CyberHunt

CRITICAL INFRASTRUCTURE SECURITY

ICS/OT Cyber Security Engineer Program

Master the security of Industrial Control Systems, SCADA environments, and Operational Technology networks. Learn to protect critical infrastructure from advanced threats in power, oil & gas, utilities, and manufacturing sectors.

- ICS/SCADA Architecture
- OT Threat Landscape
- Risk Assessment & Remediation
- IEC 62443 Compliance

5000+	95%	100+	24/7
Students Trained	Success Rate	Hiring Partners	Support

CyberHunt

Program Highlights

- 40-Hour Instructor-Led Training
- EC-Council Authorized Partner
- Practical Training on Latest Tools
- Telegram Group for Exam Support
- Learn from CEI Certified Trainers
- 98% Exam Pass Rate
- Post Training Support till Exam
- Access to Recorded Sessions
- Career Guidance & Mentorship

https://cyberhuntit.com/

CyberHunt

ABOUT COURSE

ICS/OT Cyber Security Engineer Program

The ICS/OT Cyber Security Engineer Program is designed for professionals who want to secure Industrial Control Systems, SCADA environments, and Operational Technology (OT) networks in critical infrastructure sectors.

This program focuses on OT-specific security architectures, industrial protocols, vulnerability assessment, and compliance with global standards like IEC 62443 and NIST Cybersecurity Framework.

You will learn how to identify OT vulnerabilities, design secure network segmentation using the Purdue Model, perform risk assessments, monitor threats, and respond to industrial cyber incidents while maintaining operational continuity.

This course bridges traditional IT security knowledge with real-world OT operational requirements and safety considerations.

ICS/OT Security Skill Coverage

ICS Architecture & Protocols	25%
Risk Assessment & Threat Modeling	20%
Network Segmentation & Design	20%
OT Monitoring & Detection	18%
Compliance & Standards	17%

CyberHunt

Target Audience

- Security Analysts
- Ethical Hackers
- System Administrators
- Network Administrators
- Network and Security Engineers
- Cyber Security Managers
- Information Security Auditors
- Security Professionals

Pre-Requisites

- Basic understanding of network essentials and core concepts, including server and network components.

CyberHunt

Course Curriculum

Comprehensive ICS/OT security training covering architecture, threats, protocols, and industrial compliance standards

01 Introduction to ICS & OT Security

- Difference Between IT & OT
- ICS Security Fundamentals
- Critical Infrastructure Overview
- ICS Cyber Threat Landscape
- Real-World Industrial Attacks Case Studies
- Safety vs Security in OT

Practical: Understanding industrial environment architecture diagrams.

02 ICS/SCADA Architecture & Components

- SCADA Systems Overview
- Distributed Control Systems (DCS)
- Programmable Logic Controllers (PLC)
- Human Machine Interface (HMi)
- Remote Terminal Units (RTU)
- Engineering Workstations
- Purdue Model (Level 0–5 Architecture)

Practical: Mapping ICS architecture using Purdue Model.

03 Industrial Communication Protocols

- Modbus (TCP/RTU)
- DNP3
- OPC
- IEC 60870-5-104
- Industrial Ethernet
- Protocol Vulnerabilities
- Lack of Authentication & Encryption in OT Protocols

Practical: Analyzing industrial protocol traffic in packet capture.

04 OT Risk Assessment & Threat Modeling

- Asset Identification in OT
- Risk Assessment Methodology
- Threat Modeling for ICS
- Vulnerability Identification in OT
- Attack Surface in Industrial Networks
- Safety Impact Analysis

Practical: Perform risk assessment for sample industrial environment.

05 Network Segmentation & Secure Architecture

- Purdue Model Segmentation
- DMZ in Industrial Networks
- IT-OT Network Separation
- Firewall Placement Strategy
- Secure Remote Access
- Zero Trust Concepts in OT

Practical: Design secure ICS network segmentation architecture.

06 OT Monitoring & Threat Detection

- Logging in ICS Environments
- Detecting Anomalous Traffic
- Detecting Unauthorized PLC Changes
- Monitoring Remote Access Activity
- Detecting Lateral Movement in OT
- Use Case Development for OT Monitoring

Practical: Detect suspicious command injection in PLC simulation.

07 Incident Response in ICS/OT

- Challenges of Incident Response in OT
- Safety Considerations
- Containment Strategies
- Isolation Without Production Impact
- Forensic Considerations in ICS
- Business Continuity & Recovery

Practical: Simulated OT ransomware incident handling.

08 Vulnerability Management in OT

- Patch Management Challenges
- Firmware Vulnerabilities
- Secure Configuration of PLC/HMI
- Vendor Coordination
- Compensating Controls

Practical: Develop vulnerability mitigation strategy for legacy OT device.

09 Compliance & Industrial Security Standards

- Overview of IEC 62443
- Overview of National Institute of Standards and Technology guidance
- Mapping Controls to OT Environment
- Industrial Security Governance
- Policy & Procedure Development

Practical: Create ICS security policy framework.

10 Red Team vs Blue Team in OT (Awareness Level)

- Common ICS Attack Vectors
- PLC Manipulation Attacks
- Insider Threat in OT
- Defense Strategy for Industrial Systems

Practical: OT attack simulation case study discussion.

11 Forensic Reporting & Court Presentation

- Writing Forensic Reports
- Evidence Documentation
- Presenting Technical Findings to Non-Technical Audience
- Legal Admissibility Standards
- Expert Witness Basics

Practical: Prepare complete forensic investigation report.

CyberHunt

TRAINING ENQUIRIES

Have questions or need more information about our training programs? We're here to help!

For Training
+91 99599 06195
+91 93156 97737

Email
trainings@cyberhuntit.com

Website
www.cyberhuntit.com

Empowering Your Future
Industry-relevant training designed to upskill and empower you.

Follow us on