axians

ANGA COM 2025 | Axians In-Booth Theater

Die Zukunft der Cyber-Security

MDR as-a-Service

Thomas Engl, BU-Leiter XTRO, Axians
Christian Kanders, Senior Sales Engineer, WatchGuard

axians

smartSOC Managed Detection and Response

Thomas Engl & Christian Kanders

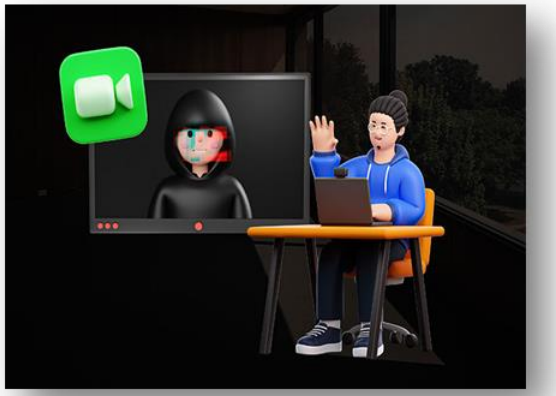
Unser Angebot

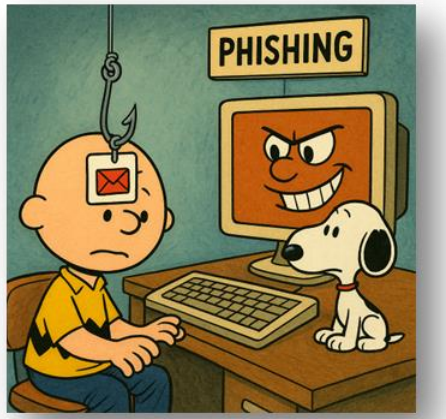
Effektive Cyber-Sicherheit mit Managed Detection and Response

Frage ans Publikum

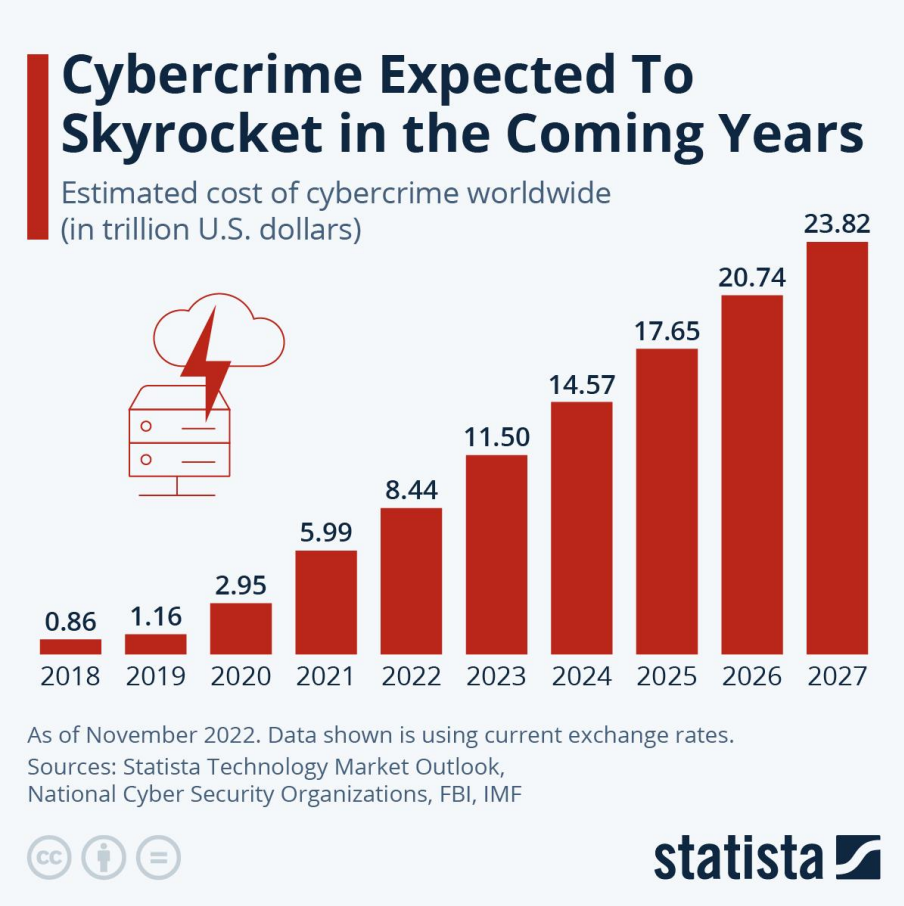
Welche Gefahren in der IT-Security sehen Sie aktuell am stärksten in Ihrem Umfeld?

