FOR528: **Ransomware and Cyber Extortion™**

4 Day Program	24 CPEs	Laptop Required

You Will Be Able To

- Investigate ransomware and cyber extortion attacks using real-world cases and forensic artifacts.
- Identify the blind spots most IR playbooks miss: persistence, exfiltration, and extortion without encryption.
- Distinguish between ransomware encryption events and extortion-only attacks to adapt your response.
- Decode attacker tools and scripts in hands-on labs—including obfuscated PowerShell and malware triage.
- Practice the full ransomware/extortion lifecycle, from intrusion to organizational recovery, in labs and a full-day CTF.
- Strengthen organizational readiness by connecting technical findings to leadership communication, legal needs, and recovery coordination.
- Recognize available telemetry depending on the maturity of your organization or that of your clients. The course includes two different scenarios: One replicating within a default Windows environment with little visibility, and one replicating a well-tooled environment that provides greater visibility.
- Leave with the confidence to handle ransomware and extortion incidents under pressure, using the same methods frontline responders rely on.

Business Takeaways

- Close the blind spots general IR training leaves behind—from hidden persistence to data exfiltration and extortion.
- Recognize and investigate ransomware activity fast, via review of the same tools adversaries deploy in the wild.
- Understand the full ransomware and extortion lifecycle to build a complete, actionable response plan.
- Strengthen organizational readiness by practicing both technical containment and business-critical coordination during recovery.
- Validate recovery with confidence—ensuring persistence is removed, backups are trustworthy, and systems are safe to restore.
- Differentiate ransomware-related activity from other intrusions to focus efforts on the highest-impact threats.
- Identify what data was accessed or stolen to accurately assess business impact and support regulatory or legal response.

FOR528: Ransomware and Cyber Extortion™ isn't just hands-on—it's frontline. Built entirely from real ransomware and extortion cases, this course prepares responders to face the attacks organizations fear most. You won't just study ransomware in theory—you'll investigate it the way it actually happens, using authentic artifacts and adversary tradecraft pulled from live incidents. You'll even build and run live ransomware in a controlled lab to see how it behaves and examine leaked source code to understand how encryption really works. From initial intrusion through exfiltration and encryption, you'll practice the full response lifecycle and tie technical findings into organizational recovery and communication.

Ransomware today is no longer "just encryption." Human-Operated Ransomware (HumOR) groups and Ransomware-as-a-Service (RaaS) affiliates run full-scale campaigns that exploit the blind spots traditional IR training leaves behind: persistence, lateral movement, data theft, and even extortion-only attacks where no files are ever encrypted. The fallout is both technical and human—impacting operations, customers, and leadership decisions.

In FOR528,™ you'll practice the full ransomware and extortion lifecycle, from initial intrusion to organizational recovery. You'll learn how to prevent, detect, respond, and hunt for ransomware activity; analyze obfuscated scripts and attacker tools; identify stolen data; and validate recovery efforts with confidence. More importantly, you'll see how forensic findings tie directly into business-critical actions: communicating with leadership, coordinating across teams, and restoring trust in systems after an attack.

This four-day course features hands-on labs built from real cases and a full-day capture-the-flag (CTF) event to test your skills under pressure. All hands-on training is conducted using freely available and/or open-source tooling to ensure that you can return to work and implement everything covered without needing to purchase any commercial products. By the end, you'll not only recognize ransomware and extortion activity—you'll be ready to respond with the same speed, confidence, and precision as the professionals who handle these incidents on the frontline.

Course Topics

- Explore the history and ecosystem of ransomware and extortion, including Human-Operated Ransomware (HumOR), Ransomware-as-a-Service (RaaS), and non-encrypting Cyber Extortion.
- Identify which forensic artifacts to collect, learn how to parse those artifacts, and focus in-depth on how to analyze the parsed output.
- Investigate the full lifecycle of a typical ransomware campaign including Initial Access, Execution (tooling and living-off-the-land), Defense Evasion, Persistence, Command and Control, Privilege Escalation, Credential Access, Lateral Movement, Active Directory attacks, Data Access and Collection, Data Exfiltration, Payload Deployment, and Encryption.
- Examine how attackers collect, stage, and exfiltrate data in both encryption and extortion-only campaigns.
- Analyze attacker tooling in-depth via malware analysis such as deobfuscating scripts, analyzing the deobfuscated scripts, and identifying TTPs and IOCs within your results.
- Examine the inner workings of ransomware encryption payloads to learn about how encryption works through review of leaked source code.
- Learn how to scope incidents, validate recovery, and coordinate across IT, legal, and leadership during a ransomware crisis.
- Apply your skills in daily hands-on labs built from real cases and a full-day CTF that simulates a ransomware incident end-to-end.

Section Descriptions

SECTION 1: Ransomware Incident Response Fundamentals

Section 1 begins with a review of ransomware's history, as we deep-dive into the roles, processes, communication methods, and activities related to these threats. After learning how we can apply incident response practices, we begin our deep-dive into the Windows-based forensic artifacts best suited to ransomware campaign analysis.

TOPICS: Ransomware Evolution and History; Forensic Artifact Collection; Incident Response Processes and Application to Ransomware; Windows Forensic Artifacts; Analysis At-Scale via TimeSketch

SECTION 2: Ransomware Modus Operandi

Ransomware incidents often follow familiar patterns. In Section 2, you'll learn to detect these recurring tactics, techniques, and procedures (TTPs) through hands-on labs and analysis.

TOPICS: Analysis At-Scale via Kibana; Malware Infection vs. Credential Harvesting; Malicious Attachments and Links; Identifying Malicious RDP Activity; Scripting

SECTION 3: Advanced Ransomware Concepts

Section 3 covers Privilege Escalation, Credential Access, and Lateral Movement, detailing tools ransomware actors use to escalate privileges, access credentials, and dump processes. You'll explore lateral movement methods like RDP, SMB (PsExec), and WinRM.

TOPICS: Privilege Escalation and Credential Access; Lateral Movement Techniques; Exploiting Active Directory (AD); Data Access and Exfiltration Methods; Hunting Ransomware Operators

SECTION 4: Ransomware Incident Response Challenge

Our CTF challenge consists of 50 questions pertaining to a specially crafted attack scenario against our victim organization.

TOPICS: Digital Forensics Capture-the-Flag Event; Review Parsed Artifact and Log Data; Identify Tools and Processes in Scenario

Who Should Attend

- Information security professionals who want to learn how to collect, parse, and analyze forensic artifacts in support of ransomware incident response
- Incident response team members who need to use deep-dive digital forensics to help solve their Windows data breach and intrusion cases, perform damage assessments, and develop indicators of compromise
- Incident triage analysts such as those working in a Security Operations Center (SOC), Computer Incident Response Team, or similar
- Managed Services Provider (MSP) and Managed Security Services Provider (MSSP) analysts who may need to aid in ransomware incident response
- Law enforcement officers, federal agents, and detectives who want to become deep subject-matter experts on ransomware investigations
- Medical and hospitality IT staff who may need to respond to ransomware events
- Anyone interested in a deep understanding of ransomware-specific incident response who has a background in information systems, information security, computers

"The course presented real-life scenarios and detection mechanisms to enhance your organization's security posture to detect and prevent ransomware before it can cause damage to your operations."

—Eric B., **Fluidra**

"The course is pack filled with highly valuable information that will take your company to the next level of being prepared for ransomware."

—Nicolas B., **Publix**

"The content is engaging, and has shown me plenty of new open-source tools."

—Jason T., **Triskele Labs**