Cybersecurity for Critical Infrastructure (ICS/SCADA) Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Critical infrastructure systems—including power grids, water treatment facilities, oil and gas pipelines, and transportation networks—are increasingly targeted by sophisticated cyber threats. With industrial control systems and SCADA environments becoming more interconnected, the vulnerabilities within operational technology (OT) environments pose significant national, economic, and operational risks. Cybersecurity for Critical Infrastructure (ICS/SCADA) Training Course equips participants with advanced knowledge and high-impact practical skills required to protect, detect, and respond to cyber incidents affecting industrial control systems. Through a combination of strategic frameworks and hands-on exercises, participants gain actionable skills aligned with global cybersecurity best practices, NIST frameworks, and ICS-specific standards.

As cyberattacks escalate in scale and severity, organizations require specialists who understand the unique configurations, legacy systems, and safety-critical constraints of OT environments. This course delivers in-depth, scenario-based guidance on threat hunting, malware analysis, network segmentation, secure architecture design, and incident response for ICS networks. With strong emphasis on emerging attack vectors, convergence of IT/OT, and resilience strategies, participants learn how to strengthen defenses, ensure business continuity, and safeguard essential national assets.

Programme Curriculum

Cybersecurity for Critical Infrastructure (ICS/SCADA) Training Course

Introduction

Critical infrastructure systems—including power grids, water treatment facilities, oil and gas pipelines, and transportation networks—are increasingly targeted by sophisticated cyber threats. With industrial control systems and SCADA environments becoming more interconnected, the vulnerabilities within operational

technology (OT) environments pose significant national, economic, and operational risks. Cybersecurity for Critical Infrastructure (ICS/SCADA) Training Course equips participants with advanced knowledge and high-impact practical skills required to protect, detect, and respond to cyber incidents affecting industrial control systems. Through a combination of strategic frameworks and hands-on exercises, participants gain actionable skills aligned with global cybersecurity best practices, NIST frameworks, and ICS-specific standards.

As cyberattacks escalate in scale and severity, organizations require specialists who understand the unique configurations, legacy systems, and safety-critical constraints of OT environments. This course delivers in-depth, scenario-based guidance on threat hunting, malware analysis, network segmentation, secure architecture design, and incident response for ICS networks. With strong emphasis on emerging attack vectors, convergence of IT/OT, and resilience strategies, participants learn how to strengthen defenses, ensure business continuity, and safeguard essential national assets.

Course Objectives

1. Understand key concepts, architectures, and components of ICS and SCADA systems.
2. Identify cyber threats, vulnerabilities, and attack vectors targeting critical infrastructure.
3. Apply trending global cybersecurity frameworks and best practices for OT protection.
4. Analyze ICS-specific malware, ransomware, and APT campaigns impacting infrastructure.
5. Implement secure network segmentation and ICS firewall configurations.
6. Establish robust identity, authentication, and access controls for OT networks.
7. Conduct real-time threat detection, monitoring, and anomaly identification in ICS environments.
8. Develop incident response plans tailored to SCADA and OT security requirements.
9. Strengthen resilience through system hardening, patching, and configuration baselines.
10. Conduct risk assessments, vulnerability scans, and security audits for critical infrastructure.
11. Coordinate IT/OT cybersecurity integration and cross-departmental defense strategies.
12. Apply governance, regulatory, and compliance requirements affecting critical infrastructure.
13. Conduct post-incident analysis and implement long-term resilience improvements.

Organizational Benefits

- Improved cyber resilience for mission-critical infrastructure
- Reduced operational downtime through proactive threat mitigation
- Enhanced readiness against ICS-targeted malware and APT threats
- Strengthened compliance with national and international cybersecurity regulations
- More secure and segmented operational technology environments
- Improved monitoring, detection, and anomaly response capabilities
- Stronger collaboration between IT and OT security teams
- Increased operational safety and reliability of industrial systems
- Reduced financial impact from cyber incidents and service disruption
- Enhanced organizational reputation and stakeholder confidence

Target Audiences

- Critical infrastructure cybersecurity teams
- ICS/SCADA engineers and operations staff
- Industrial automation and control system specialists
- National security and utility sector professionals
- Cyber defense, SOC and CERT/CSIRT analysts
- IT/OT integration managers and system architects

- Risk management and compliance officers
- Infrastructure regulators, auditors, and policy makers

Course Duration: 10 days

Course Modules

Module 1: Overview of ICS/SCADA Cybersecurity

- Define ICS/SCADA components, architecture, and roles
- Examine unique OT security challenges
- Differentiate IT vs. OT cybersecurity priorities
- Identify major ICS threat actors and motivations
- Analyze real-world impacts of infrastructure cyber failures
- Case Study: BlackEnergy attack on Ukrainian power grid

Module 2: Threat Landscape for Critical Infrastructure

- Review advanced persistent threats targeting ICS
- Analyze ransomware trends in industrial environments
- Examine supply-chain risks affecting OT
- Study insider threats and operational misuse
- Assess geopolitical drivers of infrastructure attacks
- Case Study: Triton/Trisis attack on safety instrumented systems

