

OT110 OT Security Professional

Kurzbeschreibung:

Produktionsleiter, OT-Security-Verantwortliche und Ingenieure erhalten eine praxisnahe Einführung in Prinzipien und Best Practices der industriellen Cybersecurity. Vermittelt wird, wie etablierte IT-Security-Ansätze im OT-Umfeld angewendet und an dessen Besonderheiten angepasst werden können. Behandelt wird die Absicherung von Produktionsanlagen sowie von Bereichen wie Energie- und Wasserversorgung oder Gebäudeautomatisierung durch Übungen, Praxisbeispiele und Live-Demos.

Zielgruppe:

Der Kurs **OT110 OT Security Professional** richtet sich an:

- Produktionsverantwortliche
- Ingenieure und Techniker aus dem Bereich Automatisierungstechnik
- OT-Verantwortliche
- IT- und Cybersecurity-Experten

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo des Trainings **OT110 OT Security Professional** gut folgen zu können, sind folgende Kenntnisse nötig:

- Grundlegende IT- und Netzwerk-Kenntnisse
- Grundkenntnisse im Bereich IT-Security

Sonstiges:

Dauer: 4 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

Produktionsanlagen sind zunehmend Cybersicherheitsrisiken ausgesetzt. Das Training **OT110 OT Security Professional** vermittelt das erforderliche Wissen, um Cybersicherheit im Kontext industrieller Produktion bewerten und verbessern zu können.

Die Teilnehmer lernen u.a.

- den grundlegenden Aufbau industrieller Produktionsanlagen und anderer OT-Systeme zu verstehen
- Bedrohungen angemessen einzuordnen und die Bedrohungslage abzuschätzen
- Schwachstellen zu identifizieren und deren (mögliche) Auswirkungen zu verstehen

Inhalte/Agenda:

- **Systeme, Komponenten und Vernetzung in der industriellen Produktion**
 - ◆ Typische Systeme und Komponenten, deren Aufbau und Funktion
 - ◆ Kommunikationsprotokolle und Netzwerkarchitektur
 - ◆ Anbindung an andere Netzwerke
 - ◆ Purdue-Referenzarchitektur
- ◆
- **Besonderheiten und Herausforderungen der Cybersicherheit in der Produktion**
 - ◆ Rollen und Verantwortlichkeiten in der OT
 - ◆ Ablauf eines Cyberangriffs in der IT und OT
 - ◆ Bekannte Vorfälle und typische Bedrohungen
 - ◆ Schwachstellen in OT-Komponenten, -Protokollen und -Architekturen
 - ◆ Auswirkungen von Cybersicherheitsvorfällen in OT-Umgebungen
 - ◆ Übertragbarkeit und Grenzen bestehender IT-Security-Ansätze
- ◆
- **Etablierte Standards und Best Practices**
 - ◆ IEC 62443 Normenreihe (und deren Zusammenspiel mit der ISO 27001/2)
 - ◆ NIST Cybersecurity Framework
 - ◆ NIST SP 800-82
 - ◆ CIS Critical Security Controls
 - ◆ BSI ICS-Security-Kompendium
- ◆
- **Netzwerkarchitektur und -sicherheit**
 - ◆ Netzwerksegmentierung und industrielle DMZ
 - ◆ Sichere Umsetzung der Kommunikation zwischen Zonen
 - ◆ Fernzugriff
 - ◆ Absicherung von WIFI-Netzen
 - ◆ Umgang mit mobilen Geräten / Datenträgern, Modems, etc.
- ◆
- **System-/ Anwendungssicherheit**
 - ◆ Hard- und Software-Inventarisierung
 - ◆ Schwachstellen- und Patchmanagement
 - ◆ System-Härtung
 - ◆ Security-Software
 - ◆ Backup und Wiederherstellung
- ◆
- **Zugangs- und Zugriffskontrolle**
 - ◆ Sichere Authentifizierung und Autorisierung
 - ◆ Physische Sicherheit
- ◆
- **Angriffserkennung und Incident Response**
 - ◆ Methoden und Technologie für Angriffserkennung
 - ◆ Security Incident Management
 - ◆ Incident Response-Phasen und -Pläne
- ◆
- **OT-Security Assessments**
 - ◆ Security Audit / Gap Analyse
 - ◆ Risk Assessment
 - ◆ Vulnerability Assessment
- ◆
- **IT-Sicherheitsmanagement in der Produktion**
 - ◆ Organisation und Verantwortlichkeiten
 - ◆ Richtlinien, Konzepte und Prozesse
 - ◆ Schulung und Sensibilisierung
 - ◆ Kontinuierliche Verbesserung