Das Controlware OT-SOC

OT-Basispaket

Die Situation

Industrieunternehmen stehen heute vor großen Herausforderungen im Bereich der Cybersicherheit für ihre betriebstechnischen Systeme. Im Gegensatz zur IT-Welt, in der Systeme regelmäßig aktualisiert und ersetzt werden, beruhen OT-Umgebungen oft auf Legacy-Systemen. Diese Systeme sind meistens für stark spezialisierten Anwendungen und industrielle Steuerungen konzipiert, die speziell für langlebige Betriebszyklen entwickelt wurden und deren Austausch oder Modernisierung kostspielig und komplex ist. Gleichzeitig steigt der Vernetzungsgrad von OT-Systemen stetig an, um die Effizienz und Produktionsleistung zu steigern, was aber auch die Angriffsfläche erheblich vergrößert.

Um die Sicherheit von Infrastrukturen zu gewährleisten, benötigen Unternehmen Lösungen, die speziell auf die Anforderungen und den Schutz von OT-Netzwerken ausgerichtet sind. In vielen Unternehmen fehlt es jedoch an ausreichender Transparenz über die sicherheitsrelevanten Ereignisse und Schwachstellen. Dies erhöht zudem die Risiken. Nicht selten sehen Unternehmen sich oft in einem Spagat zwischen maximaler Verfügbarkeit der Systeme und einer soliden Sicherheitsstrategie gegenüber – eine Balance, die mit zunehmenden Bedrohungen immer schwieriger wird.

Die Herausforderung

Das OT-SOC-Angebot von Controlware unterstützt Unternehmen dabei, die Sicherheit und Zuverlässigkeit ihrer betriebstechnischen Systeme mithilfe spezialisierter Überwachungsdienste zu fördern.

Das Angebot umfasst:

- **8x5 Verfügbarkeit**
- **Fernwartung**
- **Datendioden**
- **VMS**
- **Anomalie-Erkennung**

Durch den Einsatz unserer spezialisierten Technologien und Verfahren ist es uns möglich, Bedrohungen frühzeitig zu erkennen und Risiken aktiv zu managen. Die Integration von Datendioden stellt dabei sicher, dass die OT-Umgebung bestmöglich abgeschottet bleibt, während die Fernwartung eine sichere externe Betreuung gewährleistet. Anomalien-Erkennung hilft zudem, verdächtige Aktivitäten bereits in der Entstehungsphase zu identifizieren und die Reaktionszeit auf Bedrohungen signifikant zu verkürzen.

Mit dem OT-Basispaket ist es möglich, dass OT-Systeme unter erhöhten Sicherheitsvorkehrungen kontinuierlich verfügbar bleiben und Ausfälle reduziert werden. Das OT-SOC von Controlware versetzt Unternehmen in die Lage, bessere Kontrolle und umfangreiche Transparenz über ihre OT-Systeme zu gewinnen, was in modernen OT-Umgebungen von großer Bedeutung ist. Damit lassen sich Betriebsstabilität und Schutz der OT-Assets langfristig unterstützen – ein Ansatz, der potenziell Risiken mindert und das Vertrauen in die betriebliche Infrastruktur stärk.

Erweiterungsmodule: OT-Leitstand

1. Erweiterungsmodul: SIEM

Mit dem **SIEM-Erweiterungsmodul** bietet Controlware eine zuverlässige Lösung für den operativen Betrieb Ihres OT-Security Operations Centers (SOC). Die Basis bildet die Plattform **Splunk**, die eine zentrale Erfassung, Analyse und Korrelation von sicherheitsrelevanten Protokolldaten aus unterschiedlichen OT-Systemen und Netzwerken ermöglicht. Somit wird Transparenz geschaffen und die Überwachung der OT-Infrastruktur erheblich verbessert.

