

„Das neue SOC ermöglicht uns den Zugang zu fortschrittlichen Funktionen und Sicherheitstechnologien, und es verbessert auch spürbar die Unternehmens-Performance.“

Christian Schmidhofer, Vice President IT,
Kontron Europe GmbH

REFERENZ

Kontron Europe GmbH

Managed SOC für maximale Cybersicherheit

Projektumfeld

Kontron ist ein globaler Spitzenreiter im Bereich IoT/Embedded Computer Technologie (ECT). Mit einem aus Hardware, Software und Services kombinierten Portfolio bietet das seit 1959 bestehende Unternehmen mit über 1.200 Mitarbeitenden maßgeschneiderte Lösungen für das Internet der Dinge (IoT) und die Industrie 4.0 an.

In jüngster Zeit haben Hacker ihr Augenmerk vermehrt auf die IoT-Branche gerichtet. Dies hat zu einer zunehmenden Bedrohungslage geführt und die Anforderungen an die Cybersicherheit auch bei Kontron stark erhöht. Deshalb sollte ein neues SOC (Security Operations Center) implementiert werden, welches der Überwachung, Echtzeiterkennung und schnellen Reaktion auf Cybervorfälle dient. Gleichzeitig wurde ein Managed Security Service Provider benötigt, der die Betreuung der Sicherheitsinfrastruktur im SOC rund um die Uhr übernimmt.

Die Wahl fiel Kontron leicht: Als langjähriger Stammkunde der Axians – ehemals XTRO/München und nun Teil der Axians – konnte man auf ein sehr gutes Vertrauensverhältnis aufbauen. Bereits in mehreren Projekten hatte sich die Axians als zuverlässiger Partner erwiesen, der in puncto Planung, Installation sowie Betrieb verlässlich arbeitet und dabei ein herausragendes Preis-/Leistungsverhältnis bietet.

Nachdem Axians ebenfalls aufzeigen konnte, dass hinter dem SOC ein breit aufgestelltes Team mit tiefem Wissen und praktischer Erfahrung steht, das nicht nur die IT-, sondern auch OT-Security umfassend abdeckt, war Kontron vollends überzeugt.

Projektanforderungen & Projektziele

In einem gefährdeten Umfeld löst ein SOC das Problem der proaktiven Erkennung und schnellen Abwehr von Cyberbedrohungen. Denn die zunehmende Verbreitung von vernetzten Geräten und Systemen ermöglicht es den Angreifenden, neue Eintrittspunkte und potenzielle Schwachstellen leichter auszunutzen. Gleichzeitig stehen Unternehmen wie Kontron mit der zunehmenden Komplexität und Raffinesse der Cyberangriffe vor der großen Herausforderung, die eigenen digitalen Assets rund um die Uhr schützen zu müssen. So sollte das SOC neben geeigneten Tools und Prozessen einen dedizierten Service beinhalten, der die eigene Sicherheitsinfrastruktur 24x7x365 überwacht.

Das Projektziel war damit eine Kombination von **optimierter Sicherheit mit reduzierter Reaktionszeit und effektiv entlasteten internen IT-Ressourcen**. Dazu kamen die proaktive Überwachung sowie Reaktion auf Cyberbedrohungen, die auch außerhalb der Bürozeiten gewährleistet sein sollte.

AUFGABE / ZIEL

- Kontinuierliche Überwachung der Sicherheitsinfrastruktur
- Proaktive Erkennung und schnelle Abwehr von Cyberbedrohungen
- Effektive Entlastung interner IT-Ressourcen

LÖSUNG

- Implementierung eines SOC (Security Operations Center)
- Integration der Sicherheitslösung SentinelOne
- Nutzung der Managed Services der Axians

NUTZEN

- Optimale Absicherung der digitalen Assets und Unternehmensressourcen
- Echtzeiterkennung und schnelle Reaktionsfähigkeit auf Security Incidents
- Ausgelagerte Betreuung und Überwachung rund um die Uhr

REFERENZ

Kontron Europe GmbH

Auch menschlich musste es passen, denn von seinem Managed-Security-Service-Provider (MSSP) wünschte sich Kontron vor allem Zuverlässigkeit, eine hohe Erreichbarkeit und ein breit aufgestelltes Team mit umfassendem Know-how.

Umsetzung

Nach der Vertragsvereinbarung startete Axians mit der Implementierung der führenden EDR-Lösung (Endpoint Detection and Response) von SentinelOne. Diese sammelt Daten aus unterschiedlichsten Quellen wie Endpunkten, Cloud-Servern und Netzwerken, um Bedrohungen automatisiert zu analysieren und kürzere Reaktionszeiten zu ermöglichen.

Das Onboarding in das IT/OT SOC (Security Operations Center) konnte innerhalb kurzer Zeit erfolgen, da die Lösung von SentinelOne Agent-basiert ist. Um die Systeme von Kontron bestmöglich vor Cyberangriffen zu schützen und eventuelle Sicherheitsprobleme frühzeitig zu beheben, führt Axians regelmäßig Threat Hunting durch.

Dazu kommen die umfassende Betreuung und Überwachung via Managed Services, bei der ein erfahrenes Team aus Sicherheitsexperten und -expertinnen rund um die Uhr dafür sorgt, Bedrohungen in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren.

Projektergebnis

Seit Anfang Juli 2023 ist das SOC im Einsatz. Dank der zentralen Cyber-Security-Leitstelle kann Kontron sich stets darauf verlassen, dass die eigenen Daten, digitalen Assets und Unternehmensressourcen optimal abgesichert sind.

Dabei hat der Entschluss, die vorhandene Lösung zu ersetzen, den Zugang zu fortschrittlichen Funktionen und modernsten Sicherheitstechnologien ermöglicht und auch zu einer spürbar verbesserten Leistung geführt. Dazu kommt der Managed Service der Axians, der für eine zuverlässige Betreuung und Überwachung der Sicherheitsinfrastruktur sorgt.

Kontron ist mit der Lösung sehr zufrieden und schätzt es, dass sie eine höhere Performance bietet und dadurch den Schutz wertvoller Ressourcen und Daten weiter optimiert. Dazu verfügt das Unternehmen über die gewünschte Kombination von Technologien, Prozessen und qualifiziertem Personal, um in Sachen Sicherheit bestens für die Zukunft gerüstet zu sein.

KUNDENINFO



Unternehmen: Kontron Europe GmbH

Branche: IoT/Embedded Computing Technology (ECT)

Gründung: 1959

Dimension: Über 1.200 Mitarbeitende sorgen dafür, dass verschiedenste Branchen innovative Lösungen in den Bereichen Internet der Dinge (IoT) und Industrie 4.0 erhalten.

Internet: www.kontron.com/de

ÜBER AXIANS

Die Axians-Gruppe in der Schweiz ist Teil des globalen Markennetzwerks für ICT-Lösungen von VINCI Energies. Mit einem ganzheitlichen ICT-Portfolio unterstützt Axians Unternehmen, Kommunen, öffentliche Institutionen, Netzbetreiber und Service Provider bei der Modernisierung ihrer digitalen Infrastrukturen und Lösungen. In den Geschäftsbereichen in der Schweiz sorgen Berater, Entwickler und Techniker dafür, das Leben von Menschen zu verbessern – etwa durch Breitbandausbau, Cloud- und Data-Center-Infrastrukturen, Cybersicherheit, Enterprise Networks, IoT-Plattformen und führende Software für die öffentliche Verwaltung.

KONTAKT

E-Mail: info-ch.security@axians.com · Tel.: +41 61 716 70 70

axians.ch

Stand 12/23