Training Course on Building and Maturing an Incident Response Program

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 rapidly evolving cybersecurity landscape, building and maturing an Incident Response Program (IRP) is not only a necessity but a strategic advantage. Training Course on Building and Maturing an Incident Response Program equips cybersecurity professionals and IT leaders with the critical knowledge and tactical skills required to develop, enhance, and maintain a resilient, scalable, and compliant incident response framework. Through a hands-on, case-driven approach, participants will explore proactive incident response planning, threat detection, breach containment, forensics, recovery strategies, and post-incident improvement.

As organizations face increasingly sophisticated cyber threats—ranging from ransomware to advanced persistent threats (APT)—this course focuses on creating agile, effective, and fully integrated response mechanisms. Learners will master essential components such as incident response lifecycle management, regulatory alignment (GDPR, HIPAA, ISO/IEC 27035), cloud and hybrid response strategies, communication protocols, and automation with SOAR technologies. This course is designed to help organizations minimize risk exposure, protect digital assets, and maintain business continuity.

Programme Curriculum

Training Course on Building and Maturing an Incident Response Program

Introduction

In today's rapidly evolving cybersecurity landscape, building and maturing an Incident Response Program (IRP) is not only a necessity but a strategic advantage. Training Course on Building and Maturing an Incident Response Program equips cybersecurity professionals and IT leaders with the critical knowledge and tactical skills required to develop, enhance, and maintain a resilient, scalable, and compliant incident response framework. Through a hands-on, case-driven approach, participants will explore proactive incident response planning, threat detection, breach containment, forensics, recovery strategies, and post-incident improvement.

As organizations face increasingly sophisticated cyber threats—ranging from ransomware to advanced persistent threats (APT)—this course focuses on creating agile, effective, and fully integrated response mechanisms. Learners will master essential components such as incident response lifecycle management, regulatory alignment (GDPR, HIPAA, ISO/IEC 27035), cloud and hybrid response strategies, communication protocols, and automation with SOAR technologies. This course is designed to help organizations minimize risk exposure, protect digital assets, and maintain business continuity.

Course Objectives

1. Understand the core components of a robust incident response program.
2. Identify, analyze, and categorize cyber threats in real-time.
3. Develop a risk-based incident classification and escalation matrix.
4. Design a custom incident response policy and workflow.
5. Apply industry-standard frameworks (NIST, ISO, CIS) for IR maturity.
6. Integrate threat intelligence feeds into the response process.
7. Implement Security Orchestration, Automation, and Response (SOAR).
8. Conduct incident simulations and tabletop exercises.
9. Align IR activities with data privacy laws and compliance mandates.
10. Manage and mitigate insider threats and third-party risks.
11. Automate alert triage and incident prioritization.
12. Strengthen cross-functional communication during crises.
13. Perform effective post-incident reviews and continual improvement.

Target Audiences

1. Chief Information Security Officers (CISOs)
2. Cybersecurity Analysts and Engineers
3. Security Operations Center (SOC) Teams
4. IT Risk Managers
5. Compliance Officers and Auditors
6. Digital Forensics Experts
7. Cloud Security Professionals
8. Government and Law Enforcement Agencies

Course Duration: 5 days

Course Modules

Module 1: Fundamentals of Incident Response Programs

- Introduction to Incident Response Lifecycle
- Importance of IR Policies and Governance
- Overview of Roles and Responsibilities
- Legal and Regulatory Drivers
- Basic Response Metrics and KPIs
- **Case Study:** Designing an IR Plan for a Small Healthcare Provider

Module 2: Threat Intelligence and Detection Techniques

- Types of Threat Intelligence (Strategic, Tactical, Operational)
- Indicators of Compromise (IoC) and TTPs
- Integrating Threat Feeds and SIEM Tools
- Threat Hunting Fundamentals
- Real-Time Detection and Alerting Techniques
- **Case Study:** Threat Detection in a Financial Services Organization

Module 3: Security Playbooks and IR Workflow Automation

- Creating Customized Playbooks
- Playbook Templates for Different Attack Types
- Using SOAR for Workflow Automation
- Building Response Escalation Paths
- Orchestrating Cross-System Responses
- **Case Study:** Automating a Ransomware Response in a Retail Chain

Module 4: Cloud and Hybrid Environment Response Strategies

- Cloud-Specific Threat Models
- IR in AWS, Azure, and Google Cloud
- Data Visibility and Access Challenges
- Hybrid Infrastructure Considerations
- Cloud Forensics and Log Retention
- **Case Study:** Containing a Cloud Breach in a SaaS Startup

Module 5: Digital Forensics and Evidence Preservation

- Chain of Custody and Legal Considerations
- Memory and Disk Forensics Tools
- Log Analysis Techniques
- Timeline Reconstruction
- Evidence Reporting and Documentation
- **Case Study:** Forensic Analysis of a Phishing-Induced Breach

Module 6: Regulatory Compliance and Incident Reporting

- GDPR, HIPAA, and CCPA IR Requirements
- Timely Breach Disclosure Practices
- Documentation and Audit Trails
- Collaboration with Legal Teams
- Cross-Border Incident Handling
- **Case Study:** Regulatory Reporting for a Global Data Leak

Module 7: Crisis Communication and Stakeholder Engagement

- Internal and External Communication Plans
- Handling the Media During a Breach
- Engaging Executive Leadership and Board Members
- Messaging Templates and Timing
- Maintaining Customer Trust
- **Case Study:** Communication Strategy for a Compromised e-Commerce Platform

Module 8: Continuous Improvement and IR Program Maturity

- Conducting Post-Incident Reviews
- Tracking Lessons Learned and Metrics
- Updating Playbooks and Policies
- Maturity Models and Roadmaps
- Investment in Tools and Training
- **Case Study:** Maturing the IR Program of a Global Manufacturer

Training Methodology

- Instructor-led interactive sessions

- Real-world case studies and scenarios
- Hands-on labs and cyber range simulations
- Group-based tabletop exercises
- Access to downloadable toolkits and templates
- Knowledge checks and final assessment

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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