Axians SOC Service für Endpoints

Mit unserem Service reduzieren Sie die Angriffsflächen Ihres Unternehmens, verhindern Malware-Infektionen, erkennen und entschärfen potenzielle Bedrohungen in Echtzeit und automatisieren Reaktions- und Abwehrmassnahmen.

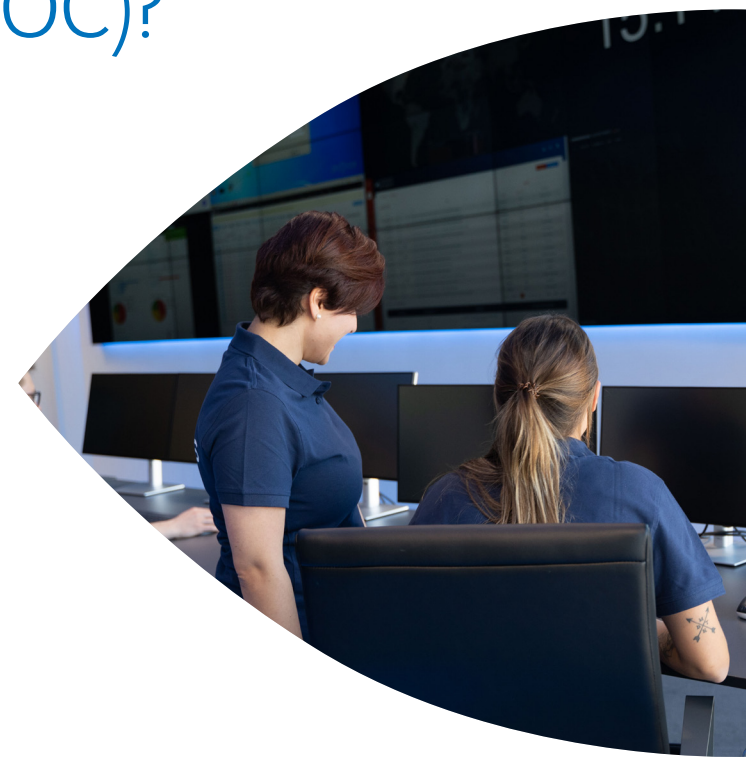
GEFAHR VOR DEM UNBEKANNTEN

Herausforderungen unserer Kunden

In der heutigen digital vernetzten Welt stehen Unternehmen vor einer wachsenden und immer komplexeren Bedrohungslandschaft. Ein besorgniserregendes Problem ist, dass viele Unternehmen nicht einmal sicher sind, ob sie bereits Ziel eines Cyberangriffs wurden. Die Dynamik von Cyberbedrohungen hat sich im Laufe der Jahre erheblich verändert. So erhöht die wachsende Vernetzung von Systemen – von traditionellen IT-Netzwerken bis hin zu IoT-Geräten – die potenzielle Angriffsfläche. Zusätzlich zur technischen Komplexität verschmelzen IT (Informationstechnologie) und OT (Betriebstechnologie) immer stärker, wobei beide oft unterschiedliche Sicherheitsstandards und -protokolle aufweisen. Und als ob das noch nicht genug wäre, werden Kriminelle zunehmend raffinierter. Sie nutzen fortschrittliche Techniken und künstliche Intelligenz, wie zum Beispiel Tools wie WormGPT, um traditionelle Sicherheitsmassnahmen zu überlisten.

Wie hilft ein Security Operations Center (SOC)?

Angesichts dieser wachsenden und sich ständig weiterentwickelnden Herausforderungen ist eine proaktive Verteidigungsstrategie unerlässlich. Hierbei zeigt sich der Wert eines Security Operations Center (SOC). Ein SOC ist nicht nur ein physischer Ort oder eine Organisationseinheit, sondern vielmehr ein Bollwerk gegen Cyberbedrohungen. Es besteht aus einem spezialisierten Team von Sicherheitsexperten, die rund um die Uhr die Netzwerksicherheit überwachen, Bedrohungen in Echtzeit analysieren und darauf reagieren. Durch den Einsatz modernster Technologien und fortgeschrittener Analysetools können SOCs potenzielle Angriffe frühzeitig erkennen, bevor sie Schaden anrichten. Dies ermöglicht es Unternehmen, nicht nur zu reagieren, wenn etwas passiert, sondern proaktiv Massnahmen zu ergreifen, um Angriffe von vornherein zu verhindern. Ein gut ausgestattetes und effizient arbeitendes SOC kann somit die Sicherheitslage eines Unternehmens erheblich verbessern und Vertrauen bei Kunden und Partnern aufbauen.



