Training Course on Threat Intelligence Integration into Incident Response Simulation

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 digital ecosystem, cybersecurity professionals must go beyond reactive measures and adopt proactive threat intelligence strategies to detect, prevent, and respond to cyber threats effectively. Training Course on Threat Intelligence Integration into Incident Response Simulation is designed to equip IT professionals, SOC teams, and cybersecurity leaders with the practical skills and intelligence-driven methodologies needed to combat advanced persistent threats, zero-day vulnerabilities, and nation-state attacks. This hands-on training ensures alignment with real-time threat data and best practices to elevate your organization’s cyber defense posture and resilience.

This course combines tactical incident response frameworks, real-world case studies, and automated threat intelligence feeds to help participants build robust and dynamic incident response programs. Using industry-leading tools and methodologies such as MITRE ATT&CK, STIX/TAXII, and threat intelligence platforms (TIPs), learners will master the art of intel-enriched response plans, indicator correlation, and threat-hunting operations to swiftly mitigate breaches and minimize damage. Gain a competitive edge with this SEO-optimized training crafted for today’s digital defenders.

Programme Curriculum

Training Course on Threat Intelligence Integration into Incident Response Simulation

Introduction

In today's rapidly evolving digital ecosystem, cybersecurity professionals must go beyond reactive measures and adopt proactive threat intelligence strategies to detect, prevent, and respond to cyber threats effectively. Training Course on Threat Intelligence Integration into Incident Response Simulation is designed to equip IT professionals, SOC teams, and cybersecurity leaders with the practical skills and intelligence-driven methodologies needed to combat advanced persistent threats, zero-day vulnerabilities, and nation-state attacks. This hands-on training ensures alignment with real-time threat data and best practices to elevate your organization’s cyber defense posture and resilience.

This course combines tactical incident response frameworks, real-world case studies, and automated threat intelligence feeds to help participants build robust and dynamic incident response programs. Using industry-leading tools and methodologies such as MITRE ATT&CK, STIX/TAXII, and threat intelligence platforms (TIPs), learners will master the art of intel-enriched response plans, indicator correlation, and threat-hunting operations to swiftly mitigate breaches and minimize damage. Gain a competitive edge with this SEO-optimized training crafted for today's digital defenders.

Course Objectives

1. Understand core concepts of threat intelligence lifecycle
2. Integrate threat intelligence into incident response plans
3. Use MITRE ATT&CK framework for mapping adversary behavior
4. Correlate IOCs (Indicators of Compromise) using TIPs
5. Automate threat feeds with STIX/TAXII protocols
6. Develop enriched detection and response workflows
7. Identify and analyze Advanced Persistent Threats (APTs)
8. Build actionable threat reports for C-level executives
9. Enhance real-time alerting and triage mechanisms
10. Leverage machine learning in threat detection
11. Conduct threat hunting using threat intelligence
12. Assess cyber threat landscapes and risk indicators
13. Apply intelligence-driven SOC operations

Target Audiences

1. Security Operations Center (SOC) Analysts
2. Cybersecurity Engineers
3. Incident Response Teams
4. Threat Intelligence Analysts
5. IT Security Managers
6. Penetration Testers / Ethical Hackers
7. Risk and Compliance Officers
8. Government and Critical Infrastructure Cyber Units

Course Duration: 5 days

Course Modules

Module 1: Fundamentals of Threat Intelligence

- Introduction to threat intelligence lifecycle
- Strategic vs tactical intelligence
- Types of threat data sources
- Key threat intelligence platforms (TIPs)
- Challenges in intelligence consumption
- **Case Study:** SolarWinds supply chain attack

Module 2: Threat Intelligence Frameworks

- Overview of MITRE ATT&CK and D3FEND
- Application of STIX, TAXII, and OpenIOC
- Mapping threat behaviors and techniques
- Aligning with industry frameworks (NIST, ISO 27035)
- Framework selection based on organization type
- **Case Study:** Mapping Conti ransomware via MITRE ATT&CK

Module 3: Integration into SOC and IR Workflow

- Building IR playbooks with threat intel
- Automating enrichment of alerts
- IOC matching and triage in SIEM/SOAR
- Prioritizing threats based on risk scoring
- Real-time collaboration across teams
- **Case Study:** Automating response using Splunk Phantom

Module 4: Advanced Threat Detection Techniques

- Correlation of threat feeds with internal logs
- Behavioral analytics and anomaly detection
- Leveraging machine learning for threat detection
- Real-time dashboarding for executive visibility
- Threat intelligence in endpoint detection
- **Case Study:** Detecting Lazarus Group lateral movement

Module 5: Threat Hunting Strategies

- Hunting hypothesis formulation using intel
- Building threat-hunting queries (YARA, Sigma)
- Using ELK stack and Splunk for hunt operations
- Pivoting from IOCs to TTPs
- Evidence collection and incident scoping
- **Case Study:** Proactive hunting in a retail data breach

Module 6: Intelligence-Driven Response Planning

- Designing response strategies using threat intel
- Resource allocation and playbook execution
- Enrichment of IR reports with intelligence
- Mapping response to business priorities
- Measuring effectiveness of intel integration
- **Case Study:** IR plan for ransomware in healthcare sector

Module 7: Legal, Ethical, and Compliance Issues

- Legal considerations in threat data sharing
- Privacy implications of external feeds
- Regulatory compliance (GDPR, HIPAA, NIS2)
- Cyber threat intelligence sharing alliances (ISACs)
- Balancing intel usage with ethical boundaries
- **Case Study:** Cross-border threat sharing compliance audit

Module 8: Threat Intelligence Maturity and Future Trends

- Building a threat intelligence maturity model
- Evolving from reactive to predictive defense
- Leveraging AI and predictive analytics
- Creating a roadmap for organizational adoption
- Emerging trends: Deepfakes, AI-enhanced malware
- **Case Study:** Predictive threat modeling in financial sector

Training Methodology

- Instructor-led interactive sessions

- Hands-on labs using industry tools (MISP, OpenCTI, ELK)
- Group discussions and scenario-based problem solving
- Real-world simulations of attack scenarios
- Assignments and quizzes to reinforce learning
- Final capstone project to demonstrate integration

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

Start Date	End Date	Location	Price
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