axians

KOMPLEXE ANALYSEN. ECHTZEIT PROZESSE.

SOC-as-a-Service

Security Operations Center (SOC) by Axians

Axians Deutschland ist ein agiles Unternehmensnetzwerk aus spezialisierten ICT-Dienstleistern und Softwareherstellern unter der globalen ICT-Marke Axians der VINCI Energies. Dank einer flächendeckenden Präsenz in 24 Städten bietet Axians unmittelbare Nähe zum Kunden.

Anfang 2018 hat Axians zwei Security Operations Center in Deutschland aufgebaut. Nicht nur in Deutschland betreibt Axians SOC, sondern auch international: Portugal, die Niederlande, Tschechien, Frankreich und Schweiz sind ebenfalls mit einem Experten-Team und eigenem SOC aufgestellt. Durch die Inanspruchnahme von internationalen SOC-Dienstleistungen profitieren Axians-Kunden von länderübergreifender Security-Expertise.

Das Threat Intelligence Center Europe, ein virtuelles Team von Security-Experten aus ganz Europa, analysiert grenzübergreifend aktuelle Angriffsszenarien und Zusammenhänge bei Sicherheitsvorfällen. Dazu gehört ein Computer Emergency Response Team, AlliaCERT by Axians, das aktuelle Sicherheitsbedrohungen erkennt, analysiert und Warnungen sowie Handlungsempfehlungen ausspricht.

Darüber hinaus hat Axians eine internationale Allianz gegen Internetkriminalität mit Axians Mitgliedern aus Europa gegründet: den Cyber Security Club. Der internationale Austausch und die Zusammenarbeit zu Security-Themen ist für Axians besonders wichtig und bietet Kunden einen großen Mehrwert. Daher finden regelmäßig Konferenzen der Security-Experten zu den wichtigsten Security-Themen statt. So kann Axians seinen Kunden Cyber Security mit europaweiter Fachexpertise bieten.

SOC: Das Zentrum der Cyber Security

Was ist ein SOC?

Die Zahl der Unternehmen, die zielgerichteten Angriffen ausgesetzt sind, steigt. Ihr Unternehmen konnte bisher keinen Sicherheitsvorfall verzeichnen? Dies könnte ebenso bedeuten, dass die Angreifer noch unbemerkt in Ihrem Unternehmen aktiv sind. Laut einer aktuellen Studie von Bitcom und F-Secure sind 67% der Unternehmen von Angriffen betroffen. Diese Angriffe bleiben zum Teil monatelang unerkannt, sodass sensible und hochwertige Daten problemlos entwendet werden können.

