Zscaler Business Update
05. März 2024

Cyber Defense – Teil 2

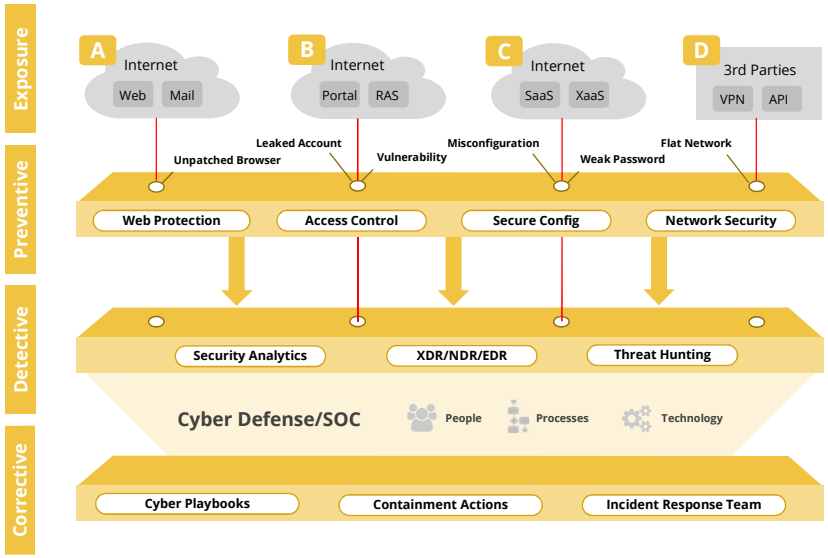
Mike Thurnherr
Cyber Defense Specialist
thurnherr@avantec.ch

Agenda

1. Bezug zu Bewältigungsstrategie
2. Zscaler Integration Ecosystem
3. Zscaler Integrationsmöglichkeiten
4. XDR - Extended Detection & Response
5. XDR - Requirements

Zscaler Business Update
05. März 2024

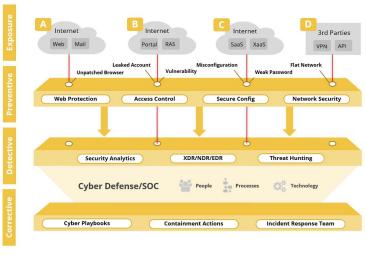
Bewältigungsstrategie



1) Es ist davon auszugehen, dass Angreifer vorhandene Schwachstellen ausnutzen
2) Neben präventiven Massnahmen sind detektive Massnahmen unerlässlich
3) Gezielter Beizung externer Cyber Defense Leistungen, um Lücken im Sicherheits-dispositiv zu schliessen

Einordnung Zscaler - Bewältigungsstrategie

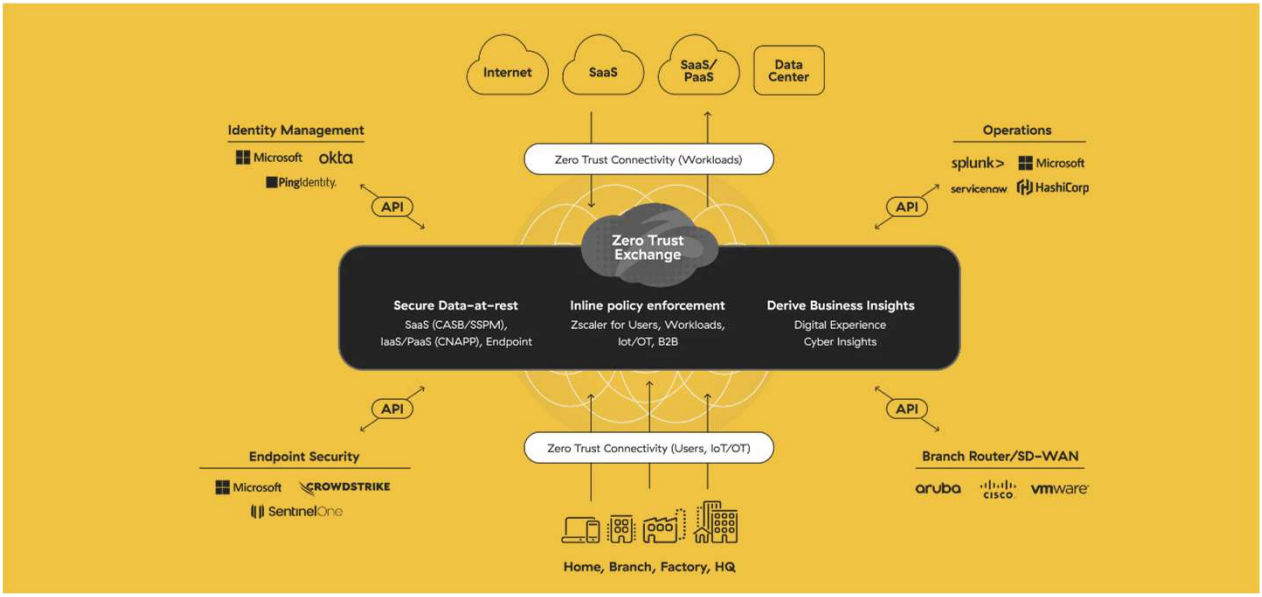
	Preventive	Detective
ZIA	1) URL & Cloud App Control 2) Browser Control 3) Browser Isolation 4) File Type Control 5) DLP 6) MFA AuthN / SAML / SCIM 7) Zero Trust Exchange	1) Traffic Inspection 2) Sandbox 3) Log Streaming 4) Alerting
ZPA	1) App based Access Control 2) Cloud Apps and On-Prem 3) Client-less Privilege Remote Access 4) Browser Isolation 5) MFA AuthN / SAML / SCIM 6) Zero Trust Exchange	1) Log Streaming 2) PRA Session Monitoring



