Training Course on Incident Response and Handling

Professional Development Training Course Outline

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

Course Introduction

In today's rapidly evolving digital landscape, organizations face an increasing barrage of cyber threats and security incidents. A robust Incident Response and Handling capability is no longer optional but a critical necessity for business continuity and resilience. Training Course on Incident Response and Handling equips individuals and teams with the essential knowledge and practical skills to effectively detect, analyze, contain, eradicate, recover from, and learn from security incidents. By mastering industry best practices and leveraging cutting-edge threat intelligence, participants will gain the confidence to minimize the impact of breaches, protect valuable assets, and maintain stakeholder trust. This training delves into the core principles of digital forensics, malware analysis, and proactive security posture improvement, ensuring a holistic understanding of the incident lifecycle.

This intensive program is designed to cultivate proactive cybersecurity professionals capable of navigating the complexities of modern security challenges. Through a blend of theoretical foundations and hands-on exercises, participants will develop proficiency in building and executing effective incident response plans. Key areas of focus include understanding legal and ethical considerations, effective communication strategies during a crisis, and the importance of continuous improvement through post-incident analysis. By the end of this course, attendees will be empowered to lead and contribute significantly to their organization's cyber resilience and overall security strategy, fostering a culture of proactive risk management and rapid threat mitigation.

Programme Curriculum

Training Course on Incident Response and Handling

Introduction

In today's rapidly evolving digital landscape, organizations face an increasing barrage of cyber threats and security incidents. A robust Incident Response and Handling capability is no longer optional but a critical necessity for business continuity and resilience. Training Course on Incident Response and Handling equips individuals and teams with the essential knowledge and practical skills to effectively detect, analyze, contain, eradicate, recover from, and learn from security incidents. By mastering industry best practices and leveraging cutting-edge threat intelligence, participants will gain the confidence to minimize the impact of breaches, protect valuable assets, and maintain stakeholder trust. This training delves into the core principles of digital forensics, malware analysis, and proactive security posture improvement, ensuring a holistic understanding of the incident lifecycle.

This intensive program is designed to cultivate proactive cybersecurity professionals capable of navigating the complexities of modern security challenges. Through a blend of theoretical foundations and hands-on exercises, participants will develop proficiency in building and executing effective incident response plans. Key areas of focus include understanding legal and ethical considerations, effective communication strategies during a crisis, and the importance of continuous improvement through post-incident analysis. By the end of this course, attendees will be empowered to lead and contribute significantly to their organization's cyber resilience and overall security strategy, fostering a culture of proactive risk management and rapid threat mitigation.

Course Objectives

Upon completion of this Incident Response and Handling course, participants will be able to:

1. Understand the fundamental concepts and lifecycle of incident response.
2. Develop and implement effective incident response plans and procedures.
3. Master techniques for threat detection and early warning systems.
4. Conduct thorough security incident analysis and triage.
5. Apply various digital forensics methodologies for evidence collection and preservation.
6. Implement effective incident containment strategies to limit damage.
7. Perform comprehensive malware analysis to understand attack vectors.
8. Execute efficient incident eradication and system remediation processes.
9. Manage the incident recovery process and restore normal operations.
10. Conduct thorough post-incident analysis and lessons learned documentation.
11. Understand relevant legal and regulatory compliance requirements related to incident handling.
12. Develop effective communication strategies during security incidents.
13. Proactively improve organizational cybersecurity posture based on incident insights.

Target Audience

This course is designed for the following target audience:

1. Security Analysts: Professionals responsible for monitoring and responding to security events.
2. IT Administrators: Individuals managing and maintaining IT infrastructure and systems.
3. Network Engineers: Professionals responsible for the design, implementation, and maintenance of network infrastructure.
4. System Administrators: Individuals responsible for the configuration, operation, and maintenance of computer systems and servers.
5. Security Managers: Professionals overseeing the organization's security posture and incident response capabilities.
6. Compliance Officers: Individuals responsible for ensuring adherence to relevant security regulations and standards.
7. Risk Managers: Professionals involved in identifying, assessing, and mitigating organizational risks, including cybersecurity risks.
8. Anyone interested in developing skills in incident response and cybersecurity.

Course Duration:

- 5 days

Course Modules

Module 1: Foundations of Incident Response

- Understanding the definition and importance of incident response.
- Exploring the different phases of the incident response lifecycle.
- Identifying common types of security incidents and their impact.
- Understanding key roles and responsibilities within an incident response team.
- Overview of relevant frameworks and standards (e.g., NIST, ISO 27035).

Module 2: Preparation and Planning

- Developing and documenting a comprehensive incident response plan.
- Establishing communication protocols and escalation procedures.
- Identifying and inventorying critical assets and data.
- Implementing proactive security controls and preventative measures.
- Conducting risk assessments and vulnerability management.

Module 3: Detection and Analysis

- Implementing and utilizing security monitoring tools and technologies (e.g., SIEM).
- Analyzing security alerts, logs, and indicators of compromise (IOCs).
- Performing initial triage and determining the scope and severity of incidents.
- Understanding different attack vectors and methodologies.
- Leveraging threat intelligence feeds and resources.

Module 4: Containment, Eradication, and Recovery

- Implementing various containment strategies to limit the impact of incidents.
- Developing and executing eradication plans to remove threats from affected systems.
- Performing data recovery and system restoration procedures.
- Ensuring business continuity and minimizing downtime.
- Documenting all actions taken during the containment, eradication, and recovery phases.

Module 5: Digital Forensics and Evidence Handling

- Understanding the principles of digital forensics and evidence preservation.
- Utilizing forensic tools and techniques for data acquisition and analysis.
- Maintaining the chain of custody for digital evidence.
- Preparing forensic reports and documentation.
- Understanding legal considerations related to digital evidence.

Module 6: Malware Analysis

- Understanding different types of malware and their characteristics.
- Performing static and dynamic malware analysis techniques.
- Identifying malware behavior, capabilities, and potential impact.
- Extracting indicators of compromise (IOCs) from malware samples.
- Utilizing malware analysis tools and sandboxing environments.

Module 7: Post-Incident Activities and Lessons Learned

- Conducting thorough post-incident analysis meetings.
- Documenting lessons learned and identifying areas for improvement.
- Updating incident response plans and procedures based on insights.
- Communicating findings to relevant stakeholders.
- Implementing continuous improvement strategies for the security program.

Module 8: Legal, Ethical, and Communication Aspects

- Understanding relevant legal and regulatory requirements related to incident reporting.
- Addressing ethical considerations in incident response and data handling.
- Developing effective internal and external communication strategies during incidents.
- Managing public relations and stakeholder expectations.
- Understanding data privacy regulations and breach notification requirements.

Training Methodology

This course employs a blended learning approach incorporating:

- **Interactive Lectures:** Engaging presentations covering theoretical concepts and industry best practices.
- **Hands-on Labs:** Practical exercises using simulated environments and real-world scenarios to reinforce learning.
- **Case Studies:** Analysis of past security incidents to understand different approaches and outcomes.

- **Group Discussions:** Collaborative sessions to foster knowledge sharing and problem-solving skills.
- **Simulations:** Realistic incident response scenarios to test and refine participants' abilities.

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

Start Date	End Date	Location	Price
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
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