Training Course on Post-Incident Analysis and Lessons Learned

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 threat landscape, Post-Incident Analysis and Lessons Learned is no longer optional—it is essential. Training Course on Post-Incident Analysis and Lessons Learned equips IT professionals, incident responders, risk managers, and organizational leaders with the skills to perform structured post-incident reviews that uncover root causes, minimize future risks, and enhance cybersecurity resilience. By understanding what went wrong and why, your team can build better systems, enforce stronger protocols, and drive continuous improvement.

With a focus on data-driven decision-making, incident response frameworks, and forensic review, this course provides the tools and methodologies required to conduct post-incident investigations that lead to actionable improvements. Attendees will gain hands-on experience through real-world case studies, modern tools for documentation, and collaborative analysis techniques aligned with industry standards such as NIST, ISO 27001, and MITRE ATT&CK.

Programme Curriculum

Training Course on Post-Incident Analysis and Lessons Learned

Introduction

In today's rapidly evolving threat landscape, Post-Incident Analysis and Lessons Learned is no longer optional—it is essential. Training Course on Post-Incident Analysis and Lessons Learned equips IT professionals, incident responders, risk managers, and organizational leaders with the skills to perform structured post-incident reviews that uncover root causes, minimize future risks, and enhance cybersecurity resilience. By understanding what went wrong and why, your team can build better systems, enforce stronger protocols, and drive continuous improvement.

With a focus on data-driven decision-making, incident response frameworks, and forensic review, this course provides the tools and methodologies required to conduct post-incident investigations that lead to actionable improvements. Attendees will gain hands-on experience through real-world case studies, modern tools for documentation, and collaborative analysis

techniques aligned with industry standards such as NIST, ISO 27001, and MITRE ATT&CK.

Course Objectives

1. Understand the fundamentals of post-incident analysis and how it supports cybersecurity maturity.
2. Apply root cause analysis (RCA) to identify the origin of incidents.
3. Document and communicate findings using incident reporting templates.
4. Analyze cyber threat intelligence (CTI) inputs to enrich post-event findings.
5. Apply the MITRE ATT&CK Framework in post-incident classification.
6. Facilitate after-action reviews (AARs) and create clear lesson-learned documentation.
7. Distinguish between technical and organizational failures during security events.
8. Integrate SIEM and forensic tools in the analysis workflow.
9. Drive continuous improvement through trend identification and feedback loops.
10. Build a culture of accountability and resilience post-incident.
11. Map incident findings to compliance and regulatory frameworks.
12. Develop mitigation strategies based on analytical insights.
13. Align post-incident procedures with incident response playbooks.

Target Audiences

1. Cybersecurity Analysts
2. IT Incident Response Teams
3. Risk and Compliance Officers
4. Security Operations Center (SOC) Staff
5. DevSecOps Engineers
6. IT Managers and Directors
7. Digital Forensics Specialists
8. Business Continuity Planners

Course Duration: 5 days

Course Modules

Module 1: Introduction to Post-Incident Analysis

- Importance of structured reviews after incidents
- Lifecycle of incident response
- Linking incident response to business resilience
- Common types of post-incident reports
- Key performance indicators (KPIs) for analysis
- **Case Study:** Ransomware attack on a healthcare institution

Module 2: Root Cause Analysis Techniques

- Fishbone (Ishikawa) diagrams and the 5 Whys
- Distinguishing symptoms from causes
- Tools for collaborative RCA
- Documenting findings for stakeholders
- Preventative actions based on RCA
- **Case Study:** Data breach via insider threat in a finance company

Module 3: Frameworks and Standards

- Overview of MITRE ATT&CK for mapping techniques
- NIST SP 800-61 guidelines on incident handling

- ISO 27001:2013 and lessons learned integration
- Aligning findings to regulatory compliance (GDPR, HIPAA)
- Framework selection strategy
- **Case Study:** SOC response review aligned to NIST

Module 4: After-Action Review (AAR) Implementation

- Setting objectives for effective AARs
- Creating a safe environment for discussion
- Key questions and structure of a productive AAR
- Encouraging team participation and transparency
- Reporting lessons learned organization-wide
- **Case Study:** Cloud misconfiguration incident at a SaaS provider

Module 5: Documentation and Reporting

- Post-incident templates and logs
- Categorization of security events
- Executive summaries for leadership
- Technical appendices for engineers
- Leveraging automation in documentation
- **Case Study:** Insider sabotage and its documentation trail

Module 6: Integrating Forensics and Threat Intelligence

- Digital forensics role in post-incident reviews
- Using SIEM data to reconstruct timelines
- Correlating logs and indicators of compromise (IOCs)
- Integrating external threat intelligence feeds
- Forensic triage and retention policies
- **Case Study:** Credential stuffing in an e-commerce platform

Module 7: Action Plans and Improvement Strategy

- Designing improvement plans from findings
- Prioritization using risk impact assessment
- Monitoring the effectiveness of actions
- Implementing feedback loops
- KPI dashboard development
- **Case Study:** Phishing campaign affecting remote workers

Module 8: Culture and Communication

- Building a no-blame culture post-incident
- Training and communication strategies
- Sharing lessons across departments
- Executive briefings and board-level updates
- Embedding learning in organizational processes
- **Case Study:** Public sector DDoS attack and internal communications

Training Methodology

- Interactive lectures with subject matter experts
- Scenario-based group activities
- Real-world case study reviews
- Hands-on sessions with tools like SIEM, RCA software

- Template-driven workshops for reporting and improvement plans
- Post-training quiz and knowledge checks

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
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