Wenn Sie Enterprise Search Abfragen und ein Appliance Upgrade gleichzeitig ausführen, kann sich dies auf die Leistung des Upgrades auswirken.

Schnellsuchabfragen für ein ganz spezifisches Datenstück resultieren in einer Liste von Hosts, die mit der Abfrage übereinstimmen. Sie können die durch die Abfrage zurückgegebene Liste der Hosts gruppieren und sehen, wie viele Hosts mit der Abfrage übereinstimmen sowie wie oft Ergebnisse auf jedem Host gefunden wurden.

Bei ausführlichen Suchabfragen handelt es sich um tiefer gehende Abfragen mit zusätzlichen Optionen und sie dauern deshalb länger als Schnellsuchen. Diese Suchvorgänge erfordern, dass der Agent auf dem Host eine vollständigere Suche durchführt. Unter bestimmten Umständen erfasst der Agent nicht regelmäßig alle Daten, die Sie benötigen. Beispielsweise werden nicht alle Verzeichnisaktivitäten regelmäßig von Agenten erfasst. Sie können eine ausführliche Suche des Verzeichnisses anfordern, um sicherzustellen, dass das gesamte Verzeichnis durchsucht wird.

Ein Beispiel einer Schnellsuchabfrage ist eine Abfrage für alle in Ihrem Unternehmen verwendeten Browser. Ein Beispiel für eine ausführliche Suche ist eine Abfrage nach den

Pfaden auf jedem Host in Ihrem Unternehmen, auf denen eine bestimmte MD5 Datei gefunden wird.

Dieser Teil behandelt die folgenden Themen:

- Suchmodi verstehen auf Seite 255
- Suchvorgänge erstellen und verwalten auf Seite 257
- Suchergebnisse überprüfen auf Seite 269
- Suchtoken Referenz auf Seite 273

Das Zeitlimit für die Inaktivität der Endpoint Security Web-UI wird ignoriert, wenn eine aktive Enterprise Search ausgeführt wird und die Enterprise Search Seite im Browser geöffnet bleibt.

KAPITEL 16: Suchmodi verstehen

Es gibt zwei Modi für Enterprise Searches: *Host-Modus* und *Grid* Modus. Jeder meldet Ergebnisse anders.

Host Modus

Host Modus Suchen zeigen Ergebnisse eine Suche nach eindeutigem Host an. Dies ist der Standard Modus.

Eine Liste der Hosts, die eine oder mehrere Übereinstimmungen mit der Suchabfrage enthalten, wird zurückgegeben. Suchvorgänge im Host Modus werden hauptsächlich dazu verwendet, Dinge zu finden, von denen Sie annehmen, dass sie in Ihrem Unternehmen selten sind. Sie können beispielsweise eine Suche im Host Modus verwenden, um festzustellen, ob auf einem Ihrer Endpunkte eine ausführbare Datei ausgeführt wird.

Grid Modus

Der Grid (Raster) Modus, auch Group By Modus genannt, gruppiert die Suchergebnisse nach einem oder mehreren ausgewählten Feldern, fasst die Ergebnisse nach den angegebenen Feldern zusammen und präsentiert sie in einem Raster. Der Grid Modus wird aktiviert, wenn Sie das **Group By** Token als letztes Token in Ihrem Suchbegriff festlegen. Durch Hinzufügen des **Group By** Tokens zu einer Suche wird die Suche von einer Host Modus Suche auf eine Grid Modus Suche geändert.

Der Group By Modus wird verwendet, um einzigartige Wertkombinationen zu finden, die auf Ihren Endpunkten vorhanden sind. Sie können zum Beispiel eine Group By Suche ausführen, um ein bekannte fehlerhafte IP-Adresse zu finden und alle Ports zu identifizieren, die diese IP für die Kommunikation verwendet (IP-Adresse entspricht 192.168.1.1 AND Group By Port).

Die Ergebnisse des Grid Modus werden in einem Raster dargestellt.

Sie können auf die Liste der in jeder Gruppe enthaltenen Hosts zugreifen, indem Sie auf die Host Anzahl klicken, die einer bestimmten Rasterlinie zugeordnet ist. Die Hosts Seite wird nur mit diesen Hosts angezeigt.

Group By muss die letzte in der Suche festgelegte Token-Zeichenfolge sein, wenn es in der Suchleiste als ein Suchtoken festgelegt ist.

KAPITEL 17: Suchvorgänge erstellen und verwalten

Enterprise Search Abfragen können nur für Windows und macOS Endpunkte, sowie Linux Endpunkte, die Endpoint Security Agent Version 34 oder später ausführen, durchgeführt werden.

In diesem Kapitel wird beschrieben, wie Sie mit Hilfe der Enterprise Search Seite in der Endpoint Security Web-UI eine Suchanfrage erstellen, starten, stoppen und löschen können.

Voraussetzungen

- Administrator, Analyst, Senior Analyst, API Analyst oder Investigator Berechtigungen (Vollzugriff)
- Die umfassende Suchfunktion ist nur für Enterprise Suchen verfügbar, wenn Sie eine Endpoint Security Power Lizenz installiert haben. Sehen Sie "Lizenzverwaltung" im *Endpoint Security Server-System-Administrationshandbuch*.

Die Enterprise Search Seite abrufen

Zu die Enterprise Search Seite abzurufen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Enterprise Search** am Anfang der Web UI Seite.

Suchbegriffe erstellen

Verwenden Sie die Suchleiste auf der Enterprise Search Seite, um Suchbedingungen zu erstellen und Ihre Suche zu starten. Suchbedingungen sind Token Zeichenfolgen, die mit Hilfe von Token, Operatoren und Werten erstellt werden. In einem Suchbegriff kann mehr als eine Bedingung (Token-Zeichenfolge) festgelegt werden. Allerdings wird die Liste der verfügbaren Token mit wachsenden Suchbegriffen eingeschränkt. Dies liegt daran, dass bestimmte Token automatisch die Verwendung anderer Token im selben Suchausdruck eliminieren. Beschreibungen für jedes Token finden Sie unter Suchtoken Referenz auf Seite 273. Weitere Informationen zu den Einschränkungen von Enterprise-Searches finden Sie unter Suchlimits auf Seite 264

Zwei spezielle Token sind für Bedingungen verfügbar:

- Der Host Set Token ermöglicht Ihnen, die Suche auf einen bestimmten Hostsatz zu beschränken. Standardmäßig ist der Suchwert für dieses Token auf **All hosts** eingestellt (einen interner Hostsatz umfasst alle dem Endpoint Security bekannten Hosts).
- Das Group By Token ermöglicht Ihnen, Ergebnisse im Grid (Raster) Modus anzuzeigen (auch Group By Modus genannt). Dieser Modus gruppiert Suchergebnisse nach einem oder mehreren ausgewählten Feldern, fasst die Ergebnisse nach den Felder zusammen und zeigt sie in einem Raster an. Wenn festgelegt muss Group By das letzte Token in dem Suchbegriff sein. Siehe Suchmodi verstehen auf Seite 255.

Dieser Abschnitt behandelt die folgenden Themen:

Eine Schnellsuche erstellen

Befolgen Sie die Anweisungen in diesem Abschnitt, um mit der Erstellung von Suchen mit Hilfe der integrierten Eingabeaufforderungen für die Suchbedingungen zu beginnen. Suchbedingungen sind Token Zeichenfolgen, die mit Hilfe von Token, Operatoren und Werten erstellt werden.

Um eine Schnellsuche zu erstellen:

1. Wählen Sie **Enterprise Search** in der Endpoint Security Web-UI.
2. Klicken Sie auf das Pluszeichen (+) auf der linken Seite der Suchleiste und wählen Sie ein Token von der Dropdown-Liste. Siehe Suchtoken Referenz auf Seite 273.

   Die Dropdown-Liste bietet einen Filterbereich, mit dem Sie Ihr Token schnell finden können. Beginnen Sie mit der Eingabe des Tokennamens. Die Token, die mit den eingegebenen Zeichen übereinstimmen, werden angezeigt.
3. Wählen Sie eine Operatorschaltfläche aus der Zeile am Ende der Dropdown-Liste. Siehe Suchbedingungsoperatoren auf Seite 263.
4. Geben Sie den Wert oder die Werte an, nach denen Sie suchen möchten. Es werden keine Platzhalterzeichen unterstützt.

   Achten Sie darauf, alle nachfolgenden Leerzeichen in den angegebenen Werten zu entfernen. Enterprise Search entfernt diese nachgestellten Leerzeichen nicht und Ihre Suche kann deshalb fehlschlagen.
5. Wiederholen Sie die vorherigen Schritte, um Bedingungen zu dem Suchbegriff hinzuzufügen.

   Wenn Japanische oder Chinesische Zeigen in der Enterprise Search Leiste mit Hilfe eines Japanischen oder Chinesischen Input Method Editor (IME) in Firefox oder Microsoft Edge eingegeben werden, bewegt sich der Cursor unerwartet oder beginnt mit der Suche, bevor die Suchanfrage abgeschlossen ist.

   Wenn Sie in der Suchleiste auf das Ende der Suchzeichenfolge klicken, wird eine Nachricht angezeigt, die angibt, welche Arten von Host Endpunkten die Suche ausführen können.
6. Beginnen Sie die Suche. Siehe Eine Suche beginnen auf Seite 266.

Eine ausführliche Suche erstellen

Sie können eine ausführliche Suche nach Bedingungen durchführen, die bestimmte Token enthalten. Einige Token *erfordern* eine ausführliche Suche. Wenn allerdings eine Bedingung in einer Enterprise Search keine ausführliche Suche unterstützt, wird keine umfassende Suche durchgeführt. Um zu bestimmen, welche Token ausführliche Suchen zulassen und welche ausführliche Suchen erfordern, lesen Sie die Suchtoken Referenz auf Seite 273.

Um eine ausführliche Suche durchzuführen, müssen Sie eine Endpoint Security Power Lizenz haben.

Um eine ausführliche Suche zu erstellen:

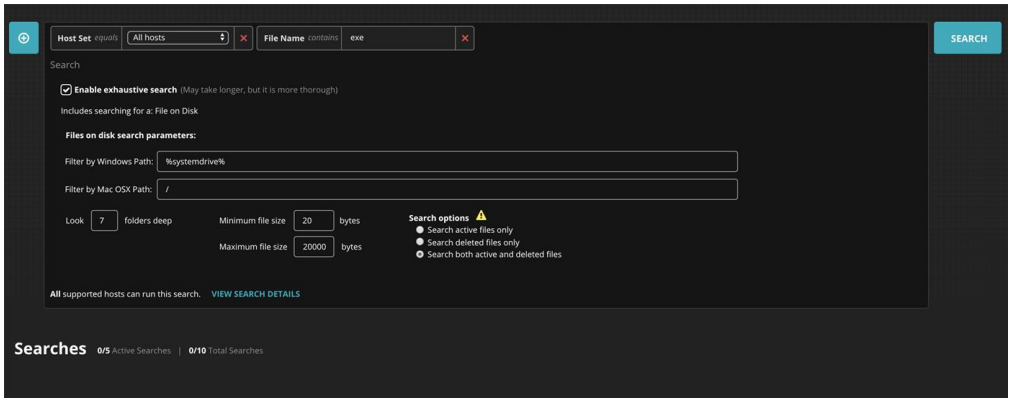
1. Wählen Sie **Enterprise Search** in der Endpoint Security Web-UI.
2. Klicken Sie auf das Pluszeichen (+) auf der linken Seite der Suchleiste und wählen Sie ein Token von der Dropdown-Liste, das eine ausführliche Suche zulässt. Siehe Suchtoken Referenz auf Seite 273.

   Die Dropdown-Liste bietet einen Filterbereich, mit dem Sie Ihr Token schnell finden können. Beginnen Sie mit der Eingabe des Tokennamens. Die Token, die mit den eingegebenen Zeichen übereinstimmen, werden angezeigt.
3. Wählen Sie einen Operator in der Dropdown-Liste. Siehe Suchbedingungsoperatoren auf Seite 263.
4. Geben Sie den Tokenwert oder -werte an, nach denen Sie suchen möchten. Es werden keine Platzhalterzeichen unterstützt.

   Entfernen Sie alle nachgestellten Leerzeichen in den von Ihnen angegebenen Werten. Enterprise Search entfernt diese nachgestellten Leerzeichen nicht und Ihre Suche kann deshalb fehlschlagen.

   Wenn Japanische oder Chinesische Zeigen in der Enterprise Search Leiste mit Hilfe eines Japanischen oder Chinesischen Input Method Editor (IME) in Firefox oder Internet Explorer 11 eingegeben werden, bewegt sich der Cursor unerwartet oder beginnt mit der Suche, bevor die Suchanfrage abgeschlossen ist.

   Wenn Sie in der Suchleiste auf das Ende der Suchzeichenfolge klicken, wird eine Nachricht angezeigt, die angibt, welche Arten von Host Endpunkten die Suche ausführen können.
5. Wählen Sie **Enable exhaustive search**. Der exhaustive search Bereich wird erweitert.



6. Optional können Sie Werte für ausführliche Suchoptionen eingeben, wie unter Optionen für ausführliche Suche unten beschrieben.
7. Nachdem alle optionalen ausführlichen Suchoptionen festgelegt sind, starten Sie die Suche. Siehe Eine Suche beginnen auf Seite 266.

Optionen für ausführliche Suche

Die folgenden möglichen ausführlichen Suchoptionen sind für einige Suchtoken verfügbar.

Option	Beschreibung
Filter by macOS Path	Bestimmen Sie den macOS Pfad, auf dem Sie die Suche ausführen wollen.
Filter by Windows path	Bestimmen Sie den Windows Pfad, auf dem die Suche durchgeführt werden soll. Die Umgebungsvariable `%systemdrive%` (C: \) ist der Standardwert. Bestimmen Sie einen genauen Pfadnamen oder eine andere geeignete, pfad-basierte Windows Umgebungsvariable. Hier sind einige Beispiele anderer gültiger Windows Umgebungsvariablen:
Filter by Registry Hive	Bestimmen Sie die Registrierungsstruktur, auf der die Suche durchgeführt werden soll.

`%appdata%`	`C:\Users\{username}\AppData\Roaming`
`%commonprogramfiles%`	`C:\Program Files (x86)\Common Files` (x86)
`%localappdata%`	`C:\Users\{username}\AppData\Local`
`%programdata%`	`C:\ProgramData`
`%programfiles%`	`C:\Program Files`
`%systemdrive%`	`C:\`
`%systemroot%`	der Pfad, auf dem Windows installiert ist, normalerweise `C:\Windows`
`%temp%%tmp%`	`C:\Users\{Username}\AppData\Local\Temp`
`%userprofile%`	`%SystemDrive%\Users\<username>`

Option	Beschreibung
Look <nn> folders deep	Bestimmen Sie die Ordnertiefe, die durchsucht werden soll, wobei <nn> die Ordnertiefe ist. Gültige Werte sind positive Ganzzahlen, 0 und -1. • Durch Festlegen von -1 wird eine Suche auf allen Verzeichnisebenen beantragt (eine unbegrenzte Suchtiefe). • Durch Festlegen von 0 in Windows Umgebungen wird auf keiner Ebene gesucht. Durch Festlegen von 0 in macOS Umgebungen wird eine Suche auf der aktuellen Verzeichnisebene angefordert. • Durch Festlegen von 1 in Windows Umgebungen wird eine Suche auf der aktuellen Verzeichnisebene angefordert. Durch Festlegen von 1 in macOS Umgebungen wird eine Suche auf der aktuellen Verzeichnisebene und eine Ebene darunter angefordert. • Durch Festlegen einer anderen positiven Ganzzahl in Windows Umgebungen werden Ordner in einer Tiefe durchsucht, die die aktuelle Verzeichnisebene einschließt. Wenn Sie z.B. 2 festlegen, wird eine Suche auf der aktuellen Verzeichnisebene und eine Ebene darunter angefordert. Durch Festlegen einer anderen positiven Ganzzahl in macOS Umgebungen wird die Suchtiefe von der aktuellen Verzeichnisebene eingestellt. Wenn Sie z.B. 2 festlegen, wird eine Suche auf der aktuellen Verzeichnisebene und zwei Ebenen darunter angefordert.
Maximum file size	Bestimmen Sie die maximale Dateigröße in Bytes, die in die Suche einbezogen werden soll. Gültige Werte sind Ganzzahlen größer oder gleich -1 (negative 1). Durch Festlegen von -1 wird angezeigt, dass keine maximale Dateigrößenbeschränkung erzwungen werden sollte. Durch Festlegen von 0 wird angezeigt, dass nur Dateien mit einer Größe von Null Bytes gemeldet werden sollten. Wenn die Größe (in Bytes) einer Enterprise Search die maximale Dateigröße der ausführlichen Suche überschreitet, wird die Suche trotzdem erstellt. In macOS Umgebungen sucht eine umfassenden Enterprise Search, die 0 als Option für die maximale Dateigröße festlegt, nicht richtig nach Dateien mit einer Größe von 0.
Minimum file size	Bestimmen Sie die minimale Dateigröße in Bytes, die in die Suche einbezogen werden soll. Gültige Werte sind Ganzzahlen größer oder gleich -1 (negative 1). Durch Festlegen von -1 oder 0 wird angezeigt, dass keine Mindestgröße für die Datei gelten soll.

Suchbedingungsoperatoren

Die folgende Tabelle beschreibt die Suchoperatoren, die für die Verwendung in Suchbegriffen verfügbar sind. Einige Suchoperatoren sind nur mit bestimmten Tokentypen gültig.

Operator	Eine Übereinstimmung tritt auf, wenn
between	Der Host Wert liegt zwischen zwei festgelegten Suchwerten.
contains	Der Host Wert enthält die festgelegte Suchzeichenfolge.
equals	Der Host Wert entspricht dem festgelegten Suchwert.
greater than	Der Host Wert ist größer als der festgelegte Suchwert.
less than	Der Host Wert ist geringer als der festgelegte Suchwert.
not contains	Der Host Wert enthält nicht die festgelegte Suchzeichenfolge.
not equals	Der Host Wert entspricht nicht dem festgelegten Suchwert.

Verknüpfungen für Suchbedingungen

Suchbedingungen sind Token Zeichenfolgen, die mit Hilfe von Token, Operatoren und Werten erstellt werden. Die folgenden Verknüpfungen für die Erstellung von Bedingungen sind verfügbar:

- Klicken Sie in der Suchleiste und geben Sie Ihre Bedingungen ein. Sie können immer nur eine Bedingung eingeben. Klicken Sie auf **Eingabe**, um eine Bedingung zu dem Suchbegriff hinzuzufügen.
- Verwenden Sie die Pfeiltasten auf Ihrer Tastatur, um durch die Token in der Dropdown-Liste zu blättern. Klicken Sie auf **Enter**, wenn das gewünschte Token hervorgehoben ist.
- Beginnen Sie in der Dropdown-Tokenliste mit der Eingabe des Tokennamen. Die Token, die mit den eingegebenen Zeichen übereinstimmen, werden angezeigt.
- Um nach einem MD5-, SHA1- oder SHA256-Hash oder nach einer IP-Adresse zu suchen, kopieren Sie das Hash oder die IP-Adresse in die Suchleiste und klicken Sie auf **Eingabe**. Die Endpoint Security Software erstellt die Bedingung automatisch.

Wie werden mehrere Bedingungen ausgewertet

Suchbedingungen sind Token Zeichenfolgen, die mit Hilfe von Token, Operatoren und Werten erstellt werden. Wenn in einem Suchbegriff mehrere Bedingungen angegeben sind, müssen die Hostdaten mit *allen* Bedingungen übereinstimmen, die in den Suchergebnissen

zurückgegeben werden. Mit anderen Worten, mehrere Bedingungen in einer Suche werden als AND Operatoren behandelt. Jede Bedingung wird vor der AND Verarbeitung ausgewertet.

Wenn dasselbe Token allerdings in mehr als einer Bedingung in derselben Suche verwendet wird, müssen beide für das Token angegebenen Werte übereinstimmen, damit Hostdaten in den Suchergebnissen zurückgegeben werden. Mit anderen Worten, getrennte Bedingungen in derselben Suche unter Verwendung desselben Tokens werden als OR-Operator behandelt. Um beispielsweise nach mehreren verschiedenen Dateinamen zu suchen, müssen Sie für jeden Dateinamen in der Suche eine separate Bedingung angeben.

Suchlimits

Die folgenden Limits gelten für Enterprise Searches um sicherzustellen, dass Leistung nicht beeinträchtigt wird und die Menge der gesammelten Daten nützlich ist.

1. Bei einer Suche können maximal 25 Bedingungen verwendet werden. Fehlermeldungen werden angezeigt, wenn Sie mehr als 25 Bedingungen angeben und die Suche nicht ausgeführt wird.
2. Es können maximal 15 Suchvorgänge gleichzeitig ausgeführt werden, dieser Wert ist jedoch konfigurierbar. Der Standardwert ist auf fünf gleichzeitige Suchen eingestellt. Wenn Sie versuchen, mehr gleichzeitige Suchvorgänge als das konfigurierte Maximum auszuführen, werden Fehlermeldungen angezeigt. Informationen zum Konfigurieren dieser Einstellung finden Sie unter Die Anzahl der gleichzeitigen Suchen einschränken auf Seite 151.
3. Auf der Enterprise Search Seite können maximal 15 Suchvorgänge definiert werden, aber dieser Wert ist konfigurierbar. Der Standardwert ist auf 10 Suchvorgänge festgelegt. Wenn Sie versuchen, mehr Suchvorgänge als das konfigurierte Maximum zu definieren, werden Fehlermeldungen angezeigt. Informationen zum Konfigurieren dieser Einstellung finden Sie unter Die Anzahl definierter Suchen einschränken auf Seite 149.

4. Im Grid (Group By) Modus können höchstens 1000 Zeilen und im Host Modus höchstens 1000 Hosts, die den Suchkriterien entsprechen, zurückgegeben werden. Erwägen Sie, Ihre Suche zu verfeinern, wenn die zurückgegebenen Ergebnisse diesen Grenzwert überschreiten.

   Im Host Modus zeigt die Endpoint Security Web-UI Ergebnisse von den ersten 1000 Agents an, die auf die Suche reagieren. Wenn das Limit von 1.000 Agents erreicht ist, zeigt die Web UI keine Daten mehr an. Wenn jedoch zusätzliche Agents die Suchanforderung erhalten haben, werden ihre Ergebnisse trotzdem erfasst, obwohl sie nicht in der Web UI angezeigt werden.

   Im Grid (Raster) Modus (Group by) kann eine beliebige Anzahl von Hosts verarbeitet werden, jedoch werden nicht mehr als 1.000 eindeutige Rasterzeilen in der Web-UI angezeigt.

   Wenn die von einer Enterprise Search zurückgegebenen Daten mehrere Übereinstimmungen für verschachtelte Elemente in der Ausgabe enthalten, wird nur die letzte Übereinstimmung auf der Enterprise Search Seite aufgeführt.

   Wenn die Suchergebnisse in eine CSV-Datei heruntergeladen werden, sind alle zurückgegebenen Daten enthalten. Die CSV-Datei kann mehr als 1000 Zeilen enthalten. Siehe Suchergebnisse überprüfen auf Seite 269.

5. Im Host Modus können höchsten 20 Treffer pro Host zurückgegeben werden. Wenn mehr als 20 Treffer empfangen werden, werden die zusätzlichen Treffer für diesen Host ignoriert. Erwägen Sie, Ihre Suche zu verfeinern, wenn die zurückgegebenen Ergebnisse diesen Grenzwert überschreiten.
6. Es können maximal 5 MB Daten von einem Host Endpunkt zurückgegeben werden. Wenn die vom Agent zurückgegebenen Daten 5 MB überschreiten, schneidet der Agent die Nutzdaten ab. Erwägen Sie, Ihre Suche zu verfeinern, wenn die zurückgegebenen Ergebnisse diesen Grenzwert überschreiten.
7. Enterprise Search Daten werden nur von Endpunkten gesammelt, die macOS und Windows auf Endpoint Security Agent Version 25 oder später ausführen und von Endpunkten, die Linux auf Agent 34 oder später ausführen.

Eine Suche beginnen

Um eine Enterprise Search zu starten:

1. Wählen Sie **Enterprise Search** in der Endpoint Security Web-UI.
2. Verwenden Sie die Suchleiste, um einen Suchbegriff zu erstellen. Siehe Suchbegriffe erstellen.
3. Wenn Sie eine Endpoint Security Power Lizenz besitzen und die Felder, die Sie durchsuchen, es gestatten, können Sie eine ausführliche Suche auswählen, indem Sie auf **Enable exhaustive search** klicken.
4. Klicken Sie auf **SEARCH**.

   Die Suche wird gestartet.

   Es können maximal fünf Suchvorgänge gleichzeitig ausgeführt werden. Es können maximal zehn Suchvorgänge auf der Enterprise Search Seite definiert werden.

   Wenn die Ergebnisse zurückgegeben werden, werden die ersten 25 Ergebnisse angezeigt. Um mehr als die ersten 25 Ergebnisse zu sehen, klicken Sie auf **Load More**.

Suchanfragen werden auch weiter ausgeführt, wenn alle Hosts geantwortet haben. Sie laufen weiter, bis sie manuell gestoppt werden oder bis sie eines der Suchlimits erreichen.

Eine Suche stoppen

Suchanfragen werden auch weiter ausgeführt, wenn alle Hosts geantwortet haben. Eine Suche wird automatisch gestoppt, wenn eins der Suchlimits erreicht ist. Siehe Suchlimits auf Seite 264. Sie können eine Suche auch manuell stoppen.

Um eine Enterprise Search manuell zu stoppen:

1. Wählen Sie **Enterprise Search** in der Endpoint Security Web-UI.
2. Wählen Sie die Suche, die Sie stoppen wollen.
3. Klicken Sie auf **Stop collecting results**.

   Die Suche wird gestoppt.

   Eine gestoppte Suche kann nicht erneut gestartet werden.

Suchergebnisse löschen

Wenn Sie Suchergebnisse löschen, löschen Sie auch die Suchanfrage. Sie können die Abfrage nicht speichern.

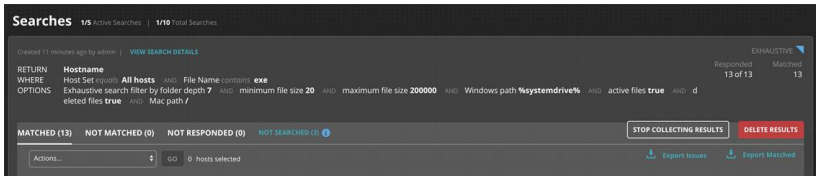
Um eine Suche und ihre Ergebnisse zu löschen:

1. Wählen Sie **Enterprise Search** in der Endpoint Security Web-UI.
2. Klicken Sie auf **Delete Results**.
3. Klicken Sie auf **Delete**, um die Löschanfrage zu bestätigen.

Die Suchanfrage und die Ergebnisse werden gelöscht.

KAPITEL 18: Suchergebnisse überprüfen

Um die Ergebnisse einer Enterprise Search zu überprüfen, klicken Sie auf der Enterprise Search Seite in der Endpoint Security Web UI auf die Suche. Die Suche wird erweitert und zeigt Suchanfragen und Ergebnisse an.



Der Suchanfragebereich wird am Anfang der erweiterten Suchanfrage angezeigt und zeigt die Suchbedingungen (Suchtoken und Werte), die von der Suche angefordert wurden und alle ausführlichen Suchoptionen, die angefordert wurden. Die Suchbedingungen werden auf der **WHERE** Zeile des Suchanfragenbereichs angezeigt. Die Optionen für die ausführliche Suche werden auf der **OPTIONS** Zeile des Suchanfragebereichs angezeigt.

Suchergebnisse werden auf einer Reihe von Registern angezeigt:

Registername	Beschreibung
Matched	Führt Hosts auf, für die eine Übereinstimmung mit dem Suchbegriff gefunden wurde.
Not Matched	Führt Hosts auf, die durchsucht wurden, aber für die keine Übereinstimmung mit dem Suchbegriff gefunden wurde.
Not Responded	Führt Hosts auf, die noch nicht auf die Suchanfrage geantwortet haben. Alle Hosts sind zunächst in dieser Kategorie. Wenn Hosts antworten, werden Sie auf die **Matched** und **Not Matched** Register verschoben. Hosts auf dem **Not Respondet** Register sind ggf. inaktiv oder führen weiterhin die Suche aus.

Registername	Beschreibung
Not Searched	Führt Hosts auf, für die die Suche nicht anwendbar war. Eine Suche ist für einen Host Endpunkt nicht anwendbar, wenn eine Suchbedingung in der Enterprise Search für das Betriebssystem des Host-Endpunkts oder die Version des FireEye Endpoint Security Agent, die auf dem Host Endpunkt ausgeführt wird, ungültig ist. Wenn dieses Register nicht in den Suchergebnissen angezeigt wird, wird die Suche auf alle Host Endpunkte in Ihrem Unternehmen angewendet.
Errors	Führt Fehler auf, die während der Suche aufgetreten sind. Wenn dieses Register nicht in den Suchergebnissen angezeigt wird, gab es während der Suche keine Fehler.

Klicken Sie auf das ⚠ Symbol neben einem Hostnamen, um die Elementtypen anzuzeigen, die von fehlerhaften oder unerwarteten Daten betroffen sind, auf die die Suche auf dem Host gestoßen ist. Solche Suchprobleme kommen häufig vor, können jedoch bedeuten, dass der Host nicht vollständig nach diesen Elementtypen durchsucht werden kann. Standardmäßig zeichnet der Endpoint Security bis zu zehn einzigartige Probleme auf, die durch fehlerhafte oder unerwartete Daten während einer Suche hervorgerufen wurden und meldet diese. Dieser Standardwert kann mit Hilfe des `hx server search issues items-limit` CLI Befehls geändert werden. Weitere Informationen finden Sie in der *CLI Befehlsreferenz*.

Wenn Sie den Host Modus festgelegt haben, enthält jedes Register eine Liste von Hosts. Wenn Sie den Raster Modus festgelegt haben, zeigt das **Matched** Register die Ergebnisse in einem Raster an, in dem die angeforderten Group By Feldwerte und Gruppierung von Hosts, die mit der Suchanfrage nach diesen Werten übereinstimmen, aufgeführt sind. Siehe Suchmodi verstehen.

Suchanfragen werden auch weiter ausgeführt, wenn alle Hosts geantwortet haben. Sie laufen weiter, bis sie manuell gestoppt werden oder bis sie eines der Suchlimits erreichen.

Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.

Sie können die Suchergebnisse nicht nur auf der Enterprise Search Seite überprüfen, sondern auch in eine CSV-Datei herunterladen.

Um die Ergebnisse einer Enterprise Search auf eine CSV-Datei herunterzuladen:

1. Wählen Sie **Enterprise Search** in der Endpoint Security Web-UI.
2. Wählen Sie die Suchanfrage mit den Suchergebnissen, die Sie herunterladen wollen.
3. Wählen Sie das Register mit den Daten, die Sie herunterladen wollen (**Matched**, **Not Matched** oder **Not Responded**).

4. Klicken Sie auf die Download Schaltfläche ().

   Die Ergebnisse auf dem ausgewählten Register werden in eine CSV-Datei heruntergeladen.

   Das Limit für Suchergebnisse, die in der Web UI angezeigt werden, ist 1000 Zeilen. Die CSV-Datei kann mehr als 1000 Zeilen enthalten. Die Matched und Not Matched CSV-Dateien überschreiten jedoch nur 1000 Zeilen, wenn das Limit von 1000 Zeilen mitten in der Verarbeitung erreicht wird. Die Not Responded CSV-Datei zeigt jeden Host an, der nicht auf die Suche reagiert hat. Je nach der Anzahl der durchsuchten Hosts können 1000 Zeilen regelmäßig überschritten werden.

KAPITEL 19: Suchtoken Referenz

Die Suchfeldformate und Token, die in einer Enterprise Search Anfrage verwendet werden können, werden hier beschrieben.

Wertformate für Suchbedingungen

Die folgenden Wertformate werden in Suchbedingungen verwendet.

Format	Beschreibung
boolean	Ein Boolescher Wert: `true`, `false`, `1` oder `0`
ipaddress	Eine gültige IPv4 oder IPv6-Adresse
md5hash	Ein 32-Zeichen MD5 Hash
naturalnumber	Eine nicht-negative Ganzzahl
sha1hash	Ein 40-Zeichen SHA1 Hash
sha256hash	Ein 64-Zeichen SHA256 Hash
string	Eine nicht-leere Zeichenfolge von weniger als 5000 Zeichen
timestamp	Ein RFC 2822 oder ISO 8061 Zeitstempel Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Token Referenz

Die folgende Tabelle zeigt die Endpunkt Betriebssystemplattformen, die von jedem Token unterstützt wird und ob eine ausführliche Suche erforderlich, optional oder nicht zutreffend ist. Klicken Sie auf den Namen des Tokens, um weitere Informationen zu erhalten.

Token	Windows	macOS	Linux	Ausführliche Suche
Application Name	Nein	Ja		---
Browser Name	Ja	Ja		---
Browser Version	Ja	Ja		---
Cookie Flags	Ja	Nein		---
Cookie Name	Ja	Ja		---
Cookie Value	Ja	Ja		---
DNS Hostname	Ja	Ja		---
Driver Device Name	Ja	Nein		Erforderlich
Driver Module Address	Nein	Nein	Ja	Ja
Driver Module In-Tree	Nein	Nein	Ja	Ja
Driver Module License	Nein	Nein	Ja	Ja
Driver Module Name	Ja	Nein	Ja	Erforderlich

Token	Windows	macOS	Linux	Ausführliche Suche
Driver Module Parameters	Nein	Nein	Ja	Ja
Driver Module Return Trampoline	Nein	Nein	Ja	Ja
Driver Module Signature	Nein	Nein	Ja	Ja
Driver Module Signer	Nein	Nein	Ja	Ja
Driver Module Signing Hash Algorithm	Nein	Nein	Ja	Ja
Driver Module Signing Key	Nein	Nein	Ja	Ja
Driver Module Status	Nein	Nein	Ja	Ja
Driver Module Vermagic	Nein	Nein	Ja	Ja
Driver Module Version	Nein	Nein	Ja	Ja
Executable Exported Dll Name	Ja	Nein		Erforderlich
Executable Exported Function Name	Ja	Nein		Erforderlich

Token	Windows	macOS	Linux	Ausführliche Suche
Executable Imported Function Name	Ja	Nein		Erforderlich
Executable Imported Module Name	Ja	Nein		Erforderlich
Executable Injected	Ja	Nein		Erforderlich
Executable PE Type	Ja	Nein		Erforderlich
Executable Resource Name	Ja	Nein		Erforderlich
File Attributes	Ja	Ja		Erforderlich
File Certificate Issuer	Ja	Ja		Optional (nur Windows)
File Certificate Subject	Ja	Ja		Optional (nur Windows)
File Download Mime Type	Ja	Nein		---
File Download Referrer	Ja	Ja		---
File Download Type	Ja	Ja		---
File Full Path	Ja	Ja		Optional

Token	Windows	macOS	Linux	Ausführliche Suche
File MD5 Hash	Ja	Ja		Optional
File Name	Ja	Ja		Optional
File SHA1 Hash	Ja	Ja		Optional
File SHA256 Hash	Ja	Ja		Optional
File Signature Exists	Ja	Ja		Optional (nur Windows)
File Signature Verified	Ja	Ja		Optional (nur Windows)
File Stream Name	Ja	Nein		Erforderlich
File Text Written	Ja	Nein		---
Group By (grid mode)	Ja	Ja		---
Group ID	Nein	Nein	Ja (schnell)	---
Group Name	Ja	Ja	Ja (schnell)	---
Host Set	Ja	Ja		---
Hostname	Nein	Ja		Erforderlich
HTTP Header	Ja	Ja		---
INode	Nein	Nein	Ja	Ja
IP Address	Ja	Ja		---
Local IP Address (Lokale IP-Adresse)	Ja	Ja		---
Local Port	Ja	Ja		---
Login Failed	Nein	Nein	Ja	Ja

Token	Windows	macOS	Linux	Ausführliche Suche
Login Record Type	Nein	Nein	Ja	Ja
Network Route Flags	Nein	Nein	Ja (schnell)	---
Parent Process Name	Ja	Ja		---
Parent Process Path	Ja	Ja		---
Port	Ja	Ja		---
Port Protocol	Ja	Ja		---
Port State	Ja	Ja		---
Process Arguments	Ja	Ja		Optional
Process Name	Ja	Ja		Optional
Quarantine Event Sender Address	Nein	Ja		---
Quarantine Event Sender Name	Nein	Ja		---
Registry Key Full Path	Ja	Nein		Optional
Registry Key Value Name	Ja	Nein		Optional
Registry Key Value Text	Ja	Nein		Optional
Remote IP Address (Remote IP-Adresse)	Ja	Ja		---

Token	Windows	macOS	Linux	Ausführliche Suche
Remote Login	Nein	Nein	Ja	Ja
Remote Port	Ja	Ja		---
Service DLL	Ja	Nein		---
Service Mode	Ja	Ja		---
Service Name	Ja	Ja		---
Service Status	Ja	Ja		---
Service Type	Ja	Ja		---
Session Length	Nein	Nein	Ja	Ja
Shell Command	Nein	Nein	Ja	Ja
Shell Type	Nein	Nein	Ja	Ja
Size in bytes	Ja	Ja		Optional
Socket Protocol	Nein	Nein	Ja	Ja
Socket State	Nein	Nein	Ja	Ja
Socket Type	Nein	Nein	Ja	Ja
Sudo Command	Nein	Nein	Ja	Ja
Sudo Command Success	Nein	Nein	Ja	Ja
Syslog Event ID	Nein	Ja		Erforderlich
Syslog Event Message	Nein	Ja		Erforderlich
Syslog Facility	Nein	Ja		Erforderlich
Syslog File	Nein	Nein	Ja	Ja

Token	Windows	macOS	Linux	Ausführliche Suche
Syslog Sender	Nein	Ja		Erforderlich
Syslog Severity Level	Nein	Ja		Erforderlich
Task Flag	Ja	Nein		---
Task Name	Ja	Ja		---
Task Reference	Nein	Ja		---
Task Status	Ja	Nein		---
Terminal Type	Nein	Nein	Ja	Ja
Timestamp - Accessed	Ja	Ja		Optional
Timestamp - Changed	Ja	Ja		Erforderlich
Timestamp - Created	Ja	Ja		Optional
Timestamp - Event	Ja	Ja		---
Timestamp - Last Login	Ja	Ja		---
Timestamp - Last Run	Ja	Ja		---
Timestamp - Modified	Ja	Ja		Optional (Windows und macOS. Registrierungs- und Windows-Ereignisdatensatzsuchen nur für Windows.)
Timestamp - Started	Ja	Ja		Optional
URL	Ja	Ja		---

Token	Windows	macOS	Linux	Ausführliche Suche
Username	Ja	Ja		Optional (Windows und macOS. Registrierungs- und Windows-Ereignisdatensatzsuchen nur für Windows.)
Web Page Origin URL	Nein	Ja		---
Web Page Title	Ja	Ja		---
Windows Event ID	Ja	Nein		Erforderlich
Windows Event Log Type	Ja	Nein		Erforderlich
Windows Event Message	Ja	Nein		Erforderlich

Applikationsname

Sucht nach dem Namen einer Applikation. macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Browser Name

Sucht nach dem Namen eines Browsers. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

Browser Version

Sucht nach einer Browser Version. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

Cookie Flags

Sucht nach einer Cookie Markierung. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

Cookie Name

Sucht nach einem Cookie Namen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Cookie Value

Sucht nach einem Cookie Wert. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

DNS-Hostname

Sucht nach einem DNS Hostnamen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Driver Device Name

Sucht nach dem Namen eines Gerätetreibers. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Enthält die Suche nach einem Kerneltreiber.

Driver Module Name

Sucht nach dem Namen eines Treibermoduls. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Enthält die Suche nach einem Kerneltreibermodul.

Executable Exported Dll Name

Sucht nach dem Namen einer exportierten ausführbaren DLL. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Executable Exported Function Name

Sucht nach dem Namen einer exportierten ausführbaren Funktion. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Executable Imported Function Name

Sucht nach dem Namen einer importierten ausführbaren Funktion. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Executable Imported Module Name

Sucht nach dem Namen eines importierten ausführbaren Moduls. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Executable Injected

Sucht nach Hinweisen, dass eine ausführbare Datei injiziert wurde. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
boolesch	Erforderlich	Umfasst die Suche nach einem Prozess.

Executable PE Type

Sucht nach einem ausführbaren PE Typ. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst Suchen nach einer Datei auf einem Datenträger oder einem Prozess. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Executable Resource Name

Sucht nach dem Namen einer ausführbaren Ressource. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einer Datei auf einem Datenträger. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Attributes

Sucht nach Dateiattributen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einer Datei auf einem Datenträger. Ermöglicht Ihnen, nach Windows oder macOS Pfadnamen zu filtern und die folgenden Datenträger-Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Certificate Issuer

Sucht nach dem Aussteller eines Zertifikats. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden. Ausführliche Suchvorgänge gelten nur für Windows Endpunkte.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional (nur Windows)	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Certificate Subject

Sucht nach einem Zertifikat Betreff. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden. Ausführliche Suchvorgänge gelten nur für Windows Endpunkte.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional (nur Windows)	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Download Mime Type

Sucht nach dem MIME-Typ eines Dateidownloads. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

File Download Referrer

Sucht nach einem Dateidownload-Referrer. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

File Download Type

Sucht nach einem Dateidownload-Typ. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

File Full Path

Sucht nach einem vollständigen Dateipfad, einschließlich Dateinamen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional	Umfasst die Suche nach einer Datei auf Datenträger, einem Kerneltreibermodul, einem Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

File MD5 Hash

Sucht nach einem MD5 Datei Hash. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
md5hash	Optional	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Name

Sucht nach einem Dateinamen Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional	Umfasst die Suche nach einer Datei auf einem Datenträger. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

File SHA1 Hash

Sucht nach einem SHA1 Datei Hash. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
sha1hash	Optional	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File SHA256 Hash

Sucht nach einem SHA256 Hash. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
sha256hash	Optional	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Signature Exists

Sucht nach Hinweisen, dass eine Dateisignatur vorhanden sind. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden. Ausführliche Suchvorgänge gelten nur für Windows Endpunkte.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
boolean	Optional (nur Windows)	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Signature Verified

Sucht nach Hinweisen, dass eine Dateisignatur verifiziert ist. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden. Ausführliche Suchvorgänge gelten nur für Windows Endpunkte.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
boolean	Optional (nur Windows)	Umfasst die Suche nach einer Datei auf Datenträger, einer Kerneltreiber oder einem Prozess. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Stream Name

Sucht nach dem Namen eines Dateistroms. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einer Datei auf einem Datenträger. Ermöglicht Ihnen, nach Windows Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

File Text Written

Sucht nach Text in einer Datei. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Group By

Bestimmt, dass die Suchergebnisse im Rastermodus angezeigt werden (auch als Group By Modus bekannt). Dieser Modus gruppiert Suchergebnisse nach einem oder mehreren ausgewählten Feldern, fasst die Ergebnisse nach den Felder zusammen und zeigt sie in einem Raster an. Wenn es in einem Suchbegriff festgelegt ist, muss Group By das letzte Token in dem Suchbegriff sein. Siehe Suchmodi verstehen auf Seite 255.

Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Group Name

Sucht nach einem Gruppennamen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Hostname

Sucht nach dem Hostnamen des Systems für einen Protokolleintrag im macOS Systemprotokoll. macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zahl	Erforderlich	Eine Systemprotokollsuche muss als ausführliche Suche durchgeführt werden. Umfasst die Suche nach einem Syslog Ereignisdatensatz.

Host Set

Bestimmt, dass die Suchergebnisse nach Hostsatz angezeigt werden.

Sie können einen Hostsatz für die Suche festlegen. Standardmäßig ist der Suchwert für dieses Token auf **All hosts** eingestellt (einen interner Hostsatz umfasst alle dem Endpoint Security bekannten Hosts). Wenn Sie dieses Token auswählen, müssen Sie einen Hostsatz von einer Dropdown-Liste auswählen.

Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

HTTP Header

Sucht nach einem HTTP Header. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

IP Address

Sucht nach einer IP-Adresse. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
ipaddress	Nein	---

Local IP Address

Sucht nach einer lokalen IP-Adresse. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
ipaddress	Nein	---

Local Port

Sucht nach einer lokalen Portnummer. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
naturalnumber	Nein	---

Lokale Portspezifikationen in einer Netzwerkverbindungsbedingung eines benutzerdefinierten Indikators darf nicht Null (0) sein. Bei der Suche nach dem lokalen Portwert 0 werden keine benutzerdefinierten Indikatorregeln gefunden.

Parent Process Name

Sucht nach einem übergeordneten Prozessnamen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Parent Process Path

Sucht nach einem übergeordneten Prozesspfad. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Port

Sucht nach einer Portnummer. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
naturalnumber	Nein	---

Port Protocol

Sucht nach einem Portprotokoll. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Port State

Sucht nach einem Portstatus. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Process Arguments

Sucht nach Prozessargumenten. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional	Umfasst die Suche nach einem Prozess.

Process Name

Sucht nach einem Prozessnamen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional	Umfasst die Suche nach einem Prozess.

Absenderadresse des Quarantäneereignisses

Sucht nach der Absenderadresse des Quarantäneereignisses. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Absendername des Quarantäneereignisses

Sucht nach dem Absendernamen des Quarantäneereignisses. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Vollständiger Pfad des Registrierungsschlüssels

Sucht nach dem vollständigen Pfad eines Registrierungsschlüssels. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional	Beinhaltet die Suche nach einem Registrierungsschlüssel. Ermöglicht Ihnen, die Suche nach Registrierungsstrukturpfad zu filtern. Der Standard Registrierungsstrukturpfad ist `HKEY_LOCAL_MACHINE\Software` wenn kein Pfad angegeben ist. Das Filtern nach Registrierungsstruktur erweitert die Standard Registrierungssuche und gibt möglicherweise Ergebnisse zurück, die in einer Schnellsuche mit derselben Abfrage nicht gefunden wurden.

Wertname des Registrierungsschlüssels

Sucht nach einem Registrierungsschlüsselnamen. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional	Beinhaltet die Suche nach einem Registrierungsschlüssel. Ermöglicht Ihnen, die Suche nach Registrierungsstrukturpfad zu filtern. Der Standard Registrierungsstrukturpfad ist `HKEY_LOCAL_MACHINE\Software` wenn kein Pfad angegeben ist. Das Filtern nach Registrierungsstruktur erweitert die Standard Registrierungssuche und gibt möglicherweise Ergebnisse zurück, die in einer Schnellsuche mit derselben Abfrage nicht gefunden wurden.

Registry Key Value Text

Sucht nach einem Registrierungsschlüsseltext. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional	Beinhaltet die Suche nach einem Registrierungsschlüssel. Ermöglicht Ihnen, die Suche nach Registrierungsstrukturpfad zu filtern. Der Standard Registrierungsstrukturpfad ist `HKEY_LOCAL_MACHINE\Software` wenn kein Pfad angegeben ist. Das Filtern nach Registrierungsstruktur erweitert die Standard Registrierungssuche und gibt möglicherweise Ergebnisse zurück, die in einer Schnellsuche mit derselben Abfrage nicht gefunden wurden.

Remote IP Address

Sucht nach einer remote IP-Adresse. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
ipaddress	Nein	---

Remote Port

Sucht nach einem remote Port. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
naturalnumber	Nein	---

Remote Portspezifikationen in einer Netzwerkverbindungsbedingung eines benutzerdefinierten Indikators darf nicht Null (0) sein. Bei der Suche nach dem remote Portwert 0 werden keine benutzerdefinierten Indikatorregeln gefunden.

Service DLL

Sucht nach dem Namen einer Service-DLL. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Service Modus

Sucht nach einem Service Modus. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Servicename

Sucht nach einem Servicenamen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Service Status

Sucht nach dem Status eines Service. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Service Type

Sucht nach einem Servicetyp. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Größe in Byte

Sucht nach einer Größe in Bytes ausgedrückt. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
naturalnumber	Optional	Umfasst die Suche nach einer Datei auf einem Datenträger. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Syslog Ereignis-ID

Sucht nach der Identifizierungsnummer eines Protokolleintrags im macOS Systemprotokoll. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
naturalnumber	Erforderlich	Eine Systemprotokollsuche muss als ausführliche Suche durchgeführt werden. Umfasst die Suche nach einem Syslog Ereignisdatensatz.

Syslog Ereignisnachricht

Sucht nach der Protokollnachricht in einem Protokolleintrag im macOS Systemprotokoll. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Eine Systemprotokollsuche muss als ausführliche Suche durchgeführt werden. Umfasst die Suche nach einem Syslog Ereignisdatensatz.

Syslog Facility

Sucht nach dem Teil des Systems, der im macOS Systemprotokoll eine Protokollnachricht generiert hat. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Eine Systemprotokollsuche muss als ausführliche Suche durchgeführt werden. Umfasst die Suche nach einem Syslog Ereignisdatensatz.

Syslog Sender

Sucht nach dem Namen des Prozesses, der eine Protokollnachricht im macOS Systemprotokoll generiert hat. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Eine Systemprotokollsuche muss als ausführliche Suche durchgeführt werden. Umfasst die Suche nach einem Syslog Ereignisdatensatz.

Syslog Schweregrad

Sucht im macOS Systemprotokoll nach dem Schweregrad einer Protokollnachricht. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Eine Systemprotokollsuche muss als ausführliche Suche durchgeführt werden. Umfasst die Suche nach einem Syslog Ereignisdatensatz.

Aufgabenmarkierung

Sucht nach einer Aufgabenmarkierung. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Aufgabenname

Sucht nach einem Aufgabennamen. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Aufgabenreferenz

Sucht nach einem Aufgabenelement. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Task Status

Sucht nach dem Status einer Aufgabe. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Zeitstempel - Aufgerufen

Sucht nach einer Zugriffszeit. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zeitstempel	Optional	Umfasst die Suche nach einer Datei auf einem Datenträger. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

Zeitstempel - Geändert

Sucht nach einer Aktualisierungszeit. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zeitstempel	Erforderlich	Umfasst die Suche nach einer Datei auf einem Datenträger. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Zeitstempel - Erstellt

Sucht nach einer Erstellungszeit. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zeitstempel	Optional	Umfasst die Suche nach einer Datei auf Datenträger, einem Windows Ereignisdatensatz oder einem macOS syslog Ereignisdatensatz. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße

Zeitstempel - Ereignis

Sucht nach einer Ereigniszeit. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zeitstempel	Nein	---

Timestamp - Last Login

Sucht nach einer letzten Anmeldezeit. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zeitstempel	Nein	---

Timestamp - Last Run

Sucht nach einer letzten Laufzeit. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zeitstempel	Nein	---

Zeitstempel - Verändert

Sucht nach einer Veränderungszeit. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden. Ausführliche Suchen für Registrierungs- und Windows Ereignisdaten treffen nur auf Windows Endpunkte zu.

Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zeitstempel	Optional	Umfasst die Suche nach einer Datei auf Datenträger, einem Registrierungsschlüssel oder einem Windows Ereignisdatensatz. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße Mit diesem Token können Sie auch die Suche nach dem Windows Registrierungsstrukturpfad filtern. Der Standard Registrierungsstrukturpfad ist `HKEY_LOCAL_MACHINE\Software` wenn kein Pfad angegeben ist. Das Filtern nach Registrierungsstruktur erweitert die Standard Registrierungssuche und gibt möglicherweise Ergebnisse zurück, die in einer Schnellsuche mit derselben Abfrage nicht gefunden wurden.

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

Timestamp - Started

Sucht nach einer Startzeit. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Gültige Zeitstempel müssen zwischen den 1. Januar 1970 UTC und den 19. Januar, 3:14:07, 2038 UTC fallen.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
Zeitstempel	Optional	Umfasst die Suche nach einem Prozess.

Zu diesem Zeitpunkt geben Anfragen für Browser-Datei und Cookie Daten begrenzte Datenfelder, auf Grund der aktuellen Beschränkungen in der Agent Datensammlung zurück.

URL

Sucht nach einer URL. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Eine Enterprise Search, die das URL Token verwendet, kann zu hohen Datenträger E/A führen.

Username

Sucht nach einem Usernamen Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden. Ausführliche Suchen für Registrierungs- und Windows Ereignisdaten treffen nur auf Windows Endpunkte zu.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Optional	Umfasst die Suche nach einer Datei auf Datenträger, einem Prozess, einem Registrierungsschlüssel oder einem Windows Ereignisdatensatz. Ermöglicht Ihnen, nach Pfadnamen zu filtern und die folgenden Datenträger Suchoptionen festzulegen: • Ordnertiefe • minimale Dateigröße • maximale Dateigröße Mit diesem Token können Sie auch die Suche nach dem Windows Registrierungsstrukturpfad filtern. Der Standard Registrierungsstrukturpfad ist `HKEY_LOCAL_MACHINE\Software` wenn kein Pfad angegeben ist. Das Filtern nach Registrierungsstruktur erweitert die Standard Registrierungssuche und gibt möglicherweise Ergebnisse zurück, die in einer Schnellsuche mit derselben Abfrage nicht gefunden wurden.

Web Page Origin URL

Sucht nach der Ursprungs-URL der Webseite. macOS Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Webseitentitel

Sucht nach einem Webseitentitel. Windows und macOS Host-Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Nein	---

Windows Event ID

Sucht nach einer Windows Ereignis-ID. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
naturalnumber	Erforderlich	Umfasst die Suche nach einem Windows Ereignisdatensatz.

Windows Event Log Type

Sucht nach einem Windows Ereignisprotokolltyp. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einem Windows Ereignisdatensatz.

Windows Ereignisnachricht

Sucht nach einer Windows Ereignisnachricht. Window Host Endpunkte können mit Hilfe dieses Tokens durchsucht werden.

Suchdaten werden in der Windows Ereignismeldung nicht gefunden, wenn die Nachricht Zeilenumbrüche oder Interpunktion enthält.

Feldformat	Ausführliche Suche?	Details über ausführliche Suche
string	Erforderlich	Umfasst die Suche nach einem Windows Ereignisdatensatz.

TEIL IV: Forensische Daten analysieren

Warnungen sind Übereinstimmungen zwischen einer oder mehreren Indikatorbedingungen oder Quellenwarnungen und Aktivitäten, die Agents auf Ihren Host Endpunkten finden.

Um Warnungen zu untersuchen, durchsuchen Sie forensische Daten, um festzustellen, ob eine Warnung eine harmlose Aktivität oder einen Systemkompromiss darstellt. Vom Endpoint Security bereitgestellte Informationen können Ihnen bei der Beantwortung der folgenden Fragen helfen:

- Wie ist Malware auf einen Host-Endpunkt gelangt?
- Auf welche IP-Adressen wurde zugegriffen?
- Auf welche URLs wurde zugegriffen?
- Welche andere Systeme sind betroffen?
- Was hat der bösartige Prozess sonst getan?

Dieser Teil beschreibt die folgenden Themen:

KAPITEL 20: Forensische Datentypen

Der Endpoint Security kann die folgenden forensischen Datentypen abrufen.

- Dateierfassungen
- Triage Sammlungen
- Datenerfassungen
- Agent Diagnostics

Zusätzlich können Sie Ihr Unternehmen nach spezifischen Regelbedingungen durchsuchen. Siehe Ihr Unternehmen durchsuchen auf Seite 253.

Sie können konfigurieren, wie Erfassungen vom Endpoint Security ausgeführt, gespeichert und gealtert werden . Siehe Erfassungseinstellungen konfigurieren auf Seite 101.

Dateierfassungen

Dateierfassungsanfragen weisen einen Endpoint Security Agent an, eine Datei von seinem Host-Endpunkt abzurufen. Dateierfassungen werden für statische oder dynamische Analyse von potentiellen oder bestätigten Kompromittierungen verwendet, sowie für die Aufbewahrung von Beweisen bei Insider Bedrohungsermittlungen.

Autorisierte Benutzer können eine Dateierfassung anfordern. Siehe Dateierfassungen anfordern auf Seite 315. Die daraus resultierende herunterladbare `.zip` Datei ist mit einer Passphrase leicht verschlüsselt.

Die Sicherheit wird nicht durch Ändern der Passphrase verbessert. Die Passphrase verhindert, dass Antivirus Software das Paket beim Herunterladen als bösartig kennzeichnet. Erfassungspakete können bösartige Inhalte enthalten.

Jede Erfassungsanfrage kann jeweils nur eine Datei von einem individuellen Host Endpunkt abrufen. Sie können die gleiche Datei von mehreren Host Endpunkten mit Hilfe von Host Sätzen anfordern. Sie können andere Dateien von dem gleichen Host Endpunkt

anfordern, indem Sie zusätzliche Anfragen tätigen. Die einzigen Beschränkungen für die Gesamtzahl der Erfassungsanfragen, die Sie für jeden Host-Endpunkt tätigen können, beziehen sich auf die Einstellungen für Erfassungsalterung.

Die Endpoint Security Appliance kann Dateien von auf Netzwerk gemounteten Freigaben nicht aufführen oder erfassen. Wenn Sie versuchen, solche Dateien aufzuführen oder zu erfassen, tritt ein Fehler auf.

Zusätzlich können Dateierfassungen nicht für temporäre Dateien ausgeführt werden.

Triage Sammlungen

Informationen über Host-Endpunkte, die vom FireEye Endpoint Security gesammelt wurden, werden in als Download bereitgestellten `.mans`-Datei Triage-Sammlungen geliefert. Triage-Sammlungen werden automatisch für jede Warnung ausgeführt, der vom Endpoint Security erfasst wurde. Triage-Sammlungen können auch für Hosts mit Warnungen angefordert werden.

HINWEIS: Malware Warnungen lösen keine automatische Triage aus, wie dies bei anderen Warnungen der Fall ist.

Die Triage Summary Seite in der Endpoint Security Web-UI liefert eine Zusammenfassung der Informationen in einer Triage Sammlung, die auf eine mögliche Kompromittierung hinweisen. Dieser Abschnitt der Web-UI wird Triage Viewer genannt. Siehe Triage-Sammlungen im Triage Viewer überprüfen auf Seite 334.

Triage Daten können auch mit Hilfe der folgenden Methoden überprüft werden.

- Sie können Triage Daten im Audit Viewer verarbeiten und anzeigen. Siehe Forensische Daten im Audit Viewer überprüfen auf Seite 339.
- Sie können die gesamte Triage `.mans` Datei herunterladen, um alle Triage Daten in Redline zu überprüfen. Siehe Forensische Daten in Redline überprüfen auf Seite 355.

Triage-nformationen bieten eine Momentaufnahme der Ereignisse, die auf einem Host-Endpunkt zum Zeitpunkt eines Alarms aufgetreten sind. Eine Triage Sammlung kann die folgenden Arten von Informationen enthalten.

- Systeminformation
- Verarbeitungsaktivität
- Dateiaktivität (`*.exe`, `*.dll`, `*.sys`, `*.bat`, `*.ini`)
- Windows und Userverzeichnisse

- Verzeichnisinformationen, einschließlich Informationen über HKEY_CLASSES_ROOT, `.bat`, `.com`, `.exe`, `.hta`, `.pif` Dateien, HKEY_LOCAL_MACHINE, Software, System, HKEY_USERS, Dienste, Persistenzmechanismen und Agent Ereignisse (Ereignis/Ringbuffer)
- Benutzerinformationen
- Aufgabenaktivitäten, einschließlich Auslöser und Aktionen
- Portinformationen
- ARP Einträge
- Routeneinträge
- Prefetch Informationen
- Datenträger- und Volumeninformationen
- Browser URL Verlauf
- Dateidownload-Verlauf

HINWEIS: Stellen Sie sicher, dass Sie Ihre vorhandenen Triage-Sammlungen nach Aufrüstung Ihrer Software aktualisieren. Siehe Erfassungsdaten aktualisieren auf Seite 325.

Weitere Informationen finden Sie in einem der folgenden Themen.

- Triageerfassungen anfordern auf Seite 319
- Erfassungsdaten aktualisieren auf Seite 325
- Forensische Daten herunterladen auf Seite 329
- Triage-Sammlungen im Triage Viewer überprüfen auf Seite 334
- Forensische Daten im Audit Viewer überprüfen auf Seite 339
- Forensische Daten in Redline überprüfen auf Seite 355

Datenerfassungen

Datenerfassungen (manchmal auch *Live Response (Live-Antwort) Anfragen* genannt) ermöglichen Ihnen, Daten, die Sie benötigen, von einem einzelnen laufenden Endpunkt zu erfassen. Mit Hilfe der Data Acquisition Scripts Seite können Sie die für Datenerfassungsanfragen verwendeten Datenerfassungsscripts erstellen, bearbeiten, kopieren und löschen. FireEye liefert mehrere Datenerfassungsscripts (manchmal als *Audits* bezeichnet). Diese Scripts können nicht gelöscht werden, aber Sie können einige davon kopieren und bearbeiten, um Sie als Basis für Ihre eigenen Scripts zu verwenden. Siehe Bereitgestellte Datenerfassungsscripts auf Seite 459.

Wenn eine Datenerfassungsanfrage getätigt wird, sammelt der Endpoint Security Agent auf dem ausgewählten Host-Endpunkt die von dem zugehörigen Datenerfassungsscript angeforderten forensischen Daten.

Von einer Datenerfassung zurückgegebenen Daten können mit Hilfe der folgenden Methoden überprüft werden.

- Sie können die Daten im Audit Viewer verarbeiten und anzeigen. Siehe Forensische Daten im Audit Viewer überprüfen auf Seite 339.
- Sie können die zurückgegebenen Daten in einer `.mans` Datei zurückgeben, um alle Daten in Redline zu überprüfen. Siehe Forensische Daten in Redline überprüfen auf Seite 355.

Für Full Memory und Full Disk Akquisitionen können Sie die zurückgegebenen Daten in einer `.zip` Datei herunterladen.

- Bereitgestellte Datenerfassungsscripts auf Seite 459
- Eine Datenerfassung anfordern auf Seite 321
- Eine Process Detail Datenerfassung anfordern auf Seite 323
- Forensische Daten herunterladen auf Seite 329
- Forensische Daten im Audit Viewer überprüfen auf Seite 339
- Forensische Daten in Redline überprüfen auf Seite 355

Full Memory oder Full Disk Datenerfassungen können mehr Informationen als erwartet zurückgeben und Leistungs- und Speicherprobleme hervorrufen. FireEye empfiehlt, dass Sie den Umfang dieser Scripts begrenzen.

Agent Diagnostics

Agent Diagnostics ist ein spezieller Akquisitionstyp, der verwendet wird, um FireEye Customer Support mit den Daten zu beliefern, die zur Lösung Ihres Problem benötigt werden.

Wenn Agent Diagnostics angefordert werden, sammelt der Endpoint Security Agentauf dem ausgewählten Host-Endpunkt die forensischen Daten und erstellt eine herunterladbare `.zip` Datei, die Sie überprüfen oder and Ihren FireEye Customer Support Mitarbeiter senden können.

- Agent Diagnostics beantragen auf Seite 324
- Forensische Daten herunterladen auf Seite 329
- Agent Diagnostics überprüfen auf Seite 357

KAPITEL 21: Forensische Daten erfassen

Um Warnungen und verdächtige Aktivitäten auf Ihren Host Endpunkten zu untersuchen, müssen Sie zuerst forensische Daten erfassen.

Voraussetzungen

- Analyst, Senior Analyst, Investigator oder Administrator Zugriff

Dateierfassungen anfordern

Sie können Dateien von Hosts mit Hilfe der Endpoint Security Web-UI erhalten. Mehrere Dateierfassungen können gleichzeitig von einem einzigen Windows Endpunkt angefordert werden. Diese Option ist nicht für macOS und Linux Endpunkte verfügbar.

Zusätzlich können Sie mehrere Hosts auswählen und Dateierfassungen von ihnen anfordern, solange die Hosts die gleiche Plattform ausführen. So können Sie zum Beispiel keinen macOS und Linux Host auswählen und Dateierfassungen von ihnen in der gleichen Akquisitionsanfrage anfordern. Sie können allerdings Dateierfassungen von den macOS und Linux Hosts individuell anfordern.

HINWEIS: Versuche, eine *gelöschte* Datei zu abzurufen, funktionieren möglicherweise nicht. Sie können eine gelöschte Datei nicht erfassen, wenn die der Datei zugewiesenen Systemressourcen seit dem Löschen der Datei wiederverwendet wurden.

Dateierfassungen können nicht auf temporären Dateien ausgeführt werden.

WICHTIG: Bei der Erfassungen von Dateien, deren komprimierte Größe 3 GB überschreitet, können möglicherweise keine genaue Download-Größe zurückgeben.

Um eine Dateierfassung von der Hosts Seite anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Im **Actions** Menü wählen Sie **Acquire: File**.
4. Klicken Sie auf **Go**.

   Das **Acquire file from *nnn* host** Dialogfeld wird angezeigt-
5. Geben Sie die erforderlichen Informationen ein. Siehe Datei vom nnn Host Dialogfeld erfassen auf der nächsten Seite.
6. Klicken Sie auf **Acquire**.

Sie können Dateien auch von den host alert details und host details Abschnitten der Hosts Seite erfassen.

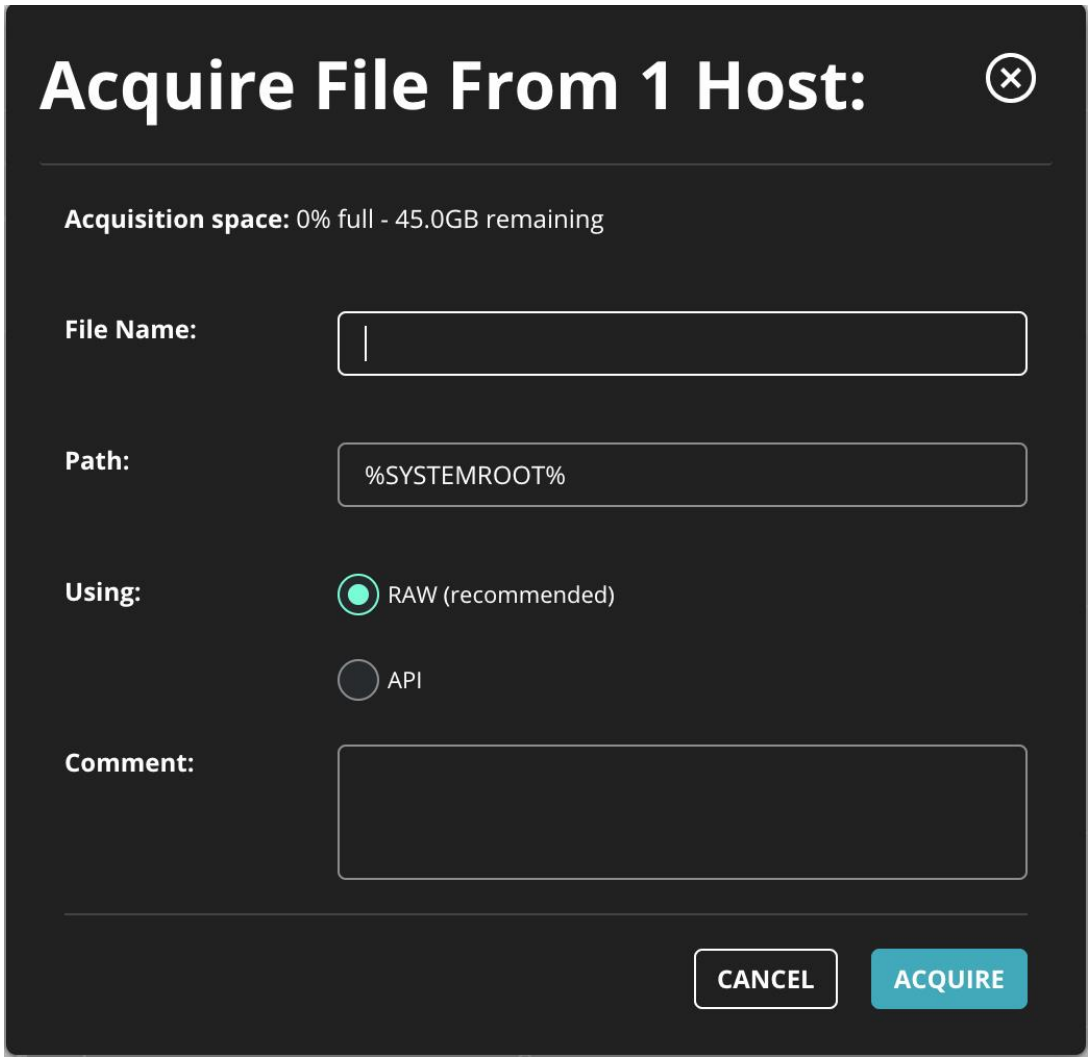
Um Dateien von einem Host Endpunkt mit Hilfe der Host Alert Details oder Host Details Abschnitte zu erfassen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Fordern Sie Host Details an, indem Sie auf das mit einem Host verbundene Erweiterungssymbol (⊕) klicken.
3. Im **Acquire** Menü wählen Sie **File**.

   Das **Acquire file from *nnn* host** Dialogfeld wird angezeigt-
4. Geben Sie die erforderlichen Informationen ein. Siehe Datei vom nnn Host Dialogfeld erfassen auf der nächsten Seite.
5. Klicken Sie auf **Acquire**.

Sie können den Status der Dateierfassung auf der Acquisitions Seite in der **Status** Spalte auf dem Acquisitions Raster überwachen. Der Status wechselt von **Requested** auf **Acquiring** und dann auf **Acquired**, wenn die Erfassung abgeschlossen ist.

Datei vom *nnn* Host Dialogfeld erfassen



Das **Acquire file from *nnn* host** Dialogfeld enthält die folgenden Felder:

Feld	Beschreibung
File Name	Geben Sie den Namen der Datei ein, die Sie erfassen wollen. Der ursprüngliche Dateiname wird in der herunterladbaren `.zip` Datei gespeichert, nachdem die Datei erfasst wurde. Dateinamen, die Doppelbytezeichen enthalten, überschreiten möglicherweise das 255 Zeichen Limit. Wenn dies geschieht, wird der Dateiname auf seine ersten 200 Zeichen abgekürzt. Wenn Sie eine erfasste Datei mit Doppelbytezeichen im Dateinamen speichern, wird die Datei gespeichert, aber die Double-Byte Zeichen werden durch Unterstriche ersetzt. Alle Dateinamen in der `.zip` Datei enthalten einen Unterstrich am Ende des Dateinamens. Dies schützt Ihr System, nachdem Sie die Datei extrahiert haben und stellt sicher, dass eine bösartige Datei nicht versehentlich ausgeführt werden kann.
Path	Geben Sie den vollständigen Pfad ein, in dem die Datei gespeichert werden soll. Bestimmen Sie einen genauen Pfadnamen oder eine andere geeignete, pfad-basierte Windows Umgebungsvariable. Beispielsweise ist die Standard Umgebungsvariable in dieser Tafel `%systemroot%`. Dies erweitern den Pfad, auf dem Windows installiert ist, normalerweise `C:\Windows\`. Sie müssen den Laufwerksbuchstaben oder Pfadnamen festlegen. Unterschiedliche Endpunkte können verschiedene Laufwerkzuordnungen haben. Wenn Sie ausdrücklich einen Ordnernamen angeben, können Sie den Pfad mit einem Backslash beenden. Der letzte Backslash ist jedoch nicht obligatorisch. Seien Sie vorsichtig, wenn Sie System Umgebungsvariable in Ordnerpfaden festlegen. Die erweiterten Pfade der in Ordnerpfaden festgelegten System Umgebungsvariablen unterscheiden sich je nach der installierten Version von Windows. Vollständige Informationen zu Windows Umgebungsvariablen finden Sie in der Windows Dokumentation (Microsoft TechNet). Benutzerspezifische Umgebungsvariablen (die den Benutzernamen in ihrem erweiterten Pfad enthalten), z. B.% APPDATA% oder% USERPROFILE%, werden nicht unterstützt. Da Sie den Benutzer, für den eine Umgebungsvariable gilt, nicht angeben können, muss die erweiterte Umgebungsvariable nicht unbedingt der Benutzer sein, der auf dem Endpunkt Host angemeldet ist.

Feld	Beschreibung
Using (Nur Windows)	Wählen Sie entweder RAW oder API. FireEye empfiehlt die Verwendung der RAW (Standard) -Einstellung. Obwohl RAW-Audits langsam sein können und manchmal auf einigen RAID oder verschlüsselten Geräten fehlschlagen könnten, können sie gesperrte und gelöschte Dateien wiederherstellen, die API Audits ggf. nicht finden konnten. Wenn eine RAW Akquisitionsanfrage fehlschlägt, können Sie versuchen, die Datei erneut mit Hilfe von API zu erfassen. Ein schwerwiegender Fehler kann zurückgegeben werden, wenn RAW Modus angefordert wurde und der Dateipfad nicht gefunden werden kann. Die Option ist nicht für macOS und Linux Endpunkte verfügbar, weil nur die API-Option gültig ist.
Comment	Optional können Sie den Grund für das Abrufen der Datei eingeben.

Triageerfassungen anfordern

Sie können Triage-Sammlungen von Hosts mit Hilfe der Endpoint Security Web-UI erfassen. Mehrere Triagesammlungen können gleichzeitig von einem Host angefordert werden. Zusätzlich können Sie mehrere Hosts auswählen und Triagesammlungen von ihnen anfordern.

HINWEIS: Malware Alarme in Windows Umgebungen lösen keine automatische Triage aus, wie dies bei anderen Alarmen der Fall sein kann (je nach den Einstellungen für automatische Triage-Erfassung).

Der FireEye Endpoint Security Agent benötigt Internetzugriff während der Triage-Sammlung, um digitale Signaturen zu validieren. Wenn der Computer, auf dem der Agent installiert ist, keinen Zugriff auf das Internet hat, könnte die Triagesammlung erheblich verzögert werden. Wenn das System konfiguriert ist, ein Proxy für den Zugriff auf das Internet zu verwenden, stellen Sie sicher, dass das lokale Systemkonto konfiguriert ist, das Proxy zu verwenden, um Verzögerungen bei der Triagesammlung zu verhindern.

Um eine Triageerfassung von der Hosts Seite anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Im **Actions** Menü wählen Sie **Acquire: Triage**.

4. Klicken Sie auf **Go**.

   Das **Acquire triage from *nnn* host** Dialogfeld wird angezeigt.

5. Geben Sie die erforderlichen Informationen ein. Siehe Triage für nnn Host Dialogfeld erfassen.

6. Klicken Sie auf **Acquire**.

Sie können Triagen auch von den host alert details und host details Abschnitten der Hosts Seite erfassen.

Um Triagen von einem Host Endpunkt mit Hilfe der Host Alert Details oder Host Details Abschnitte zu erfassen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Fordern Sie Host Details an, indem Sie auf das mit einem Host verbundene Erweiterungssymbol (⊕) klicken.
3. Im **Acquire** Menü wählen Sie **Triage**.

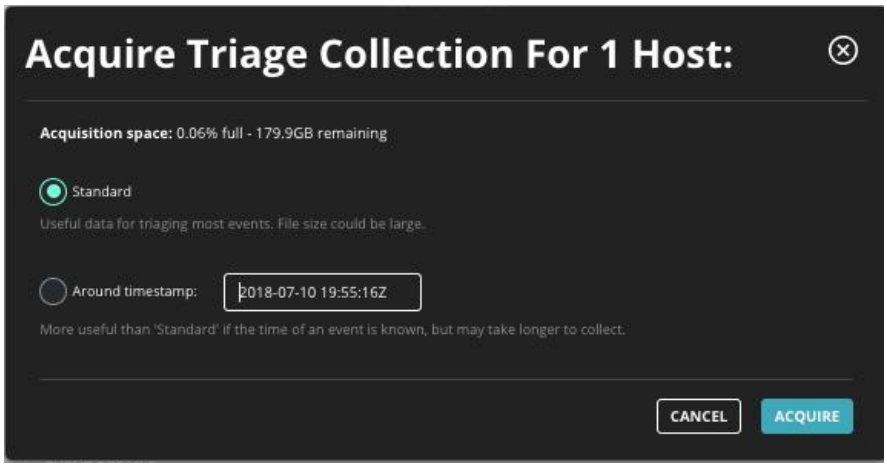
   Das **Acquire triage from *nnn* host** Dialogfeld wird angezeigt.

4. Geben Sie die erforderlichen Informationen ein. Siehe Triage für nnn Host Dialogfeld erfassen.
5. Klicken Sie auf **Acquire**.

Sie können den Status einer Akquisitionsanfrage in der Status Spalte der Acquisitions Seite überwachen. Der Status wechselt von **Requested** auf **Acquiring** und dann auf **Acquired**, wenn die Akquisition fertig ist.

Weitere Informationen über erfasste Triagedaten finden Sie unter Forensische Daten herunterladen, Forensische Daten in Redline überprüfen und Triage-Sammlungen im Triage Viewer überprüfen.

Triage für *nnn* Host Dialogfeld erfassen



Verwenden Sie das **Acquire triage for *mm* host** Dialogfeld, um eine Standard oder Zeitstempel Triage zu wählen.

Wenn Sie **Standard** auswählen, fordert die Endpoint Security Appliance Informationen von dem Host für alle Daten rund um ein Ereignis an.

Wenn Sie **Around timestamp** wählen, geben Sie das Datum und die Uhrzeit im folgenden Format ein: `yyyy-mm-dd hh:mm:ssz` Die Zeiten werden in UTC (Coordinated Universal Time) ausgedrückt und verwenden den speziellen UTC Designator **Z**.

```
2013-04-11 20:09:13Z
```

Einstellungen für den Triage-Zeitstempel treffen nur auf Agent URL Ereignisse (`URL Monitor Events`) und Verzeichnisschlüssel Ereignisse (`Reg Key Events`) zu.

Die Endpoint Security Appliance fordert Informationen vom Host für einen festgelegten Zeitraum um den Zeitstempel an. Informationen über die Einstellung des Zeitraums um den Zeitstempel finden Sie unter Zeitstempel-Einstellungen konfigurieren auf Seite 118.

Eine Datenerfassung anfordern

Sie können Daten von einem Host mit Hilfe der Endpoint Security Web-UI erfassen. Mehrere Datenerfassungen können gleichzeitig von einem Host angefordert werden. Zusätzlich können Sie mehrere Hosts auswählen und Datenerfassungen von ihnen anfordern.

Voraussetzungen

- Analyst, Senior Analyst, Investigator oder Administrator Zugriff
- Die Daten, die Sie erfassen wollen, werden in einem Datenerfassungsscript definiert. Siehe Datenerfassungsscripts verwalten.
- Eine aktive Endpoint Security Power Lizenz ist installiert. Sehen Sie "Lizenz-Management" im *Endpoint Security Server System-Administrationshandbuch*.

  Wenn Ihre Lizenz abläuft, nachdem Sie Ihre eigenen Datenerfassungsscripts erstellt habe oder die gelieferten Script bearbeitet haben, können Sie diese Scripts auf der Data Acquisition Scripts Seite sehen, aber Sie können sie nicht bearbeiten oder zum Erfassen von Daten verwenden. Sie können sie exportieren.

Eine Datenerfassung von der Hosts Seite anfordern

Um eine Datenerfassung von der Hosts Seite anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.

   HINWEIS: Wenn Sie mehrere Hosts aussuchen, sind die folgenden gelieferten Datenerfassungen nicht verfügbar: Driver Memory, Full Disk, Full Memory und Process Memory. Sie sind nur verfügbar, wenn ein einzelner Host ausgewählt ist.

3. Im **Actions** Menü wählen Sie das Datenerfassungsscript, das verwendet werden soll.

   VORSICHT: Full Memory oder Full Disk Datenerfassungen können mehr Informationen als erwartet zurückgeben und Leistungs- und Speicherprobleme hervorrufen. FireEye empfiehlt, dass Sie den Umfang dieser Scripts begrenzen.

4. Wenn das von Ihnen ausgewählte Datenerfassungsscript, zusätzliche Informationen erfordert, wird ein Aquire Dialogfeld angezeigt. Geben Sie die Informationen ein und klicken Sie auf **Acquire**. Weitere Informationen über jedes Dialogfeld finden Sie unter Bereitgestellte Datenerfassungsscripts.

   Wenn das Script keine weiteren Informationen erfordert. wird die Datenerfassungsanfrage automatisch eingereicht.

Sie können auch Datenerfassungen von den Host Alert Details und Host Details Abschnitten auf der Hosts Seite anfordern.

Eine Datenerfassung von einer Host Details Seite anfordern

Um eine Datenerfassung von einem Host Endpunkt mit Hilfe der Host Alert Details oder Host Details Abschnitte anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Fordern Sie Host Details an, indem Sie auf das mit einem Host verbundene Erweiterungssymbol (⊕) klicken.

3. Im **Acquire** Menü wählen Sie das Datenerfassungsscript, das verwendet werden soll.

   VORSICHT: Full Memory oder Full Disk Datenerfassungen können mehr Informationen als erwartet zurückgeben und Leistungs- und Speicherprobleme hervorrufen. FireEye empfiehlt, dass Sie den Umfang dieser Scripts begrenzen.

4. Wenn das von Ihnen ausgewählte Datenerfassungsscript, zusätzliche Informationen erfordert, wird ein Aquire Dialogfeld angezeigt. Geben Sie die Informationen ein und klicken Sie auf **Acquire**. Weitere Informationen über jedes Dialogfeld finden Sie unter Bereitgestellte Datenerfassungsscripts.

   Wenn das Script keine weiteren Informationen erfordert. wird die Datenerfassungsanfrage automatisch eingereicht.

Sie können den Status einer Erfassungsanfrage in der Status Spalte der Acquisitions Seite überwachen. Der Status wechselt von **Requested** auf **Acquiring** und dann auf **Acquired**, wenn die Erfassung abgeschlossen ist.

Weitere Informationen über erfasste forensische Daten finden Sie unter Forensische Daten herunterladen und Forensische Daten in Redline überprüfen.

Eine Process Detail Datenerfassung anfordern

Verwenden Sie die Anweisungen in diesem Thema, um Process Details Daten von einem Host mit Hilfe der Endpoint Security Web-UI zu erfassen. Sie können Process Detail Datenerfassungen nur für eine Triage des Hosts anfordern.

Voraussetzungen

- Analyst, Senior Analyst, Investigator oder Administrator Zugriff
- Eine Triage muss bereits für einen Windows, macOS oder Linux Host Endpunkt erworben worden sein.

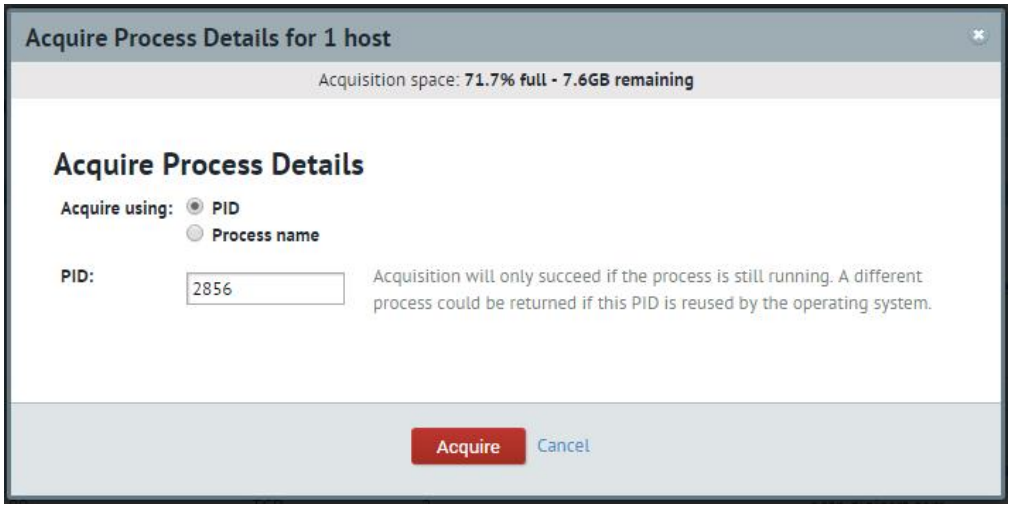
Um eine Process Detail Datenerfassung anzufordern:

1. Auf der Acquisitions Seite wählen Sie eine Triageerfassung, für die Sie Process Detail Daten erfassen wollen.
2. Im Acquisition Detail Bereich der Seite wählen Sie **Triage Summary**.

   Der Triage Viewer wird geöffnet.

3. Wählen Sie den Prozess, für den Sie Process Detail Daten erfassen wollen. Sie können den Prozess auch später im Acquire Process Details Dialogfeld auswählen.
4. Wählen Sie **Acquire process details**.

   Das Acquire Process Details Dialogfeld wird angezeigt. Wenn Sie bereits einen Prozess ausgewählt haben, wird er angezeigt, wenn das Dialogfeld geöffnet wird.



5. Wählen Sie entweder **PID** (Prozess ID) oder **Process name** und geben Sie die Prozess ID oder Namen ein.
6. Klicken Sie auf **Acquire**.

Sie können den Status der Process Details Akquisitionsanfrage in der Status Spalte der Acquisitions Seite überwachen. Der Status wechselt von **Requested** auf **Acquiring** und dann auf **Acquired**, wenn die Akquisition fertig ist.

Weitere Informationen über erfasste forensische Daten finden Sie unter Forensische Daten herunterladen und Forensische Daten in Redline überprüfen.

Agent Diagnostics beantragen

Sie können Agent Diagnostics von einem Host mit Hilfe der Endpoint Security Web-UI abrufen.

Voraussetzungen

- Analyst-, Senior Analyst- oder Administratorzugriff
- Der Host führt die FireEye Endpoint Security Agent Version 20 oder später aus.

Um Agent Diagnostics zu beantragen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie den Host, für den Sie Agent Diagnostics erhalten möchten.
3. Im **Actions** Menü wählen Sie **Acquire: Agent Diagnostics**.
4. Klicken Sie auf **Go**.

Sie können den Status einer Erfassungsanfrage in der Status Spalte der Acquisitions Seite überwachen. Der Status wechselt von **Requested** auf **Acquiring** und dann auf **Acquired**, wenn die Erfassung fertig ist.

HINWEIS: Der folgende Fehler deutet an, dass zum Zeitpunkt der Anfrage das Agent Protokoll aktiv geschrieben wurde und ausgelastet war.

`1729, MX_API_SQLITE_DATABASE_BUSY, "SQL database busy".`

Wenn dieser Fehler auftritt, reichen Sie die Anfrage erneut ein.

Erfassungsdaten aktualisieren

Möglicherweise müssen Sie Ihre vorhandenen Triage- oder Datenerfassungen aktualisieren, nachdem Sie Ihre Endpoint Security Software aktualisiert haben. Erfassungen, die aktualisiert werden müssen, haben den Status **Update required**.

Um eine Akquisition von der Acquisitions Seite zu aktualisieren:

1. Im Acquisitions Raster auf der Acquisitions Seite wählen Sie die Trage Sammlung.

   Details über die Triage Sammlung werden im Acquisition Detail Abschnitt angezeigt.
2. Wählen Sie **Update acquisition** auf dem **Actions** Menü und klicken Sie auf **Go**.

   Der **Update required** Status verschwindet.

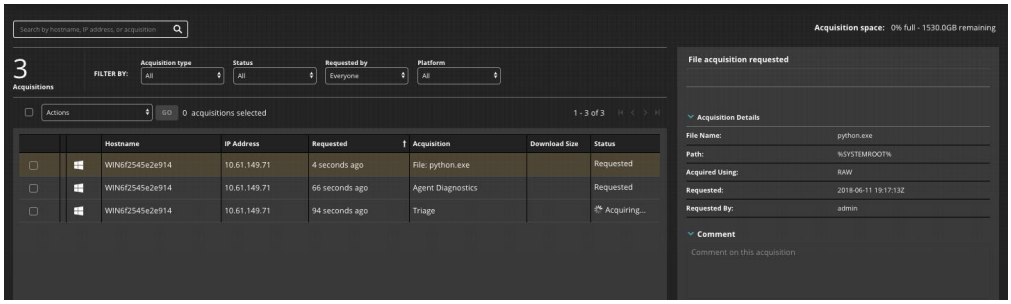
KAPITEL 22: Erfassungen auflisten

Sie können die Datei, Triage und Datenerfassungen, die Sie in der Endpoint Security Web-UI gesammelt haben, auflisten.

Um die Erfassungen aufzulisten:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Acquisitions** am Anfang der Seite.

   Die Acquisisitons Seite wird angezeigt.



Weitere Informationen finden Sie unter Acquisitions Seite auf Seite 73.

Voraussetzungen

- Analyst, Senior Analyst, Investigator oder Administrator Zugriff

KAPITEL 23: Forensische Daten herunterladen

Sie können erfasste Dateien, Triage Sammlungen, Agent Diagnostics und Host Endpunkt Daten von der Acquisitions Seite mit Hilfe der Endpoint Security Web UI finden und herunterladen.

Die Status Spalte auf dem Acquisitions Raster der Acquisitions Seite zeigt den Fortschritt einer Triage- oder Datenerfassungsanfrage. Der Status wechselt von **Requested** auf **Acquiring** und dann auf **Acquired** (wenn die Acquisition zum Herunterladen bereit ist).

Die folgende Tabelle fasst die Akquisitionsdateien zusammen, die Sie für jeden Akquisitionstyp herunterladen können.

Akquisitionstyp	Dateityp	Beschreibung
Files	`.zip`	Die `.zip` Datei enthält die Dateien, die Sie erfasst haben. Alle Dateinamen in der `.zip` Daten haben am Ende des Dateinamens einen Unterstrich. Dies schützt Ihr System, nachdem Sie die Datei extrahiert haben und stellt sicher, dass eine bösartige Datei nicht versehentlich ausgeführt wird.
Triages	`.mans`	Die Endpoint Security Appliance liefert eine Zusammenfassung der Triagedaten im Triage Viewer, wenn mögliche kompromittierende Informationen in einer Triage Sammlung identifiziert wird. Siehe Triage-Sammlungen im Triage Viewer überprüfen auf Seite 334. Sie können auch alle Triagedaten im Audit Viewer verarbeiten und überprüfen, oder die gesamte Triage `.mans` Datei herunterladen und alle Triagedaten in Redline überprüfen. Siehe Forensische Daten im Audit Viewer überprüfen auf Seite 339 und Forensische Daten in Redline überprüfen auf Seite 355

Akquisitionstyp	Dateityp	Beschreibung
Data	`.mans` oder `.zip`	Die meisten Datenerfassungen erzeugen eine herunterladbare `.mans` Datei, die in Redline überprüft werden kann. Siehe Forensische Daten in Redline überprüfen auf Seite 355. Sie können alle erfassten Daten auch im Audit Viewer verarbeiten und überprüfen. Siehe Forensische Daten im Audit Viewer überprüfen auf Seite 339. Die Full Memory und Full Disk Scripts erzeugen eine herunterladbare `.zip` Datei. Extrahieren Sie den Inhalt der Zip-Datei mit Hilfe eines Unzip-Tools. Finden und konvertieren Sie die Datei mit der größten Dateigröße auf Imageformat (`*.img`). Öffnen Sie dann die Image Formatdatei mit einem open Source forensischem Tool (z.B.Forensic Toolkit (FTK) oder dem Speicher Forensik-Framework der Volatility Foundation).
Agent Diagnostik	`.zip`	Diese `.zip` Datei enthält die Daten, die FireEye Customer Support benötigt, um Probleme zu beheben.

Sie können erfasste forensische Daten von den Hosts oder Acquisitions Seiten herunterladen. Triage Erfassungsdateien können auch von der Triage Summary Seite herunterladen.

Voraussetzungen

- Analyst, Senior Analyst, Investigator oder Administrator Zugriff

Forensische Daten von der Hosts Seite herunterladen

Um erfasste forensische Daten von der Hosts Seite herunterzuladen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Klicken Sie in der Liste auf einem der Register auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Alert Detail Informationen benötigen.

   Die Host Alert Details werden angezeigt.
3. Finden Sie die Akquisition im Acquisitions Raster am Ende der Seite.

4. Klicken Sie auf **Download** oder **Download Full Triage**. Der Linkname hängt von der Art der forensischen Datenerfassung ab, die Sie ausgewählt haben.

Die Erfassungsdatei wird auf Ihren Computer heruntergeladen. Informationen zum Überprüfen forensischer Daten finden Sie unter Forensische Daten überprüfen auf Seite 333.

Forensische Daten von der Acquisitions Seite herunterladen

Um erfasste forensische Daten von der Acquisitions Seite herunterzuladen:

1. Wählen Sie **Acquisitions** in der Endpoint Security Web-UI.
2. Filtern Sie optional die Liste der Akquisitionen im Acquisitions Raster, indem Sie auf dem Register einen Akquisitionstyp vom **Acquisition type** Menü auswählen. Sie können **File**, **Triage**, **Data** oder **Agent Diagnostics** auswählen. Sie können auch nach dem Status der Akquisition und nach dem Benutzer filtern, der die Erfassung angefordert hat.
3. Im Acquisitions Raster wählen Sie die Zeile, die den Akquisitionsdaten entspricht, die Sie herunterladen wollen.

   Details über die Akquisition werden im Acquisition Detail Abschnitt angezeigt. Sie können diese Details im Acquisition Detail Bereich erweitern, um einige der Akquisitionsdaten zu überprüfen.
4. Klicken Sie auf **Download** oder **Download full triage** im Acquisition Detail Bereich. Der Linkname hängt von der Art der forensischen Datenerfassung ab, die Sie ausgewählt haben.

Die Erfassungsdatei wird auf Ihren Computer heruntergeladen. Informationen zum Überprüfen forensischer Daten finden Sie unter Forensische Daten überprüfen auf Seite 333.

Eine Triage von der Triage Summary Seite herunterladen

Um eine Triage `.mans` Datei von der Triage Summary Seite herunterzuladen:

1. Rufen Sie die Triage Summary Seite für eine Triage ab. Weitere Informationen finden Sie unter Zugriff auf die Triage Summary auf Seite 336.

2. Klicken Sie am Anfang der Triage Summary Seite auf **Download full triage**.

   Die Erfassungsdatei `.mans` wird auf Ihren Computer heruntergeladen.

   Heruntergeladene `.mans` Dateien können mit Redline geöffnet und überprüft werden. Weitere Informationen finden Sie unter Forensische Daten in Redline überprüfen auf Seite 355.

KAPITEL 24: Forensische Daten überprüfen

Sie können forensische Daten überprüfen, die Sie von Ihren Host Endpunkten gesammelt haben.

- Heruntergeladene Dateierfassungen überprüfen auf der nächsten Seite
- Triage-Sammlungen im Triage Viewer überprüfen auf der nächsten Seite
- Auto-Triage in Storytime überprüfen auf Seite 339
- Forensische Daten im Audit Viewer überprüfen auf Seite 339
- Forensische Daten in Redline überprüfen auf Seite 355
- Agent Diagnostics überprüfen auf Seite 357

Wenn die Summe der entpackten Größen der in einer Erfassung (oder Triage Sammlung) enthaltenen Audits 3 GB überschreitet, wird eine Fehlermeldung angezeigt, die darauf hinweist, dass die Erfassung nicht im Audit Viewer oder im Triage Viewer angezeigt werden kann.

Exploit Guard Daten können derzeit nicht im Audit Viewer angezeigt werden.

Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.

Voraussetzungen

- Analyst, Senior Analyst, Investigator oder Administrator Zugriff

Heruntergeladene Dateierfassungen überprüfen

Um eine heruntergeladene Dateierfassung zu überprüfen:

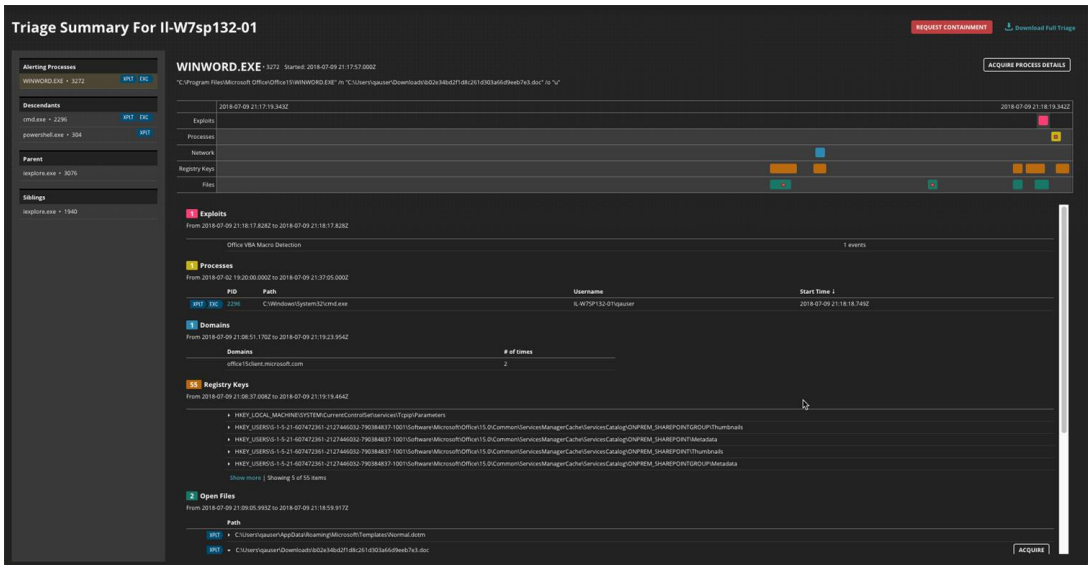
1. Öffnen Sie die Dateiakquisition `.zip` Datei.
2. Geben Sie das erforderliche Passwort ein, um die Datei zu öffnen. Sie können den Mauszeiger über den **Download** Link im Detail Fenster, um das Passwort anzuzeigen. Weiter Informationen über dieses Passwort finden Sie unter Erfassungseinstellungen konfigurieren auf Seite 101.
3. Öffnen und überprüfen Sie die Dateien innerhalb der `.zip` Datei mit Hilfe eines Text- oder XML-Editors.

Triage-Sammlungen im Triage Viewer überprüfen

Die Endpoint Security Appliance bietet eine Zusammenfassung der Triage auf der Triage Summary Seite, wenn eine Triage-Sammlung Alarme oder andere Informationen enthält, die auf eine System-Kompromittierung hinweisen könnte. Die Triage Summary ist eine hochgradige Ansicht der Triage Daten.

Wenn die Summe der entpackten Größen der in einer Triage Sammlung enthaltenen Audits 3 GB überschreitet, wird eine Fehlermeldung angezeigt, die darauf hinweist, dass die Akquisition nicht im Triage Viewer (oder dem Audit Viewer) angezeigt werden kann.

Um alle Triage Daten anzuzeigen, verwenden Sie den Audit Viewer oder Redline.



Auf der linken Seite der Triage Summary werden alle Warnvorgänge auf dem Host Endpunkt aufgelistet, die in der Triage-Sammlung enthalten sind. Symbole, die die Warnungstypen identifizieren, die für jeden Prozess auf dem Host auftreten: Exploit (XPLT), Präsenz (PRS) oder Ausführung (EXC). Wenn ein ausgenutzter Prozess abgebrochen wird oder der Start blockiert wird, wird das Blockiersymbol (BLK) angezeigt. Wenn ein Versuch, einen ausgenutzten Prozess zu blockieren oder zu beenden fehlschlägt, wird das Blockierung fehlgeschlagen Symbol (FAIL) angezeigt. Klicken Sie auf diese Symbole, um zusätzliche Informationen zu erhalten.

Zeitleisten oben auf der Triage Summary zeigen an, wann Vorgänge erstellt wurden, Netzwerkzugriffe (einschließlich DNS, IP und URL Zugriffe) stattfanden und Verzeichnis- und Dateischreibvorgänge von einem Warnungsvorgang ausgeführt wurden. Die roten Punkte in den Zeitleisten identifizieren die Alarme im zeitlichen Verlauf. Klicken Sie auf einen der roten Punkte (oder seinen Ereignisblock), um detailliertere Informationen über die Warnung zu sehen.

Der untere Bereich der Triage Summary Seite bietet zusätzliche Einzelheiten über den ausgewählten Warnungsvorgang und zeigt an:

- Vorgänge, die erstellt wurden
- Domains, auf die zugegriffen wurde
- Verbindungen mit IP-Adressen
- URLs, die Alarme erstellt haben, weil sie mit einem IOC übereinstimmen (andere URLs sind nicht eingeschlossen)
- Erkannte Expoits
- Registrierungsschlüssel, die erstellt oder geändert wurden
- Dateien, die geschrieben wurden

- Symbole, die die Warnungstypen identifizieren, die auf dem Host aufgetreten sind: Exploit (XPLT), Präsenz (PRS) oder Ausführung (EXC).
- Wenn ein ausgenutzter Prozess abgebrochen wird oder der Start blockiert wird, wird das Blockiersymbol (BLK) angezeigt. Wenn ein Versuch, einen ausgenutzten Prozess zu blockieren oder zu beenden fehlschlägt, wird das Blockierung fehlgeschlagen Symbol (FAIL) angezeigt.

