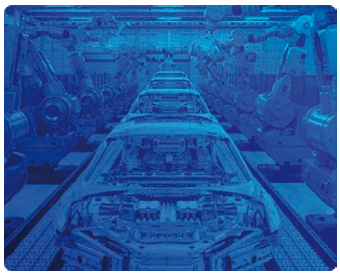
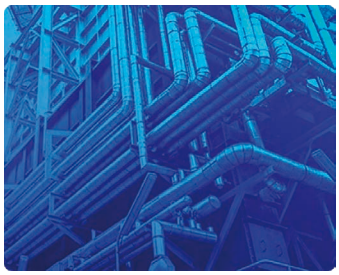
„Digitaler Zwilling“ für die OT-Sicherheit

Der Digital-Twin-Ansatz für OT-Sicherheit hilft Unternehmen, das Risiko von Störungen bei allen Anlagen und potenziellen Szenarien richtig einzuschätzen

Die Industrie kennt schon lange das Konzept des Digital Twin, eines digitalen Zwillings für Anwendungsfälle zur Optimierung der Produktion, zum „Einlernen“ von Robotern oder zur Prozesssimulation. Die Idee, einen digitalen Zwilling zum Zweck der OT-Sicherheit zu verwenden ist hingegen neu. Ziel ist es hierbei, eine OT-Umgebung digital nachzustellen und diese dann als „Testobjekt“ für Cyberangriffe zu verwenden. Simulierte Angriffe auf den digitalen Zwilling sollen Sicherheitslücken in der realen Produktionsumgebung sichtbar machen.

Cybersicherheit in OT-Umgebungen

Sicherheitsteams benötigen einen einheitlichen Überblick über alle Netzwerkkomponenten sowie ihre Abhängigkeiten und Beziehungen zu den betrieblichen und geschäftlichen Zielen. Um die Ausfallsicherheit der OT-Umgebung zu erreichen, müssen Sicherheitsexperten den Anlagenbestand, die potenziellen Schwachstellen und die Bedrohungsanfälligkeit kennen. Selbst versierte OT-Sicherheitsteams stehen bei der Sicherung der Betriebsumgebung jedoch oft vor Herausforderungen.

Problem: unklares Bild

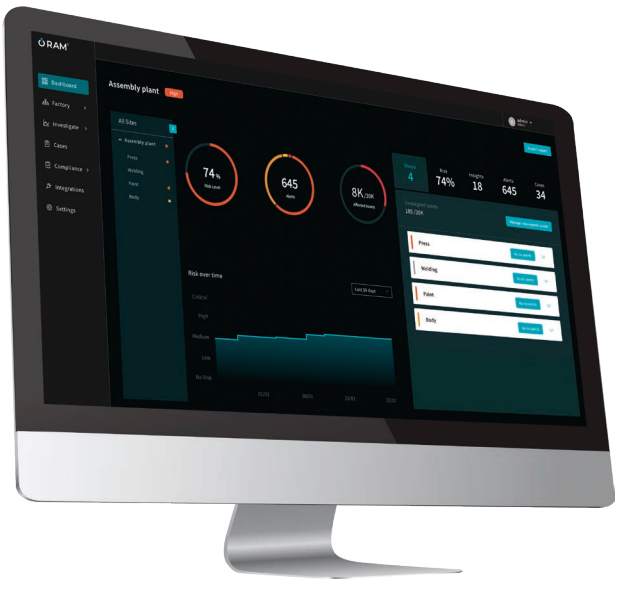
Ein gängiges Problem stellt ein unklares Bild des Anlagenbestands aufgrund von begrenzter Sichtbarkeit und unvollständigen Inventardaten dar. Die Erfassung der Bedrohungsanfälligkeit konzentriert sich oft auf die Schwachstellen von Endgeräten, ohne zu wissen, wie stark diese tatsächlich potenziellen Bedrohungen ausgesetzt sind. Eine umfassende Bewertung der OT-Sicherheitslage ist oft nicht möglich, und es kommen ineffiziente Maßnahmen zur Risikominderung zum Einsatz, die nicht auf die individuelle betriebliche Umgebung zugeschnitten sind. Ein weiteres Problem ist die Ineffizienz aufgrund mangelnder wirkungsbasierter Priorisierungsmechanismen.

