

Zscaler Business Update

05. März 2024

AVANTEC
Competence. Security. Trust.



Cyber Defense – Teil 2

Mike Thurnherr
Cyber Defense Specialist
thurnherr@avantec.ch

Agenda

AVANTEC
Competence. Security. Trust.

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

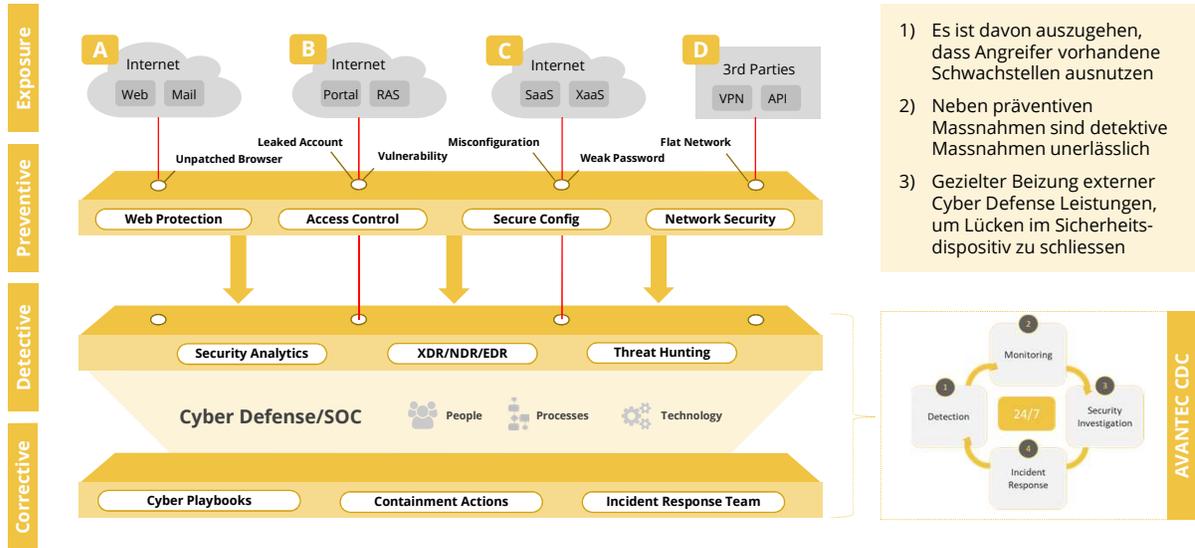
AVANTEC
Competence. Security. Trust.