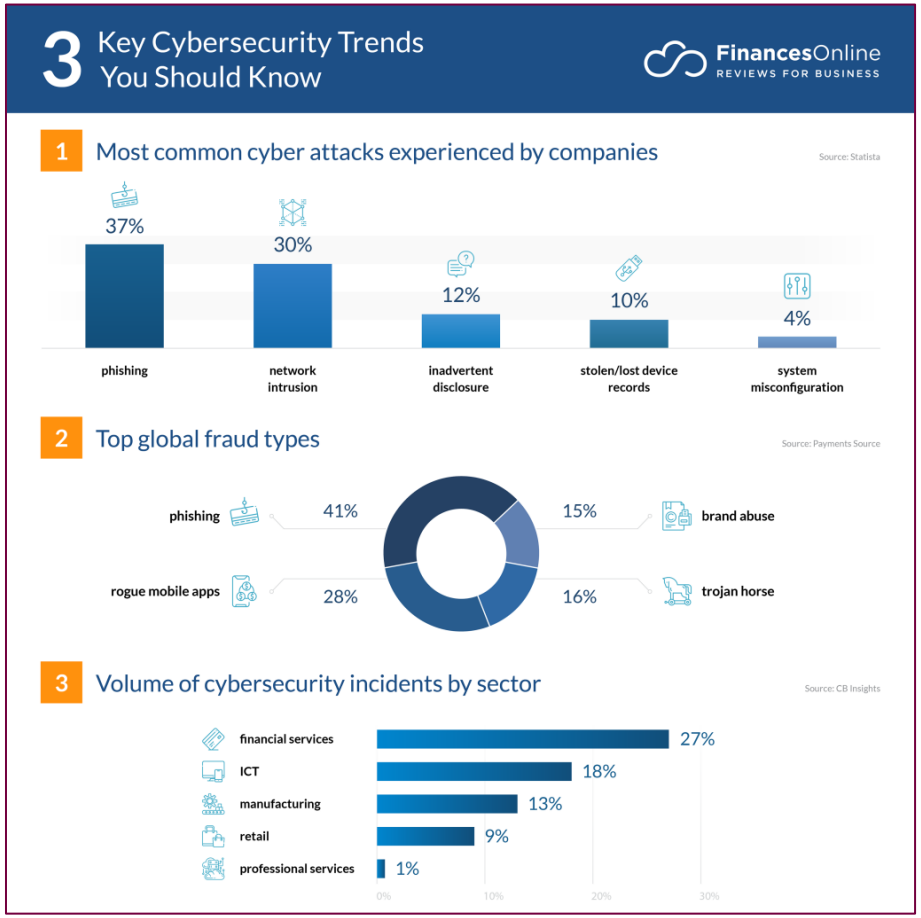
Angriffsvektoren vermehren sich





Markprognosen - CyberCrime





Neue Richtlinien

NIS2: Wie können Unternehmen NIS2 umsetzen?

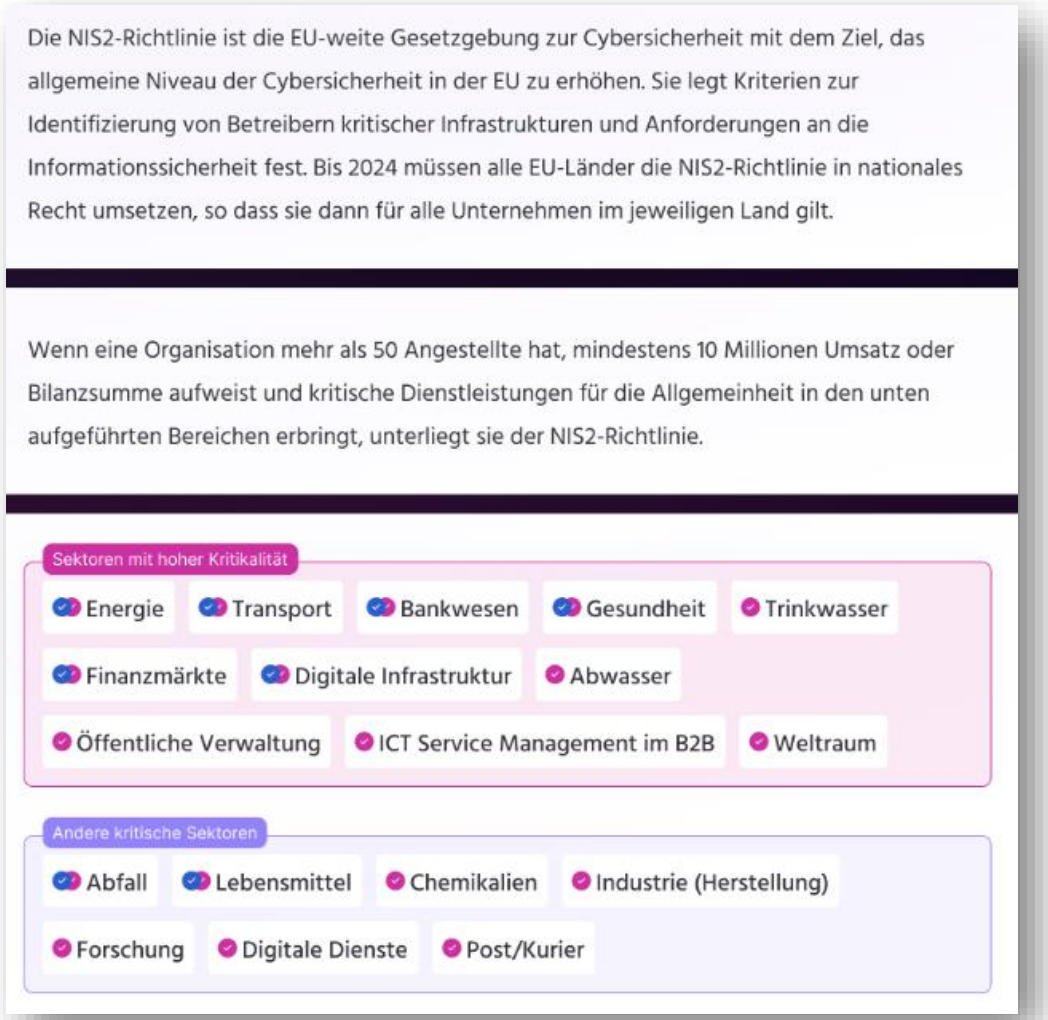
Wesentliche und wichtige Organisationen müssen laut NIS2-Richtlinie „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme (…) zu beherrschen“. Zudem sollen „die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste“ und andere Dienste verhindert oder möglichst gering gehalten werden.