Sie können auf Vorgangs-IDs, URLs, Dateien, Exploits und Verzeichnisschlüssel klicken, um detailliertere Informationen darüber anzuzeigen.

Sie können auf das Symbol für einen Warnungstyp im Details Bereich, um die Alarme als ein Falsch Positiv zu markieren. Weitere Informationen finden Sie unter Falsch positiv Regeln auf der Triage Summary Seite definieren auf Seite 410

Verwenden Sie die Schaltflächen im oberen Bereich der Triage Summary:

- **Request containment**—Fordern Sie an, den Host einzudämmen, für den die Triage erstellt wurde.
- **Cancel containment request**—Brechen Sie eine Anfrage ab, den Host einzudämmen, für den die Triage erstellt wurde.
- **Triage Summary**—Wählen Sie andere Triage Sammlungen für den gleichen Host.
- **Download full triage**—Laden Sie die Triage `.mans` Datei auf Ihren Computer herunter. Die vollständige Triage kann mit Hilfe von Redline überprüft werden. Weitere Informationen finden Sie unter Forensische Daten in Redline überprüfen.
- **Acquire process details** —Fordern Sie eine Prozessdetailerfassung für den im linken Fenster ausgewählten Prozess an. Diese Anforderung erfasst Details über den Prozess. Sie können die Daten im Audit Viewer überprüfen. Wenn Sie die Erfassung herunterladen, können die Daten in Redline überprüft werden. Die erfassten Daten enthalten Zeichenfolgen im Speicher für den Prozess.

Zugriff auf die Triage Summary

Wenn die Triage im noch verarbeitet wird, ist die Triage Summary nicht verfügbar. Eine Nachricht wird im Detailbereich angezeigt.

Sie können auf die Triage Summary Seite auf der Acquisitions Seite oder im Host Alert Detail Bereich der Hosts Seite zugreifen.

Um eine Triage in der Triage Summary anzuzeigen:

1. Auf der Acquisitions Seite wählen Sie die Akquisition. Wenn die Triage Warnungen enthält, wird automatisch eine Triage Summary (Zusammenfassung) erstellt, und im Detailbereich für den ausgewählten Akquisitionslink wird ein Link angezeigt.

Auf der Hosts Seite erweitern Sie (klicken Sie auf das ⊕ Symbol) den Host, für den Triage Daten gesammelt wurden und überprüfen Sie die Host Alert Details.

2. Klicken Sie im Detail Bereich der Acquisitions Seite auf **Triage Summary**. Die Triage Summary für die ausgewählte Triageerfassung wird angezeigt.

   Klicken Sie am unteren Rand des Host Alert Details Abschnitts der Host Seite auf **View triage** für die Triage, die Sie überprüfen wollen.

Auto-Triage in Storytime überprüfen

Das Storytime Systemmodul verarbeitet Warnungen von Indicators of Compromise (IOC) und Exploit Guard (EXG), die ein zugehöriges Auto-Triage-Paket enthalten. Storytime analysiert die Auto-Triage-Artefakte, generiert eine Kapiteldatei und speichert sie in der Datenbank. Wenn zwei oder drei IOC- oder EXG-Warnungen kurz hintereinander generiert werden, generiert Storytime mehrere Kapiteldateien und speichert diese in der Datenbank. Dies bietet dem Administrator eine Auto-Triage Sammlung, in der er jede individuelle Warnung und die Beziehung zwischen den Warnungen untersuchen kann. Wenn der Endpoint Security Server mit Helix integriert ist, streamt er die Kapiteldatei an Helix.

Verwenden Sie die Storytime Visualization, um eine grafische Darstellung der Triagedaten anzuzeigen. Storytime fokussiert auf die wichtigsten Daten der Auto-Triage in der Warnung und zeigt den kritischen Pfad auf den Ereignisknoten an, der die Erkennung ausgelöst hat. Die Visualisierung stellt sicher, dass Endpoint Security Nutzer Warnungen schnell analysieren und präventive und korrigierende Maßnahmen ergreifen können. Weitere Informationen finden Sie unter Storytime Systemmodul.

Forensische Daten im Audit Viewer überprüfen

Sie können die forensischen Daten im Audit Viewer untersuchen, die in einer Triage oder Datenerfassung gesammelt wurden.

Um die Daten im Audit Viewer anzuzeigen:

1. Verarbeiten Sie die Akquisition. Siehe Die Erfassung verarbeiten auf der nächsten Seite.
2. Zeigen Sie die Akquisition im Audit Viewer an. Siehe Die Erfassungsdaten anzeigen auf Seite 342.

Wenn die forensischen Daten im Audit Viewer angezeigt werden, können Sie die gewünschten Daten auswählen, Daten suchen, Spalten bearbeiten, Daten filtern und sortieren, Datenzeilen taggen und Kommentare hinzufügen. Sehen Sie die folgenden Abschnitte:

Wenn die Summe der entpackten Größen der Audits, die in einer Akquisition enthalten sind, 3 GB überschreitet, wird eine Fehlermeldung angezeigt, die angibt, dass die Akquisition nicht im Audit Viewer angezeigt werden kann.

Exploit Guard Daten können derzeit nicht im Audit Viewer angezeigt werden.

Zwei Einträge für Agent Ereignisse werden derzeit im Audit Viewer für automatische Triage Anforderungen angezeigt.

Voraussetzungen

- Analyst, Senior Analyst, Investigator oder Administrator Zugriff

Die Erfassung verarbeiten

Bevor Sie den Audit Viewer zum Anzeigen der forensischen Daten verwenden können, die in einer Triage oder Datenerfassung enthalten sind, müssen Sie die Erfassung verarbeiten. Sie können dies von der Acquisitions Seite tun, oder während Sie die Host Alert Details überprüfen.

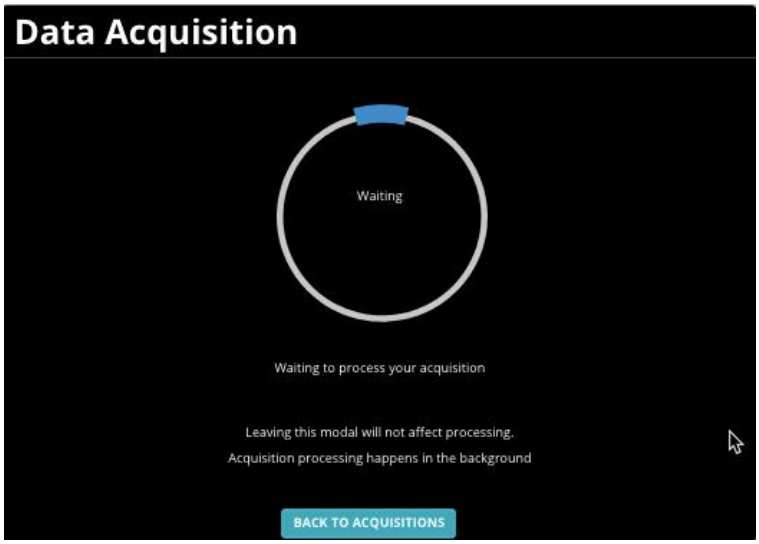
Eine Erfassung von der Acquisitions Seite verarbeiten

Um eine Erfassung für den Audit Viewer von der Acquisitions Seite zu verarbeiten:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Greifen Sie auf die Acquisitions Seite zu, indem Sie **Acquisitions** am Anfang der Seite auswählen.
3. Auf der Acquisitions Seite wählen Sie die Akquisition.

4. Klicken Sie auf **Process Data Acquisition** im Detailfenster der Acquisitions Seite.

   Ein Dialogfeld für die Data Acquisition Verarbeitung wird angezeigt.



   Je nach Größe der Erfassungsdatei kann die Verarbeitung einige Minuten dauern. Sie können darauf warten, dass die Erfassung verarbeitet wird oder auf die Acquisitions Seite zurückkehren und an anderen Dingen arbeiten.

   - Wenn Sie darauf warten, dass die Erfassung verarbeitet wird, wird der Audit Viewer geöffnet und zeigt die Erfassungsdaten an, wenn die Verarbeitung abgeschlossen ist.
   - Wenn Sie auf **Back to Acquisitions** klicken, um auf die Acquisitions Seite zurückzukehren, wird die Verarbeitung der Erfassung fortgesetzt. Wenn die Verarbeitung abgeschlossen ist, wechselt die **Process Data Acquisition** Schaltfläche im Detailfenster der Acquisitions Seite auf eine **View Data Acquisition** Schaltfläche.

Eine Erfassung während der Überprüfung von Host Alert Details verarbeiten:

Um eine Erfassung für den Audit Viewer bei der Überprüfung von Host Alert Details zu verarbeiten:

1. Greifen Sie auf die Hosts Seite zu, indem Sie **Hosts** am Anfang der Endpoint Security Web-UI auswählen.
2. Wählen Sie den **Hosts With Alerts** Tab.
3. Klicken Sie auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Warnungsdetails und Akquisitionsinformationen überprüfen wollen.

4. Im Acquisitions Abschnitt am Ende der Host Alert Details Seite klicken Sie auf **Process Data Acquisition** für die Erfassung, die Sie überprüfen wollen.

   Ein Dialogfeld für die Data Acquisition Verarbeitung wird angezeigt.

   Je nach Größe der Erfassungsdatei kann die Verarbeitung einige Minuten dauern. Sie können darauf warten, dass die Erfassung verarbeitet wird oder auf die Host Alert Details zurückkehren, um an anderen Dingen zu arbeiten.

   - Wenn Sie darauf warten, dass die Erfassung verarbeitet wird, wird der Audit Viewer geöffnet und zeigt die Erfassungsdaten an, wenn die Verarbeitung abgeschlossen ist.
   - Wenn Sie auf **Back to Host Details** klicken, um auf die Host Alert Detailinformationen zurückzukehren, wird die Erfassungsverarbeitung fortgesetzt. Wenn die Verarbeitung abgeschlossen ist, wechselt die **Process Data Acquisition** Schaltfläche im Detailfenster der Acquisitions Seite auf eine **View Data Acquisition** Schaltfläche.

Die Erfassungsdaten anzeigen

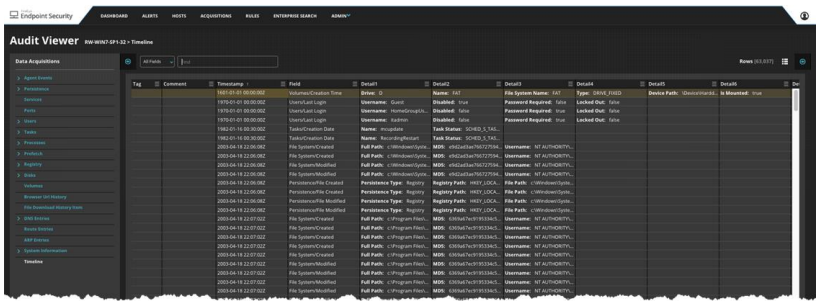
Akquisitionen werden im Audit Viewer von der Acquisitions Seite oder dem Host Alert Details Bereich geöffnet.

Um die verarbeiteten Erfassungsdaten im Audit Viewer von der Acquisitions Seite oder dem Host Alert Details Bereich anzuzeigen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Greifen Sie auf die Acquisitions Seite oder den Host Alert Details Bereich zu.
3. Wählen Sie die Triage oder Datenerfassung, die die Erfassungsdaten enthält.
4. Klicken Sie auf die **View Data Acquisition** Schaltfläche. Auf der Acquisitions Seite wird dies im Detailbereich für die Erfassung angezeigt. Im Host Alert Details Bereich wird dies in der Zeile für die Erfassung unter Acquisitions angezeigt.

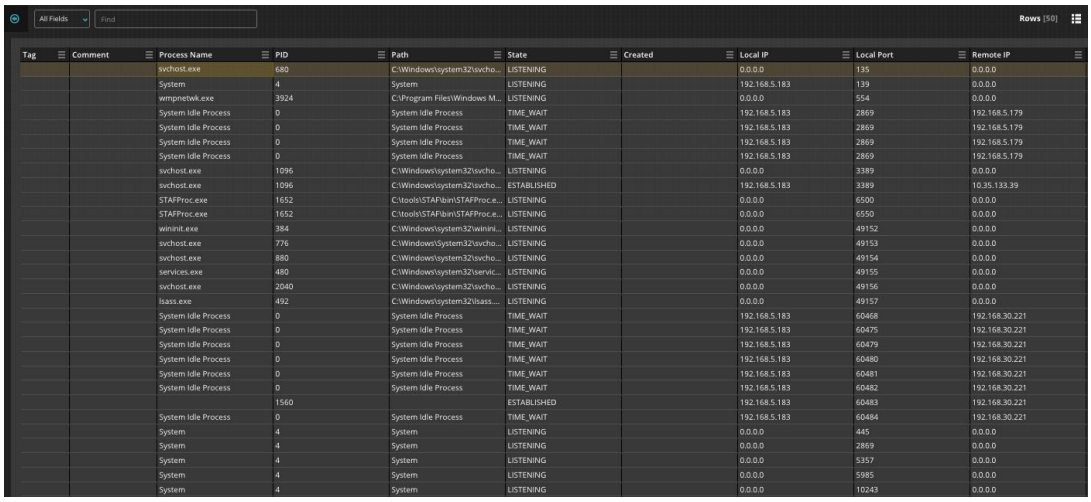
   Wenn die **Process Data Acquisition** Schaltfläche stattdessen angezeigt wird, befinden sich Erfassungsdaten noch nicht für die Verarbeitung in der Warteschlange im Audit Viewer. Siehe Die Erfassung verarbeiten auf Seite 340

Die Standardansicht, die auf der Timeline Ansicht angezeigt wird (**Timeline** ist im Data Acquisitions Abschnitt ausgewählt). Die Spaltenwerte innerhalb jeder Überschrift der Timeline Ansicht sind je nach dem Betriebssystem des Host Endpunktes, von dem die Daten gesammelt wurden, unterschiedlich.



Sie können andere Datentypen in der Akquisition zur Überprüfung auswählen. Siehe Daten für die Überprüfung auswählen auf Seite 346. In der linken Spalte des Audit Viewers werden die verschiedenen Datentypen angezeigt, die zur Überprüfung verfügbar sind. Die Daten in dieser Liste hängen vom Typ der Auditdaten ab, die für die Erfassung ausgewählt wurden. Das hervorgehobene (schwarz) Element in der Liste identifiziert den im Audit Viewer angezeigten Datentyp.

Die Hauptauswahl des Audit Viewers zeigt die Akquisitionsdaten in einem Raster an.



Eine Suchleiste wird direkt über dem Raster angezeigt.

Eine Zeile am unteren Rand der Audit Viewer Seite deutet an, wie viele Seiten des ausgewählten Datentyps in den erfassten Daten vorhanden sind.

Verwenden Sie die Pfeile rechts auf der Seite, um durch die Daten zu blättern.

Sie können auch detaillierte Informationen über jede Zeile anzeigen, die Sie im Audit Viewer Raster ausgewählt haben. Siehe Zugriff auf das Audit Viewer Detailfenster unten.

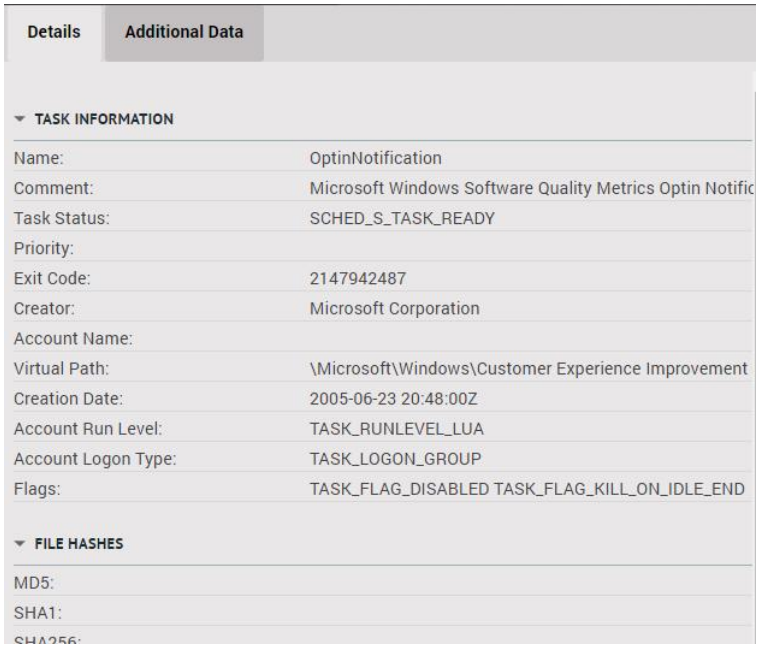
Zugriff auf das Audit Viewer Detailfenster

Das Audit Viewer Detailfenster liefert Details über eine Zeile von Auditdaten, die Sie ausgewählt haben. Die im Detailfenster angezeigten Informationen hängen von den Erfassungsdaten ab, die Sie ausgewählt haben und dem Betriebssystem des Host Endpunkts, von dem die Daten erfasst wurden. Sie können auch Tags und Kommentare zu den ausgewählten Auditdaten mit Hilfe des Detailfensters hinzufügen. Siehe Zeilen von Audit Viewer Daten markieren auf Seite 353 und Kommentare zu Zeilen von Audit Viewer Daten hinzufügen auf Seite 354.

Um auf das Audit Viewer Detailfenster zuzugreifen:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, für die Sie Detailinformationen benötigen, im Raster angezeigt werden. Siehe Daten für die Überprüfung auswählen auf Seite 346.
3. Wählen Sie eine Zeile, für die Sie detaillierte Informationen im Audit Viewer Raster anzeigen wollen.

4. Klicken Sie auf die Schaltfläche zum Öffnen des Detailfensters in der oberen rechten Ecke der Audit Viewer Seite. Die Detailinformationen für die ausgewählte Rasterlinie wird auf dem **Details** Tab angezeigt.



Das Additional Data Register wird nur angezeigt, wenn Daten in der ausgewählten Zeile mit anderen Datenerfassungstypen in den Erfassungsdaten oder in verschachtelten Datei von der gleichen Erfassungszeit korreliert werden, die möglicherweise nicht in dem Raster angezeigt werden. Die Korrelation basiert auf einem gemeinsamen Feld, z.B. einer Prozess ID.

Die Zeitstempel auf dem Detailfenster kommen aus dem Tabelleneintrag der Masterdatei für eine Datei und enthalten: Das Datum, an dem die Datei erstellt wurde, das Datum, an dem die Datei verändert wurde, das Datum, an dem die Datei abgerufen wurde und das Datum, an dem die Datei geändert wurde. Das Datum, an dem der Dateiname erstellt wurde, das Datum, an dem der Dateiname verändert wurde, das Datum, an dem der Dateiname abgerufen wurde und das Datum, an dem der Dateiname geändert wurde sind ebenfalls eingeschlossen.

Wenn ein Audit Objekte mit mehreren Zeitstempeln erstellt, werden mehrere Zeilen in der Timeline Ansicht angezeigt (eine für jeden Zeitstempel). Auf diese Weise können Sie die vollständige Zeitleiste der Ereignisse nachverfolgen, die auf dem Endpunkt stattfinden. Sie können bestimmen, welcher Zeitstempel von einer ausgewählten Zeile in der Zeitleiste repräsentiert wird, indem Sie auf die entsprechende **Field** Spalte schauen. So wird zum Beispiel in einem Dateiaudit die gleiche Datei mehrmals in der Timeline Ansicht angezeigt, einmal für jeden Zeitstempel, der der Datei zugeordnet ist.

Um das Audit Viewer Detailfenster zu schließen:

1. Klicken Sie auf die Schaltfläche zum Schließen des Detailfensters in der oberen rechten Ecke der Audit Viewer Seite.

Daten für die Überprüfung auswählen

Standardmäßig zeigt der Audit Viewer Akquisitionsdaten in der Timeline Ansicht an. Die Daten hängen von den Daten ab, die durch die Triage oder Datenerfassungsanfrage gesammelt wurden.

Um verschiedene forensische Daten zur Überprüfung im Audit Viewer auszuwählen, klicken Sie auf den Datentyp, den Sie im Data Acquisitions Abschnitt auf der linken Seite der Seite sehen wollen. Informationen zu diesen Erfassungstypen finden Sie unter Verweis auf Erfassungsdatentyp auf Seite 135.

Spalten im Audit Viewer manipulieren

Sie können Spalten im Audit Viewer neu anordnen, anzeigen und ausblenden. Sie können auch die Spaltenbreite anpassen.

Spaltenänderungen für spezifische Datentypen werden für alle Erfassungen beibehalten, die die gleiche Art von Auditdaten sammelt. Selbst wenn Sie sich aus der Endpoint Security Web-UI aus- und dann wieder einloggen, werden die von Ihnen festgelegten Spaltenänderungen beibehalten.

Spalten neu anordnen

Sie können Spalten im Audit Viewer auf verschiedene Arten neu anordnen. Sie können Spalten neu anordnen, indem Sie sie auf die Seiten ziehen und ablegen. Sie können Spalten auch mit Hilfe der Columns Liste neu anordnen.

Um Spalten im Audit Viewer mit Hilfe der Columns Liste neu anzuordnen:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, die Sie überprüfen und neu anordnen wollen, im Raster angezeigt werden. Siehe Daten für die Überprüfung auswählen oben.
3. Klicken Sie auf das Columns Symbol in der oberen rechten Ecke.

   Die Columns Liste wird angezeigt. Spalten werden in der Liste in der gleichen Reihenfolge von links nach rechts angezeigt wie im Audit Viewer Raster.
4. Klicken und ziehen Sie den Namen der Spalte in der Columns Liste an ihre neue Position.

Spalten ausblenden

Um Spalten im Audit Viewer auszublenden:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, für die Sie Spalten ausblenden wollen, im Raster sichtbar sind. Siehe Daten für die Überprüfung auswählen auf der vorherigen Seite.
3. Klicken Sie auf das Columns Symbol in der oberen rechten Ecke.

   Die Columns Liste wird angezeigt. Jede Spalte in der Liste hat ein zugehöriges Kontrollkästchen. Ein markiertes Kontrollkästchen bedeutet, dass die Spalte im Audit Viewer Raster angezeigt wird.
4. Deaktivieren Sie Kontrollkästchen neben einer Spalte, die Sie ausblenden wollen.

Spalten anzeigen

Um Spalten im Audit Viewer auszuwählen und anzuzeigen:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, für die Sie Spalten hinzufügen (anzeigen) wollen, im Raster angezeigt werden. Siehe Daten für die Überprüfung auswählen auf der vorherigen Seite.
3. Klicken Sie auf das Columns Symbol in der oberen rechten Ecke.

   Die Columns Liste wird angezeigt. Jede Spalte in der Liste hat ein zugehöriges Kontrollkästchen. Ein markiertes Kontrollkästchen bedeutet, dass die Spalte im Audit Viewer Raster angezeigt wird.
4. Wählen Sie das Kontrollkästchen neben der Spalte, die Sie anzeigen wollen.

Die Spaltenbreite anpassen

Um die Spaltenbreite im Audit Viewer anzupassen:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, für die Sie die Spaltenbreite anpassen möchten, im Raster angezeigt werden. Siehe Daten für die Überprüfung auswählen auf der vorherigen Seite.
3. Klicken Sie auf die Leiste, die zwei Spalten in der Rastertitelleiste trennt. Ziehen Sie die Spaltenleiste, um die Spaltenbreite zu ändern.

4. Wiederholen Sie den vorherigen Schritt, um alle Spalten anzupassen, die Sie für die Anpassung im Audit benötigen.

Audit Viewer Daten filtern

Sie können Audit Viewer Daten nach Spalte filtern. Sie können Filter von Spalten hinzufügen oder entfernen. Sie können auch Filter, die Sie eingestellt haben, deaktivieren, ohne sie zu entfernen.

Die Filter, die Sie im Audit Viewer für eine `.mans` Datei festgelegt haben, werden für diese Datei beibehalten. Allerdings werden die für unterschiedliche `.mans` Dateien festgelegten Filter im Audit Viewer nicht geteilt, selbst wenn die `.mans` Dateien die gleiche Art von Auditdaten enthalten.

Filter einstellen

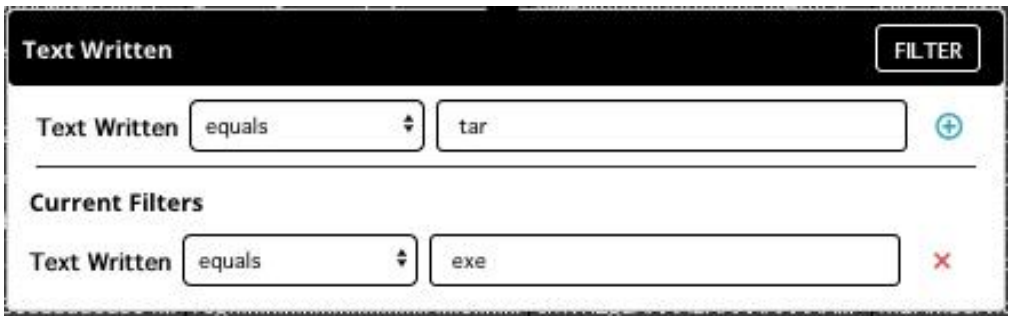
Um einen Spaltenfilter im Audit Viewer einzustellen und anzuwenden:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, die Sie filtern wollen, im Raster sichtbar sind. Siehe Daten für die Überprüfung auswählen auf Seite 346.
3. Klicken Sie auf das Filter Symbol ( ) in der Spaltenüberschrift, Der Filterdialog für die Spalte wird angezeigt.

   Filteroptionen hängen von dem Datentyp in der Spalte ab. Das nachfolgende Beispiel zeigt die Application Version Spalte.

4. Wählen Sie gegebenenfalls einen Operator für den Filter im Operator Dropdown-Menü (als `equals` in dem Beispiel gezeigt). Die folgenden allgemeinen Filteroperatoren können angezeigt werden.

5. Geben Sie gegebenenfalls einen Wert in dem Feld rechts neben dem Filteroperator ein. Klicken Sie dann auf das große Plus Zeichen (+) rechts neben dem Feld. Der Filter ist im Filter Dialogfeld unter **Current Filters** aufgeführt.



   Wiederholen Sie diesen Schritt, um zusätzliche Filter für die Spalte hinzuzufügen. Wenn mehrere Filter für eine Spalte festgelegt sind, müssen alle Filter erfüllt sein, damit eine Zeile in den gefilterten Daten angezeigt wird. Mehrere Filtern werden als verbindende Bedingungen behandelt.

6. Um den Filter anzuwenden, klicken Sie auf die blaue **Filter** Schaltfläche.

   Der Audit Viewer Raster wird neu geladen, um nur die Zeilen in dem Raster anzuzeigen, die den Filterkriterien entsprechen. Die Zeilenanzahl unten auf der Seite ändert sich entsprechend der aktuellen Anzahl der im Raster angezeigten Zeilen. Ein Trichtersymbol (▼) im Spaltentitel deutet an, dass die Spalte gefiltert wurde.

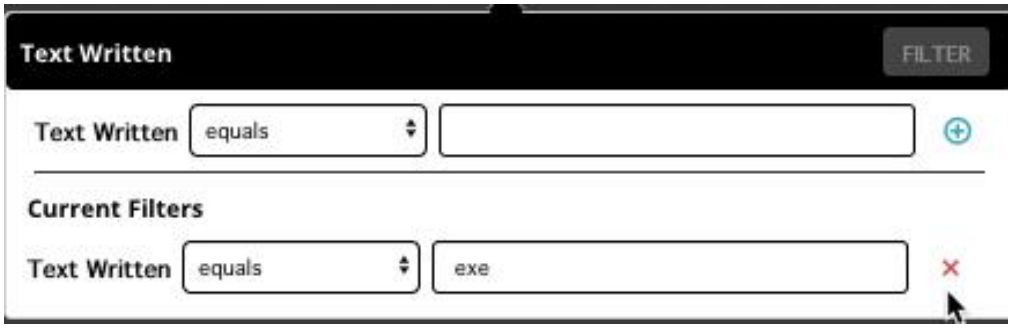
7. Um das Filter Dialogfeld zu schließen, klicken Sie erneut auf das Filter Symbol (▢).

Filter deaktivieren

Um einen Spaltenfilter zu deaktivieren und die Änderung im Audit Viewer anzuwenden:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, die Sie filtern, im Raster sichtbar sind. Siehe Daten für die Überprüfung auswählen auf Seite 346.
3. Klicken Sie auf das Filter Symbol in der Spaltenüberschrift. Das Filter Dialogfeld für die Spalte wird angezeigt.

4. Entfernen Sie das Häkchen links neben dem Filter, den Sie im Current Filters Bereich deaktivieren wollen.



5. Um den aktualisierten Filter anzuwenden, klicken Sie auf die **Filter** Schaltfläche.

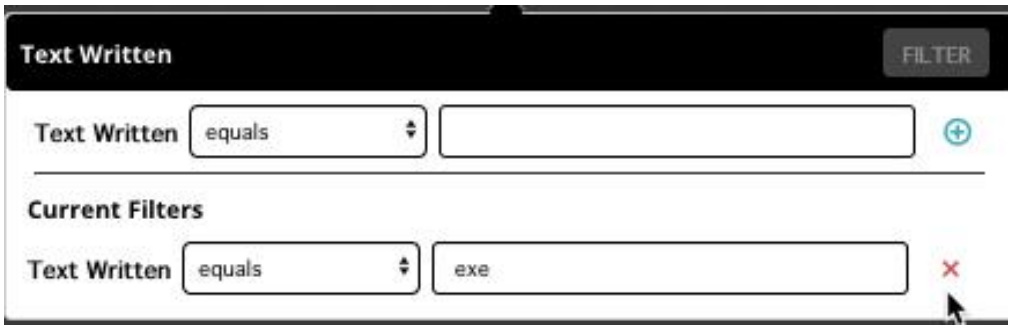
   Der Audit Viewer Raster wird neu geladen, um nur die Zeilen in dem Raster anzuzeigen, die den Filterkriterien entsprechen. Die Zeilenanzahl unten auf der Seite ändert sich entsprechend der aktuellen Anzahl der im Raster angezeigten Zeilen.

6. Um das Filter Dialogfeld zu schließen, klicken Sie erneut auf das Filter Symbol.

Filter löschen

Um einen Spaltenfilter zu löschen und die Änderung im Audit Viewer anzuwenden:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, die Sie filtern, im Raster sichtbar sind. Siehe Daten für die Überprüfung auswählen auf Seite 346.
3. Klicken Sie auf das Filter Symbol ( ) in der Spaltenüberschrift, Das Filter Dialogfeld für die Spalte wird angezeigt.
4. Klicken Sie auf das Filter löschen Symbol rechts neben dem Filter, den Sie löschen wollen.



   Um alle Filter für eine Spalte vollständig zu entfernen, klicken Sie auf **Delete all** in der oberen rechten Ecke des Current Filters Abschnitts.

5. Um den aktualisierten Filter anzuwenden, klicken Sie auf die **Filter** Schaltfläche.

   Das Audit Viewer Raster wird neu geladen, um nur die Zeilen in dem Raster anzuzeigen, die allen verbleibenden Filterkriterien entsprechen.

   Wenn alle Filter entfernt wurden, wird das Audit Viewer Raster neu geladen, um alle Daten für den ausgewählten Datentyp in der Erfassung anzuzeigen. Das kleine Trichtersymbol verschwindet von der Spaltenüberschrift was bedeutet, dass die Spalte nicht länger gefiltert wird.

   Die Zeilenanzahl unten auf der Seite ändert sich entsprechend der aktuellen Anzahl der im Raster angezeigten Zeilen.
6. Um das Filter Dialogfeld zu schließen, klicken Sie erneut auf das Filter Symbol.

Audit Viewer Daten sortieren

Sie können die Daten im Audit Viewer Raster nach Spalte sortieren. Klicken Sie auf die Spaltenüberschrift, um die Daten zu sortieren. Der Pfeil neben dem Spaltenname deutet an, ob die Daten in auf- oder absteigender Reihenfolge sortiert sind. Wenn kein Pfeil angezeigt wird, werden die Daten nicht länger sortiert.

Durch wiederholtes Klicken auf den Spaltennamen wird die Sortierung der Daten in der folgenden Reihenfolge geändert.

1. Der erste Klick sortiert die Daten in aufsteigender Reihenfolge.
2. Der zweite Klick sortiert die Daten in absteigender Reihenfolge.
3. Der dritte Klick entfernt die Sortiert und gibt die Daten an ihre Standardorganisation zurück.

Ein vierter Klick auf die Spalte startet die Sequenz erneut und sortiert die Daten in aufsteigender Reihenfolge.

Obwohl die meisten Spalten sortierbar sind, sind es die Detail Spalten in der Timeline Ansicht nicht, weil sie heterogene Daten enthalten.

Die für spezifische Datentypen ausgewählte Sortierung wird für alle Akquisitionen beibehalten, die die gleiche Art der Auditdaten sammeln. Selbst wenn Sie sich aus der Endpoint Security Web-UI ab- und wieder anmelden, werden die Sortieränderungen, die Sie festgelegt haben, beibehalten.

Nach Audit Viewer Daten suchen

Sie können nach allen Daten suchen, wenn diese Daten im Audit Viewer Raster angezeigt werden. Die Daten die Im Raster angezeigt werden, hängen von dem Datentyp ab, den Sie

in der Data Acquisition Spalte ausgewählt haben.

Um nach Daten im Raster zu suchen:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass der Datentyp, nach dem Sie suchen wollen, im Raster sichtbar ist. Siehe Daten für die Überprüfung auswählen auf Seite 346.
3. Finden Sie die Suchleiste direkt über dem Raster.

4. Optional können Sie die Spalte der Daten in dem Raster auswählen, die im **All Fields** Menü durchsucht werden sollen. Wenn Sie alle Daten im Raster durchsuchen wollen, überspringen Sie diesen Schritt.
5. Bestimmen Sie die Daten für die Suche in dem Feld und drücken Sie **Eingabe**.

   Die Rasterdaten werden durchsucht und alle Objekte, die mit der Suchanfrage übereinstimmen, werden hervorgehoben. Wenn mehr als 1000 Übereinstimmungen gefunden werden, zeigt eine Nachricht an, dass nur die ersten 1000 Übereinstimmungen angezeigt werden.

   Sie können durch die Übereinstimmungen mit Hilfe der Schaltflächen rechts neben der Suchleiste blättern.

Um das Suchfeld zu löschen, klicken Sie auf die Schaltfläche in dem Feld.

Audit Viewer Daten kopieren

Sie können die Daten in jeder individuellen Zelle im Audit Viewer Raster oder in mehreren Zellen anzeigen, die Sie ausgewählt haben. Sie können die Daten, die Sie kopiert haben, nicht in Erfassungen oder andere Daten einfügen, die in der Endpoint Security Web-UI angezeigt werden. Die Daten können in eine E-Mail oder einen externen Editor eingefügt werden.

Um Daten von einer individuellen Zelle im Raster zu kopieren:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Finden Sie die Daten, die Sie in das Raster kopieren wollen.
3. Klicken Sie auf die Zelle mit den Daten, die Sie kopieren wollen.
4. Drücken Sie **Ctrl+C** (Windows) oder **CMD+C** (macOS), um die Daten zu kopieren.

Um Daten in mehreren Zellen auszuwählen und zu kopieren:

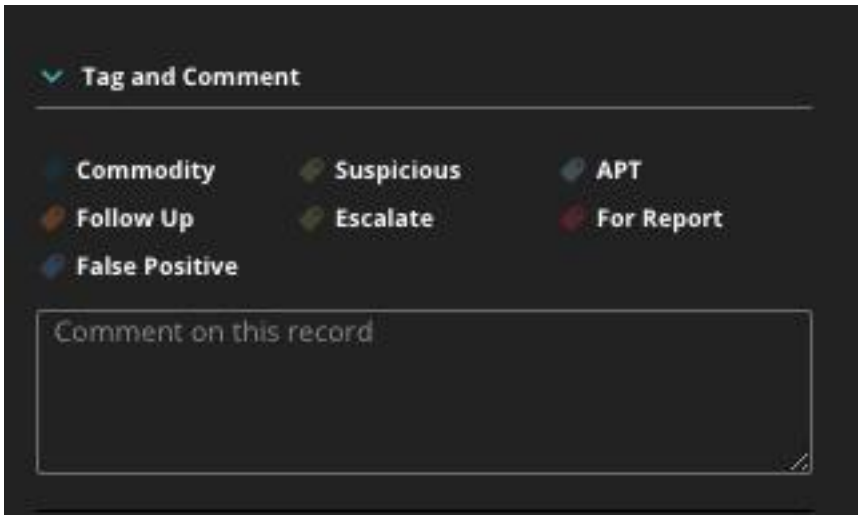
1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Finden Sie die Daten, die Sie in das Raster kopieren wollen.
3. Halten Sie die linke Maustaste gedrückt und ziehen Sie die Maus über die Zellen der Daten, die Sie kopieren möchten.
4. Drücken Sie **Ctrl+C** (Windows) oder **CMD+C** (macOS), um die Daten zu kopieren.

Zeilen von Audit Viewer Daten markieren

Sie können eine Datenzeile im Audit Viewer Raster markieren.

Um eine Zeile von Audit Viewer Daten zu markieren:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, für die Sie ein Tag hinzufügen wollen, im Raster sichtbar sind. Siehe Daten für die Überprüfung auswählen auf Seite 346.
3. Wählen Sie eine Zeile im Audit Viewer Raster.
4. Klicken Sie auf die Schaltfläche zum Öffnen des Detailfensters ( ) in der oberen rechten Ecke der Audit Viewer Seite.
5. Finden Sie den Tag and Comment Abschnitt unten im Details Register im Detailfenster.



6. Klicken Sie auf das Tag, das Sie für die Zeile wollen. Pro Zeile kann nur ein Tag ausgewählt werden. Die folgenden Tags stehen zur Verfügung:

Tag Name	Verwendung
APT	Verwenden Sie dieses Tag, um eine Zeile zu markieren, die auf ein Advanced Persistent Threat (ATP) hinweist.
Commodity	Verwenden Sie dieses Tag, um eine Zeile als Commodity (Standard) Malware zu markieren. Bei Commodity Malware handelt es sich typischerweise um normale Malware, keine Exploits oder APTs.
Escalate	Verwenden Sie dieses Tag, um eine Zeile als Eskalation zu markieren.
False Positive	Verwenden Sie dieses Tag, um eine Zeile als ein Falsch/Positiv zu markieren.
Follow Up	Verwenden Sie dieses Tag, um eine Zeile als etwas zu markieren, das Sie weiterverfolgen müssen.
For Report	Verwenden Sie dieses Tag, um eine Zeile für einen Bericht zu markieren.
Suspicious	Verwenden Sie dieses Tag, um eine Zeile als verdächtig zu markieren.

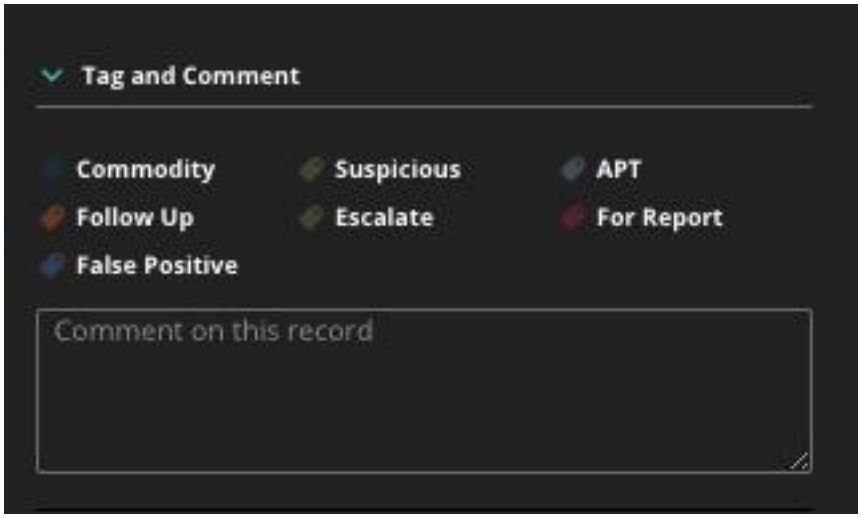
Kommentare zu Zeilen von Audit Viewer Daten hinzufügen

Sie können Kommentare zur einer Zeile von Audit Viewer Daten hinzufügen.

Um einen Kommentar zu einer Zeile von Audit Viewer Daten hinzuzufügen:

1. Überprüfen Sie eine Erfassung im Audit Viewer. Siehe Die Erfassungsdaten anzeigen auf Seite 342.
2. Stellen Sie sicher, dass die Daten, für die Sie Kommentare hinzufügen wollen, im Raster sichtbar sind. Siehe Daten für die Überprüfung auswählen auf Seite 346.
3. Wählen Sie eine Zeile im Audit Viewer Raster.

4. Klicken Sie auf die Schaltfläche zum Öffnen des Detailfensters ( ) in der oberen rechten Ecke der Audit Viewer Seite.
5. Finden Sie den Tag and Comment Abschnitt unten im Details Register im Detailfenster.



6. Geben Sie Ihren Kommentar für die ausgewählte Zeile im Kommentarfeld ein.

Forensische Daten in Redline überprüfen

Sie können Triage Sammlung und Datenerfassungs-`.mans` Dateien in Redline untersuchen.

Wenn Sie Daten in Redline anzeigen, untersuchen Sie einen Snapshot eines Host Endpunktsystems zum Zeitpunkt eines Warnungs-Ereignisses auf Hinweise dazu, wie ein Angreifer möglicherweise operiert hat. Wenn Sie wissen, dass ein Host Endpunkt eine Datei heruntergeladen hat, können Sie sich verdächtige Dateipfade ansehen und sehen, was zu dem Zeitpunkt geschah, zu dem der Host die Datei heruntergeladen hat. Es gibt viele Untersuchungspfade, die Sie nach zusätzlichen Informationen durchsuchen können.

Beispielsweise können Sie das Timeline Tool von Redline verwenden, um nach netzwerkbezogenen Aktivitäten (nach IP oder DNS Namen) oder nach Host Endpunktaktivitäten (z. B. einem bösartigen Dateinamen) anhand eines Dateinamens, einer Prozess ID oder eines Zeitstempels zu suchen. Mit der Zeitleiste können Sie herausfinden, welche Prozesse bestimmte Aktivitäten verursacht haben. Mit TimeWrinkles und Timeline Filtering können Sie sehen, was ein Prozess tatsächlich gemacht hat, Dateien, die er erstellt hat, Netzwerkverbindungen, die er generiert hat, oder Registrierungsschlüssel, die er geändert hat. Dieser Prozess hilft Ihnen, den Umfang und die Schwere der Kompromittierung zu bestimmen.

Voraussetzungen

- Installieren Sie Redline auf dem Computer, den Sie zur Untersuchung oder Analyse verwenden werden. Anweisungen werden in Redline installieren unten bereitgestellt.
- Laden Sie die Triage Sammlung oder Datenerfassungs-`.mans` Datei, die Sie überprüfen wollen, auf den gleichen Computer herunter. Weitere Informationen finden Sie unter Forensische Daten herunterladen auf Seite 329.

Redline installieren

Sie können Redline Software vonhttps://www.fireye.com/services/freeware.html herunterladen. Sie können die Redline Benutzerdokumentation auf derselben Website herunterladen.

Die Daten in Redline untersuchen

Um Daten in Redline zu untersuchen

1. Doppelklicken Sie die `.mans` Datei.

   Redline wird geöffnet und importiert die Triage Sammlung.

2. Auf der Redline **Start Your Investigation** Seite bewegen Sie den Mauszeiger über **I am Reviewing a Triage Collection from HX** bis der Block rot wird. Klicken Sie dann auf den roten Block oder den **Investigate** Link.

   Wenn Sie zuvor die `.mans` Datei in Redline geöffnet und Ihre Analyse gespeichert haben, können Sie die gespeicherte Analyse auf folgende Weise öffnen:

   - Auf der Redline **Home** Seite wählen Sie **Open a Saved Analysis**.
   - Wählen Sie im Redline Menü die Triage Sammlung aus.

   Die Timeline Ansicht wird geöffnet. Verwenden Sie die Filterfunktion, um sich auf Ihre Ermittlungsarbeit zu konzentrieren.

3. Untersuchen Sie Hinweise in Ihren Triage- und Datenerfassungsdaten. Folgen Sie Informationssträngen für jeden Hinweis, bis Sie eindeutige Beweise für verdächtige Aktivitäten finden.

   Es gibt keinen festgelegten Pfad zum Abschließen einer `.mans` Dateiuntersuchung. Jede Untersuchung hängt davon ab, was Sie finden, wenn Sie jedem Hinweis nachgehen.

4. Folgen Sie in der Endpoint Security Appliance nach.

Je nach Ihren Untersuchungsergebnissen können Sie beispielsweise Dateien erfassen oder zusätzliche Datenerfassungen für weitere Analysen anfordern. Siehe Forensische Daten erfassen auf Seite 315. Sie können auch einen Hostendpunkt eindämmen, von dem Sie glauben, dass er kompromittiert wurde. Siehe Überblick über Eindämmung auf Seite 421.

Agent Diagnostics überprüfen

Um eine Agent Diagnostics Erfassung zu überprüfen:

1. Öffnen Sie die Akquisition `.zip` Datei. Zur Extraktion der Dateien in dieser `.zip` Datei ist kein Passwort erforderlich.
2. Öffnen Sie die Dateien innerhalb der `.zip` Datei mit Hilfe eines Text- oder XML-Editors.

Die Agent Diagnostics Daten sind für Ihren FireEye Customer Support-Mitarbeiter sehr hilfreich.

KAPITEL 26: Forensische Daten löschen

Für einen Host Endpunkt gesammelte Triage und Datenerfassungen werden automatisch gelöscht, wenn der Host gelöscht wird. (Host Endpunkte können automatisch gelöscht erden, wenn die Einstellungen für Host Alterung auf diese Art festgelegt sind. Siehe Host Alterungsintervalle festlegen auf Seite 177. Andernfalls werden Akquisitionen so lange erhalten, wie ihre zugehörigen Host Endpunkte aktiv bleiben.

Sie können Triage und Akquisitionsdaten manuell löschen, um Akquisitionsspeicher frei zu machen.

Um forensische Daten manuell von der Acquisitions Seite zu löschen:

1. Wählen Sie **Acquisitions** in der Endpoint Security Web-UI.
2. Im Acquisitions Raster wählen Sie das Kontrollkästchen, das der Zeile in dem Raster entspricht, die Sie löschen wollen.

   Details über die Zeile werden im Acquisition Detail Abschnitt angezeigt. Sie können diese Details im Acquisition Detail Bereich erweitern, um einige der Akquisitionsdaten zu überprüfen.

   Eine einzelne Zeile in dem Raster könnte sowohl Triage Summary und Daten Akquisition Ansichten enthalten. Wenn Sie eine Zeile im Acquisitions Raster löschen, löschen Sie beide Ansichten.

3. Wählen Sie **Delete acquisition** vom **Actions** Menü, um die Zeile zu löschen.

KAPITEL 27: Cache- und Wiederverarbeitungserfassungen löschen

Triage-Datenerfassungen könnten fehlschlagen, wenn sie länger dauern als die von Ihnen konfigurierte Zeit. Um dieses Problem zu lösen, erhöhen Sie das Zeitlimit, löschen Sie die zwischengespeicherten Dateien für die Erfassungen, die aufgrund des Zeitlimits fehlgeschlagen sind, und verarbeiten Sie die Erfassungen erneut. Datenerfassungen können wegen der benötigten Festplattenkapazität für Speicher oder Sicherung auch eine Herausforderung darstellen.

Durch das Löschen Ihrer zwischengespeicherten Dateien wird Speicherplatz auf Ihrem lokalen Laufwerk freigesetzt. Die Delete cache Aktion entfernt alle Triage Viewer Artefakte und löscht die nicht-komprimierten .sqlite Triage-Dateien für die ausgewählten Erfassungen vom Triage .zip Verzeichnis, einschließlich der folgenden Dateitypen:

- Triages (nur manuell)
- Quick File Listing
- Full Disk
- Full Memory
- Driver Memory
- Process Memory
- Comprehensive Investigative Details
- Standard Investigative Details
- Power Shell
- Command Shell History

Die folgenden Verfahren erläutern, wie Sie Erfassungen, die aufgrund einer Zeitüberschreitung fehlgeschlagen sind, erneut verarbeiten können, wie Sie den Datenbedarf erfolgreich verarbeiteter Erfassungen durch Löschen des Caches und erneutes Verarbeiten der Erfassungen reduzieren können und wie Sie Erfassungen nach Bedarf nach einem Endpoint Security Upgrade erneut verarbeiten können.

Erfassungen verwalten, die aufgrund der Überschreitung von Zeitlimits fehlschlagen

Wenn Ihre Erfassungen aufgrund der Überschreitung von Zeitlimits fehlschlagen, wird die folgende Nachricht im Details Bereich auf der Acquisitions Seite angezeigt: Acquisition not viewable. Server timeout while processing data. Delete cache and re-process after increasing server timeout. Sie können die folgenden Schritte ausführen, um sicherzustellen, dass Ihre Triage-Erfassungen erfolgreich verarbeitet werden:

1. Erhöhen Sie das Zeitlimit für Erfassungsextraktionen.

   hostname (config) # `hx server acquisition extraction timeout <seconds>`

2. Löschen Sie die Triage-Daten für die fehlgeschlagene Erfassung von Ihrem Zwischenspeicher.

   a. Wählen Sie die Erfassungen, die aufgrund der Überschreitung des Zeitlimits fehlgeschlagen sind, auf der Acquisitions Seite. Sie können mehr als eine Erfassung auswählen.

   b. Im Actions Menü wählen Sie **Delete cache**.

   c. Klicken Sie auf **Go**.

   d. Klicken Sie im Konfirmations-Dialogfeld auf **Delete**.