Zscaler Business Update

05. März 2024

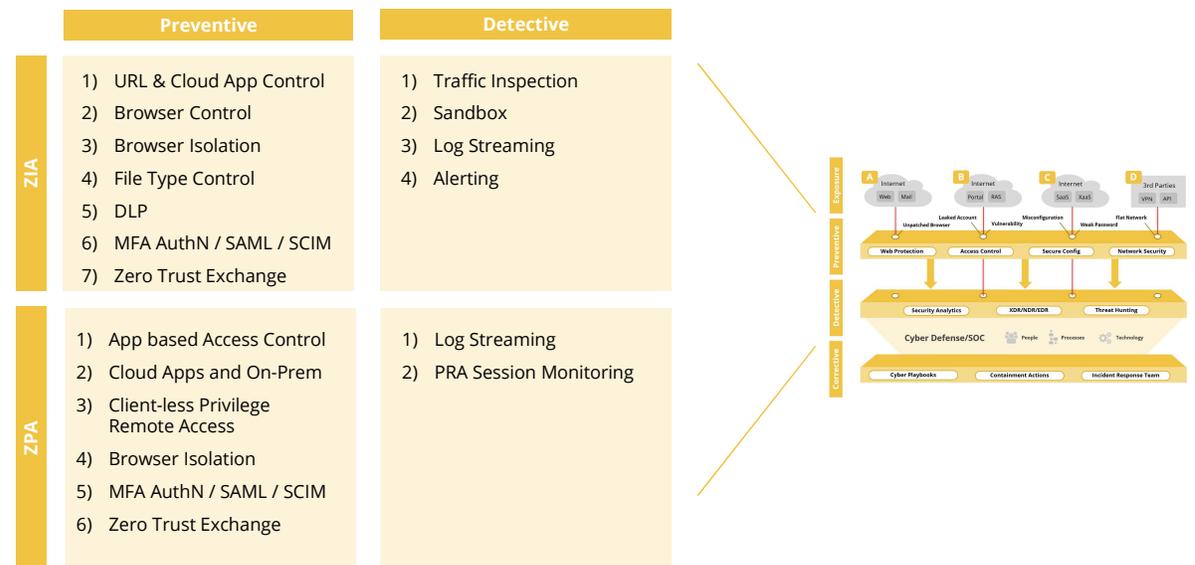
Bewältigungsstrategie

AVANTEC
Competence. Security. Trust.



Einordnung Zscaler - Bewältigungsstrategie

AVANTEC
Competence. Security. Trust.

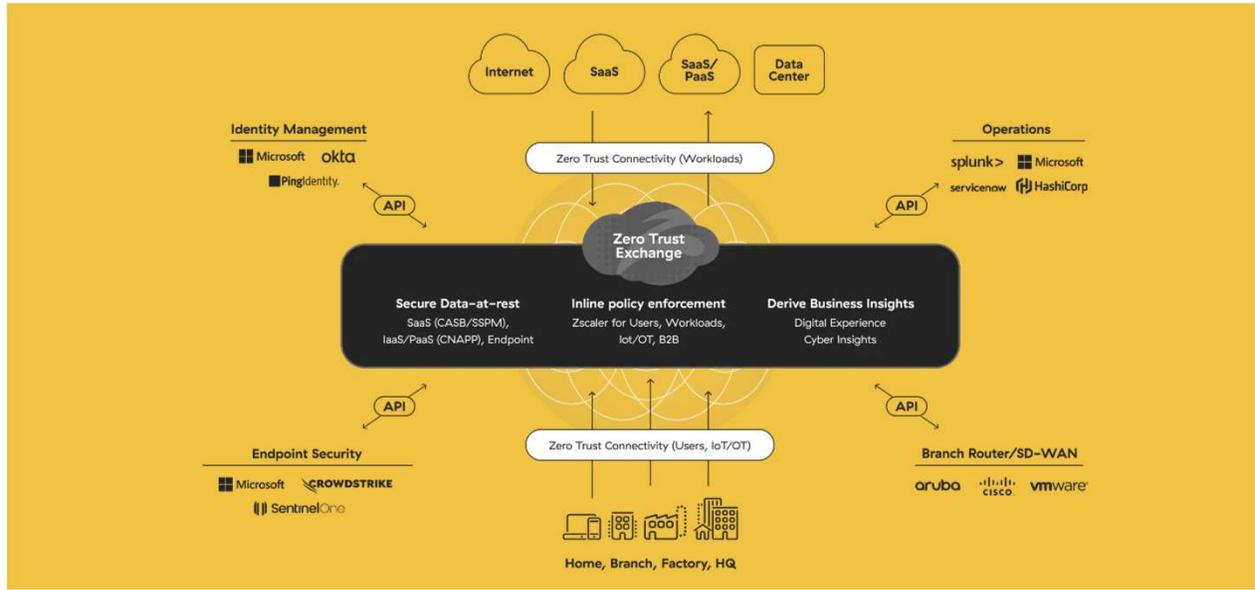


Zscaler Business Update

05. März 2024

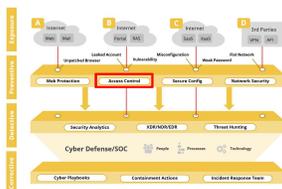
Zscaler Integration Ecosystem

AVANTEC
Competence. Security. Trust.

