Orange
Cyberdefense

Industrial Security

Orange Cyberdefense unterstützt Unternehmen bei Analyse, Planung, Integration und Betrieb OT-spezifischer Sicherheitssysteme für Ihre Produktionsumgebung und Anlagentechnik.

Verlässliche Cyber Security – Voraussetzung für Industrie 4.0

Die Enterprise-IT verschmilzt mit der operativen IT im Produktionsumfeld und den Anlagensteuerungen. Dies schafft zusätzliche Angriffsvektoren für Produktionssteuerungsanlagen. Durch die Verknüpfung der bislang eigenständigen Produktionsinseln gelangen Angreifer nicht nur an geschäftskritische Informationen, sondern sind immer öfter in der Lage, Produktionsprozesse zu manipulieren und ganze Anlagen zum Stillstand zu bringen.

Aktuelle Studien verdeutlichen, dass Anzahl und Professionalität der Cyberangriffe auf SCADA-Systemen (Supervisory Control and Data Acquisition) und Industrial Control Systems (ICS) dramatisch zugenommen haben – mit Konsequenzen, die viele Unternehmen nach Jahren der Orientierung jetzt zum Handeln veranlassen.

Bei der Digitalisierung der Industrie haben Unternehmen des Maschinen- und Anlagenbaus eine wichtige Doppelfunktion: Während sie als Betreiber von Anlagen ihre eigenen Produktions- und Geschäftsprozesse digitalisieren, bieten sie als Technologieintegratoren ihren Kunden komplette Anlagen und Systeme an. Für Herstellung, Integration und Betrieb braucht es neben verlässlichen europäischen Standards vor allem technische Lösungen und Services, die den Maschinenbau im Blut haben und nicht halbherzig aus der IT abgeleitet wurden.

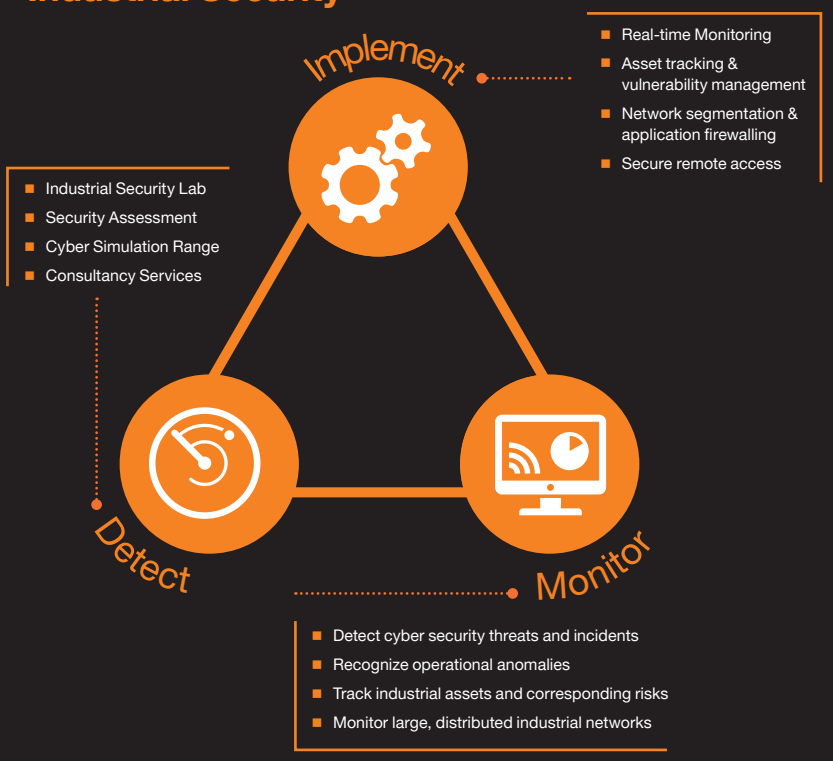
Kennen Sie den? „Treffen IT und OT aufeinander...“

... so ist oft auch interkulturelle Kompetenz gefordert, denn beide Seiten haben unterschiedliche Philosophien, Herangehensweisen und Herausforderungen zu meistern. So wundert es nicht, wenn Sicherheitsverantwortliche im Werk den Themen Zuverlässigkeit und Verfügbarkeit der Produktion einen höheren Stellenwert einräumen als z.B. Netzwerk-Segmentierung oder unkontrolliertes Vulnerability Scanning oder Patching, wenn dadurch Konfigurationen und Schnittstellen sowie alte Betriebssysteme nicht mehr funktionieren und die Abläufe in der Produktion gefährdet sind.

Expertise in Industrial Security

- 75 Security Monitoring Projekte in den letzten 10 Jahren in D/A/CH
- 24x7-CyberSOC für IT und OT
- ISO-zertifiziertes SOC-Setup aus Spitzentechnologie, optimierten Prozessen und erfahrenen Sicherheitsexperten
- Cyber Simulation Range für Praxistraining mit OT-spezifischen Komponenten
- Dedizierte Teams für Analyse, Incident Response, Forensik und Notfalleinsätze

360° Industrial Security



Erfahren Sie mehr unter:
orangecyberdefense.com/de/ot-iot

Managed Cyber Defense Services für Infrastruktur- und Anlagenbetreiber

Orange Cyberdefenses Managed Security Services steigern die Widerstandsfähigkeit gegenüber Cyberattacken gegen Produktionsanlagen und kritische Infrastrukturen und ermöglichen erhebliche Verbesserung der Sichtbarkeit gegenüber Spionage, Manipulation und Sabotage. Wenn intrusive Sicherheitskonzepte nicht umgesetzt werden können, stellt passives Monitoring eine wirkmächtige und kompensierende Maßnahme dar. Viele aus der IT abgeleitete Lösungen sind nur umständlich und mit hohem Aufwand auf die OT anwendbar. Wir setzen stattdessen auf künstliche Intelligenz (AI) und maschinelles Lernen mit umfassenden ICS-Kenntnissen. Dadurch sind wir in der Lage, selbst größte, heterogene Industrieanlagen automatisiert modellieren und überwachen zu können. Aus unseren ISO-zertifizierten CyberSOCs weltweit überwachen wir 24x7 Ihre IT und OT Infrastruktur.

