Office 365 E-Mail Security Webinar
18. & 23. März 2021

xorlab

Your employees are your early warning system – use it.

Avantec webinar series on O365 email security | March 2021

Adrian Kyburz, adrian.kyburz@xorlab.com

Spinoff ETH zürich

Quick introduction

About me

- Adrian Kyburz
- MSc. ETH Computer Science
- Joined xorlab in 2017 as Head of Sales

About xorlab

- Founded 2015 as ETH spin-off
- First product: hard-to-evade sandbox
- Now: machine-intelligent communication defense

AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

Reality check: attackers bypass defenses and people click

1) Results from a recent attack simulation on O365 with Advanced Threat Protection (ATP 2)

	Simulated cases	Delivered to user mailbox	Delivered to Junk
Phishing	84	47	37
Malware	27	13	14
BEC & Fraud	6	2	4
Extortion	1	1	0
Total	118	63	55

Source: xorlab, simulating attackers with a budget of 50 USD per month

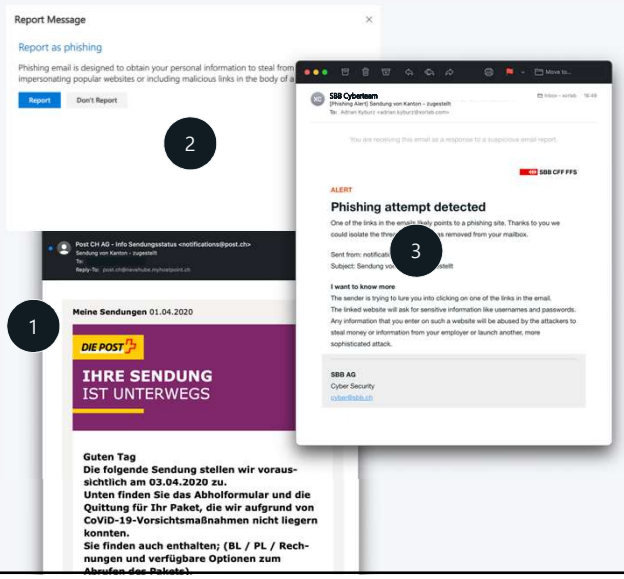
2) Findings from a not yet published ETH study

- Phishing works! 32% of the recipients of phishing clicked at least once and 25% completed the malicious action (submitted credentials, downloaded malware, …)
- There's hope! 30% of malicious messages get reported within 30' of delivery.

Source: ETH Zürich, large-scale phishing study

What if your users could warn each other?

xorlab ActiveGuard: Automated User Incident Response



Benefits

Lower risk of compromise

Medium-sized bank reduced incident resolution time from 27 hours to 2 minutes.

Lower cost of operations

1 existing customer with 5'000 employees saved 1.5 FTE through automation and reduced analysis effort for high-risk incidents.

True employee engagement

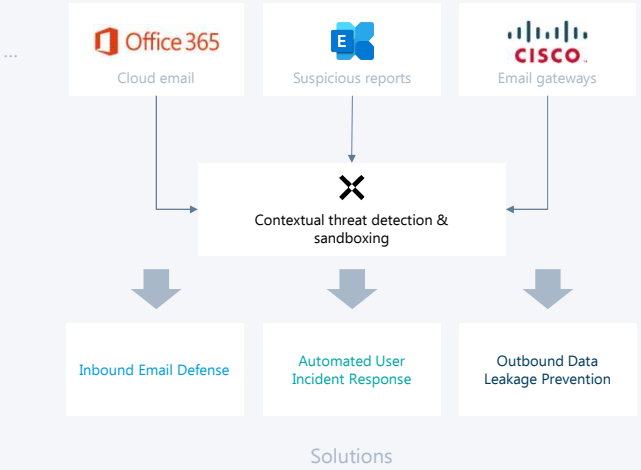
Users get fast response to their report and by that are motivated to stay engaged.

AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

The ActiveGuard platform

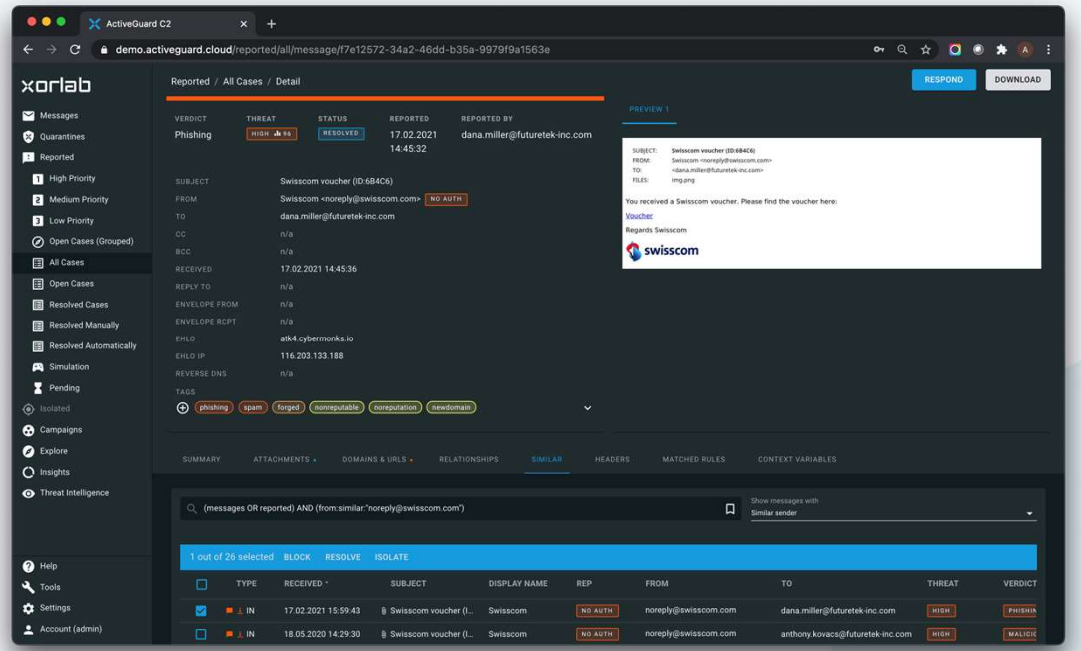
xorlab matches the risk profile of every email against the behavioral norms of your organization in real-time to detect attacks at first sight.



xorlab ActiveGuard is a proactive communications defense platform that continuously measures the risk of emails and other messages that flow in and out of your organizations using machine-intelligence and advanced payload analysis.

Applications

- Automated mailbox incident analysis, orchestration and response
- Low-maintenance inbound email threat filtering
- Outbound data leakage prevention



AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

Summary

	xorlab ActiveGuard Email Defense Platform	Microsoft Office 365 Security & Compliance Center
User incident submissions	✓ Through plugin	✓ Through Microsoft plugin
End-user feedback	✓ Instant, always	✗ Not available
Customizable feedback templates	✓ Yes	✗ Not available
Workflow automation	✓ Yes	✗ Not available
Intuitive and efficient user interface	✓ Yes	✗ Cumbersome

xorlab

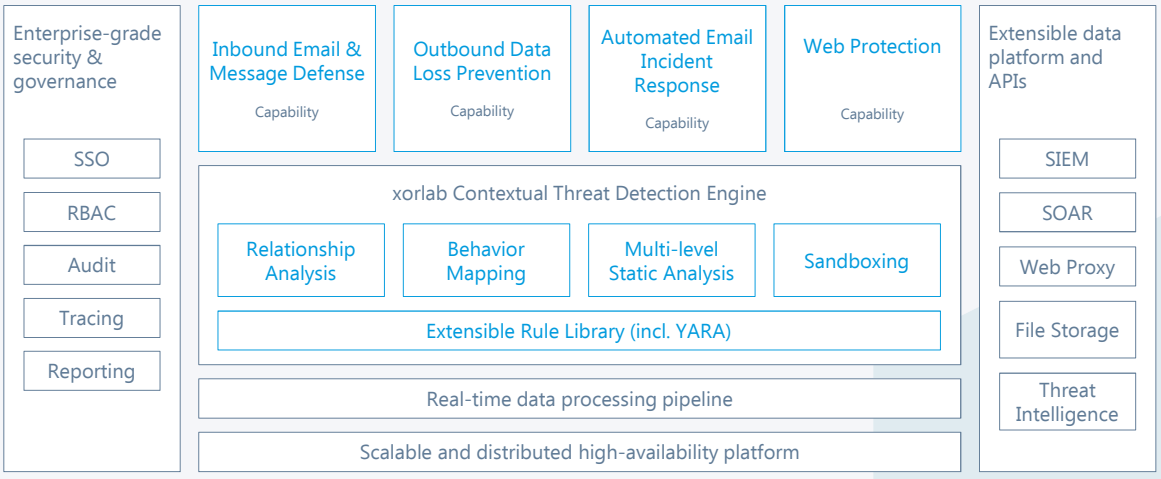
Machine-intelligent email defense for modern organizations