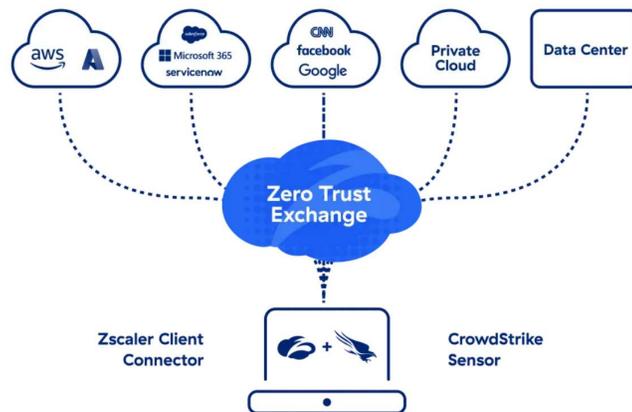


Integration #1 – Zero Trust mit Device Posture

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.

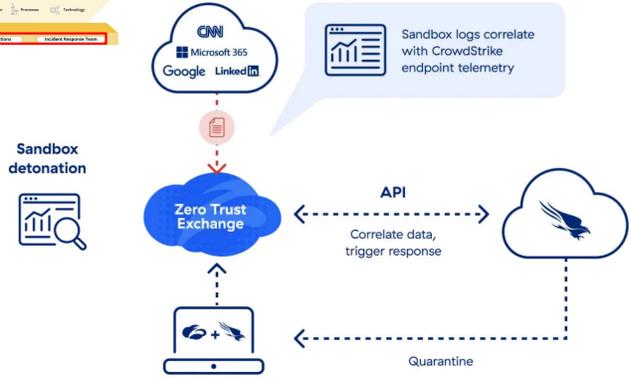
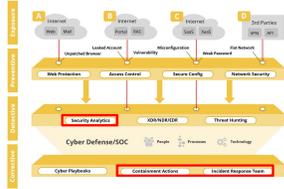


Zscaler Business Update

05. März 2024

Integration #2 – Advanced Threat Detection mit ZIA Sandbox

AVANTEC
Competence. Security. Trust.



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

AVANTEC
Competence. Security. Trust.

Sandbox Detail Report
Report ID (MD5): 8FC3813C25D012BAEA0F0287E68BEF Analysis Performed: 9/20/2019 4:43:50 PM

CLASSIFICATION
Class Type: Malicious
Sandbox Score: 74
Machine Learning Analysis: Malicious - High Confidence
Category: F00K/Keylogger
Malware & Botnet Detected: Win32/Agent.H2Z Trojan

SECURITY BYPASS
• Tries to detect sandboxes and other dynamic analysis tools
• Launches processes in debugging mode
• All process strings found
• Uses taskkill to terminate processes
• Binary may include packed or encrypted data
• Checks for kernel debuggers

NETWORKING
• Uses ping.exe
• Checks the public IP address of the machine
• Downloads files
• Found strings which match to known social media URLs
• Performs DNS lookups
• URLs found in memory or binary data

STEALTH
• Creates files inside the volume of volume information
• Detaches itself after installation
• Disables application error messages

SPREADING
• Shows file infection information gathering behavior

INFORMATION LEAKAGE
• Overrides MacOs FileFix settings
• Enumerates the file system
• Steals IE cookies

EXPLOITING
• May try to detect the Windows Ex

PERSISTENCE
• Creates an autorun registry key
• Creates an undocumented autorun registry key
• Creates a start menu entry
• Creates temporary files
• Drops PE files
• Stores files to the Windows startup directory

SYSTEM SUMMARY
• Spawns drivers
• Creates files inside the user directory
• Creates guard pages
• Creates mutexes
• Enables driver privilege
• PE file contains an invalid checksum
• Queries a list of all running processes

CROWDSTRIKE ENDPOINT HITS

Affected Users (38)

User Name	User ID	Location	Endpoints
Derek Byrd	derek.byrd@yahoo.com	Quentinland	Derek's iPhone XS Max
Annie Collier	annie.collier@hotmail.com	North Reuben	Annie's Pixel 3
Clyde Sandoval	clyde.sandoval@hotmail.com	South Marianatown	Clyde's iPhone XR
William Holt	william.holt@hotmail.com	Fredside	William's Samsung S10
Patrick Warren	patrick.warren@yahoo.com	North Milton	Patrick's iPhone 8 Plus

Affected Endpoints (72)

Endpoint Name	Endpoint ID	Hostname	IP Address	OS	Action	User ID
Derek's iPhone XS Max	0544CE8B	z32-sp452-eme	240.187.123.151	iOS 12.4.1	Quarantine	derek.byrd@yahoo.com
Annie's Pixel 3	290E260E	z11-sp442-eme	99.172.93.114	Android 10	Quarantine	annie.collier@hotmail.com
Clyde's iPhone XR	5F795F795F79	z53-sp452-eme	146.103.87.19	iOS 12.4.1	Quarantine	clyde.sandoval@hotmail.com
William's Samsung S10	BA75BA75	z11-sp452-eme	192.19.176.140	Android 9	Quarantine	william.holt@hotmail.com
Patrick's iPhone 8 Plus	AF841557582E	z52-sp452-eme	160.148.120.47	iOS 12.3	Quarantine	patrick.warren@yahoo.com

AVANTEC
Competence. Security. Trust.

Zscaler Business Update

05. März 2024

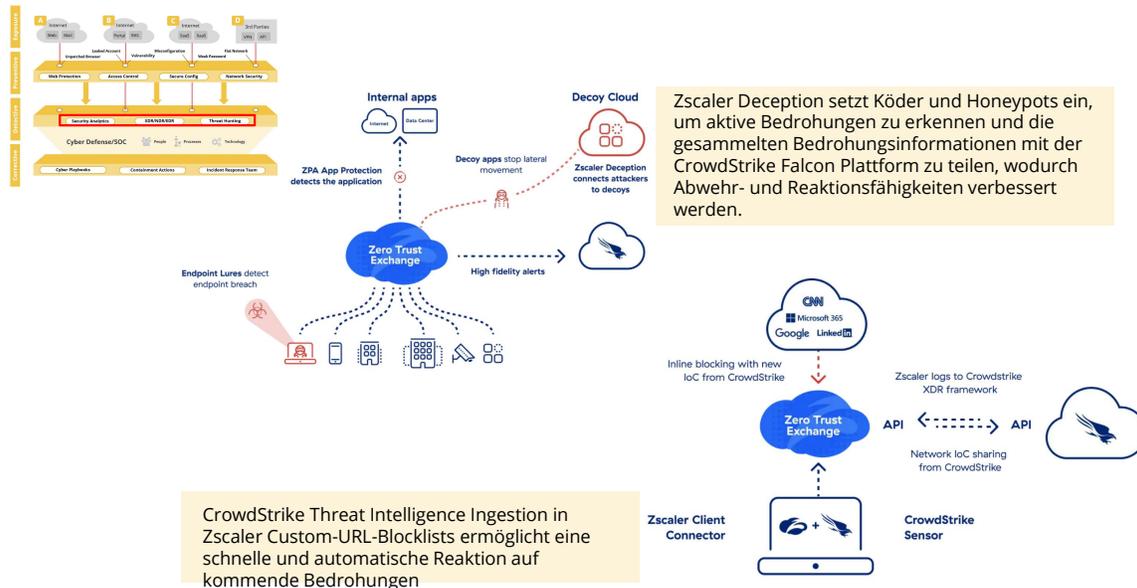
Integration #2 – Advanced Threat Detection mit ZIA Sandbox

AVANTEC
Competence. Security. Trust.