Eine Anforderung von NIS2 ist die Kombination verschiedener Abwehrmethoden: einerseits mithilfe von technologischen Security-Tools, andererseits durch spezialisierte Experten für diesen Bereich. Aber was können und müssen Unternehmen tun, um das zu gewährleisten? Die EU verlangt, dass sich um diese Aufgaben das oberste Management kümmert – NIS2 ist also Chefsache.

Die Richtlinie nennt verschiedene Bereiche und Maßnahmen, die mindestens abgedeckt werden müssen. Dazu gehören unter anderem:

- Konzepte in Bezug auf Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs durch Backup-Management und Wiederherstellung nach einem Notfall sowie Krisenmanagement
- Sicherheit der Lieferkette, auch bei unmittelbaren Anbietern oder Diensteanbietern
- Management und Offenlegung von Schwachstellen
- Schulungen im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptographie und Verschlüsselung

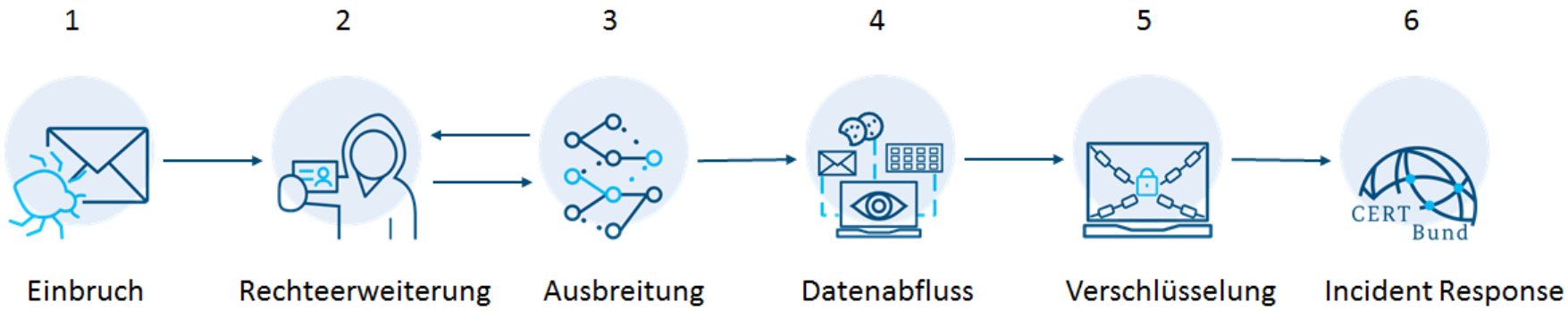
Quelle: Heise.de



Quelle: secjur.com

Angriffe in der Realität

Ablauf eines Angriffes



Patches, Makros & Remote-Zugänge

Benutzer-Berechtigungen, Programmausführungen, Segmentierungen

BackUps, Notfallplan, Autarkie

Use Case Story

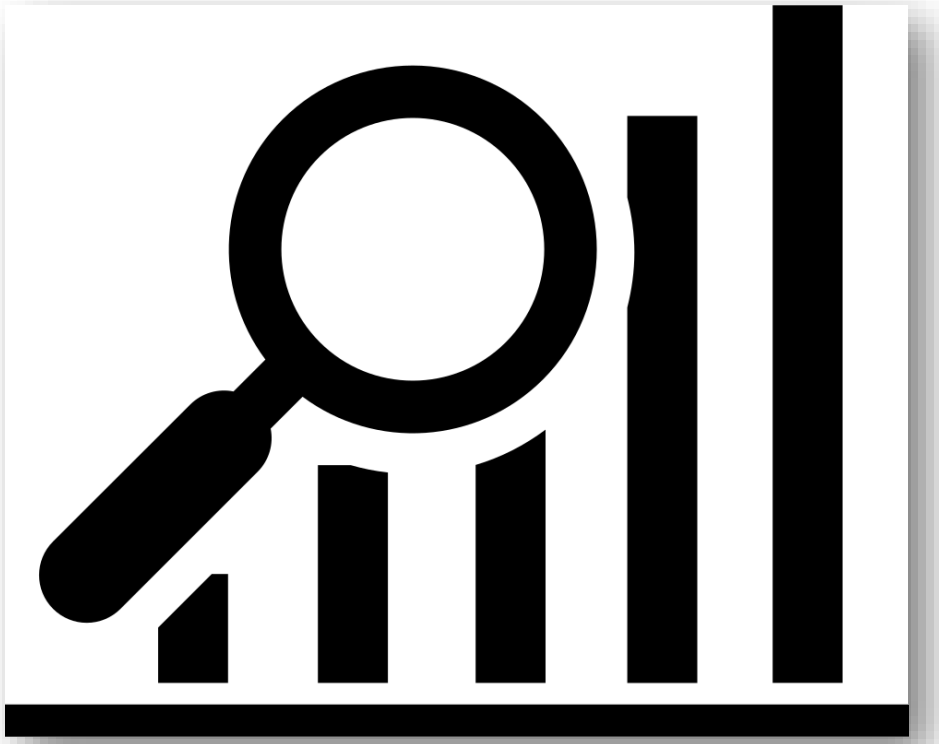
Überflutung an Events

Use Case

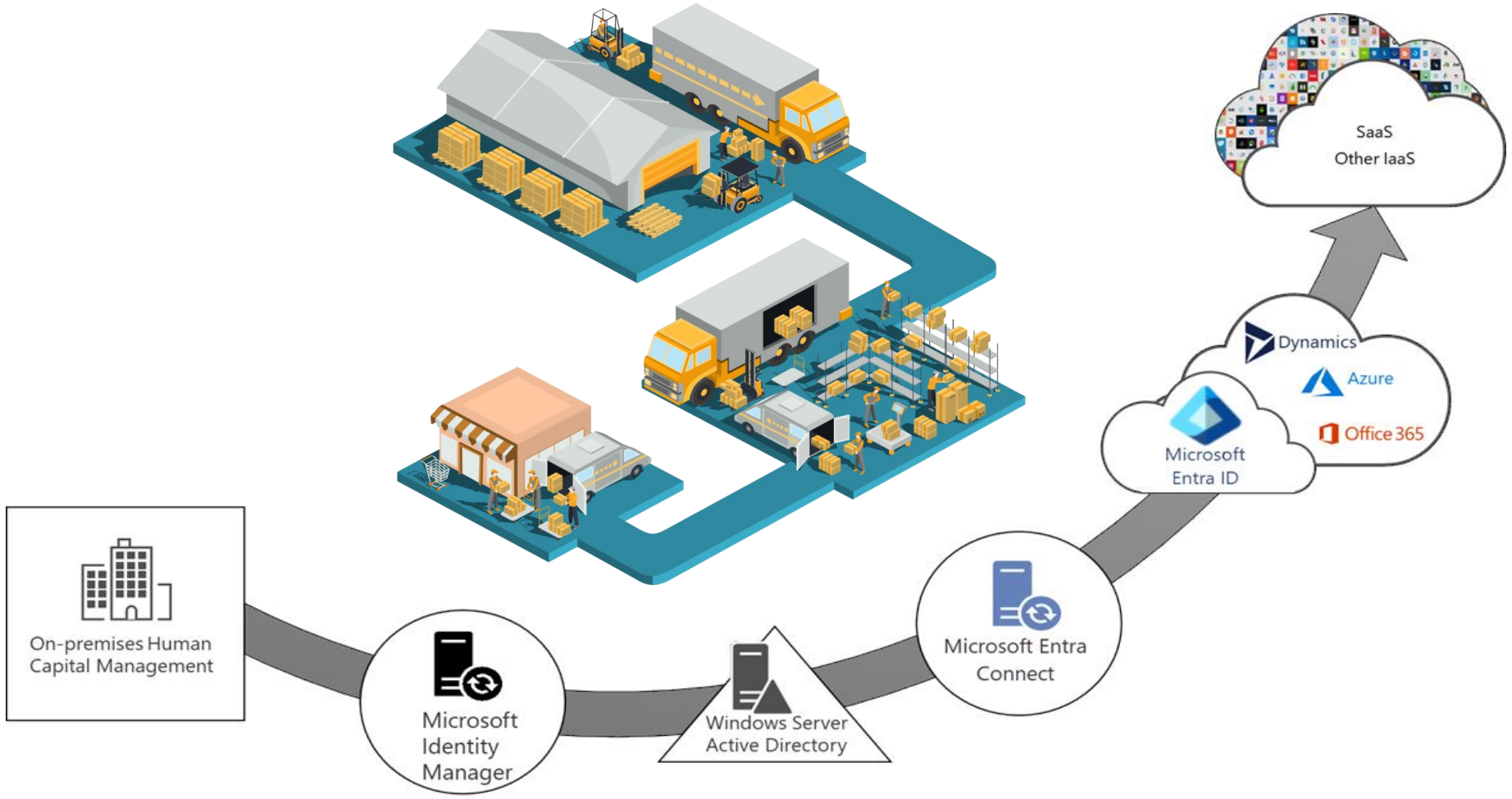
Herausforderungen in 2024

ISO 27001

NIS2



Hybride Umgebungen



Wie Axians SmartSOC MDRS funktioniert

CYBER HYGIENE

Regelmäßige Bewertung der Angriffsfläche zur Identifizierung von :