Zscaler Business Update
05. März 2024

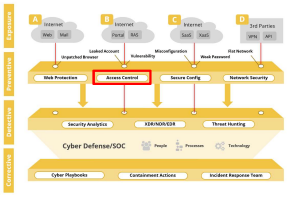
Zscaler Integration Ecosystem

AVANTEC
Competence. Security. Trust.

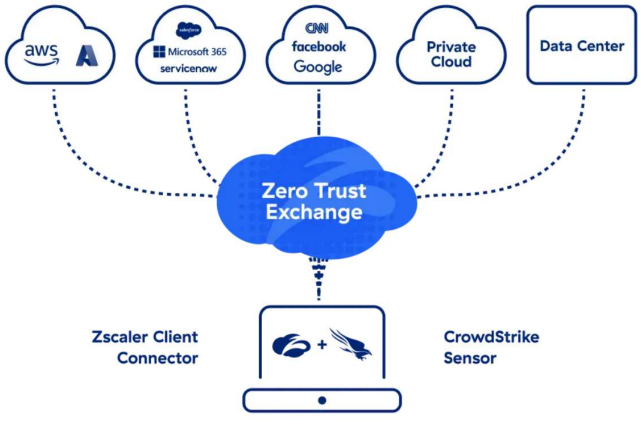


Integration #1 – Zero Trust mit Device Posture

AVANTEC
Competence. Security. Trust.



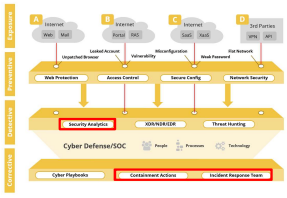
Zscaler ZIA und ZPA ermöglicht die Nutzung von CrowdStrike's ZTA (Zero Trust Assessment) Score, um den Zugang zu definierbaren Ressourcen zu kontrollieren.

