Training Course on Incident Response for Managed Security Service Providers (MSSP)

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, Managed Security Service Providers (MSSPs) play a critical role in delivering proactive, scalable, and real-time cybersecurity defense. The ability to swiftly detect, analyze, respond to, and recover from security incidents is essential in minimizing damage and maintaining trust with clients. Training Course on Incident Response for Managed Security Service Providers (MSSP) equips participants with advanced skills, frameworks, and real-world scenarios to manage cybersecurity incidents effectively and maintain compliance with global standards.

With increasing cyber threats such as ransomware, supply chain attacks, and insider threats, organizations demand responsive, resilient, and technically sound MSSPs. This course provides end-to-end training in threat intelligence, automated response, forensic analysis, communication protocols, and compliance practices tailored to MSSP environments. Participants will gain hands-on experience using top-tier tools, frameworks (like NIST and MITRE ATT&CK), and threat simulation techniques to create a mature, rapid-response incident management program.

Programme Curriculum

Training Course on Incident Response for Managed Security Service Providers (MSSP)

Introduction

In today’s rapidly evolving threat landscape, Managed Security Service Providers (MSSPs) play a critical role in delivering proactive, scalable, and real-time cybersecurity defense. The ability to swiftly detect, analyze, respond to, and recover from security incidents is essential in minimizing damage and maintaining trust with clients. Training Course on Incident Response for Managed Security Service Providers (MSSP) equips participants with advanced skills, frameworks, and real-world scenarios to manage cybersecurity incidents effectively and maintain compliance with global standards.

With increasing cyber threats such as ransomware, supply chain attacks, and insider threats, organizations demand responsive, resilient, and technically sound MSSPs. This course provides end-to-end training in threat intelligence, automated response, forensic analysis, communication protocols, and compliance practices tailored to MSSP environments. Participants will gain hands-on experience using top-tier tools, frameworks (like NIST and MITRE ATT&CK), and threat simulation techniques to create a mature, rapid-response incident management program.

Course Objectives

1. Understand incident response lifecycle tailored for MSSPs
2. Integrate SIEM and SOAR tools for real-time incident detection
3. Apply NIST 800-61 and MITRE ATT&CK frameworks in incident analysis
4. Conduct forensic investigations for malware and ransomware cases
5. Develop automated incident triage and prioritization workflows
6. Establish secure communication protocols during breach containment
7. Perform root cause analysis and post-incident reporting
8. Implement cyber threat intelligence (CTI) for proactive defense
9. Evaluate legal and compliance obligations like GDPR, HIPAA, and PCI-DSS
10. Build SLAs and client escalation matrices for incident handling
11. Create MSSP incident response playbooks and runbooks
12. Use AI and machine learning tools in incident prediction and response
13. Conduct tabletop exercises and red-blue team simulations

Target Audience

1. SOC Analysts
2. MSSP Incident Response Teams
3. Threat Intelligence Analysts
4. IT Security Managers
5. Managed Security Service Consultants
6. Cybersecurity Engineers
7. Compliance and Risk Officers
8. Network and Systems Administrators

Course Duration: 5 days

Course Modules

Module 1: Foundations of Incident Response for MSSPs

- Overview of MSSP Incident Response lifecycle
- Key roles and responsibilities in MSSP environments
- Understanding NIST 800-61 and MITRE ATT&CK alignment
- Incident types: phishing, malware, insider threats
- Key metrics for success and KPIs for IR teams
- **Case Study**: Coordinating MSSP response to a supply chain breach

Module 2: Threat Detection Tools & Techniques

- SIEM deployment and log correlation strategies
- Real-time threat detection using behavioral analytics
- Integrating SOAR for automated alerts
- Custom detection rules and threat hunting
- Role of AI in early threat identification
- **Case Study**: Detecting advanced persistent threats (APT) with SIEM+SOAR

Module 3: Incident Triage & Prioritization

- Triage models and risk categorization
- Workflow automation in ticketing systems
- Impact analysis for MSSP clients
- SLAs and urgency-based client communication
- Incident tracking and status updates
- **Case Study**: Handling a large-scale phishing campaign across multiple clients

Module 4: Containment, Eradication & Recovery

- Isolation protocols for endpoints and networks
- Malware removal and system clean-up
- Secure restoration and recovery
- Communication plans during containment
- Business continuity strategies for MSSPs
- **Case Study**: Ransomware containment and decryption strategy for healthcare client

Module 5: Digital Forensics & Evidence Handling

- Chain of custody in digital evidence
- Tools for file system, memory, and network forensics
- Analyzing malicious binaries and scripts
- Reporting and documentation best practices
- Legal considerations for evidence sharing
- **Case Study**: Forensic investigation of insider data exfiltration

Module 6: Threat Intelligence & Proactive Defense

- Sources of threat intelligence (open-source and commercial)
- Building IOCs and threat profiles
- Threat sharing and collaboration platforms (ISACs)
- Integrating CTI into IR plans
- Evaluating CTI effectiveness for MSSPs
- **Case Study**: Using CTI to prevent a zero-day exploit across MSSP clients

Module 7: Compliance, Legal & Regulatory Incident Handling

- GDPR, HIPAA, PCI-DSS: Incident response obligations
- Breach notification requirements and timelines
- Working with legal and public relations teams
- Audit and assessment preparation
- Documentation standards for compliance
- **Case Study**: HIPAA-compliant breach response for a healthcare MSSP client

Module 8: Simulation, Testing & Continuous Improvement

- Tabletop exercises and live simulations
- Red and blue team incident response scenarios
- Lessons learned: reviews and refinement cycles
- Updating MSSP playbooks and runbooks
- Building a culture of continuous improvement
- **Case Study**: Annual incident response drill for a multinational MSSP

Training Methodology

- Instructor-led interactive lectures

- Live demos and simulation labs
- Real-world case studies and use cases
- Red-blue team interactive exercises
- Group discussions, quizzes, and hands-on assignments

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

Start Date	End Date	Location	Price
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