Ransomware Negotiation and Post-Attack Forensics 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 today's cyber-driven landscape, ransomware attacks have become one of the most pressing threats to organizations across the globe. These high-stakes intrusions disrupt critical infrastructure, compromise sensitive data, and demand hefty payouts. The ability to respond rapidly, negotiate effectively, and conduct post-attack forensics is no longer optional—it is vital. Training Course on Ransomware Negotiation & Post-Attack Forensics equips cybersecurity professionals, IT leaders, digital forensics experts, and law enforcement with the knowledge and tools required to manage ransomware incidents strategically and minimize operational and reputational damage.

Leveraging real-world case studies, cutting-edge negotiation strategies, and advanced forensic techniques, this comprehensive training delivers SEO-friendly, hands-on learning tailored for threat response and recovery. Participants will gain expertise in ransomware incident lifecycle management, digital evidence handling, attacker profiling, negotiation playbooks, and breach remediation. In a constantly evolving threat landscape, this training positions participants at the frontline of ransomware defense and recovery.

Programme Curriculum

Ransomware Negotiation and Post-Attack Forensics Training Course

Introduction

In today's cyber-driven landscape, ransomware attacks have become one of the most pressing threats to organizations across the globe. These high-stakes intrusions disrupt critical infrastructure, compromise sensitive data, and demand hefty payouts. The ability to respond rapidly, negotiate effectively, and conduct post-attack forensics is no longer optional—it is vital. Ransomware Negotiation and Post-Attack Forensics Training Course equips cybersecurity professionals, IT leaders, digital forensics experts, and law enforcement with the knowledge and tools required to manage ransomware incidents strategically and minimize operational and reputational damage.

Leveraging real-world case studies, cutting-edge negotiation strategies, and advanced forensic techniques, this comprehensive training delivers SEO-friendly, hands-on learning tailored for threat response and recovery. Participants will gain expertise in ransomware incident lifecycle management, digital evidence handling, attacker profiling, negotiation playbooks, and breach remediation. In a constantly evolving threat landscape, this training positions participants at the frontline of ransomware defense and recovery.

Course Objectives

1. Understand the full ransomware attack lifecycle and evolving threat vectors.
2. Analyze ransomware threat actors and their negotiation tactics.
3. Build and implement effective ransomware response playbooks.
4. Learn best practices for data backup, system recovery, and decryption.
5. Master digital forensic techniques for post-attack investigation.
6. Understand legal and compliance obligations during and after ransomware events.
7. Engage in real-time ransomware negotiation simulations.
8. Evaluate ransom payment risks and cryptocurrency tracking.
9. Implement secure incident communication protocols.
10. Conduct internal threat assessments and vulnerability audits.
11. Apply threat intelligence for ransomware prevention.
12. Utilize blockchain analysis tools in tracing ransom payments.
13. Design an enterprise ransomware resilience and mitigation strategy.

Target Audience

1. Cybersecurity Analysts
2. Incident Response Teams
3. Law Enforcement Cyber Units
4. IT Security Managers
5. Risk and Compliance Officers
6. Digital Forensic Investigators
7. Chief Information Security Officers (CISOs)
8. Emergency Management & Crisis Response Professionals

Course Duration: 10 days

Course Modules

Module 1: Introduction to Ransomware Threat Landscape

- History and evolution of ransomware
- Common attack vectors and payload delivery
- Categories and types of ransomware (locker, crypto, double extortion)
- Notorious ransomware groups and APTs
- Industry-specific attack trends
- *Case Study: WannaCry Global Outbreak*

Module 2: Incident Detection and Early Response

- Identifying ransomware indicators of compromise (IOCs)
- Internal alert systems and detection tools
- Responding to the first signs of encryption
- Isolating infected systems
- Engaging cyber incident response teams
- *Case Study: Colonial Pipeline Early Containment Tactics*

Module 3: Ransomware Negotiation Fundamentals

- Understanding attacker psychology and motivation
- Assessing demands and communication strategies
- Legal implications of ransom negotiations
- Role of intermediaries and negotiators
- Secure negotiation communication tools
- *Case Study: Kaseya VSA Negotiation and Recovery*