      Am Anfang der Seite wird ein Banner angezeigt, dass angibt, dass der Zwischenspeicher für die ausgewählte Anzahl von Erfassungen zum Löschen markiert wurde und ein Deleting cache processing Symbol mit einer View Data Acquisition Schaltfläche wird im Acquisition Details Abschnitt angezeigt.

3. Verarbeiten Sie Ihre Erfassungen erneut. Wählen Sie die Erfassungen und klicken Sie auf **Process Data Acquisitions** im Details Bereich der Acquisitions Seite.

   Der Status der Erfassung wird von Wating auf Process to Acquired geändert, wenn die Neuverarbeitung abgeschlossen ist.

Erfolgreich verarbeitete Erfassungen verwalten

Nachdem Ihre Triage-Datenerfassungen erfolgreich verarbeitet wurden (Acquired Status), können Sie die nicht-komprimierten Dateien von Ihrem Zwischenspeicher löschen, um den zum Speichern oder Sichern der Erfassungen erforderlichen Speicherraum zu minimieren.

Verwenden Sie die folgenden Schritte, um die zwischengespeicherten Triage-Daten zu löschen:

1. Wählen Sie die Erfassung auf der Acquisitions Seite. Sie können mehr als eine Erfassung auswählen.
2. Im Action Menü wählen Sie **Delete cache**.

3. Klicken Sie auf **Go**.
4. Klicken Sie im Konfirmations-Dialogfeld auf **Delete**.

   Am Anfang der Seite wird ein Banner angezeigt, dass angibt, dass der Zwischenspeicher für die ausgewählte Anzahl von Erfassungen zum Löschen markiert wurde und ein Deleting cache processing Symbol mit einer View Data Acquisition Schaltfläche wird im Acquisition Details Abschnitt angezeigt.

   Die Process Data Acquisitions Schaltfläche wird im Details Bereich der Acquisitions Seite nach Abschluss des Löschvorgangs angezeigt.
5. Verarbeiten Sie Ihre Erfassungen erneut. Wählen Sie die Erfassungen aus, die Sie erneut verarbeiten wollen und klicken Sie auf **Process Data Acquisitions**.

Automatische Triagen nach einem Upgrade erneut verarbeiten

Wenn eine neue Version von Endpoint Security Änderungen oder Erweiterungen am Audit Viewer oder am automatischen Triage-Prozess enthält, müssen Sie nach dem Upgrade Ihrer Endpoint Security Instanz möglicherweise Ihre bestehenden automatischen Triage-Prozesse neu verarbeiten.

Führen Sie die folgenden Schritte aus, um automatische Triagen erneut zu verarbeiten:

1. Wählen Sie die Erfassungen, die Sie erneut verarbeiten wollen, auf der Acquisitions Seite. Sie können mehr als eine Erfassung auswählen.
2. Im Actions Menü wählen Sie die **Reprocess acquisition** Option .
3. Klicken Sie auf **Go**.

Wenn die erneute Verarbeitung abgeschlossen ist, ändert sich der Status für die ausgewählten Erfassungen auf Acquired und die View Data Acquisition Schaltfläche wird im Aquisition Details Bereich angezeigt.

TEIL V: Alarme, Dateien in Quarantäne und Falsch Postive verwalten

KAPITEL 28: Warnungen, Dateien in Quarantäne und Falsch Postive verwalten

Warnungen sind Übereinstimmungen zwischen einer oder mehreren Indikatorregelbedingungen oder Quellwarnungen und Aktivitäten, die Agents auf Ihren Host Endpunkten finden. Analysten und Investigatoren überprüfen Warnungen, um festzustellen, ob die Übereinstimmungen harmlose oder normale Aktivitäten (Falsch Positive) oder mögliche Gefährdungen repräsentieren. Nicht jede Warnung beinhaltet bösartige Aktivitäten.

Wenn Ihre Überprüfung andeutet, dass ein Endpunkt kompromittiert wurde, können Sie den Endpunkt eindämmen, so dass die Bedrohung sich nicht ausbreiten kann. Siehe Überblick über Eindämmung auf Seite 421.

Wenn eine Warnung eine harmlose Aktivität meldet, die keine weitere Überprüfung erfordert, können Sie die Warnung löschen und zukünftige Warnungen unterdrücken, indem Sie zugehörige Indikatorregeln löschen und falsch positive Bedingungen minimieren.

Dieser Abschnitt behandelt die folgenden Themen:

Warnungen anzeigen und verwalten

Verwenden Sie die Endpoint Security Web-UI, um Warnungen von der Alerts Seite oder dem Hosts Tab anzuzeigen oder zu verwalten.

- Die Alerts Seite bietet Ihnen eine ausführliche Ansicht *aller* Warnungen. Auf diesem Tab können Sie Warnungen nach Kriterien wie Hostname oder IP-Adresse sortieren, filtern und suchen. Weitere Informationen finden Sie unter Warnungen auf der Alerts Seite anzeigen unten.
- Der Hosts Tab ermöglicht Ihnen, Warnungen für einen bestimmten Host-Endpunkt anzuzeigen. Weitere Informationen finden Sie unter Warnungs- und Ereignisinformationen je nach Host anzeigen auf Seite 385.

  Erweitern Sie die Informationen zum Host-Endpunkt, um zu sehen, welche Warnungen für den Host aufgetreten sind. Wenn eine Warnung von einem anderen FireEye Produkt oder Service ausgeht (*eine Quellwarnung*), bietet diese Seite auch Informationen und Links, um Trends zu erkennen und umfassendere Informationen zu erhalten. Weitere Informationen über Quellenwarnungen finden Sie auf der Rules Seite. Siehe FireEye Quellenwarnungen auf Seite 415.

Voraussetzungen

- Administrator, Analyst, Senior Analyst oder Investigator Zugriff.

Warnungen auf der Alerts Seite anzeigen

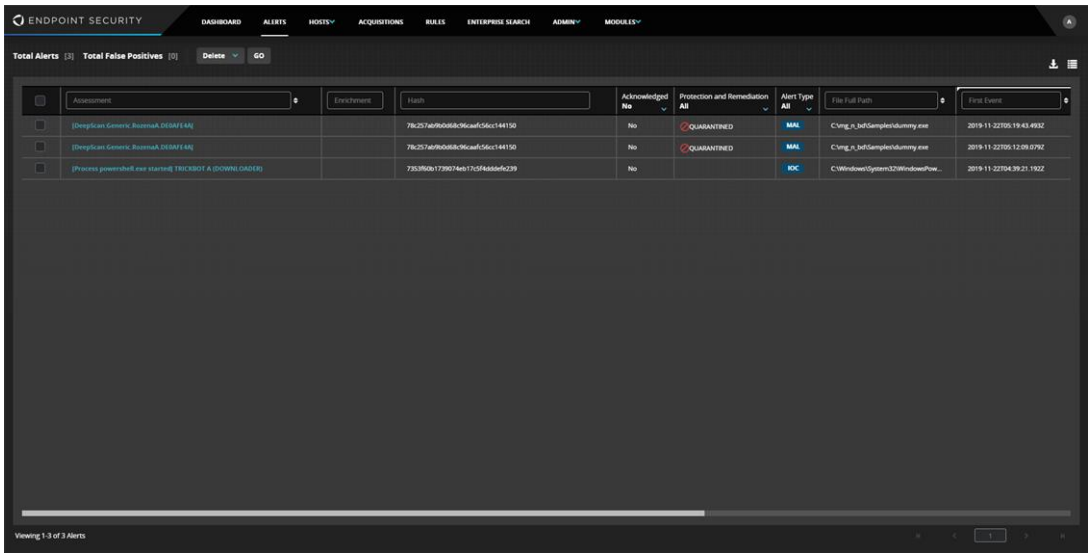
Sie können alle Warnungen von der Alerts Seite anzeigen. Dieser Abschnitt behandelt die folgenden Informationen über die Verwendung und das Verständnis der Alerts Seite.

- Alle Warnungen anzeigen unten
- Alerts Tabelle auf der nächsten Seite

HINWEIS: Zeitstempel in der Web-UI werden in UTC Zeit präsentiert.

Alle Warnungen anzeigen

Um eine Zusammenfassung aller Warnungen für Ihre Endpunkt Umgebung an einer Stelle anzuzeigen, wählen Sie **Alerts** auf dem Menü am Anfang der Seite.



Am Anfang der Alerts Seite finden Sie eine Zusammenfassung der verfügbaren Warnungen, einschließlich der Anzahl der Warnungen, Anzahl der Falsch Positiven und eine Option, die ausgewählten Warnungen zu löschen oder zu bestätigen.

- **Total Alerts**—Zählt alle Warnungen, einschließlich der als False Positive markierten.
- **Total False Positives**—Zählt alle als False Positive markierten Warnungen.
- **Delete**—Löscht oder bestätigt ausgewählte Warnungen.

Alerts Tabelle

Die Alerts Tabelle zeigt eine Zeile für jede Warnung oder Warnungsgruppe an. Wenn mehrere Warnungen des gleichen Typs für einen Host gemeldet werden, werden Sie in der gleichen Zeile der Alerts Tabelle gruppiert. Weitere Informationen finden Sie unter Warnungsgruppen verstehen auf Seite 386.

In der folgenden Tabelle werden die einzelnen Spalten in der Alerts Tabelle aufgelistet und beschrieben.

Spalte	Beschreibung	Standardspalte
Acknowledged	Zeigt den Bestätigungsstatus für jeden Alarm an. • All (Standard) • Ja (bestätigte Alarme) • Nein (unbestätigte Alarme)	J

Spalte	Beschreibung	Standardspalte
Acknowledged By	Zeigt den Usernamen von Administrator, Analyst, Senior Analyst oder Investigator an, der die Warnung bestätigt.	N
Acknowledged Date/Time	Zeigt Datum und Uhrzeit der Bestätigung der Warnung an.	N

Alert Type	Zeigt den Warnungstyp an. Sie können Warnungen für einen bestimmten Typ filtern, indem Sie den Typ von der Dropdown-Liste wählen. Der derzeit ausgewählte Typ wird in der Spaltenüberschrift angezeigt.
	• ALL (Standard)
	• IOC—Indicators of Compromise
	  • PRS—Presence
	  • EXC—Execution
	• MAL—Malware
	• XPLT—Exploit
		J

Spalte	Beschreibung	Standardspalte
Assessment	Zeigt den Beurteilungsnamen für die Warnung als Link zu weiteren Details auf der Host Alert Details Seite an. Weitere Informationen finden Sie unter Scan-Zusammenfassung auf Seite 63. Sie können Warnungen nach Bewertung auf folgende Weise filtern: • Klicken Sie innerhalb der Spaltenüberschrift, um Warnungen nach einem vollständigen oder Teil des Bewertungsnamen zu filtern. • Klicken Sie auf die Spaltenüberschrift, um Warnungen nach Bewertungsnamen in auf- oder absteigender Reihenfolge zu sortieren.	J
Kommentare	Zeigt alle vom Benutzer eingegebenen Kommentare an.	N
Disposition	Zeigt einen Teilsatz von Warnungen an. • All (Standard) • False Positive • Not False Positive	J
Enrichment	Zeigt Metadaten an, die die Warnung beschreiben.	J
Ereignisse	Zeigt die Anzahl der Ereignisse in der Warnung an. Klicken Sie auf die Spaltenüberschrift, um Warnungen nach Ereigniszählung in auf- oder absteigender Reihenfolge zu sortieren.	J

Spalte	Beschreibung	Standardspalte
File Full Path	Zeigt den Dateipfad des neuesten Ereignisses für die Warnung an. Dateipfade sind immer für MAL-Warnungen und EXD-Warnungen, aber nicht immer für IOC-Warnungen verfügbar.	J
First Event	Der Zeitstempel der ältesten Warnungsgruppe. Sie können eine relative Zeit auswählen (**Today**, **Yesterday**, **Last 7 Days**, **Last 30 Days**, **This Month** oder **Last Month**). Wählen Sie **Custom**, um einen Kalender zu öffnen und einen bestimmten Bereich einzugeben. Klicken Sie auf die Spaltenüberschrift, um Warnungen nach First Event (erstes Ereignis) Zeitstempeln in auf- oder absteigender Reihenfolge zu sortieren. Sie können First Event mit Last Event verwenden, um Ihre Ergebnisse einzugrenzen.	J
Hash	Zeigt das mit der Warnung verbundene Hash an. • Klicken Sie innerhalb der Spaltenüberschrift, um Warnungen nach einem vollständigen oder Teil des Hash zu filtern. **HINWEIS**—Nicht alle Warnungen haben ein zugehöriges Hash.	J

Spalte	Beschreibung	Standardspalte
Host	Zeigt den Hostnamen an, wobei es sich um einen Link auf die Detailseite des Host handelt. • Klicken Sie innerhalb der Spaltenüberschrift, um Warnungen nach einem vollständigen oder Teil des Hostnamen zu filtern. • Klicken Sie auf die Spaltenüberschrift, um Warnungen nach Hostnamen in auf- oder absteigender Reihenfolge zu sortieren.	J
Host IP	Zeigt die mit der Warnung verbundene Quell- oder Ziel-IP-Adresse an. • Klicken Sie innerhalb der Spaltenüberschrift, um Warnungen nach einem vollständigen oder Teil der IP-Adresse zu filtern. • Klicken Sie auf die Spaltenüberschrift, um Warnungen nach IP-Adressen in auf- oder absteigender Reihenfolge zu sortieren.	J
Last Event	Der Zeitstempel der neuesten Warnung in der Warngruppe. Klicken Sie auf die Spaltenüberschrift, um Warnungen nach Last Event Zeitstempeln in auf- oder absteigender Reihenfolge zu sortieren.	J

Spalte	Beschreibung	Standardspalte
Optionen	Um eine Warnung zu bestätigen, wählen Sie Acknowledge. Weitere Informationen finden Sie unter Bestätigte Warnungen auf Seite 387.	J
Protection and Remediation	Zeigt die Aktion an, die auf die Warnung ausgeführt wurde. Sie können Warnungen nach einen bestimmten Status filtern, indem Sie den Status von der Dropdown-Liste wählen. Der derzeit ausgewählte Status wird in der Spaltenüberschrift angezeigt. • ALL (Standard) • BLOCK • PARTIAL BLOCK • QUARANTINED • CLEANED	J
Selected	Ermöglicht Ihnen, alle auszuwählen, alle zu löschen oder spezifische Warnungszeilen zum Löschen oder Bestätigen zu wählen. Sie können die Spalte verwenden, um Massenlöschung oder Bestätigung aller Warnungen in der Alerts Tabelle vorzunehmen.	J

Die Alerts Tabelle verwalten

Sie können die Alerts Tabellenansicht verwalten und anpassen, indem Sie Spalten auswählen und neu anordnen, die Spaltenbreite ändern und alle Filter löschen und wiederherstellen.

Dieser Abschnitt behandelt die folgenden Themen:

- Spalten in der Alerts Tabelle auswählen auf der nächsten Seite
- Spalten in der Alerts Tabelle neu anordnen, ihre Größe ändern und wiederherstellen auf der nächsten Seite
- Filter in der Alerts Tabelle verwenden auf Seite 379

- Filter in der Alerts Tabelle löschen auf Seite 382
- Daten von der Alerts Tabelle exportieren auf Seite 383

Spalten in der Alerts Tabelle auswählen

Sie können die Spaltenauswahl auf der Alerts Seite für die Anpassung der Alerts Table Ansicht verwenden.

Um die Alerts Tabelle anzupassen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Klicken Sie auf das Spaltenauswahl ( ) Symbol.
3. Um eine bestimmte Spalte in der Tabelle anzuzeigen, wählen Sie das Kontrollkästchen neben dem Spaltennamen. Wenn Sie eine Spalte auswählen, wird die Alerts Tabelle automatisch aktualisiert und zeigt die neue Spalte an.

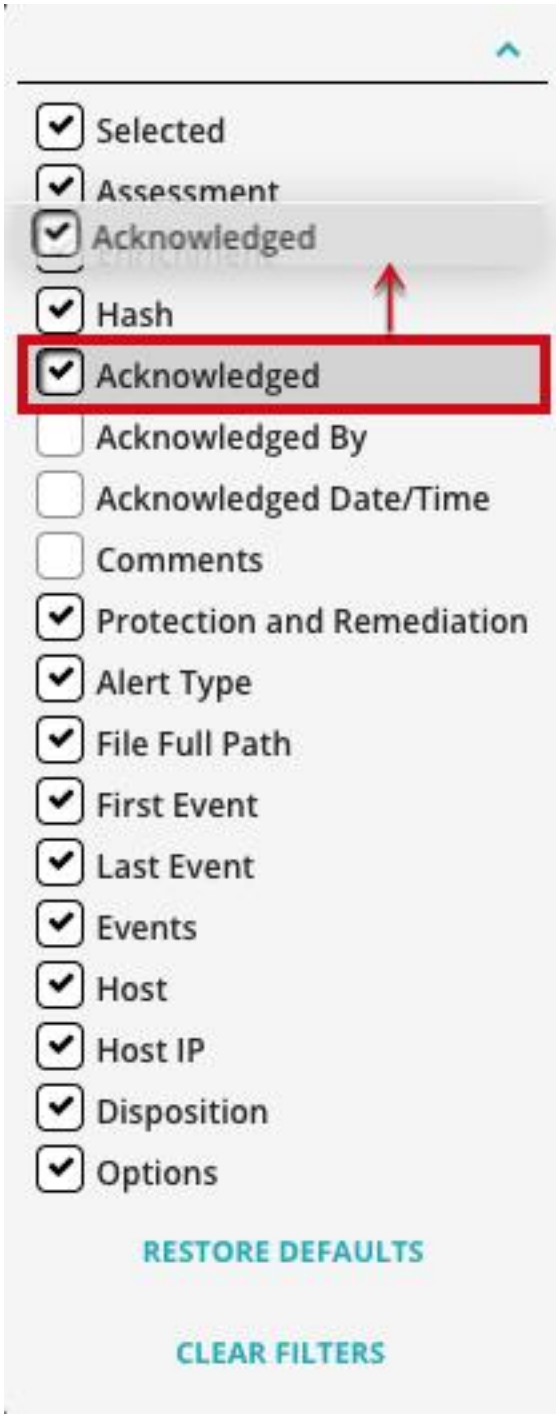
Spalten in der Alerts Tabelle neu anordnen, ihre Größe ändern und wiederherstellen

Sie können Ihre Alerts Tabelle auch anpassen, indem Sie die Tabellenspalten neu anordnen, ihre Größe ändern und sie wiederherstellen.

Um Spalten in der Alerts Tabelle neu anzuordnen:

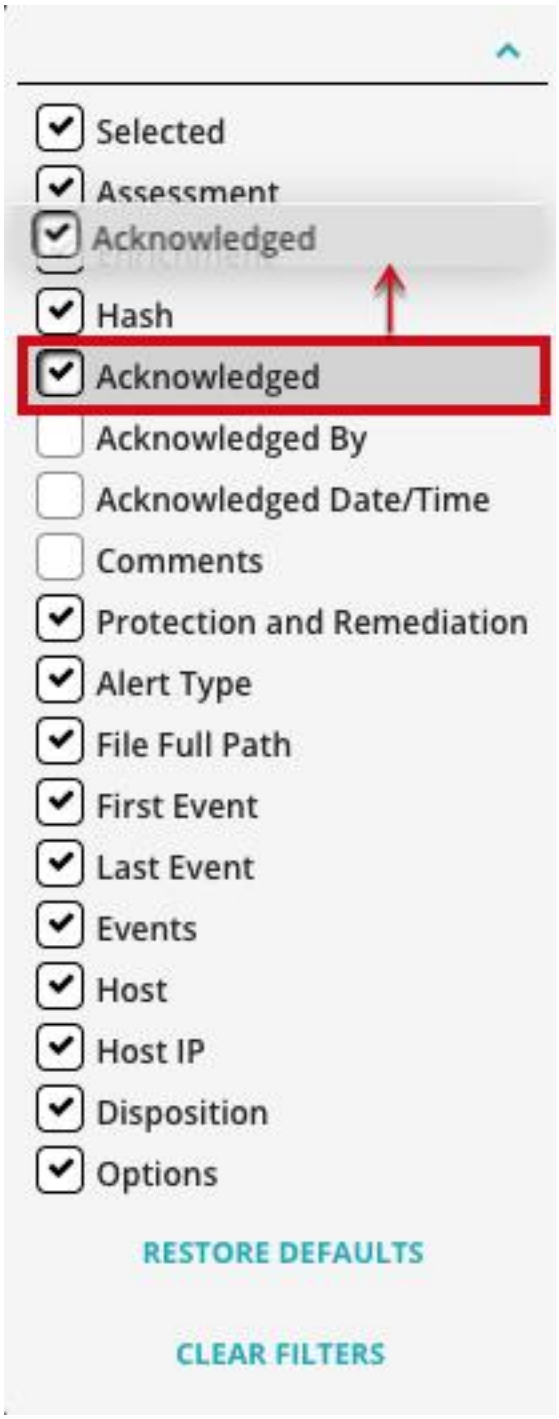
1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.

2. Klicken Sie auf das Spaltenauswahl ( ) Symbol, um die Liste der Tabellenspalten zu öffnen.
3. Klicken Sie auf eine bestimmte Spalte und ziehen Sie die Spalten in der Liste nach oben oder nach unten.



Um die Größe von Spalten in der Alerts Tabelle zu ändern:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die Alerts Seite zuzugreifen.
2. Finden Sie die Spalte, deren Größe Sie ändern wollen, in der Alerts Tabelle.
3. Klicken Sie auf die Spaltengrenze auf der rechten Seite der Spalte



4. Ziehen Sie die Grenze nach rechts oder links, um die Spaltengröße anzupassen.

Um alle Spalten in der Alerts Tabelle wieder herzustellen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die Alerts Seite zuzugreifen.

2. Klicken Sie auf das Spaltenauswahl () Symbol, um die Liste der Tabellenspalten zu öffnen.
3. Klicken Sie auf **Restore All**.

Standardspalten in der Alerts Tabelle wiederherstellen

Sie können die Alerts Tabelle wiederherstellen, um nur die Standardspalten anzuzeigen.

So stellen Sie alle Spalten in der Alerts Tabelle wieder her:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Klicken Sie auf das Spaltenauswahl () Symbol.
3. Klicken Sie auf **Restore All**.

Filter in der Alerts Tabelle verwenden

Sie können Ihre Alerts Tabelle verfeinern, indem Sie Filter für die Anzeige der Informationen verwenden, die Sie anzeigen wollen. Die nachfolgende Tabelle beschreibt die Attribute, die Sie zum Filtern der Alerts Tabelle verwenden können:

Alert Attribut	Beschreibung
Acknowledged	Filtern Sie Warnungen nach dem Bestätigungsstatus für jede Warnung: • Alle (Standard) • Ja (bestätigte Warnungen) • Nein (unbestätigte Warnungen)
Acknowledged By	Filtern Sie Warnungen nach dem Usernamen des Administrators, Analysts, Senior Analysts oder Investigators, der die Warnung bestätigt hat.
Acknowledged Date/Time	Filtern Sie nach dem Datum und der Uhrzeit, zu der die Warnung bestätigt wurde.

Alert Attribut	Beschreibung

Alert Type	Filtern Sie nach dem Warnungstyp, indem Sie den Typ von der Dropdown-Liste auswählen. Der ausgewählte Typ wird in der Spaltenüberschrift angezeigt.
	• ALLE (Standard)
	• IOC—Indicators of Compromise
	  • PRS—Presence
	  • EXC—Execution
	• MAL—Malware
	• XPLT—Exploit

Assessment	Filtern Sie Warnungen nach der Bewertung auf die folgenden Arten: • Klicken Sie innerhalb der Spaltenüberschrift, um Warnungen nach einem vollständigen oder Teil des Bewertungsnamen zu filtern. • Klicken Sie auf die Spaltenüberschrift, um Warnungen nach Bewertungsnamen in auf- oder absteigender Reihenfolge zu sortieren.
Disposition	Filtern Sie Warnungen nach einer Teilmenge. Filteroptionen umfassen: • Alle (Standard) • False Positive • Not False Positive
File Full Path	Filtern Sie nach dem mit dem letzten Ereignis für eine Warnung verbundenen Dateipfad. Dateipfade sind immer für MAL-Warnungen und EXD-Warnungen, aber nicht immer für IOC-Warnungen verfügbar.
First Event	Filtern Sie nach dem Zeitstempel einer Warnungensgruppe. Sie können nach einer relativen Zeit (**Today**, **Yesterday**, **Last 7 Days**, **Last 30 Days**, **This Month** oder **Last Month**) oder einer benutzerdefinierten Zeit filtern. Wählen Sie **Custom**, um einen Kalender zu öffnen und geben Sie einen bestimmten Zeitstempelbereich ein.

Alert Attribut	Beschreibung
Hash	Filtern Sie nach dem vollständigen oder partiellen Hash, das der Warnung zugeordnet ist. **HINWEIS—** Nicht alle Warnungen haben ein zugehöriges Hash.
Host	Filtern Sie nach dem mit der Warnung verknüpften Hostnamen. • Klicken Sie innerhalb der Spaltenüberschrift, um Warnungen nach einem vollständigen oder Teil des Hostnamen zu filtern. • Klicken Sie auf die Spaltenüberschrift, um Warnungen nach Hostnamen in auf- oder absteigender Reihenfolge zu sortieren.
Host IP	Zeigt die mit der Warnung verbundene Quell- oder Ziel-IP-Adresse an. • Klicken Sie innerhalb der Spaltenüberschrift, um Warnungen nach einem vollständigen oder Teil der IP-Adresse zu filtern. • Klicken Sie auf die Spaltenüberschrift, um Warnungen nach IP-Adressen in auf- oder absteigender Reihenfolge zu sortieren.
Last Event	Filtern Sie nach dem Zeitstempel der letzten Warnungen in der Warnungsgruppe. Sie können nach einer relativen Zeit (**Today**, **Yesterday**, **Last 7 Days**, **Last 30 Days**, **This Month** oder **Last Month**) oder einer benutzerdefinierten Zeit filtern. Wählen Sie **Custom**, um einen Kalender zu öffnen und geben Sie einen bestimmten Zeitstempelbereich ein.
Protection and Remediation	Filtern Sie Warnungen für einen bestimmten Status, indem Sie den Status von einer Dropdown-Liste auswählen. Der ausgewählte Status wird in der Spaltenüberschrift angezeigt. • ALLE (Standard) • BLOCK • PARTIAL BLOCK • QUARANTINED • CLEANED

Um die Alerts Tabelle nach einem bestimmten Warnungsattribut zu filtern:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Wählen Sie die Spalte in der Alerts Tabelle, nach der Sie filtern wollen und geben Sie das Warnungsfilterattribut im Filterfeld ein. Siehe Alert Attribut auf Seite 379.

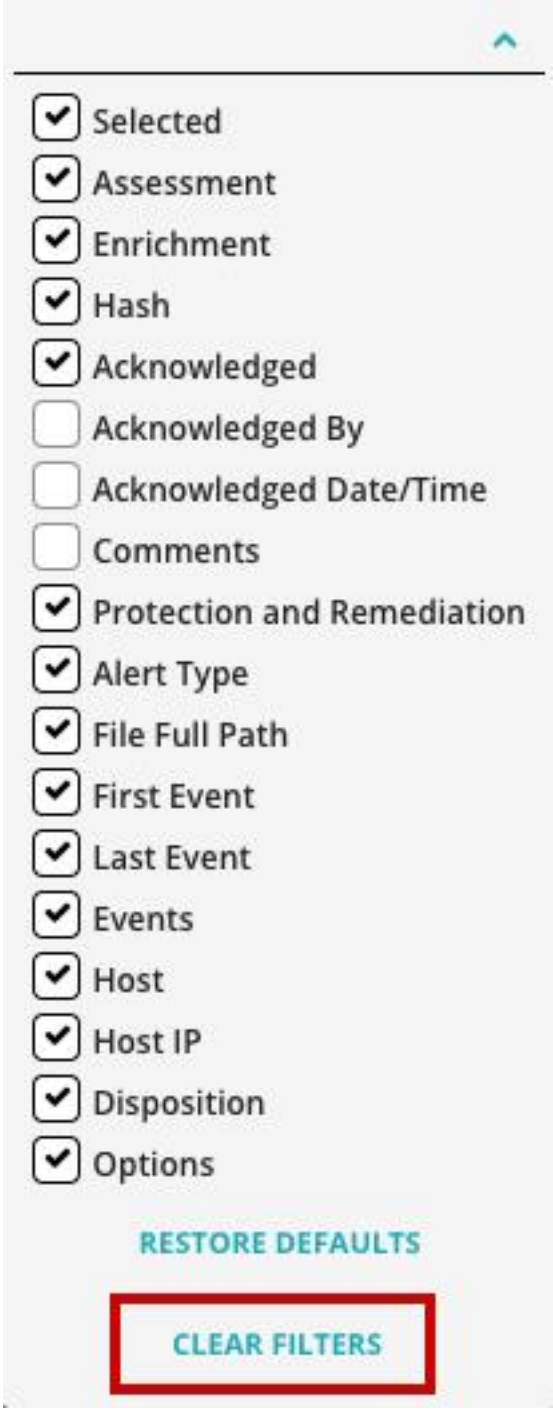
Filter in der Alerts Tabelle löschen

Verwenden Sie die Spaltenauswahl, um alle Filter in der Alerts Tabelle schnell zu löschen.

Um alle Filter in der Alerts Tabelle zu löschen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Klicken Sie auf das Spaltenauswahlsymbol  über der oberen rechten Ecke der Alerts Tabelle.

3. Klicken Sie auf **Clear Filters**.



Daten von der Alerts Tabelle exportieren

Sie können die Export Funktion verwenden, um Daten von der Alerts Tabelle in eine `.csv` Datei zu exportieren.

HINWEIS: Alle Warnungsdaten werden mit allen von Ihnen angewendeten Filtern und Sortierung exportiert.

Um Daten von der Alerts Tabelle in eine .csv Datei zu exportieren:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Klicken Sie auf das Downloadsymbol ( ), um Alarmdaten von der Tabelle in eine CSV-Datei zu exportieren.

Warnungs- und Ereignisinformationen je nach Host anzeigen

Die Hosts Seite der Endpoint Security Web-UI bietet eine Möglichkeit, Warnungen für einen bestimmten Host zu untersuchen. Erweitern Sie Host Endpunkt Informationen um zu sehen, welche Warnungen für den Host aufgetreten sind. Weitere Informationen finden Sie unter Hosts Menü auf Seite 40. Wenn eine Warnungen von einem anderen FireEye Produkt oder Service ausgeht (*ein Quellenwarnung*), bietet diese Seite auch Informationen und Links, um Trends zu erkennen und umfassendere Informationen zu erhalten. Weitere Informationen über Quellwarnungen finden Sie auf der Rules Seite. Siehe FireEye Quellenwarnungen auf Seite 415.

Warnungsinformationen für einen Host anzeigen

Voraussetzungen

- Administrator, Analyst, Senior Analyst oder Investigator Zugriff.

Um Warnungsdetails für einen Host anzuzeigen:

1. Wählen Sie **Hosts** am Anfang der Endpoint Security Seite.
2. Bestätigen Sie, dass dem **Hosts with Alerts** Tab ausgewählt ist.
3. Klicken Sie im Raster auf den Hosts With Alerts Tab auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Informationen über Warnungsdetails benötigen.

   Die Host Alert Details Seite wird angezeigt. Detaillierte Informationen über die Warnungen werden auf dem Alerts Tab auf dieser Seite angezeigt. Informationen über Dateien in Quarantäne werden auf dem Quarantines Tab auf dieser Seite angezeigt.

Weitere Informationen finden Sie unter Scan-Zusammenfassung auf Seite 63.

Warnungsgruppen verstehen

Die Alerts Tabelle zeigt eine Zeile für jede Warnung oder Warngruppe an. Wenn mehrere Alarme auf dem gleichen Host für den gleichen Indicator of Compromise (IOC) auftreten, beispielsweise über einen Zeitraum hinweg, werden diese Warnungen als eine Zeile in der Alerts Tabelle angezeigt.

Warnungen enthalten die Agent ID, was sich darauf auswirkt, wie Warnungen gruppiert werden. Zwei Warnungen von verschiedenen Agents sind nie in der gleichen Gruppe enthalten.

In den folgenden Abschnitten werden Warnungsgruppen für Malware, IOC, Exploit-Erkennung und allgemeine Warnungen beschrieben.

Gruppierung von Malware Alarmen

Malware Alarme werden gruppiert, wenn sie das gleiche MD5 Hash, Dateipfad, Malware Namen, Scantyp und Signaturinformationen haben. Wenn sie gruppiert sind, werden sie als eine Warnung mit mehreren Instanzen angezeigt.

HINWEIS: Von einem Malware Boot-Scan generierte Warnungen werden nur nach Infektionsnamen gruppiert.

IOC Warnungsgruppierung

IOC Warnungen werden nach Bedingungskennung gruppiert.

Exploit Warnungsgruppierung

Auf Exploit-Erkennung basierende Warnungen sind nach Zeitstempel, Dateipfad und MD5 Hash gruppiert.

Warnungszähler verstehen

Auf den Host Seiten in der Endpoint Security Web-UI werden mehrere verschiedene Warnungszähler angezeigt.

- Die Warnungen anzeigen und verwalten auf Seite 367 Seite und der Hosts with Alerts Tab zeigen die Anzahl der Warnungen an, die generiert wurden, wenn Agents übereinstimmende Aktivitäten auf Ihren Host-Endpunkten gefunden haben. Für jede Bedingung kann mehr als eine Warnung generiert werden.

- Die Warnungsliste im Host Alert Details Abschnitt der Host Alert Details Seite zeigt die Warnungen an, die generiert wurden, wenn Agents übereinstimmende Aktivitäten für den Host-Endpunkt gefunden haben. Wenn Sie auf eine Warnung klicken, werden die Bedingung, die die Warnung ausgelöst hat und die Ereignisse, die der Bedingung entsprechen, angezeigt.
- Die Beschreibung der im **Alerted *nnn* times on** Feld auf der Host Alert Details Seite aufgeführte Bedingung zeigt die Anzahl der Warnungen an, die von der Bedingung auf dem Host erstellt wurden. Die ist die Anzahl der *Vorkommnisse* der Warnung, die für den Host generiert wurden.

Wenn zum Beispiel ein Agent Endpoint-Beaconing an einen bekannten bösartigen Command and Control (CnC) meldet, gruppiert der Endpoint Security alle zukünftigen Berichte über Beaconing-Aktivitäten an diesen Server als eine Bedingung. Der Endpoint Security zeigt nicht jedes Mal eine separate Warnung an, wenn der Agent eine Aktivität meldet, die einer Bedingung entspricht. Die tatsächliche Anzahl der Vorkommnisse für eine Bedingung wird am Anfang des Alert Details Abschnitts auf der Seite als **Alerted *nnn* times on** gemeldet.

Wenn Sie Endpoint Security Warnungen in einer SIEM Konsole anzeigen, könnten Sie jedes Vorkommnis einer Aktivität als eine separate Warnung sehen.

Bestätigte Warnungen

Die neue Alert Acknowledgment Funktion in der Endpoint Security Web-UI ermöglicht Ihnen und Ihrem Team, eingehende Warnungen und mit jeder Warnung verbundene Ermittlungsaufgaben zu verwalten. Sie können Warnungen bestätigen und eine Bestätigung für eine einzelne Warnung oder mehrere Warnungen auf der Alerts Tabelle löschen. Sie können auch auf die Alert Acknowledgment Funktion für einen einzelnen Host auf der Host Details Seite zugreifen.

Verwenden Sie die Comment Funktion, um Details über die Warnung oder die Untersuchung aufzuzeichnen oder zu bearbeiten.

Verwenden Sie die Acknowledged Spalte, um die Alerts Tabelle zu filtern und zeigen Sie nur die gewünschten Warnungen an. Weitere Informationen finden Sie unter Filter in der Alerts Tabelle verwenden auf Seite 379.

Dieser Abschnitt behandelt die folgenden Themen:

- Eine Warnungsbestätigung von der Alerts Seite löschen auf Seite 390
- Eine Warnungsbestätigung von der Host Details Seite löschen auf Seite 391
- Bestätigung für mehrere Warnungen löschen auf Seite 391

Voraussetzungen

- Administrator, Analyst, Senior Analyst oder Investigator Zugriff.

Eine einzelne Warnung auf der Alerts Seite bestätigen

Folgen Sie diesen Schritten, um eine einzelne Warnung auf der Alert Seite in der Endpoint Security Web-UI zu bestätigen.

Um eine einzelne Warnung zu bestätigen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Suchen Sie die Warnung in der Alerts Tabelle, die Sie bestätigen wollen.
3. Klicken Sie auf das **Options** Symbol für diese Warnung.
4. Wählen Sie **Acknowledge**, um das Acknowledge Alert Fenster zu wählen.
5. Optional können Sie alle spezifischen Details über die Warnung oder die Ermittlung, die Sie aufzeichnen wollen, im **Comment** Feld eingeben
6. Klicken Sie auf **Acknowledge**.

   Wenn Sie eine Warnung bestätigen, wird die **Alerts** Seite automatisch aktualisiert und aktualisiert die Acknowledged, Acknowledged By und Acknowledged Date/Time Felder der Warnung.

Eine einzelne Warnung auf der Host Details Seite bestätigen

Folgen Sie diesen Schritten, um eine einzelne Warnung auf der Host Details Seite zu bestätigen.

Um eine einzige Warnung von der Host Details Seite zu bestätigen:

1. Wählen Sie **Hosts** am Anfang der Seite. Die Hosts Seite wird angezeigt.
2. Wählen Sie den Host with Alerts Tab, um eine Liste Ihrer Host-Endpunkte mit Warnungen anzuzeigen, oder wählen Sie den All Hosts Tab, um eine Liste Ihrer Host-Endpunkte anzuzeigen.

3. Klicken Sie in der Liste auf einem der Tabs auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Host Detail Informationen anzeigen wollen. Die Host Details Seite wird angezeigt.
4. Klicken Sie auf **Acknowledge**, um das Acknowledge Alert Fenster zu öffnen.
5. Im **Comment** Feld geben Sie alle spezifischen Details über die Warnung oder Ermittlung ein, die Sie aufzeichnen wollen.
6. Klicken Sie auf **Acknowledge**.

   Wenn Sie eine Warnung bestätigen, wird die **Alerts** Seite automatisch aktualisiert und die Acknowledged, Acknowledged By und Acknowledged Date/Time Felder der Warnung werden aktualisiert.

Mehrere Warnungen bestätigen

Folgen Sie diesen Schritten, um mehrere Warnungen auf der Alert Seite in der Endpoint Security Web-UI zu bestätigen.

Um mehrere Alarme zu bestätigen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. In der Alerts Tabelle klicken Sie auf das Kontrollkästchen (☐) neben jede Warnung, die Sie bestätigen wollen.
3. Klicken Sie auf das **Delete** Menü am Anfang der Alerts Tabelle und wählen Sie **Acknowledge**.

4. Wählen Sie **Go**.

   Wenn Sie mehrere Warnungen bestätigen, wird die **Alerts** Seite automatisch aktualisiert und aktualisiert Acknowledged, Acknowledged By und Acknowledged Date/Time Felder für alle Warnungen, die Sie bestätigt haben

Warnungskommentare hinzufügen oder bearbeiten

Folgen Sie diesen Schritten, um einen Kommentar für eine Warnung hinzuzufügen oder zu bearbeiten. Sie können einen Warnungskommentar hinzufügen oder zu bearbeiten, ohne die Warnung zu bestätigen.

HINWEIS: Die Endpoint Security Web-UI speichert nur die neuesten Alarmkommentare. Historische Kommentare und Zeitstempel werden nicht unterstützt.

Um einen Warnungskommentar hinzuzufügen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Suchen Sie in der Alerts Tabelle nach der Warnung, zu der Sie einen Kommentar hinzufügen wollen.
3. Klicken Sie auf das **Options** Symbol für diese Warnung.
4. Wählen Sie **Add Comment**, um das Comment Fenster zu öffnen.
5. Geben Sie Details über die Warnung oder Ermittlung ein, die Sie aufzeichnen wollen.

Um einen Warnungskommentar zu bearbeiten:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Suchen Sie die Warnung in der Alerts Tabelle, für die Sie den Kommentar bearbeiten wollen.
3. Klicken Sie auf das **Comments** Feld für die Warnung, um das **Edit Comment** Fenster zu öffnen.
4. Verändern oder fügen Sie Details über die Warnung oder Ermittlung hinzu, die Sie aufzeichnen wollen.

Eine Warnungsbestätigung von der Alerts Seite löschen

Folgen Sie diesen Anleitungen, um eine Warnungsbestätigung von der Alerts Seite zu löschen:

Um eine Warnungsbestätigung von der Alerts Seite zu löschen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Suchen Sie die einzelne Warnung in der Alerts Tabelle, die Sie bestätigen wollen.
3. Klicken Sie auf das **Options** Symbol für diese Warnung.
4. Wählen Sie **Unacknowledged**.

   Wenn Sie die Bestätigung für eine Warnung löschen, wird die **Alerts** Seite automatisch aktualisiert und das Acknowledged Feld der Warnung wird verändert. Die Inhalte in den Acknowledged By und Acknowledged Date/Time Feldern werden ebenfalls gelöscht. Notizen, die im Comments Feld aufgezeichnet wurden, werden beibehalten.

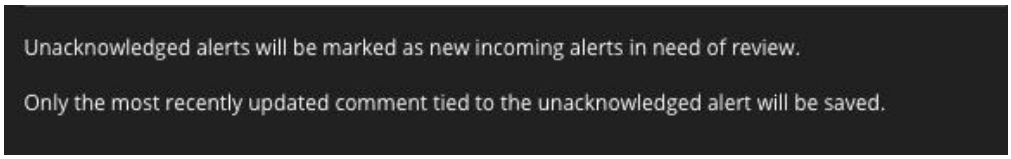
Eine Warnungsbestätigung von der Host Details Seite löschen

Folgen Sie diesen Schritten, um eine Warnungsbestätigung von der Host Details Seite zu löschen.

Um eine Warnungsbestätigung von der Host Details Seite zu löschen:

1. Wählen Sie **Hosts** am Anfang der Seite. Die Hosts Seite wird angezeigt.
2. Wählen Sie den Host with Alerts Tab, um eine Liste Ihrer Host-Endpunkte mit Warnungen anzuzeigen, oder wählen Sie den All Hosts Tab, um eine Liste Ihrer Host-Endpunkte anzuzeigen.
3. Klicken Sie in der Liste auf einem der Tabs auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Host Detail Informationen anzeigen wollen. Die Host Details Seite wird angezeigt.
4. Klicken Sie auf **Unacknowledge**, um das Unacknowledge Alert Fenster zu öffnen.

   Die folgende Warnmeldung und Erinnerung werden angezeigt:

5. Klicken Sie auf **Unacknowledge**.

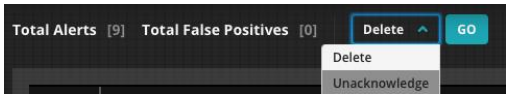
   Wenn Sie die Bestätigung für eine Warnung löschen, wird die **Alerts** Seite automatisch aktualisiert und die Acknowledged, Acknowledged By und Acknowledged Date/Time Felder der Warnung werden aktualisiert.

Bestätigung für mehrere Warnungen löschen

Verwenden Sie die Web-UI für den Zugriff auf die Alerts Seite, um Bestätigung für mehrere Warnungen zu löschen, die vorher bestätigt wurden.

Um Bestätigung für mehrere Warnungen zu löschen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Klicken Sie in der Alerts Tabelle auf das Kontrollkästchen (☐) neben jeder Warnung, deren Bestätigung Sie löschen wollen.
3. Klicken Sie auf das **Delete** Menü am Anfang der Alerts Tabelle und wählen Sie **Unacknowledge**.

4. Wählen Sie **Go**.

   Wenn Sie die Bestätigung für mehrere Warnungen löschen, wird die **Alerts** Seite automatisch aktualisiert und das Acknowledged Feld für alle Warnungen, deren Bestätigung Sie gelöscht haben, wird aktualisiert. Die Inhalte in den Acknowledged By und Acknowledged Date/Time Feldern werden ebenfalls gelöscht. Notizen, die im Alert Comments Feld aufgezeichnet wurden, werden beibehalten.

Warnungen löschen

Warnungen können auf verschiedene Arten gelöscht werden:

- Sie können Warnungen manuell löschen.
- Wenn eine Warnung abgelaufen ist, wird sie automatisch gelöscht. Siehe Warnungsalterung auf Seite 209.
- Wenn eine Indikatorregel gelöscht wird, werden alle zugehörigen Warnungen automatisch gelöscht. Siehe Indikatorregeln löschen auf Seite 234.

Auf diese Weise gelöschte Warnungen werden nicht länger auf der Warnungen auf der Alerts Seite anzeigen oder Hosts Seite oder in anderen Warnungszählungen angezeigt.

Dieses Thema beschreibt, wie Warnungen manuell mit Hilfe der Endpoint Security Web-UI gelöscht werden. Die CLI kann nicht nur Löschung von Warnungen verwendet werden.

Voraussetzungen

- Administrator, Senior Analyst oder Investigator Zugriff.

Um ausgewählte Warnungen manuell zu löschen:

1. Klicken Sie auf **Alerts** auf dem Dashboard-Menü, um auf die **Alerts** Seite zuzugreifen.
2. Verwenden Sie die Selection Spalte in der Alerts Tabelle, um das Kontrollkästchen neben jeder Warnung auszuwählen, den Sie löschen wollen.
3. Klicken Sie auf die **Delete** Schaltfläche über der Tabelle und wählen Sie **Delete** vom Menü.

Um alle Warnungen von einem Host manuell zu löschen.

1. Wählen Sie **Hosts** am Anfang der Seite.

   Die Hosts Seite wird angezeigt.
2. Klicken Sie auf dem der Host With Alerts oder All Hosts Register auf das Auswahlfeld links neben einem Hostnamen.

3. Auf dem **Actions** Menü wählen Sie **Delete alerts**.
4. Klicken Sie auf **Go** und bestätigen Sie, dass Sie die Warnungen für den Host löschen wollen.

Unter Quarantäne gestellte Dateien verwalten

Wenn Malware Schutz und Malware Beseitigung (Quarantäne) aktiviert sind, werden die infizierten Datein automatisch auf einen Quarantänebereich kopiert. Sie können diese Dateien für die Analyse erfassen.

Zusätzlich zur Quarantäne der infizierten Datei könnten Versuche unternommen werden, die Datei in Ihrem ursprünglichen Speicherort zu bereinigen.

- Wenn die Infektion infizierten Code an Benutzerdateien angehängt hat, wird versucht, die Infektion aus den Dateien zu entfernen. Wenn der Versuch, die Datei zu bereinigen, fehlschlägt, wird ein Versuch unternommen, die Datei auf den Endpunkt zu löschen.
- Wenn die Infektion neue Dateien auf den Endpunkt eingebracht hat, wird versucht, sie zu löschen. Wenn die infizierten Dateien gesperrt sind und nicht ohne Neustart des Endpunktes gelöscht werden können, wird eine Benachrichtigung auf dem Endpunkt angezeigt.

Dateien unter Quarantäne werden im Quarantänebereich auf dem Host-Endpunkt gespeichert, bis Sie sie manuell löschen oder sie den Zeitraum für die Quarantäne-Alterungsperiode überschreiten. Die Alterungsperiode der Quarantänedatei wird nach der Richtlinie festgelegt. Der Standardwert ist 90 Tage. Ausführliche Informationen zum Festlegen von Einstellungen für den Malware Schutz finden Sie im *Endpoint Security Agent Administrationshandbuch*.

In diesem Abschnitt wird beschrieben, wie Sie isolierte Dateien im Quarantänebereich verwalten.

- Unter Quarantäne gestellte Dateien anzeigen auf der nächsten Seite
- Unter Quarantäne gestellte Dateien erfassen auf Seite 395
- Unter Quarantäne gestellte Dateien wiederherstellen auf Seite 396
- Unter Quarantäne gestellte Dateien löschen auf Seite 397

Voraussetzungen

- Administrator, Analyst, Senior Analyst oder Investigator Zugriff.

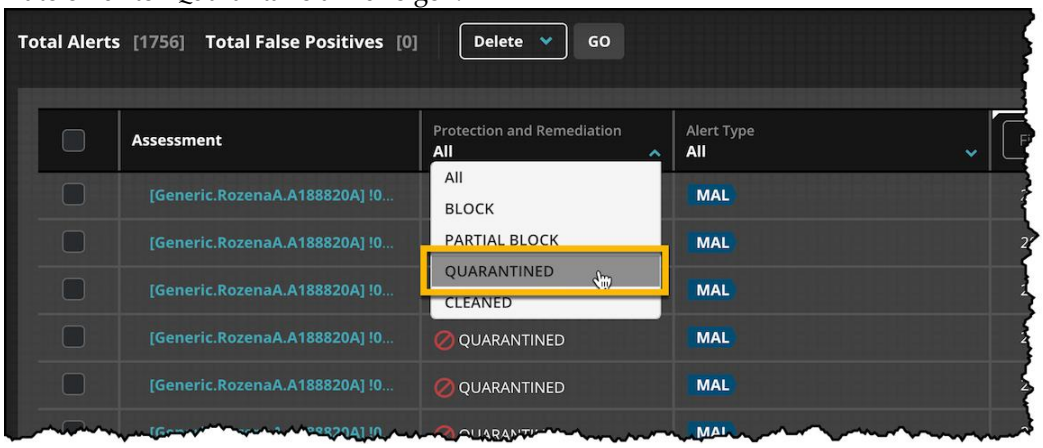
Unter Quarantäne gestellte Dateien anzeigen

Sie können die Endpoint Security Web-UI oder die API verwenden, um Dateien unter Quarantäne anzuzeigen. Die CLI kann nicht für deren Anzeige verwendet werden. Informationen über die Verwendung der API, um die Quarantänedateien anzuzeigen, finden Sie im Endpoint Security REST API-Handbuch.

Um Dateien unter Quarantäne mit Hilfe der Alerts Seite in der Web-UI anzuzeigen:

1. Wählen Sie **Alerts** am Anfang der Endpoint Security Seite.
2. Wählen Sie eine Malware Warnung, für die Sie Dateien unter Quarantäne sehen wollen. Die Alert Details Seite wird geöffnet.

   Tipp: Sie können Ergebnisse auf der Alerts Seite filtern, um nur die Warnungen mit Dateien unter Quarantäne anzuzeigen.



