SC681 Industrial Security Professional

Kurzbeschreibung:

Der Kurs Industrial Security Professional" knüpft an den Basis-Kurs SC680 "Industrial Security in der digitalen Transformation" an. **Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von methodischen 360° Ansätzen zur Planung und Umsetzung der Informationssicherheit in IT-gestützten Steuerungs- und Automatisierungsanlagen.**

Die Teilnehmer haben nach Abschluss der Ausbildung ein fundiertes Verständnis für das Zusammenwirken von IT-Sicherheit und Anlagensicherheit, für die Bewertungskriterien eines sicheren Betriebs von ICS-Umgebungen. Sie sind in der Lage, im Unternehmen ein eigenes Security-Programm unter Berücksichtigung der Schnittstellen von Technik, Organisation, Mensch entsprechend der aktuellen gegebenen regulatorischen Rahmenbedingungen, Normen und Standards zu konzipieren und umzusetzen.

Zielgruppe:

Experten aus dem Bereich Fabrikautomation und Prozesssteuerung, die ihre Qualifikationen um Cyber-Sicherheit für den eigenen Verantwortungsbereich erweitern wollen. IT- und IT– Sicherheitsexperten, die Ihren Horizont zu Produktionsthemen erweitern wollen.
Produktions-CISO, Ingenieure, Infrastruktur-Betriebspersonal, Wartungstechniker, Instandhalter- also mit einem technischen Hintergrund in ICS und mit der Planung, Entwicklung, Integration/Errichtung, Betrieb oder Instandhaltung betraut

Voraussetzungen:

- Teilnahme am Kurs Industrial Security in der Digitalen Transformation SC680 (Basis Training)

- Gutes Verständnis für Produktionsabläufe, Automation und IT Grundverständnis

Sonstiges:

Dauer: 3,0 Tage

Preis: 2750 Euro plus Mwst.

Ziele:

Der Kurs beinhaltet fachlich theoretische Elemente, praktische Übungen, gemeinsame Auswertungen und Diskussionen, Coaching-Elemente sowie praktische Aufgaben aus der Praxis der Teilnehmer.

Die Teilnehmer sind aufgefordert eigene Praxisbeispiele in das Advanced Training einzubringen. Teilnehmer erhalten ein Zertifikat zum Industrial Security Professional durch erfolgreiche Anfertigung einer Übungsaufgabe und Bestehen des finalen 2-stündigen Abschlusstestes. Durch beide Prüfungsbestandteile wird Verständnis und Umsetzungskompetenz für Industrial Security Lösungen gewährleistet.

- grundlegendes Verständnis der relevanten Begrifflichkeiten, Technologien und Elemente der IT/IT-Sicherheit auf Basis einer systemischen 360° Perspektive
- fundiertes Verständnis der Bedrohungslage zur Bewertung der eigenen Betroffenheit/Gefährdungslage im

Spannungsfeld von Technik, Mensch und Organisation
- Vermittlung der Grundsätze von ISMS, BCM
- vertiefende Kenntnisse von organisatorischen und technischen Maßnahmen
- konkrete Ansatzpunkte für die Umsetzung im operativen Betrieb/bei der Planung neuer Anlagen/bei der Leitung von Sicherheitsprojekten.

Inhalte/Agenda:

- 360° Ansatz
  - Überblick
  - Perspektiven und Konsequenzen Digitale Vernetzung
  - Handlungsbedarf

- Rahmenbedingungen und Herangehensweisen
  - Notwendigkeit für Industrial Security
  - Herangehensweise für Industrial Security
  - Regulatorische Anforderungen
  - Standards & Normen allgemein bzw. branchenspezifisch
  - Kunden-Anforderungen, Anforderungen Stakeholder, Anforderungen Wertschöpfungskette
  - Ganzheitlicher Scope, Management-Systeme (z.B. ISMS/BCMS) und deren Anwendung in der Industrie

- Organisation
  - Unternehmensorganisation (Zentral, Dezentral)
  - Rollen und Kompetenzen
  - Roadmap Security Lifecycle
  - Methodische Ableitung von Budgets
  - Kommunikations- & Berichtswege

- Prozesse
  - Vom Geschäftsprozess zu den Security Basis Prozessen
  - Basisprozesse nach 27001 (z.B. Changemanagement, Notfallmanagement, Incident Management, Backup Recovery, Konfigurationsmanagement)
  - Risikomanagement
  - Risikobewertung
  - Maßnahmen
  - Risiko-Indikatoren
  - Kontinuierlicher Verbesserungsprozess
  - Messbarkeit von Security, Reports und Kennzahlen

- Technik
  - Grundsätzliche Anforderungen der Produktion
  - OT und IT
  - Industrielle Infrastruktur
  - Netzwerke und Segmentierung, klassische Produktionsnetzwerke
  - Infrastruktur 4.0
  - Angriff- und Bedrohungsszenarien

- Lösungen und Konzepte
  - Remotezugänge
  - Patchmanagement
  - Virenschutz
  - Whitelisting
  - Sandboxing
  - Anomaliedetection
  - Monitoring
  - Honeypots
  - Best Practice bei portablen Medien

- Faktor Mensch
  - Rolle des Menschen im Kontext des ganzheitlichen Securitymanagements
  - Risiko- und Bedrohungsszenartien
  - Social Engineering

  - Reifegradmodell Security (Bradley-Kurve)
  - Führungs und Unternehmenskultur
  - Awareness Next Generation
  - Systemische und vernetzte Kommunikation
  - Wissensmanagement und Qualifikation

- Vorbereitung und Zertifizierung

- Test
- Erarbeitung und Besprechung Aufgabenstellung
- Durchführung Übungsaufgabenn
- Abschlussprüfung
- Coaching und Begleitung (im Nachgang zum Kurs)

- **Integrativer Bestandteil des praxisnahen Intensivtrainings zum "Industrial Security Professional" ist ein 4-stündiges Coaching mit unserem Trainer** - einem Experten für 360 Grad Industrial Security Lösungen mit langjähriger Erfahrung. Die Coaching Stunden zielen darauf ab, dass im Training erlernte Wissen in der Praxis umzusetzen. **Die Coachingstunden können bis maximal 6 Monate nach Kursende genutzt werden.**