Industrial Control Systems (ICS) Security Assessment 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

Industrial Control Systems (ICS) are the backbone of critical infrastructure across energy, manufacturing, utilities, transport, and industrial operations. As cyber threats targeting operational technology environments increase in frequency and sophistication, organizations must strengthen their ability to conduct comprehensive security assessments that identify vulnerabilities, reduce potential attack surfaces, and ensure uninterrupted operations. Industrial Control Systems (ICS) Security Assessment Training Course provides a detailed understanding of ICS security assessment methodologies, cybersecurity frameworks, risk analysis techniques, incident response integration, and threat intelligence specific to industrial environments. Through rich practical insights and analytical tools, participants gain the knowledge required to secure SCADA systems, PLCs, RTUs, HMIs, and other essential OT assets.

The course introduces participants to modern ICS threat landscapes, including ransomware, supply-chain attacks, nation-state actors, and AI-driven attack vectors, while exploring techniques such as network segmentation, secure architecture design, vulnerability scanning, protocol analysis, and ICS penetration assessment. It strengthens organizational capacity to implement robust security governance, align with international standards, and mitigate cyber disruptions that could affect industrial operations. The learning experience blends technical guidance with real-world case studies that enhance strategic decision-making and operational resilience.

Programme Curriculum

Industrial Control Systems (ICS) Security Assessment Training Course

Introduction

Industrial Control Systems (ICS) are the backbone of critical infrastructure across energy, manufacturing, utilities, transport, and industrial operations. As cyber threats targeting operational technology environments

increase in frequency and sophistication, organizations must strengthen their ability to conduct comprehensive security assessments that identify vulnerabilities, reduce potential attack surfaces, and ensure uninterrupted operations. Industrial Control Systems (ICS) Security Assessment Training Course provides a detailed understanding of ICS security assessment methodologies, cybersecurity frameworks, risk analysis techniques, incident response integration, and threat intelligence specific to industrial environments. Through rich practical insights and analytical tools, participants gain the knowledge required to secure SCADA systems, PLCs, RTUs, HMIs, and other essential OT assets.

The course introduces participants to modern ICS threat landscapes, including ransomware, supply-chain attacks, nation-state actors, and AI-driven attack vectors, while exploring techniques such as network segmentation, secure architecture design, vulnerability scanning, protocol analysis, and ICS penetration assessment. It strengthens organizational capacity to implement robust security governance, align with international standards, and mitigate cyber disruptions that could affect industrial operations. The learning experience blends technical guidance with real-world case studies that enhance strategic decision-making and operational resilience.

Course Objectives

1. Understand the structure, functions, and components of Industrial Control Systems.
2. Analyze modern cyber threats targeting ICS and operational technology environments.
3. Apply global ICS cybersecurity frameworks such as NIST, IEC 62443, and ISO standards.
4. Conduct comprehensive ICS security assessments using structured methodologies.
5. Evaluate ICS vulnerabilities through network mapping and asset discovery.
6. Identify weaknesses in ICS protocols, control networks, and remote access interfaces.
7. Integrate threat intelligence into ICS security decision-making.
8. Apply secure architecture and segmentation strategies for OT environments.
9. Assess the security posture of SCADA, PLC, and HMI systems.
10. Evaluate supplier, vendor, and third-party risks in industrial environments.
11. Design ICS incident response strategies aligned with operational needs.
12. Strengthen ICS security governance, policies, and compliance processes.
13. Recommend mitigation actions and develop improvement plans after security assessments.

Organizational Benefits

- Improved resilience of critical industrial operations
- Strengthened cybersecurity posture across OT and ICS networks
- Enhanced risk visibility through structured assessments
- Reduced exposure to ICS-specific cyberattacks
- Better alignment with global OT security standards
- Increased reliability and uptime of industrial systems
- Stronger vendor and supply-chain risk controls
- Improved capability to detect and respond to ICS threats
- Enhanced operational governance and regulatory compliance
- Reduced long-term recovery costs after cybersecurity incidents

Target Audiences

- ICS cybersecurity engineers and security analysts
- SCADA and OT system administrators
- Industrial automation and control engineers

- Critical infrastructure security managers
- IT/OT convergence professionals
- Cyber risk managers and compliance officers
- Incident response and threat intelligence teams
- Engineering, utilities, energy and manufacturing operators

Course Duration: 10 days

Course Modules

Module 1: Introduction to Industrial Control Systems

- Understand key ICS components including PLCs, RTUs, DCS and SCADA
- Explore operational technology architecture and system interconnections
- Identify differences between IT and OT environments
- Assess ICS roles in industrial operations and critical infrastructure
- Review typical industrial communication processes
- Case Study: ICS architecture mapping in a manufacturing plant

Module 2: ICS Threat Landscape and Attack Vectors

- Identify key threat actors targeting ICS environments
- Explore malware families affecting OT systems
- Analyze vulnerabilities in industrial networks
- Examine social engineering and remote access risks
- Review evolving global trends in OT cyberattacks
- Case Study: Ransomware attack on a utility control system