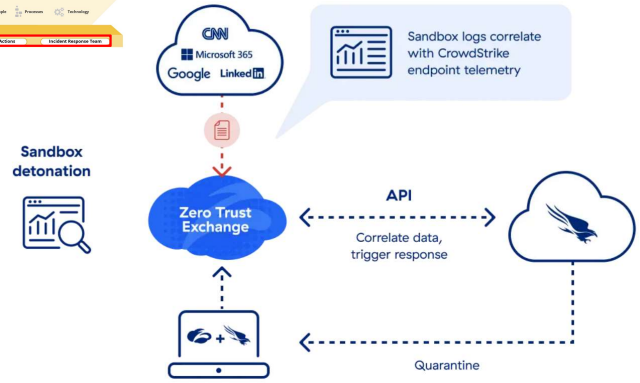


AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

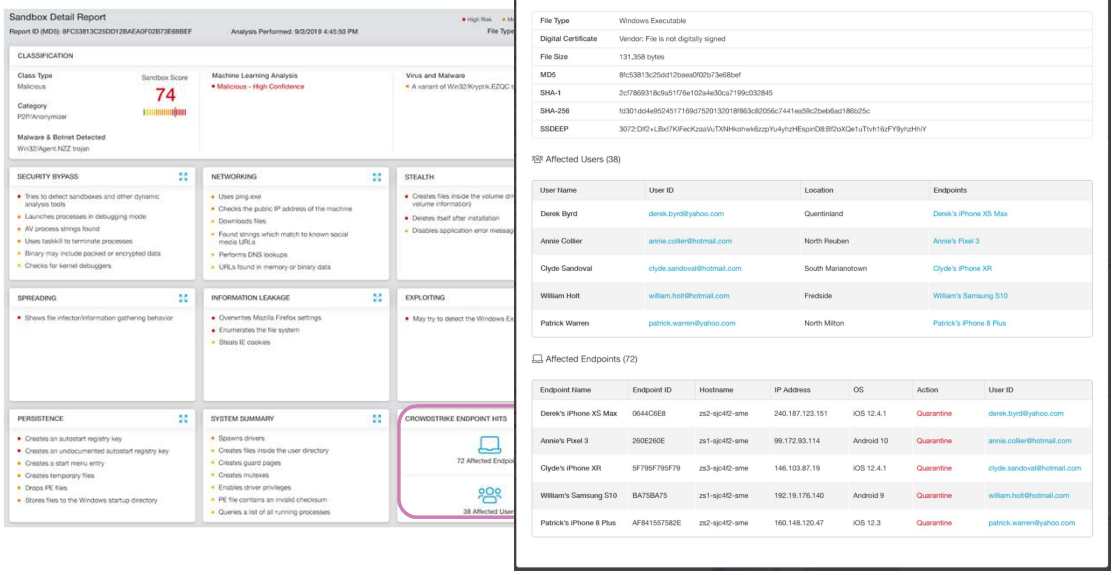
Integration #2 – Advanced Threat Detection mit ZIA Sandbox





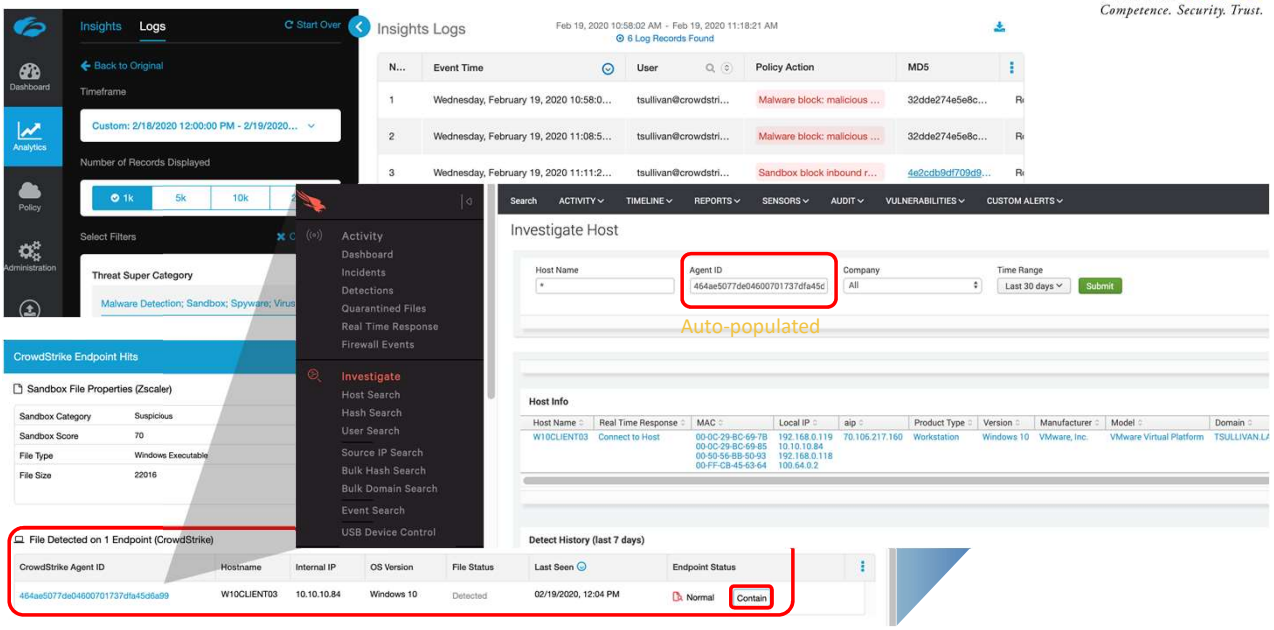
Zscaler Sandbox Logs werden mit den gesammelten CrowdStrike Telemetriedaten abgeglichen. Das ermöglicht eine schnelle Übersicht über betroffene Hosts und eine Host Isolation direkt aus dem Zscaler Admin UI.