Module 3: ICS Network Architecture & Secure Design

- Understand network topologies in industrial environments
- Apply secure segmentation using Purdue Model
- Implement zoning and conduit principles
- Configure perimeter firewalls for OT systems
- Document secure communication paths and protocols
- Case Study: Redesigning SCADA segmentation for a national utility

Module 4: ICS Protocols & Communication Security

- Identify key OT protocols (Modbus, DNP3, OPC-UA)
- Detect vulnerabilities within legacy communication protocols
- Secure data transmission and endpoint authentication
- Apply encryption and integrity controls where feasible
- Implement traffic logging and monitoring techniques
- Case Study: Exploitation of Modbus in a water treatment plant

Module 5: ICS/SCADA Vulnerability Assessment

- Conduct asset discovery and system mapping
- Identify vulnerabilities in control system components
- Apply scanning tools safely in fragile OT environments
- Prioritize remediation based on operational impact
- Coordinate assessments with engineering teams
- Case Study: Vulnerability discovery in a refinery SCADA network

Module 6: Malware Targeting ICS Systems

- Analyze ICS-specific malware behavior
- Understand industrial ransomware evolution
- Examine malicious firmware and PLC exploitation
- Apply malware detection tools and sandboxes
- Develop containment strategies for OT malware outbreaks
- Case Study: Analysis of Stuxnet attack chain

Module 7: Monitoring & Threat Detection in ICS

- Use SIEM, IDS, and anomaly detection tools for OT
- Configure log collection from field devices and HMIs
- Detect command injection and unauthorized configuration changes
- Apply behavior-based anomaly detection
- Develop threat monitoring dashboards
- Case Study: Intrusion detected via abnormal PLC command traffic

Module 8: ICS Incident Response & Recovery

- Establish OT-specific incident response workflows
- Develop containment steps that protect operational safety
- Coordinate escalation with engineering stakeholders
- Restore ICS operations after cyber disruption
- Document forensic evidence for analysis
- Case Study: Emergency response to a pipeline SCADA compromise

Module 9: IT/OT Convergence Security

- Integrate cybersecurity policies across both environments
- Mitigate risks from shared networks and remote access
- Secure interfaces between enterprise IT and operations
- Apply unified identity and access frameworks
- Strengthen monitoring across converged systems
- Case Study: Incident caused by insecure IT/OT bridge

Module 10: Access Control, Authentication & Identity Management

- Implement role-based access models for OT
- Apply multi-factor authentication in control systems
- Secure remote access to industrial environments
- Review credential management best practices
- Monitor privileged accounts and activity
- Case Study: Unauthorized access due to weak password controls

Module 11: System Hardening & Patch Management

- Harden PLCs, RTUs, HMIs and network equipment
- Apply secure configuration baselines
- Develop OT patching policies aligned with safety requirements
- Test patches in controlled offline environments
- Document system-level configuration changes

- Case Study: Outdated firmware exploited in a power substation

Module 12: Governance, Policies & Compliance

- Review regulatory frameworks for critical infrastructure
- Develop OT cybersecurity policies and operational guidelines
- Implement compliance monitoring and reporting
- Align governance structures with risk-based priorities
- Engage leadership in cybersecurity oversight
- Case Study: Compliance gaps identified during a regulatory audit

Module 13: Business Continuity & Disaster Recovery for ICS

- Develop ICS-aligned continuity plans
- Conduct risk impact analysis for critical systems
- Plan redundancies and failover strategies
- Integrate physical and cyber components of resilience
- Test continuity plans through simulation exercises
- Case Study: Restoration of a water utility after cyber disruption

Module 14: Physical Security & Insider Threat Mitigation

- Integrate cybersecurity with physical protection layers
- Control access to industrial zones and equipment
- Monitor insider behavior and privilege misuse
- Deploy threat-detection technologies in facilities
- Train staff to identify suspicious activities
- Case Study: Insider compromise of a SCADA workstation

Module 15: Future Trends in Critical Infrastructure Cybersecurity

- Analyze emerging ICS technologies and risks
- Study AI-driven attacks and autonomous malware
- Evaluate next-generation intrusion detection tools
- Explore zero-trust models for OT networks
- Prepare institutions for evolving global threats
- Case Study: Predictive risk modelling in large-scale power networks

Training Methodology

- Instructor-led presentations and technical walkthroughs
- Hands-on simulations using realistic ICS/SCADA scenarios
- Group activities focusing on threat detection and response
- Case study reviews of major ICS cyber incidents
- Practical exercises using tools for analysis and monitoring
- Action plans for implementing ICS cybersecurity improvements

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
02 Nov 2026	13 Nov 2026	Online	$2,000
02 Nov 2026	13 Nov 2026	Physical	$3,000
02 Nov 2026	13 Nov 2026	Physical	$6,000
02 Nov 2026	13 Nov 2026	Physical	$6,000
02 Nov 2026	13 Nov 2026	Physical	$12,000
02 Nov 2026	13 Nov 2026	Physical	$9,000
02 Nov 2026	13 Nov 2026	Physical	$12,000
02 Nov 2026	13 Nov 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now