- Anfällige Betriebssysteme und Anwendungen
- Fehlkonfigurationen beim Schutz
- Nicht verwaltete Endoints, etc.

damit der MSP die Sicherheitslage verbessern kann

PREVENTION

Automatisierte Präventionsschichten sind entscheidend :

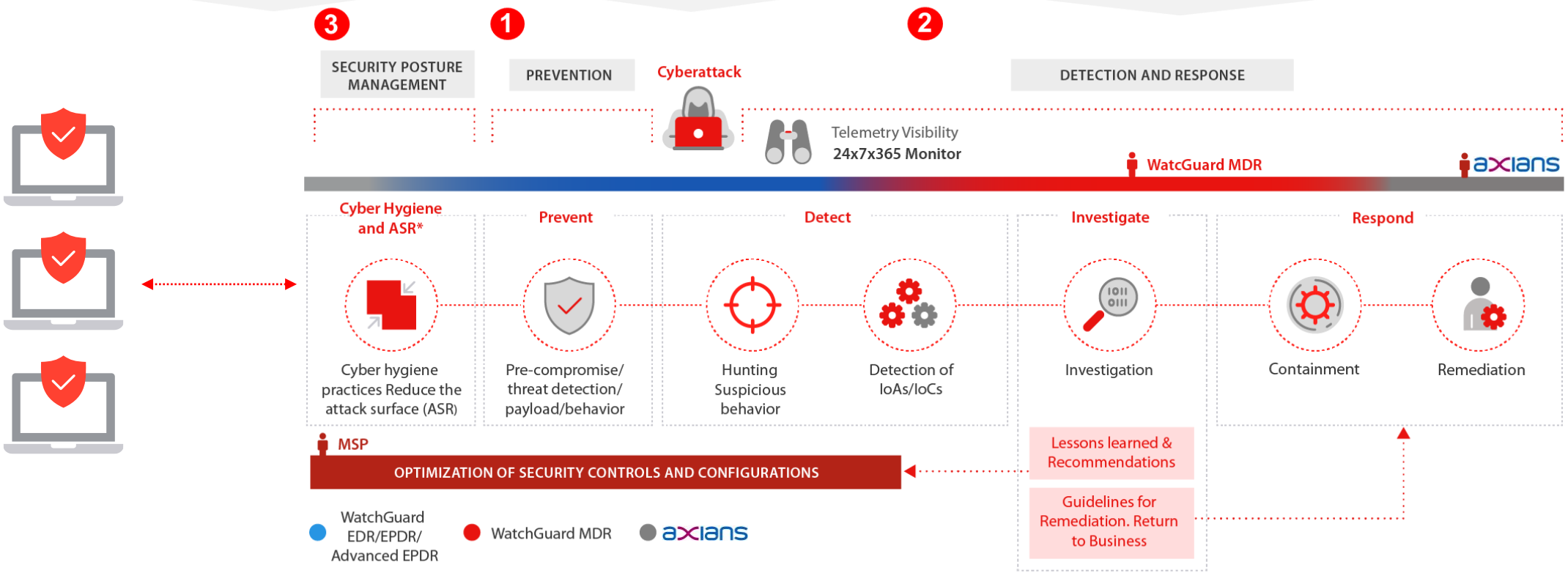
- Bequemes Herausfiltern von Vorfällen
- Verringerung der Arbeitsbelastung der Mitarbeiter
- Verringerung von Verstößen

Zero-Trust Application Service

DETECTION AND RESPONSE

Integrieren Sie das Fachwissen, die Technologie und die Prozesse des WatchGuard SOC zur kontinuierlichen Überwachung, Erkennung, Untersuchung und Eindämmung von Bedrohungen und leiten Sie Ihre Partner bei der Behebung von Problemen an.

