SCALTEL

ZERO TRUST

Devices

Inhalte

Warum brauchen Sie Zero Trust? Welche Herausforderungen warten bei der Implementierung dieser Sicherheitsstrategie auf Ihr Unternehmen? Diese Fragen wurden in unserem sechsten Webinar der Online-Seminar Reihe "Zero Trust" aufgedeckt. Die wichtigsten Fragen zeigen wir hier nochmals auf!

Rückblick - Warum ist eine gesamtheitliche Security-Strategie wichtig?

Never Trust, always verify - Der Plattformansatz ist die Basis für eine effektive Automatisierung

ZERO TRUST

Warum eine gesamtheitliche Security-Strategie wichtig ist

Netzwerke sind heutzutage unglaublich vielschichtig, weit verzweigt und häufig unübersichtlich. Hacker nutzen dies gerne aus und greifen an mehreren Stellen gleichzeitig an. Ein Angriff findet nicht zwangsläufig im Datacenter statt, sondern kann ebenso in Niederlassungen oder in weiteren beliebigen Geräten mit unterschiedlichen Schwachstellen auftreten. Eine Analyse des aktuellen IST-Zustandes ordnet die Situation einem Reifegrad zu und zeigt den bestmöglichen Weg zu einer erfolgreichen Zero Trust Security Strategie auf.

Zero Trust – eine Security-Strategie

Zero Trust beschreibt einen Sicherheitsanspruch, der diverse Zugriffe auf ein Unternehmen bewacht und vor unbefugtem Zugriff schützt. Dies zeigt eine Haltung, wie ein Netzwerk geführt werden kann. Jede Unternehmung definiert hier einen eigenen Startpunkt und geht einen individuellen Sicherheitsweg, welcher niemals endet. Dabei gilt: Vertrauen Sie niemanden, vergeben Sie immer nur zwingend notwendige Rechte und gehen Sie jederzeit von einem Angriff aus!

Cyber Security Assessment - Warum wird es benötigt?

Cyber Security Assessment ist ein Modell, das den Sicherheitsansatz in einem Unternehmen kontinuierlich verbessert. Im ersten Schritt findet eine IST-Analyse statt, anschließend erfolgt die Einstufung in Reifegrad. Anhand dieses Reifegrades lassen sich Verbesserungsmöglichkeiten und Ziele definieren, die technisch umgesetzt werden können.

UNSER WEG ZU ZERO TRUST

Devices - Grundlage Risikobewertung

Zero Trust Visibility ist ein wichtiger Aspekt des Zero Trust Sicherheitsmodells, bei dem keine implizite Vertrauensstellung zwischen Netzwerkressourcen oder Nutzern angenommen wird. Stattdessen müssen alle Zugriffsversuche auf Netzwerkressourcen kontinuierlich überprüft und validiert werden. Zero Trust Classification bezieht sich auf die Kategorisierung von Daten, Benutzern, Geräten und Anwendungen, um den Zugriff und die Sicherheit gemäß dem Zero Trust Sicherheitsmodell zu steuern. Endpoint Protection ist ein entscheidender Aspekt des Zero Trust Sicherheitsmodells und konzentriert sich auf den Schutz von Endgeräten wie Desktop-Computern, Laptops, Smartphones und IoT-Geräten.

Prevent everything you can

Everything you can't prevent, detect and investigate fast

Malware Prevention
- Portable Executable and DLL Examination
- Office Files with Macros Examination
- Behavioral Threat Protection
- Ransomware Protection
- Malicious Child Process Protection
- Password Theft Protection (Mimikatz)
- Network Packet Inspection Engine
- Sandboxing (Wildfire)

Exploit Prevention
- Browser Exploit Protection
- Logical Exploits Protection
- Known Vulnerable Processes Protection
- Operating System Exploit Protection
- Unpatched Vulnerabilities Protection