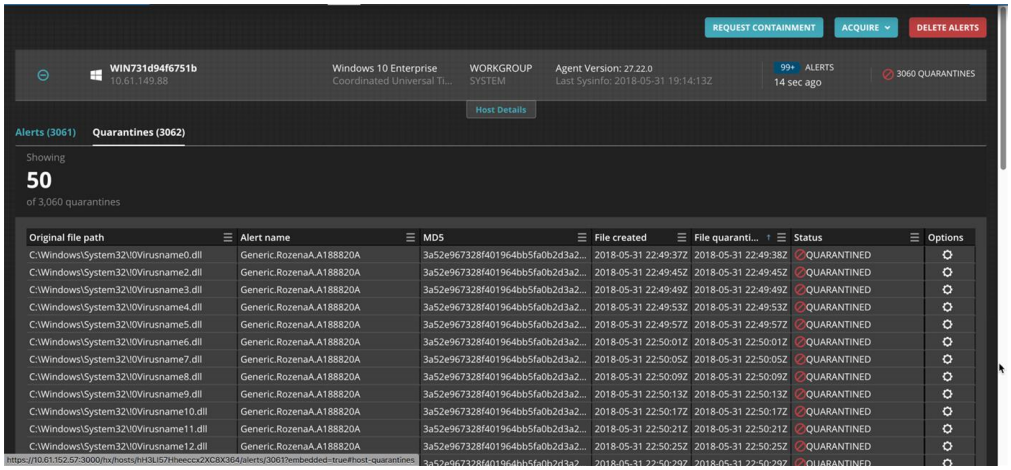
3. Wählen Sie den Quarantines Tab. Die Dateien unter Quarantäne sind aufgeführt.

Um Dateien unter Quarantäne mit Hilfe der Hosts Seite in der Web-UI anzuzeigen:

1. Wählen Sie **Hosts** am Anfang der Endpoint Security Web-UI Seite.
2. Bestätigen Sie, dass der **Hosts with Alerts** Tab ausgewählt ist.
3. Klicken Sie in dem Raster auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Informationen über Alarmdetails benötigen.

   Die Host Alert Details Seite wird angezeigt. Detaillierte Informationen über die Alarme werden auf dem Alerts Register auf dieser Seite angezeigt. Informationen über Dateien unter Quarantäne werden auf dem Quarantines Register auf dieser Seite angezeigt.

4. Wählen Sie den Quarantines Tab. Die Dateien unter Quarantäne sind aufgeführt.



Die Liste der unter Quarantäne befindlichen Dateien zeigt keine Malware an, die in Boot Abschnitten gefunden wurde.

Unter Quarantäne gestellte Dateien erfassen

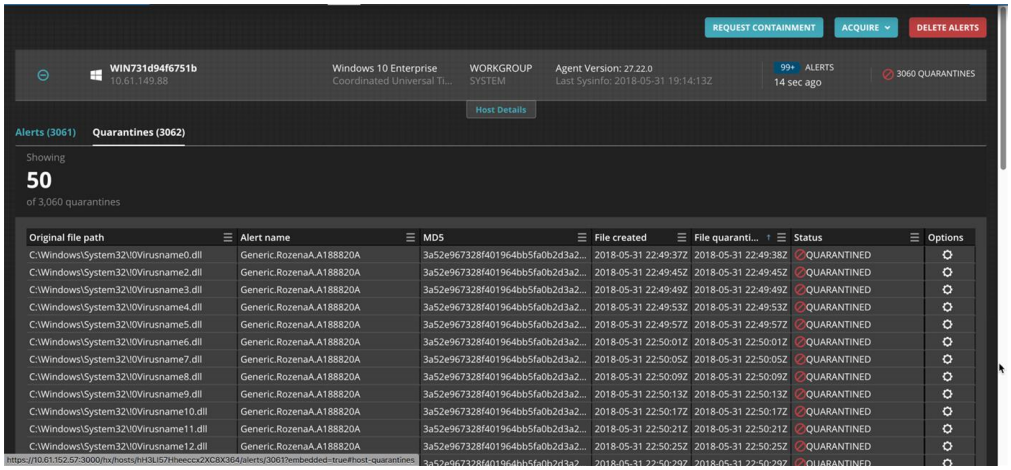
Sie können die Endpoint Security Web-UI oder die API verwenden, um Dateien unter Quarantäne aus dem Quarantänebereich eines Endpunktes zu erfassen. Die CLI kann nicht für die Erfassung verwendet werden. Informationen über die Verwendung der API für die Erfassung von Dateien unter Quarantäne finden Sie im Endpoint Security REST API-Handbuch.

Um Dateien unter Quarantäne mit Hilfe der Web-UI zu erfassen:

1. Wählen Sie **Hosts** am Anfang der Endpoint Security Web-UI Seite.
2. Bestätigen Sie, dass der **Hosts with Alerts** Tab ausgewählt ist.
3. Klicken Sie in dem Raster auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Informationen über Warndetails benötigen.

   Die Host Alert Details Seite wird angezeigt. Detaillierte Informationen über die Alarme werden auf dem Alerts Register auf dieser Seite angezeigt. Informationen über Dateien unter Quarantäne werden auf dem Quarantines Register auf dieser Seite angezeigt.

4. Wählen Sie den Quarantines Tab. Die Dateien unter Quarantäne sind aufgeführt.



5. Klicken Sie auf die Schaltfläche, die der Datei zugeordnet ist, die Sie erfassen wollen und wählen Sie **Acquire File**.

Unter Quarantäne gestellte Dateien wiederherstellen

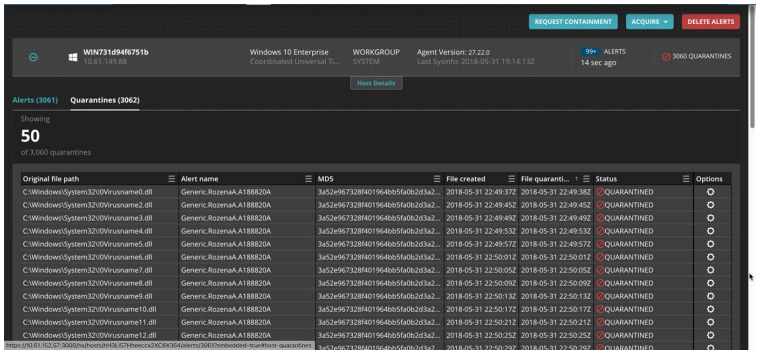
Sie können die Endpoint Security Web-UI oder API verwenden, um unter Quarantäne gestellte Dateien aus dem Quarantänebereich auf Ihre ursprünglichen Speicherorte auf dem Endpunkt wiederherzustellen. Die CLI kann nicht für die Wiederherstellung verwendet werden. Informationen über die Verwendung der API für die Wiederherstellung von Dateien unter Quarantäne finden Sie im Endpoint Security REST API-Handbuch.

Um Dateien unter Quarantäne mit Hilfe der Web-UI wiederherzustellen:

1. Wählen Sie **Hosts** am Anfang der Endpoint Security Web-UI Seite.
2. Bestätigen Sie, dass der **Hosts with Alerts** Tab ausgewählt ist.
3. Klicken Sie in dem Raster auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Informationen über Warndetails benötigen.

   Die Host Alert Details Seite wird angezeigt. Detaillierte Informationen über die Alarme werden auf dem Alerts Register auf dieser Seite angezeigt. Informationen über Dateien unter Quarantäne werden auf dem Quarantines Register auf dieser Seite angezeigt.

4. Wählen Sie den Quarantines Tab. Die unter Quarantäne gestellten Dateien werden aufgelistet.



5. Klicken Sie auf die Schaltfläche der Datei, die Sie wiederherstellen wollen und wählen Sie **Restore File**.

Unter Quarantäne gestellte Dateien löschen

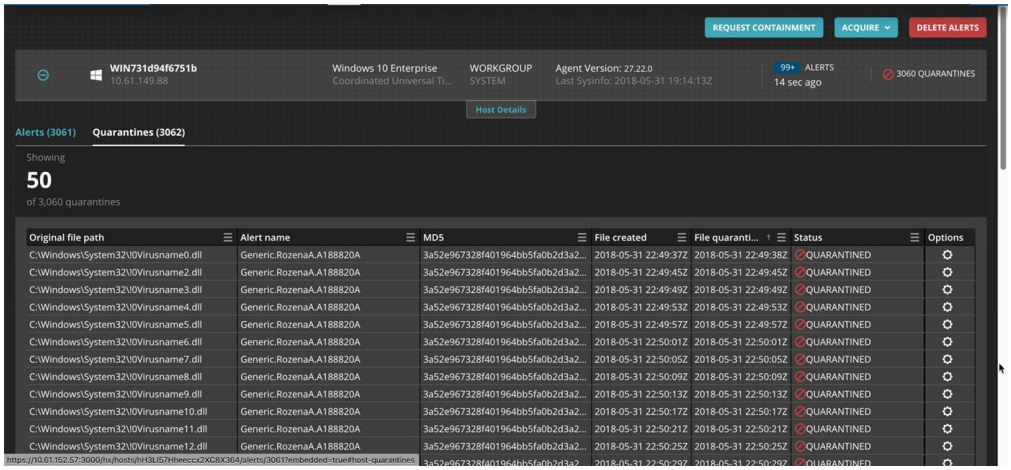
Sie können die Endpoint Security Web-UI oder die API verwenden, um Dateien unter Quarantäne aus dem Quarantänebereich eines Endpunktes zu löschen. Sie können die CLI nicht zum Löschen verwenden. Informationen über die Verwendung der API zum Löschen von Quarantänedateien finden Sie im Endpoint Security REST API-Handbuch.

Um Dateien unter Quarantäne mit Hilfe der Web-UI zu löschen:

1. Wählen Sie **Hosts** am Anfang der Endpoint Security Web-UI Seite.
2. Bestätigen Sie, dass der **Hosts with Alerts** Tab ausgewählt ist.
3. Klicken Sie in dem Raster auf das Erweiterungssymbol (⊕) neben dem Host, für den Sie Informationen über Warndetails benötigen.

   Die Host Alert Details Seite wird angezeigt. Detaillierte Informationen über die Alarme werden auf dem Alerts Register auf dieser Seite angezeigt. Informationen über Dateien unter Quarantäne werden auf dem Quarantines Register auf dieser Seite angezeigt.

4. Wählen Sie den Quarantines Tab. Die unter Quarantäne gestellten Dateien werden aufgelistet.



5. Klicken Sie auf die Schaltfläche, die der Datei zugeordnet ist, die Sie löschen wollen und wählen Sie **Delete File from Quarantine**, um die Datei aus dem Quarantänebereich zu löschen.

Warnung als ein Falsch Positiv einstellen

Wenn Sie auf einer Warnung auf **Mark False Positive** klicken, wird die Mark as False Positive Seite angezeigt. Sie können eine Warnung anzeigen und sie als ein falsch positiv von einer diesen Alert Seiten markieren:

- Alerts Seite—Wählen Sie **Mark as False Positive** vom Options Menü für eine Warnung. Weitere Informationen über die Alerts Seite finden Sie unter Warnungen auf der Alerts Seite anzeigen auf Seite 368.
- Host Alert Details Seite—Wählen Sie eine Warnung und klicken Sie auf **Mark False Positive** in den Warnungsdetails. Weitere Informationen finden Sie unter Scan-Zusammenfassung auf Seite 63.

HINWEIS: Sie können eine IOC oder XPLT Warnung auch auf der Triage Seite als falsch positiv markieren, aber durch diesen Workflow kann die Mark as False Positive Seite nicht geöffnet werden. Weitere Informationen finden Sie unter Falsch positiv Regeln auf der Triage Summary Seite definieren auf Seite 410

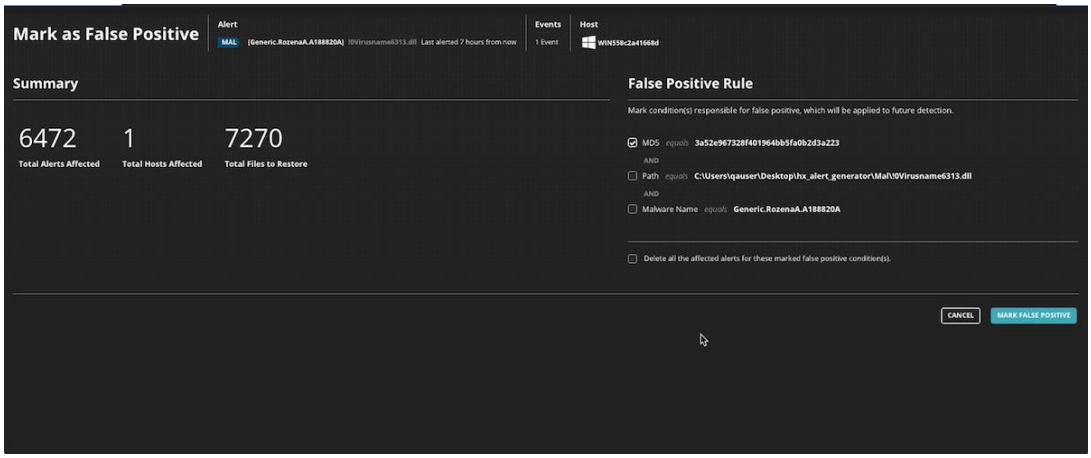
WICHTIG: Sie können keine allgemeine (GEN) Warnung als falsch positiv markieren.

Mark as False Positive Seite

Die Mark as False Positive Seite zeigt eine Zusammenfassung von Optionen für die falsch positiv Regel an. Die Falsch Positiv Regel wird auf alle zukünftigen Erkennungen mit Ausnahme von Exploit (XPLT) Warnungen angewendet. Für Exploit-Alarme werden die vorhandenen Warnungen im System als falsch positiv markiert, aber zukünftige Erkennung wird durch die falsch positiv Regel nicht beeinträchtigt.

WICHTIG: Um die falsch positiv Regel für alle zukünftigen Erkennungen von Exploit Warnungen zu aktivieren, müssen Sie das Exploit Timestamp Kontrollkästchen deaktivieren. Es ist standardmäßig ausgewählt.

Im folgenden Beispiel zeigt die Zusammenfassung, dass 6.472 Warnungen auf einem einzelnen Host aufgetreten sind und 7.270 Dateien in die Quarantäne verschoben wurden.



Voraussetzungen

- Administrator, Senior Analyst oder Investigator Zugriff.

Falsch Positiv Kriterien

In der Endpoint Security Web-UI können Sie eine Warnung je nach bestimmten Kriterien als falsch positiv markieren. Diese Informationen werden dann auf andere Warnungen angewendet, die den gleichen Kriterien entsprechen. Die verfügbaren falsch positiv Kriterien für jeden Warnungstyp werden in der nachfolgenden Tabelle bereitgestellt.

Warnungstyp	Falsch Positiv Kriterien
Malware (MAL)	• Malware Name • Path • MD5 Hash • Digitale Signatur
Exploit (XPLT)	• Exploit Timestamp • Exploit Prozesspfad • Exploit Prozess MD5 Hash
Indicator of Compromised (IOC)	Bedingung—Sie können die spezifische Bedingung markieren, die diese Warnung als falsch positiv identifiziert. Sie können keine individuellen Ausdrücke innerhalb der IOC Warnung markieren.
 **WICHTIG:** Sie können keine allgemeine (GEN) Warnung als falsch positiv markieren.	

Um eine Falsch Postiv Regel zu definieren:

1. Wählen Sie **Alerts** am Anfang der Endpoint Security Seite.
2. Wählen Sie die Warnung in der Alerts Tabelle, die Sie als falsch positiv markieren wollen. Sie können Filter verwenden, um Ihre Suchergebnisse einzugrenzen.

   Die Alert Details Seite wird angezeigt. Details werden auf der rechten Seite der Seite angezeigt. Die Regel oder der Indikator, der die Warnung ausgelöst hat, wird am Anfang angezeigt.

   - Für MAL und XPLT Warnungen wird die **Mark False Positive** Schaltfläche rechts von der Regel angezeigt.
   - Für IOC Warnungen klicken Sie auf den **Alerted on** Tab. Die **Mark False Positive** Schaltfläche wird auf der rechten Seite angezeigt.
3. Klicken Sie auf **Mark False Positive**.

   Die Mark as False Postitive Seite wird für MAL oder XPLT Warnungen angezeigt.

4. Wählen Sie eine oder mehrere Bedingungen von der Warnung, die in der falsch positiv Regel enthalten sein sollen.

   HINWEIS: Die Zusammenfassung links auf der Seite zeigt die Gesamtzahl der Warnungen an, die von Ihrer Auswahl betroffen sind, die Gesamtzahl der von Ihrer Auswahl betroffenen Hosts sowie die Gesamtzahl der Dateien, die auf Ihrer Auswahl basierend, nach der Definition der falsch positiv Regel wiederhergestellt werden sollen.

5. (Optional) Wählen Sie **Delete all the affected alerts for these marked false positive condition(s)**, wenn Sie die betroffenen Warnungen löschen wollen.
6. Klicken Sie auf **Mark False Positive**.
7. Klicken Sie auf **Export False Positive Alert Details**, um die Details über die falsch positiv Regel auf eine CSV-Datei zu exportieren.
8. Optional können Sie auf **Export Quarantined File Details** klicken, um Details über die Dateien in Quarantäne, die von der falsch positiv Regel betroffen ist, auf eine CSV-Datei zu exportieren.
9. Indem Sie auf der Bestätigungsseite auf **Confirm** klicken, fassen Sie die falsch positiv Regeldefinition zusammen.

   Die falsch positiv Regel wird zum False Positives Tab der Rules Seite hinzugefügt.

Falsch Positiv Regeln verwalten

Alarme, die auf Regeln basieren, die mit harmlosen Aktivitäten übereinstimmen, werden als falsch positive Alarme bezeichnet. Die Überprüfung von falsch positiv Alarmen kann wertvolle Administrator, Senior Analyst und Investigator Zeit verschwenden. Sie können falsch positiv Warnungen unterdrücken, indem Sie relevante Indicator of Compromise (IOC) Bedingungen sowie spezifische Malware oder Exploit Warninformationen identifizieren. Die Klassifizierung ist nicht dauerhaft und kann entfernt werden.

- Die Auswirkung Falsch Positiver Regeln auf Warnungen auf der nächsten Seite
- Info über Falsch Positiv Badges auf Seite 405
- Falsch positiv Regel überprüfen auf Seite 406
- Falsch Positiv Regeln definieren auf Seite 408
- Nach Falsch Positiv Regeln suchen auf Seite 412
- Falsch positiv Regeln entfernen auf Seite 413

Die Auswirkung Falsch Positiver Regeln auf Warnungen

Malware Warnungen

Sie können bestimmte, in Malware Regeln enthaltene Informationen verwenden, um eine *Malware falsch positiv Regel* zu erstellen. Einige Malware falsch positiv Regeln werden von FireEyes Dynamic Threat Intelligence (DTI) Cloud auf den Endpoint Security heruntergeladen. Wenn Endpoint Security Agents den Server abfragen, werden alle Malware falsch positiv Regeln automatisch auf die Endpunkte angewendet.

WICHTIG: Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

Der Endpoint Security führt die folgenden Aktionen aus, nachdem eine Malware falsch positiv Regel definiert wurde:

- Die spezifischen Malware Informationen in der Malware falsch positiv Regel werden für alle vorhandenen Malware Warnungen als falsch positiv markiert, die die Malware Informationen sowie alle neuen Malware Warnungen enthalten, die später erstellt werden könnten.
- Durch die Malware falsch positiv Regel ausgelösten Warnungen werden mit einem falsch positiv Badge markiert, aber nicht standardmäßig entfernt, wenn Sie die Malware falsch positiv Regel definieren, aber Sie können wählen, sie zu entfernen.
- Die Anzahl der von falsch positiv Malware Regeln betroffenen Malware Warnungen ist in den Warnungzählungen auf den Alerts und Hosts with Alerts Seiten enthalten.
- Wenn ein Host Endpunkt nur Warnungen für die falsch positiv Regel hat, verbleiben die Warnungen auf den Alerts und Hosts with Alerts Seiten, zeigen jedoch ein falsch positiv Badge an.

Das Entfernen einer benutzerdefinierten Malware falsch positiv Regel führt dazu, dass der Endpoint Security die folgenden Aktionen ausführt:

- Die spezifischen Malware Informationen in der falsch positiv Malware Regel werden nicht länger für alle bestehenden Warnungen als falsch positiv markiert, die die Malware Informationen enthalten. Der falsch positiv Badge wird von den vorhandenen Malware Warnungen entfernt, die nur von der Regel betroffen sind.
- Neue Malware Warnungen generieren normale Malware Warnungen.
- Die Anzahl der Malware Warnungen, die von falsch positiv Malware Regeln betroffen sind, wird in der Anzahl der Warnungen auf den Tabs der Alerts oder Hosts Seiten verringert.

- Der falsch positiv Badge wird auf den Hosts oder Hosts with Alerts Seiten entfernt, für die nur Alarme für die Malware falsch positiv Regeln vorhanden waren.

Malware falsch positive Regeln werden von der DTI entfernt, wenn FireEye feststellt, dass die falsch positiv Regel wirklich ein wahres positiv ist. FireEye Endpoint Security Agents werden benachrichtigt, wenn sie den Server das nächste Mal abfragen. Wenn DTI-basierte falsch postive Malware Regeln entfernt werden, werden die folgenden Aktionen ausgeführt:

- Zukünftige Vorkommnisse der Malware Informationen, die in der falsch positiv Regel benutzt wurden, generieren normale Malware Warnungen.
- ***Bestehende*** Malware Warnungen, die als falsch positive Warnungen markiert wurden, während die Regel eine falsch positive Regel war, werden weiterhin als falsch positiv Warnungen markiert und nicht auf true positiv Warnungen konvertiert. Dies unterscheidet sich von dem, was geschieht, wenn benutzerdefinierte falsch positiv Malware Regeln entfernt werden.

Indikator (IOC) Warnungen

Indicators of Compromise Regeln (IOC Regeln) sind aus Bedingungen zusammengesetzt. Sie können bestimmte Bedingungen in einem IOC markieren, um eine IOC falsch positiv Regel zu definieren. Sie können die IOC falsch positiv Regeln auch entfernen, wenn Sie feststellen, dass sie wirklich positiv sind.

Zusätzlich zu Ihren eigenen IOC falsch positiv Regeln aktualisiert FireEye Intel in regelmäßigen Abständen. Wenn FireEye feststellt, dass ein IOC Falsch Positiv verursacht, wird dieses IOC von der Intel entfernt. Wenn der Endpoint Security Server die aktualisierte Intel das nächste Mal herunterlädt, wird das IOC, das das falsch positiv verursacht hat, entfernt. Endpoint Security Agents empfangen diese aktualisierten Informationen, wenn sie den Server das nächste Mal abfragen.

Der Endpoint Security führt die folgenden Aktionen aus, nachdem eine IOC falsch positiv Regel definiert wurde:

- Die Bedingung, die in der IOC falsch positiv Regel enthalten ist, wird in allen vorhandenen Indikatorregeln sowie in allen neuen Indikatorregeln, die später erstellt werden können, als falsch positiv gekennzeichnet.
- Die Anzahl der aktiven Bedingungen wird für die Indikatorregeln aktualisiert, die das falsch positiv Ergebnis enthalten.

Das Entfernen von IOC falsch positiv Regeln verursacht, dass der Endpoint Security Server die folgenden Aktionen ausführt:

- Die zugrunde liegende Bedingung wird in allen vorhandenen Indikatorregeln und allen zukünftigen Indikatorregeln, die die Bedingung enthalten, wieder als aktiv angezeigt.
- Mit der Bedingung verbundene Alarme können auf Hosts erneut angezeigt werden.

- Die Anzahl der aktiven Bedingungen für vorhandene Indikatorregeln, die die Bedingung enthalten, wird zunehmen.
- Die Gesamtzahl der Warnungen auf der Hosts Seite könnte sich erhöhen. Hosts, die nur mit dieser Bedingung übereinstimmen, können auf dem Hosts with Alerts Register der Seite erneut angezeigt werden.

Historische Bedingungen

Eine *historische Bedingung* ist ein kollaterales Ergebnis der Erstellung einer IOC Falsch Positiv Regel. Wenn Sie einen Indikator mit IOC Falsch Positiv Regeln löschen, werden die Bedingungen in den Falsch Positiv Regeln, die nur mit diesem Indikator verbunden sind, verwaist und verbleiben als historische Bedingungen in dem System.

Sie können historische Bedingungen auf der Rules Seite anzeigen, nachdem Sie nach dem Wert der historischen Bedingung auf dem False Postives Tab gesucht haben, wenn die Bedingung als Falsch Positiv markiert war. Siehe Nach Falsch Positiv Regeln suchen auf Seite 412.

Das Entfernen von Falsch Positiv Klassifikationen aus historischen Bedingungen führt zu folgenden Ergebnissen:

- Die historische Bedingung wird nicht in Warnungen oder als aktive Bedingung angezeigt, bis jemand eine Indikatorregel erstellt oder bearbeitet, die diese enthält.
- Die historische Bedingung wird nicht länger auf der Rules Seite angezeigt, wenn Sie nach ihrem Indikatorregelwert suchen.

Exploit Warnungen

Warnungen über Exploit Erkennung basieren auf von FireEye erhaltenen Erkenntnissen über eine Vielzahl bekannter Exploits und online-Angriffen. Sie können ein Exploit als Falsch Positiv markieren und eine Falsch Positiv Regel entfernen, wenn Sie feststellen, dass das Exploit ein Richtig positiv ist.

User-definierte Exploit falsch positiv Regeln werden nicht auf den Endpoint Security Agent verteilt. Verwenden Sie Exploit falsch positiv Regeln nur zum Markieren von vorhandenen Warnungen auf dem Endpoint Security.

FireEye liefert regelmäßige Aktualisierungen für die Exploit falsch positiv Regeln (Ausnahmen) von der Dynamic Threat Intelligence (DTI) Cloud auf den Endpoint Security.

Der Endpoint Security führt die folgenden Aktionen aus, nachdem eine Exploit falsch positiv Regel definiert wurde:

- Das spezifische Exploit in der falsch positiv Regel ist für alle vorhandenen Exploit Warnungen als falsch positiv markiert, die die Exploit-Information enthalten. Sie

können auch wählen, falsch positive für alle neuen Exploit Warnungen zu markieren, die später erstellt werden (siehe "Mark as False Positive Seite" in Warnung als ein Falsch Positiv einstellen auf Seite 398).

- Durch die Exploit falsch positiv Regel ausgelösten Warnungen sind mit einem falsch positiv Badge markiert, werden aber nicht standardmäßig entfernt, wenn Sie die Regel definieren. Sie können die Warnungen entfernen.
- Die Anzahl der von Exploit falsch positiv Regen betroffenen Exploit-Warnungen ist in den Warnungzählungen auf den Alerts und Hosts with Alerts Seiten enthalten.
- Wenn ein Host-Endpunkt nur Warnungen für die Falsch Positiv Exploit-Regel enthält, verbleibt der Endpunkt auf den Alerts und Hosts with Alerts Seiten aber zeigt ein Falsch Positiv Badge an.

Info über Falsch Positiv Badges

In der Endpoint Security Web-UI können sowohl Hosts als auch Warnungen in Hostlisten und Warnungslisten mit Falsch Positiv Badges (FP)gekennzeichnet werden.

Wenn ein falsch positiv Badge einen roten Kreis um die Buchstaben "FP" anzeigt (FP MAL) wurde die falsch positiv Regel von FireEye identifiziert. Sie können von FireEye identifizierte falsch positiv Regeln nicht entfernen.

Wenn der falsch positiv Badge einen schwarzen Kreis um die Buchstaben "FP" (FP MAL) anzeigt, wurde die falsch positiv Regel von einer Person in Ihrer Organisation hinzugefügt. Diese falsch positiv Regeln können entfernt werden.

Wenn Falsch Positiv Badges auf der Alerts Seite angezeigt werden

Warnungen auf der Alerts Seite können wie unter Warnungsgruppen verstehen auf Seite 386 beschrieben gruppiert werden. Sie können Ihre Ergebnisse in der Alerts Tabelle filtern (z.B. nach Host oder nach Warntyp). Eine Warnung zeigt ein falsch positiv Badge an, wenn sie mit einer der falsch positiv Regeln übereinstimmt. Der falsch positiv Badge wird für jede eindeutige Warnung getrennt angewendet. Auf dieser Seite können Sie die falsch positiv Malware Warnungen genauer von den kritischeren Warnungen trennen.

Wenn Falsch Positiv Badges in Hostlisten angezeigt werden

Auf dem Hosts with Alerts Register zeigen Hosts ein falsch positiv Badge nur an, wenn *alle* Warnungen für den Host falsch positiv Warnungen sind. Wenn die Gesamtzahl der eindeutigen IOC (Indikator) Exploit und Malware Warnungen mit der Gesamtzahl eindeutiger IOC, Exploit und Malware falsch positiv Warnungen für einen Host übereinstimmt, wird der falsch positiv Badge auf der Zeile für den Host angezeigt.

Zusätzlich wird dieser Host auf dem Hosts with Alerts Register angezeigt, wenn er nach **False Positiv** Dispositionen gefiltert wird. Wenn Sie den Cursor über den Warnzähler für einen Host bewegen, zeigt ein Tool-Tip die Anzahl jedes Warntyps und die Anzahl von falsch positiven an.

Falsch positiv Regeln können für Hosts bestehen, die kein falsch positiv Badge auf dem Hosts with Alerts Tab anzeigen, weil nicht jede Bedingung, die einen Alarm für den Host generiert hat, mit einer falsch positiv Regel übereinstimmt. Ein Host mit falsch positiv Alarme aber ohne Badge könnten auf dem Hosts with Alerts Tab angezeigt werden, wenn er nach **Not False Positive** Dispositionen gefiltert wird.

Um zu ermitteln, ob für einen Host falsch positiv Malware vorhanden ist, erweitern Sie den Host auf dem Hosts with Alerts Register, um die Alarmdetails auf der Host Alert Details Seite anzuzeigen.

Falsch positiv Regel überprüfen

Sie können alle in Ihrer FireEye Endpoint Security Umgebung identifizierten falsch positiv Regeln mit Hilfe der Endpoint Security Web-UI überprüfen. Sie können nicht mit Hilfe der CLI überprüft werden.

Falsch positiv Regeln können individuelle Indicator of Compromise (IOC) Bedingungen, spezifische Malware Alarminformationen oder als falsch positiv identifizierte Exploit Alarminformationen sein.

- Alle falsch positiv Regeln überprüfen unten
- Falsch positiv Regeln mit Auswirkung auf eine Warnung überprüfen auf der nächsten Seite

Voraussetzungen

- Administrator, Senior Analyst oder Investigator Zugriff.

Alle falsch positiv Regeln überprüfen

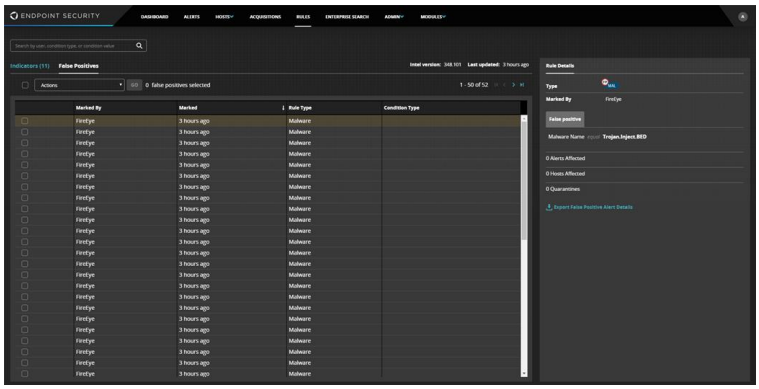
Sie können alle falsch positiv Regeln auf dem False Positives Register auf der Rules Seite überprüfen.

Um alle falsch positiv Regeln in Ihrer Endpoint Security Umgebung mithilfe der Web-UI zu überprüfen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Rules**, um die Rules Seite aufzurufen.

3. Wählen Sie das **False Positives** Register.

   Das False Positives Register führt alle falsch positiv Regeln auf, die in Ihrer Umgebung definiert sind.



4. Um die falsch positiv Regeldetails zu exportieren, klicken Sie im Detail Bereich auf **Export False Positive Alert Details**.

Doppelte falsch positiv Malware Regeln werden zum False Positives Register auf der Rules Seite hinzugefügt. Diese Duplikate können im Rule Details Bereich auf dem False Positives Register eine unterschiedliche Anzahl von betroffenen Hosts anzeigen. Duplikate können auftreten, wenn FireEye eine für einen Malware Scantyp spezifische Malware falsch positiv Regel hinzufügt, die mit einer vom User erstellten falsch positiv Regel übereinstimmt, die auf alle Malware Scantypen zutrifft. Wenn der Malware Scan für einen bestimmten Scantyp nicht ausgeführt wurde, ist die Anzahl der betroffenen Hosts (im False Positives Detail Bereich) für diesen Scantyp Null für diese Regel. Nicht-Null Host Zählungen werden nur für Scantypen angezeigt, die tatsächlich ausgeführt wurden und eine Warnung für die Regel generiert haben, bevor sie als falsch positiv markiert wurde.

Die vier Arten von on-Demand Malware Scans, die ausgeführt werden können sind Full Scan, Memory Scan, Quick Scan und Boot Scan. Der Boot Scan geschieht automatisch mit dem vollstandigen Scan und dem Kurzscan (full und quick scan). Die einzige Art von On-Acces Scan, der ausgeführt wird, ist der Echtzeitscan (real-time scan).

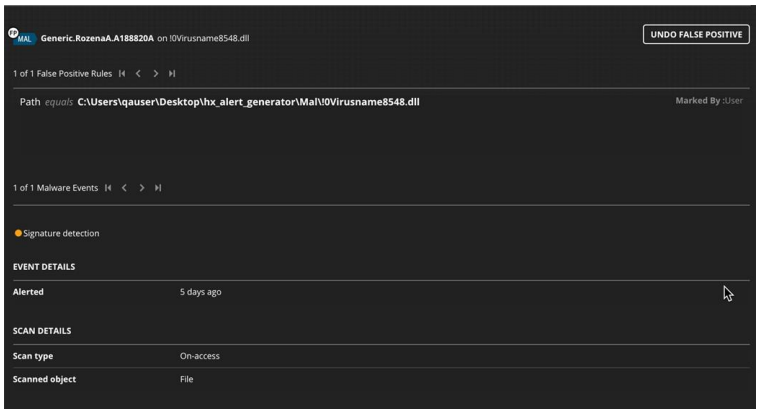
Falsch positiv Regeln mit Auswirkung auf eine Warnung überprüfen

Sie können falsch positiv Regeln mit Auswirkung auf eine Warnung auf der Alerts oder Hosts Seite überprüfen.

Um die falsch positiv Regeln mit Auswirkung auf eine individuelle Warnung mit Hilfe der Alerts Seite zu überprüfen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Alerts**.

3. Wählen Sie **False Positive** in der Disposition Spalte, um nach falsch positiv Warnung zu filtern.
4. Wählen Sie eine Warnung mit einem falsch positiv Badge. In den Warnungsdetails werden falsch positiv Informationen für die Warnung am Anfang der Details angezeigt. Wenn mehr als eine falsch positiv Regel die Warnung betreffen, können Sie durch diese abrollen.



Um die falsch positiv Regeln mit Auswirkung auf eine individuelle Warnung mit Hilfe der Hosts Seite zu überprüfen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie **Hosts**.
3. Wählen Sie das **Hosts with Alerts** Register.
4. Erweitern Sie einen (klicken Sie auf ⊕ neben einem) Host mit Alarmen, der auch falsch positiv Regeln enthält. Sie können diese Hosts auf dem Host with Alerts Register identifizieren, indem Sie den Mauszeiger über den Warnungszähler in der Hostliste ziehen. Die Anzahl jedes Warntyps sowie die Anzahl von Malware Warnungen, die von Falsch Positiv Malware Regeln betroffen sind, wird in einem Tool-Tip angezeigt.

   Die Host Details Seite für den Host wird angezeigt.
5. Wählen Sie eine Warnung mit einem falsch positiv Badge. In den Warnungsdetails werden falsch positiv Informationen für die Warnung am Anfang der Details angezeigt. Wenn mehr als eine falsch positiv Regel die Warnung betreffen, können Sie durch diese abrollen.

Falsch Positiv Regeln definieren

Sie können die folgenden Arten von falsch positiv Regeln definieren.

- Sie können eine Bedingung in einer Indicator of Compromise (IOC) Regel als falsch positiv markieren, um eine IOC falsch positiv Regel zu definieren. Dadurch wird die Bedingung von allen vorhandenen IOC Regeln entfernt und in zukünftigen IOC Regeln als falsch positiv markiert. Der Endpoint Security markiert automatisch alle Alarme, die mit der IOC falsch positiv Regel verknüpft sind, mit einem falsch positiv Badge. Ob die Warnung entfernt wird, hängt von Ihren Angaben ab, wenn Sie die IOC falsch positiv Regel definieren.
- Sie können Informationen in eines Malware (MAL) Alarms als falsch positiv markieren, um eine falsch positiv Malware Regel zu definieren. Der Endpoint Security markiert Malware Alarme, die mit Malware Alarmen verknüpft sind mit einem falsch positiv Badge. Ob der Alarm entfernt wird, hängt von Ihren Angaben ab, wenn Sie die falsch positiv Malware Regel definieren.
- Sie können Informationen in einem Exploit (XPLT) Alarm als falsch positiv markieren, um einen neuen falsch positiv Alarm zu definieren. Der Endpoint Security markiert Exploit Alarme, die mit Exploit falsch positiv Regeln verknüpft sind, mit einem falsch positiv Badge. Ob die Warnung entfernt wird, hängt von Ihren Angaben ab, wenn Sie die falsch positiv Exploit Regel definieren.

Falsch positiv Regeln können auf folgende Weise mit Hilfe derEndpoint Security Web-UI definiert werden.Sie können nicht mit Hilfe der CLI definiert werden.

- Warnung als ein Falsch Positiv einstellen auf Seite 398
- Falsch positiv Regeln auf der Host Details Seite definieren unten
- IOC falsch positiv Regeln auf der Rules Seite definieren auf Seite 411
- Falsch positiv Regeln auf der Triage Summary Seite definieren auf der nächsten Seite

Falsch positiv Regeln auf der Alerts Seite definieren

Sie können eine Warnung auf der Alerts Seite als falsch positiv markieren. Dadurch wird eine falsch positiv Regel erstellt, die dann auf andere Alarme angewendet wird, die den gleichen Kriterien entsprechen. Weitere Informationen über die Markierung einer Warnung als falsch positiv von der Alerts Seite finden Sie unter Warnung als ein Falsch Positiv einstellen auf Seite 398.

Falsch positiv Regeln auf der Host Details Seite definieren

Um eine falsch positiv Regel auf der Host Details Seite zu definieren:

1. Wählen Sie **Hosts** am Anfang der Endpoint Security Seite. Die Hosts Seite wird angezeigt.
2. Wählen Sie das **Hosts with Alerts** Register.

3. Klicken Sie auf das Erweiterungssymbol (⊕) neben dem Host mit der Warnung, die Sie als falsch positiv markieren wollen.

   Die Host Alert Details Seite wird angezeigt.

   Details werden auf der rechten Seite der Seite angezeigt. Die Regel oder der Indikator, der die Warnung ausgelöst hat, wird am Anfang angezeigt.

4. Wählen Sie eine Warnung in der Liste, um Details anzuzeigen.
   - Für MAL und XPLT Alarme wird die, **Mark False Positive** Schaltfläche rechts von der Regel angezeigt.
   - Für IOC Regeln klicken Sie auf den **Alerted on** Tab. Die **Mark False Positive** Schaltfläche wird auf der rechten Seite angezeigt.

5. Klicken Sie auf **Mark as false positive**

   .Die Mark as False Positive Seite wird für MAL oder XPLT Alarme angezeigt.

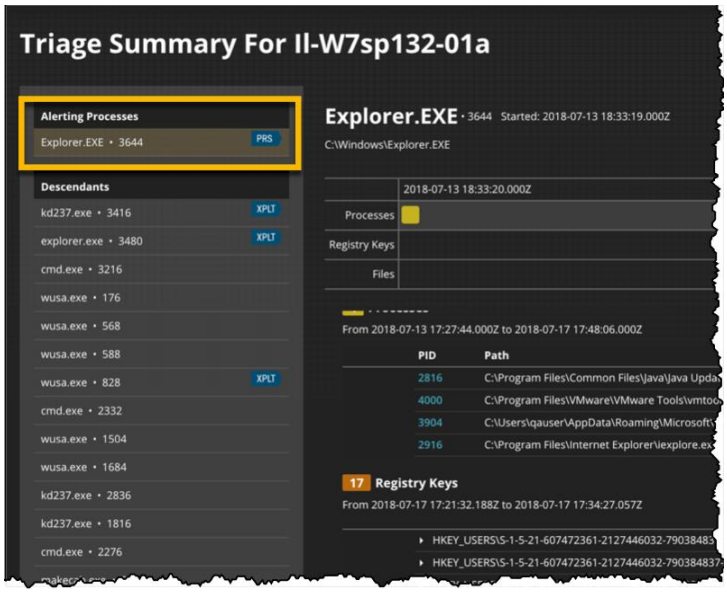
6. Konfigurieren Sie die Regel mit Hilfe der Anweisungen unter Warnung als ein Falsch Positiv einstellen auf Seite 398.

Falsch positiv Regeln auf der Triage Summary Seite definieren

Sie können eine Indicator of Compromise (IOC) oder Exploit (XPLT) Warnung auf der Triage Summary Seite mit Hilfe des folgenden Vorgangs als falsch positiv markieren.

Um eine IOC oder XPLT Warnung als falsch positiv Regel auf der Triage Summary Seite zu definieren:

1. Öffnen Sie eine Triage Zusammenfassung entweder von der Hosts Seite oder der Acquisitions Seite. Weitere Informationen finden Sie unter Triage-Sammlungen im Triage Viewer überprüfen auf Seite 334.
2. Wählen Sie einen Alerting Process im linken Abschnitt. Ein Beispiel wird in der folgenden Abbildung angezeigt.



3. Im Details Bereich auf der rechten Seite klicken Sie auf den Badge für die Warnbedingung, die Sie als ein falsch positiv markieren wollen. Im folgenden Beispiel haben wir den Presence (PRS) Warnbadge ausgewählt.

   Das Details Dialogfeld wird geöffnet.

4. Klicken Sie auf **Mark as false positive**.

IOC falsch positiv Regeln auf der Rules Seite definieren

Um eine IOC falsch positiv Regel auf der Rules Seite zu definieren:

1. Wählen Sie **Rules**, um die Rules Seite aufzurufen.
2. Auf dem Indicators Register wählen Sie die Indikatorregel, die die Bedingung enthält, die Sie als ein falsch positiv in einer IOC falsch positiv Regel definieren wollen.

3. Im Detail Abschnitt auf der rechten Seite klicken Sie auf die Bedingung, die Sie als ein falsch positiv kennzeichnen wollen.

   Eine **Mark as false positive** Option wird rechts über der Bedingung angezeigt.

4. Klicken Sie auf **Mark as false positive**.

   Die Mark as False Positive Seite wird angezeigt.

5. Konfigurieren Sie die Regel mit Hilfe der Anweisungen unter Warnung als ein Falsch Positiv einstellen auf Seite 398.

   Die Bedingung bleibt im Indicator Details Bereich sichtbar, ist jedoch inaktiv. Die IOC falsch positiv Regel für diese Bedingung wird definiert und zu dem False Positives Register auf der Rules Seite hinzugefügt.

Nach Falsch Positiv Regeln suchen

Möglicherweise haben Sie von einer neue Bedrohung gehört und wollen herausfinden, ob Ihr Unternehmen bereits nach solchen Aktivitäten sucht. Oder Sie finden möglicherweise eine verwaiste oder historische Bedingung.

Die Rules Seite der Endpoint Security Web-UI zeigt Falsch Positiv Regeln im Details Abschnitt auf dem Indicators Register und dem False Positives Register an. Durchsuchen Sie eine der Listen, um eine falsch positiv Regel zu finden, die die Bedrohungsbedingung enthält. Sie können auch auf dem False Positives Register nach falsch positiv Regeln suchen. Sie können nach falsch positiv Bedingungen nicht mit Hilfe der CLI suchen.

In der Regel ist es einfacher, anhand ihres MD5-Hashs oder Dateinamens nach falsch positiv Regeln zu suchen, aber Sie können auch auf einer beliebigen Bedingung oder Malware Information basierend in der falsch positiv Regel suchen.

In diesem Thema wird beschrieben, wie auf dem False Positive Register nach falsch positiv Regeln gesucht wird.

Voraussetzungen

- Administrator, Senior Analyst oder Investigator Zugriff.

Um falsch positiv Regeln auf dem False Positives Register zu finden:

1. Wählen Sie **Rules**, um auf die Rules Seite auf der Endpoint Security Web-UI zuzugreifen.
2. Wählen Sie das False Positives **Register.**
3. Im **Search by user, condition type, or condition value** Feld geben Sie eins der Folgenden ein:

- User—Der Endpoint Security Username. Von FireEye bereitgestellte falsch positiv Regeln haben den Usernamen `FireEye`.
- Condition type—der Bedingungstyp, z.B. `fileWriteEvent`
- Condition value—der Wert der Bedingung, z.B. der MD5 Hashwert oder Dateiname

4. Klicken Sie auf das Vergrößerungsglas auf der rechten Seite des Suchfeldes oder drücken Sie **Eingabe**.

   Die Liste der falsch positiv Regeln auf dem False Positives Tab wird nur nach den Regeln angezeigt, die Ihren Suchkriterien entsprechen.

Falsch positiv Regeln entfernen

Sie können eine falsch positiv Regel mit Hilfe der Alerts Seite, der Host Details Seite oder dem False Positives Tab auf der Rules Seite entfernen.

- Falsch positiv Regeln mit Hilfe der Alerts Seite entfernen unten
- Falsch positiv Regeln mit Hilfe der Host Details Seite entfernen auf der nächsten Seite
- Falsch positiv Regeln mit Hilfe der Rules Seite entfernen auf Seite 415

Wenn Sie eine falsch positiv Regel finden müssen, sehen Sie Nach Falsch Positiv Regeln suchen auf der vorherigen Seite.

Voraussetzungen

- Admin, Senior Analyst oder Investigator Zugriff.

Falsch positiv Regeln mit Hilfe der Alerts Seite entfernen

Um eine falsch positv Regel mit Hilfe der Alerts Seite zu entfernen:

1. Wählen Sie **Alerts**, um auf die Alerts Seite zuzugreifen.
2. Stellen Sie den Wert in der Disposition Spalte auf **False Positive** ein, um nur die Alarme anzuzeigen, die als falsch positiv markiert sind. Sie können Ihre Ergebnisse weiter einschränken, indem Sie andere Spalten filtern (z.B. nach Warntyp). Weitere Informationen finden Sie unter Warnungen anzeigen und verwalten auf Seite 367.
3. Finden Sie die Warnung, die Sie ändern wollen.
4. Auf dem Options Menü wählen Sie **Undo False Positive**.

   Die Undo False Postive Seite wird geöffnet.

5. Optional klicken Sie auf **Export Undo False Positive Alert Details**, um die Details über die Entfernung der falsch positiv Regel auf eine CSV-Datei zu exportieren.
6. Klicken Sie auf der Undo False Positive Seite auf **Undo False Positive**.

   Die falsch positiv Regel wird entfernt.

Falsch positiv Regeln mit Hilfe der Host Details Seite entfernen

Um eine falsch positiv Regel mit Hilfe der Host Details Seite zu entfernen:

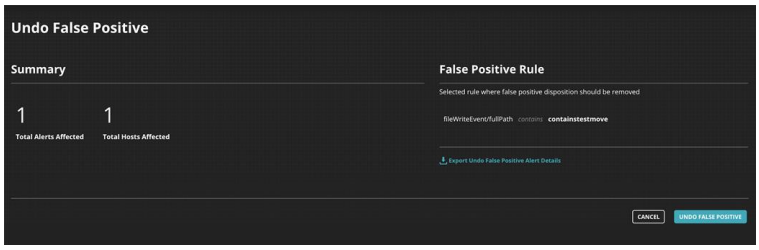
1. Wählen Sie **Hosts** am Anfang der Endpoint Security Web-UI Seite.

   Die Hosts Seite wird angezeigt.
2. Wählen Sie das **Hosts with Alerts** Register.
3. Klicken Sie auf das Erweiterungssymbol (⊕) neben dem Host mit der Warnung, von dem Sie die falsch positiv Regel entfernen möchten.

   Die Host Alert Details Seite wird angezeigt.
4. Wählen Sie die Warnung auf der Liste.

   Die Regel oder der Indikator, der der Alarm ausgelöst hat, wird am Anfang des Details Abschnitts angezeigt.
5. Finden und klicken Sie auf die **Undo False Positive** Schaltfläche.
   - Für MAL und XPLT Warnungen wird die **Undo False Positive** Schaltfläche rechts von der Regel angezeigt.
   - Für IOC Regeln klicken Sie auf den **Alerted on** Tab. Die **Undo False Positive** Schaltfläche wird auf der rechten Seite angezeigt.

   Die Undo False Positive Seite wird angezeigt.



6. Optional klicken Sie auf **Export Undo False Positive Alert Details**, um die Details über die Entfernung der falsch positiv Regel auf eine CSV-Datei zu exportieren.

7. Klicken Sie auf der Undo False Positive Seite auf **Confirm**.

   Die falsch positiv Regel wird entfernt.

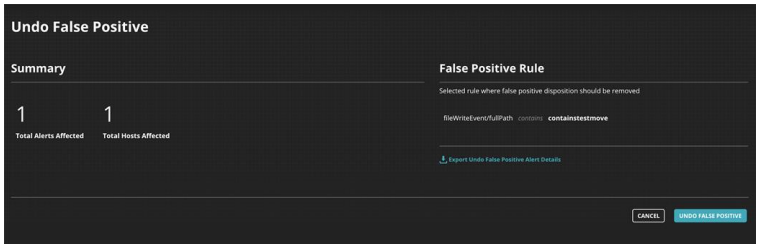
   Ein Teil einer falsch positiv Regel kann nicht entfernt werden Wenn Sie eine einzelne Bedingung aus einer falsch positiv Regel entfernen müssen, die mehrere Bedingungen enthält, entfernen Sie die gesamte Regel, und erstellen Sie sie dann erneut nur mit den Bedingungen, die Sie benötigen.

