Ransomware Investigation and Response Training Course

Professional Development Training Course Outline

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

Course Introduction

In an era where cyber threats are escalating in frequency and complexity, ransomware attacks have emerged as a critical threat vector affecting organizations of all sizes. From healthcare institutions and financial services to government and private corporations, no sector is immune. Training Course on Ransomware Investigation & Response equips cybersecurity professionals, IT teams, and digital forensics experts with the advanced tools, practical knowledge, and hands-on skills to detect, analyze, respond to, and prevent ransomware attacks in real-time.

This intensive training program dives deep into cyber forensics, incident response planning, malware analysis, and data recovery strategies, empowering professionals to act swiftly and intelligently in high-pressure scenarios. With case studies, real-world scenarios, and simulation exercises, this course aims to bridge the knowledge gap between basic cybersecurity awareness and expert ransomware response tactics.

Programme Curriculum

Ransomware Investigation and Response Training Course

Introduction

In an era where cyber threats are escalating in frequency and complexity, ransomware attacks have emerged as a critical threat vector affecting organizations of all sizes. From healthcare institutions and financial services to government and private corporations, no sector is immune. Ransomware Investigation and Response Training Course equips cybersecurity professionals, IT teams, and

digital forensics experts with the advanced tools, practical knowledge, and hands-on skills to detect, analyze, respond to, and prevent ransomware attacks in real-time.

This intensive training program dives deep into cyber forensics, incident response planning, malware analysis, and data recovery strategies, empowering professionals to act swiftly and intelligently in high-pressure scenarios. With case studies, real-world scenarios, and simulation exercises, this course aims to bridge the knowledge gap between basic cybersecurity awareness and expert ransomware response tactics.

Course Objectives

1. Understand the evolution and ecosystem of modern ransomware threats.
2. Identify early indicators of ransomware infiltration using forensic tools.
3. Master threat intelligence analysis to track and profile attack vectors.
4. Develop strategic incident response protocols for ransomware.
5. Perform effective ransomware containment and mitigation.
6. Apply advanced malware reverse engineering techniques.
7. Conduct cybercrime investigations using digital evidence.
8. Learn effective communication and legal coordination during ransomware crises.
9. Implement secure backup and data recovery practices.
10. Evaluate risk management frameworks tailored for ransomware resilience.
11. Strengthen endpoint protection and network monitoring systems.
12. Examine post-breach analysis and reporting compliance standards.
13. Explore emerging trends in ransomware-as-a-service (RaaS) and cyber extortion.

Target Audience

1. Cybersecurity Analysts
2. IT Security Managers
3. Incident Response Teams
4. Penetration Testers
5. Law Enforcement Officers (Cybercrime Units)
6. Threat Intelligence Analysts
7. Security Operations Center (SOC) Staff
8. Cybersecurity Students & Educators

Course Duration: 10 days

Course Modules

Module 1: Introduction to Ransomware

- History and evolution of ransomware
- Ransomware attack lifecycle
- Common delivery vectors
- Impact on businesses and infrastructure

- Overview of major ransomware families (e.g., Ryuk, LockBit, Conti)
- **Case Study:** Analysis of WannaCry global outbreak

Module 2: Ransomware Variants and Threat Actor Tactics

- Understanding ransomware families and strains
- Ransomware-as-a-Service (RaaS) explained
- Behavioral analysis of threat actors
- Use of obfuscation and encryption
- Mapping MITRE ATT&CK techniques to ransomware
- **Case Study:** REvil attack on JBS Foods

Module 3: Initial Compromise and Infiltration Techniques

- Phishing and social engineering
- Exploiting remote desktop protocols (RDP)
- Credential stuffing and brute force
- Supply chain attacks
- Exploit kits and dropper malware
- **Case Study:** Kaseya VSA ransomware breach

Module 4: Threat Detection and Monitoring Tools

- SIEM and EDR technologies
- IOC (Indicators of Compromise) identification
- Real-time monitoring practices
- Threat hunting strategies
- Anomaly-based detection
- **Case Study:** Using Splunk to identify early-stage ransomware

Module 5: Incident Response Planning

- Building an incident response (IR) team
- Defining IR policies and procedures
- Escalation matrix and notification workflows
- Business continuity planning
- Coordination with external agencies (FBI, CISA)
- **Case Study:** Maersk ransomware recovery response

Module 6: Ransomware Containment Techniques

- Network segmentation
- Host isolation practices
- Firewall reconfiguration
- Killing malicious processes
- Securing remote access tools
- **Case Study:** City of Atlanta containment strategy

Module 7: Digital Forensics for Ransomware Attacks

- Memory and disk analysis
- Timeline reconstruction
- File artifact recovery
- Analyzing registry and system logs
- Preserving chain of custody
- **Case Study:** Forensic investigation of Colonial Pipeline attack

Module 8: Malware Reverse Engineering

- Introduction to reverse engineering tools (IDA Pro, Ghidra)
- Static vs. dynamic analysis
- Decryption techniques
- Debugging and unpacking malware
- Sandbox testing environments
- **Case Study:** Unpacking the LockBit 3.0 ransomware sample

Module 9: Backup and Data Recovery Strategies

- Offline vs. cloud backups
- Air-gapped backup infrastructure
- Restoring infected systems
- Immutable storage options
- Data integrity validation
- **Case Study:** Rapid recovery from DarkSide ransomware using backups

Module 10: Legal and Regulatory Implications

- GDPR, HIPAA, and data breach laws
- Mandatory breach notifications
- Working with law enforcement
- Ransom payment and ethical considerations
- Digital evidence submission and reporting
- **Case Study:** Legal response to the Garmin ransomware incident

Module 11: Communication During a Ransomware Crisis

- Internal and external communications planning
- Crafting press releases and disclosures
- Communicating with attackers (if necessary)
- Legal review of public statements
- Managing stakeholder expectations
- **Case Study:** Crisis communication during the Acer ransomware attack

Module 12: Threat Intelligence and Attribution

- Gathering threat intel from open and closed sources

- Profiling threat groups (APT28, FIN11)
- TTP (Tactics, Techniques, Procedures) mapping
- Collaborating with ISACs and intelligence sharing networks
- OSINT tools for investigation
- **Case Study:** Attribution of NotPetya attack to state actors

Module 13: Dark Web and Cryptocurrency Tracing

- Identifying ransom payment wallets
- Monitoring Tor and underground forums
- Cryptocurrency transaction tracing
- Working with blockchain analytics platforms
- Collaborating with FinCEN and crypto firms
- **Case Study:** Tracing Bitcoin ransom from Colonial Pipeline

Module 14: Post-Incident Analysis & Reporting

- Conducting post-mortem reviews
- Root cause analysis
- Lessons learned documentation
- Compliance reporting standards
- Updating policies and procedures
- **Case Study:** NHS ransomware recovery and lessons learned

Module 15: Simulation & Tabletop Exercises

- Live attack simulations
- Blue team vs. red team exercises
- IR playbook testing
- Decision-making under pressure
- Cross-departmental coordination drills
- **Case Study:** Full-scale simulated ransomware attack on a healthcare system

Training Methodology

- Instructor-led online and on-site training
- Real-world case study evaluations
- Hands-on labs and sandbox environments
- Role-play and group simulations
- Downloadable tools, checklists, and templates

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
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