Training Course on Advanced Cyber Incident Triage and Scoping

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s ever-evolving threat landscape, organizations must equip cybersecurity professionals with cutting-edge skills in incident triage, forensic analysis, and threat detection. Training Course on Advanced Cyber Incident Triage and Scoping delivers high-impact, hands-on training that addresses sophisticated threat vectors, zero-day exploits, and persistent advanced attacks. Designed for security analysts, incident responders, and SOC teams, this course provides the essential tools to rapidly identify, triage, and scope cyber incidents before they escalate.

With a focus on real-world incident response, malware behavior analysis, and endpoint visibility, this course empowers cybersecurity teams to minimize downtime, preserve evidence integrity, and contain attacks efficiently. Participants will leverage powerful technologies like SIEMs, EDR tools, and network forensics platforms to make confident and time-sensitive triage decisions.

Programme Curriculum

Training Course on Advanced Cyber Incident Triage and Scoping

Introduction

In today’s ever-evolving threat landscape, organizations must equip cybersecurity professionals with cutting-edge skills in incident triage, forensic analysis, and threat detection. Training Course on Advanced Cyber Incident Triage and Scoping delivers high-impact, hands-on training that addresses sophisticated threat vectors, zero-day exploits, and persistent advanced attacks. Designed for security analysts, incident responders, and SOC teams, this course provides the essential tools to rapidly identify, triage, and scope cyber incidents before they escalate.

With a focus on real-world incident response, malware behavior analysis, and endpoint visibility, this course empowers cybersecurity teams to minimize downtime, preserve evidence integrity, and contain attacks efficiently. Participants will leverage powerful technologies like SIEMs, EDR tools, and network forensics platforms to make confident and time-sensitive triage decisions.

Course Objectives

1. Master cyber threat detection and event correlation using advanced SIEM tools.
2. Perform real-time log analysis and pattern recognition in compromised environments.
3. Understand attack lifecycle mapping with frameworks like MITRE ATT&CK.
4. Apply machine learning techniques in triage automation.
5. Develop playbooks for incident classification and severity assessment.
6. Conduct deep packet inspection (DPI) and memory dump analysis.
7. Build capabilities for malware sandboxing and reverse engineering fundamentals.
8. Use endpoint detection and response (EDR) platforms for root cause investigation.
9. Implement risk-based prioritization of security incidents.
10. Document incident findings using forensically sound methods.
11. Utilize cloud-native tools for multi-platform triage and scoping.
12. Improve coordination across CSIRT, SOC, and DevSecOps teams.
13. Simulate and assess sophisticated threat actor campaigns using red-blue team scenarios.

Target Audiences

1. Security Operations Center (SOC) Analysts
2. Incident Response Team Members
3. Cybersecurity Consultants
4. IT Security Managers
5. Threat Intelligence Analysts
6. Network Administrators
7. Penetration Testers and Ethical Hackers
8. Cloud Security Engineers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Advanced Incident Response

- Overview of modern cyber threats and threat actors
- Role of triage in minimizing breach impact
- Scoping vs. containment: key differences
- Introduction to incident response frameworks
- Key metrics and success indicators
- **Case Study:** Nation-state attack on a financial services company

Module 2: Triage Workflow and Playbook Design

- Standardized triage workflows for rapid response
- Playbook automation techniques using SOAR platforms
- Integrating threat intelligence into workflows
- Mapping triage playbooks to MITRE ATT&CK
- Playbook validation and version control
- **Case Study:** Response to ransomware in a healthcare organization

Module 3: Log and SIEM Analytics

- Log collection and normalization strategies
- Query optimization for high-fidelity threat detection
- Event correlation and anomaly detection
- Custom SIEM dashboards for triage

- Alert tuning and false positive reduction
- **Case Study:** Detecting insider threats through log analysis

