SC605 Industrial Security Advanced

Kurzbeschreibung:

Sie erhalten vertieftes Wissen für die Umsetzung von Industrial-Security-Prozessen und profitieren von Best-Practices-Konzepten, das Sie in der betrieblichen Praxis einsetzen können.

Zielgruppe:

Mitarbeiter, die mit der Umsetzung, Betreuung und Verantwortung von Industrial Security im Unternehmen betraut sind.

Voraussetzungen:

Besuch des Kurses SC601 oder SC602 oder gleichwertige Vorkenntnisse im Bereich der IT/IT-Security und Produktion.

Sonstiges:

Dauer: 3 Tage

Preis: 2190 Euro plus Mwst.

Ziele:

Sie erhalten tiefergehendes Wissen für die Umsetzung von Industrial-Security-Prozessen und profitieren von Best-Practices-Konzepten, die Sie in der betrieblichen Praxis einsetzen können.

Inhalte/Agenda:

- Anwendung in der Produktion
  - ◊ Applikations-Stacks
  - ◊ User-/Rechte-Management
  - ◊ Betriebssysteme
  - ◊ Netzwerk (Ethernet)
  - ◊ Software-Lifecycle
  - ◊ Konfigurationsmanagement

- Schnittstellen
  - ◊ Innerhalb einer Ebene und zu übergelagerten Ebenen
  - ◊ Schnittstellen über Unternehmensgrenzen hinweg

- Angriffsmuster & Bedrohungen
  - ◊ Täter-Profile (Innen vs. Außen)
  - ◊ Massenangriff vs. gezielter Angriff (z.B. Stuxnet) vs. menschliches Versagen
  - ◊ Angriffs-Vektoren (Technik & Mensch)
  - ◊ Angriffswerkzeuge und -methoden
  - ◊ Aktuelles Lagebild
  - ◊ Typische Security-Bedrohungen
  - ◊ Attack Trees
  - ◊ Trends
  - ◊ Social Engineering
  - ◊ Zugriff von extern

- Sicherheitsmaßnahmen und Lösungsansätze
  - ◊ Schutzziele
  - ◊ Security by Design
  - ◊ White-/Blacklisting
  - ◊ Virenscanner
  - ◊ PKI / Signaturen
  - ◊ Verschlüsselungstechniken
  - ◊ Netz-Segmentierung
  - ◊ Firewall, VPN – Strukturen
  - ◊ Kommunikationsflow-Regelungen
  - ◊ Schutzmechanismen aus den Prozessen heraus ableiten
  - ◊ Best-Practice-Ansätze / Empfehlungen
  - ◊ Top-Down & Bottom-Up - Ansätze
  - ◊ Sicherheitsmaßnahmen und deren Auswirkung auf das Risiko
  - ◊ Angriffsfläche reduzieren, indem die Funktionsvielfalt reduziert wird
  - ◊ Logging & Log-Management
  - ◊ Honeypots
  - ◊ SIEM
  - ◊ Industrial-Security-Prozesse
  - ◊ Bei Remote-Zugriff von Herstellern

- Risiko-Management
  - ◊ Durchführung Risikobewertung
  - ◊ Risikobehandlung / passende Maßnahmen
  - ◊ Individual-Risiken als auch Verkettungen berücksichtigen
  - ◊ Induzierte Risiken durch flache interne Wertschöpfungstiefe und langer Wertschöpfungskette
  - ◊ Risiko-Indikatoren

- Audits & Zertifizierungen
  - ◊ Wie plane ich Audits?
  - ◊ Was muss dokumentiert werden?
  - ◊ Wie führt man ein Audit-Gespräch?
  - ◊ Interview-Technik

- Reporting, KPI-Kriterien & Überwachung

- Incident-Management