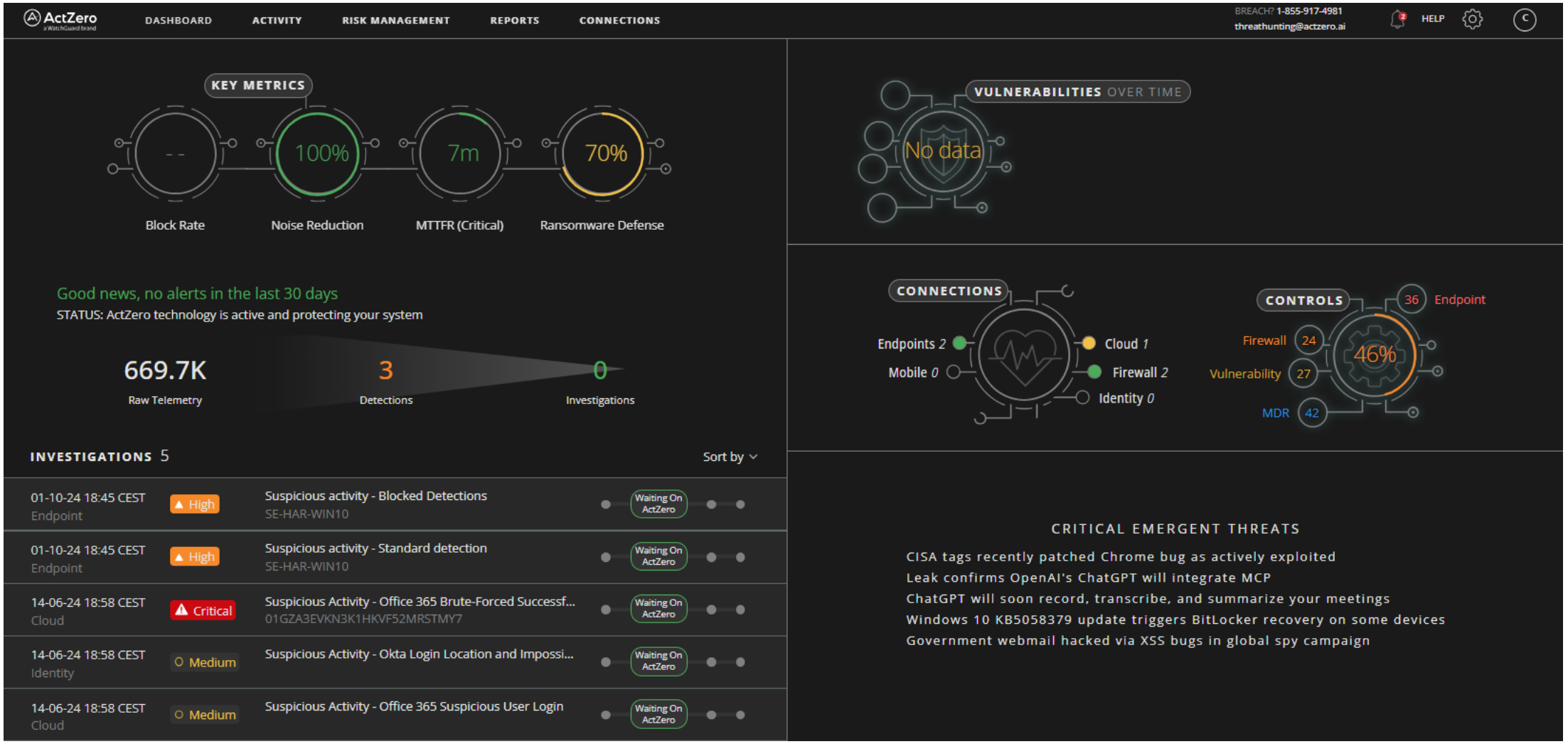
- **Zero-Trust Application Service**
- **Security-Analysen in der Cloud**
- **365-Tage Telemetrie**
- **Threat intelligence**



Mehrwerte des Axians Services

Eine ganzheitliche Sicherheitslösung
-als White-Label-Service verfügbar-

Axians SmartSOC MDRS Platform

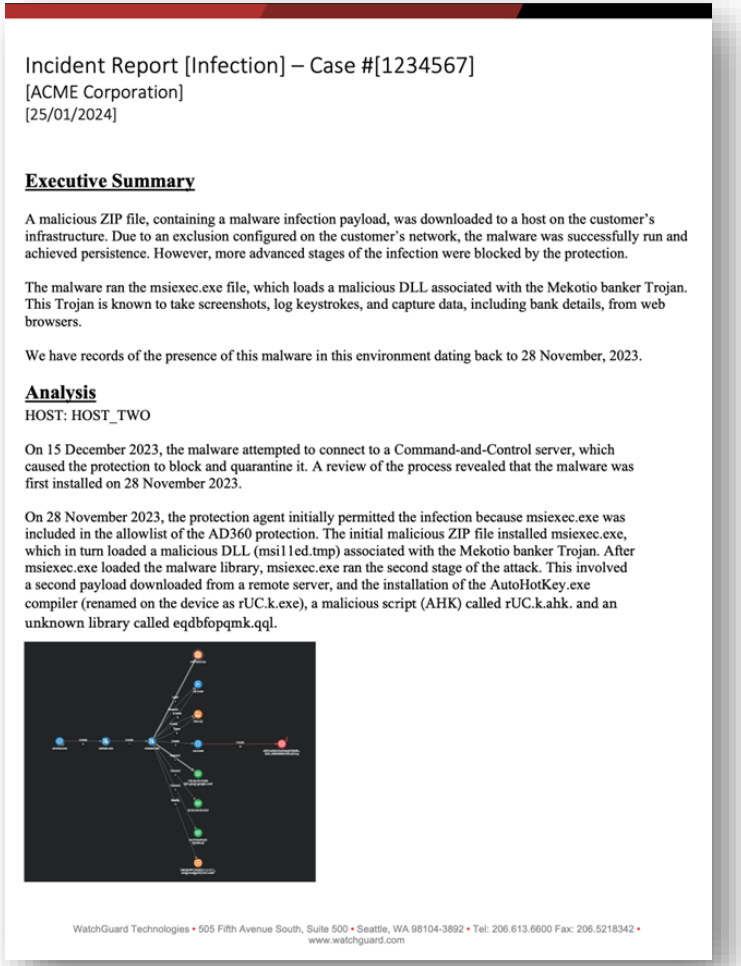


IOA vs IOC

- Indikator für Angriffe (IOA): Proaktiv
  - Antizipieren Sie die Kompromittierung, indem Sie verdächtige Aktivitäten untersuchen
- Indikator für eine Kompromittierung (IOC): Reaktiv
  - Diagnose eines Sicherheitsproblems, das gerade aufgetreten ist
  - Es ist der Nachweis, dass eine Sicherheitskompromittierung stattgefunden hat oder kurz davor war