Das Modul umfasst ein umfassendes **SIEM-Monitoring**, das kontinuierlich Protokolldaten sammelt und auf Anomalien oder potenzielle Bedrohungen untersucht. Die Lösung geht über die einfache Protokollerfassung hinaus: Durch die Implementierung spezifischer **Use Cases** wird das Monitoring auf die individuellen Bedürfnisse Ihrer OT-Umgebung zugeschnitten. Diese Use Cases bilden die Grundlage für automatisierte Erkennungsregeln, die speziell auf typische Bedrohungsszenarien in OT-Umgebungen ausgelegt sind − wie etwa ungewöhnliche Netzwerkaktivitäten,

auffällige Benutzeraktionen oder verdächtige Zugriffe auf kritische Steuerungssysteme.

Ein wichtiger Bestandteil des Moduls sind die **Threat-Feeds**, die regelmäßig aktualisierte Informationen über aktuelle Bedrohungen und neue Angriffsvektoren liefern. Diese Bedrohungsinformationen werden direkt in die Analyseprozesse integriert, so dass neue Risiken schnell erkannt werden. Dadurch wird es möglich, auf Veränderungen in der Bedrohungslandschaft zeitnah zu reagieren und Erkennungsregeln entsprechend anzupassen. Diese proaktive Integration externer Bedrohungsdaten trägt wesentlich zur Verbesserung der Erkennungsgenauigkeit bei und minimiert das Risiko, dass Angriffe unentdeckt bleiben.

Eine weitere optionale Komponente des Moduls ist die **Hotline**. Die Hotline dient als Anlaufstelle für technische Fragen und bietet als Service Desk den Single Point of Contact. Dieser Service ist besonders wertvoll in akuten Situationen, da eine schnelle und kompetente Unterstützung gewährleistet wird.

Die Kombination aus kontinuierlichem Monitoring, spezifischen Use Cases und der Einbindung aktueller Threat-Feeds ermöglicht es, die Sicherheit der OT-Systeme effektiv zu steigern, ohne den laufenden Betrieb zu beeinträchtigen.

Das SIEM-Erweiterungsmodul bildet somit einen integralen Bestandteil des OT-SOC und trägt dazu bei, die Transparenz und Reaktionsfähigkeit zu erhöhen. Durch die zentrale Überwachung und Analyse aller sicherheitsrelevanten Ereignisse werden Unternehmen dabei unterstützt, die Betriebssicherheit und den Schutz kritischer Infrastrukturen nachhaltig zu gewährleisten.

2. Erweiterungsmodul: PAM

Das **PAM (Privileged Access Management)** Modul bietet eine gezielte Kontrolle über privilegierte Zugänge in OT-Umgebungen. Mit der **Just-in-Time-Zuweisung** von Rechten erhalten Nutzer nur temporär die benötigten Berechtigungen, was potenziellen Missbrauch erschwert. Eine zusätzliche **Multi-Faktor-Authentifizierung** sorgt für höheren Schutz bei kritischen Zugriffen.

Das Modul umfasst die **Echtzeit-Überwachung** und Aufzeichnung privilegierter Sitzungen, wodurch verdächtige Aktivitäten schneller sichtbar werden. Ein automatisiertes **Passwort-Management** ermöglicht die sichere Speicherung und regelmäßige Aktualisierung von Zugangsdaten und beugt somit Sicherheitslücken vor.

Das PAM-Modul bietet eine detaillierte Übersicht über die Zugriffsaktivitäten und vereinfacht die Einhaltung von **Compliance-Anforderungen** wie IEC 62443.

Warum Controlware

Die Controlware GmbH ist ein führender IT-Dienstleister und Managed Service Provider mit über 40 Jahren Erfahrung. Wir entwickeln, implementieren und betreiben umfassende IT- und OT-Lösungen für Cloud-, Data Center-, Enterprise- und industrielle Umgebungen. Mit unserem ISO 27001-zertifizierten Customer Service Center gewährleisten wir höchste Servicequalität.

Die Controlware Experten verfügen über fundiertes Know-how in der Gestaltung moderner Netzwerke, einschließlich IT- und OT-Sicherheitslösungen. Wir unterstützen Kunden aus unterschiedlichsten Branchen bei der Absicherung und Optimierung ihrer IT- und OT-Infrastrukturen. Dabei legen wir besonderen Fokus auf die Integration von IT- und OT-Systemen, um Stabilität und Sicherheit zu gewährleisten.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf: