



# 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](http://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.

ICS-SCADA

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

Stand 24.01.2025

EC-Council



EXPERTeach



# Inhaltsverzeichnis

## ICS-SCADA – Cybersecurity

<b>Introduction to ICS/SCADA Network Defense</b>	ICS/SCADA Vulnerability Uniqueness	ICS/SCADA IDS
IT Security Model	Challenges of Vulnerability Management Within	
ICS/SCADA Security Model	ICS/SCADA	
LAB: Security Model	LAB: Vulnerability Assessment	
Security Posture	Prioritizing Vulnerabilities	
Risk Management in ICS/SCADA	CVSS	
Risk Assessment	OVAL	
Defining Types of Risk	<b>Standards and Regulations for Cybersecurity</b>	
Security Policy	ISO 27001	
LAB: Allowing a Service	ICS/SCADA	
<b>TCP/IP 101</b>	NERC CIP	
Introduction and Overview	CFATS	
Introducing TCP/IP Networks	ISA99	
Internet RFCs and STDs	IEC 62443	
TCP/IP Protocol Architecture	NIST SP 800-82	
Protocol Layering Concepts	<b>Securing the ICS Network</b>	
TCP/IP Layering	Physical Security	
Components of TCP/IP Networks	Establishing Policy – ISO Roadmap	
ICS/SCADA Protocols	Securing the Protocols Unique to the ICS	
<b>Introduction to Hacking</b>	Performing a Vulnerability Assessment	
Review of the Hacking Process	Selecting and Applying Controls to Mitigate Risk	
Hacking Methodology	Monitoring	
Intelligence Gathering	Mitigating the Risk of Legacy Machines	
Footprinting	<b>Bridging the Air Gap</b>	
Scanning	Do You Really Want to Do This?	
Enumeration	Advantages and Disadvantages	
Identify Vulnerabilities	Guard	
Exploitation	Data Diode	
Covering Tracks	Next Generation Firewalls	
LAB: Hacking ICS/SCADA Networks Protocols	<b>Introduction to Intrusion Detection Systems (IDS)</b>	
How ICS/SCADA Are Targeted	<b>and Intrusion Prevention Systems (IPS)</b>	
Study of ICS/SCADA Attacks	What IDS Can and Cannot Do	
ICS/SCADA as a High-Value Target	Types IDS	
Attack Methodologies In ICS	Network	
<b>Vulnerability Management</b>	Host	
Challenges of Vulnerability Assessment	Network Node	
System Vulnerabilities	Advantages of IDS	
Desktop Vulnerabilities	Limitations of IDS	
ICS/SCADA Vulnerabilities	Stealth the IDS	
Interpreting Advisory Notices	Detecting Intrusions	
CVE	LAB: Intrusion Detection	
ICS/SCADA Vulnerability Sites	Log Analysis	
Life Cycle of a Vulnerability and Exploit	ICS Malware Analysis	
Challenges of Zero-Day Vulnerability	LAB: ICS Malware Analysis	
Exploitation of a Vulnerability	Essential Malware Mitigation Techniques	
Vulnerability Scanners	ICS/SCADA Network Monitoring	

