DAS SIEM-STARTERKIT

Schnell und effizient zu mehr OT-Sicherheit

Im Zeitalter der zunehmenden Vernetzung und Digitalisierung von Industrie- und Steuerungsanlagen ist die Sicherheit der Operational Technology (OT) von größter Bedeutung. Um den Schutz kritischer Infrastrukturen (KRITIS) und industrieller Prozesse zu gewährleisten, bedarf es daher eines Security Information and Event Management (SIEM) Systems, das neben der klassischen IT auch die OT im Visier hat.

Im Speziellen waren und sind Firmen und Organisationen aus den KRITIS-Sektoren durch das IT-Sicherheitsgesetz (IT-SiG) 2.0 dazu verpflichtet, bis Mai 2023 Systeme zur Angriffserkennung zu implementieren und zu betreiben.

EIN SIEM IMPLEMENTIEREN – LEICHTER GESAGT ALS GETAN?

In dem Fall nicht: Denn wir haben mit dem SIEM-Starterkit für die OT einen Ansatz entwickelt, mit dem Sie schnell und effizient die Sicherheit ihrer OT-Systeme verbessern können. Dank der pragmatischen Lösung muss im Unternehmen keine SIEM- und SOC-Struktur von Grund auf neu erfunden oder designt werden.

Wir nutzen das, was bereits vorhanden ist und setzen auf das Pareto-Prinzip, um schnellstmöglich mit bekannten Ressourcen, Prozessen und Mitteln ein erhöhtes Maß an Sicherheit zu gewährleisten. Daher basiert unser Ansatz auf der Nutzung bestehender IT-Use-Cases und -Prozesse in der OT-Umgebung sowie der Integration bekannter SIEM-Tools und -Methoden.

DIE FÜNF WICHTIGSTEN KOMPONENTEN UNSERES SIEM-STARTERKITS

1. Use-Case-Anpassung: Die IT-Use-Cases werden an die spezifischen Anforderungen der OT angepasst. Dies umfasst die Identifizierung kritischer Assets, das Erkennen von Anomalien und verdächtigen Aktivitäten sowie die Echtzeitüberwachung.

2. Log-Integration: Die OT-Geräte und -Systeme werden so konfiguriert, dass sie relevante Log-Daten an das SIEM-System senden. Dies ermöglicht eine umfassende Überwachung und Analyse.

3. Regelwerke und Alarme: Basierend auf den angepassten Use Cases werden Regelwerke und Alarme erstellt, um auf potenzielle Sicherheitsvorfälle hinzuweisen. Damit kann schnell auf Bedrohungen reagiert werden.

4. Angliederung an Prozesse und der Richtlinien der IT: In Rückgriff auf bereits bestehende Prozesse und Richtlinien der IT wird eine Dokumentation hinsichtlich Compliance und Prozessintegration geschaffen. Eine Mitnutzung bestehender Komponenten ist hierbei ausdrücklich erwünscht.

5. Schulung: SOC-Mitarbeiter:innen in der OT werden im Umgang mit dem SIEM geschult.

UNTERWEGS ZUR UMFASSENDEN OT-SICHERHEIT

Das SIEM-Starterkit bietet Ihnen eine praktische und kosteneffiziente Möglichkeit, die Sicherheit Ihrer OT-Systeme zu verbessern und den Anforderungen des IT-SiG 2.0 an die OT hinsichtlich Systemen zur Angriffserkennung zu begegnen – ohne erhebliche Investitionen tätigen zu müssen.

Ein weiterer Pluspunkt: Da das SIEM-Starterkit schrittweise mit Ihren Anforderungen wachsen kann, ist eine Skalierung zu jeder Zeit gewährleistet. Nutzen Sie vorhandene IT-Tools und -Prozesse und integrieren Sie diese mit uns nahtlos in die OT. Auf diese Weise ist bereits ein entscheidender Schritt auf dem Weg zur umfassenden OT-Sicherheit getan.

SIE MÖCHTEN MEHR ÜBER DAS SIEM-STARTERKIT ERFAHREN?

Sprechen Sie gern Ihren Account Manager an oder kontaktieren Sie uns über unsere Website: **www.computacenter.com/m/automotive/**

Computacenter

Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen

computacenter.com
+49 (0)2273 5970