Extensions
- Device Control
- Host Firewall
- Host Disk Encryption

Actions
- Isolate Host
- Remote Terminal
- Run Command

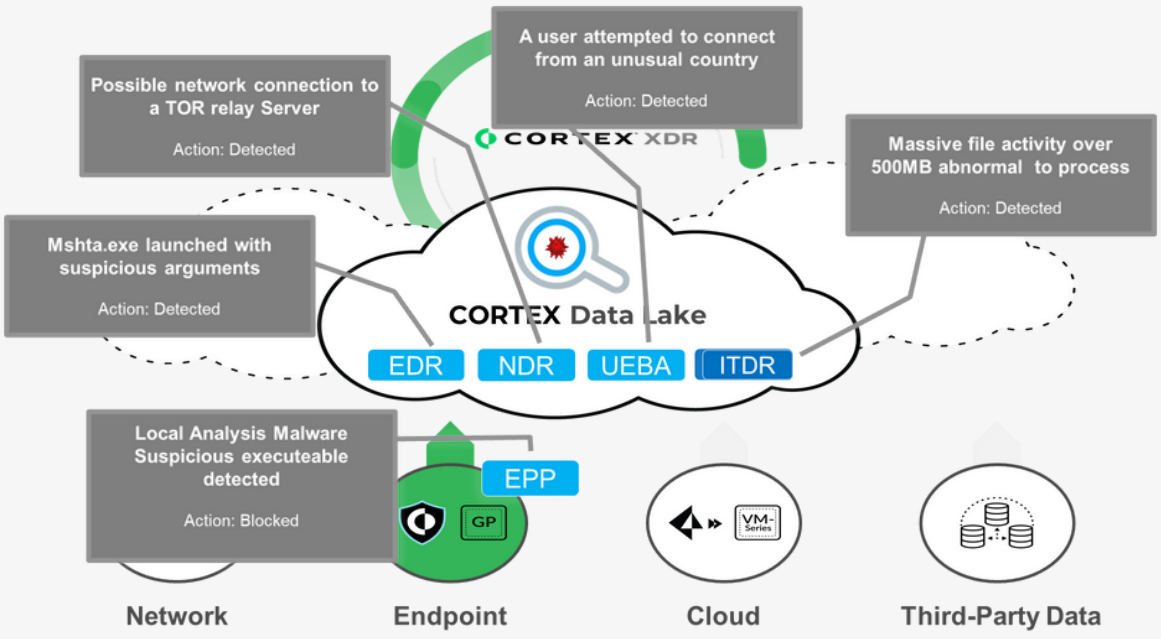
EDR / XDR
- Data Analytics: File Access, Image Load (DLL), Processes, Network Communication, Registry, Eventlog
- ~400 BIOC Rules
- ~350 AI-based detection Rules
- XQL queries to search captured data

- Network, Cloud, Third Party

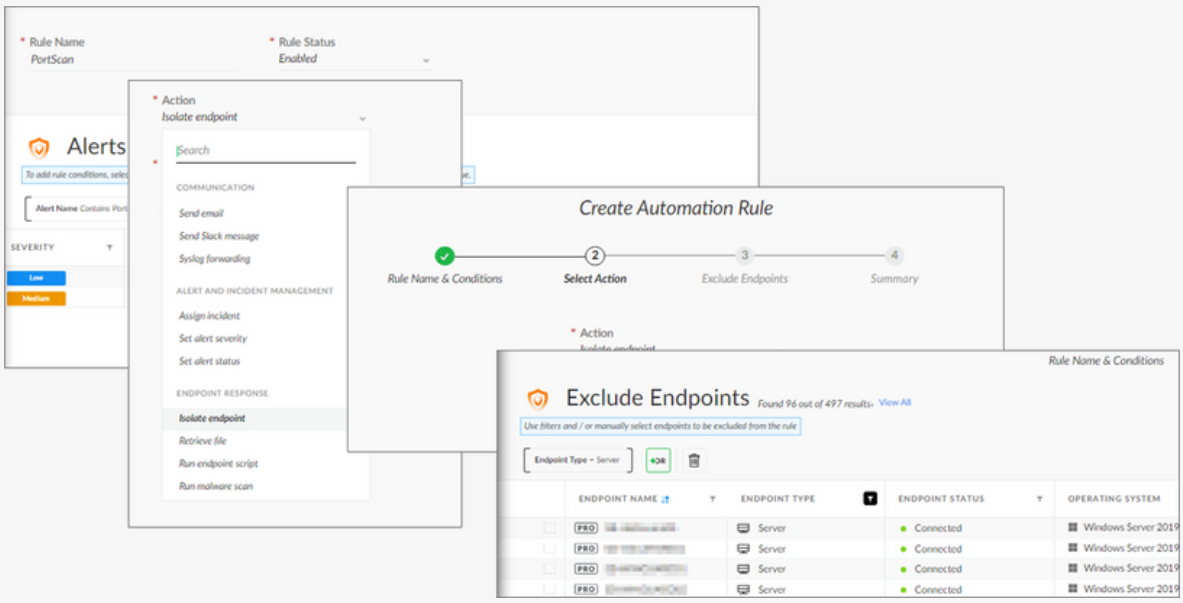
Hosts Insights
- Software Inventory
- Vulnerabilities
- Search and destroy (remediation)