Spinoff ETH zürich

AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

ActiveGuard Defense Platform



Deployment options

AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

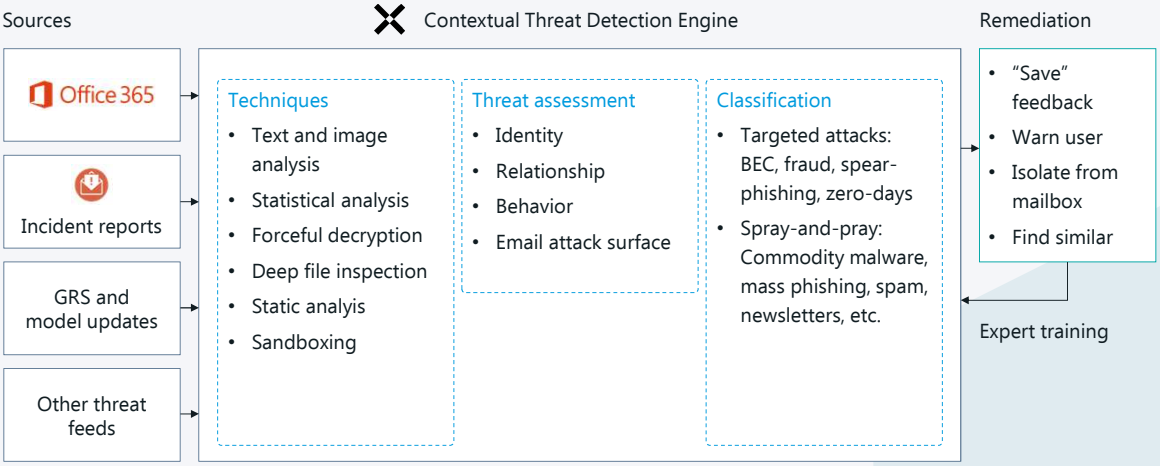
Automated incident analysis, orchestration and response

Benefits compared to alternative solutions

	Customized processes and tools (e.g. ticketing, shared mailboxes)	Phishing Simulation and Triage Tools	xorlab ActiveGuard Email Defense Platform	CISO benefit
Time to detect / time to respond	Very slow – Incident prioritization and threat analysis are manual.	Slow – Incident prioritization & analysis use reactive threat intel.	Fast – Proactive threat analysis enables accurate prioritization and fast response.	Significant reduction of risk of compromise
Analyst efficiency and automation	Inefficient – Threat analysis is manual, and nothing can be automated.	Medium – Lack of local context hinders analysis and limits automation potential.	High – Local context information speeds up analysis and unlocks full automation potential.	Cost savings through automation and faster analysis of high-risk incidents
Security engagement	Inexistent – Feedback delays make people stop reporting incidents.	Low – Lack of local context leads to generic feedbacks. People stop reporting incidents.	High – Automatic, timely, contextual feedback effectively engages people in the long run.	CISO organization is perceived as a responsive enabler

Automated incident analysis, orchestration and response

Solution description

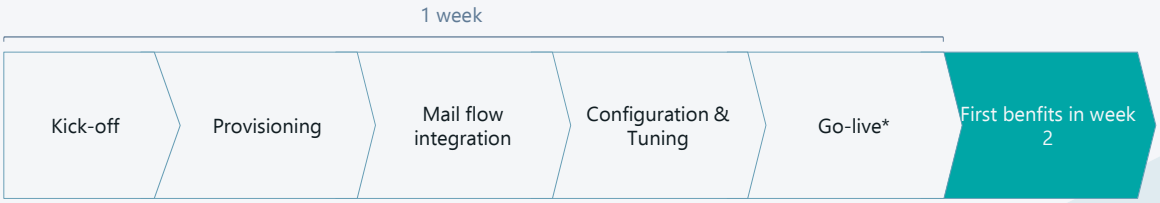


AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

First benefits in week 2

Our battle-tested, 1 week rollout plan to automate the collection, analysis and response to user reported suspicious email



- Analysis and discussion of requirements
- Implementation concept

- Provisioning of customer Cloud instance by xorlab

- Integration of mail flow with ActiveGuard:
  - Setup BCC monitoring
  - Connect reporting interfaces

- User response templates
- Email routing topology

- Training of customer team
- Handover to customer organization

- Earlier detection thanks to more visibility
- Lower incident resolution time
- Spotlight on security

* We recommend to run an internal promotion campaign prior to going live

Activities required on the customer side

Integration

- Relay copies of incoming and outgoing emails to xorlab
  - xorlab recommends to install a BCC copy rule on the outermost gateway
- Report button integration

Effort: max. 4h incl. testing

Configuration & tuning

- Mail routing topology
- VIP configuration
- Protected domain setup
- Response templates

Effort: max 1d

Analyst training

- How to resolve cases?
- How to track campaigns?
- How to automate?

Effort: 2h

AVANTEC
Competence. Security. Trust.