Zscaler Technical Update
25. Januar 2023

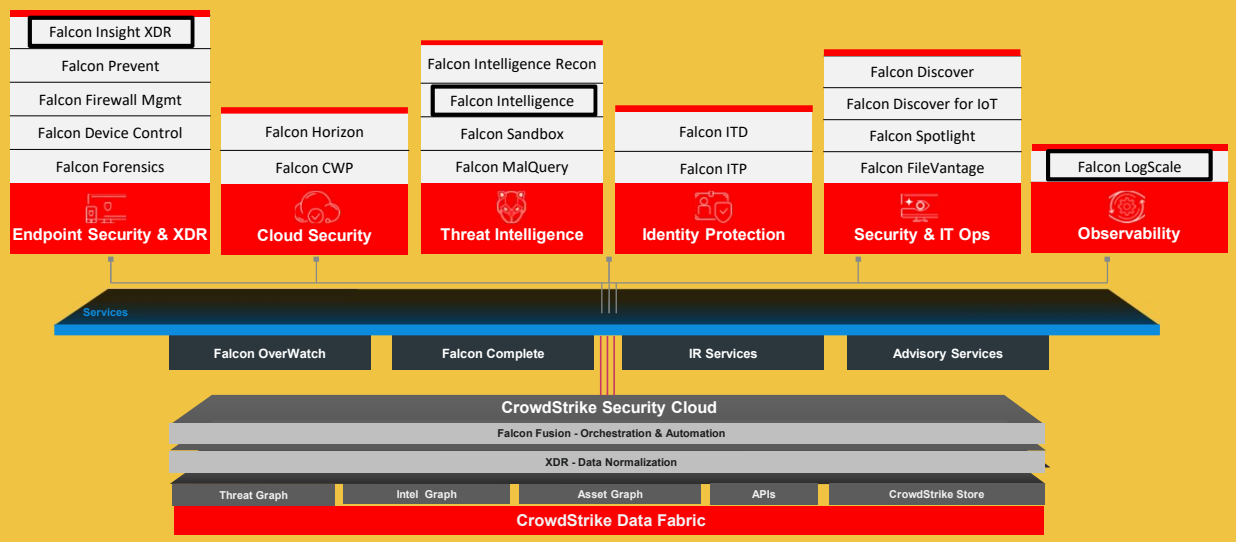
AVANTEC
Competence. Security. Trust.

Integration Zscaler und CrowdStrike

Mike Thurnherr
Senior Security Engineer
thurnherr@avantec.ch

CrowdStrike Falcon Platform

AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

Übersicht – Mögliche Integrationen

AVANTEC
Competence. Security. Trust.

- ZIA & ZPA – Posture Check Integration mit CrowdStrike ZTA
- ZPA – Posture Check Integration (ohne ZTA)
- ZIA – Sandbox Integration
- ZIA – Threat Intelligence Sharing
- ZIA & ZPA – NSS Logs Integration mit Falcon LogScale
- ZIA – Falcon XDR Integration

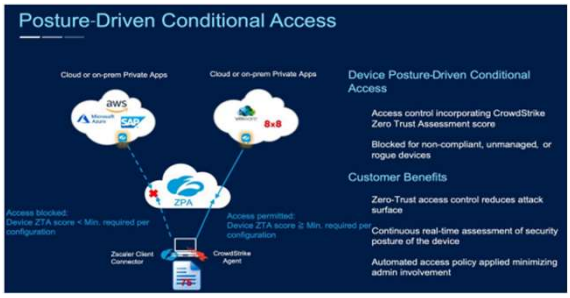
ZIA & ZPA – Posture Check Integration mit CrowdStrike ZTA

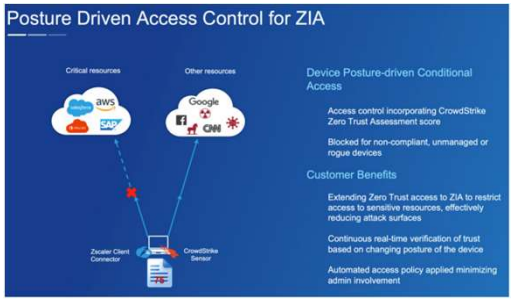
AVANTEC
Competence. Security. Trust.

