Training Course on Incident Response for Critical Infrastructure

Professional Development Training Course Outline

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

Course Introduction

In today’s increasingly connected and digitized world, Critical Infrastructure (CI)—including energy, healthcare, transportation, water systems, and communications—faces unprecedented threats from both cyberattacks and physical disruptions. The rise of ransomware attacks, nation-state actors, zero-day vulnerabilities, and supply chain exploits has amplified the need for robust and adaptive incident response (IR) strategies. With growing regulatory compliance demands and sophisticated threat landscapes, this training course is designed to arm professionals with actionable insights, real-time response capabilities, and strategic frameworks to secure vital systems.

Training Course on Incident Response for Critical Infrastructure equips participants with the tools to detect, analyze, contain, and recover from incidents impacting critical infrastructure. By leveraging advanced threat intelligence, SOC best practices, and MITRE ATT&CK frameworks, learners will develop the necessary skills to manage emergencies, reduce downtime, and ensure resilience. This course integrates live simulations, case-based learning, and automated response tools to empower professionals with both technical and decision-making competencies in the realm of incident response.

Programme Curriculum

Training Course on Incident Response for Critical Infrastructure

Introduction

In today’s increasingly connected and digitized world, Critical Infrastructure (CI)—including energy, healthcare, transportation, water systems, and communications—faces unprecedented threats from both cyberattacks and physical disruptions. The rise of ransomware attacks, nation-state actors, zero-day vulnerabilities, and supply chain exploits has amplified the need for robust and adaptive incident response (IR) strategies. With growing regulatory compliance demands and sophisticated threat landscapes, this training course is designed to arm professionals with actionable insights, real-time response capabilities, and strategic frameworks to secure vital systems.

Training Course on Incident Response for Critical Infrastructure equips participants with the tools to detect, analyze, contain, and recover from incidents impacting critical infrastructure. By leveraging advanced threat intelligence, SOC best practices, and MITRE ATT&CK frameworks, learners will develop the necessary skills to manage emergencies, reduce downtime, and ensure resilience. This course integrates live simulations, case-based learning, and automated response tools to empower professionals with both technical and decision-making competencies in the realm of incident response.

Course Objectives

1. Understand the cyber-physical threat landscape in critical infrastructure.
2. Develop proactive incident detection capabilities using real-time telemetry.
3. Apply NIST and ISO 27035 frameworks in incident handling.
4. Build and lead a Security Operations Center (SOC) tailored for CI.
5. Enhance forensic investigation and evidence preservation techniques.
6. Implement automated response systems using SOAR tools.
7. Perform root cause analysis (RCA) and post-incident reviews.
8. Manage communications during a breach with media and stakeholders.
9. Design redundancy and failover systems to ensure business continuity.
10. Incorporate threat hunting and intelligence into IR strategies.
11. Integrate compliance and governance controls (GDPR, NERC CIP).
12. Practice tabletop and red team-blue team exercises.
13. Strengthen cross-sector collaboration and information sharing (ISACs, CISA).

Target Audience

1. Cybersecurity Analysts
2. IT & OT Engineers in Utilities
3. Incident Response Teams
4. Emergency Management Professionals
5. Infrastructure Risk Managers
6. Government Cyber Defense Units
7. SCADA System Administrators
8. Compliance Officers in Critical Sectors

Course Duration: 5 days

Course Modules

Module 1: Understanding Critical Infrastructure Threat Landscape

- Definition and sectors of Critical Infrastructure (CI)
- Cyber-physical attack vectors and tactics
- Threat actors: state-sponsored, APTs, hacktivists
- Common vulnerabilities in OT and ICS
- Regulatory context (NIST, CISA, NERC CIP)
- **Case Study**: Stuxnet – Nation-state attack on Iranian nuclear facility

Module 2: Building a Resilient Incident Response Framework

- Introduction to NIST and ISO 27035 IR lifecycle
- Roles and responsibilities in IR teams
- Integration of IT and OT incident protocols
- IR documentation and runbooks
- Communication protocols and escalation matrices
- **Case Study**: Colonial Pipeline attack and response framework

Module 3: Incident Detection & Threat Intelligence Integration

- Monitoring tools: SIEM, IDS/IPS, and anomaly detection
- Telemetry and log correlation
- Use of MITRE ATT&CK for TTP mapping
- Threat feeds and CTI platforms
- Real-time alert triage and event prioritization
- **Case Study**: Ukraine Power Grid cyberattack via BlackEnergy

Module 4: Investigating and Containing Cyber Incidents

- Digital forensics fundamentals
- Chain of custody and evidence handling
- Malware sandboxing and reverse engineering basics
- Isolation techniques for infected systems
- Memory and disk analysis tools
- **Case Study**: Norsk Hydro ransomware attack forensic analysis

Module 5: Recovery, Business Continuity & Root Cause Analysis

- Restoration protocols and clean environment setups
- Data backup and restore policies
- RCA methods: 5 Whys, Fishbone, Timeline Analysis
- Updating defense mechanisms post-incident
- Business Continuity Plan (BCP) in CI sectors
- **Case Study**: Sony Pictures breach – Lessons on resilience and recovery

Module 6: Automation & SOAR Integration in CI

- Introduction to SOAR platforms
- Use cases of automation in IR
- Playbook creation and orchestration
- Integrating threat feeds with automated responses
- Metrics and KPIs for SOAR effectiveness
- **Case Study**: Using IBM Resilient for rapid response in healthcare breach

Module 7: Red Team/Blue Team & Tabletop Exercises

- Benefits of adversary simulation in CI
- Designing tabletop exercise scenarios
- Roles and rules in Red vs. Blue exercises
- Debriefing and performance evaluation
- Building resilience through simulated stress
- **Case Study**: Simulated cyber-attack on water utility systems

Module 8: Governance, Compliance & Sector Collaboration

- Overview of legal and compliance frameworks
- Sector-specific guidelines (HIPAA, NERC CIP, etc.)
- Working with ISACs and threat intelligence communities
- Public-private partnerships for cyber defense
- Developing an IR compliance checklist
- **Case Study**: European ENISA-led initiative in energy infrastructure

Training Methodology

- Instructor-led live sessions and Q&A

- Hands-on labs and real-world simulations
- Interactive group case study discussions
- Threat scenario-based assessments
- Red team-blue team exercises with evaluation reports
- Templates, playbooks, and toolkit downloads

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

Start Date	End Date	Location	Price
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