The screenshot displays the AVANTEC ZIA interface. On the left, a sidebar shows navigation options like Dashboard, Analytics, Policy, and Administration. The main area shows 'Insights Logs' with a table of events. A table with 5 columns (N., Event Time, User, Policy Action, MDS) lists three events from February 19, 2020, all categorized as 'Malware block: malicious...'. Below this, the 'Investigate Host' section shows details for host 'W10CLIENT03', including its IP (10.10.10.84) and a 'Contain' button. A table below lists 'Detect History (last 7 days)' with columns for Agent ID, Hostname, Internal IP, OS Version, File Status, Last Seen, and Endpoint Status. A table with 10 columns (Host Name, Real Time Response, MAC, Local IP, aip, Product Type, Version, Manufacturer, Model, Domain) provides further technical details for the host.

Integration #3 – Threat Intelligence sharing

AVANTEC
Competence. Security. Trust.

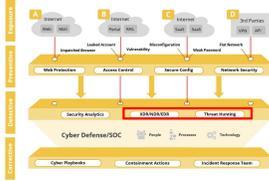


Zscaler Business Update

05. März 2024

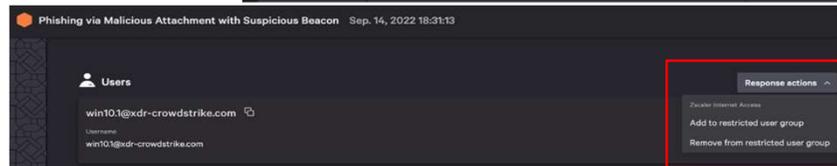
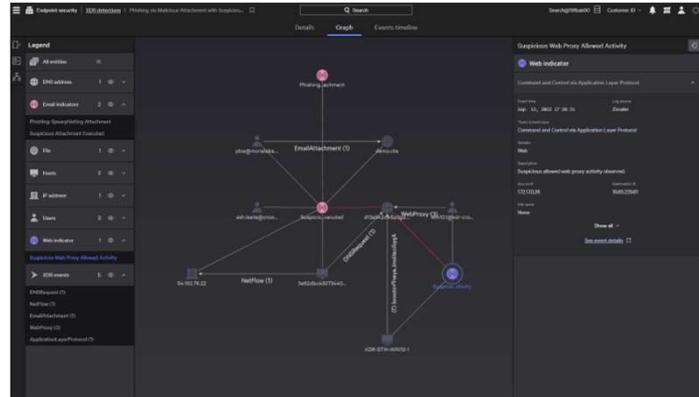
Integration #4 – XDR Detection

AVANTEC
Competence. Security. Trust.



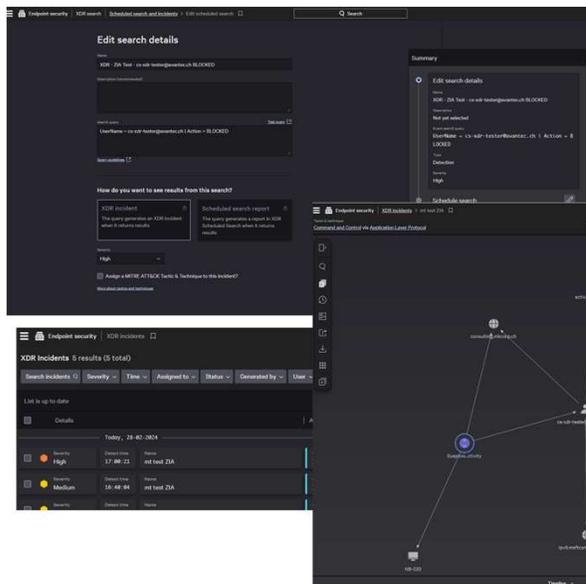
XDR bietet Detection Handling und Log Analyse über eine einzige zentrale Konsole. Zscaler Logs werden über Cloud NSS zu CrowdStrike transferiert.

Schnelle Reaktion bei Detection durch die Nutzung von Response Action.



Integration #4 – XDR Custom Incidents

AVANTEC
Competence. Security. Trust.



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



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)



DANKE