Training Course on Managing Ransomware Incidents: A Comprehensive Guide

Professional Development Training Course Outline

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

Course Introduction

Ransomware attacks are one of the most pressing cybersecurity threats faced by modern organizations. As cybercriminals grow more sophisticated, businesses, governments, and individuals must strengthen their cyber defense mechanisms and incident response capabilities. Training Course on Managing Ransomware Incidents: A Comprehensive Guide is designed to empower IT professionals, CISOs, and emergency response teams with the knowledge and practical skills necessary to identify, contain, recover, and mitigate ransomware threats in real-time.

Leveraging real-world case studies, threat intelligence, and best practices in cybersecurity operations, this course provides step-by-step guidance on managing ransomware attacks before, during, and after incidents. By incorporating trending cybersecurity frameworks, incident playbooks, digital forensics, and business continuity planning, this course ensures participants leave with a ransomware response plan that is actionable, scalable, and aligned with today's zero-trust architecture standards.

Programme Curriculum

Training Course on Managing Ransomware Incidents: A Comprehensive Guide

Introduction

Ransomware attacks are one of the most pressing cybersecurity threats faced by modern organizations. As cybercriminals grow more sophisticated, businesses, governments, and individuals must strengthen their cyber defense mechanisms and incident response capabilities. Training Course on Managing Ransomware Incidents: A Comprehensive Guide is designed to empower IT professionals, CISOs, and emergency response teams with the knowledge and practical skills necessary to identify, contain, recover, and mitigate ransomware threats in real-time.

Leveraging real-world case studies, threat intelligence, and best practices in cybersecurity operations, this course provides step-by-step guidance on managing ransomware attacks before, during, and after incidents. By incorporating trending

cybersecurity frameworks, incident playbooks, digital forensics, and business continuity planning, this course ensures participants leave with a ransomware response plan that is actionable, scalable, and aligned with today's zero-trust architecture standards.

Course Objectives

1. Understand the evolution of ransomware threats in the digital era
2. Identify signs of ransomware infiltration and lateral movement
3. Implement proactive threat hunting and detection strategies
4. Develop and execute a ransomware incident response plan
5. Conduct forensic analysis of compromised systems
6. Utilize endpoint detection and response (EDR) tools effectively
7. Integrate threat intelligence feeds into security operations
8. Strengthen data backup and recovery protocols
9. Assess and mitigate ransomware attack vectors
10. Simulate ransomware attacks for incident response drills
11. Build cross-functional cybersecurity crisis communication plans
12. Evaluate post-incident reporting and legal compliance
13. Design and implement a zero-trust ransomware defense strategy

Target Audiences

1. IT Security Managers
2. Chief Information Security Officers (CISOs)
3. System Administrators
4. Incident Response Teams
5. SOC Analysts
6. Government Cybersecurity Officials
7. Disaster Recovery Planners
8. Compliance & Risk Officers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Ransomware Threat Landscape

- Types of ransomware (crypto, locker, RaaS)
- Trends and evolution in ransomware attacks
- Impact on businesses and national infrastructure
- Key threat actors and their tactics
- Mapping ransomware to MITRE ATT&CK
- **Case Study: WannaCry Attack on the NHS (2017)**

Module 2: Early Detection and Threat Identification

- Indicators of compromise (IOCs)
- Deploying honeypots and traps
- Real-time alerting with SIEM tools
- Network traffic analysis
- Email phishing detection techniques
- **Case Study: Ryuk Ransomware in Municipal Networks**

Module 3: Containment and Isolation Techniques

- Isolating infected endpoints

- Network segmentation practices
- Blocking malicious IPs and domains
- Disabling affected services
- Communication protocols during an outbreak
- **Case Study: Maersk Containment Strategy during NotPetya**

Module 4: Digital Forensics & Root Cause Analysis

- Capturing volatile and non-volatile data
- Analyzing ransomware payloads
- Identifying patient zero
- Reverse engineering malware
- Using forensic tools (FTK, Autopsy, Volatility)
- **Case Study: Colonial Pipeline Forensics Investigation**

Module 5: Recovery and Restoration Planning

- Disaster recovery (DR) best practices
- Validating clean backups
- Secure system rebuilds
- Testing recovery timelines
- Post-recovery patch management
- **Case Study: Garmin's RansomExx Recovery Journey**

Module 6: Communication and Crisis Management

- Internal communication protocols
- External stakeholder management
- Public relations and reputation recovery
- Legal and regulatory notifications
- Drafting media statements and FAQs
- **Case Study: Kaseya's Public Communication Strategy**

Module 7: Legal, Ethical & Compliance Considerations

- Understanding data breach laws
- GDPR, HIPAA, and regional requirements
- Cyber insurance and liability concerns
- Ransomware negotiation ethics
- Collaboration with law enforcement
- **Case Study: JBS Foods Ransomware Payment Compliance**

Module 8: Developing a Future-Proof Response Framework

- Creating a ransomware playbook
- Regular tabletop exercises
- Building a zero-trust network
- Employee cybersecurity awareness training
- Vendor and supply chain security assessments
- **Case Study: IBM's Proactive Ransomware Readiness Model**

Training Methodology

- Interactive instructor-led sessions
- Hands-on labs and simulations
- Downloadable response plan templates

- Real-life ransomware case study breakdowns
- Access to ransomware threat intel feeds
- Group discussions and tabletop exercises

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