Module 3: ICS Security Frameworks and Standards

- Review NIST CSF and its OT applications
- Align ICS operations with IEC 62443 standards
- Assess ISO 27001 applicability in industrial settings
- Map frameworks to organizational control requirements
- Integrate compliance into ICS risk assessments
- Case Study: IEC 62443 implementation in an energy utility

Module 4: ICS Network Architecture and Segmentation

- Conduct ICS network segmentation planning
- Analyze data flows, zones, and conduits
- Identify insecure network paths and traffic exposure
- Design defense-in-depth layers for OT environments
- Implement demilitarized zones for secure IT/OT integration
- Case Study: Segmentation overhaul in a refinery network

Module 5: ICS Asset Inventory and Network Mapping

- Develop full OT asset inventories
- Apply automated and manual discovery techniques
- Map communication flows across industrial networks
- Identify unauthorized devices and hidden attack surfaces

- Use network mapping tools to enhance visibility
- Case Study: Asset discovery improvement in a chemical plant

Module 6: ICS Vulnerability Assessment Techniques

- Conduct ICS vulnerability scanning using safe methods
- Evaluate risks from outdated firmware and legacy systems
- Examine misconfigurations in OT environments
- Prioritize vulnerabilities based on operational impact
- Apply tools optimized for industrial systems
- Case Study: Vulnerability review of PLCs in a factory

Module 7: ICS Protocol Analysis and Security Testing

- Understand common ICS protocols such as Modbus, DNP3 and OPC
- Identify protocol weaknesses and potential exploitation paths
- Conduct protocol traffic analysis for anomalies
- Evaluate insecure communication channels
- Apply security testing tools designed for ICS protocols
- Case Study: Protocol misuse in a water treatment facility

Module 8: Security Assessment of SCADA Systems

- Examine SCADA topology and communication layers
- Assess SCADA servers, HMIs and field devices
- Identify SCADA-specific vulnerabilities
- Evaluate remote access and monitoring risks
- Review patch management strategies in SCADA environments
- Case Study: SCADA security flaws at an electricity distributor

Module 9: Security Assessment of PLCs and Field Devices

- Understand PLC architecture and operational logic
- Identify configuration and firmware vulnerabilities
- Assess physical security of field devices
- Analyze logic manipulation and unauthorized changes
- Evaluate vendor-specific security controls
- Case Study: PLC misconfiguration affecting process control

Module 10: ICS Risk Assessment and Analysis

- Conduct operational risk reviews for industrial processes
- Apply qualitative and quantitative ICS risk methodologies
- Map threat likelihood and potential impacts
- Identify critical assets requiring priority protection
- Develop risk treatment and mitigation recommendations
- Case Study: ICS risk assessment for a power generation facility

Module 11: Supplier, Vendor & Third-Party Risk

- Assess vendor compliance with ICS cybersecurity requirements
- Review third-party remote access risks

- Analyze supply-chain security vulnerabilities
- Develop vendor assurance and testing protocols
- Implement contract-based cybersecurity obligations
- Case Study: Vendor-induced breach affecting manufacturing controls

Module 12: ICS Monitoring, Detection & Threat Intelligence

- Apply OT monitoring tools for real-time visibility
- Analyze ICS logs for threat indicators
- Integrate threat intelligence into assessments
- Deploy anomaly detection for industrial environments
- Strengthen detection capabilities using behavioral analytics
- Case Study: Threat intelligence leading to early breach detection

Module 13: ICS Incident Response and Recovery

- Establish OT-specific incident response procedures
- Conduct forensic investigation in industrial environments
- Coordinate IT/OT response collaboration
- Develop operational continuity and system recovery steps
- Build post-incident lessons learned frameworks
- Case Study: Coordinated response to an ICS network compromise

Module 14: Governance, Policies & ICS Security Management

- Develop ICS security governance frameworks
- Establish roles, responsibilities and escalation paths
- Define policies for access, operations and maintenance
- Strengthen training programs for ICS operators
- Integrate security governance into daily operations
- Case Study: Governance improvement program in a utility

Module 15: Developing ICS Security Assessment Reports

- Document assessment findings and risk exposure
- Prepare structured vulnerability and mitigation summaries
- Communicate technical risks to non-technical leadership
- Develop improvement plans and remediation priorities
- Build reporting templates aligned with compliance frameworks
- Case Study: Comprehensive ICS assessment report for an industrial plant

Training Methodology

- Instructor-led presentations and interactive technical sessions
- Hands-on demonstrations of ICS assessment tools and techniques
- Scenario-based group exercises simulating ICS security events
- Real-world case study analysis for applied learning
- Guided development of ICS assessment and mitigation plans
- Practical templates, checklists and reporting tools for implementation

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com