Axians IT/OT Security Operations Center

Die Frage lautet nicht, ob Ihr Unternehmen kompromittiert wird, sondern wann. Unser Security Operations Center steuert und überwacht alle Cyber-Security-Mass-nahmen rund um die Uhr.

VINCI ENERGIES

DER REALITÄTSCHECK FÜR UNTERNEHMEN

Protection allein ist nicht ausreichend

Die Digitalisierung im IT/OT-Umfeld erhöht die Flexibilität und Effizienz von Unternehmen enorm. Gleichzeitig werden sie jedoch auch zu attraktiven Zielen für Kriminelle. Mit immer professionelleren Methoden richten sie Schaden an und versuchen Daten und Information zu ihrem Vorteil zu nutzen. Ihre Angriffe zu erkennen und einzudämmen stellt die Unternehmen vor vielschichte Herausforderungen, ganz speziell aufgrund der grossen Zahl der eingesetzten Systeme mit unterschiedlichsten Schwachstellen.

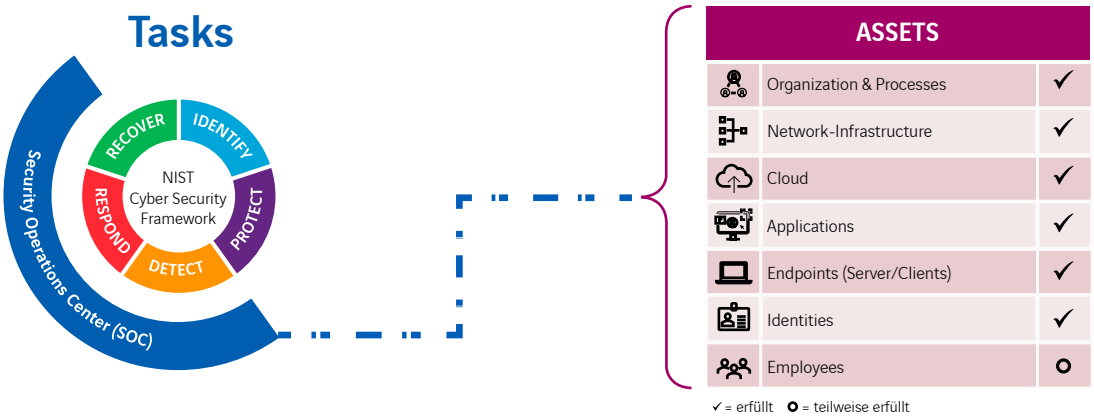
VIELE UNTERNEHMEN ERFAHREN VON DRITTER STELLE ÜBER ERFOLGREICHE ANGRIFFE AUF DAS EIGENE UNTERNEHMEN

DIE MEISTEN OPFER HATTEN AKTUELLE (UP-TO-DATE) PRÄVENZMASSNAHMEN, BZW. SCHUTZVORRICHTUNGEN

ES GIBT KEINEN 100%-SCHUTZ. DIE FRAGE IST NICHT OB, SONDERN WANN EIN ANGRIFF ERFOLGREICH SEIN WIRD

Der Realitätscheck für Unternehmen veranlasst Massnahmen und Investitionen in den Bereichen Detect und Response

Präventivmassnahmen allein, durch den Ausbau von weiteren Elementen im Bereich Protection, genügen nicht, um das Unternehmen langfristig vor Schaden durch Cyber-Angriffe zu bewahren. Unternehmen sollten Ihre Cyber-Security-Investitionen in den Bereichen Detect und Response erhöhen, um Sicherheitsvorfälle schneller entdecken und darauf zeitgerecht reagieren zu können.
Unter Security Operations Center (SOC) versteht Axians eine Kombination aus Experten, Werkzeugen und Prozessen mit dem Ziel Cyber Security Risiken zu entdecken, zu verhindern, zu analysieren und zu bewerten. Dies beinhaltet zusätzlich die Unterstützung bei der Umsetzung von Massnahmen zur Behebung von Cyber-Security-Risiken, so wie die Lieferung von forensischen Daten zur Beweissicherung und Dokumentation bei Cyber-Security-Vorfällen.