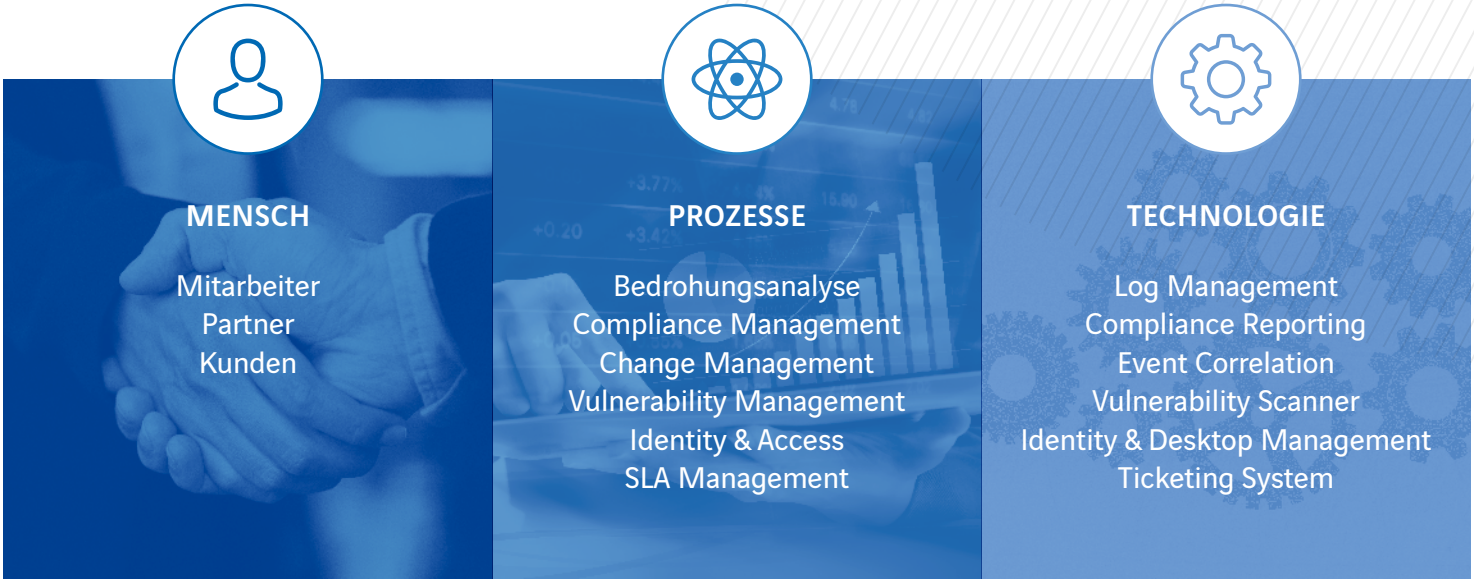
Um diese Angriffe zu vermeiden sind herkömmliche, rein präventive Sicherheitsmaßnahmen nicht ausreichend. Die Qualität der Angriffe erhöht sich zunehmend, was es selbst Großkonzernen schwer macht die vielfältigen Gefährdungen durch Internetkriminalität im Alleingang zu beherrschen. Wichtig ist, sich im Klaren zu sein, dass technische Security-Lösungen ihr volles Potential nur im gemeinsamen Zusammenspiel entfalten können. Zum Einen werden proaktive Gegenmaßnahmen benötigt, zum Anderen muss eine Abwehr zielgerichtet und Unternehmensübergreifend erfolgen, um Synergien nutzen zu können.

Ein SOC ist ein Zusammenspiel in Echtzeit aus Experten, Werkzeugen und Prozessen mit einem klaren Ziel: Nicht nur gegen bekannte Angriffe zu schützen, sondern auch unbekannte Angriffsmethoden proaktiv zu erkennen und sofortige Gegenmaßnahmen einzuleiten. Hier laufen also alle Fäden der Cybersicherheit zusammen.

Wichtig ist, das ein SOC im Schichtbetrieb funktioniert, um Angreifern rund um die Uhr standhalten zu können. Nicht nur der Personalbedarf eines eigenen SOC übertrifft häufig die Möglichkeiten unserer Kunden, auch der akute Fachkräftemangel ist ein erschwerender Faktor.

SOC by Axians: Erreichen Sie die Fähigkeit auf professionelle Angreifer herabsehen zu können.

Die Aufgaben des SOC-Teams im Überblick



MENSCH

Mitarbeiter
Partner
Kunden

PROZESSE

Bedrohungsanalyse
Compliance Management
Change Management
Vulnerability Management
Identity & Access
SLA Management

