Training Course on Incident Response Playbook Development and Customization

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 cyber threat landscape, organizations must adopt proactive and systematic strategies to manage and mitigate security incidents. An effective Incident Response Playbook is a cornerstone of any resilient cybersecurity program, providing predefined steps to detect, respond to, and recover from various cyber threats. This course empowers cybersecurity professionals with the skills to develop, tailor, and operationalize incident response playbooks aligned with industry best practices such as NIST, MITRE ATT&CK®, and ISO 27035.

Training Course on Incident Response Playbook Development and Customization is designed for both emerging and experienced security practitioners and emphasizes playbook automation, real-world use cases, and adaptive response mechanisms. Participants will learn how to structure playbooks by attack vector, customize actions per threat actor profile, and integrate with SIEM/SOAR platforms to reduce response time. By the end of the course, you'll be equipped with the strategic and technical skills to build agile, scalable, and threat-informed response procedures.

Programme Curriculum

Training Course on Incident Response Playbook Development and Customization

Introduction

In today's rapidly evolving cyber threat landscape, organizations must adopt proactive and systematic strategies to manage and mitigate security incidents. An effective Incident Response Playbook is a cornerstone of any resilient cybersecurity program, providing predefined steps to detect, respond to, and recover from various cyber threats. This course empowers cybersecurity professionals with the skills to develop, tailor, and operationalize incident response playbooks aligned with industry best practices such as NIST, MITRE ATT&CK®, and ISO 27035.

Training Course on Incident Response Playbook Development and Customization is designed for both emerging and experienced security practitioners and emphasizes playbook automation, real-world use cases, and adaptive response

mechanisms. Participants will learn how to structure playbooks by attack vector, customize actions per threat actor profile, and integrate with SIEM/SOAR platforms to reduce response time. By the end of the course, you'll be equipped with the strategic and technical skills to build agile, scalable, and threat-informed response procedures.

Course Objectives

1. Understand the fundamentals of incident response frameworks and standards (NIST, ISO, MITRE).
2. Design cyber incident playbooks for various attack vectors (phishing, ransomware, insider threats).
3. Customize playbooks for cloud, on-premise, and hybrid environments.
4. Integrate playbooks with SOAR platforms (Security Orchestration, Automation and Response).
5. Develop automated response workflows to enhance operational efficiency.
6. Identify critical stakeholders and establish clear communication protocols during incidents.
7. Leverage threat intelligence feeds to update and refine response strategies.
8. Map incident workflows using tools like Lucidchart, Draw.io, or MISP.
9. Implement response escalation protocols based on risk severity.
10. Evaluate playbook effectiveness through tabletop exercises and red team simulations.
11. Apply compliance-driven customization for GDPR, HIPAA, and PCI-DSS.
12. Reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
13. Create post-incident review mechanisms to update playbooks iteratively.

Target Audience

1. Cybersecurity Analysts
2. Incident Response Team Leads
3. SOC Managers
4. IT Risk & Compliance Officers
5. Cloud Security Engineers
6. CIOs / CISOs
7. DevSecOps Professionals
8. Security Architects

Course Duration: 5 days

Course Modules

Module 1: Foundations of Incident Response Playbooks

- Introduction to Incident Response Lifecycle (Preparation to Recovery)
- Frameworks: NIST 800-61r2, ISO/IEC 27035, MITRE ATT&CK
- Key components of an IR playbook
- Categorizing incidents: Low, Medium, High
- Establishing roles & responsibilities
- **Case Study:** Mapping NIST standards to an enterprise ransomware playbook

Module 2: Threat Landscape and Use Case Identification

- Identifying top threat vectors (Phishing, DDoS, Malware, Zero-day)
- Creating threat profiles and risk classification
- Selecting relevant use cases for playbook development
- Prioritizing based on business impact and frequency
- Involving threat intelligence in use case design
- **Case Study:** Building a phishing response playbook for a fintech company

Module 3: Designing Playbook Templates and Structures

- Playbook structure: triggers, actions, escalation paths

- Incorporating SOAR-compatible workflows
- Building decision trees and flowcharts
- Aligning with business units and functions
- Version control and change management
- **Case Study:** Template creation for insider threat playbook at a healthcare provider

Module 4: Playbook Customization Strategies

- Adapting templates per environment (Cloud, On-prem, Hybrid)
- Compliance-based customization (HIPAA, PCI-DSS, GDPR)
- Regional threat actor alignment (APT Groups)
- Custom actions and mitigations
- Localization and language translation needs
- **Case Study:** GDPR-specific data breach response playbook for an EU-based firm

Module 5: Automation & Orchestration with SOAR

- Introduction to SOAR tools: Splunk Phantom, Cortex XSOAR, IBM Resilient
- Linking playbooks with SIEM & ticketing systems
- Automating containment and remediation tasks
- Alert enrichment through CTI
- Reducing false positives through contextual playbooks
- **Case Study:** Automated ransomware playbook using Splunk SOAR for an eCommerce company

Module 6: Testing, Simulation, and Optimization

- Conducting Tabletop Exercises (TTX)
- Red/Blue Team engagement for playbook validation
- Metrics to track: MTTD, MTTR, FNR
- Feedback loops for continuous improvement
- Incident review and root cause analysis
- **Case Study:** Optimizing MTTR through quarterly simulation in a multinational bank

Module 7: Cross-Functional Communication and Coordination

- Engaging legal, PR, HR, and leadership during incidents
- Drafting communication templates and press statements
- Decision-making matrix for incident escalation
- Coordinating with third-party vendors and MSSPs
- Building war room strategies and logging processes
- **Case Study:** Crisis communication playbook during a data breach at a SaaS startup

Module 8: Governance, Compliance & Documentation

- Regulatory reporting timelines (e.g., GDPR 72-hour rule)
- Documentation standards for audits
- Legal hold and evidence preservation
- Integration with risk management frameworks
- Ensuring audit-readiness and traceability
- **Case Study:** Developing a compliance-aligned playbook for a healthcare audit scenario

Training Methodology

- Live instructor-led sessions with industry experts
- Hands-on labs using simulation environments (SOAR, SIEM)
- Collaborative group exercises to design and customize playbooks

- Case study analysis per module
- Access to customizable templates, checklists, and flowcharts
- Certification quiz and capstone project at course end

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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