ICS-SCADA
Cybersecurity

Aufgrund der potenziellen Auswirkungen eines Angriffs auf die physische Sicherheit von Gemeinden, Mitarbeitern oder Kunden hat die Sicherheit von ICS/SCADA-Systemen eine noch höhere Priorität als bei traditionellen IT-Systemen. Cyberkriminelle haben bereits Malware-Bedrohungen wie Triton/TRISIS und Stuxnet entwickelt, die industrielle Betriebstechnologie (OT) stören können.

Der ICS/SCADA Cyber Security Training Kurs ist ein praxisorientiertes Training, das Ihnen die Grundlagen der Sicherheit und der Verteidigung von Architekturen gegen Angriffe vermittelt. Sie werden das Konzept des „Denkens wie ein Hacker " kennenlernen, um Techniken zu erlernen, die gegen die Arten von Angriffen verteidigen, die häufig gegen die IT-Unternehmens- und Steuerungsnetzwerke in der Öl- und Gasindustrie durchgeführt werden.

Sie werden leistungsstarke Methoden zur Analyse der Risiken sowohl des IT- als auch des Firmennetzwerks erlernen. Nachdem Sie das Fundament gelegt haben, werden Sie sich mit Best Practices und Empfehlungen zur Überbrückung des Air-Gaps beschäftigen. Sie werden einen systematischen Prozess der Eindring- und Malware-Analyse erlernen. Sobald Sie den Analyseprozess beherrschen, werden Sie in den digitalen Forensik-Prozess eingeführt und lernen, wie Sie auf Vorfälle reagieren, wenn ein Sicherheitsverstoß festgestellt wird.

Kursinhalt
- Introduction to ICS/SCADA Network Defense
- TCP/IP 101
- Introduction to Hacking
- Vulnerability Management
- Standards and Regulations for Cybersecurity
- Securing the ICS Network
- Bridging the Air Gap
- Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Zielgruppe
Dieser Kurs ist speziell für IT-Fachleute konzipiert, die in die Verwaltung oder Leitung der IT-Infrastruktur ihrer Organisation involviert sind und für die Erstellung und Aufrechterhaltung von Informationssicherheitsrichtlinien, -praktiken und -verfahren verantwortlich sind.

Voraussetzungen
- Grundlagen des Betriebssystems Linux, einschließlich der grundlegenden Verwendung der Befehlszeile.
- Konzeptionelle Kenntnisse der Programmierung/Skripterstellung.
- Solides Verständnis grundlegender Netzwerkkonzepte (OSI-Modell, TCP/IP, Netzwerkgeräte und Übertragungsmedien).
- Verständnis grundlegender Sicherheitskonzepte (z. B. Malware, Intrusion Detection Systems, Firewalls und Schwachstellen).
- Vertrautheit mit Tools zur Überprüfung des Netzwerkverkehrs (Wireshark, TShark oder TCPdump) wird dringend empfohlen.

Dieser Kurs im Web
Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/**ECIC**

Vormerkung
Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine
Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert
Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Termine in Österreich	**3 Tage**	**€ 2.995,-**
Online Training	**3 Tage**	**€ 2.995,-**
Termine auf Anfrage		

ICS-SCADA

Stand 07.05.2025

EC-Council

ExperTeach

Inhaltsverzeichnis

ICS-SCADA – Cybersecurity

Introduction to ICS/SCADA Network Defense
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
Introduction to 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
Vulnerability Management
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 and Regulations for Cybersecurity
ISO 27001
ICS/SCADA
NERC CIP
CFATS
ISA99
IEC 62443
NIST SP 800-82
Securing the ICS Network
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
Bridging the Air Gap
Do You Really Want to Do This?
Advantages and Disadvantages
Guard
Data Diode
Next Generation Firewalls
Introduction to Intrusion Detection Systems (IDS) and 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
LAB: Intrusion Detection
Log Analysis
ICS Malware Analysis
LAB: ICS Malware Analysis
Essential Malware Mitigation Techniques
ICS/SCADA Network Monitoring
ICS/SCADA IDS

ExperTeach Training & Consulting GmbH
Handelskai 94-96 · 1200 Wien · Telefon: +43 1 2350 383-0 · Fax: +43 1 2350 383-19 · info@experteach.at · www.experteach.at