GEFAHREN ERKENNEN UND RICHTIG REAGIEREN

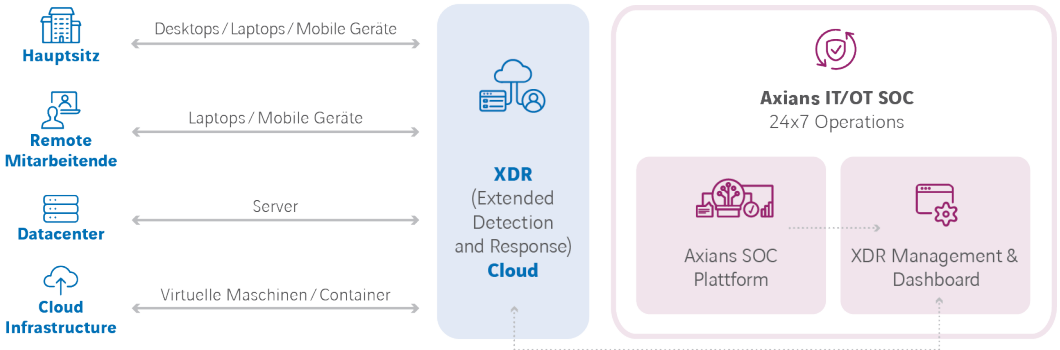
Axians SOC setzt auf XDR

Axians verlässt sich in seinem Security Operations Center auf die fortschrittliche XDR-Technologie (Extended Detection and Response), um Unternehmen vor digitalen Bedrohungen zu schützen. Somit revolutioniert Axians den Ansatz der Endpoint-Sicherheit, indem es die Vorteile einer Endpoint Protection Plattform (EPP) und Endpoint Detection and Response (EDR) nahtlos vereint. Mit seiner einzigartigen Kombination aus präventiven und reaktiven Funktionen bietet Axians eine umfassende Endpoint-Sicherheitslösung für Unternehmen. Bei der Integration des Services arbeitet Axians

eng mit dem Kunden zusammen, beginnend mit Konzept und Projektplanung, über die Installation und Konfiguration der XDR-Lösung bis hin zur Netzwerkeinrichtung. Einmal eingerichtet, bietet das SOC kontinuierliches Monitoring, Alarm-Triage und gezieltes Sicherheitsvorfallmanagement. Darüber hinaus übernehmen die Experten von Axians das Patch-, Release- und Change-Management und legen einen besonderen Fokus darauf, die Rate der False-Positives kontinuierlich zu reduzieren, um effiziente und zielgerichtete Sicherheitsmassnahmen zu gewährleisten.

Service-Architektur

Die Service-Architektur umfasst die Installation von Agenten auf allen Endpoints, einschliesslich Windows-, Mac OS X- und Linux-basierten Geräten. Diese Agenten überwachen kontinuierlich die Endpoints, blockieren bekannte Angriffe und senden Alarme an das Security Operations Center (SOC), wenn potenzielle Sicherheitsvorfälle erkannt werden.



Kunden-Infrastruktur

Leistungspakete

LEISTUNG	SILBER	GOLD
Analyse von Alarmen	9x5	24x7
Service Review Meetings	Quartalsweise	Monatlich
Reaktionszeiten	2 Stunden	2 Stunden
Endpoint Service	ja	ja
Service Tuning (Reduktion von False Positives)	ja	ja
Threat Intelligence	ja	ja
Kunden-Webportal	ja	ja
Patch-, Update-, Problem-, Change-Management	ja	ja
Hot based Vulnerability Management	ja	ja
Penetration Testing	Optional	Optional
Incident Response Retainer	Optional	Optional

IHR ANSPRECHPARTNER

Kaan Tanriverdi (Presales Consultant)

E-Mail: kaan.tanriverdi@axians.com

08/2024

Axians IT Services AG · Arlesheim · Lausanne · Zürich
Tel.: +41 61 716 70 70
E-Mail: consulting-ch.security@axians.com · www.axians.ch