SC681 OT Security Professional

Kurzbeschreibung:

Moderne Produktionsanlagen sind durch ihren hohen Vernetzungsgrad und die Einbindung von Standard-IT-Komponenten zunehmend Cybersicherheitsrisiken ausgesetzt. Gleichzeitig lassen sich etablierte Maßnahmen der IT-Sicherheit in diesem Umfeld nicht uneingeschränkt anwenden, sodass sich in der industriellen Cybersecurity spezifische Ansätze etabliert haben.

Das Training **SC681 OT Security Professional** vermittelt die Prinzipien und Best Practices der industriellen Cybersecurity und damit das erforderliche Wissen und die Fähigkeiten, um Cybersicherheit im Kontext industrieller Produktion bewerten und verbessern zu können. Der Fokus des Kurses liegt auf industriellen Produktionsanlagen. Die vermittelten Inhalte sind aber nicht nur in Produktionsbetrieben, sondern auch in anderen Bereichen (z.B. Energie- und Wasserversorgung, Gebäudeautomatisierung) anwendbar. Das Training vermittelt die Inhalte durch theoretische Elemente, praktische Übungen und die Diskussion von Beispielen aus der Praxis.

Zielgruppe:

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

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo im Workshop **SC681 OT Security Professional** gut folgen zu können, sind folgende Kenntnisse nötig:

- Grundkenntnisse in Automatisierungstechnik und Fabrikautomation
- Grundlegende IT- und Netzwerk-Kenntnisse
- Grundkenntnisse im Bereich IT-Security

Sonstiges:

Dauer: 3,0 Tage

Preis: 2290 Euro plus Mwst.

Ziele:

Moderne Produktionsanlagen sind zunehmend Cybersicherheitsrisiken ausgesetzt. Das Training **SC681 OT Security Professional** vermittelt das erforderliche Wissen, um Cybersicherheit im Kontext industrieller Produktion bewerten und verbessern zu können.

Die Teilnehmer lernen u.a.

- Bedrohungen angemessen einzuordnen und die Bedrohungslage abzuschätzen
- Schwachstellen zu identifizieren und deren (mögliche) Auswirkungen zu verstehen

- Sicherheitsrisiken zu analysieren und zu bewerten
- Maßnahmenempfehlungen und Sicherheitskonzepte zu erarbeiten

Inhalte/Agenda:

- **Cybersicherheitsvorfälle und deren Auswirkungen**
  - Bekannte Vorfälle und typische Bedrohungen
  - Schwachstellen in OT-Komponenten, -Protokollen und -Architekturen
  - Auswirkungen von Cybersicherheitsvorfälle in OT-Umgebungen

- **Etablierte Standards und Best Practices**
  - IEC 62443
  - 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**
  - Rollen und Verantwortlichkeiten
  - Richtlinien, Konzepte und Prozesse
  - Schulung und Sensibilisierung
  - Kontinuierliche Verbesserung