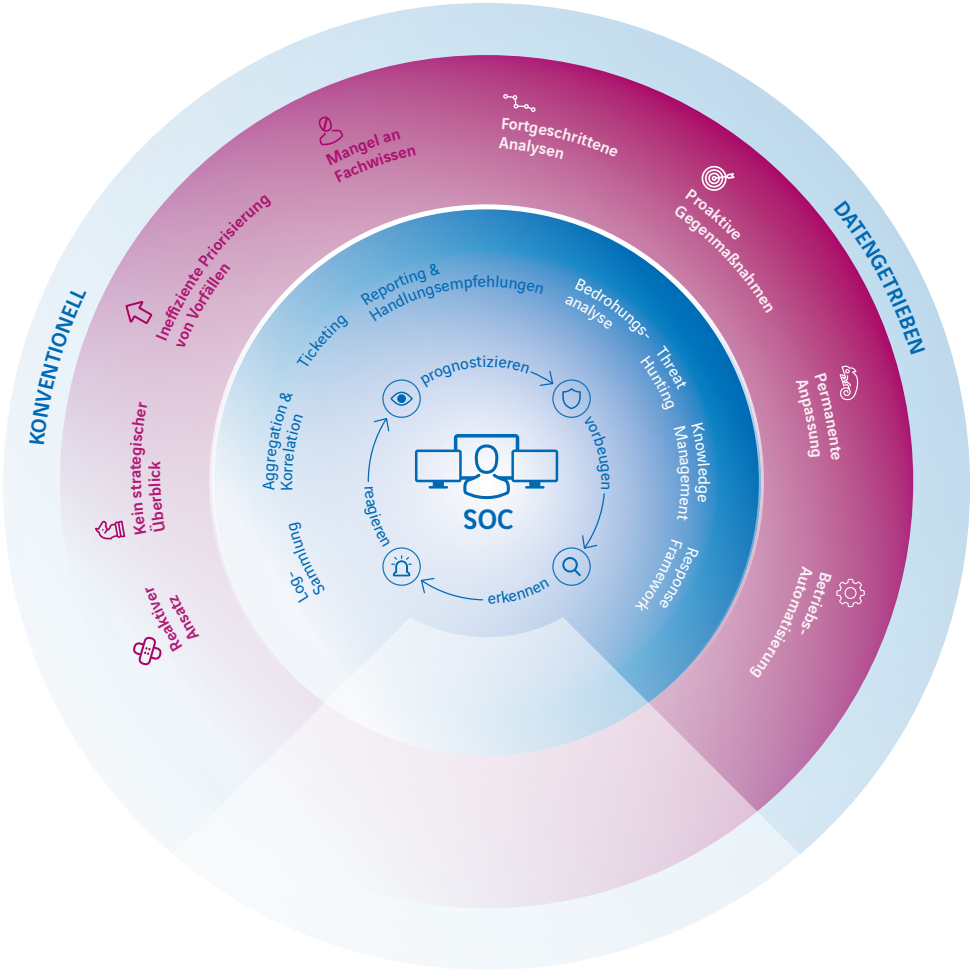
TECHNOLOGIE

Log Management
Compliance Reporting
Event Correlation
Vulnerability Scanner
Identity & Desktop Management
Ticketing System

Die Kommandobrücke der Cyber Security: SOC-as-a-Service

Im Axians SOC laufen alle Informationen zu relevanten Angriffsszenarien zusammen. Unsere Cyber Threat Analysten erstellen für Ihre individuellen Bedürfnisse ein angemessenes Regelwerk für das SOC und analysieren, welche Unternehmenswerte wie viel Schutz benötigen, an welchen Stellen die IT-Systeme ungeschützt sind und angegriffen werden, ebenso deckt ein SOC Motive, Methoden und Werkzeuge potenzieller Cyberkriminelle auf.

Dazu untersuchen unsere Cyber Threat Analysten im SOC den Datenverkehr des Unternehmens auf Anomalien. Die Big-Data Analyse erfolgt gesetzeskonform und wo erforderlich anonymisiert. Erweist sich eine erkannte Anomalie als sicherheitsrelevant, bekämpft das SOC den Angriff im Initialstadium und begrenzt seine Wirkung auf ein Minimum.



Ihre Vorteile mit SOC-as-a-Service von Axians

24/7 Überwachung aller sicherheitsrelevanten Loginformationen und **Monitoring** der Sicherheitssysteme

Eröffnen von Incidents und **Problem-Analyse,** inklusive **Unterstützung von AlliaCERT by Axians** bei forensischen Untersuchungen

Unsere Cyber Threat Analysten setzen sich permanent mit der **aktuellen Bedrohungslage** auseinander und **analysieren Informationen** aus allen relevanten Quellen

Durchführung von **Abwehrmaßnahmen bei Angriffen** durch unsere Experten. Hierbei werden viele **Angriffe schon im Vorfeld vermieden**

Effizienter Einsatz Ihrer Mitarbeiter: **Axians übernimmt die komplette Betreuung des SOC**

Cognitive oder AI-Systeme **analysieren Trends,** destillieren aus Millionen von Daten **entscheidende Informationen** und entwickeln daraus **effektive Abwehrmaßnahmen**

Permanente Anpassung der Abwehrstrategie durch Pentester und Analysten

Regelmäßiges Reporting und Handlungsempfehlungen bieten Ihnen Transparenz und somit eine detaillierte Grundlage bei Security-Entscheidungen

