infopulse

Fallbeispiel für **Hersteller von Industrielösungen**

Ein SOC mit einem Cloud SIEM/SOAR-System verbesserte die Sicherheitslage eines Schweizer Herstellers_

24/7 Monitoring und Incident Response mit Azure Sentinel
für einen führenden Hersteller

Branche: **Herstellung** **Ort:** **Schweiz** **Mitarbeiter:** **über 3.500**

Über den Kunden

Unser Kunde ist einer der weltweit führenden Anbieter von Spitzenlösungen für Industrieprodukte. Mit einer Präsenz in über 30 Ländern versorgt unser Kunde seine Kunden aus den unterschiedlichsten Branchen mit maßgeschneidertem und umfassendem Know-how.

Anforderung

Der Kunde trat an Infopulse mit der Bitte heran, seine Sicherheitslösungen zu synchronisieren und zu zentralisieren. Die Einrichtung eines Security Operations Center (SOC) war ein vorrangiges Ziel und die beste Möglichkeit, professionellen Service, Branchenexperten und solides Sicherheitsmanagement in einer Lösung zu vereinen.

Da unser Kunde zahlreiche Niederlassungen mit unterschiedlichen Standards und Prozessen betreibt, sah er sich mit der Herausforderung konfrontiert, die Cybersecurity-Standards und -Richtlinien zu synchronisieren und einen besseren Einblick in die Sicherheitsprozesse zu erhalten. Nach sorgfältiger Abwägung der Kundenbedürfnisse empfahlen wir Azure Sentinel von Microsoft als die geeignetste Sicherheitsplattform im Hinblick auf ihre wirtschaftliche und technische Effizienz. Es passte perfekt, da unser Kunde bereits über ein Microsoft-Ökosystem verfügte, das einfachere integrierte Integrationen und geringere Gemeinkosten ermöglichte.

Lösung

Im Zeitraum von 6 Monaten implementierte das Infopulse-Team Azure Sentinel als SIEM/SOAR-Plattform, um die Sicherheitsabläufe des Kunden zu erleichtern.

In der Onboarding-Phase führten wir eine eingehende Sicherheitsbewertung der Infrastruktur, der Geschäftsprozesse und der Arbeitsabläufe der User des Kunden durch, um einen maßgeschneiderten SOC-Implementierungsplan zu erstellen.

3 zentrale Elemente eines SOC

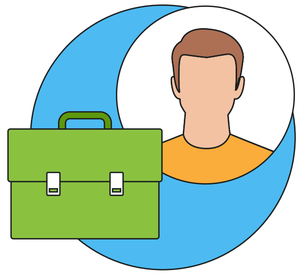
Bevor wir mit der Einrichtung des SOC begannen, definierten und vereinbarten wir die wichtigsten Aspekte mit dem Kunden:

1. Eine leistungsstarke technische Plattform:

Wir entschieden uns für Azure Sentinel als SIEM/SOAR-Lösung, um ein hohes Maß an Ausfallsicherheit für geschäftskritische Systeme zu gewährleisten.

2. Leistungsumfang:

Wir definierten relevante Anwendungsfälle, die durch den SOC-Service abgedeckt werden mussten, indem wir die Kernaspekte der Infrastruktur des Kunden identifizierten.



3. Zusammenstellung eines Teams:

Im Rahmen eines Modells der geteilten Verantwortung boten wir ein Team von Branchenexperten mit den passenden Fähigkeiten für die Analyse von Vorfällen, das Management und Empfehlungen an.

Die Einrichtung des SOC umfasste die folgenden Aktivitäten:

- Bereitstellung einer Cloud-basierten Azure-Sentinel-Lösung für die Azure-Umgebung des Unternehmens
- Aufbau eines Teams von Sicherheitsexperten für den Level1/Level2-Support
- Ermöglichen eines schrittweisen Onboardings zur Anbindung der verschiedenen Regionen an die Plattform, abgestimmt auf das interne Reorganisationsprojekt
- Konfiguration der Protokollerfassung von Cloud-basierten und lokalen Systemen wie Domain-Controllern, Firewalls und Antivirenprogrammen; Entwicklung benutzerdefinierter Konnektoren
- Einrichtung von Prozessen, die eine kontinuierliche Überwachung, eine schnelle Reaktion auf Vorfälle und eine Eskalation an das interne Team ermöglichen
- Entwicklung einer Reihe von benutzerdefinierten Anwendungsfällen zusätzlich zu den eingebauten, um spezifische, für die Kundenumgebung relevante Bedrohungen abzudecken
- Initiierung der Entwicklung eines einheitlichen Dashboards für die Sicherheitsüberwachung in Echtzeit
- Unterstützung des Kunden bei der Einführung des EDR-Systems für eine bessere Sichtbarkeit der Endpunkte und eine schnellere Bedrohungsabwehr
- Automatisierung des Incident Response-Prozesses, um den Druck auf das Sicherheitsteam durch das Alarmmanagement zu verringern

Technologien

Azure Sentinel

Azure Logic Apps

Custom Log Parsing Scripts

Jira

Azure Arc

O365 Identity Protection

Commercial threat intelligence feeds

FortiEDR and others

Ergebnis

Durch die umfassende Sicherheitsprüfung und die Einrichtung eines SOC hat der Kunde Einblick in seine Sicherheitslage gewonnen und kann nun seine Sicherheitsstrategie optimieren. Das Projekt brachte folgende Vorteile:

- ein neu eingeführter proaktiver Ansatz für die Cybersecurity
- deutlich geringeres Risiko von Datenschutzverletzungen und Cyberangriffen
- monatlich werden mehr als 500 Sicherheitsvorfälle entdeckt und behoben
- Ausgereifte Sicherheitsstufe hinsichtlich der Sicherheitsmaßnahmen
- Ermöglicht 24/7-Überwachung und Schwachstellen-Scanning in den Niederlassungen des Kunden in Mitteleuropa, Asien sowie Nord- und Südamerika
- Ausarbeitung umfassender Empfehlungen zur Feinabstimmung der internen Sicherheitsrichtlinien und zur Stärkung des Schutzes der Arbeitslasten des Unternehmens

Seit Februar 2021 erbringt Infopulse weiterhin diesen SOC-Service und fungiert derzeit als vertrauenswürdiger Sicherheitsberater für den Kunden.

Über Infopulse

Infopulse, Teil des führenden nordischen, digitalen Dienstleistungs-Unternehmens Tietoevry, ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Software-F&E, Anwendungsmanagement, Cloud- und IT-Betrieb sowie Cybersicherheit für KMUs und Fortune 100 Unternehmen auf der ganzen Welt. Das in 1991 gegründete Unternehmen verfügt über ein Team von über 2.300 Fachleuten und ist weltweit in 7 Ländern - in Europa sowie in Nord-, Mittel- und Südamerika - vertreten.

Infopulse genießt das Vertrauen vieler etablierter Marken wie BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group und vieler anderer.

Für weitere Informationen besuchen Sie bitte **www.infopulse.com/de**

Kontaktieren sie uns:

PL +48 (221) 032-442

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UK +44 (8455) 280-080

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

BR +55 (21) 99298-3389

info@infopulse.com