Computer Security Incident Management and Playbook Development 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 landscape of cyber threats is evolving rapidly, making a proactive and structured Incident Response (IR) capability a non-negotiable requirement for all organizations. Computer Security Incident Management and Playbook Development Training Course equips participants with the expert-level skills to establish, operate, and mature a world-class Incident Response Team (IRT). We will dive deep into the complete incident lifecycle, mastering critical phases like triage, containment, eradication, and the crucial post-incident analysis. Strong keywords: Cyber Resilience, Incident Response Lifecycle, Digital Forensics, Security Operations Center (SOC), Threat Hunting.

This course emphasizes the strategic creation of customized, actionable IR Playbooks the essential blueprints for handling specific, high-impact threats such as Ransomware Attacks, Advanced Persistent Threats (APTs), and Cloud Security breaches. By leveraging industry-standard frameworks like NIST SP 800-61 and the MITRE ATT&CK matrix, participants will learn to codify response procedures, automate steps, and ensure regulatory compliance. The focus is on practical, hands-on application, transforming theoretical knowledge into the muscle memory needed to achieve swift Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), thereby minimizing business impact and ensuring organizational security. Strong keywords: IR Playbooks, NIST Framework, MITRE ATT&CK, Ransomware Response, Business Continuity.

Programme Curriculum

Computer Security Incident Management and Playbook Development Training Course

Course Introduction

The landscape of cyber threats is evolving rapidly, making a proactive and structured Incident Response (IR) capability a non-negotiable requirement for all organizations. Computer Security Incident Management and

Playbook Development Training Course equips participants with the expert-level skills to establish, operate, and mature a world-class Incident Response Team (IRT). We will dive deep into the complete incident lifecycle, mastering critical phases like triage, containment, eradication, and the crucial post-incident analysis. Strong keywords: Cyber Resilience, Incident Response Lifecycle, Digital Forensics, Security Operations Center (SOC), Threat Hunting.

This course emphasizes the strategic creation of customized, actionable IR Playbooks the essential blueprints for handling specific, high-impact threats such as Ransomware Attacks, Advanced Persistent Threats (APTs), and Cloud Security breaches. By leveraging industry-standard frameworks like NIST SP 800-61 and the MITRE ATT&CK matrix, participants will learn to codify response procedures, automate steps, and ensure regulatory compliance. The focus is on practical, hands-on application, transforming theoretical knowledge into the muscle memory needed to achieve swift Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), thereby minimizing business impact and ensuring organizational security. Strong keywords: IR Playbooks, NIST Framework, MITRE ATT&CK, Ransomware Response, Business Continuity.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Strategically design and implement a robust Cybersecurity Incident Response Team structure.
2. Master the complete NIST Incident Response Lifecycle
3. Develop custom, threat-specific IR Playbooks for critical incidents like Zero-Day Exploits.
4. Apply practical Digital Forensics and evidence collection techniques for legal admissibility.
5. Reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) using automation.
6. Utilize the MITRE ATT&CK Framework for effective threat analysis and proactive Threat Hunting.
7. Implement effective Containment Strategies for complex environments, including Cloud Security and hybrid systems.
8. Formulate a clear Incident Communication Plan for both technical and executive stakeholders.
9. Conduct thorough Post-Incident Analysis and leverage Lessons Learned for continuous improvement.
10. Integrate Security Orchestration, Automation, and Response (SOAR) platforms into the IR process.
11. Ensure Regulatory Compliance during data breach reporting and handling.
12. Manage the response to specialized attacks, including Advanced Persistent Threats (APTs) and supply chain compromise.
13. Establish Cyber Resilience and Business Continuity by fully integrating IR with organizational strategy.

Target Audience

1. Incident Response Team (IRT) Members and Leads
2. Security Operations Center (SOC) Analysts and Managers
3. Cyber Security Architects and Engineers
4. IT/Information Security Managers and Directors
5. Threat Hunters and Digital Forensics Specialists
6. IT Risk and Compliance Professionals
7. System Administrators and Network Engineers with security duties
8. Business Continuity and Disaster Recovery Specialists

Course Modules

Module 1: Foundational Incident Response & CSIRT Establishment

- The Cybersecurity Incident Response Lifecycle
- Defining and scoping an effective Computer Security Incident Response Team
- Measuring MTTD, MTTR, and overall Cyber Resilience.
- Tools and infrastructure.
- Case Study: Target Data Breach (2013).

Module 2: Detection, Triage, and Analysis

- Identifying Indicators of Compromise and Indicators of Attack.
- Leveraging the MITRE ATT&CK Framework for adversarial behavior mapping.
- Effective Triage procedures and incident severity classification.
- Techniques for initial evidence preservation and digital forensics readiness.
- Case Study: SolarWinds Supply Chain Attack (2020).

Module 3: Incident Containment and Eradication Strategies

- Developing immediate, short-term, and long-term Containment Strategies.
- Network segmentation, isolation, and host-based containment techniques.
- Deep-dive into Eradication procedures, threat removal, and patching.
- Specialized containment for Cloud-based and Virtualized Environments.
- Case Study: NotPetya Ransomware Outbreak (2017).

Module 4: Incident Playbook Development Methodology

- Structuring an actionable IR Playbook.
- Creating a library of threat-specific playbooks
- Integrating decision trees, communication scripts, and tool-specific steps.
- Mapping playbook steps to the NIST IR Lifecycle and MITRE ATT&CK tactics.
- Case Study: Maersk Ransomware Recovery.

Module 5: Playbooks for Advanced Cyber Threats

- Developing playbooks for Ransomware Attack.
- Playbook strategies for defending against Advanced Persistent Threats (APTs).
- Handling incidents involving Cloud Security
- Response planning for compromised identities and Business Email Compromise (BEC).
- Case Study: Colonial Pipeline Attack (2021).

Module 6: Incident Recovery and Post-Incident Activities

- System restoration, verification, and hardening processes.
- Developing a comprehensive Post-Incident Analysis report structure.
- Implementing Lessons Learned and continuous IR program maturity.
- Managing regulatory reporting obligations and legal hold requirements.
- Case Study: Equifax Data Breach (2017)

Module 7: Automation and Communication in Incident Response

- Introduction to SOAR platforms and automated playbooks/runbooks.
- Writing effective Executive-Level Communication during a crisis.

- Managing internal and external communication
- Conducting effective Tabletop Exercises and simulation drills for team readiness.
- Case Study: Uber Data Breach Communication (2016/2017).

Module 8: Building a Mature and Compliant IR Program

- Aligning IR with Risk Management and Business Continuity goals.
- Integrating threat intelligence into the Incident Response Plan.
- Understanding the role of cyber insurance and legal counsel in an incident.
- Measuring and improving IR Program maturity using frameworks.
- Case Study: Mandiant?ÇÖs Incident Response Report on State-Sponsored Attacks.

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	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

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

Register Online Now

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