Module 4: Endpoint Visibility and EDR Usage

- Leveraging EDR for behavioral analysis
- Timeline reconstruction from endpoint artifacts
- Root cause analysis from process trees
- EDR integration with triage tools
- Endpoint isolation and containment best practices
- **Case Study:** Zero-day malware detected via EDR telemetry

Module 5: Network Forensics and DPI

- Packet capture and traffic pattern analysis
- Using DPI for data exfiltration detection
- Identifying lateral movement through NetFlow
- Wireshark and Suricata in triage workflows
- Encryption-aware inspection strategies
- **Case Study:** Detecting C2 traffic in an APT breach

Module 6: Malware Triage and Static Analysis

- Static malware analysis techniques
- File hashing, strings, and signature-based detection
- Understanding PE headers and obfuscation
- Malware sandboxing for behavior profiling
- Tooling for quick triage: Cuckoo, Any.Run
- **Case Study:** Analyzing a polymorphic worm in an enterprise network

Module 7: Memory Forensics

- Memory acquisition best practices
- Identifying malicious processes and DLLs
- Analyzing volatile memory with Volatility
- Detecting credential dumping and process hollowing
- Correlating memory data with endpoint logs
- **Case Study:** RAM dump analysis of a compromised server

Module 8: Email and Phishing Incident Triage

- Identifying malicious payloads in email headers
- Link analysis and domain reputation scoring
- Correlating phishing attempts with user behavior
- Tools for phishing triage: VirusTotal, URLscan.io
- Email quarantine and reporting best practices
- **Case Study:** Business Email Compromise (BEC) on a CEO's mailbox

Module 9: Cloud Incident Triage (AWS/Azure)

- Cloud-native tools for incident triage
- Log analysis in CloudTrail and Azure Monitor
- Scoping IAM abuse and key leakage
- Multi-cloud threat detection strategies
- Cloud artifact preservation during response
- **Case Study:** Unauthorized access to cloud storage bucket

Module 10: Insider Threat and Behavioral Analytics

- Behavioral analytics and user baselines
- Insider threat indicators and triggers
- Integration of UEBA platforms in triage
- HR and legal collaboration during insider cases
- Remediation and containment procedures
- **Case Study:** Data theft by a departing employee

Module 11: Threat Hunting Integration

- Proactive triage in threat hunting cycles
- IOC and TTP-based hypothesis development
- Threat hunt automation via scripts and queries
- Pivoting through threat intelligence platforms
- Retrospective data analysis for scoping
- **Case Study:** Discovering dormant RAT through threat hunting

Module 12: Mobile Device and IoT Incident Scoping

- Mobile forensic acquisition methods
- Identifying rogue IoT device traffic
- MDM integration into triage pipelines
- IoT behavior profiling and anomalies
- Response strategies for mobile compromise
- **Case Study:** Compromised smart devices in a corporate LAN

Module 13: Chain of Custody and Documentation

- Evidence collection and preservation
- Legal admissibility of digital evidence
- Chain of custody forms and processes
- Secure evidence storage solutions
- Documentation for regulatory compliance
- **Case Study:** PCI-DSS incident documentation audit

Module 14: Communication and Stakeholder Coordination

- Internal and external stakeholder mapping
- Breach notification workflows
- Communicating with PR, legal, and executives
- Use of war rooms and chat ops
- Incident reporting templates and protocols
- **Case Study:** Coordinated comms during data leak incident

Module 15: Simulation, Drills, and Post-Incident Review

- Designing realistic triage simulations
- Tabletop and red team-blue team exercises
- Review processes and root cause documentation
- Updating triage protocols post-incident
- Continuous improvement metrics
- **Case Study:** Post-mortem of a simulated phishing campaign breach

Training Methodology

- Interactive instructor-led workshops

- Hands-on labs and technical simulations
- Real-world case study analysis
- Group exercises and threat-hunting challenges
- Live walkthroughs of tools (SIEMs, EDRs, forensics platforms)
- Post-training assessment and certification

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	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 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