- **ZIA** – Kontrollierter Zugang zu Saas Services
- **ZPA** – Kontrollierter Zugang zu definierten On-Prem oder Cloud Apps
- **ZTA** – CrowdStrike Zero Trust Assessment > Access nur ab 75 Punkten

Host ID	Hostname	Platform	Host type	Score version	Last updated	OS assessment	Sensor assessment	Overall assessment
1906dfc15e434caaa759aae2d8bba213	TECHIE-N0-MT-V2	Windows	Workstation	3.6.0	2023-01-11 19:49:58	88	100	96
22cc4f610b7045f4b25a21fe2ab804db	WIN10-CS-PREV	Windows	Workstation	3.5.1	2022-11-25 06:31:10	84	100	87

Host ID	Hostname	Platform	Host type	Score version	Last updated	OS assessment	Sensor assessment	Overall assessment
b54162aa36c948e4b15e5ee75a1d16a8	WIN10-CS-MON	Windows	Workstation	3.5.1	2022-11-25 08:12:36	64	26	39
4e89eff6ffdc4aeba3b7f84a76cab280	WINSRV2019	Windows	Server	3.6.0	2023-01-06 11:47:09	63	26	38





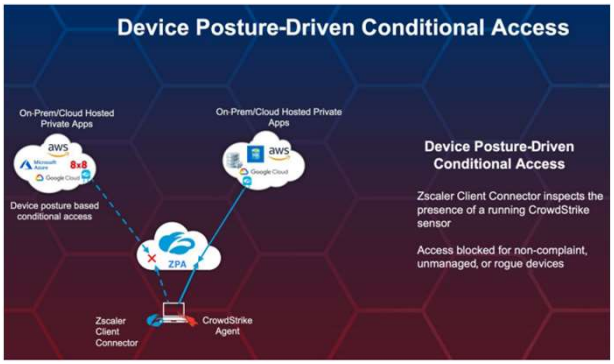
AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

ZPA – Posture Check Integration (ohne ZTA)

AVANTEC
Competence. Security. Trust.

- Zscaler Client Connector prüft ob CrowdStrike Sensor läuft
  - Falls nicht > Access denied
- ZTA wird nicht verwendet
- Nur möglich mit ZPA



ZPA – Posture Check Integration (ohne ZTA)

AVANTEC
Competence. Security. Trust.

- Demo Video ZPA_PostureCheck.mp4

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

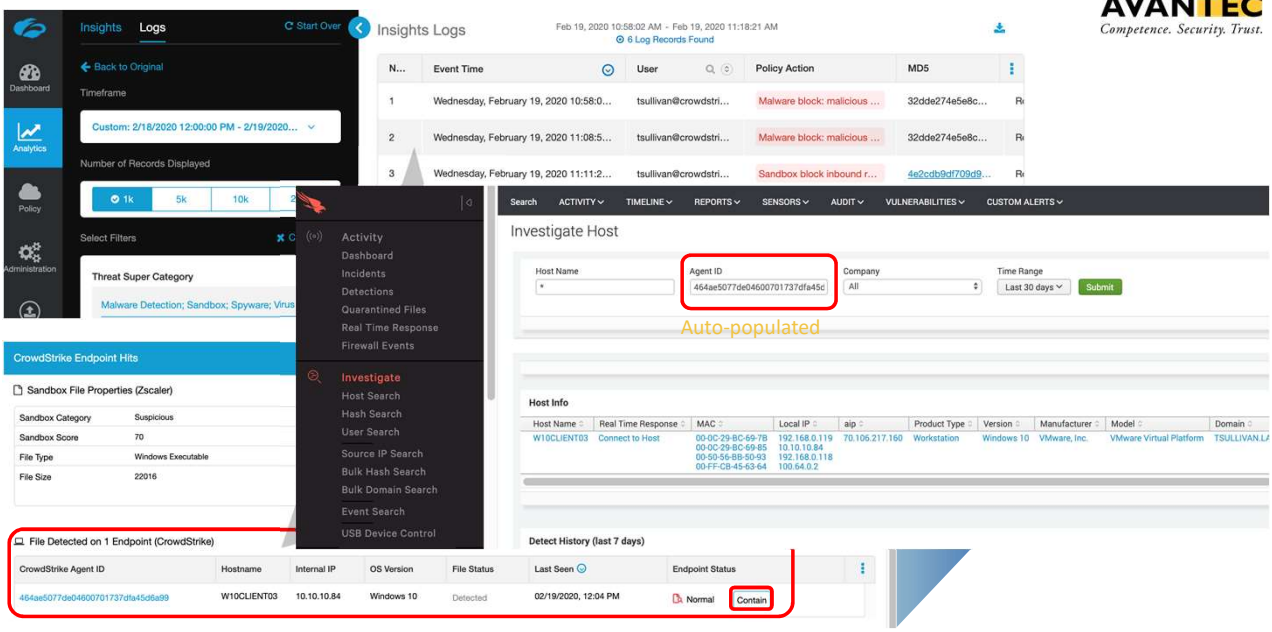
ZIA – Sandbox Integration

AVANTEC
Competence. Security. Trust.

- Setzt Zscaler Advanced Sandbox und CrowdStrike Insight voraus
- Malware in Zscaler Sandbox detoniert
- Threat Data wird mit CrowdStrike Sensor Metadata abgeglichen

ZIA – Sandbox Integration

AVANTEC
Competence. Security. Trust.