Module 4: Forensic Analysis Post-Attack

- Data recovery and chain of custody
- Memory and disk imaging techniques
- Analyzing ransomware binaries and logs
- Tracing lateral movement and privilege escalation
- Identifying patient zero and breach points
- *Case Study: Norsk Hydro Deep Forensic Dive*

Module 5: Cryptocurrency and Ransom Tracking

- How ransoms are paid via cryptocurrencies
- Wallet tracing and blockchain analysis
- Use of mixers and laundering techniques
- Tools for crypto forensics
- Reporting and collaborating with exchanges
- *Case Study: Bitcoin Recovery from NetWalker Gang*

Module 6: Communication, PR & Legal Strategy

- Drafting breach notification messages
- Engaging stakeholders and regulators
- Managing internal communications securely
- Avoiding reputational damage
- Understanding GDPR, HIPAA, and CCPA compliance
- *Case Study: Travelex Crisis Communication Management*

Module 7: Data Backup & Recovery Protocols

- Backup segmentation and air-gap techniques
- Immutable backups and snapshot recovery
- Building ransomware-proof architecture
- Testing and validating disaster recovery plans
- Role of cloud platforms in backup restoration
- *Case Study: MSP Recovery After REvil Attack*

Module 8: Advanced Threat Actor Profiling

- Threat intelligence sources and OSINT
- Behavioral analysis of ransomware gangs
- Tracking evolution in malware code
- Language, infrastructure, and geopolitical indicators
- Mapping attacker TTPs with MITRE ATT&CK
- *Case Study: DarkSide Group Behavioral Mapping*

Module 9: Negotiation Playbook Development

- Creating templates and SOPs for crisis scenarios

- Internal and external coordination checklists
- Legal review of playbook strategies
- Simulation and tabletop exercises
- Real-time decision trees and escalation paths
- *Case Study: Simulated CryptoLocker Negotiation Tabletop*

Module 10: Legal & Ethical Considerations

- Ethics of ransom payment and moral dilemmas
- National laws on negotiating with cybercriminals
- Insurance coverage and limitations
- Cross-border jurisdiction and data handling
- Insider threats and liability issues
- *Case Study: Legal Fallout from Garmin Ransomware Payout*

Module 11: Resilience and Futureproofing Strategy

- Building cyber-resilient networks
- Employee awareness and phishing prevention
- Continuous system monitoring and patching
- Red-teaming and penetration testing
- Vendor and supply chain assessments
- *Case Study: Resilience Plan of Singapore Health System*

Module 12: Post-Breach Remediation & Recovery

- System hardening post-attack
- Credential resets and access control
- Decryptor deployment and testing
- Post-mortem reporting and audit trails
- Lessons learned and continuous improvement
- *Case Study: University of Utah Incident Report*

Module 13: Insider Threats and Internal Risks

- Understanding unintentional vs. malicious insiders
- Monitoring tools for internal threats
- Awareness campaigns and training
- Privileged access management
- Behavioral red flags and mitigation
- *Case Study: Healthcare Insider Incident Enabling Ransomware*

Module 14: Insurance and Financial Recovery

- Cyber insurance coverage analysis
- Claim filing process and documentation
- Interaction with insurers and adjusters
- Valuation of damage and data loss
- Financial impact and cost modeling
- *Case Study: Insurance Response Post-Acer Hack*

Module 15: Global Response Coordination

- Working with international law enforcement (INTERPOL, Europol)
- Threat sharing through ISACs and CERTs
- Global frameworks and cooperative tools

- Language and time zone coordination
- Engaging vendors and third-party specialists
- *Case Study: Joint Global Takedown of Emotet Infrastructure*

Training Methodology

- Instructor-led virtual and in-person training
- Real-world case-based learning
- Hands-on labs and simulations
- Interactive negotiation roleplays
- Post-training assessments and certifications
- Group discussions and Q&A with industry experts

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	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

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

Register Online Now

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