Ransomware Training Course

Professional Development Training Course Outline

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

Course Introduction

In today's digital era, ransomware attacks are among the most disruptive and financially damaging cyber threats to governments, corporations, healthcare institutions, and small businesses. With evolving malware variants, phishing tactics, and sophisticated encryption techniques, cybercriminals are extorting millions of dollars globally. Ransomware Training Course is designed to equip IT professionals, cybersecurity teams, and system administrators with the advanced knowledge and hands-on skills required to prevent, detect, respond to, and recover from ransomware incidents effectively.

This comprehensive training covers ransomware detection tools, threat intelligence integration, incident response, and recovery strategies. Learners will explore real-world case studies, master critical risk mitigation techniques, and learn how to implement robust endpoint protection systems. The course is enriched with SEO-driven and trending cyber security insights, empowering learners to build ransomware-resilient digital environments in both private and public sectors.

Programme Curriculum

Ransomware Training Course

Introduction

In today's digital era, ransomware attacks are among the most disruptive and financially damaging cyber threats to governments, corporations, healthcare institutions, and small businesses. With evolving malware variants, phishing tactics, and sophisticated encryption techniques, cybercriminals are extorting millions of dollars globally. Ransomware Training Course is designed to equip IT professionals, cybersecurity teams, and system administrators with the advanced knowledge and hands-on skills required to prevent, detect, respond to, and recover from ransomware incidents effectively.

This comprehensive training covers ransomware detection tools, threat intelligence integration, incident response, and recovery strategies. Learners will explore real-world case studies, master critical risk mitigation techniques, and learn how to implement robust endpoint protection systems. The course is enriched with SEO-driven and trending cyber security insights, empowering learners to build ransomware-resilient digital environments in both private and public sectors.

Course Objectives

1. Understand the evolution and classification of ransomware threats.
2. Analyze ransomware attack vectors and exploitation mechanisms.
3. Identify early signs and symptoms of ransomware infiltration.
4. Deploy proactive ransomware prevention strategies using AI and machine learning.
5. Implement endpoint protection and advanced firewall configurations.
6. Develop real-time incident response and threat containment plans.
7. Evaluate ransomware encryption tactics and decryption methods.
8. Utilize forensic investigation tools for post-attack analysis.
9. Apply risk assessment models for enterprise ransomware protection.
10. Learn how to conduct a ransomware tabletop exercise for readiness.
11. Design a ransomware backup and disaster recovery plan.
12. Examine the legal and regulatory frameworks on ransomware compliance.
13. Build a security culture to reduce human error and phishing exposure.

Target Audiences

1. IT Security Professionals
2. System and Network Administrators
3. Cybersecurity Analysts
4. Chief Information Security Officers (CISOs)
5. Government Cyber Defense Units
6. Law Enforcement Cybercrime Units
7. Compliance Officers and Auditors
8. University Students in Cybersecurity Tracks

Course Duration: 5 days

Course Modules

Module 1: Introduction to Ransomware

- History and rise of ransomware
- Common types: crypto, locker, doxware, scareware
- Ransomware-as-a-Service (RaaS) model
- Lifecycle of a ransomware attack
- Impact on businesses and infrastructure
- **Case Study:** WannaCry attack on the NHS (2017)

Module 2: Attack Vectors and Exploitation Techniques

- Phishing emails and social engineering
- Malicious downloads and infected ads
- Exploiting RDP and unpatched software
- Zero-day vulnerabilities
- Credential harvesting techniques
- **Case Study:** Ryuk ransomware in the healthcare sector

Module 3: Ransomware Prevention Strategies

- Endpoint detection and response (EDR) solutions
- Implementing AI-based threat detection
- Multi-factor authentication (MFA)
- Patch and update management

- Creating secure email gateways
- **Case Study:** City of Atlanta attack and prevention gaps

Module 4: Incident Detection and Response

- Building an incident response plan
- Indicators of compromise (IOCs)
- Threat hunting techniques
- Isolating infected systems
- Communication protocols during attack
- **Case Study:** Colonial Pipeline ransomware response (2021)

Module 5: Data Protection and Backup Systems

- Ransomware-resilient backup strategies
- Cloud-based storage and security
- Offline and immutable backups
- Continuous data protection (CDP)
- Verifying backup integrity
- **Case Study:** Norsk Hydro's response using backups

Module 6: Legal, Ethical, and Compliance Considerations

- GDPR, HIPAA, and other compliance standards
- Legal implications of paying ransom
- Reporting obligations and timelines
- Cyber insurance and liability
- Coordinating with law enforcement
- **Case Study:** Garmin ransomware payment controversy

Module 7: Recovery and Post-Incident Analysis

- System recovery without paying ransom
- Eradication and restoration procedures
- Root cause analysis
- Documentation and audit trail
- Lessons learned review
- **Case Study:** Baltimore city government's costly recovery

Module 8: Building Organizational Cyber Resilience

- Employee cybersecurity awareness training
- Implementing zero-trust architecture
- Continuous threat intelligence sharing
- Security culture and phishing simulations
- Integrating cybersecurity into business strategy
- **Case Study:** How Maersk bounced back from NotPetya

Training Methodology

- Interactive instructor-led sessions
- Hands-on lab simulations and ransomware drills
- Real-life case study discussions
- Group incident response exercises
- Access to premium ransomware simulation tools
- Final 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	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
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