Unverzügliche Meldung von Vorfällen

- Indikator Sofortige Benachrichtigung über Vorfälle und detaillierte Angriffsberichte
  - Nutzung des MITRE ATT&CK-Frameworks
- Maßgeschneiderte Playbooks zur automatischen Eindämmung, die nach Endpoints gefiltert werden
  - Richtlinien zur Schadensbegrenzung und -behebung
  - Kontinuierliche Bewertung der Angriffsoberfläche



Incident Report [Infection] – Case #[1234567]
[ACME Corporation]
[25/01/2024]

Executive Summary

A malicious ZIP file, containing a malware infection payload, was downloaded to a host on the customer's infrastructure. Due to an exclusion configured on the customer's network, the malware was successfully run and achieved persistence. However, more advanced stages of the infection were blocked by the protection.

The malware ran the msiexec.exe file, which loads a malicious DLL associated with the Mekotio banker Trojan. This Trojan is known to take screenshots, log keystrokes, and capture data, including bank details, from web browsers.

We have records of the presence of this malware in this environment dating back to 28 November, 2023.

Analysis

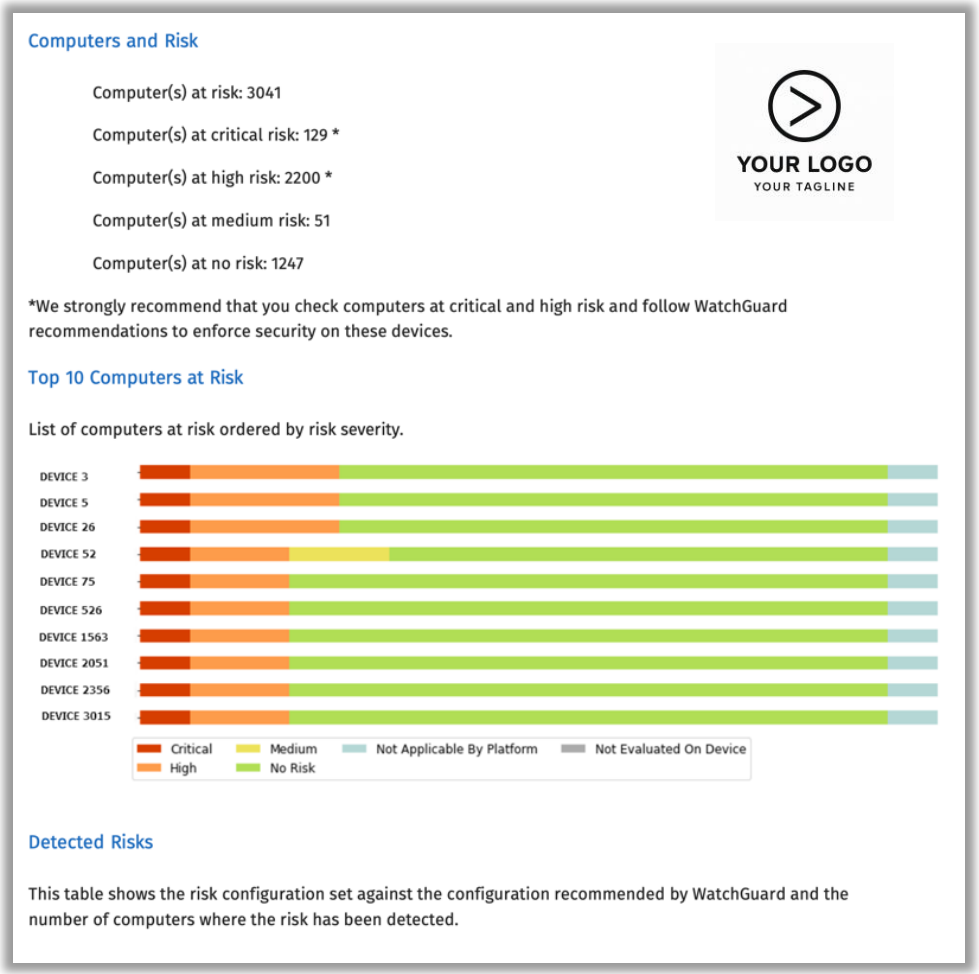
HOST: HOST_TWO

On 15 December 2023, the malware attempted to connect to a Command-and-Control server, which caused the protection to block and quarantine it. A review of the process revealed that the malware was first installed on 28 November 2023.

On 28 November 2023, the protection agent initially permitted the infection because msiexec.exe was included in the allowlist of the AD360 protection. The initial malicious ZIP file installed msiexec.exe, which in turn loaded a malicious DLL (msi11ed.tmp) associated with the Mekotio banker Trojan. After msiexec.exe loaded the malware library, msiexec.exe ran the second stage of the attack. This involved a second payload downloaded from a remote server, and the installation of the AutoHotKey.exe compiler (renamed on the device as rUC.k.exe), a malicious script (AHK) called rUC.k.ahk. and an unknown library called eqdbfopqmk.qql.

