6 gute Gründe SentinelOne Endpoint Security genauer unter die Lupe zu nehmen

Intelligenz direkt auf dem Endpoint | Entgegen des allgemeinen Trends, die Bedrohungsanalyse auf externe Systeme auszulagern (Cloud, Sandbox, usw.), untersuchen wir sämtliche Vorgänge direkt auf dem jeweiligen Endgerät – egal ob Server, Workstation oder virtuelle Umgebung.

Vorteil:
Die Analyse findet direkt auf dem Zielsystem statt, also in „natürlicher Umgebung" der Malware. Dadurch vermeiden wir, dass die Schadsoftware inaktiv bleibt, sich sozusagen „schlafen legt", weil sie erkennt, dass sie nicht auf einem realen Endpoint, sondern in einer „vorgegaukelten" Umgebung ausgeführt wird. Zudem kann auch eine mögliche Reaktion direkt und in Echtzeit erfolgen, da nicht erst die Beurteilung eines externen Systems abgewartet werden muss.

On-premise, Cloud oder Hybrid | Da die Intelligenz im Wesentlichen direkt auf dem Endpunkt verortet ist, können Sie entscheiden, ob Ihr Managementsystem „On-premise" oder in der „Cloud" betrieben werden soll. Eine Hybri-dlösung ist natürlich ebenfalls möglich.

Vorteil:
Kritische Infrastrukturen - wie zum Beispiel Banken - erlauben in der Regel keine Cloud-Infrastruktur. Mit SentinelOne „On-premise" ist das kein Problem!

Ein schlanker Agent | Es gibt einen Agenten für Windows, MacOS und Linux; egal ob Laptop, Workstation, Server, virtualisierte Infrastruktur oder dergleichen. Der Agent selbst ist äußerst schlank und benötigt lediglich 1-2% CPU Performance.

Vorteil:
einfacher und flexibler Betrieb mit nahezu unbegrenzten Einsatzmöglich-keiten - z. B. auch auf Produktions- und Kassensystemen. Das Lizenzmodell ist dabei äußerst unkompliziert und überschaubar.

SentinelOne™

6 gute Gründe SentinelOne Endpoint Security genauer unter die Lupe zu nehmen

Endpoint Detect & Response - ActiveEDR | Der installierte Agent (kein weiterer Agent notwendig) kann in Sekunden um EDR-Funktionalitäten erweitert werden.

Vorteil:
Es steht zusätzlich eine Vielzahl an forensischen Daten zur Verfügung, um tiefergehende Analysen auch „post mortem" und über längere Zeiträume hinweg ausführen zu können (Stichwort Threat Hunting, IOC-Search, usw.), die gerade in modernen SOCs benötigt werden. Zudem können Systeme auf Knopfdruck in gesäubertem Zustand wiederhergestellt werden, ohne neu installiert zu werden (selektiver Roll-Back).

Mandantenfähigkeit | Es können innerhalb eines Managementsystems mehrere Mandanten (Sites) angelegt und diese mit separaten Regelwerken versehen werden.

Vorteil:
Saubere Segmentierung innerhalb verteilter Unternehmen, oder auch die Trennung von Produktion und Office. Darüber hinaus auch interessant für MSSPs, um unterschiedliche Kunden zentral zu verwalten.

Integrierbarkeit (API) | Ihnen steht eine sauber dokumentierte, offene REST API zur Anbindung und Integration bereits bestehender Systeme zur Verfügung.

Vorteil:
Kann in bestehende Systeme wie SIEM, NAC, Firewalls etc. integriert werden. Fertige Konnektoren für diverse Anbieter stehen bereits zur Verfügung (Fortinet, Splunk, uvm.)