Falsch positiv Regeln mit Hilfe der Rules Seite entfernen

Um eine falsch positiv Regel mit Hilfe des Rules Tabs auf der Rules Seite zu entfernen:

1. Wählen Sie **Rules**, um die Rules Seite aufzurufen.
2. Wählen Sie den **False Positives** Tab.
3. Wählen Sie die falsch positiv Regel, die Sie entfernen wollen.
4. Im Detailabschnitt auf der rechten Seite klicken Sie auf die falsch positiv Regel.
5. Klicken Sie auf **Undo False Positive**.

   Die Undo False Positive Seite wird angezeigt.



6. Optional klicken Sie auf **Export Undo False Positive Alert Details**, um die Details über die Entfernung der falsch positiv Regel auf eine CSV-Datei zu exportieren.
7. Klicken Sie auf der Undo False Positive Seite auf **Confirm**.

   Die falsch positiv Regel wird entfernt.

   Ein Teil einer falsch positiv Regel kann nicht entfernt werden Wenn Sie eine einzelne Bedingung aus einer falsch positiv Regel entfernen müssen, die mehrere Bedingungen enthält, entfernen Sie die gesamte Regel, und erstellen Sie sie dann erneut mit den Bedingungen, die Sie benötigen.

FireEye Quellenwarnungen

Quellenwarnungen sind Warnungen, die verdächtigen Aktivitäten entsprechen, die durch von anderen FireEye Produkten und Diensten empfangene Intelligenz identifiziert wurden.

Um Quellenwarnungen in Ihrer Umgebung zu aktivieren, muss Ihr Endpoint Security mit anderen FireEye Produkten und Diensten integriert werden.

Wenn der FireEye mit einem anderen Endpoint Security Produkt integriert ist, empfängt er Berichte über verdächtige Aktivitäten von diesem Produkt, analysiert die Berichte und erstellt relevante Indikatorregeln auf Grundlage von verwertbaren Daten in den Berichten. Diese Indikatorregeln werden automatisch mit dem Agent für jeden Endpunkt geteilt. Die Agents bestätigen das Vorhandensein von Übereinstimmungen für diese Indikatorregeln auf Ihren Hosts. Warnungen, die auf Indikatorregeln basieren, die von anderen FireEye Produkten stammen, werden *Quellenwarnungen* genannt.

Verwenden Sie die Anweisungen in diesem Thema, um zusätzliche Informationen über Quellenwarnungen auf der Rules Seite in der Endpoint Security Web UI anzuzeigen.

Voraussetzungen

- Analyst, Senior Analyst, Investigator oder Admin Zugriff
- Ein Konto auf der Appliance, von der die Quellenwarnung stammt.

Um Informationen über Quellenwarnungen anzuzeigen:

1. Suchen Sie auf dem Indicators Register der Rules Seite nach den mit Quellenwarnungen verbundenen Indikatorregeln mit Hilfe einer der folgenden Methoden:
    - Sortieren Sie Indikatorregeln auf dem Indicators Register nach Kategorie (Benutzerdefiniert oder FireEye). FireEye Indikatorregeln sind die einzigen Indikatorregeln, die Quellenwarnungen erzeugen. Im Indicators Raster klicken Sie auf die **Category** Überschrift und dann auf den nach oben Pfeil.

      Die Indikatorregeln werden in alphabetischer Reihenfolge nach Kategorientyp neu organisiert und die FireEye Indikatorregeln sind zusammen gruppiert.
    - Sortieren Sie Indikatorregeln auf dem Indicators Register nach der Source Alerts Spalte. Klicken Sie auf die **Source Alerts** Überschrift in dem Raster und klicken Sie dann auf den nach unten Pfeil.

      Die Indikatorregeln mit der höchsten Anzahl von Quellenwarnungen werden am Anfang der Indikatorliste angezeigt.
    - Suchen Sie nach einer spezifischen Indikatorregel auf dem Indicators Register der Rules Seite, die eine Quellenwarnung erzeugt hat, wenn Sie ihren Namen oder bestimmte Bedingung kennen. Geben Sie relevante Informationen über den Indikator im **Search by name, created by, signature oder condition value** Feld über dem Raster ein und drücken Sie **Eingabe**.

      Nur Indikatorregeln, die den Suchbedingungen entsprechen, werden im Indicators Raster angezeigt.

2. Klicken Sie auf einen Indikator. Details über den Indikator werden in Detail Bereich angezeigt.
3. Informationen zu Indikatorbedingungen und Alarmen, die für diesen Indikator generiert wurden, finden Sie auf de Indicator Details im Detail Bereich.
4. Auf dem Source Alerts Register im Detail Bereich zeigen Sie die folgenden Informationen an:
    - Der Source Alert Detected Bereich enthält Zeitstempel für jeden mit diesem Indikator verbundenen Quellenalarm. Jeder dieser Zeitstempel ist ein Link. Klicken Sie auf den Link, um den Bericht des ursprünglichen Dienstes auf der FireEye Produktappliance anzuzeigen, die den zugehörigen Indikator generiert hat. Dieser Bericht liefert wichtige Informationen zur Unterstützung Ihrer Untersuchung.
    - Der Validated Bereich zeigt Ihnen, ob ein Agent eine Quellenwarnung bestätigt hat. Ein Häkchen in der **Validated** Spalte bedeutet:
        - Eine Quellenwarnung war mit der IP-Adresse eines Agent verbunden, als Endpoint Security die Warnung verarbeitet hat. Endpoint Security Agents bestätigen Übereinstimmungen für Quellenwarnungen auf Ihren Hosts, wenn Endpoint Security die Quellenwarnungen zuerst verarbeitet und wenn Agents zukünftige Aktivitäten überwachen.
        - Ein Agent hat auf seinem Host Beweise von Aktivitäten gefunden, die mit einer oder mehreren Bedingungen des Indikators übereinstimmen, der mit der Quellenwarnung verbunden ist.

Wenn viele Quellenwarnungen vorhanden sind, könnte dieses Register hinter dem Detail Register umbrechen und scheint zu verschwinden. Wenn dies der Fall ist, verkleinern oder vergrößern Sie die Breite des Browserfensters.

TEIL VI: Host Endpunkte eindämmen

KAPITEL 29: Überblick über Eindämmung

Die Endpoint Security Appliance Eindämmungsfunktion ermöglicht Ihnen, Host Endpunkte schnell zu isolieren und gibt Ihrem Unternehmen eine leistungsstarke Waffe zur Verhinderung weiterer Kompromittierung von Host-Endpunkt Systemen. Durch Eindämmung von Hosts wird ihr Zugriff auf und vom Netzwerkverkehr unterbrochen, mit Ausnahme der Kommunikation mit IP-Adressen, die Ihr Unternehmen für die Untersuchung und Beseitigung verwendet und für Netzwerkprotokolle, die für die Aufrechterhaltung der grundlegenden Netzwerkkonnektivität erforderlich sind. Zum Beispiel muss der Endpoint Security Agent immer mit Appliances kommunizieren können.

Die Administratoren Ihres Unternehmens können zusätzliche Kommunikation für eingedämmte Endpunkte zulassen und andere Eindämmungseinstellungen anpassen. Sie können festlegen, dass einige Hosts nicht eingedämmt werden dürfen, wählen, wie Host Endpoint Benutzer über eine Kompromittierung informiert werden sollen oder die Containment Funktion vollständig deaktivieren.

Eindämmung stoppt Angreifer schnell davon, Endpunkte zu kontrollieren und zu verwenden, aber es kann einen Angreifer auch warnen, so dass diese neue Ansätze versuchen. Darüber hinaus kann die Eindämmung eines Endpunkts möglicherweise unternehmenskritische Arbeiten stören.

Ein eingedämmter Host bleibt so lange eingedämmt, wie der Endpoint Security Agent installiert ist und auf dem Host-Endpunkt ausgeführt wird oder bis Sie den Host aus der Eindämmung entfernen. Wenn der Agent von einem eingedämmten Host heruntergefahren oder deinstalliert wird, ist der Host nicht länger eingedämmt.

Agent Upgrade Überlegungen für eingedämmte Hosts

FireEye empfiehlt, dass eingedämmte Hosts von Agent-Upgrades ausgeschlossen werden, weil der Upgradeprozess den Endpunkt vorübergehend nicht eindämmt. Der Aktualisierungsvorgang ermöglicht, dass ausgewählte Hostsätze von einem Upgrade ausgeschlossen werden.

Weitere Informationen finden Sie im *Endpoint Security Agent Administrationshandbuch*.

Eingedämmte Hosts in einer Proxy-Umgebung

Endpoint Security Version 4.6 oder später unterstützt Host-Eindämmung in einer Proxy-Umgebung. Mit Hilfe der Endpoint Security Web-UI können Sie kompromittierte Hosts eindämmen, die einen Proxy-Server für die Kommunikation mit dem Endpoint Security verwenden.

HINWEIS: Host-Eindämmung über Proxy-Support wird für Windows Endpunkte bereitgestellt, die Endpoint Security Agent Version 28 und später ausführen, für macOSS Endpunkte, die Endpoint Security Agent Version 30 und später ausführen und für Linux Endpunkte, die Endpoint Security Agent Version 34 und später ausführen.

Nachdem Sie Ihre Endpoint Security Agent Software auf Version 28 oder später aufgerüstet haben, werden Agent-Kommunikationen automatisch zur Containment-Whiteliste hinzugefügt. Auf diese Weise können Sie einen gefährdeten Host eindämmen und gleichzeitig die Kommunikation zwischen dem Agent und dem Server über den Proxyserver aufrechterhalten. Ihr eingedämmter Host kann nur mit dem Endpoint Security über den Proxy-Server kommunizieren. Alle anderen Kommunikationspfade sind deaktiviert.

Wenn Ihre Host-Endpunkte ein System-Proxy verwenden, dass zu der Containment-Whitelist hinzugefügt wurde, kann ein eingedämmter Host immer noch Web und anderen Verkehr senden und empfangen. Eindämmung funktioniert nicht, wenn Sie ein System-Proxy verwenden.

WICHTIG: Whitelisting funktioniert nur, wenn eine direkte Verbindung zwischen Ihrem Host-Endpunkt und einem verbundenen System besteht. Wenn Ihr eingedämmter Host mit anderen System über den Proxy-Server verbunden ist, können Sie die eingedämmte Host IP-Adresse nicht whitelisten.

Informationen über die Einstellung Ihres Proxy-Servers finden Sie im *Endpoint Security Agent Administrationshandbuch* und Informationen über die Eindämmung eines Windows Host in einer Proxy-Umgebung finden Sie unter Die Whitelist für eingedämmte Hosts verwalten auf Seite 161.

Eingedämmte Hosts auf VPNs

Um sicherzustellen, dass eingedämmte Hosts auf einer VPN-Verbindung weiterhin mit dem Endpoint Security kommunizieren, fügen Sie die IP-Adresse für Ihr VPN zu der Containment-Whiteliste hinzu. Wenn die VPN-IP-Adresse nicht auf der Whiteliste steht, könnten Endpoint Security Anfragen, einschließlich Anfragen zur Aufhebung der Eindämmung, den Host-Endpunkt nicht erreichen, weil die VPN-Verbindung nach der Eindämmung unterbrochen wird. Siehe Die Whitelist für eingedämmte Hosts verwalten auf Seite 161.

Agent Dateianforderung korrigieren

In Windows Umgebungen laden Sie die `.cms`-Datei für die Version des Agent auf dem Host-Endpunkt auf den Endpoint Security hoch. Die Datei muss auf der Agent Versions Seite der Endpoint Security Web-UI sichtbar sein.

Der Containment Treiber ist die Agent `.cms` Datei. Wenn Eindämmung eines Host-Endpunktes angefordert wird, aktualisiert der Endpoint Security die `.cms`Datei und sendet die Datei an den Endpunkt. Folglich kann der Host nicht eingedämmt werden, wenn auf dem Endpoint Security nicht die richtige `.cms`-Datei hochgeladen ist. Informationen über den Upload von `.cms`-Dateien auf den Endpoint Security finden Sie im *Endpoint Security Agent Deploymenthandbuch*.

In macOS Umgebungen ist dies nicht erforderlich, weil auf macOS Endpunkten der erforderliche Driver mit dem Agent installiert wurde.

KAPITEL 30: Der Eindämmungsprozess

Bevor der Endpoint Security einen Host eindämmt, muss eine Eindämmungsanfrage gestellt und dann von einem Administrator oder Investigator genehmigt werden. Der Endpoint Security bereitet dann einen Eindämmungsjob für den Agent mit den Anweisungen über die Eindämmung des Hosts vor. Der Endpoint Security Agent führt diese Anweisungen aus und meldet die Ergebnisse an den Endpoint Security.

Während des Eindämmungsprozesses durchlaufen Host-Endpunkte eine Reihe von Containment Status (oder Statusänderungen). Wo immer der Endpoint Security Hosts aufführt, werden Eindämmungs-Statussymbole für jeden Host angezeigt:

Statussymbol	Beschreibung
	Eindämmung angefordert
	Eindämmung genehmigt
	Eingedämmt
	Eindämmung fehlgeschlagen
	Eindämmung stoppen
	Eindämmungsabbruch fehlgeschlagen
	Nicht für Eindämmung geeignet.

Im Allgemeinen werden alle Endpoint Security-Aufgaben in der Reihenfolge der eingehenden Aufgaben verarbeitet. Eindämmungsaufgaben werden allerdings ausdrücklich als Aufgaben mit hoher Priorität markiert und kommen allen Datenerfassungsaufgaben, wie z.B. Enterprise Search und Datenerfassungsanfragen zuvor.

KAPITEL 31: Eindämmung verwalten

Sie können die Endpoint Security Web-UI verwenden, um die Eindämmung Ihrer Host-Endpunkte zu verwalten.

- Eindämmung anfordern
- Eine Eindämmungsanfrage abbrechen
- Eine Eindämmungsanfrage genehmigen
- Eindämmung mit Hilfe der Web-UI stoppen
- Eindämmung mit Hilfe eines Freischaltcodes stoppen auf Seite 432

Eindämmung anfordern

Sie können die Eindämmung für einen Host-Endpunkt über die Endpoint Security Web-UI von der Host Seite oder der Host Detail Seite anfordern. Der Endpunkt wird nicht durch Anforderung von Eindämmung eingedämmt. Die Anfrage muss zuerst von einem Administrator oder Investigator genehmigt werden. Siehe Eine Eindämmungsanfrage genehmigen.

Sie können auch die Eindämmung eines Host Endpunkts mit Hilfe der API anfordern, wenn Sie ein Userkonto haben, dem die **api-admin** Rolle zugewiesen ist. Wenn Sie die API-Methode verwenden, muss die Eindämmungsanfrage nicht genehmigt werden. Siehe Endpoint Security REST API-Handbuch.

Voraussetzungen

- Administrator, Investigator, Senior Analyst oder Analyst Web-UI Zugriff

Um die Eindämmung eines Host-Endpunktes von der Host Seite aus anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Klicken Sie auf das Auswahlfeld () links neben den Host Endpunkten, die Sie eindämmen möchten.
3. Auf dem **Actions** Menü wählen Sie **Request containment**.
4. Klicken Sie auf **Go**.

Sie können Eindämmung auch von den host alert details und host details Abschnitten der Hosts Seite anfordern.

Um Eindämmung eines Host-Endpunktes von der Host Details Seite aus anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Fordern Sie Host Details an, indem Sie auf das mit einem Host verbundene Erweiterungssymbol () klicken.
3. Am Anfang der Details Seite klicken Sie auf **Request containment**.

Nachdem Eindämmung angefordert wurde, wird der Containment Status des Host auf **Containment requested** verändert. Ein Eindämmung angefordert Symbol () wird neben dem Hostnamen auf jeder Seite angezeigt, auf der der Host aufgeführt ist. Der **Contained Hosts** Bereich auf dem Dashboard zeigt einen zusätzlichen Host in der Anzahl von Hosts an, für die Eindämmung angefordert wurde.

WICHTIG: Wenn Sie Eindämmung für mehr als einen Host zur gleichen Zeit anfordern und einer der Hosts ein **Ineligible for containment** Symbol () anzeigt, schlägt die Eindämmung für alle Hosts fehl.

Eine Eindämmungsanfrage abbrechen

Sie können eine Eindämmungsanfrage für einen Host-Endpunkt jederzeit abbrechen.

Nachdem die Eindämmungsanfrage abgebrochen wurde, werden keine weiteren Eindämmungsaktionen für den Endpunkt zugelassen, bis sein Agent erneut bei der HX Appliance eingecheckt hat und die Abbruchaufgabe abgeschlossen ist.

Voraussetzungen

- Administrator, Investigator, Senior Analyst oder Analyst Zugriff
- Eine Eindämmunganfrage läuft noch. Siehe Eindämmung anfordern.

Um eine Eindämmungsanfrage abzubrechen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie das Kontrollkästchen links neben einem Host Endpunkt für den Eindämmung beantragt, aber nicht genehmigt wurde.
3. Wählen Sie **Cancel containment request** auf dem **Actions** Menü.
4. Klicken Sie auf **Go**.

Sie können Eindämmung auch von den host alert details und host details Abschnitten der Hosts Seite abbrechen.

Um Eindämmung eines Host Endpunkts von den host alert details oder host details Abschnitten abzubrechen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Fordern Sie Host Details an, indem Sie auf das mit einem Host verbundene Erweiterungssymbol () klicken.
3. Am Anfang der Details Seite klicken Sie auf **Cancel containment request**.

Nachdem Sie eine Eindämmunganfrage für einen Host abgebrochen haben, wird der Status des Host auf **Stopping containment** geändert.

Wenn der Abbruch erfolgreich ist, werden alle Eindämmungssymbole neben dem Hostnamen entfernt. Der **Contained Hosts** Bereich auf dem Dashboard zeigt einen Host weniger in der Anzahl der Hosts an, deren Eindämmung angefordert wurden.

Wenn der Abbruch für einen Host fehlschlägt, wechselt sein Containment Status auf **Containment cancellation failed**. Das Symbol für den fehlgeschlagenen Eindämmungsabbruch wird neben dem Hostnamen auf jeder Seite angezeigt, auf der der Host aufgeführt ist.

Eine Eindämmungsanfrage genehmigen

Um einen Host Endpunkt einzudämmen, müssen Sie seine Eindämmungsanfrage genehmigen.

Wenn Sie Eindämmung eines Host Endpunkts mit Hilfe der API anfordern, ist keine Genehmigung erforderlich. Siehe Endpoint Security REST API-Handbuch.

Voraussetzungen

- Administrator oder Investigator Zugriff
- Eine Eindämmungsanfrage muss zuerst gemacht werden. Siehe Eindämmung anfordern.

Um eine Eindämmungsanfrage zu genehmigen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie das Kontrollkästchen links neben einem Host Endpunkt für den Eindämmung beantragt, aber nicht genehmigt wurde.
3. Wählen Sie **Contain** auf dem **Actions** Menü.
4. Klicken Sie auf **Go**.

Sie können Eindämmung auch von den Host Alert Details und Host Details Abschnitten auf der Hosts Seite genehmigen.

Um eine Eindämmungsanfrage für einen Host-Endpunkt von den Host Alert Details oder Host Details Abschnitten zu genehmigen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Fordern Sie Host Details an, indem Sie auf das mit einem Host verbundene Erweiterungssymbol () klicken.
3. Am Anfang der Details Seite klicken Sie auf **Contain**.

Nachdem die Containment Anfrage genehmigt wurde, wird der Containment Status des Host Endpunkts auf **Containment approved** geändert. Ein Eindämmung genehmigt Symbol () wird neben dem Hostnamen auf jeder Seite angezeigt, auf der der Host aufgeführt ist.

Wenn Containment für den Host erfolgreich ist, wird sein Containment Status auf **Contained** geändert. Eine Eindämmungssymbol () wird neben dem Hostnamen auf jeder Seite angezeigt, auf dem der Host aufgeführt ist. Der **Contained Hosts** Bereich auf dem Dashboard zeigt einen zusätzlichen Host in der Anzahl der Hosts an, die eingedämmt wurden.

Wenn Eindämmung für den Host fehlschlägt, wird sein Containment Status auf **Containment failed** geändert. Das Eindämmung fehlgeschlagen Symbol wird neben dem Host auf jeder Seite angezeigt, auf der der Host aufgeführt ist. Der **Contained Hosts** Bereich auf dem Dashboard zeigt einen zusätzlichen Host in der Anzahl der Hosts an, für die Eindämmung fehlgeschlagen ist.

Eindämmung mit Hilfe der Web-UI stoppen

Endpoint Security ermöglicht Ihnen, einen Host mit Hilfe der Endpoint Security Web-UI von der Eindämmung zu entfernen.

Voraussetzungen

- Administrator oder Investigator Zugriff
- Ein Host Endpunkt ist eingedämmt. Siehe Eine Eindämmungsanfrage genehmigen.

Um Eindämmung eines eingedämmten Hosts zu stoppen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie das Kontrollkästchen auf der linken Seite eines Host Endpunkts, der eingedämmt ist.
3. Wählen Sie **Stop containment** auf dem **Actions** Menü.
4. Klicken Sie auf **Go**.

Sie können Eindämmung auf von den host alert details und host details Abschnitten auf der Hosts Seite stoppen.

Um Eindämmung eines Host Endpunkts von den host alert details oder host details Abschnitten zu stoppen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Fordern Sie Host Details an, indem Sie auf das mit einem Host verbundene Erweiterungssymbol (⊕) klicken.
3. Klicken Sie am Anfang der Details Seite auf **Stop containment**.

Nachdem der Stop der Eindämmung für einen Host angefordert ist, wird sein Status auf **Stopping containment** geändert. Das Eindämmung abbrechen Symbol (🔒) wird neben dem Hostnamen auf jeder Seite angezeigt, auf der der Host ausgeführt ist.

Wenn die Eindämmung erfolgreich beendet wird, werden alle Eindämmungssymbole neben dem Hostnamen entfernt. Der **Contained** Hosts Bereich auf dem Dashboard zeigt einen Host weniger in der Anzahl der Hosts an, die eingedämmt wurden.

Wenn Eindämmung für einen Host nicht erfolgreich gestoppt wird, wird der Containment Status auf **Containment cancellation failed** geändert. Das Symbol für den fehlgeschlagenen Eindämmungsabbruch wird neben dem Hostnamen auf jeder Seite angezeigt, auf der der Host aufgeführt ist.

Wenn Eindämmung für einen Windows Endpunkt gestoppt wird, werden die Benachrichtigungsdateien, die mit der ursprünglichen Eindämmung auf dem Endpunkt verbunden sind, gelöscht. Wenn die Eindämmung allerdings für einen macOS Endpunkt gestoppt wird, werden die Benachrichtigungsdateien, die mit der ursprünglichen Eindämmung des Endpunkts verbunden sind, beibehalten.

Eindämmung mit Hilfe eines Freischaltcodes stoppen

Wenn Sie einen Windows Host eindämmen, der Endpoint Security Agent Version 28 oder später ausführt oder einen macOS Host, der Endpoint Security Agent Version 30 oder später ausführt oder einen Linux Host, der Endpoint Security Agent Version 34 oder später ausführt, wird ein Eindämmungs-Freischaltcode vom Endpoint Security generiert. Wenn Ihr Endpoint Security Agent nicht mit dem Endpoint Security kommunizieren kann, können Sie den Freischaltcode verwenden, um den Host aus der Eindämmung zu entfernen.

Wenn die Eindämmungs-Freischaltcode-Funktion aktiviert ist, kann Ihr Systemadministrator den Freischaltcode von der Endpoint Security Web-UI Host Details Seite anfordern oder eine API-Anfrage verwenden und dem lokalen User bereitstellen. Der lokale User kann FireEyes uncontain ausführbare Datei mit dem Freischaltcode auf der Windows, macOS oder Linux Eingabeaufforderung ausführen, um die Eindämmung des Host-Systems zu stoppen.

WICHTIG: Die Eindämmungs-Freischaltcode-Funktion muss aktiviert sein, damit Ihr Systemadministrator den Freischaltcode für einen eingedämmten Host mit Hilfe der Web-UI oder einer API-Anfrage anfordern kann.

Jeder Endpoint Security Agent besitzt einen eindeutigen Freischaltcode, bei dem es sich um eine zufällige Zeichenfolge von alphanumerischen Zeichen handelt.

Voraussetzungen

- Administratorzugriff
- Ein Host-Endpunkt wird eingedämmt und kann nicht mit Endpoint Security kommunizieren. Siehe Eine Eindämmungsanfrage genehmigen.

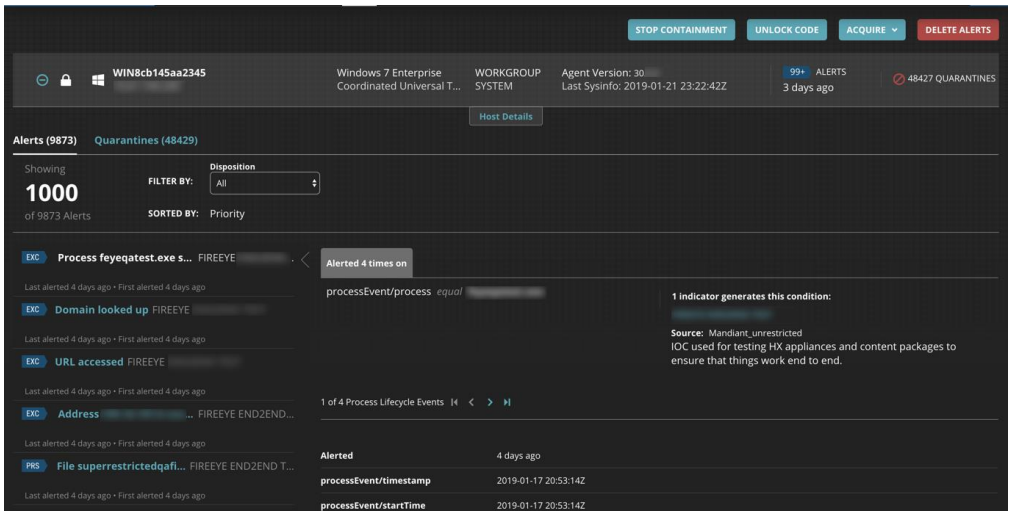
Dieser Abschnitt behandelt die folgenden Themen:

Einen Eindämmungs-Freischaltcode anfordern

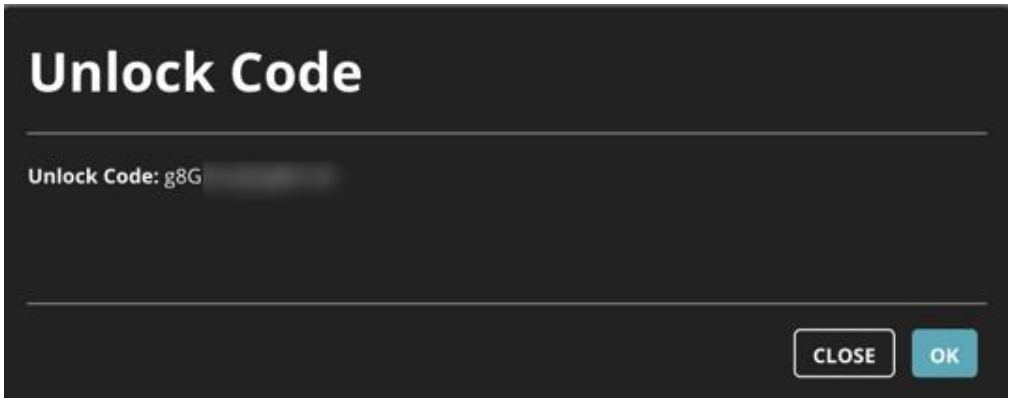
Sie können einen Freischaltcode für Ihren eingedämmten Windows, MacOS oder Linux Host mit Hilfe der Host Details Seite oder einer API-Anfrage beantragen.

Um einen Freischaltcode für einen eingedämmten Host mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Klicken Sie auf das mit dem eingedämmten Host verbundene Erweitern Symbol ( ).
3. Am Anfang der **Host Details** Seite klicken Sie auf die **Unlock Code** Schaltfläche.



4. Wenn das **Unlock Code** Dialogfeld angezeigt wird, kopieren Sie den mit dem eingedämmten Host verbundenen Freischaltcode.



5. Klicken Sie auf **OK**.

Um einen Freischaltcode für einen eingedämmten Host mit Hilfe einer API anzufordern, verwenden Sie die folgende Anfrage.

GET https://{{address}}:3000/hx/api/v3/hosts/:<agentid>/containment/unlock_codes

Einen Freischaltcode verwenden, um die Eindämmung eines Window Host zu beenden

In diesem Abschnitt wird die Verwendung des Freischaltcodes für die Beendigung der Eindämmung Ihres Windows Host beschrieben.

Um einen Freischaltcode zu verwenden, um einen Windows Host von der Eindämmung zu entfernen:

1. Melden Sie sich auf dem eingedämmten Windows Host an.
2. Öffnen Sie die Eingabeaufforderung und verwenden Sie die `cd` Befehl, um auf das `C:\Windows\FireEye` Verzeichnis zu wechseln:
   ```
   cd C:\Windows\FireEye
   ```
3. Führen Sie die `uncontain` ausführbare Datei mit dem Freischaltcode aus:
   ```
   uncontain.exe <unlock code>
   ```

Einen Freischaltcode verwenden, um die Eindämmung eines macOS Host zu beenden

In diesem Abschnitt wird die Verwendung des Freischaltcodes für die Beendigung der Eindämmung Ihres macOS Host beschrieben.

Um einen Freischaltcode für die Entfernung eines macOS Host von der Eindämmung zu verwenden:

1. Melden Sie sich auf dem eingedämmten macOS Host an.
2. Öffnen Sie die Eingabeaufforderung und verwenden Sie den `cd` Befehl, um das `/Library/FireEye/xagt/xagt.app/Contents/MacOS/bin` Verzeichnis für Agent Version 31 und früher oder das `/Library/FireEye/xagt/xagt.app/Contents/MacOS` Verzeichnis für Agent Version 32 und höher zu ändern:
   ```
   cd /Library/FireEye/xagt/xagt.app/Contents/MacOS/bin
   ```
3. Führen Sie die `uncontain` ausführbare Datei mit dem Freischaltcode aus:
   ```
   ./uncontain <unlock code>
   ```

Einen Freischaltcode verwenden, um die Eindämmung eines Linux Host zu beenden

In diesem Abschnitt wird die Verwendung des Freischaltcodes für die Beendigung der Eindämmung Ihres Linux Host beschrieben.

Um einen Freischaltcode für die Entfernung eines Linux Host von der Eindämmung zu verwenden:

1. Melden Sie sich als Root-Benutzer auf dem eingedämmten Linux Host an.
2. Auf der Eingabeaufforderung verwenden Sie den `cd` Befehl, um das `/opt/fireeye/bin/uncontain` Verzeichnis zu ändern.
   ```
   cd /opt/fireeye/bin/uncontain
   ```
3. Führen Sie die `uncontain` ausführbare Datei mit dem Freischaltcode aus:
   ```
   ./uncontain <unlock code>
   ```

TEIL VII: Module verwalten

Dieser Abschnitt enthält die folgenden Informationen:

KAPITEL 32: Module verwenden

Sie können die Modules Seite in der Endpoint Security Web-UI verwenden, um Ihre Module zu verwalten.

Überblick über Module

Module sind zusätzliche Fähigkeiten, die Sie zu Ihrer Endpoint Security Web-UI hinzufügen können und direkt an einen zugewiesenen Hostsatz senden können. Wenn Sie ein Modul installieren, werden neue Richtlinien zu Endpoint Security hinzugefügt. Wenn ein Modul Erkennungsfähigkeiten liefert, werden die Ergebnisse in Ihrer vorhandenen Workflow angezeigt.

Einige Module, die *System Modules* genannt werden, sind im Endpoint Security Produkt enthalten und standardmäßig aktiviert. Zusätzliche Module können direkt von der DTI mit Hilfe des Additional Modules Tabs installiert werden oder Sie können auf die Find Modules Schaltfläche klicken, um auf den FireEye Market zuzugreifen, wo Sie die Konfigurationsdatei für ein Modul herunterladen und dann auf Ihre Endpoint Security Web-UI hochladen können.

Jedes der auf dem FireEye Market verfügbare Modul verfügt über eine eigene Bedienungsanleitung, die ebenfalls von der gleichen FireEye Market Seite wie das Modul heruntergeladen werden kann. Normalerweise sind Module zunächst auf einer Tech Preview Basis verfügbar. In nachfolgenden Versionen werden diese Module dann für General Availability (allgemeine Verfügbarkeit) angeboten.

Nachdem Sie ein Modul installiert und aktiviert haben, wird es im Modules Menü der Web-UI angezeigt. Sie haben direkten Zugriff auf ein Modul indem Sie das Modules Menü oder auf Endpoint Module Administration klicken.

Endpoint Module Administration ist eine Benutzerschnittstelle (UI), auf der Sie alle Aspekte Ihrer Module verwalten können. Sie bietet Zugriff auf die Modules Seite, die separate Tabs für System Modules, Installed Modules und Available Modules enthält. Sie können die Modules Seite verwenden, um eine Liste aller, auf Ihrer Web-UI installierten Module anzuzeigen, zusätzliche Module zu installieren oder deinstallieren, Module zu aktivieren oder deaktivieren, Module zu aktualisieren, wenn eine neue Version verfügbar wird, ein Modul als Ihr Dashboard einzustellen und auf die Web-UI Seiten für die individuellen, auf der Seite aufgeführten Module zuzugreifen.

HINWEIS: Sie können Systemmodule nicht deaktivieren oder deinstallieren.

Module installieren oder deinstallieren

Sie können ein Modul auf Ihrer Endpoint Security Web-UI entweder vom FireEye Market installieren oder Sie können den Additional Modules Tab für die Installation eines Moduls vom Modulkatalog verwenden, der auf FireEyes DTI-Inhaltsserver gehostet wird. Die Module, die Sie installieren, sind standardmäßig deaktiviert. Vor der Benutzung muss jedes Modul aktiviert werden. Nachdem Sie ein Modul installiert und aktiviert haben, wird das Modul auf dem Modules Menü angezeigt.

Ein Modul über das Additional Modules Tab installieren

Um ein Modul über den Additional Modules Tab auf die Endpoint Security Web-UI zu installieren:

1. Melden Sie sich auf der Endpoint Security Web-UI mit Ihren Administrator Berechtigungen an.
2. Vom **Modules** Menü wählen Sie **Endpoint Module Administration**, um auf die **Modules** Seite zuzugreifen.
3. Klicken Sie auf der Modules Seite auf den **Additional Modules** Tab.
4. Klicken Sie im Actions Menü auf **Install** für das Modul, das Sie installieren möchten.
5. Klicken Sie im Bestätigungsdialogfeld auf **Install**.

   Die Installed Modules Seite wird angezeigt und eine Bannernachricht informiert Sie darüber, dass der Installationsprozess für das Modul begonnen hat. Wenn der Installationsvorgang abgeschlossen ist, werden Sie durch eine Bannernachricht darüber informiert, dass das Modul installiert ist und das Datum und die Uhrzeit der Installation wird in der Installation Date Spalte für das Modul angezeigt.

Ein Modul aus dem FireEye Market installieren

Um ein Modul aus dem FireEye Market zu installieren, führen Sie die folgenden Aufgaben aus:

- Laden Sie das Module Installer Package vom FireEye Market herunter.
- Laden Sie das Module Installer Package auf die Endpoint Security Web-UI hoch.
- Wenn das Modul über eine Agent-bezogene Komponente verfügt, fügen Sie diese zu der Agent Richtlinie hinzu.

Das Module Installer Package herunterladen

Um das Module Installer Package vom FireEye Market herunterladen:

1. Melden Sie sich auf der Endpoint Security Web-UI mit Ihren Administrator Berechtigungen an.
2. Vom **Modules** Menü wählen Sie **Endpoint Module Administration**, um auf die **Modules** Seite zuzugreifen.
3. Klicken Sie auf der Modules Seite auf **Find Modules**, um auf den FireEye Market zuzugreifen.

   Der FireEye Market wird auf einem neuen Browsertab geöffnet.
4. Auf der Types Filterliste auf dem FireEye Market wählen Sie **Endpoint Security Modules**.
5. Klicken Sie in den Suchergebnissen auf das Modul, das Sie installieren wollen.
6. Klicken Sie auf der FireEye Market Seite für das ausgewählte Modul auf **Download**, um die Modul .cms Datei auf Ihr lokales Laufwerk herunterzuladen.

   Notieren Sie sich den Navigationspfad auf das Verzeichnis, auf dem Sie die .cms Datei heruntergeladen haben.

Das Module Installer Package hochladen

Um das Module Installer Package auf Ihre Endpoint Security Web-UI hochzuladen:

1. Melden Sie auf der Endpoint Security Web-UI mit Ihren Administrator-Anmeldeinformationen an.
2. Vom **Modules** Menü wählen Sie **Endpoint Module Administration**, um auf die **Modules** Seite zuzugreifen.
3. Klicken Sie auf der Modules Seite auf **Install Modules**.
4. Klicken Sie im Upload Module Dialogfeld auf **Select File**.

5. Navigieren Sie auf die heruntergeladene Module .cms Datei, wählen Sie diese aus und klicken auf **Open**.

   Die ausgewählte .cms Datei wird im Upload Module Dialogfeld angezeigt.

6. Klicken Sie im Upload Module Dialogfeld auf **Upload**.

   Eine Nachricht am Anfang der Seite teilt Ihnen mit, dass die Installation des Moduls eingeleitet wurde. Wenn der Installationsvorgang abgeschlossen ist, erhalten Sie eine Bestätigung, dass das Modul installiert wurde und in der State Spalte für das Modul wird Installed angezeigt.

   Wenn bei der Installation ein Problem auftritt, zeigt die State Spalte für das Modul Failed an und Sie können weitere Informationen über den Fehler in der Status Information Spalte für das Modul finden.

Nachdem Sie ein Modul installiert haben, wird das Modul auf der Modulliste auf der installed Modules Seite angezeigt. Möglicherweise müssen Sie die Endpoint Security Web-UI aktualisieren, bevor das neue Modul auf der Installed Modules Seite angezeigt wird.

Ein Modul zu der Agent Richtlinie hinzufügen

Um ein Modul zu Ihrer Agent Richtlinie hinzuzufügen:

1. Melden Sie sich auf der Endpoint Security Web-UI als ein Administrator an.
2. Auf dem **Admin** Menü wählen Sie **Policies**, um die Policies Seite aufzurufen.
3. Klicken Sie auf der Policies Seite auf das **Actions** Symbol für die Richtlinie des Agent, auf dem Sie das Modul aktivieren wollen, und wählen Sie **Edit Policy**.
4. Im Configurations Abschnitt der Edit Policy Seite wählen Sie das Modul oder die Module, die Sie zu Ihrer Agent Richtlinie hinzufügen wollen.
5. Schalten Sie den Enable Selektor auf **ON**, um das Modul für die Agent Richtlinie zu aktivieren.
6. Klicken Sie auf der Edit Policy Seite auf **Save**.

HINWEIS: Einige Module enthalten zusätzliche Konfigurationsfelder für Ihre Agent Komponente. Weitere Informationen über diese Felder finden Sie in der Bedienungsanleitung für das Modul.

Module aktivieren oder deaktivieren

Nachdem Sie ein Modul installiert haben, muss es aktiviert werden, bevor Sie die vom Modul bereitgestellten Funktionen nutzen können. Die folgende Ausgabe triff nur auf Module zu, die Sie installieren. Systemmodule werden standardmäßig aktiviert und können nicht von Ihnen deaktiviert werden.

Um ein auf der Installed Modules Seite angezeigtes Modul zu aktivieren oder deaktivieren.

1. Melden Sie auf der Endpoint Security Web-UI mit Ihren Administrator-Anmeldeinformationen an.
2. Vom **Modules** Menü wählen Sie **Endpoint Module Administration**, um auf die **Modules** Seite zuzugreifen.
3. Klicken Sie auf der Modules Seite auf den **Installed Modules** Tab.
4. Klicken Sie in der Modulliste auf das **Actions** Symbol für das Modul und wählen Sie **Enable** oder **Disable**.
5. Klicken Sie in dem Bestätigungsdialogfeld auf **Enable** oder **Disable**.

   Eine Nachricht am Anfang der Seite bestätigt, dass das Modul aktiviert oder deaktiviert wurde und die Status Spalte wird aktualisiert, um Enabled oder Disabled (Aktiviert oder Deaktiviert) anzuzeigen.

   HINWEIS: Wenn das Modul über eine Agent Komponente verfügt, müssen Sie diese Agent Komponente auch in der Agent Richtlinie aktivieren, bevor Sie die Funktionalität nutzen können.

Module aufrüsten

Sie können die System Modules oder Installed Modules Seiten in Endpoint Module Administration verwenden, um die Module aufzurüsten, die Sie auf Ihrer Endpoint Security Web-UI installiert haben.

Um ein Modul zu aktualisieren, muss eine Version des Moduls bereits auf Ihrer Endpoint Security Web-UI installiert sein und die Versionsnummer des installierten Moduls muss geringer als die Versionsnummer des Moduls sein, auf das Sie aktualisieren wollen. Wenn Sie auf eine neuere Version eines Moduls aufrüsten, werden die Status- (Enabled oder Disabled) und Konfigurationseinstellungen des aktuell installierten Moduls gesichert und in der aufgerüsteten Version wiederhergestellt.

Sie werden darauf hingewiesen, dass in der Up to Date Spalte auf den System Modules und Installed Modules Seiten eine neuere Version eines Moduls verfügbar ist. Wenn eine neuere Version eines Moduls verfügbar ist, wird das Upgrade Available Symbol in der Up to Date Spalte angezeigt. Wenn Aktualisierungen verfügbar sind, wird neben jedem Tab auf der Modules Seite ein nummeriertes Symbol angezeigt. Die in dem Symbol angezeigte Zahl stellt die Anzahl der Module auf diesem Tab dar, für die eine neuere Version verfügbar ist.

Um ein Modul aufzurüsten:

1. Melden Sie auf der Endpoint Security Web-UI mit Ihren Administrator-Anmeldeinformationen an.

2. Vom **Modules** Menü wählen Sie **Endpoint Module Administration**, um auf die **Modules** Seite zuzugreifen.
3. Klicken Sie auf der Modules Seite auf **Find Modules**, um auf den FireEye Market zu navigieren.
4. Im FireEye Market suchen Sie nach und wählen Sie das Modul, das Sie aktualisieren wollen.
5. Klicken Sie auf der ausgewählten Modulseite im FireEye Market auf **Download** und bestimmten Sie den Download-Speicherort für die .cms Datei.

   Die .cms Datei für das ausgewählte Module wird auf das von Ihnen festgelegte Verzeichnis heruntergeladen.
6. Wählen Sie **System Modules** oder **Installed Modules** auf der Modules Seite, je nach dem Typ des Moduls, das Sie aktualisieren.
7. Klicken Sie auf das **Actions** Symbol für das Modul, das Sie aktualisieren wollen und klicken Sie auf **Upgrade**.
8. Klicken Sie im **Upgrade Module** Dialogfeld auf **Select File**.
9. Wählen Sie die .cms Datei und klicken Sie auf **Open**.

   Die ausgewählte .cms Datei wird im Upgrade Module Dialogfeld angezeigt.
10. Klicken Sie im Upgrade Module Dialogfeld auf **Upgrade**.

    Eine Nachricht am Anfang der Seite zeigt an, ob die Aktualisierung erfolgreich war. Sie können das Upgrade verifizieren, indem Sie die Versionsnummer des Moduls in der Version Spalte auf der Modules Seite überprüfen und die Up to Date Spalte zeigt an, dass das Module auf dem neuesten Stand ist.

Ein Modul als Ihr Dashboard anzeigen

Sie können die Modules Seite verwenden, um Ihre Dashboard Seite zu konfigurieren, die Moduldaten anzuzeigen.

Die Dashboard Seite zeigt weiterhin die ausgewählten Modulinformationen an, bis Sie entweder ein anderes Modul als Ihre Dashboard Seite anzeigen, auf die Standard Dashboard Seite zurückfallen oder das Modul deaktivieren.

Ein Modul als Ihr Dashboard anzeigen

Um ein Modul als Ihr Dashboard anzuzeigen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Vom Modules Menü wählen Sie **Endpoint Module Administration**, um auf die **Modules** Seite zuzugreifen.
3. Klicken Sie auf der Modulliste auf der System Modules oder der Installed Modules Seite auf das **Actions** Symbol für das gewünschte Modul und wählen Sie **Set as Dashboard**.

   Ihr Dashboard zeigt die ausgewählte Modulseite an und am Anfange der Web-UI Seite wird Plugin Powered Dashboard angezeigt.

Auf das Standard Dashboard zurückfallen

Um auf die Standard Dashboard Seite zurückzufallen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Vom Modules Menü wählen Sie **Endpoint Module Administration**, um auf die **Modules** Seite zuzugreifen.
3. Klicken Sie auf der Modulliste auf der Modules Seite auf das **Actions** Symbol für das Modul, das als Ihr Dashboard eingestellt ist und wählen Sie **Undo as Dashboard**.

   Ihr Dashboard kehrt auf die Anzeige der Standard Dashboardinformationen zurück.

KAPITEL 33: Modulseiten anpassen

In diesem Abschnitt wird die Anpassung Ihrer Modulseiten beschrieben.

Spalten ein- und ausblenden

Jede Modulseite enthält eine Anzahl von Spalten, die standardmäßig nicht angezeigt werden. Sie können auswählen, welche Spalten auf einer Modulseite angezeigt oder ausgeblendet werden sollen.

Spalten auf einer Modulseite anzeigen

Um zusätzliche Spalten auf einer Modulseite anzuzeigen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Modules** Menü wählen Sie das Modul, für das Sie zusätzliche Spalten anzeigen wollen.
3. Klicken Sie auf der ausgewählten Modulseite auf das **Toggle_Columns** Tool.
4. Wählen Sie das Kontrollkästchen für die Spalten, die Sie auf der Modulseite anzeigen wollen, im **Columns** Dialogfeld.

   Die ausgewählten Spalten werden auf der Modulseite angezeigt.

Sie können zur Standardansicht zurückkehren, indem Sie im **Columns** Dialogfeld auf **Restore Defaults** klicken.

WICHTIG: Durch Klicken auf **Restore Defaults** werden alle Änderungen zurückgesetzt, die Sie auf der Modulseite vorgenommen haben.

Spalten auf einer Modulseite ausblenden

Um Spalten auf einer Modulseite auszublenden:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Modules** Menü wählen Sie das Modul, für das Sie Spalten ausblenden wollen.
3. Klicken Sie auf der ausgewählten Modulseite auf das **Toggle_Columns** Tool.
4. Im **Columns** Dialogfeld wählen Sie die Spalten, die Sie ausblenden wollen.

   Die ausgewählten Spalten werden nicht länger auf der Modulseite angezeigt.

Sie können zur Standardansicht zurückkehren, indem Sie im **Columns** Dialogfeld auf **Restore Defaults** klicken.

WICHTIG: Durch Klicken auf **Restore Defaults** werden alle Änderungen zurückgesetzt, die Sie auf der Modulseite vorgenommen haben.

Spalten neu anordnen

Wenn Sie die auf einer Modulseite angezeigten Daten lieber in einer anderen Reihenfolge anzeigen möchten, können Sie die Reihenfolge der Spalten ändern.

Um Spalten auf einer Modulseite neu anzuordnen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Modules** Menü wählen Sie das Modul, für das Sie Spalten neu anordnen wollen.
3. Klicken Sie auf der ausgewählten Modulseite auf das **Toggle_Columns** Tool.
4. Ziehen Sie den Spaltennamen der Spalte, die Sie verschieben wollen, im **Columns** Dialogfeld auf die gewünschte neue Position.

   Die ausgewählte Spalte wird auf die neue Position auf der Modulseite verschoben.
5. Wiederholen Sie den vorherigen Schritt für jede Spalte, die Sie verschieben wollen, bis die auf der Moduleseite angezeigten Spalten in der gewünschten Reihenfolge erscheinen.

Sie können zur Standardansicht zurückkehren, indem Sie im **Columns** Dialogfeld auf **Restore Defaults** klicken.

WICHTIG: Durch Klicken auf **Restore Defaults** werden alle Änderungen zurückgesetzt, die Sie auf der Modulseite vorgenommen haben.

KAPITEL 34: Filtersätze verwalten

Filtersätze ermöglichen Ihnen, eine gefilterte Ansicht der Informationen auf einer Modulseite zu erfassen und zu speichern. Auf den Modulseiten können Sie Filtersätze erstellen, die Sichtbarkeitsstufe für Filtersätze ändern, Filtersätze exportieren und importieren sowie Filtersätze löschen.

Dieser Abschnitt enthält die folgenden Themen:

Filtersätze erstellen

Sie können Filtersätze erstellen, um nur gewünschten Informationen anzuzeigen.

Um einen Filtersatz zu erstellen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Vom **Modules** Menü wählen Sie das Modul mit den Daten, die Sie filtern wollen.
3. Auf der ausgewählten Modulseite verwenden Sie die Spaltenfilter, um die Daten einzugrenzen, bis nur die gewünschten Informationen auf der Seite angezeigt werden.
4. Klicken Sie auf der Modulseite auf das **Manage Filter Sets** Tool und klicken Sie auf **Save New Filter Set**.
5. Geben Sie einen Namen für den Filtersatz, den Sie erstellen, im **Save New Filter Set** Dialogfeld ein und wählen Sie die Sichtbarkeitsebene für den Filtersatz aus. Die Standard Sichtbarkeitsebene ist **Private**.
6. Klicken Sie im **Save New Filter Set** Dialogfeld auf **Save**.

Die Sichtbarkeit des Filtersatzes ändern

Sie können die Sichtbarkeitsebene jedes Filtersatzes ändern, den Sie auf einer Modulseite erstellt haben.

Um die Sichtbarkeitsstufe eines Filtersatzes zu ändern:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Auf dem **Modules** Menü wählen Sie das Modul mit den Daten, mit denen Sie den gewünschten Filtersatz erstellt haben.
3. Klicken Sie auf der Modulseite auf das **Manage Filter Sets** Tool.
4. In der **Filter Sets** Dropdown-Liste finden Sie Ihren Filtersatz.
5. Klicken Sie in der **Filter Sets** Dropdown-Liste auf das **Edit Filter Set** Symbol für den Filtersatz.
6. Im **Edit Filter Set** Dialogfeld ändern Sie die Sichtbarkeitsstufe für den Filtersatz.
7. Klicken Sie im **Edit Filter Set** Dialogfeld auf **Save**.