Wiederherstellung von Daten und Nachweisen nach einem Sicherheitsvorfall

Das SOC besitzt die notwendigen Kompetenzen und Know-how für die **Unterstützung bei der Planung und Priorisierung Ihrer Budgetierung**

Kontinuierliche Verbesserung der Regeln und Verfahrensweisen des SOC, um dessen Fähigkeiten permanent weiterzuentwickeln, neue Angriffstechniken zu erkennen und deren Vorfallsbehandlung zu beschleunigen

Proaktives Threat Hunting zur **Erkennung bislang unbekannter Gefahren und Angriffe**

Wählen Sie je nach Anforderungen das passende SOC-Modell

Nähere Informationen zu den jeweiligen Modellen und Modulen finden Sie auf der nächsten Seite.

Die Axians SOC-Modelle im Überblick:

SOC-AS-A-SERVICE

Neben den Vorteilen der untenstehenden Modelle bieten unsere Axians Security-Experten forensische Analysen Ihrer Systeme und Netzwerke. Daten können im Falle eines Sicherheitsvorfalls wiederhergestellt werden und Cyberkriminelle Aktivitäten können rückverfolgt werden.

Außerdem besteht das Axians SOC-as-a-Service Modell zusätzlich aus folgenden Modulen:

E-Mail Security

- Kein klassischer Anti-Virus: Sandboxing kann Schadsoftware auch ohne Signaturen erkennen
- Tiefenprüfung auf CPU-Ebene
- Bestmögliche Erkennungsrate: Prüfung auf Betriebssystemebene
- Sofortige Bereitstellung von gesichertem Content oder sicher wiederhergestellten Versionen von potenziell schadhaften Dateien

OT Security

- Lückenlose Überwachung aller Kommunikationsflüsse in industriellen Netzwerken
- Reduktion von Ausfallzeiten
- Zuverlässiges und schnelles Erkennen jeglicher Angriffe von innen und außen

Network Intrusion

- Auffälliges Verhalten im Netzwerk wird durch künstliche Intelligenz erkannt
- In Zusammenarbeit mit Vectra wird eine Kombination aus Methoden der Data Science, des maschinellen Lernens sowie der Verhaltensanalyse angewendet
- Automatische Erkennung eines unbefugten Zugriffs durch umfassende und kontinuierliche Analyse des internen und Internet-Netzverkehrs

Schwachstellen-Management

- Integration der Schwachstellen-Scanner, sowie qualifizierte Unterstützung bei der Priorisierung, Bewertung und Behebung von Schwachstellen
- Konfiguration über die Cloud-Plattform und Ausführung auf eigener Systemumgebung

BASIC+

Ergänzen Sie die Analysefähigkeiten Ihres SOC durch den Einsatz Verhaltensbasierter Analysen von Benutzern, Systemen und des Netzwerkverkehrs. Sie erhalten Einblick in Insider-Bedrohungen und detaillierte individuelle Risikobewertungen.

Das Axians Basic+ Modell umfasst zudem folgende Module:

- Netzwerk und Asset-Klassifikation
- Logdaten-Analyse in Echtzeit
- Threat Detection, dank Axians Use Case Engineering
- Threat Intelligence

BASIC

Axians betreibt sämtliche Systeme für Ihr SOC und überwacht Ihre IT-Infrastruktur in Echtzeit, rund um die Uhr, analysiert potentielle Sicherheitsvorfälle und leitet bei Bedarf entsprechende Gegenmaßnahmen ein.

Das Axians Basic Modell umfasst zudem folgende Module:

- AlliaCERT by Axians
- Incident Response

Das passende SOC-Modell noch nicht dabei?

Gerne passen wir die Varianten auf Ihre Bedürfnisse an.

Jetzt Buchungsanfrage stellen
www.axians.de/security

IHR ANSPRECHPARTNER

Thomas Scharff

Telefon: +49 40 271661-0

E-Mail: info-itsecurity@axians.de

Axians IT Security GmbH · Christoph-Probst-Weg 27 · 20251 Hamburg
Tel.: +49 40 271661-0 · Fax: +49 40 271661-44 · E-Mail: info-itsecurity@axians.de · www.axians.de