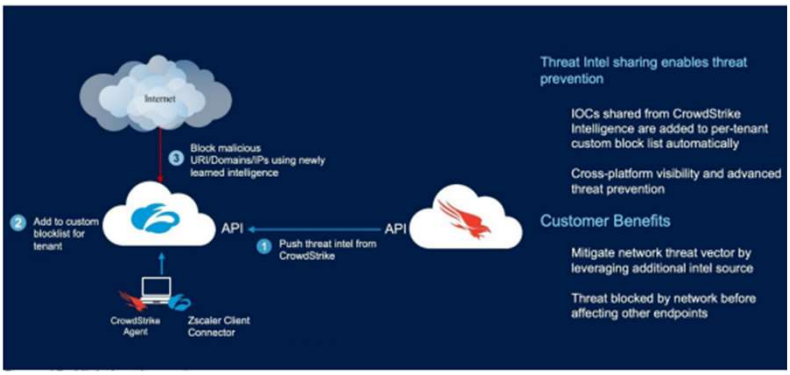


AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

ZIA – Threat Intelligence Sharing

- Setzt CrowdStrike Falcon Intelligence voraus
- Threat Intelligene (IOCs) werden automatisch in Custom URL Blocklist hinzugefügt



ZIA & ZPA – NSS Logs Integration mit Falcon LogScale

- Setzt Falcon LogScale Lizenz voraus
  - LogScale entweder Standalone oder als Falcon Long Term Repositoriy
- ZIA Nanolog Streaming Service Logs
  - Firewall Logs, DNS Logs, Tunnel Logs, etc
- LogScale bietet out-of-the-box Log Parser, Queries und Dashboards

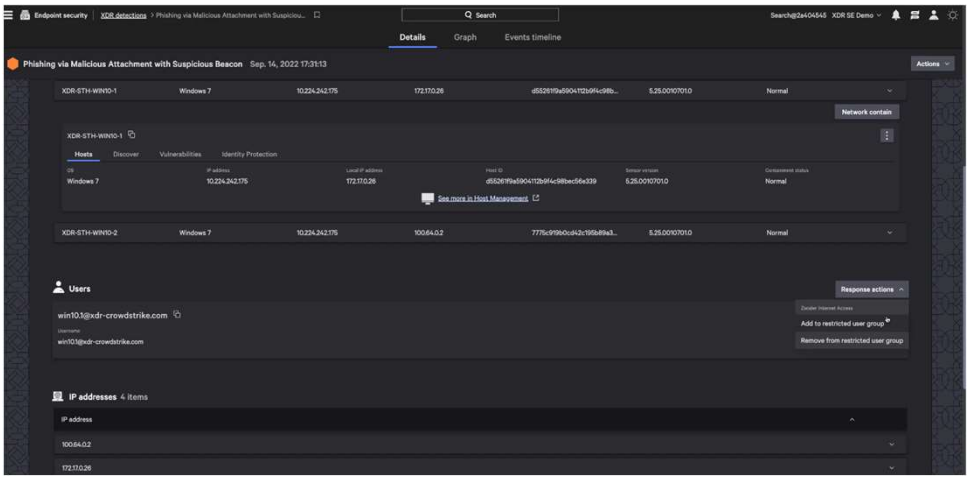
AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

ZIA – Falcon XDR Integration

AVANTEC
Competence. Security. Trust.

- Setzt CrowdStrike Insight XDR und 3rd Party Connector Lizenzen voraus
- Aktuell Integration für ZIA only
- Response aus Crowdstrike > User in ZIA Gruppe aufnehmen für eingeschränkten Internetzugang



ZIA – Falcon XDR Integration

AVANTEC
Competence. Security. Trust.

- Neue Falcon XDR Detection
  - Phishing Angriff mit maliziösem Attachment
- Unterschiedliche Log Sources
  - CrowdStrike: Informationen zu Host Aktivitäten, Korrelation der Logs
  - E-Mail Gateway: Absender, Empfänger, Subject, Attachment
  - Web Proxy: verdächtiger Beacon Traffic auf externe URL / IP Adresse
- Response Möglichkeiten
  - Host Isolation
  - Forcieren von 2FA
  - Betroffen User einer Restricted Group für Internet Access hinzufügen
  - Auch automatisierte Response möglich dank Built-In Falcon Fusion Workflows

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

CrowdXDR Alliance

AVANTEC
Competence. Security. Trust.

- Best-of-Breed Partners
- Führende Security Anbieter

- Als CrowdStrike Partner ist AVANTEC zudem:
  - Zscaler ZENITH Partner
  - Fortinet EXPERT Partner
  - Vectra PREMIER Partner
  - Cisco E-Mail Security Partner

ARMIS. | CISCO | CLAROTY | CLOUDFLARE | corelight
ExtraHop | ForgeRock | FORTINET | Google Cloud | MENLO SECURITY
mimecast | netskope | okta | PingIdentity | proofpoint | servicenow
THREAT WARRIOR | VECTRA | zscaler

Workflow

AVANTEC
Competence. Security. Trust.

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
25. Januar 2023

AVANTEC
Competence. Security. Trust.

DANKE

> Q&A

AVANTEC
Competence. Security. Trust.