1715011

Industrial Cybersecurity Professional (Level 2)

Sicherer Entwicklungslebenszyklus für Industrieprodukte

Präsenztraining 2 Tage Fortgeschrittener

Präsenz Training oder Virtuelles Klassenzimmer

Industrial Cybersecurity ist für Hersteller, Integratoren und Betreiber von Industrial IoT (Internet of Things)-Systemen sowie industriellen Automatisierungs- und Steuerungssystemen (IACS) zur Grundvoraussetzung geworden, um die hohe Qualität ihrer Produkte gewährleisten zu können. Zudem bildet Industrial Cybersecurity die Basis für einen erfolgreichen Marktzugang von IoT- und IACS-Systemen, nicht zuletzt aufgrund hoher Anforderungen von Regulierern und Gesetzgebern weltweit. Moderne und innovative IoT- und IACS-Systeme werden durch Softwaresysteme gesteuert und sind hochgradig vernetzt. Auf solche setzen innovative, zunehmend auf Cloud-Services basierende Geschäftsmodelle. Um von den Vorteilen der Digitalisierung und Vernetzung zu profitieren, ist es erforderlich, den immer größer werdenden Risiken durch OT/IT-Security-Angriffe erfolgreich entgegenzuwirken.

- Um ein hohes Cybersecurity-Niveau in IoT- und IACS-Systemen zu erzielen, braucht es einen ganzheitlichen Ansatz und systematisches Vorgehen. Nur damit werden neben den technischen auch organisatorische Aspekte abgedeckt.
- Zudem muss Cybersecurity integraler Bestandteil des gesamten Produktentwicklungs-Lebenszyklus werden, um Risiken erfolgreich und effizient begegnen zu können.
- Denn die Kosten zur Beseitigung von Schwachstellen in der OT/IT-Security wachsen rapide an, je später gehandelt wird. Deshalb legt ein professionelles Risikomanagement das Hauptaugenmerk auf die präventive Erkennung und Beseitigung von Sicherheitslücken – möglichst früh im Produktentwicklungs-Lebenszyklus.
- Diese Schulung zeichnet sich durch einen hohen Praxisbezug aus.
  - Die erlernten Kenntnisse werden in Form von Praxisübungen und Fallbeispielen vertieft und gefestigt; der Transfer in Ihr Tätigkeitsumfeld wird damit erleichtert.
  - Best Practices und Umsetzungsbeispiele unserer Fachtrainer unterstützen diesen Vorgang.
  - Denn die wichtigste Risikominimierungsmaßnahme ist, dass Sie über profunde Industrial-Cybersecurity-Kenntnisse verfügen, um IoT- und IACS-Systeme sicher entwerfen, anwenden, testen und warten zu können.

- Durch dieses gezielte Industrial Cybersecurity Training bauen Sie die notwendigen Kompetenzen auf, um Ihre Industrieprodukte über den gesamten Lebenszyklus sicher definieren, gestalten, implementieren und validieren/testen sowie warten zu können.
  - Dieses Professional Training zur Entwicklung sichererer IoT- und IACS-Systeme erweitert und vertieft Ihre fundierten Kenntnisse aus der erfolgreich absolvierten Schulung „Industrial Cybersecurity Foundation nach IEC 62443“.
  - Besonderes Augenmerk wird auf die Vermittlung von Methodenkenntnissen gelegt, die Sie zur erfolgreichen Realisierung der erlernten Security-Maßnahmen in Ihrem Arbeitsumfeld benötigen.
  - Durch spannende praktische Übungen sowie Erfahrungsberichte aus der Industrial-Security-Beratungspraxis erhalten Sie Security-Kompetenzen, die für Ihre Arbeit im veränderten Umfeld der zunehmenden Digitalisierung entscheidend sind.

Ihre Vorteile

Profitieren Sie von:

- Aktuellsten Informationen zur IEC 62443 und der Normungsentwicklung aus erster Hand
- Best Practices für eine effiziente Umsetzung der Anforderungen und Regularien an Cybersecurity in IoT- und IACS Systemen
- Erstklassigen Fachdozenten des TÜV SÜD, die neben didaktischem Know How auch fundierte Erfahrungen aus der Praxisumsetzung sowie der Auditierung einbringen.

Inhalte im Überblick

Abschluss

Teilnahmevoraussetzungen

Wichtige Hinweise

Zielgruppe

Trainer