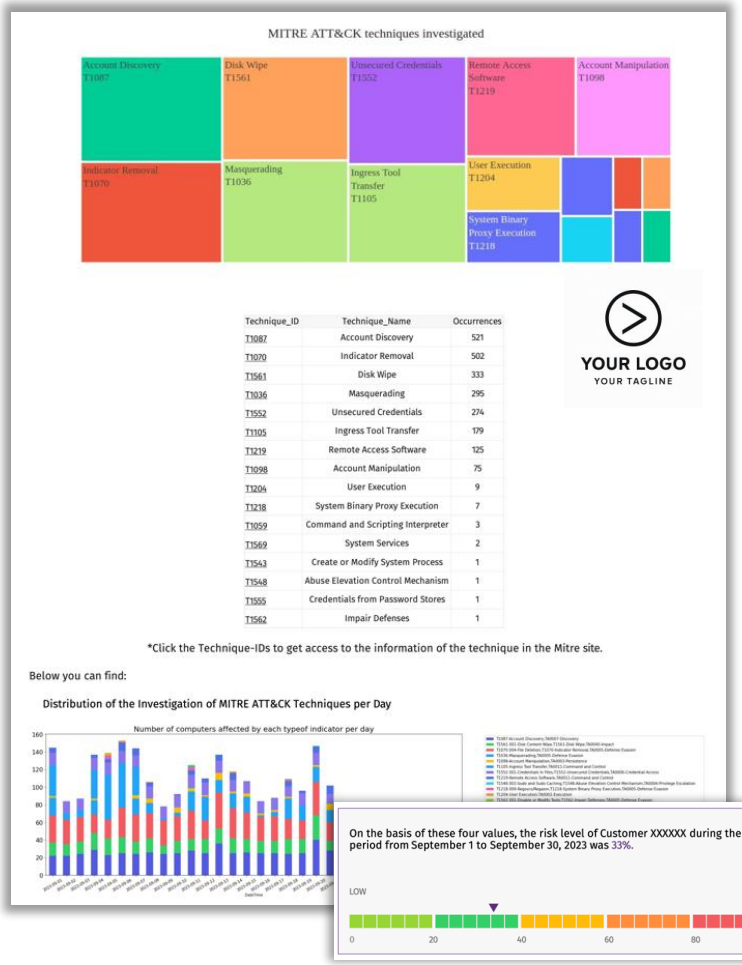
Weekly Health Assessment Report

- Indikator für eine Kompromittierung (IOC): Reaktiv
- Entwickelt, um einen schnellen Überblick über die Sicherheitslage der Endpoints des Kunden zu geben
- Ermöglicht eine schnelle Risiko-Identifizierung
- Enthält Abschnitte über
  - Entdeckte ungeschützte Endpoints ohne WatchGuard Endpoint Security-Lösung
  - Top 10 der am meisten gefährdeten Endpoints
  - Erkannte Risiken auf den Endpoints
  - Entwicklung der Risiken



Monthly Service Activity Report

- Bietet einen Überblick über die vom WatchGuard SOC-Team durchgeführten Erkennungen, Untersuchungen und Aktivitäten zur Eindämmung von Vorfällen
- Enthält Abschnitte über:
  - Aktuelle Situation und Sicherheitsempfehlungen zur Stärkung des Schutzes
  - Schutzniveau der Organisation
  - Bedrohungsgrad der Organisation
  - Monatlich durchgeführte Aktivitäten
  - Untersuchung anomaler Aktivitäten
  - Identifizierte und mitgeteilte Angriffsversuche



Technique_ID	Technique_Name	Occurrences
T1087	Account Discovery	521
T1070	Indicator Removal	502
T1561	Disk Wipe	333
T1036	Masquerading	295
T1552	Unsecured Credentials	274
T1105	Ingress Tool Transfer	179
T1219	Remote Access Software	125
T1098	Account Manipulation	75
T1204	User Execution	9
T1218	System Binary Proxy Execution	7
T1059	Command and Scripting Interpreter	3
T1569	System Services	2
T1543	Create or Modify System Process	1
T1548	Abuse Elevation Control Mechanism	1
T1555	Credentials from Password Stores	1
T1562	Impair Defenses	1

Awareness / Security-Audits

#Key Takeaways

- IT-Security boomt – Managed Services sind die Antwort
- Axians SmartSOC: ein vollwertiger MDR-Service – betriebsbereit, modular, skalierbar
- Auch als White-Label-Lösung verfügbar – unter Ihrer Marke, mit unserer operativen Stärke
- Sie liefern Sicherheit – wir den Betrieb
- Kein Invest in eigene SOC-Strukturen

Vielen Dank für Ihre Aufmerksamkeit!

Ansprechpartner: Thomas Engl
+49 175 261 4041
thomas.engl@axians.de

axians

Vielen Dank für Ihren Besuch!

Wie hat Ihnen der Vortrag gefallen?

Titel: MDR as-a-Service Referent: Thomas Engl

Jetzt abstimmen