Digitaler Zwilling im Einsatz

OTORIO geht mit seiner Plattform für das OT-Risikomanagement über die Sichtbarkeit von Anlagenkomponenten und die Identifizierung von Schwachstellen hinaus. Mit dem Cyber Digital Twin (CDT) als zentrale Komponente der Plattform gewinnen Sicherheitsteams die Kontrolle über die Sicherheitslage, können die relevanten Risiken beseitigen und einen sicheren, effizienten und zuverlässigen Betrieb gewährleisten. Der Digital-Twin-Ansatz für die OT-Sicherheit eignet sich sowohl für einen KMU-Maschinenpark mit fünf Maschinen als auch für eine Produktionshalle mit 1.000 Robotern. Insbesondere kleinere IT-Teams werden entlastet im Rahmen der angestrebten Automatisierung der OT-Sicherheit.

Automatisierte und logische Darstellung

Die CDT-Ansicht bietet eine automatisierte und logische Darstellung des Betriebsnetzwerks, der Einheiten, aus denen es besteht, und der Merkmale der Beziehungen zwischen den Einheiten. Er liefert einen Kontext zur Lage der Cybersicherheit sowie prägnante und priorisierte Handlungsaufforderungen. Durch die Kartografierung eines Sandbox-Modells der Betriebsumgebung sind sichere und nicht-intrusive Simulationen von Sicherheitslücken und Angriffen sowie datenbasierte Analysen potenzieller



Autor:
Kay Ernst
Manager DACH
Otorio
www.otorio.com

Auswirkungen möglich. Das CDT-Modell bietet dabei eine visuelle Darstellung der Topologie des OT-Netzwerks, um Segmentierungslücken und Angriffsvektoren zu identifizieren, die auf kritische Assets und Prozesse abzielen.

Die OT-Sicherheitsplattform empfiehlt praktische Maßnahmen zur Verbesserung der Sicherheitslage, wie etwa die Einschränkung der Kommunikation oder die Verschärfung der Sicherheitsrichtlinien für bestimmte Anlagenkomponenten. Sicherheitsteams erhalten priorisierte Anweisungen zur Risikominderung, basierend auf der tatsächlichen Exposition und den potenziellen betrieblichen Auswirkungen.

Vorteile des CDT-Ansatzes

Dank der verbesserten Sichtbarkeit und der konsolidierten Analyse von Netzwerkdaten, die der CDT-Ansatz bietet, können Sicherheitsteams blinde Flecken in ihrer Betriebsumgebung beseitigen, was zu einer besseren Sicherheitslage führt. Die Risikominderung wird effektiver, da die OT-Sicherheitsexperten Schwachstellen, die tatsächlich ausgenutzt werden können, priorisieren können. Insbesondere die Sandbox-Umgebung unterstützt das proaktive Handeln. Diese ermöglicht eine sichere Analyse und Vorhersage der Auswirkungen potenzieller Angriffe und Veränderungen in der Umgebung. Unternehmen können auch den Wert bestehender Sicherheitskontrollen erhöhen, indem sie Konfigurationsfehler und Optimierungsbedarf erkennen. Die CDT-Funktion führt eine automatisierte Bewertung von Online- und Offline-Daten durch. Dabei minimiert sie das Hintergrundrauschen unklarer Details und fügt den richtigen Kontext hinzu. So gelingt es, die Erkennung zu verbessern und die durch unklare Lageberichte verursachte Alarmmüdigkeit zu vermeiden.

Proaktiv Schützen

Durch die Analyse und Visualisierung von Schlüsselkomponenten wie Bedrohung, Wahrscheinlichkeit, Anfälligkeit und Auswirkung ist eine Risikominderung möglich, gestaffelt nach der tatsächlichen Gefährdung und den möglichen Auswirkungen auf den Betrieb. Auf diese Weise können Unternehmen proaktiv Maßnahmen zum Schutz ihrer betriebskritischen Anlagen und Prozesse ergreifen. Diagramme zu den Angriffsvektoren bieten eine dynamische, visuelle Darstellung der Netzwerktopologie, um sich auf einfache Art zwischen Anlagenkomponenten, Schwachstellen, ihren Verbindungen und dem Einfluss der Sicherheitskontrollen bewegen zu können. Dieser Ansatz liefert wichtige Gesichtspunkte zur realistischen Beurteilung der aktuellen Situation der OT-Sicherheit. Anhand präziser Handlungsaufforderungen können Unternehmen Prioritäten setzen und Risiken effektiv adressieren.

Bedrohungen immer einen Schritt voraus sein

Die Überwachungsfunktionen der OT-Sicherheitsplattform versetzen Unternehmen in die Lage, Schwachstellen proaktiv zu überprüfen und das Sicherheitsniveau zu erhöhen. Dies hilft ihnen dabei, die Wahrscheinlichkeit von Bedrohungen und Störungen richtig einzuschätzen. Klare Signale zur Sicherheitslage und die richtigen Gegenmaßnahmen ermöglichen es Anlagenbetreibern, neuen Bedrohungen immer einen Schritt voraus sein. ◄