Incident Response in Industrial Control Systems Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The security of Critical Infrastructure is paramount, yet Industrial Control Systems (ICS) and Operational Technology (OT) environments face a unique and rapidly evolving threat landscape. Unlike traditional IT systems, a cyber-incident in an ICS/OT network which includes SCADA, DCS, and PLC can have catastrophic cyber-physical consequences, leading to operational downtime, equipment damage, environmental disaster, and even loss of life. Incident Response in Industrial Control Systems Training Course is designed to empower security professionals and operations staff with the specialized knowledge and hands-on skills required for effective and safe incident response in these sensitive, high-availability settings. We move beyond generic IT-centric models to focus on the preservation of safety, reliability, and process integrity.

This intensive program provides a systematic methodology to prepare for, detect, analyze, contain, and recover from sophisticated attacks like ransomware and APTs targeting industrial environments. Participants will learn how to apply the NIST Cybersecurity Framework and MITRE ATT&CK for ICS to develop ICS-specific IR plans and playbooks. Through real-world case studies including Stuxnet, Triton, and recent ransomware events impacting critical manufacturing and utilities we ensure students gain practical, battle-tested expertise. Mastering ICS-IR is no longer optional; it is a mandatory competency for maintaining operational resilience and securing the digital transformation of industrial operations.

Programme Curriculum

Incident Response in Industrial Control Systems Training Course

Introduction

The security of Critical Infrastructure is paramount, yet Industrial Control Systems (ICS) and Operational Technology (OT) environments face a unique and rapidly evolving threat landscape. Unlike traditional IT

systems, a cyber-incident in an ICS/OT network which includes SCADA, DCS, and PLC can have catastrophic cyber-physical consequences, leading to operational downtime, equipment damage, environmental disaster, and even loss of life. Incident Response in Industrial Control Systems Training Course is designed to empower security professionals and operations staff with the specialized knowledge and hands-on skills required for effective and safe incident response in these sensitive, high-availability settings. We move beyond generic IT-centric models to focus on the preservation of safety, reliability, and process integrity.

This intensive program provides a systematic methodology to prepare for, detect, analyze, contain, and recover from sophisticated attacks like ransomware and APTs targeting industrial environments. Participants will learn how to apply the NIST Cybersecurity Framework and MITRE ATT&CK for ICS to develop ICS-specific IR plans and playbooks. Through real-world case studies including Stuxnet, Triton, and recent ransomware events impacting critical manufacturing and utilities we ensure students gain practical, battle-tested expertise. Mastering ICS-IR is no longer optional; it is a mandatory competency for maintaining operational resilience and securing the digital transformation of industrial operations.

Course Duration

5 days

Course Objectives with Strong Trending Keywords

1. Master the unique ICS/OT attack surface and model threats using the MITRE ATT&CK for ICS framework.
2. Apply non-invasive digital forensics techniques to collect and preserve evidence from specialized OT assets.
3. Implement cyber-physical containment strategies to safely isolate compromised segments while maintaining essential process safety.
4. Differentiate between IT and OT security models and address the realities of IT/OT convergence and the 'air-gap' myth.
5. Develop specific ICS ransomware playbooks focusing on rapid recovery and process restoration.
6. Understand NERC-CIP, ISA/IEC 62443, and other regulatory compliance requirements for incident reporting.
7. Utilize tools for deep packet inspection and analysis of proprietary and common industrial protocols.
8. Implement and tune ICS-specific SIEM and Network Security Monitoring (NSM) tools for early threat detection.
9. Integrate vulnerability assessment and patch management into the IR lifecycle for continuous improvement.
10. Execute effective crisis communication plans for technical staff, management, and external regulatory bodies.
11. Apply structured threat hunting methodologies within the OT environment to proactively search for Indicators of Compromise
12. Evaluate and integrate Zero Trust principles into industrial network segmentation and access control policies.
13. Design and practice robust OT disaster recovery and business continuity plans to minimize downtime post-incident.

Target Audience

1. OT/Control Systems Engineers.
2. IT/OT Cybersecurity Analysts

3. Industrial Network Architects.
4. Incident Response Team Members.
5. Critical Infrastructure Managers.
6. Compliance and Audit Professionals.
7. Cyber-Physical Security Specialists.
8. Forensic Investigators.

Course Modules

Module 1: Foundational Concepts & ICS Environment Context

- Key architectural, protocol, and risk differences.
- Understanding the Purdue Model and its role in network segmentation.
- Prioritizing safety instrumented systems and physical safety during IR.
- Common ICS components.
- Case Study: The Maroochy Shire Sewage Spill (1999).

Module 2: ICS Incident Response Planning and Preparation

- Adopting the NIST IR Lifecycle and tailoring it for industrial environments
- Developing an ICS Incident Response Policy and establishing clear roles and responsibilities.
- Creating and testing IR Go-Kits for remote OT sites.
- Implementing Secure Communication methods during an incident, isolated from the compromised network.
- Case Study: Colonial Pipeline Ransomware (2021).

Module 3: Detection and Analysis in OT Networks

- PLC logs, HMI alarms, firewall logs, and network traffic.
- Introduction to Industrial Protocol Analysis using Wireshark and specialized tools.
- Mapping observed malicious activity to the MITRE ATT&CK for ICS tactics and techniques.
- Initial triage and distinguishing between an incident and an operational event.
- Case Study: Ukraine Power Grid Attack (2015/2016).

Module 4: Containment, Eradication, and Mitigation

- Establishing safe and effective process-level containment.
- Network Segmentation strategies.
- Techniques for malware eradication from HMI and Engineering Workstations without impacting production.
- Utilizing threat intelligence to identify the root cause and ensure complete eradication.
- Case Study: TRITON/TRISIS Attack (2017).

Module 5: ICS Digital Forensics and Evidence Acquisition

- Challenges of live system forensics on low-resource or proprietary OT devices.
- Best practices for acquiring and preserving volatile and non-volatile evidence from PLCs and HMIs.
- Time Synchronization across IT and OT networks for accurate attack timeline reconstruction.
- Analyzing Historian database integrity and control logic for signs of tampering.
- Case Study: Stuxnet (2010).

Module 6: Recovery and Post-Incident Activities

- Developing a structured recovery plan that prioritizes process and equipment integrity.
- Securely rebuilding and restoring compromised control systems and re-integrating them into the network.
- Conducting "Lessons Learned" sessions and generating the Post-Incident Report.
- Integrating new defensive controls and security monitoring based on incident findings.
- Case Study: NotPetya's impact on a global manufacturer (2017).

Module 7: Advanced ICS Threats and Threat Hunting

- Understanding the mechanics of Advanced Persistent Threats targeting industrial espionage.
- Practical application of YARA rules and IOCs for proactive detection of novel OT malware.
- Using NetFlow/IPFIX data for detecting lateral movement and command-and-control activity in OT.
- Simulating an attack scenario using Red Team/Blue Team exercises in a lab environment.
- Case Study: Oldsmar Water Treatment Facility Intrusion Attempt (2021).

Module 8: Policy, Standards, and Program Development

- Benchmarking and implementing controls from ISA/IEC 62443 security standards.
- Integrating IR with Risk Management and Vulnerability Disclosure policies.
- Supply Chain Risk Management for hardware and software used in ICS environments.
- Conducting tabletop exercises and simulations for continuous team readiness.
- Case Study: General Industry Cyber Incident Response Example

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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