Training: Centri
Ransomware: Negotiation & Threat Intelligence

CENTRI

TRAINING GOALS:

This course is designed to equip professionals with the knowledge and skills to effectively handle ransomware incidents. From understanding the foundations of ransomware to engaging in negotiation simulations, participants will gain practical insights into managing cyber extortion scenarios. We are proud to have partnered with Validin and Crystal Intelligence to provide a real-world insight into threat intelligence.

Why choose Ransomware: Negotiation & Threat Intelligence?

Designed to prepare professionals to effectively handle ransomware incidents. From understanding the foundations of ransomware to engaging in negotiation simulations, participants will gain practical insights into managing cyber extortion scenarios. They'll also use real-world commercial tools, such as Validin for attack surface management and Crystal Intelligence for blockchain forensics.

- Ransomware Foundations
- Response Preparation
- Ransomware Threat Intelligence
- Ransomware Considerations
- Negotiation Tactics During Contact
- Ransomware Negotiation Simulation

Who is the course for?

Ideal training for CTI Analysts, Cyber Intelligence Professionals, Criminal Actor Investigators, FinCrime Investigators, Threat Hunters, Cyber Incident Responders, Digital Forensics Analysts, and LEA Professionals.

CONSPECT:

- Ransomware Foundations
  - Learn the basics of ransomware, its deployment, the negotiator's role, the ransomware ecosystem (RaaS, IAB), and communication processes.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Ransomware 101
        - Ransomware Evolution and History
        - Crypto Ransomware Ecosystem
        - Ransomware Communications 101
        - Additional Topics
- Response Preparation
    - Explore decision-making processes, internal coordination, impact and cost assessments, and general project management in preparing for ransomware incidents.
        - Immediate Issues
        - Impact and Costs
        - Decision Making
        - Internal Coordination
- Ransomware Threat Intelligence
    - Understand the key concepts and steps in conducting both proactive and reactive cyber threat intelligence — from building threat briefings and tracking modern adversarial groups to analysing chat leaks from prolific ransomware syndicates.
        - Section Introduction
        - Digital Footprinting
        - Threat Briefings
        - HUMINT
        - Know Your Adversary
        - Proactive CTI
        - Cryptocurrency Concepts
        - Crypto Wallet Exercises
        - Crypto Wallet Exercise | WalkThroughs
- Ransomware Considerations
    - Gain insight into key considerations when deciding whether to engage with ransomware actors, including legal and compliance issues, and how to build a structured response plan.
        - Negotiation Strategy Considerations
        - Ransomware Payments
        - Before Initial Contact
- Negotiation Tactics During Contact
    - Understand negotiation strategies in ransomware cases, including threat actor methods, psychological tactics, and counter-offer strategies, with case studies.
        - Domain Introduction
        - Threat Actor Negotiation Tactics
        - Negotiator's Psychological Tactics and Case Studies

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Counter-Offer Tactics
- Outcome Phase

- Ransomware Negotiation Simulation
  - Apply your knowledge from previous sections in a hands-on ransomware negotiation exercise. Good luck!
    - Accessing the Capstone

- Course Completion
  - Concluding notes, and information on how to claim your PDF certificate of completion and Credly badge.
    - Course Completion

REQUIREMENTS:

There are no entry requirements for the course. This course is designed for incident responders, SOC managers, internal managers, and ransomware negotiators. It covers both foundational and advanced topics, making it accessible to a range of experience levels.

Difficulty level

CERTIFICATE:

Successful participants will receive a certificate of completion and Credly badge.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007