Training Course on Ransomware Negotiation and Decryption Tools

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 cybersecurity landscape, ransomware attacks have evolved into one of the most dangerous and costly threats facing organizations across industries. Cybercriminals are deploying increasingly sophisticated variants, encrypting critical systems, and demanding high-stakes payments. Training Course on Ransomware Negotiation and Decryption Tools equips cybersecurity professionals, IT administrators, and risk managers with the tactical and strategic capabilities to handle ransomware incidents efficiently and legally. By focusing on real-world decryption tools, forensic analysis, and negotiation frameworks, this course empowers learners to mitigate damage and support organizational recovery.

Participants will gain hands-on exposure to ransomware negotiation simulations, data recovery protocols, and tools like CISA’s decryptors, No More Ransom, and MITRE ATT&CK mappings. This comprehensive course is designed to enhance incident response strategies, strengthen cyber-resilience, and prepare professionals for decision-making under pressure. With an emphasis on legal and ethical considerations, the training also offers guidelines for engaging third-party negotiators and law enforcement agencies. Whether you're protecting enterprise infrastructure or government assets, mastering these tools and techniques is now mission-critical.

Programme Curriculum

Training Course on Ransomware Negotiation and Decryption Tools

Introduction

In today's cybersecurity landscape, ransomware attacks have evolved into one of the most dangerous and costly threats facing organizations across industries. Cybercriminals are deploying increasingly sophisticated variants, encrypting critical systems, and demanding high-stakes payments. Training Course on Ransomware Negotiation and Decryption Tools equips cybersecurity professionals, IT administrators, and risk managers with the tactical and strategic capabilities to handle ransomware incidents efficiently and legally. By focusing on real-world decryption tools, forensic analysis, and negotiation

frameworks, this course empowers learners to mitigate damage and support organizational recovery.

Participants will gain hands-on exposure to ransomware negotiation simulations, data recovery protocols, and tools like CISA’s decryptors, No More Ransom, and MITRE ATT&CK mappings. This comprehensive course is designed to enhance incident response strategies, strengthen cyber-resilience, and prepare professionals for decision-making under pressure. With an emphasis on legal and ethical considerations, the training also offers guidelines for engaging third-party negotiators and law enforcement agencies. Whether you're protecting enterprise infrastructure or government assets, mastering these tools and techniques is now mission-critical.

Course Objectives

1. Understand ransomware attack vectors and encryption mechanisms.
2. Identify common ransomware strains (e.g., LockBit, BlackCat, Ryuk).
3. Analyze ransomware kill chains using real-world forensic evidence.
4. Learn negotiation strategies and communication protocols with attackers.
5. Evaluate legal and ethical frameworks surrounding ransomware payment.
6. Deploy open-source and commercial ransomware decryptors.
7. Integrate threat intelligence and IOCs for early detection and mitigation.
8. Execute incident response plans and ransomware playbooks.
9. Utilize memory and disk forensics to trace ransomware activity.
10. Perform impact assessment and business continuity planning.
11. Collaborate with law enforcement and cybersecurity authorities.
12. Leverage AI-driven analytics to predict ransomware threats.
13. Conduct red team exercises focused on ransomware scenarios.

Target Audiences

1. Cybersecurity Analysts
2. Incident Response Teams
3. Chief Information Security Officers (CISOs)
4. IT Risk Managers
5. Law Enforcement Cyber Units
6. Penetration Testers & Red Teams
7. Government Cybersecurity Staff
8. Managed Security Services Providers (MSSPs)

Course Duration: 5 days

Course Modules

Module 1: Understanding Ransomware Evolution

- History and rise of ransomware threats
- Analysis of ransomware variants
- Encryption methodologies and payloads
- Real-world attack scenarios
- Global impact and cost statistics
- **Case Study:** WannaCry and its global disruption

Module 2: Ransomware Attack Lifecycle

- Initial access and lateral movement
- Command and control infrastructure
- Data exfiltration and double extortion
- Encryption and system lockdown

- Detection gaps and early indicators
- **Case Study:** Ryuk's stealthy operations in healthcare

Module 3: Legal and Ethical Negotiation Practices

- Regulatory obligations and compliance
- Legal consequences of paying ransoms
- Negotiation frameworks and policies
- Role of insurers and legal counsel
- Third-party ransomware negotiators
- **Case Study:** Colonial Pipeline and FBI's involvement

Module 4: Ransomware Decryption Tools

- CISA and No More Ransom decryptors
- Evaluating decryptor effectiveness
- Matching decryptors to ransomware strains
- Live testing in sandboxed environments
- Integration with digital forensics tools
- **Case Study:** Decryption success with REvil variant

Module 5: Forensic Analysis & Data Recovery

- Memory and disk image collection
- Chain of custody and evidence handling
- Recovering partially encrypted files
- Volatility and Autopsy use cases
- Timeline reconstruction techniques
- **Case Study:** Forensic investigation of LockBit

Module 6: Threat Intelligence & Prevention

- Threat intelligence sources and feeds
- IOC identification and correlation
- Threat hunting and behavioral analytics
- Automation using SIEM/SOAR platforms
- Reducing attack surfaces via patching
- **Case Study:** Threat hunting of Black Basta activity

Module 7: Business Continuity & Response

- Business impact assessment
- Crisis communication and stakeholder roles
- Backup strategy validation
- Failover planning and system restoration
- Tabletop and red team exercises
- **Case Study:** Ransomware tabletop simulation for finance sector

Module 8: AI & Future of Ransomware Defense

- Machine learning in anomaly detection
- Predictive ransomware threat modeling
- Deepfake and AI-enhanced social engineering
- Proactive threat simulations using AI
- Ethical AI in cyber defense
- **Case Study:** AI-assisted defense against Phobos ransomware

Training Methodology

- Instructor-led virtual and in-person workshops
- Hands-on labs using ransomware simulators and decryptors
- Interactive case study discussions
- Simulation-based assessments and red teaming exercises
- Guided forensic labs and negotiation role-play exercises
- Peer-to-peer collaboration in breakout sessions

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com