Integration #2 – Advanced Threat Detection mit ZIA Sandbox

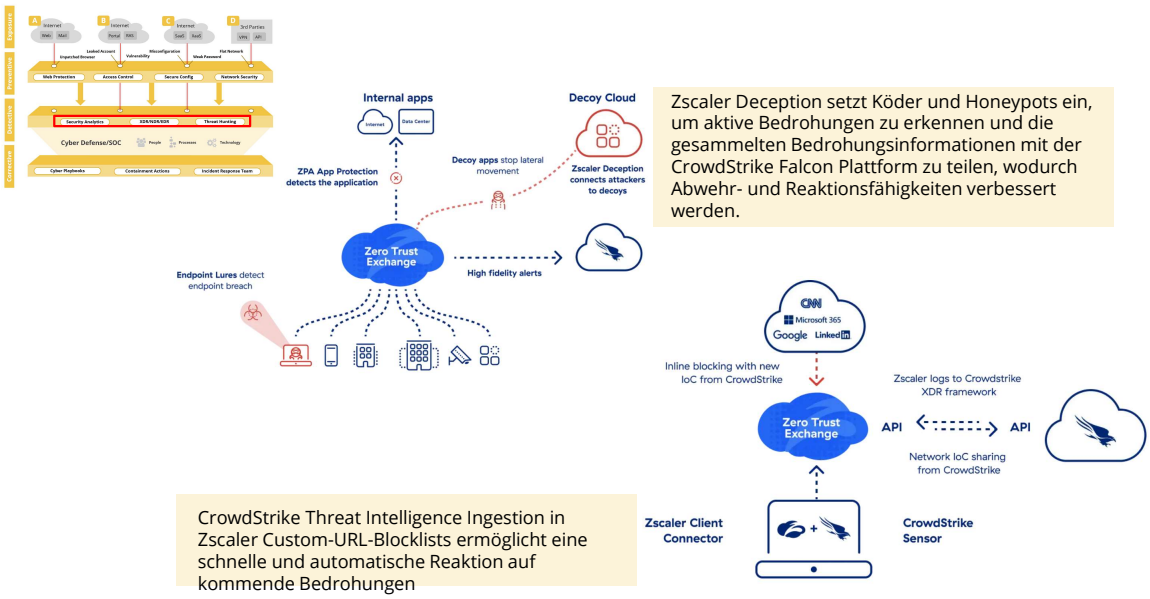


Zscaler Business Update
05. März 2024

Integration #2 – Advanced Threat Detection mit ZIA Sandbox



Integration #3 – Threat Intelligence sharing



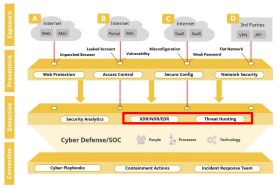
Zscaler Deception setzt Köder und Honeypots ein, um aktive Bedrohungen zu erkennen und die gesammelten Bedrohungsinformationen mit der CrowdStrike Falcon Plattform zu teilen, wodurch Abwehr- und Reaktionsfähigkeiten verbessert werden.

CrowdStrike Threat Intelligence Ingestion in Zscaler Custom-URL-Blocklists ermöglicht eine schnelle und automatische Reaktion auf kommende Bedrohungen

AVANTEC
Competence. Security. Trust.