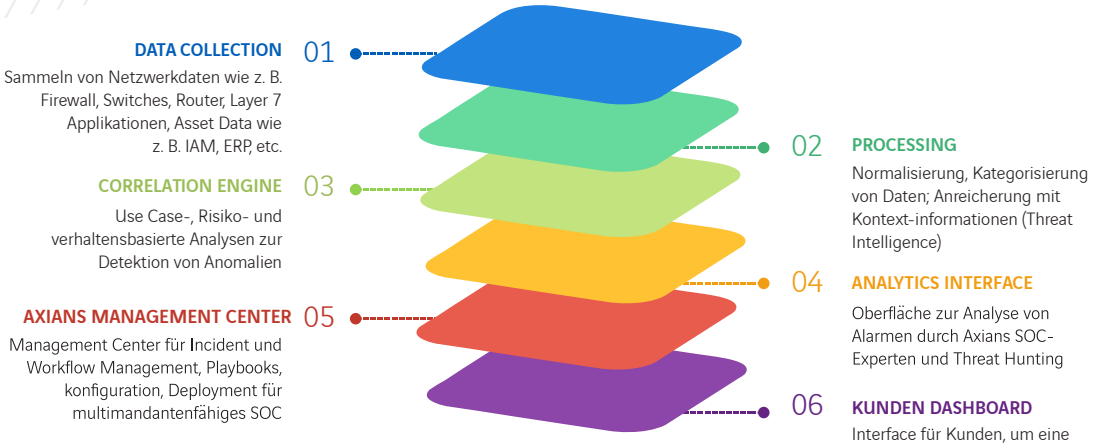


Ein SOC Service deckt die Aufgabenbereiche Detect, Respond und Recover aus dem NIST Cyber Security Framework ab und berücksichtigt dabei die oben aufgeführten Assets. Weitere Aufgaben können durch ergänzende Services (wie z. B. Schwachstellen Scanner, etc.) abgedeckt werden.

Was beinhaltet Axians IT/OT SOC?

Die Konvergenz von IT- und OT-Systemen in Kombination mit der zunehmenden Nutzung von Internet auch in industriellen Umgebungen stellt Unternehmen vor die Herausforderung Sicherheitsarchitekturen zu definieren, die sowohl Produktivität als auch Security gewährleisten. Kosten müssen niedrig gehalten werden bei gleichzeitiger Einhaltung von Industriestandards, Regularien und Richtlinien.

Axians hilft diese Konvergenz zwischen IT und OT Security zu meistern und dennoch im eigenen Kerngeschäft wettbewerbsfähig zu bleiben. Axians bietet Ihnen ein 360-Grad SOC-Service, inklusive der Integration der OT-Dimension in Kooperation unserer Schwestergesellschaft, Actemium. Im hochspezialisierten, ISO 27´001 zertifizierten IT/OT Security Operations Center im „UptownBasel" bietet Axians die Planung, Implementierung und Integration in Ihre Infrastruktur sowie den 24×7 Betrieb. Unsere Plattform ist dabei das Herzstück, die einen an Ihre Bedürfnisse angepassten Einsatz erlaubt. Ständige Updates, integrierte Threat Intelligence und laufende Verbesserungen sind inklusive. Von der Log-Daten-Analyse bis zu massgeschneidertem Reporting im Kunden-Dashboard. Wir bieten den Service im vollständigen Prozess über die Datensammlung bis hin zum Kunden Dashboard.



Ebenen der Axians SOC-Plattform

Ein SOC ergänzt die Analysetools eines SIEMs durch erweiterte Threat Hunting Funktionalitäten wie Advanced Threat Intelligence Lösungen, Network Anomaly Scanner, integriertem Schwachstellen-Management, sowie forensische Cyber-Security-Analysetools zur erweiterten Eingrenzung von möglichen Bedrohungssituationen.