Filtersätze exportieren und importieren

Sie können die Modul Seiten verwenden, um vorhandene Filtersätze zu exportieren und neue Filtersätze zu importieren.

Filtersätze exportieren

Um Filtersätze zu exportieren:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie das Modul, für das Sie Filtersatzdaten exportieren wollen vom **Modules** Menü.
3. Klicken Sie auf der Modulseite auf das **Manage Filter Sets** Tool.
4. Klicken Sie in der **Filter Sets** Dropdown Liste auf **Export Filter Sets**.

Eine filtersets.json Datei wird auf das Verzeichnis exportiert, das Sie als Ihr Standardverzeichnis für Downloads verwenden.

Filtersätze importieren

Um einen vorhandenen Filtersatz zu importieren:

1. Öffnen Sie die neue filtersets.json Datei und kopieren Sie den Inhalt.
2. Melden Sie sich auf der Endpoint Security Web-UI an.
3. Wählen Sie das Modul, für das Sie Filtersatzdaten importieren wollen, vom **Modules** Menü.
4. Klicken Sie auf der Modulseite auf das **Manage Filter Sets** Tool.
5. Klicken Sie in der **Filter Sets** Dropdown Liste auf **Import Filter Sets**.
6. Fügen Sie den Inhalt der filtersets.json Datei in das bereitgestellte Feld im **Import Filter Sets** Dialogfeld ein.
7. Klicken Sie im **Import Filter Sets** Dialogfeld auf **Import**.

Filtersätze löschen

Sie können jeden der Filtersätze löschen, den Sie auf einer Modulseite erstellt haben.

Um einen Filtersatz zu löschen:

1. Melden Sie sich auf der Endpoint Security Web-UI an.
2. Wählen Sie das Modul, das die Daten für den von Ihnen erstellten Filtersatz liefert vom **Modules** Menü.
3. Auf der Modules Seite klicken Sie auf das **Manage Filter Sets** Tool und finden Sie Ihren Filtersatz in der **Filter Sets** Dropdown-Liste.
4. Klicken Sie in der **Filter Sets** Dropdown-Liste auf das **Delete Filter Set** Symbol für den Filtersatz, den Sie löschen wollen.
5. Klicken Sie im **Delete Filter Set** Dialogfeld auf **Delete**.

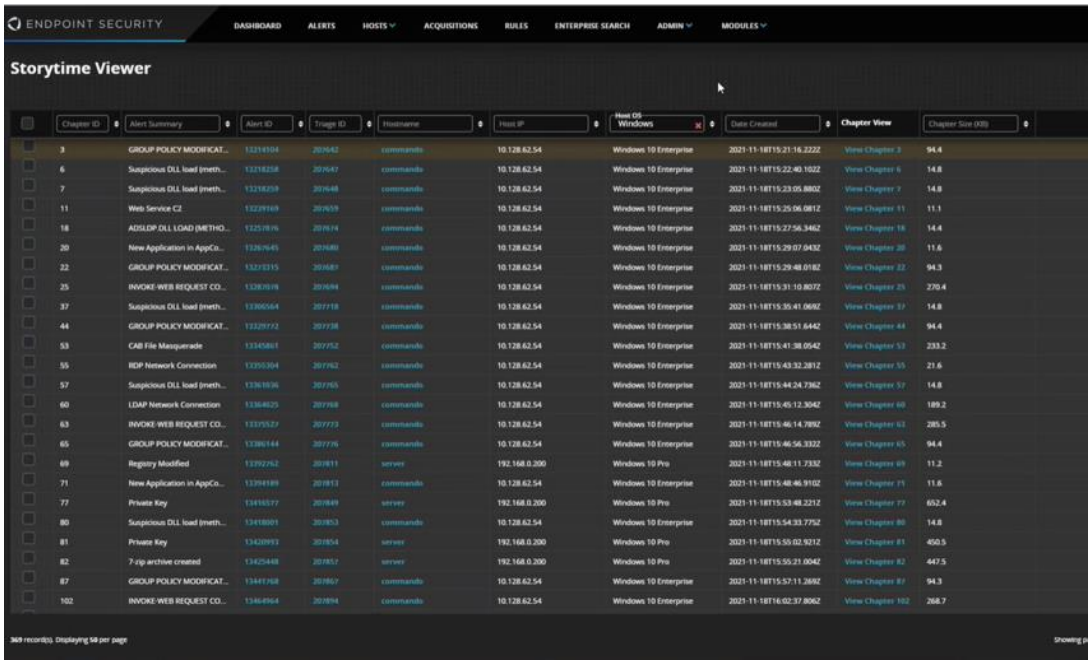
.

KAPITEL 35: Systemmodule

Systemmodule sind automatisch auf dem Endpoint Security Produkt installiert und aktiviert und können nicht deinstalliert werden. Sie können sie genauso wie Usermodule aktualisieren. Weitere Informationen finden Sie unter Module aufrüsten auf Seite 443.

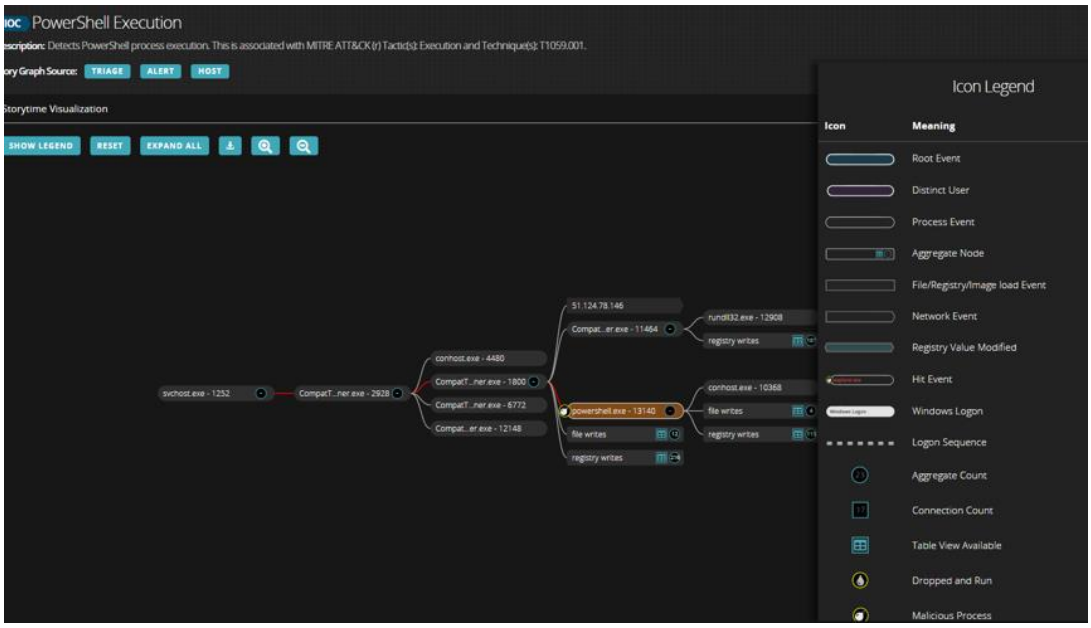
Storytime Systemmodul

Das Storytime Systemmodul verarbeitet Warnungen von Indicators of Compromise (IOC) und Exploit Guard (EXG), die ein zugehöriges Auto-Triage-Paket enthalten. Storytime analysiert die Auto-Triage-Artefakte, generiert eine Kapiteldatei und speichert sie in der Datenbank. Wenn zwei oder drei IOC- oder EXG-Warnungen kurz hintereinander generiert werden, generiert Storytime mehrere Kapiteldateien und speichert diese in der Datenbank. Dies bietet dem Administrator eine Auto-Triage Sammlung, in der er jede individuelle Warnung und die Beziehung zwischen den Warnungen untersuchen kann. Wenn der Endpoint Security Server mit Helix integriert ist, streamt er die Kapiteldatei an Helix.



Der Storytime Viewer ist ein interaktives Raster, das Details über alle Kapitel enthält. Bestimmte Spalten, wie z.B. Alert ID, Triage ID und Hostname sind Links auf weitere Informationen, die sich auf das Kapitel beziehen. Wenn Sie auf den Chapter View Link klicken, wird die Storytime Vizualization in einem getrennten Tab geöffnet.

Die Storytime Visualization ist eine grafische Darstellung der Triage-Daten in einer Warnung. Die Visualisierung konzentriert sich auf die wichtigsten Daten aus der Auto-Triage in der Warnung und zeigt den kritischen Pfad auf den Ereignisknoten, der die Erkennung ausgelöst hat. Um den kompromittierten Knoten schnell zu identifizieren, verwendet die Visualisierung eine rote Linie für den kritischen Pfad. Die Standardansicht zeigt nur den Trefferknoten, seine gleichgeordneten Elemente und minimale Informationen um ihn herum. Verwenden Sie das Erweiternsymbol auf einem Knoten oder die Expand All Schaltfläche, um parallele Ereignisse anzuzeigen.



Verwenden Sie die Show Legend Schaltfläche für eine detaillierte Erklärung über die in der Visualisierung verwendeten Knoten und Symbole. Wenn Sie auf einen Knoten klicken, sind zusätzliche Informationen entweder in einem Seitenbereich oder einer Tabellenansicht verfügbar. Von der Tabellenansicht können Sie eine CSV-Datei herunterladen. Verwenden Sie das Exportsymbol, wenn Sie die JSON-Kapiteldatei anzeigen wollen.

Um auf das Storytime System Modul zuzugreifen:

1. Melden Sie auf der Endpoint Security Web-UI mit Ihren Administrator-Anmeldeinformationen an.
2. Wählen Sie **Endpoint Module Administration** vom Modules Menü.
3. Klicken Sie auf der Modules Seite auf den **System Modules** Tab.
4. Klicken Sie in der Name Spalte auf den **Storytime** Link, um Storytime Viewer zu öffnen.

Unterstützte Plattformen

Die Storytime 2.1.0 Version wird auf Endpoint Security 5.1 oder später unterstützt.

TEIL VIII: Anhänge

ANHANG A: Bereitgestellte Datenerfassungsscripts

FireEye stellt mehrere Datenerfassungsscripts bereit, mit denen Sie mit Datenerfassungsanforderungen beginnen können. Diese Scripts können Sie nicht löschen. Sie können einige von ihnen kopieren und bearbeiten, um sie als Basis für Ihre eigenen Scripts zu verwenden. Wenn Sie sie bearbeitet haben, können Sie sie auch auf ihre werkseitig-verteilte Form zurücksetzen.

Einige dieser bereitgestellten Scripts können in einer Datenerfassungsanforderung verwendet werden. Die meisten von ihnen produzieren eine herunterladbare `.mans` Datei, die inRedline und im Audit Viewer überprüft werden kann. Das Full Memory Script und das Full Disk Script produzieren eine herunterladbare `.zip` Datei.

In der folgenden Tabelle sind die unterstützten Betriebssystemplattformen für jedes Script aufgeführt.

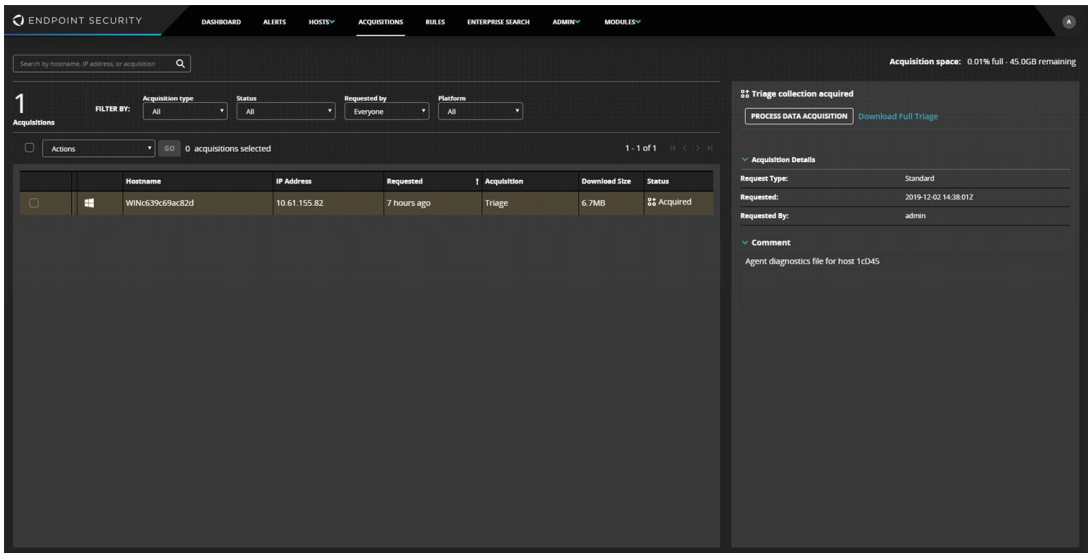
Bereitgestellter Scriptname	Endpunkt Betriebssystem Support		
	Windows	macOS	Linux
Agent Diagnostics	Ja	Yes	Ja
Command Shell History Script	Ja	Nein	Nein
Comprehensive Investigative Details Script	Ja	Yes	Ja
Driver Memory Script	Ja	Nein	Nein
Full Disk Script	Ja	Nein	Nein
Full Memory Script	Ja	Nein	Nein
PowerShell History Script	Ja	Nein	Nein
Process Details Script	Ja	Ja	Nein
Process Memory Script	Ja	Nein	Nein

Bereitgestellter Scriptname	Endpunkt Betriebssystem Support		
	Windows	macOS	Linux
Quick File Listing	Ja	Yes	Ja
Standard Investigative Details Script	Ja	Yes	Ja

Dieser Abschnitt liefert eine Beschreibung für jedes Script und Anleitung für die Hinzufügung und Bearbeitung von Kommentaren zu Ihren Datenerfassungsanfragen. Informationen über jedes von verwendeten Auditmodulen verwendete Script finden Sie im *Endpoint Security Audit Referenzhandbuch*.

Kommentare zur Datenerfassung hinzufügen und bearbeiten

Alle Erfassungsanfragen bieten jetzt ein **Comment** Feld. Verwenden Sie dieses Feld, um Kommentare zu der ausgewählten Datenerfassung hinzuzufügen, einschließlich des Grunds für die Erfassungsanfrage und alle spezifischen Details für die Erfassungsanfrage, die Sie für die Vorfallsverfolgung aufzeichnen wollen. Sie können Kommentare im **Acquisition Details** Bereich auf der **Acquisitions** Seite überprüfen und bearbeiten.



Um einen Kommentar zu einer Datenerfassungsanfrage hinzuzufügen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.

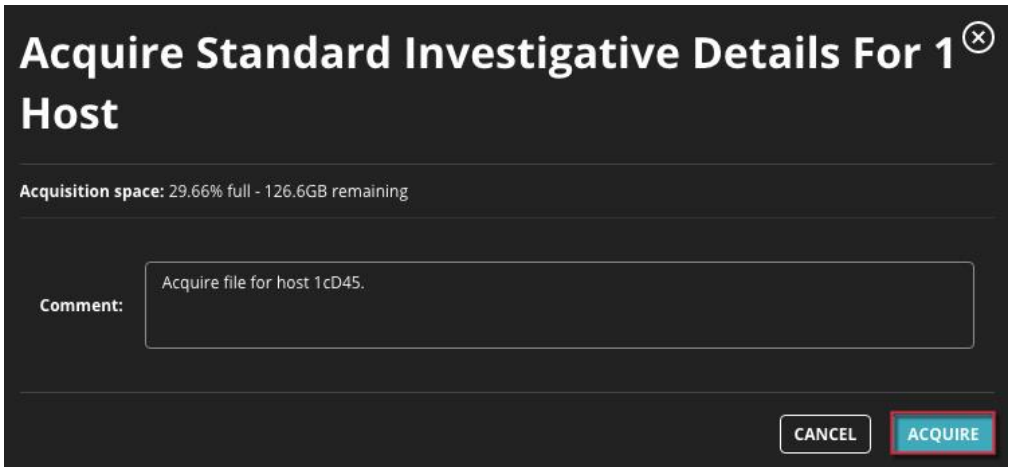
HINWEIS: Die folgenden bereitgestellten Datenerfassungen sind nicht für mehrfache Hosts verfügbar: Driver Memory, Full Disk, Full Memory und Process Memory. Diese Erfassungsanfragen sind nur für einen einzelnen Host verfügbar.

3. Im **Actions** Menü wählen Sie das Datenerfassungsscript, das Sie verarbeiten wollen.

VORSICHT: Full Memory oder Raw Disk Datenerfassungen können mehr Informationen als erwartet zurückgeben und Leistungs- und Speicherprobleme hervorrufen. FireEye empfiehlt, dass Sie den Umfang dieser Scripts begrenzen.

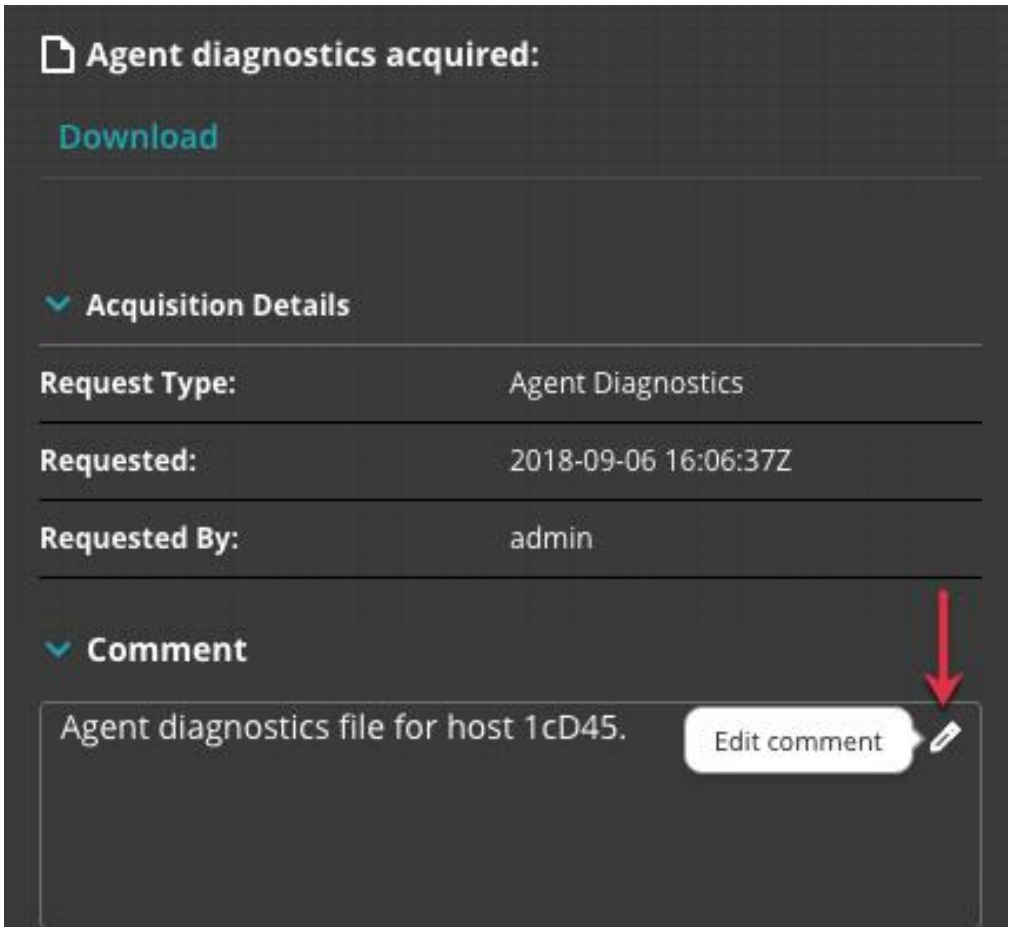
4. Klicken Sie auf **Go**, um auf das **Acquire** Dialogfeld zuzugreifen.
5. Wenn das Dialogfeld für die Datenerfassung mehrere Felder enthält, geben Sie die erforderlichen Informationen in jedem Feld ein.
6. Im **Comment** Feld geben Sie den Grund für die Erfassungsanfrage ein und alle spezifischen Details über die Erfassung, die Sie aufzeichnen wollen.

7. Klicken Sie auf **Acquire**, um den Prozess für die Datenerfassung zu starten.



Um einen Kommentar über eine Datenerfassung zu bearbeiten.

1. Wählen Sie **Acquisitions** in der Endpoint Security Web-UI.
2. Wählen Sie einen Host.
3. Im **Acquisition Details** Abschnitt klicken Sie auf das **Comment** Dropdown, um auf alle gespeicherten Kommentare für die ausgewählte Erfassung zuzugreifen.
4. Klicken Sie auf das **Edit** Symbol, um den Kommentar zu verändern oder zu aktualisieren.



5. Klicken Sie auf **Save**.

Agent Diagnostics Script

Das Agent Diagnostics Script ist ein spezielles Script, das verwendet wird, um dem FireEye Customer Support die Daten bereitzustellen, die zur Problemlösung benötigt werden. Wenn Agent Diagnostics angefordert werden, sammelt der Endpoint Security Agent auf dem ausgewählten Host-Endpunkt die forensischen Daten und erstellt eine herunterladbare `.zip` Datei, die Sie überprüfen oder an Ihren FireEye Customer Support Mitarbeiter senden können. Diese Daten enthalten Agent Scanprotokolle.

Dieses Script kann für Windows, macOS und Linux Host-Endpunkte angefordert werden.

Sie können das Agent Diagnostics Script nicht kopieren, bearbeiten, neu einstellen, importieren oder löschen oder dieses Script in Datenerfassungsscripts verwenden, die Sie erstellen. Dieses Script wird nicht auf der Data Acquisition Scripts Seite angezeigt.

Agent Diagnostics Daten anfordern

Um Agent Diagnostics Informationen mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Wählen Sie **Agent Diagnostics** vom Actions Menü. Alternativ können Sie **Agent Diagnostics** auf dem **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquiring Agent Diagnostics** Dialogfeld zuzugreifen.
5. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
6. Klicken Sie auf **Acquire**.

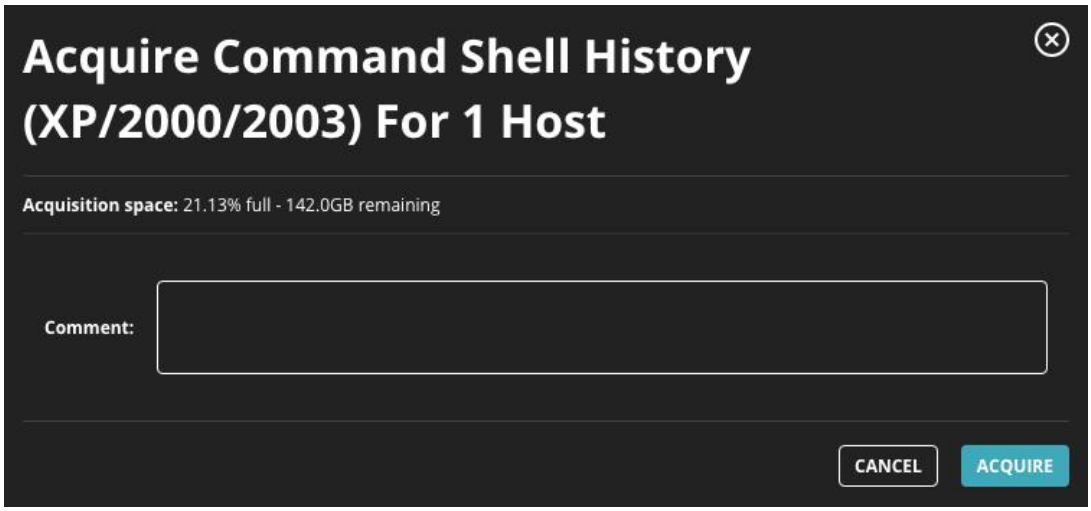
Das **Acquiring Agent Diagnostic** Dialogfeld zeigt ebenfalls den Prozentzsatz des verfügbaren Speicherplatzes, der derzeit für die Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Agent Diagnostics Daten können als eine reguläre Datenerfassung angefordert werden. Siehe Eine Datenerfassung anfordern auf Seite 321

Command Shell History Script

Das Command Shell History Script fordert einen Befehlsshellverlauf von Host Endpunkten an. Dieses Script kann nur für Windows Host Endpunkte angefordert werden. Für macOS oder Linux Host-Endpunkte wird keine Unterstützung bereitgestellt.

Dieses Script kann nicht kopiert, bearbeitet, zurückgesetzt oder gelöscht werden und erscheint nicht auf der Data Acquisition Scripts Seite. Sie können dieses Script nicht in Datenerfassungsscripts verwenden, die Sie erstellen.



Befehlsshell-Verlaufsdaten anfordern

Um Befehlsshell-Verlaufsdaten mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Wählen Sie **Command Shell History** vom Actions Menü. Alternativ können Sie auch **Command Shell History** vom **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire Command Shell History** Dialogfeld zuzugreifen.
5. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
6. Klicken Sie auf **Acquire**.

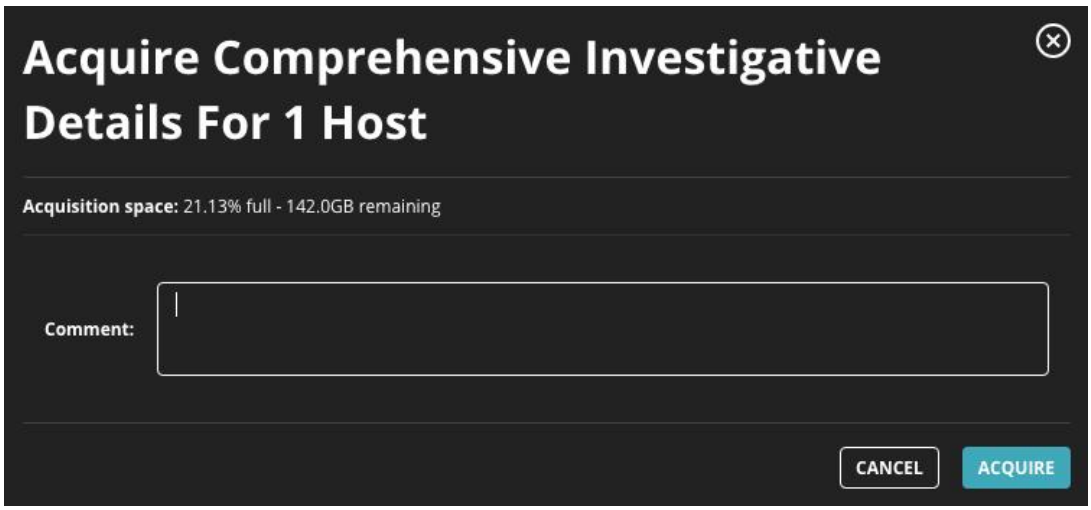
Das **Acquire Command Shell History** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Command Shell History Daten können als regelmäßige Datenerfassung angefordert werden. Siehe Eine Datenerfassung anfordern auf Seite 321.

Comprehensive Investigative Details Script

Das Comprehensive Investigative Details Script sammelt umfangreichere forensische Daten von Host Endpunkten als das Standard Investigative Details Script auf Seite 483. Alle bis auf die unerschwinglichsten Ermittlungsdaten werden gesammelt. Dieses Script kann für Windows, macOS und Linux Host-Endpunkte angefordert werden.

Sie können dieses Script auf der Data Acquisitions Script Seite kopieren, bearbeiten, zurücksetzen und exportieren.



Comprehensive Investigative Details anfordern

Um umfassende investigative Details mit Hilfe der Web-UI zu erfassen:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Wählen Sie **Comprehensive Investigative Details** vom Actions Menü. Alternativ können Sie **Comprehensive Investigative Details** vom **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire Comprehensive Investigative Details** Dialogfeld zuzugreifen.
5. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und Protokolldetails über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
6. Klicken Sie auf **Acquire**.

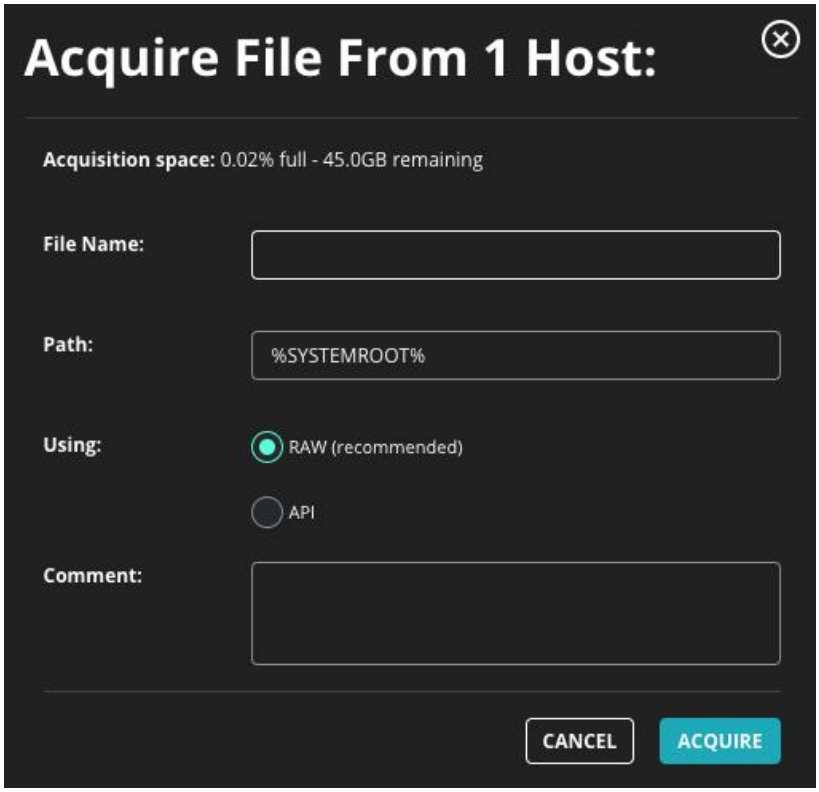
Das **Acquire Comprehensive Investigative Details** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt

Comprehensive Investigative Detail können als regelmäßige Datenerfassung angefordert werden. Siehe Eine Datenerfassung anfordern auf Seite 321.

File

Das File Script fordert eine Liste von Dateien mit Hilfe von Systemaufrufen von Ihren Host-Endpunkten an. Dieses Script kann nur für Windows Endpunkte angefordert werden.

HINWEIS: Unterstützung für File Script wird nicht für macOS oder Linux Host-Endpunkte bereitgestellt.



Die folgende Tabelle beschreibt die Felder in diesem Dialogfeld. Verwenden Sie die Standardwerte oder geben Sie neue Werte ein.

Feld	Beschreibung
Filename	(Erforderlich) Bestimmen Sie den Namen der Datenerfassungsdatei, die erfasst werden soll.

Feld	Beschreibung	
Path	Bestimmen Sie den globalen Pfad oder den symbolischen Link auf das Laufwerk oder Volumen, von dem Sie die Liste der Dateien mit Hilfe von Systemaufrufen erfassen wollen.	
Using	Raw	Sammelt eine Liste von Dateien, indem die Strukturen auf den Laufwerken des Zielsystems direkt untersucht werden.
	API	
Comment	Geben Sie Details über Ihre spezifische Datenerfassungsanfrage ein und den Grund für die Erfassung der Datei.	

Das **Quick File Listing** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Dateidaten anfordern

Um File Daten mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Auf dem **Actions** Menü wählen Sie **File**. Alternativ können Sie **File** vom **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um Zugriff auf das **File** Dialogfeld zu erhalten.
5. Geben Sie den Dateinamen im Filename Feld ein.
6. Geben Sie den Dateipfad im Path Feld ein.
7. Wählen Sie die Art der Dateierfassung, die Sie von Ihrem Host-Endpunkt abrufen wollen. Optionen umfassen Raw und API.
8. Im **Comment** Feld geben Sie den Grund für die Dateiliste ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
9. Klicken Sie auf **Acquire**.

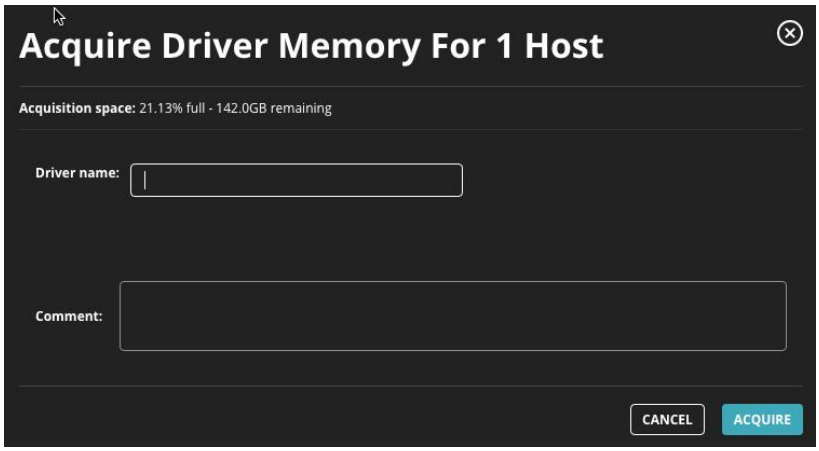
Driver Memory Script

Das Driver Memory Script fordert Treiber-Speicherdaten von Host-Endpunkten an und verwendet das `driver-memoryacquire` Audit, um einen Treiber von Live Memory oder

von einem Memory-Image eines Host-Endpunktes zu sammeln. Weitere Informationen finden Sie im *Endpoint Security Audit Referenzhandbuch*. Dieses Script kann nur für Windows Host-Endpunkte angefordert werden.

Support für Treiber Memory-Scrips wird nicht für macOS oder Linus Host-Endpunkt geboten.

Sie können das Driver Memory Script nicht kopieren, bearbeiten, neu einstellen, importieren oder löschen oder dieses Script in Datenerfassungsscripts verwenden, die Sie erstellen. Dieses Script wird nicht auf der Data Acquisition Scripts Seite angezeigt.



Driver Memory Daten anfordern

Um Driver Memory Daten mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen Host.

   Wenn Sie mehrere Hosts auswählen, ist die Driver Memory Datenerfassungsoption nicht verfügbar. Dieses Script kann nur angefordert werden, wenn ein einzelner Host ausgewählt ist.

3. Vom Actions Menü wählen Sie **Driver Memory**. Alternativ können Sie **Driver Memory** vom **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire Driver Memory** Dialogfeld zuzugreifen.
5. Im **Driver name** Feld geben Sie einen Treibernamen ein, der für die Sammlung von Treiberspeicherdaten verwaltet werden soll.
6. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und Protokolldetails über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
7. Klicken Sie auf **Acquire**.

Das **Acquire Driver Memory** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Treiber Memory Daten können als eine reguläre Datenerfassung angefordert werden. Weitere Informationen finden Sie unter Eine Datenerfassung anfordern auf Seite 321.

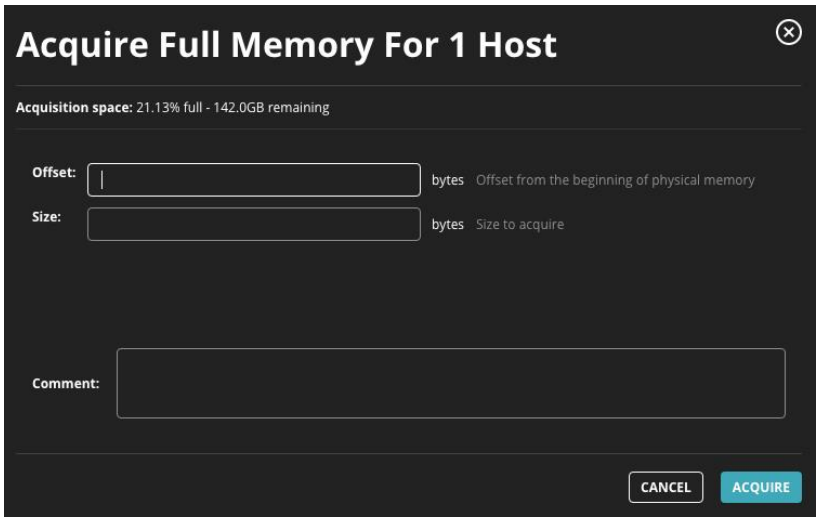
Full Memory Script

Das Full Memory Script fordert vollständige Speicherdaten von Host-Endpunkten vom Anfang des physischen Speichers an und verwendet das `memory-acquisition` Audit. Dieses Script erfasst den vollständigen Speicher des Systems. Sie können dieses Script nur für Windows Host-Endpunkte anfordern.

Support für Full Memory-Scrips wird nicht für macOS oder Linus Host-Endpunkt bereitgestellt.

Sie können das Full Memory Script nicht kopieren, bearbeiten, neu einstellen, importieren oder löschen oder dieses Script in Datenerfassungsscripts verwenden, die Sie erstellen.

Full Memory Datenerfassungen können mehr Informationen als erwartet zurückgeben und Leistungs- und Speicherprobleme hervorrufen. FireEye empfiehlt, dass Sie den Umfang für dieses Scripts mit Hilfe des Acquire Full Memory Dialogfelds beschränken.



Die folgende Tabelle beschreibt die Felder in diesem Dialogfeld. Keins dieser Felder ist ein Pflichtfeld.

Feld	Beschreibung
Offset	Geben Sie das Offset in Bytes, vom Anfang des physischen Speichers an, von dem vollständige Speicherdaten erfasst werden sollen.
Size	Geben Sie die Größe in Bytes der vollständigen Speicherdaten an, die erfasst werden sollen.
Comment	Geben Sie Details über Ihre spezifische Datenerfassungsanfrage ein und den Grund für die Erfassung der Datei.

Das **Full Memory** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Full Memory Daten anfordern

Um Full Memory Daten mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen Host.

   Wenn Sie mehrere Hosts auswählen, ist die **Full Memory** Datenerfassungsoption nicht verfügbar. Dieses Script kann nur angefordert werden, wenn ein einzelner Host ausgewählt ist.

3. Auf dem **Actions** Menü wählen Sie **Full Memory** und klicken Sie auf **Go**. Alternativ können Sie **Full Memory** auf dem **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire Full Memory** Dialogfeld zuzugreifen.
5. Im **Offset** Feld geben Sie das Disk-Offset (in Bytes) vom Anfang des physischen Speichers ein.

   Wenn Sie die Offset und Size Werte leer lassen, erfassen Sie alle Pozessspeicherdaten.

6. Im **Size** Feld geben Sie die Größe (in Bytes) der vollständigen Speicherdaten ein, die Sie erfassen wollen.
7. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
8. Klicken Sie auf **Acquire**.

Eine herunterladbare `.zip` Datei wird von einer Full Memory Erfassungsanforderung produziert. Extrahieren Sie den Inhalt der Zip-Datei mit Hilfe eines Unzip-Tools. Finden und konvertieren Sie die Datei mit der größten Dateigröße auf Imageformat (`*.img`). Öffnen Sie dann die Image Formatdatei mit einem open Source forensischem Tool (z.B.Forensic Toolkit (FTK) oder dem Speicher Forensik-Framework der Volatility Foundation).

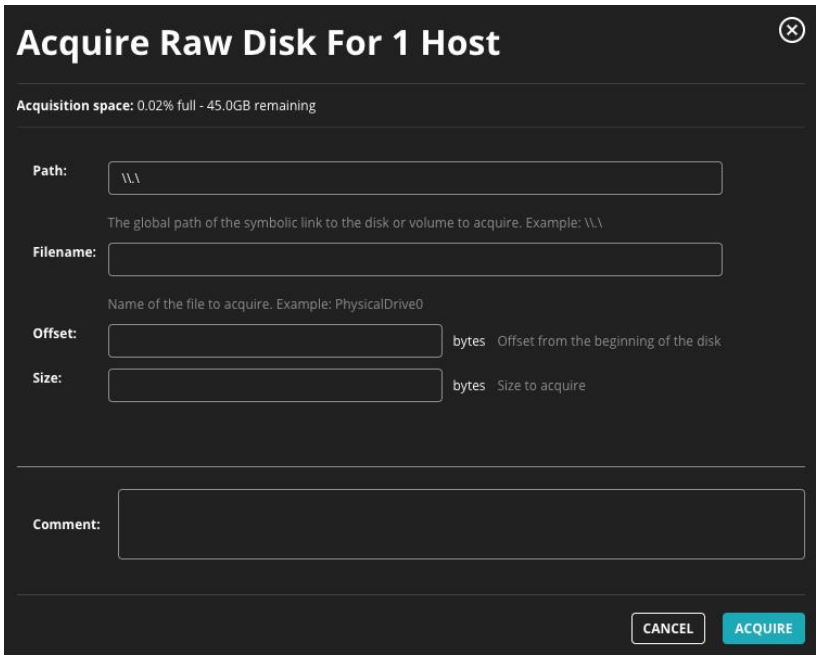
Full Memory Daten können als eine reguläre Datenerfassung angefordert werden. Siehe Eine Datenerfassung anfordern auf Seite 321.

Raw Disk Script

Das Raw Disk Script fordert vollständige Diskdaten von Host-Endpunkten an und verwendet das `disk-acquisition` Audit, um den Inhalt eines Disklaufwerks von einem Host-Endpunkt zu sammeln. Bei dieser Datenerfassung handelt es sich nicht um eine einzelne Momentaufnahme, sondern um einen tatsächlicher Stream des Datenträgerinhalts. Im Laufe der Akquisition können Änderungen an dem Laufwerk an Stellen vorgenommen werden, die das Script noch zu erfassen hat. Dieses Script kann nur für Windows Host-Endpunkte angefordert werden.

HINWEIS: Unterstützung für Raw Disk Scripts wird nicht für macOS oder Linux Host-Endpunkte bereitgestellt.

Sie können das Raw Disk Script nicht kopieren, bearbeiten, neu einstellen, importieren oder löschen oder dieses Script in Datenerfassungsscripts verwenden, die Sie erstellen. Dieses Script wird nicht auf der Data Acquisition Scripts Seite angezeigt.



Die folgende Tabelle beschreibt die Felder in diesem Dialogfeld. Ein Dateiname muss festgelegt werden.

Feld	Beschreibung
Path	Bestimmen Sie den globalen Pfad oder symbolischen Link auf das Laufwerk oder Volumen, von dem Sie Raw Laufwerkdaten erfassen wollen.
Filename	(Erforderlich) Bestimmen Sie den Namen der Datenerfassungsdatei, die erfasst werden soll.
Offset	Geben Sie das Offset in Bytes, vom Anfang des Datenträgers an, von dem Raw Datenträgerdaten erfasst werden sollen.
Size	Geben Sie die Größe der Raw Laufwerksdaten an, die erfasst werden sollen, in Bytes an. Wenn Sie die Offset und Size Werte leer lassen, können Sie Laufwerksdaten für das gesamte Laufwerk erfassen.
Comment	Geben Sie Details über Ihre spezifische Datenerfassungsanfrage ein und den Grund für die Erfassung der Datei.

Das **Acquire Raw Disk** Dialogfeld zeigt auch den Prozentsatz des zugewiesenen Speicherplatzes an, der derzeit für die Speicherung von Erfassungen verwendet wird und wie viel freier Speicherplatz in (GB) noch verfügbar ist.

Raw Diskdaten anfordern

Raw Disk Datenerfassungen können lange dauern, mehr Informationen als erwartet zurückgeben und zu Leistungs- und Speicherproblemen führen. FireEye empfiehlt, dass Sie den Umfang dieses Scripts mit Hilfe des Acquire Raw Disk Dialogfeldes einschränken und die Raw Disk Datenerfassungen außerhalb der Stoßzeiten anfordern, wenn weniger Systembenutzer betroffen sind.

Um Raw Diskdaten mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen Host.

HINWEIS: Wenn Sie mehrere Hosts auswählen, ist die **Raw Disk** Datenerfassungsoption nicht verfügbar. Dieses Script kann nur angefordert werden, wenn ein einzelner Host ausgewählt ist.

3. Auf dem **Action** Menü wählen Sie **Raw Disk** und klicken Sie auf **Go**. Alternativ können Sie **Raw Disk** auf dem **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire Raw Disk** Dialogfeld zuzugreifen.
5. Im **Path** Feld geben Sie den globalen Pfad oder den symbolischen Link auf das Laufwerk oder Volumen ein, von dem Sie Raw Diskdaten erfassen wollen.
6. Im **Filename** Feld geben Sie den Namen der Datenerfassungsdatei ein, die Sie erfassen wollen.
7. Im **Offset** Feld geben Sie das Laufwerk-Offset (in Bytes) vom Anfang des Laufwerks ein.

   HINWEIS: Wenn Sie die Offset und Size Werte leer lassen, können Sie Diskdaten für den gesamten Datenträger erfassen.

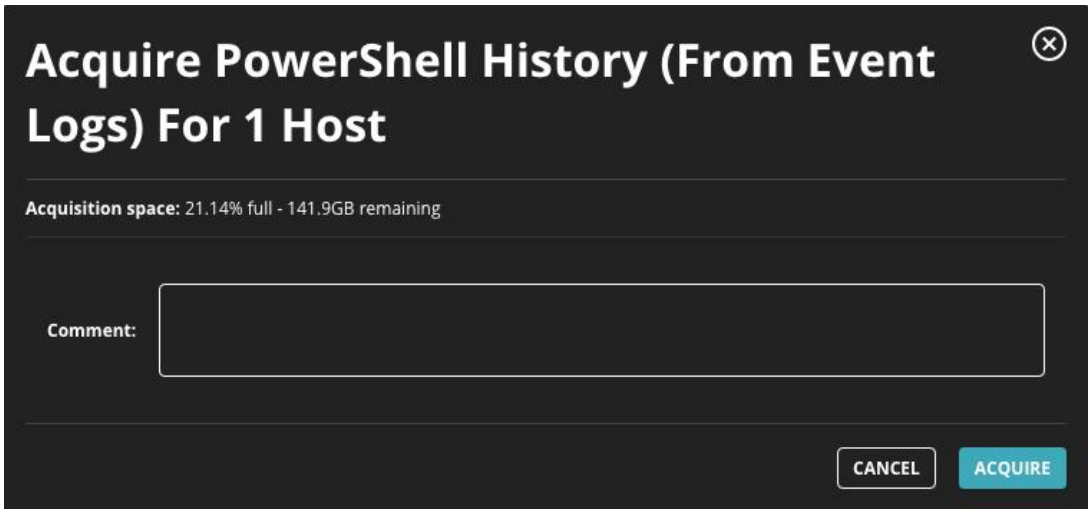
8. Im **Size** Feld geben Sie die Größe (in Bytes) der Raw Diskdaten ein, die Sie erfassen wollen.
9. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
10. Klicken Sie auf **Acquire**.

PowerShell History Script

Das PowerShell History Script erfasst Daten von den Ereignisprotokollen, die für PowerShell Verlauf spezifisch sind, wenn das Script auf Host-Endpunkten aktiviert ist. Dieses Script kann nur für Windows Host-Endpunkte angefordert werden.

Unterstützung für das PowerShell History Script wird nicht für macOS oder Linux Host-Endpunkte geboten.

Sie können das PowerShell History Script nicht kopieren, bearbeiten, neu einstellen, importieren oder löschen oder dieses Script in Datenerfassungsscripts verwenden, die Sie erstellen. Dieses Script wird nicht auf der Data Acquisition Scripts Seite angezeigt.



PowerShell History Daten anfordern

Um PowerShell History Daten mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Wählen Sie **PowerShell History** vom Actions Menü. Alternativ können Sie **PowerShell History** auf dem **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire PowerShell History** Dialogfeld zuzugreifen.
5. Im Comment **Feld geben Sie den Grund für die Erfassung der Datei ein und Protokolldetails über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.**
6. Klicken Sie auf **Aquire**, um die Anfrage einzureichen.

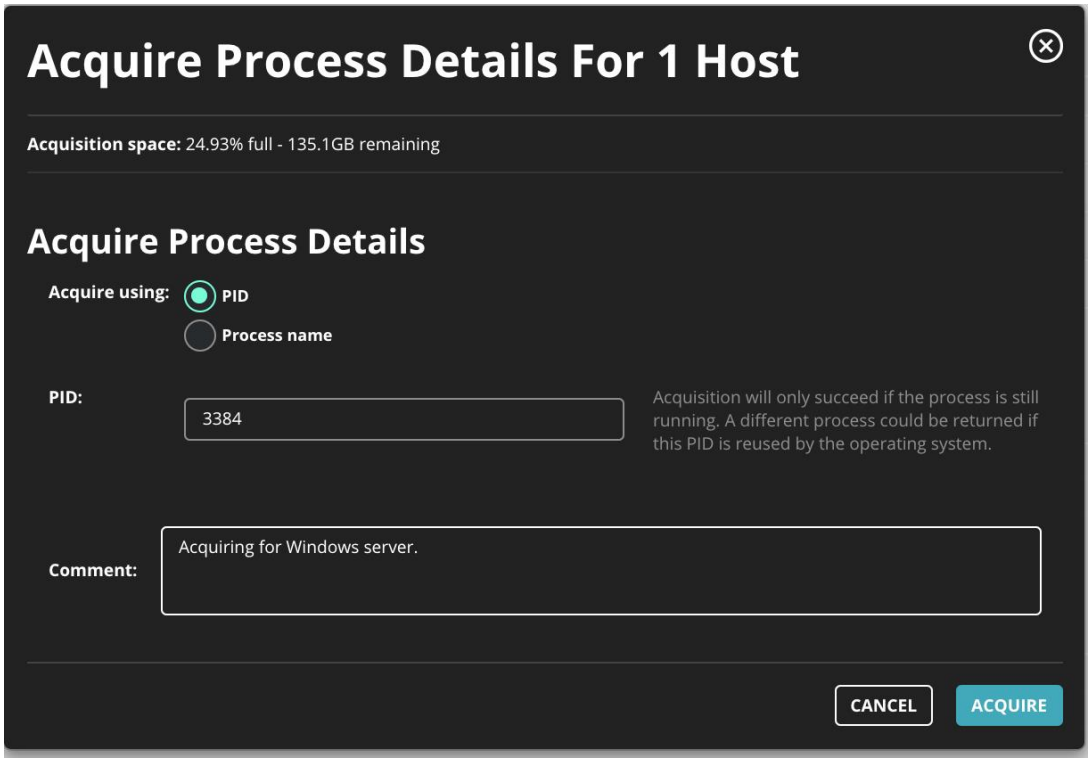
Power Shell History Daten können als regelmäßige Datenerfassung angefordert werden. Siehe Eine Datenerfassung anfordern auf Seite 321.