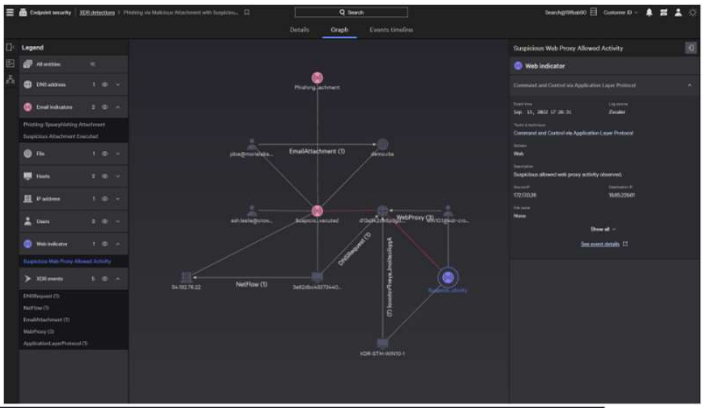
Zscaler Business Update
05. März 2024

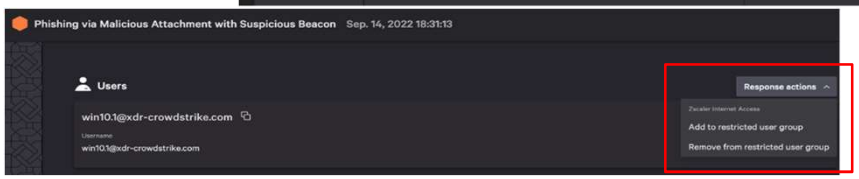
Integration #4 – XDR Detection



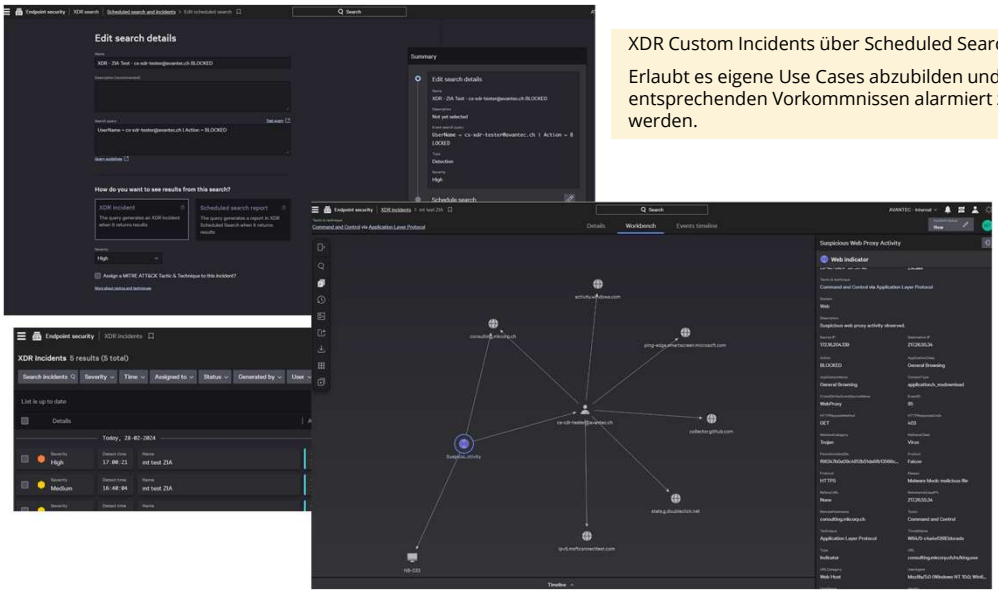
XDR bietet Detection Handling und Log Analyse über eine einzige zentrale Konsole. Zscaler Logs werden über Cloud NSS zu CrowdStrike transferiert.

Schnelle Reaktion bei Detection durch die Nutzung von Response Action.





Integration #4 – XDR Custom Incidents



XDR Custom Incidents über Scheduled Searches.

Erlaubt es eigene Use Cases abzubilden und bei entsprechenden Vorkommnissen alarmiert zu werden.

Zscaler Business Update
05. März 2024

XDR Integration - Requirements

AVANTEC
Competence. Security. Trust.

Lizenzen

- Zscaler Cloud NSS Feeds (nicht in standard NSS Lizenz enthalten)
- CrowdStrike XDR Connector - SSE (SWG & CASB)
- CrowdStrike Falcon Insight XDR

Technische Voraussetzungen

- Zscaler User AuthN über IdP mit SCIM (für XDR Response Action)

AVANTEC
Competence. Security. Trust.

DANKE