Gemeinsam stark: Hybrides SOC

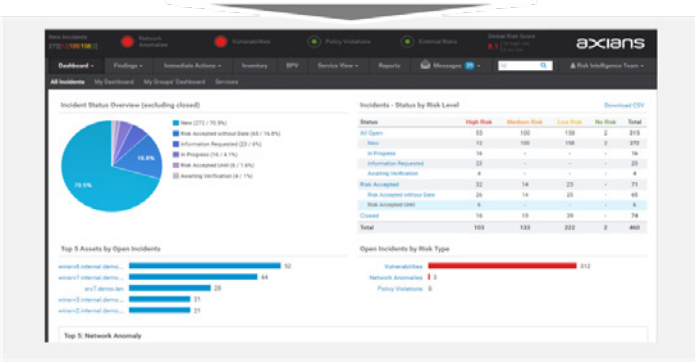
Die Auslagerung eines Security Operations Center setzt eine enge Zusammenarbeit zwischen der Kunden-Organisation und unseren Sicherheitsexperten voraus. Daher sehen wir eine Kooperation mit Ihnen als Partnerschaft, mittels welcher beide Organisationen gemeinschaftlich Herausforderungen meistern. Unsere Lösung bietet Ihnen einen SOC Service von der Datensammlung bis hin zum Kunden Dashboard.

Reporting & Dashboard

Ein intuitives und übersichtliches Reporting bzw. Dashboard ist einer der Kernbestandteile unseres Services. Übersichtliche Berichte helfen unseren Kunden immer alle Informationen zu Sicherheitsvorfällen und deren zugehörigen KPIs im Blick zu behalten. Hierbei unterscheiden wir in zwei verschiedene Reports, welche wir Ihnen zur Verfügung stellen. Dem CISO-Report als Basis für kritische Risikœntscheide und SIEM-Dashboard mit real-time Darstellung aller aktuellen Sicherheitsinformationen.

CISO - Report

Dashboard für CERT mit allen aktuellen Informationen



Ihre Vorteile auf einem Blick

- **Schnelle Erkennung von Cyber-Security-Vorfällen**, auch bei komplexen Szenarien
- **Schutz** der geschäftskritischen Assets und **Sicherstellung** von regulatorischen Anforderungen
- **Früherkennung der Bedrohungslage** und Einschätzung des Impacts auf kritische Dienste
- **Stufengerechte Reports** zur aktuellen Sicherheitslage im Unternehmen
- **Analyse und automatische Korrelation** aller relevanten Ereignisse mit Hilfe von künstlicher Intelligenz und menschlicher Expertise
- **24x7 Überwachung** - Schnelle Erkennung von Hackern, die sich im Unternehmensnetzwerk verbirgen
- **Direkte Kundenschnittstelle zum SOC Service** - Umgehende Reaktion auf Sicherheitsvorfälle durch Axians Cyber-Security Experten
- **Gemeinsam Stark – Hybrides SOC:** enge Zusammenarbeit zwischen Kunden und Axians
- **Integration in Kunden-Infrastruktur** (beispielsweise Kunden-Ticketsystem)
- **Ihre Daten, unsere Priorität:** Datenhaltung in der Kunden-Infrastruktur
- **Think Global – Protect Local:** Schweizer SOC im Kompetenzzentrum „UptownBasel", neben 9 weiteren SOC Hubs in der EMEA Region
- **Kostenreduktion** - Kein eigenes Personal für den Betrieb notwendig.
- **IT/OT Konvergenz durch Axians und Actemium** – Best of IT & OT
- **Höchste Qualität und Informationssicherheit** – ISO 9001 und ISO 27001 zertifiziertes IT/OT SOC

Integriertes Managementsystem
ISO 9001 ISO/IEC 27001

VINCI ENERGIES
CREATING YOUR DATA-DRIVEN FACTORY

ACTEMIUM axians

Industrial performance - digitally improved.

01/2023

axians

Axians IT Services AG · Arlesheim · Rotkreuz · Zürich
Tel.: +41 61 716 70 70
E-Mail: info-ch.security@axians.com · www.axians.ch / soc24x7.services