Process Details Script

Das Process Details Script fordert Daten über einen spezifischen Prozess von Host-Endpunkten an. Dieses Script kann nur für Windows oder macOS Host-Endpunkte angefordert werden. Sie können Process Details Daten nicht als eine reguläre Datenerfassung anfordern, aber Sie können dieses Script vom Triage Viewer anfordern.

Process Details Script-Support wird nicht für Linux Host-Endpunkte geboten.

Sie können dieses Script auf der Data Acquisitions Script Seite bearbeiten, zurücksetzen und exportieren, aber dieses Script kann nicht kopiert werden.



Die folgende Tabelle beschreibt die Felder in diesem Dialogfeld. Mindestens eine PID (Process ID) oder ein Prozessname muss festgelegt werden.

Feld	Beschreibung
Acquire using	Wählen Sie **PID**, um eine Prozess ID festzulegen. Wählen Sie **Process name**, um einen Prozessnamen festzulegen.
Process PID	Wenn **PID** ausgewählt wurde, legen Sie die Prozess-ID fest, die für die Sammlung von Prozessdetaildaten verwendet werden soll.
Process name	Wenn **Process name** ausgewählt wurde, legen Sie den Prozessnamen fest, der für die Sammlung von Prozessdetaildaten verwendet werden soll.

Das **Process Detail** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherraums, der derzeit für die Speicherungen von Erfassung benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Process Details anfordern

1. Wählen Sie **Acquisitions** in der Endpoint Security Web-UI.
2. Wählen Sie einen Host.

   Wenn Sie mehrere Hosts auswählen, ist die Process Details Erfassungsoption nicht verfügbar. Sie können dieses Script nur anfordern, wenn ein einzelner Host ausgewählt ist.

3. Im Triage collection acquired Abschnitt klicken Sie auf **View Triage Summary**, um auf die Triage-Zusammenfassung für den ausgewählten Host zuzugreifen.
4. Klicken Sie auf **Acquire Process Details**.
5. Auf dem **Acquire using** Menü wählen Sie **PID**, wenn Sie eine Prozess-ID festlegen wollen oder **Process name**, wenn Sie einen Prozessnamen festlegen wollen.

   Die Datenerfassung ist nur erfolgreich, wenn der Prozess noch läuft. Wenn die PID von dem Betriebssystem erneut verwendet wird, könnte die Erfassungsanfrage einen anderen Prozess zurückgeben.

6. Geben Sie die Prozess-ID oder den Prozessnamen auf Ihrer früheren Auswahl basierend ein.
7. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
8. Klicken Sie auf **Acquire**.

Das **Process Details** Dialogfeld zeigt auch Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Sie können Daten, die für diese Anfrage zurückgegeben wurden, auf der Acquisitions Seite im Acquisition Detail Bereich anzeigen und herunterladen. Siehe Eine Process Detail Datenerfassung anfordern auf Seite 323. Sie können die Daten auch im Audit Viewer überprüfen. Wenn Sie die Erfassung herunterladen, können Sie die Daten in Redline überprüfen. Die erfassten Daten enthalten Zeichenfolgen im Speicher für den Prozess.

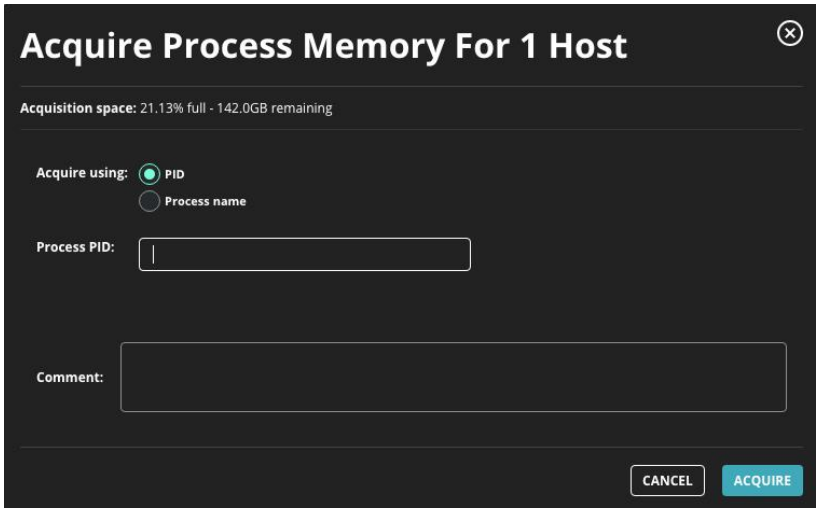
Process Memory Script

Das Process Memory Script fordert Prozessspeicherdaten von Host-Endpunkten an und verwendet das `processes-memoryacquire` Audit. Dieses Script erfasst alle Speicherabschnitte des Prozesses als Binärdateien. Allerdings kann Redline heruntergeladene Erfassungsdaten von diesem Script selbst als eine `.mans` Datei nicht öffnen. Verwenden Sie Winzip, um diese heruntergeladenen Daten anzuzeigen.

Dieses Script kann nur für Windows Host-Endpunkte angefordert werden.

Unterstützung für das Process Memory Script wird nicht für macOS oder Linux Host-Endpunkte geboten.

Sie können das Process Memory Script nicht kopieren, bearbeiten, neu einstellen, importieren oder löschen oder dieses Script in Datenerfassungsscripts verwenden, die Sie erstellen. Dieses Script wird nicht auf der Data Acquisition Scripts Seite angezeigt.



Die folgende Tabelle beschreibt die Felder in diesem Dialogfeld. Mindestens eine PID (Process ID) oder ein Prozessname muss festgelegt werden.

Feld	Beschreibung
Acquire using	Wählen Sie **PID**, um eine Prozess ID festzulegen. Wählen Sie **Process name**, um einen Prozessnamen festzulegen.
Process PID	Wenn **PID** ausgewählt wurde, legen Sie die Prozess ID fest, die für die Sammlung von Prozessspeicherdaten verwendet werden soll.
Process name	Wenn **Process name** ausgewählt wurde, legen Sie den Prozessnamen fest, der für die Sammlung von Prozessspeicherdaten verwendet werden soll.

Das **Process Memory** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Process Memory Daten anfordern

Um Prozessspeicherdaten mit Hilfe der Web-UI anzufordern:

Mindestens eine PID (Process ID) oder ein Prozessname muss festgelegt werden.

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen Host.

   Wenn Sie mehrere Hosts auswählen, ist die Process Memory Datenerfassungsoption nicht verfügbar. Sie können dieses Script nur anfordern, wenn ein einzelner Host ausgewählt ist.

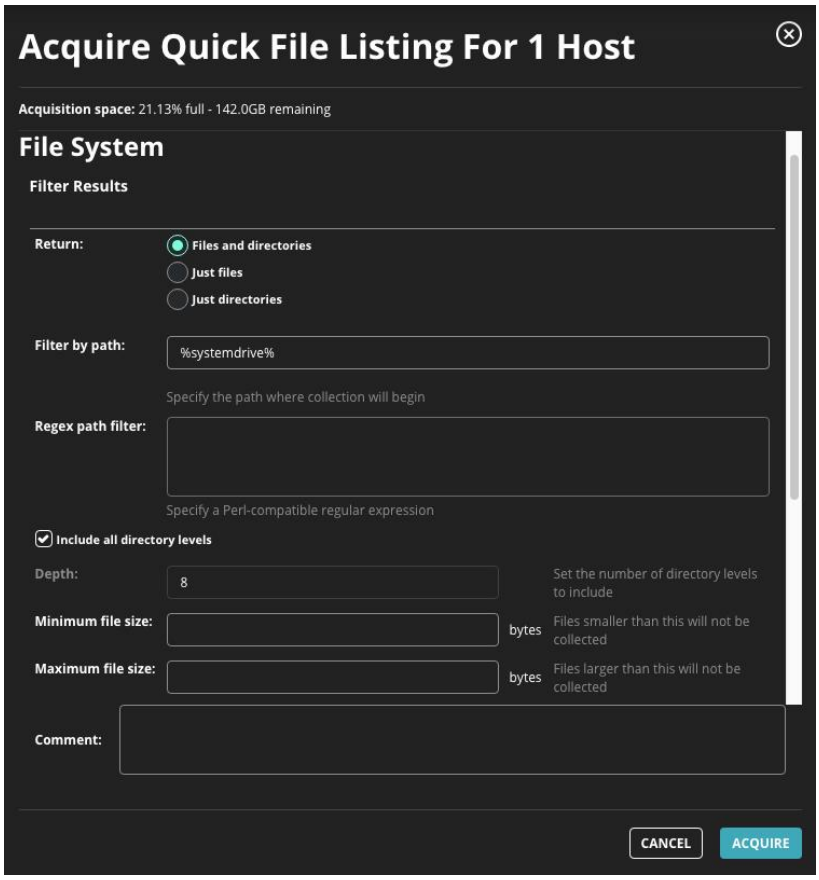
3. Vom Actions Menü wählen Sie **Process Memory**. Alternativ können Sie **Process Memory** vom **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire Process Memory** Dialogfeld zuzugreifen.
5. Im **Driver name** Feld geben Sie einen Treibernamen ein, der für die Sammlung von Treiberspeicherdaten verwaltet werden soll.
6. Auf dem Acquire using Menü wählen Sie **PID**, wenn Sie eine Prozess-ID festlegen wollen oder **Process name**, wenn Sie einen Prozessnamen festlegen wollen.
7. Geben Sie die Prozess-ID oder den Prozessnamen auf Ihrer früheren Auswahl basierend ein.
8. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
9. Klicken Sie auf **Acquire**.

Process Memory Daten können als eine reguläre Datenerfassung angefordert werden. Siehe Eine Datenerfassung anfordern auf Seite 321.

Quick File Listing

Das Quick File Listing Script fordert eine Dateiliste von Host-Endpunkten an. Dieses Script kann für Windows, macOS und Linux Host-Endpunkte angefordert werden.

Sie können das Quick File Listing Script nicht kopieren, bearbeiten, neu einstellen, importieren oder löschen oder dieses Script in Datenerfassungsscripts verwenden, die Sie erstellen. Dieses Script wird nicht auf der Data Acquisition Scripts Seite angezeigt.



Die folgende Tabelle beschreibt die Felder in diesem Dialogfeld. Verwenden Sie die Standardwerte oder geben Sie neue Werte ein.

Feld	Beschreibung
Return	Wählen Sie **Files and directories**, um sowohl Dateien als auch Verzeichnisse in der Dateiliste einzuschließen. Wählen Sie **Just files**, um nur Dateien in der Dateiliste einzuschließen. Wählen Sie **Just directories**, um nur Verzeichnisse in der Dateiliste einzuschließen.

Feld	Beschreibung
Filter by path	Legen Sie den Pfad fest, den Sie in der Dateiliste einschließen wollen. Bestimmen Sie einen genauen Pfadnamen oder eine geeignete, pfadbasierte Windows Umgebungsvariable. Zum Beispiel ist die Standard Umgebungsvariable, die in diesem Abschnitt benutzt wird, `%systemdrive%`, was normalerweise auf `C:\` erweitert wird. Die Endpoint Security Appliance führt keine Validierung des von Ihnen festgelegten Pfades durch. Für Netzwerkfreigaben bestimmen Sie Dateien und Ordner mit Hilfe von Universal (oder Uniform) Naming Conventions (UNC). Sehen Sie https://msdn.microsoft.com/en-us/library/gg465305.aspx. Der Endpoint Security validiert die von Ihnen festgelegten Datei- und Ordnernamen nicht. Legen Sie keine Laufwerksbuchstaben oder Pfadnamen fest. Unterschiedliche Endpunkte können verschiedene Laufwerkzuordnungen haben. Wenn Sie einen Ordnernamen ausdrücklich festlegen, beenden Sie den Pfad mit einem Backslash (zum Beispiel `\\fireeye.com\shared\`). Sie können Platzhalterzeichen und System Umgebungsvariable in der Datei oder dem Ordnerpfad festlegen, den Sie ausschließen wollen. Seien Sie vorsichtig, wenn Sie System Umgebungsvariable in Ordnerpfaden festlegen. Die erweiterten Pfade der in Ordnerpfaden festgelegten System Umgebungsvariablen unterscheiden sich je nach der installierten Version von Windows. Vollständige Informationen zu Windows Umgebungsvariablen finden Sie in der Windows Dokumentation (Microsoft TechNet). Benutzerspezifische Umgebungsvariablen (die den Benutzernamen in ihrem erweiterten Pfad enthalten), z. B.% APPDATA% oder% USERPROFILE%, werden nicht unterstützt. Da Sie den Benutzer, für den eine Umgebungsvariable gilt, nicht angeben können, muss die erweiterte Umgebungsvariable nicht unbedingt der Benutzer sein, der auf dem Endpunkt Host angemeldet ist.
Regex path filter	Zusätzlich zu dem Anfangspfad können Sie mit Hilfe eines Perl-kompatiblen regulären Ausdrucks (regex) filten, um den Pfad festzulegen, der in der Dateiliste eingeschlossen sein soll.

Feld	Beschreibung
Include remote locations (nur macOS und Linux)	Wählen Sie diese Option, um alle Verzeichnisse auf remote Standorten in der Dateiliste einzuschließen.
Include all directory levels	Wählen Sie diese Option, um alle Verzeichnisebenen in der Dateiliste einzuschließen.
Depth	Wenn Sie **Include all directory levels** nicht auswählen, legen Sie die Ordnertiefe fest, die in der Dateiliste eingeschlossen sein soll.
Minimum file size	Bestimmen Sie die minimale Dateigröße, in Bytes, der Dateien, die in der Dateiliste eingeschlossen sein sollen.
Maximum file size	Bestimmen Sie die maximale Dateigröße der Dateien, die in der Dateiliste eingeschlossen sein sollen, in Bytes.
Content Regex (Nur Windows)	Bestimmen Sie Perl-kompatible reguläre Ausdrücke (regex), um erforderliche Dateiinhalte für Dateien zu identifizieren, die in der Liste eingeschlossen sein soll. Bestimmen Sie einen regulären Ausdruck pro Zeile.
OR und AND (Nur Windows)	Wählen Sie **OR**, um einen der regex Ausdrücke abzugleichen, der im Content Regex Feld aufgeführt ist Wählen Sie **AND**, um alle regex Ausdrücke abzugleichen, die im Content Regex Feld aufgeführt sind.

Das **Quick File Listing** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Quick File Listing Daten anfordern

Um Quick File Listing Daten mit Hilfe der Web-UI anzufordern:

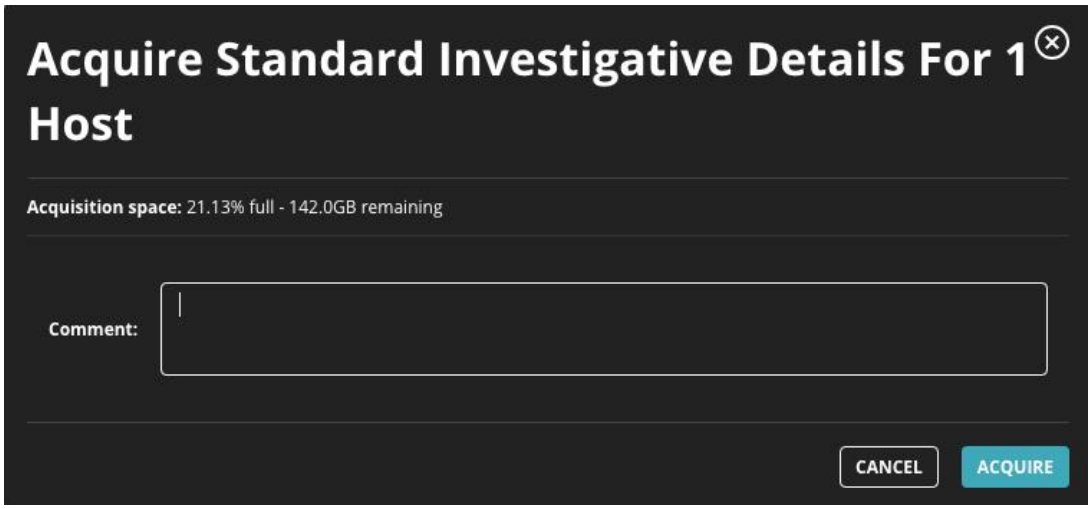
1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Auf dem **Actions** Menü wählen Sie **Quick File Listing**. Alternativ können Sie **Quick File Listing** vom **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire Quick File Listing** Dialogfeld zuzugreifen.

5. Definieren Sie die folgenden Dateisystemeinstellungen:
    - Wählen Sie die Dateitypen, die in der Aufführung eingeschlossen sein sollen. Optionen enthalten Dateien und Verzeichnisse, nur Dateien und nur Verzeichnisse.
    - Wenn Sie die Datei nach Pfad filtern wollen, geben Sie den genauen Pfad, den Sie in der Dateiliste einschließen wollen, im **Filter by path** Feld ein. Richtlinien finden Sie in der voranstehenden Tabelle.
    - Wenn Sie die Dateiliste nach Regex filtern wollen, geben Sie einen Perl-kompatiblen regulären Ausdruck im **Regex path filter** Feld ein.
    - Wählen Sie **Include all directory levels**, wenn Sie alle Verzeichnisse in der Dateiliste einschließen wollen.
    - Wenn Sie Include all directory levels nicht ausgewählt haben, geben Sie die Ordnertiefe, die in der Dateiliste eingeschlossen sein soll, im **Depth** Feld ein.
    - Im **Minimum file size** Feld geben Sie die mindeste Dateigröße (in Bytes) für die Dateien ein, die Sie in der Dateiliste einschließen wollen.
    - Im **Maximum file size** Feld geben Sie die maximale Dateigröße (in Bytes) für die Dateien ein, die Sie in der Dateiliste einschließen wollen.
6. Um die Dateien nach ihrem Inhalt zu filtern:
    - im **Regex** Feld bestimmen Sie Perl-kompatible reguläre Ausdrücke (regex), um erforderliche Dateiinhalte für die Dateien zu identifizieren, die Sie in der Dateiliste einschließen wollen. Bestimmen Sie einen regulären Ausdruck pro Zeile.
    - Wählen Sie **OR** wenn Sie wollen, dass die Dateiliste mit einem der regex Ausdrücke übereinstimmt, die im Regex Feld aufgeführt sind. Wählen Sie **AND** wenn Sie wollen, dass die Dateiliste mit allen regex Ausdrücken übereinstimmt, die im Regex Feld aufgeführt sind.
7. Im **Comment** Feld geben Sie den Grund für die Dateiliste ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
8. Klicken Sie auf **Acquire**.

Standard Investigative Details Script

Das Standard Investigative Details Script sammelt die gebräuchlichsten forensischen Daten von Host Endpunkten. Sie können dieses Script auf der Data Acquisitions Script Seite kopieren, bearbeiten, zurücksetzen und exportieren.

Dieses Script kann für Windows, macOS und Linux Host-Endpunkte angefordert werden.



Standard Investigative Details anfordern

Um Standard Investigative Details mit Hilfe der Web-UI anzufordern:

1. Wählen Sie **Hosts** in der Endpoint Security Web-UI.
2. Wählen Sie einen oder mehrere Hosts.
3. Vom Actions Menü wählen Sie **Standard Investigative Details**. Alternativ können Sie **Standard Investigative Details** vom **Acquire** Menü auf einer Host Details Seite auswählen.
4. Klicken Sie auf **Go**, um auf das **Acquire Standard Investigative Details** Dialogfeld zuzugreifen.
5. Im **Comment** Feld geben Sie den Grund für die Erfassung der Datei ein und alle Details über die Anforderung der Datenerfassung, die Sie nachverfolgen wollen.
6. Klicken Sie auf Acquire**.**

Das **Acquire Standard Investigative Details** Dialogfeld zeigt auch den Prozentsatz verfügbaren Speicherplatzes, der derzeit für die Speicherung von Erfassungen benutzt wird und wie viel freier Speicherraum (in GB) verbleibt.

Agent Diagnostics Daten können als eine reguläre Datenerfassung angefordert werden. Siehe Eine Datenerfassung anfordern auf Seite 321

ANHANG B: CEF Protokolle und Ausgabe

Der Endpoint Security kann Common Event Format (CEF) Verkehr mit Informationen über Treffer (Alarme), Erfassungsanforderungen, Triage-Sammlungen und Eindämmungsaktivitäten speichern.

Da die Beibehaltung solcher Einträge in der lokalen Protokollierung zur Folge haben kann, dass die `/var/log/messages` Datei schnell gefüllt wird, unterdrückt Endpoint Security diese Einträge standardmäßig, um die Leistung zu optimieren. Wenn Ihr Unternehmen Endpoint Security mit einer SIEM Lösung integriert, kann Ihr Unternehmen CEF Protokollierungseinstellungen konfigurieren. Weitere Informationen finden Sie im *Endpoint Security Server-System-Administrationshandbuch*.

In diesem Abschnitt werden allgemeine und spezifische Endpoint Security CEF Protokollierungsereignisse und Ereignisaktivitätsfelder beschrieben, die in SIEM-Lösungen beibehalten und exportiert werden können.

Allgemeine Protokollfelder

Alle CEF Protokolle enthalten neben den Feldern für spezifische Protokolle die folgenden Felder:

```
Time: Zeitstempel des Protokolleintrags
Device Vendor: fireeye
Device Product: hx
Device Version: 5.2.0
Name: Eine Beschreibung des protokollierten Ereignisses
ID: Dasselbe wie der Name Wert
Log Message Type:

      0: Informelle Meldung
      4: Warnmeldung
      7: Fehlermeldung für permanente Erfassung
      10: Jeder FireEye Endpunkt Treffer (Alarm), z.B. IOC,
      Malware oder Exploit Treffer

rt: Die Uhrzeit, zu der das Ereignis auf der Appliance
aufgezeichnet wurde
dvchost: Hostname des Endpoint Security Servers
deviceExternalId: Appliance ID des Endpoint Security Servers
cs1Label: Host Agent Cert Hash
cs1: The host agent certificate hash of the host generating the
event
dst: The primary IP address of the host generating the event
dmac: The MAC address of the host generating the event
dhost: The name of the host generating the event
dntdom: The domain of the host generating the event
deviceCustomDate1Label: "Agent Last Sysinfo" or "Agent Last Audit"
deviceCustomDate1: Last system audit of the host generating the
event
cs2Label: FireEye Agent Version
cs2: The version number of the agent on the host generating the
event
cs5Label: Target GMT Offset, Correlation ID (remediation), or
Actioned Objects Count (malware scans)
cs5: The GMT offset of the host generating the event in ISO 8601
duration format, the alert correlation ID for a malware quarantine
attempt, or the number of scanned objects for which action is
taken.
cs6Label: Target OS, SHA1 (Remediation) or Scanned Objects Count
(Malware Scans)
cs6: The operating system of the host generating the event, the
SHA1 hash of the quarantined file, or the number of objects
scanned for malware.
externalId: A reference number assigned to related events; events
sharing the same ID should be considered connected
categoryOutcome: The agent outcome
categorySignificance: The significance of the event
categoryBehavior: The agent behavior
cs7Label: Resolution
cs7: The result of the hit
cd8Label: Alert Types
cs8: The types of alert produced by the hit
msg: A text description of the event
```

Protokollfelder für Indikator-Treffererkennung

Der Endpoint Security protokolliert Nachrichten, wenn Indicator of Compromise (IOC) Regeln auf einem Zielhost gefunden werden. Neben den allgemeinen CEF Felder enthält Indikator Erkennungsprotokollierung die folgenden Felder und Feldeinstellungen:

IOC-Treffererkennung

```
Name: IOC Hit Found
ID: IOC Hit Found
cs4Label: IOC Name
cs4: Name of the HX threat that was found on the destination host
cs5Label: Target GMT Offset
cs5: The GMT offset of the host generating the event in ISO 8601
duration format
cs6Label: Target OS
cs6: The operating system of the host generating the event
act: Detection IOC Hit
externalId: The HX unique identifier associated with this hit
start: Timestamp when the indicator was detected on the
destination host
categoryOutcome: /Success
categoryBehavior: /Found
categoryDeviceGroup: /IDS
categoryDeviceType: Forensic Investigation
categoryObject: /Host
categorySignificance: /Compromise
categoryTechnique: Alert
categoryTupleDescription: A Detection IOC found a compromise
indication
msg: Host <hostname> IOC compromise
```

Protokollfelder für Exploit Guard

Der Endpoint Security protokolliert Nachrichten, wenn Exploits auf einem Zielhost gefunden wurden. Neben den allgemeinen CEF Felder enthält Exploit Erkennungsprotokollierung die folgenden Felder und Feldeinstellungen:

Exploit Treffererkennung

```
Name: ExD Hit Found
ID: ExD Hit Found
cs4Label: Process Name
cs4: Der Prozess, für den das Exploit erkannt wurde
cs5Label: Target GMT Offset
cs5: The GMT offset of the host generating the event in ISO 8601
duration format
cs6Label: Target OS
cs6: Das Betriebssystem des Hosts, der das Ereignis generiert
act: Detection ExD Hit
externalId: Der eindeutige HX Identifikator, der diesem Treffer
zugeordnet ist
Start: Zeitstempel, als das Exploit auf dem Zielhost erkannt wurde
categoryOutcome: /Success
categoryBehavior: /Found
categoryDeviceGroup: /IDS
categoryDeviceType: Exploit Detection
categoryObject: /Host
categorySignificance: /Compromise
categoryTechnique: Exploit
categoryTupleDescription: ExD hat den Hinweis einer
Kompromittierung gefunden
msg: Host <hostname> ExD compromise
```

Protokollfelder für Aktualisierungen des Sicherheitsinhalts

Der Endpoint Security protokolliert jedes Mal eine Nachricht, wenn ein neues Update von Sicherheitsinhalten vom DTI auf den Endpoint Security heruntergeladen wird. Zusätzlich zu den allgemeinen CEF Feldern enthalten Protokolle für Aktualisierungen des Sicherheitsinhalts die folgenden Felder und Feldeinstellungen:

WICHTIG: Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

Aktualisierungen des Sicherheitsinhalts

```
Time: Zeitstempel des Protokolleintrags
Name: Aktualisierter FireEye Sicherheitsinhalt
ID: Aktualisierter FireEye Sicherheitsinhalt
cs4Label: Security Content Version
cs4: Die Version des Sicherheitsinhalts, die der Server ausführt
cs5Label: Security Content Last Applied
cs5: Der Zeitstempel, wann der neueste Sicherheitsinhalt
angewendet wurde
categoryDeviceGroup: /IDS/Application/Service
categoryDeviceType: Forensic Investigation
categoryObject: /Host
categoryOutcome: /Success
categorySignificance: /Informational
categoryBehavior: /Modify/Content
categoryTupleDescription: Sicherheitsinhaltsversion <version>
angewendet um <timestamp>
act: Status des Sicherheitsinhalts
msg: Sicherheitsinhaltsversion <version> angewendet um <timestamp>
```

Protokollfelder für Malware Erkennung

Der Endpoint Security protokolliert Nachrichten, wenn Malware auf einem Zielhost gefunden wird. Neben den allgemeinen CEF-Feldern enthält Malware Erkennungsprotokollierung die folgenden Felder und Feldeinstellungen:

Malware Treffererkennung

```
Name: Malware Hit Found
ID: Malware Hit Found
cs4Label: Process Name
cs4: Der Prozess oder IOC, für den die Malware erkannt wurde
cs5Label: Target GMT Offset
cs5: Das GMT Offset des Hosts, der das Ereignis in ISO 8601
Dauerformat erstellt
cs6Label: Target OS
cs6: Das Betriebssystem des  Hosts, der das Ereignis generiert
cs7Label: Resolution
CS7: Der Name der Auflösung (z. B. ALERT oder QUARANTINED)
cs8Label: Alert Types
CS8: Malware, Spyware, Adware, Dialer, Pup, zipbomb
cs9Label: MD5
cs9: MD5 Hash des Malware Objekts
cs10Label: SHA1
cs10: SHA1 Hash des Malware Objekts
cs11Label: Malware Signature
cs11: Die Malware Signatur
cs12Label: Malware Category
cs12: Standort des Treffers -- Boot-Sektor, Verzeichnis oder
Vorgang. cs13Label: Malware Engine cs13=AV oder MG
act: Detection MAL Hit
externalId: Der eindeutige HX Identifikator, der diesem Treffer
zugeordnet ist
Start: Zeitstempel, als die Malware auf dem Zielhost erkannt wurde
categoryOutcome: /Success
categoryBehavior: /Found
categoryDeviceGroup: /IDS
categoryDeviceType: Malware Protection
categoryTechnique: Malware
categoryObject: /Host
categorySignificance: /Compromise
categoryTupleDescription: Der Malware Schutz hat eine
Kompromittierung gefunden
msg: Host <hostname> Malware alert
```

Protokollfelder für Malware Scans

Der Endpoint Security protokolliert Nachrichten, wenn ein Malware-Scan auf einem Endpoint-Host ausgeführt wird. Neben den allgemeinen CEF Felder enthält Malware Scanprotokollierung die folgenden Felder und Feldeinstellungen:

Malware Scan

```
Name: Malware Scan
ID: Malware Scan
cs2Label: Scan Type
cs2: Die Art des Malware Scans (vollständig, schnell oder
Speicher)
cs3Label: Scan Time Taken in Seconds
CS3: Die Scanzeit in Sekunden
cs4Label: Infected Objects Count
cs4: Die Anzahl der infizierten Objekte, die während des Scans
gefunden wurden
cs5Label: Actioned Objects Count
CS5: Die Anzahl der Objekte, für die eine Aktion ausgeführt wird
cs6Label: Scanned Objects Count
CS6: Die Anzahl der gescannten Objekte
cs7Label: Alert Correlation ID
cs7: Der Hash der Alarm ID
act: Malware Scan
msg: Host <host> Malware Scan
externalId:
start: Zeitstempel, wenn der Malware Scan auf dem Host Endpunkt
gestartet wurde
categoryOutcome: /Success
categoryBehavior: /Scan
categoryDeviceGroup: /IDS
categoryDeviceType: Malware Protection
categoryTechnique: Malware
categoryObject: /Host
categorySignificance: /Scan
categoryTupleDescription: Der Malware Scan wurde auf dem Host
durchgeführt.
```


Protokollfelder für automatische Korrektur von Malware

Der Endpoint Security protokolliert CEF Nachrichten, wenn der Agent auf einem Endpunkt-Host automatisch Malware Korrekturen für erkannte Malware durchführt. Die protokollierten CEF Einträge und Felder sind je nach den Ergebnissen des Malware Korrekturversuchs unterschiedlich.

- Datei in Quarantäne und bereinigt unten
- Datei in Quarantäne und bereinigt unten
- Datei in Quarantäne aber nicht gelöscht auf der nächsten Seite
- Protokollfelder für allgemeine Malware Korrektur auf der nächsten Seite

CEF Protokolleinträge werden auch geschrieben, wenn ein Benutzer versucht, eine Datei aus dem Malware Quarantänebereich zu löschen oder wiederherzustellen. Siehe Protokollfelder für Benutzeraktion der Quarantänedatei auf Seite 495. Darüber hinaus werden CEF Protokolleinträge geschrieben, wenn eine Datei aus dem Quarantänebereich entfernt wird. Siehe Protokollfelder für Quarantäne Dateialterung auf Seite 494

Datei in Quarantäne und bereinigt

Wenn eine infizierte Datei automatisch unter Quarantäne gestellt und bereinigt wird, schließt die Protokollierung der Korrektur neben den allgemeinen CEF Feldern und den allgemeinen Malware Korrektur CEF Feldern die folgenden Felder und Feldeinstellungen ein.

```
Name: FireEye Quarantine Completed
ID: FireEye Quarantine Completed
act: Quarantine <host> Cleaned
categoryTupleDescription: Quarantine task successfully completed,
file cleaned.
```

Datei in Quarantäne und bereinigt

Wenn eine infizierte Datei automatisch unter Quarantäne gestellt und gelöscht wird, schließt die Protokollierung der Malware Korrektur neben den allgemeinen CEF Feldern und den allgemeinen Malware Korrektur CEF Feldern die folgenden Felder und Feldeinstellungen ein.

```
Name: FireEye Quarantine Completed
ID: FireEye Quarantine Completed
act: Quarantine <host> Quarantined
categoryTupleDescription: Quarantäneaufgabe erfolgreich
```

```
abgeschlossen, Datei gelöscht.
```

Datei in Quarantäne aber nicht gelöscht

Wenn eine infizierte Datei automatisch unter Quarantäne gestellt aber nicht gelöscht werden kann, schließt die Protokollierung der Malware Korrektur neben den allgemeinen CEF Feldern und den allgemeinen Malware Korrektur CEF Feldern die folgenden Felder und Feldeinstellungen ein.

```
Name: FireEye Quarantine Failed
ID: FireEye Quarantine Failed
act: Quarantine <host> Quarantined
categoryTupleDescription: Die Quarantäneaufgabe konnte nicht
abgeschlossen werden.
```

Protokollfelder für allgemeine Malware Korrektur

Die folgenden Felder sind allen CEF Protokolleinträgen für die Malware Korrektur gemeinsam.

```
cs3Label: Quarantine Action
cs3: add
cs4Label: Quarantine ID
cs4: Die eindeutige ID für die Quarantäne
cs5Label: Correlation ID
CS5: Die Alarmkorrelations ID.
cs6Label: SHA1
cs6: Der SHA1 Hash der unter Quarantäne gestellten Datei
msg: Host <Host> Quarantäneaktion
filePath: Der vollständig qualifizierte Dateipfad der isolierten
und bereinigten Datei
fileHash: Der Datei Hash des unter Quarantäne stehenden
Dateinamens
fsize: Die Größe der unter Quarantäne stehenden Datei
start: Zeitstempel für den Start des Korrektursversuchs auf dem
Zielhost
categoryOutcome: /Success
categoryBehavior: /Access/Start
categoryDeviceGroup: /IDS/Application/Service
categoryDeviceType: Forensic Investigation
categoryObject: /Host
categorySignificance: /Informational
```

Protokollfelder für Quarantäne Dateialterung

Wenn eine Datei auf dem Quarantänebereich entfernt wird (wenn sie die Aufbewahrungsfrist für den Quarantänebereich überschreitet),umfasst Malware Protokollierung neben den allgemeinen CEF Feldern die folgenden Felder und Feldeinstellungen:

CEF Protokolleinträge werden auch geschrieben, wenn der Agent automatisch versucht, eine Malware Korrektur für eine Datei durchzuführen, in der Malware erkannt wurde. Siehe Protokollfelder für automatische Korrektur von Malware auf Seite 492. Darüber hinaus werden CEF Protokolleinträge geschrieben, wenn ein Benutzer versucht, eine Datei zu löschen oder wiederherzustellen, in der Malware entdeckt wurde. Siehe Protokollfelder für Benutzeraktion der Quarantänedatei auf der nächsten Seite.

```
Name: FireEye Quarantine Completed
 ID: FireEye Quarantine Completed
 cs3Label: Quarantine Action
 cs3: <purge | restore |restore_failed>
 cs4Label: Quarantine ID
 cs4: The unique ID for the quarantine
 cs5Label: Correlation ID
 CS5: Die Korrelations ID.
 cs6Label: SHA1
 CS6: Der SHA1 Hash
 act: Quarantine <host> <aged out | restored | restore failed>
 msg: Host <Host> Quarantäneaktion
 filePath: The fully qualified file path of the quarantined and
cleaned file
 fileHash: The file hash of the quarantined file name
 fsize: Die Größe der unter Quarantäne stehenden Datei
 start: Zeitstempel für den Start der Quarantäne Dateientfernung
 categoryOutcome: /Success
 categoryBehavior: /Access/Start
 categoryDeviceGroup: /IDS/Application/Service
 categoryDeviceType: Forensic Investigation
 categoryObject: /Host
 categorySignificance: /Informational
 categoryTupleDescription: Eine der folgenden Optionen:
<Quarantäne-Task erfolgreich abgeschlossen, Datei bereinigt |
Quarantäneaufgabe erfolgreich abgeschlossen, Datei gelöscht |
Quarantäneaufgabe konnte nicht abgeschlossen werden.>.
```


Protokollfelder für Benutzeraktion der Quarantänedatei

Wenn ein Benutzer versucht, eine Datei aus dem Malware Quarantänebereich zu löschen oder wiederherzustellen, werden CEF Protokollmeldungen geschrieben.

- Eine unter Quarantäne gestellte Datei löschen unten
- Eine unter Quarantäne stehende Datei wiederherstellen unten
- Allgemeine Felder für Benutzeraktion der Quarantänedatei auf der nächsten Seite

CEF Protokolleinträge werden auch geschrieben, wenn der Agent automatisch versucht, eine Malware Korrektur für eine Datei durchzuführen, in der Malware erkannt wurde. Siehe Protokollfelder für automatische Korrektur von Malware auf Seite 492. Darüber hinaus werden CEF Protokolleinträge geschrieben, wenn eine Datei aus dem Quarantänebereich entfernt wird. Siehe Protokollfelder für Quarantäne Dateialterung auf der vorherigen Seite

Eine unter Quarantäne gestellte Datei löschen

Wenn ein Benutzer versucht, eine unter Quarantäne stehende Datei zu löschen, umfasst die Malware Protokollierung neben den allgmeinen CEF-Felder und den allgemeinen Quarantänedatei Benutzeraktion Feldern die folgenden Felder und Feldeinstellungen:

```
cs3Label: Quarantine Action
CS3: löschen
request: https://<HX_HOSTNAME>:<HX_UI_PORT>/hx/api/v3/quarantines/
<quarantine_id>/delete
```

Eine unter Quarantäne stehende Datei wiederherstellen

Wenn ein Benutzer versucht, eine unter Quarantäne stehende Datei zu wiederherzustellen, umfasst die Malware Protokollierung neben den allgemeinen CEF-Felder und den allgemeinen Quarantänedatei Benutzeraktion Feldern die folgenden Felder und Feldeinstellungen:

```
cs3Label: Quarantine Action
CS3: Wiederherstellen
request: https://<HX_HOSTNAME>:<HX_UI_PORT>/hx/api/v3/quarantines/
<quarantine_id>/restore
```

Allgemeine Felder für Benutzeraktion der Quarantänedatei

Die folgenden Felder haben alle CEF Protokolleinträge für die Benutzeraktion der Quarantänedatei gemeinsam.

```
Name: FireEye Quarantine Request
ID: FireEye Quarantine Request
cs4Label: Quarantine ID
cs4: The unique ID for the quarantine
cs5Label: Target GMT Offset
cs5: The GMT offset of the host generating the event in ISO 8601
duration format
cs6Label: Target OS
cs6: Das Betriebssystem des Host, der das Ereignis oder den SHA1-
Hash generiert
act: Quarantine <host> request <Queued | Success | Failed>
msg: Host <host> quarantine request <Queued | Success | Failed>
externalId: Task-ID zum Verfolgen der angeforderten Aufgabe in der
Datenbank
start: Zeitstempel für den Start des Korrektursversuchs auf dem
Zielhost
categoryOutcome: </Success | /Failure>
categoryBehavior: <Queued | Success | Failed | /Access/Start>
categoryDeviceGroup: /IDS/Application/Service
categoryDeviceType: Forensic Investigation
categoryObject: /Host
categorySignificance: </Informational | /Informational/error>
categoryTupleDescription: <action> Anfrage.
```

Protokollfelder für falsch positiv Malware

Der Endpoint Security protokolliert Nachrichten, wenn Malware als falsch positiv markiert ist und wenn sie wieder in true positiv geändert wird. Neben den allgemeinen CEF Felder enthält Malware falsch positiv Protokollierung die folgenden Felder und Feldeinstellungen:

DTI-markierte falsch positive:

```
Name: FireEye False Positive Updated ID: FireEye False Positive
Updated cs1Label: False Positive action (differs from the common
CEF fields) cs1: mark_false_positive (differs from the common CEF
fields) cs2Label: condition (differs from the common CEF fields)
cs2: <condition that was marked false positive> (differs from the
common CEF fields) act: False Positive externalId: The HX unique
identifier associated with the false positive malware start:
Timestamp when the false positive was identified categoryOutcome:
/Success categoryBehavior: /Modify/Content categoryDeviceGroup:
/IDS/Application/Service categoryDeviceType: Forensic
Investigation categoryObject: /Host categorySignificance:
/Informational categoryTupleDescription: False Positive
6<externalid> mark_false_positive by mandiant msg: False Positive
<externalid> mark_false_positive by mandiant
```

Benutzerinitiierte falsch positive

Es wird kein CEF Protokoll aufgezeichnet, wenn ein Benutzer einen falschen positiven Zustand markiert oder unmarkiert. Die folgende informelle Protokollnachricht wird jedoch stattdessen in den Appliance Protokollen aufgezeichnet:

```
False Positive action taken on malware alerts. Filter: <false-
positive-filter-ID> is <marked False Positive | no longer a False
Positive> by user <user>
```

Protokollfelder für Triage und Dateierfassung

Wenn Triagen oder Dateierfassungen angefordert werden, werden CEF Protokollnachrichten geschrieben.

Acquisition Queued (Akquisition in Warteschlange)

Wenn eine Triage- oder Dateierfassungsanfrage in die Warteschlange gestellt wird, enthalten CEF Protokollnachrichten neben den allgemeinen CEF Feldern und den allgemeinen Triage und Dateierfassung Feldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Acquisition Queued
ID: FireEye Acquisition Queued
act: Acquisition Create
suser: Benutzername, der die Aquisition angefordert hat
```

Acquisition Started (Akquisition begonnen)

Wenn eine Triage- oder Dateierfassungsanfrage gestartet wird, schließen CEF Protokollnachrichten neben den allgemeinen CEF Feldern und den allgemeinen Tirage und Dateierfassung Feldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Acquisition Started
ID: FireEye Acquisition Started
act: Acquisition Status
suser: Benutzername, der die Akquisition gestartet hat
```

Acquisition Completed (Akquisition abgeschlossen)

Wenn eine Triage- oder Dateierfassungsanfrage abgeschlossen ist, enthalten CEF Protokollnachrichten neben den allgemeinen CEF Feldern und den allgemeinen Triage und Dateierfassung Feldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Acquisition Completed
ID: FireEye Acquisition Completed
act: Acquisition Status
suser: Benutzername, der die Akquisition abgeschlossen hat
```

```
in: Größe des resultierenden Erfassungspakets (in Byte)
request: Direct URL of acquisition package
```

Allgemeine Triage und Dateierfassung Felder

Die folgenden Felder haben alle CEF Protokolleinträge für die Triage und Dateierfassungen gemeinsam.

```
categoryBehavior: /Create (für Created, Queued, Started),
/Access/Start (for Completed)
categoryDeviceGroup: /IDS/Application/Service
categoryDeviceType: Forensic Investigation
categoryObject: /Host
categorySignificance: /Informatorisch
categoryTupleDescription: Ereignisbeschreibung
deviceCustomDate2Label: Triage Request Timestamp
deviceCustomDate2: Der mit der Triageerfassung verbundene
angeforderte Zeitstempel
cs3Label: Script Name
cs3: Name des Akquisitionsscripts, der auf dem Zielhost ausgeführt
wird:Triage, Timestamped Triage, API File Acquisition, Raw File
Acquisition, Live Response Acquisition, Custom Acquisition, Bulk
Acquisition oder Agent Diagnostic
cs4Label: Original Request ID
cs4: Die mit einer Triageanfrage eingeschlossene Ereignis  ID (von
einem SIEM Benutzer)
cs5Label: Target GMT Offset
cs5: The GMT offset of the host generating the event in ISO 8601
duration format
cs6Label: Target OS
cs6: Das Betriebssystem des  Hosts, der das Ereignis generiert
externalId: Die einzigartige HX ID für die Aquisitionsanfrage
fname: Der angeforderte Dateiname für die Dateierfassung
filePath: Der angeforderte vollständige Pfadname für eine
Dateierfassung
msg: Eine Textbeschreibung des Ereignisses
```

Protokollfelder für Eindämmungsaktionen

Der Endpoint Security protokolliert Nachrichten, wenn Eindämmung angefordert, aktiviert und von einem Zielhost entfernt wurde.

Eindämmung angefordert

Wenn die Eindämmung angefordert wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Felder und den allgemeinen Containment Felder die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Requested
ID: FireEye Containment Requested
act: Containment Requested
request: URL an Zielhost in HX
suser: Benutzername, der die Containment anfordert msg: Host
<Hostname> containment requested by <user>
```

Eindämmungsanfrage abgebrochen

Wenn eine Eindämmungsanfrage abgebrochen wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Cancelled
ID: FireEye Containment cancelled
act: Containment Request Cancelled
request: URL an Zielhost in HX
suser: Benutzername, der die Stop Containment Anfrage genehmigt
msg: Host <hostname> containment request cancelled by <user>
```

Containment Approved

Wenn die Eindämmung genehmigt wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Approved
ID: FireEye Containment Approved
act: Containment Approved
request: URL an Zielhost in HX
suser: Benutzername, der die Containment  genehmigt msg: Host
<hostname> containment approved by <user>
```

Eindämmung in Warteschlange

Wenn Eindämmung in die Warteschlange gestellt wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

Dies zeigt den Beginn der Wartung einer Eindämmungsanfrage an.

```
Name: FireEye Containment Queued
ID: FireEye Containment Queued
act: Containment Status
request: URL an Zielhost in HX
cs3Label: Containment action
cs3: contain msg: Host <hostname ><action> queued
```

Eindämmung gestartet

Wenn die Eindämmung gestartet wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Started
ID: FireEye Containment Started
act: Containment Status
request: URL an Zielhost in HX
```

```
cs3Label: Containment action
cs3: contain msg: Host <hostname> <action> started
```

Eindämmung abgeschlossen

Wenn die Eindämmung abgeschlossen ist, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Completed
ID: FireEye Containment Completed
act: Containment Status
request: URL an Zielhost in HX
cs3Label: Containment action
cs3: contain msg: Hostname <hostname> <action> completed
```

Eindämmungsfehler

Wenn ein Fehler für eine Eindämmungaanfrage auftritt, weil Eindämmung nicht aktiviert ist, der Host von dem Eindämmungssatz ausgeschlossen ist oder weil eine ungültige Aufrüstungsversion festgestellt wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Error
ID: FireEye Containment Error
act: Containment Status
request: URL an Zielhost in HX
suser: Benutzername, der der Eindämmungsanfrage zugeordnet ist
msg: Host <Hostname> <Aktion> failed
```

Containment Failed

Wenn eine Eindämmungsanfrage fehlschlägt, weil ein Fehler beim Abruf von Payloads auftritt, die Ergebnisse in einem falschen Ausgabeformat vorliegen oder weil das Ergebnis einen unerwarteten Containment Status zurückgegeben hat, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Failed
ID: FireEye Containment Failed
act: Containment Status
request: URL an Zielhost in HX
suser: Benutzername, der der Eindämmungsanfrage zugeordnet ist
msg: Host <Hostname> <Aktion> failed
```

Eindämmung abgebrochen

Wenn eine Eindämmungsanfrage abgebrochen wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen

Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Aborted
ID: FireEye Containment Aborted
act: Containment Status
request: URL an Zielhost in HX
suser: Benutzername, der der Eindämmungsanfrage zugeordnet ist
msg: Host <Hostname> <Aktion> aborted
```

Aufhebung der Eindämmung genehmigt

Wenn ein Versuch, einen Host von der Eindämmung zu entfernen genehmigt wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Stop Containment Approval
ID: FireEye Containment Started
act: Stop Containment Approved
request: URL an Zielhost in HX
suser: Benutzername, der die Stop Containment Anfrage genehmigt
msg: Host <hostname> stop containment approved by <user>
```

Aufhebung der Eindämmung in Warteschlange

Wenn ein Versuch, einen Host von der Eindämmung zu entfernen in eine Warteschlange gestellt wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Queued
ID: FireEye Containment Queued
act: Containment Status
request: URL an Zielhost in HX
cs3Label: Containment action
cs3: uncontain msg: Host <hostname ><action> queued
```

Aufhebung der Eindämmung gestartet

Wenn ein Versuch gestartet wird, einen Host von der Eindämmung zu entfernen, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Feldern und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Started
ID: FireEye Containment Started
act: Containment Status
request: URL an Zielhost in HX
cs3Label: Containment action
cs3: uncontain msg: Host <hostname ><action> started
```

Aufhebung der Eindämmung abgeschlossen

Wenn ein Versuch, einen Host von der Eindämmung zu entfernen abgeschlossen ist, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Felder und den

allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Completed
ID: FireEye Containment Completed
act: Containment Status
request: URL an Zielhost in HX
cs3Label: Containment action
cs3: uncontain msg: Host <hostname ><action> completed
```

Aufhebung der Eindämmung abgebrochen

Wenn eine Anfrage für die Aufhebung der Eindämmung abgebrochen wird, enthalten die CEF Protokollmeldungen neben den allgemeinen CEF Felder und den allgemeinen Eindämmungsfeldern die folgenden Felder und Feldeinstellungen:

```
Name: FireEye Containment Aborted
ID: FireEye Containment Aborted
act: Containment Status
request: URL an Zielhost in HX
suser: User name associated with the containment request msg: Host
<hostname> <action> aborted
```

Häufige Eindämmungsprotokollfelder

Die folgenden Felder gelten für alle Containment und Uncontainment CEF Protokolleinträge.

```
cs5Label: Target GMT Offset
cs5: Das GMT Offset des Hosts, der das Ereignis in ISO 8601
Dauerformat erstellt
cs6Label: Target OS
cs6: Das Betriebssystem des  Hosts, der das Ereignis generiert
categoryBehavior: /Create (für Created, Queued, Started),
/Access/Start (für Completed)
categoryDeviceGroup: /IDS/Application/Service
categoryDeviceType: Forensische Untersuchung
categoryObject: /Host categoryOutcome: /Success/Failure
categorySignificance: /Informational/Error
categoryTupleDescription: Ereignisbeschreibung
```

Technischer Support

Für technische Unterstützung wenden Sie sich an FireEye über das Support Portal:

https://csportal.fireeye.com

Dokumentation

Dokumentation für alle FireEye Produkte ist im FireEye Dokumentationsportal (Anmeldung erforderlich) verfügbar.

https://docs.fireeye.com/

FireEye, Inc.| 601 McCarthy Blvd. | Milpitas, CA | 1.408.321.6300 | 1.877.FIREEYE | www.fireeye.com