# *OT150 IEC 62443 Foundation*

**Kurzbeschreibung:**

Im Zusammenhang mit Cybersicherheit für Operational Technology (OT) gilt die Normenreihe IEC 62443 als wichtiger Standard. Die Normenreihe beschreibt, wie industrielle Cybersicherheit über den gesamten Lebenszyklus der OT geplant und umgesetzt werden kann und welche Anforderungen dabei durch die verschiedenen Beteiligten (Hersteller, Dienstleister, Betreiber) erfüllt werden müssen.

Das Training **OT150 IEC 62443 Foundation** vermittelt das erforderliche Wissen, um industrielle Cybersicherheit mithilfe der IEC 62443 bewerten und verbessern zu können. Sie lernen die zentralen Begriffe, Prinzipien und Konzepte (Industrial Automation and Control System, Zones & Conduits) der Normenreihe kennen und erhalten einen fundierten Überblick über die Best Practices und Anforderungen, die in den verschiedenen Teilen der Norm definiert werden.

**Zielgruppe:**

- CISOs und andere IT-Sicherheitsverantwortliche produzierender Unternehmen
- IT- und Cybersecurity-Experten
- Verantwortliche für Produktionsanlagen
- Ingenieure und Techniker aus dem Bereich Automatisierungstechnik
- OT-Verantwortliche
- Produkt- / Entwicklungsverantwortliche bei Herstellern von Automatisierungstechnik

**Voraussetzungen:**

Es sind keine spezifischen Vorkenntnisse für die Teilnahme am Kurs **OT150 IEC 62443 Foundation** erforderlich.

**Sonstiges:**

**Dauer:** 1 Tage

**Preis:** 790 Euro plus Mwst.

**Ziele:**

Lernen Sie industrielle Cybersecurity mithilfe der Normenreihe IEC 62443 zu bewerten und zu verbessern. Neben zentralen Begriffen, Prinzipien und Konzepte der Normenreihe erhalten Sie im Training **OT150 IEC 62443 Foundation** einen fundierten Überblick über die Best Practices und Anforderungen, die in den verschiedenen Teilen der Norm definiert werden.

Die Teilnehmer lernen u.a.

- die Normenreihe IEC 62443 und deren Konzepte kennen
- Best Practices und Anforderungen für die Absicherung industrieller Produktionsanlagen zu verstehen
- Grundlegende Prinzipien und Konzepte der Norm IEC 62443 anzuwenden

**Inhalte/Agenda:**

- **Grundlagen**
  - ◊ Begriffe, Prinzipien und Konzepte (Defense-in-depth, Zones & Conduits, Security-by-Design, Security Level, Maturity Level)
  - ◊ Rollen und Verantwortlichkeiten (Geräte- und Maschinenhersteller, Systemintegratoren, Betreiber)
- **Gemeinsamkeiten und Unterschiede zwischen den Normenreihen ISO 2700x und IEC 62443**
- **Anforderungen an Betreiber und Dienstleister**
  - ◊ Aufbau eines IT-Sicherheits-Management-System
  - ◊ Empfehlungen bzgl. Patch Management
  - ◊ Anforderungen an Dienstleister
- **Anforderungen an Automatisierungssysteme**
  - ◊ Methodik zur Risikobewertung
  - ◊ Anforderungen an das System-Design
  - ◊ Technische Anforderungen (Basis- und Systemanforderungen, Anforderungserweiterungen)
- **Anforderungen an Geräte- und Maschinenhersteller und die gelieferten Automatisierungskomponenten**
  - ◊ Sicherer Entwicklungsprozess
  - ◊ Technische Anforderungen an Automatisierungskomponenten
- **Entwicklungsstand der Normenreihe und Ausblick**