UNSER WEG ZU ZERO TRUST

EXTENDED DETECTION & RESPONSE (XDR)

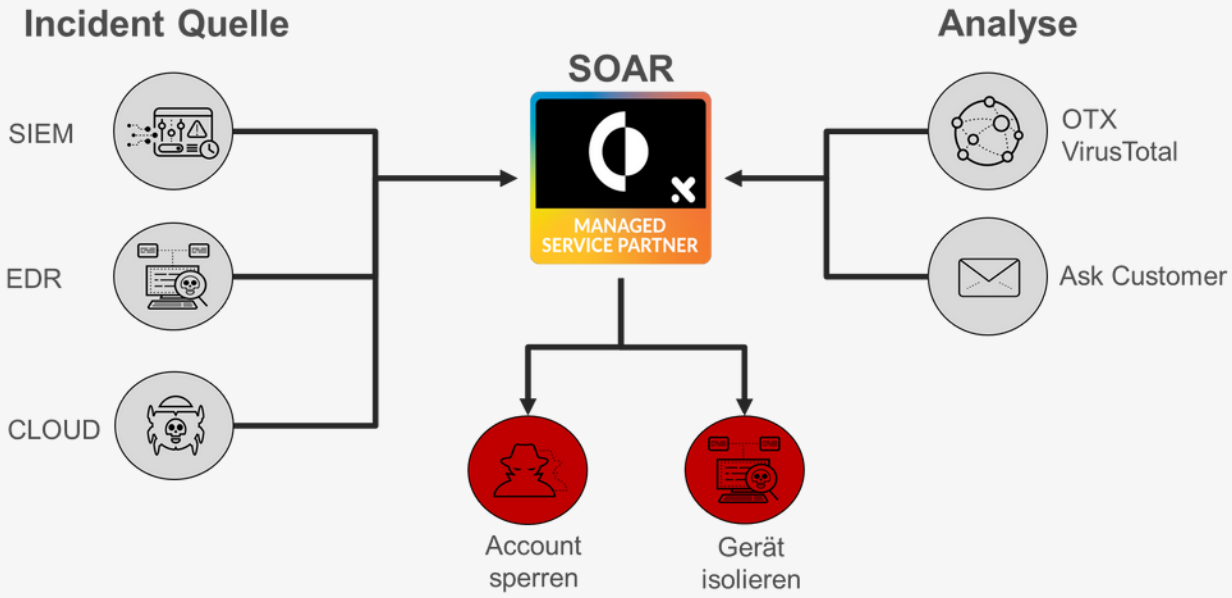


AUTOMATISIERUNG MIT CORTEX XDR



UNSER WEG ZU ZERO TRUST

AUTOMATISIERUNG MIT CORTEX XSOAR



Incident Priorisierung

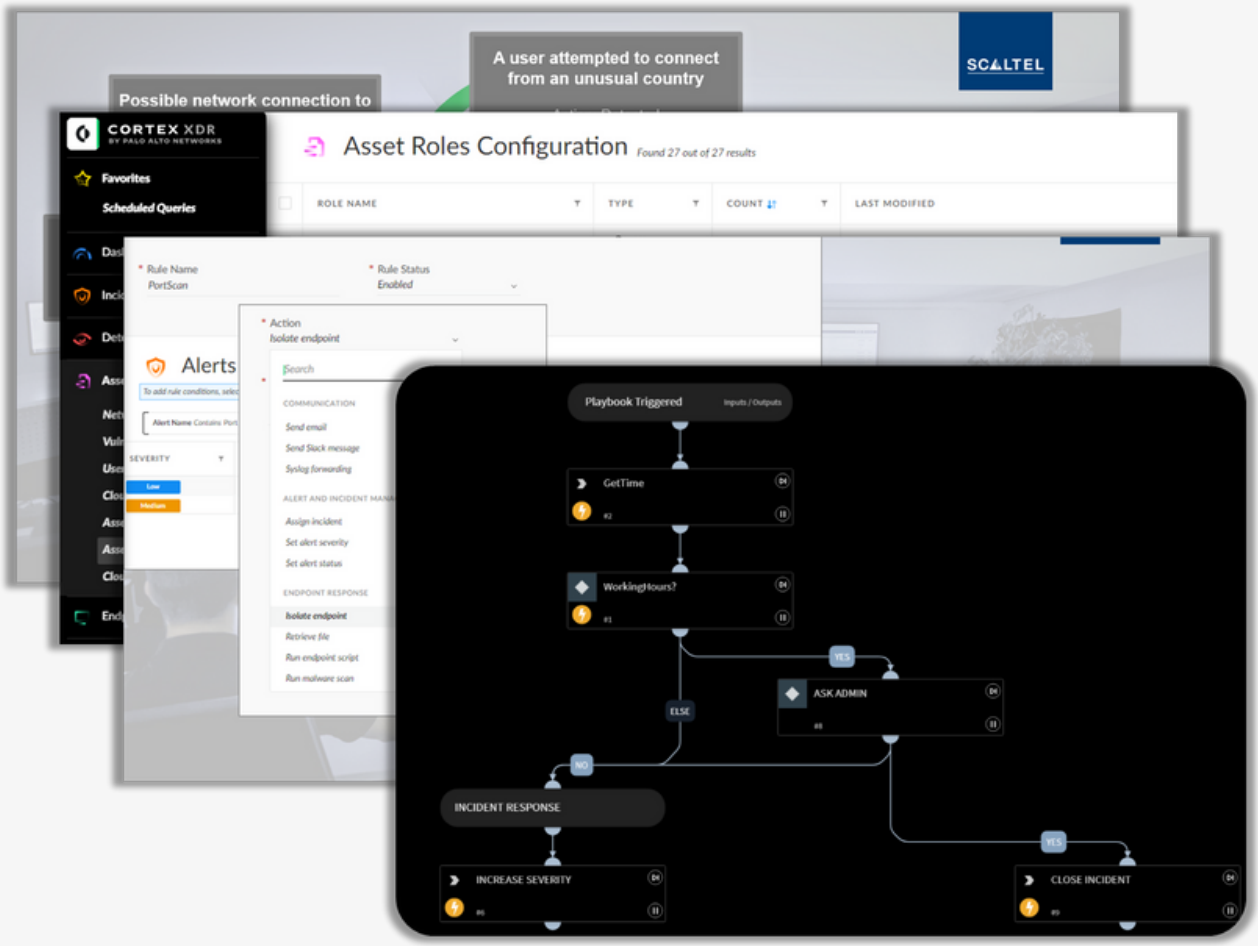
- Severity
- Stichwortliste
- Fortschritt (Mitre Attack)
- Alarmierung (z.B. SMS)

Incident Analyse

- Kontaktermittlung
- Generierung von E-Mails

UNSER WEG ZU ZERO TRUST

Zusammenfassung



- Erkennung / Alarming → Visualisierung
- Automatisierte Classification → Alarming mit Severity
- Basis-Automatsierung aus XDR
- Erweiterung durch XSOAR → Playbook-Entwicklung

- Die Angriffsdauer hat sich erheblich verkürzt
- Schnelle Erkennung und Reaktion ist nur durch Automatisierung möglich
- Endpoint Security ist ein Schlüsselfaktor zum Erfolg
- Schutz und Basis-Automatisierung in einem System
- Der Plattformansatz ist die Basis für eine effektive Automatisierung

UNSER WEG ZU ZERO TRUST

Neben den technischen Parametern müssen Budget und Komplexität sowie Zeitaufwand gegenübergestellt werden.

Im zweiten Schritt werden sämtliche Schutzflächen sowie Angriffsflächen identifiziert. Der Zusammenhang zwischen riskanten und zu schützenden online- sowie offline-Objekten muss unbedingt beachtetet werden!

Wir begleiten Sie gerne auf dem Weg zu Zero Trust.
Informieren Sie sich in unseren nächsten Webinaren über die weiteren Bausteine.

Unsere Termine zur Online-Seminarreihe "Zero Trust"

DATUM	THEMA
25.05.2023	ZERO TRUST: Data

Zur Anmeldung

Kontakt aufnehmen