

Anomaly Detection and Network Monitoring in OT-Systems with SINEC Security Monitor (IC-ADNMSM)

Kurzbeschreibung

Heutzutage sind Industrieumgebungen ohne Ethernet-Verbindungen nicht mehr vorstellbar. Einerseits ermöglichen sie einen flexiblen sowie besseren Datenaustausch von Geräten auf Feldebene und deren Verbindungen zu höheren Ebenen, einschließlich IT-Umgebungen. Andererseits erhöht sich durch die zunehmende Vernetzung auch das Risiko eines Cyberangriffes. Daher wird von industriellen Netzwerken ein hohes Maß an Zuverlässigkeit und Schutz der Daten gefordert, um mögliche Ausfallzeiten in Produktionsprozessen zu minimieren. Die Sicherung von OT-Systemen umfasst die Anwendung mehrerer Kontrollebenen, einschließlich korrekter Netzwerksegmentierung, Traffic-Überwachung und Asset-Inventarisierung.

Bei der Implementierung von OT-Netzwerksüberwachung und Asset-Inventarisierung ist es wichtig, auf eine korrekte Umsetzung zu achten, um mögliche Auswirkungen auf die Automatisierungssysteme zu vermeiden, aber dennoch die effektivste Methode zur Erkennung von Anomalien zu haben. Genau diese Art von Wissen erhalten Sie in Kurs „Anomaly Detection und Network Monitoring in OT-Systemen“.

Ziele

In diesem Kurs erlangen Sie grundlegendes Wissen über OT-Intrusion-Detection-Systeme und lernen deren Anbindung an echtzeitfähige Systeme in Theorie und Praxis kennen. Sie erhalten einen Einblick in industrielle Cybersicherheitskonzepte und erfahren, wie Sie Datenströme in industriellen Netzwerken überwachen können, um mögliche Anomalien zu erkennen und die allgemeine Sicherheitslage in industriellen Netzwerken abzuschätzen. Am Ende dieses Kurses sind Sie mit den Anforderungen an solche Lösungen vertraut und können Maßnahmen im Bereich der Netzwerksicherheit planen, umsetzen sowie betreuen, was einen Mehrwert für den täglichen Betrieb darstellt. Ihr theoretisch erlerntes Wissen vertiefen Sie durch zahlreiche praxisorientierte Übungen mit dem SINEC Security Monitor.

Zielgruppe

- Technischer Vertrieb
- COOs
- Anlagenplaner
- Instandhalter
- Inbetriebsetzer
- Projektierer
- Wartungs- und Servicetechniker
- CIOs, Netzwerkplaner
- Administratoren
- Servicepersonal
- Anlageningenieure
- Steuerungsingenieure
- Systemingenieure
- Anwendungsingenieure
- OT- und IT-Netzwerkingenieure

Inhalte

- OT-Cybersicherheitskonzept
- Typische sichere Netzwerkarchitekturen
- Empfehlungen und Besonderheiten in der Implementierung vom SINEC Security Monitor
- Integration von Endgeräten über Protokolle wie Syslog, WinRM und Remote WIM
- Asset-Identifizierung und Organisation in OT-System
- Erkennung und Verwaltung von Cybersicherheitsereignissen

Teilnahmevoraussetzung

Die Teilnehmer sollten über Grundkenntnisse zu Themen wie „Industrial Ethernet“ und „Cybersecurity“ verfügen. Sie sollten mit Topologien, Übertragungsverfahren, Adressierung und Transport von Daten vertraut sein und das Fachvokabular dazu verstehen. Darüber hinaus ist es hilfreich, wenn Sie mit den Funktionsprinzipien von Routern und Switches, dem OSI-Referenzmodell sowie Cybersicherheitsstandards wie IEC-62443 vertraut sind. Den Teilnehmern wird empfohlen, den Kurs [„Security in Industrial Networks mit SCALANCE“](#) und den Kurs [„Ethernet-Grundlagen in industriellen Netzwerken“](#) zu besuchen.

Hinweise

Zertifizierung (Siemens CPIN-LEVEL)

Nach dem Training besteht die Möglichkeit die Zertifizierung „Siemens Certified Professional for Industrial Networks – Detection and Monitoring“ zu erlangen. Dazu legen Sie am letzten Tag des Qualifizierungsmoduls eine freiwillige Prüfung ab. Optional kann die Prüfung zu einem späteren Zeitpunkt abgelegt werden.

Typ

Präsenztraining

Dauer

3 Tage

Sprache

en