EC-Council ICS/SCADA Cybersecurity.

Risiken minimieren, Bedrohungen abwehren – Ihre Cybersecurity-Abwehrlinie für kritische Systeme.

Seminar | 4 Termine verfügbar | Zertifikat

Präsenz / Virtual Classroom | 16 Unterrichtseinheiten | Online durchführbar

Seminarnummer: 31479

Stand: 09.02.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31479

Der ICS/SCADA Cybersecurity Kurs ist ein praktisches Trainingsmodul, für die Grundlagen der Sicherheit von Netzwerk-Architekturen vor Angriffen.
ICS/SCADA vermittelt wirkungsvolle Methoden zur Analyse von Risiken, die durch die Netzwerkinfrastruktur in IT- und Unternehmensumgebungen entstehen. Sobald die Grundlagen oder Basis-Konzepte klar sind, lernen Teilnehmer einen systematischen Prozess zur Analyse von Eindringversuchen und Schadsoftware. Danach erfährst du mehr über digitale Forensik und Techniken zur Reaktion auf Sicherheitsvorfälle, sobald eine Sicherheitsverletzung entdeckt wird.

Industrielle Automatisierungsprozesse verwenden industrielle Steuerungssysteme (ICS) und Supervisory Control und Data Acquisition (SCADA)-Systeme, um industrielle Prozesse lokal oder aus der Ferne zu steuern sowie Echtzeitdaten zu überwachen, zu erfassen und zu verarbeiten.

Nutzen

Sie werden in kurzer Zeit fundiertes Wissen und praktische Fähigkeiten erwerben, um industrielle Steuerungssysteme (ICS) und SCADA-Netzwerke effektiv vor Cyberangriffen zu schützen.

Konkret profitieren Sie von:

- Verständnis der Sicherheit von ICS/SCADA-Systemen

Zielgruppe

- OT-Sicherheitsverantwortliche in Industrieunternehmen
- IT-/OT-Administratoren in kritischen Infrastrukturen (KRITIS)
- Ingenieure & Techniker, die ICS/SCADA-Systeme betreiben oder integrieren

- CISOs & IT-Security-Manager, die für industrielle Netzwerke verantwortlich sind
- Regulierte Unternehmen, die NIS2/NISG, ISO/IEC 62443 oder ähnliche Vorgaben erfüllen müssen

Voraussetzungen

Für eine optimale Teilnahme werden folgende Vorkenntnisse empfohlen:

- Grundkenntnisse in Linux und der Befehlszeile.
- Verständnis für Programmierung und Skripterstellung.
- Fundiertes Wissen über Netzwerkgrundlagen, einschließlich OSI-Modell und TCP/IP.
- Kenntnisse in Sicherheitsprinzipien wie Malware, IDS, Firewalls und Schwachstellen.
- Erfahrung mit Netzwerküberwachungstools wie Wireshark TShark oder TCPdump.

Inhalte des Seminars

Einführung in die Verteidigung von ICS/SCADA-Netzwerken

- IT Security Model
- ICS/SCADA Security Model
- LAB: Security Model
- Security Posture
- Risk Management in ICS/SCADA
- Risk Assessment
- Defining Types of Risk
- Security Policy
- LAB: Allowing a Service

TCP/IP 101

- Introduction and Overview
- Introducing TCP/IP Networks
- Internet RFCs and STDs
- TCP/IP Protocol Architecture
- Protocol Layering Concepts
- TCP/IP Layering
- Components of TCP/IP Networks
- ICS/SCADA Protocols

Einführung in Hacking

- Review of the Hacking Process

- Hacking Methodology
- Intelligence Gathering
- Footprinting
- Scanning
- Enumeration
- Identify Vulnerabilities
- Exploitation
- Covering Tracks
- LAB: Hacking ICS/SCADA Networks Protocols
- How ICS/SCADA Are Targeted
- Study of ICS/SCADA Attacks
- ICS/SCADA as a High–Value Target
- Attack Methodologies In ICS

Schwachstellenmanagement

- Challenges of Vulnerability Assessment
- System Vulnerabilities
- Desktop Vulnerabilities
- ICS/SCADA Vulnerabilities
- Interpreting Advisory Notices
- CVE
- ICS/SCADA Vulnerability Sites
- Life Cycle of a Vulnerability and Exploit
- Challenges of Zero-Day Vulnerability
- Exploitation of a Vulnerability
- Vulnerability Scanners
- ICS/SCADA Vulnerability Uniqueness
- Challenges of Vulnerability Management Within ICS/SCADA
- LAB: Vulnerability Assessment
- Prioritizing Vulnerabilities
- CVSS
- OVAL

Standards und Vorschriften für Cybersicherheit

- ISO 27001
- ICS/SCADA
- NERC CIP
- CFATS
- ISA99

- IEC 62443
- NIST SP 800-82

Sicherung des ICS-Netzwerks

- Physical Security
- Establishing Policy – ISO Roadmap
- Securing the Protocols Unique to the ICS
- Performing a Vulnerability Assessment
- Selecting and Applying Controls to Mitigate Risk
- Monitoring
- Mitigating the Risk of Legacy Machines

Überbrückung der Luftlücke

- Do You Really Want to Do This?
- Advantages and Disadvantages
- Guard
- Data Diode
- Next Generation Firewalls

Einführung in Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS)

- What IDS Can and Cannot Do
- Types IDS
- Network
- Host
- Network Node
- Advantages of IDS
- Limitations of IDS
- Stealthing the IDS
- Detecting Intrusions

Wichtige Hinweise

- Die TÜV Rheinland Akademie ist ein akkreditiertes EC-Council Schulungszentrum (Accredited Training Center)
- Es wird die aktuelle Kursversion geschult.
- Der Kurs findet in deutscher Sprache statt. Der Kurstrainer spricht sowohl Deutsch als auch Englisch.
- Die Kursunterlagen, Dokumentationen und die Abschlussprüfung sind nur auf Englisch verfügbar.
- Die im Seminar bereitgestellte eCoursware steht Ihnen nach der Aktivierung zu Seminarbeginn für 12 Monate zur Verfügung, sodass Sie auch nach dem Training die Übungen zur Vertiefung des Gelernten nutzen können.

- Wir empfehlen eine individuelle Prüfungsvorbereitung nach dem Lehrgang.
- Der Prüfungsvoucher hat eine Gültigkeit von 12 Monaten.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31479 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.