Security Monitoring für Produktionsnetze

Orange Cyberdefense implementiert nicht-intrusive Lösungen zur Echtzeitüberwachung von Produktionsanlagen, ohne das dafür Betriebsunterbrechungen oder Netzwerktrennungen erforderlich werden. Die Lösungen arbeiten rein passiv auf verschiedenen Netzebenen und liefern folgende Funktionen:

- Ermittlung der ICS-Assets
- Ermittlung von Software Versionen, Schwachstellen und assoziierten Risiken
- Vollständige Ermittlung der Verkehrstopologie aller Systeme und deren Verbindungen
- Erfassung des Normalverhalten basierend auf künstlicher Intelligenz und maschinellem Lernen
- Detektion und Alarmierung bei Verhaltensanomalien, Regelverletzungen, kritischen Zuständen oder Änderungen, verdächtigen Aktivitäten, Angriffen, etc.
- Anpassbare Visualisierung nach topografischen Gruppen, logischen Ebenen, Systemtypen, Protokollen, Kritikalität, etc.
- Zentrales Monitoring verteilter Produktionsnetze, inkl. kontextueller Anreicherung und SIEM-Integration

Netzwerk-Segmentierung & Application Firewalling

Portbasierte SPI-Firewalls haben ausgedient und werden durch Next Generation Firewalls (NGFW) ersetzt, die in der Lage sind, gängige ICS Protokolle by default wie z.B. Modbus, OPC oder IPPC zu filtern. Damit lassen sich Netzsegmentierungsvorgaben, wie sie für Produktionsumgebungen in den Normen ISA-99 bzw. ISO 62443 und ISO 27002 beschrieben sind, auf verschiedenen Protokollebene realisieren und OT-Netze von der Office-IT abtrennen.

Asset Überwachung & Schwachstellenmanagement

Innerhalb von Produktionsumgebungen ist ein aktives Scannen der Komponenten, wie es in der Office-IT üblich ist, kaum möglich. Orange Cyberdefense setzt dazu auf alternative Verfahren, um die vorhandenen Systeme, Softwarestände und deren Schwachstellen zu identifizieren. Je nach eingesetzten System können die Informationen passiv aus dem Netzwerkverkehr extrahiert oder periodisch von den PLCs/RTUs abgefragt werden.

Sichere Fernwartung

Die zentrale Fernwartung und Überwachung (Remote Access) von geographisch abgelegenen Steuerungsanlagen ist eine Grundvoraussetzung in heutigen Produktionslandschaften. Doch gerade bei Remote Access kommt es darauf an, sichere Kommunikationskanäle zwischen Headquarter und Remote Standort zu etablieren, da häufig öffentliche Übertragungskanäle wie das Internet und 2G- oder 3G-Netzwerke (als Failover und redundante Anbindung) zum Einsatz kommen. Zudem ist die eindeutige Identifizierung der Benutzer durch den Einsatz starker Authentisierungsverfahren notwendig, die einen potenziellen Missbrauch von Zugangsdaten verhindern. Orange Cyberdefense liefert hierzu bewährte und sichere Lösungen für jeden Einsatzfall.

Cyber War Gaming in Produktionsanlagen

Mit der Cyber Simulation Range, einer hyper-realistischen Trainingsumgebung, die Orange Cyberdefense in Kooperation mit dem Information Security Hub (ISH) des Flughafens München betreibt, bereiten wir Ihre Sicherheitsexperten nachhaltig auf die Herausforderungen der Arbeit in einem SOC-Team vor. Die Range umfasst dazu eine Vielzahl von Komponenten typischer ICS-Netz und ermöglicht ein breites Spektrum von Angriffsszenarien zu trainieren.

Antworten

Orange Cyberdefense Lösungen und Services im Bereich Industrial Security liefern Ihnen u.a. Antworten auf folgende Fragen:

- Mit welchen Lösungen und Services kann ich die gesetzlichen Vorgaben für KRITIS einhalten?
- Welche Sicherheitslösungen sind besser in Produktionsumgebungen einsetzbar als IT-Security-Produkte?
- Welche Gefahr geht von gefundener Schadsoftware und event. Hintertüren aus?
- Wie wird mein SOC in die Lage versetzt, auch meine Produktionsanlagen zu überwachen?
- Welchen Reifegrad haben aktuelle Security Monitoring Lösungen für ICS / SCADA?

Kundenspektrum

Unsere Interessenten und Kunden im Bereich Industrial Security kommen aus folgenden Branchen:

- Betreiber von Produktionsanlagen aus Automobilbau, Chemie, Pharma, Luft- und Raumfahrt
- Anlagen- und Gerätebauer inkl. Fahrzeugbau
- Energieversorger und Stadtwerke
- Verkehr und Logistik
- Staatliche und militärische Einrichtungen

Mehr Infos finden Sie auf
https://orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00