Advanced Ransomware Defense and Incident Recovery Training Course



16 - 20 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #CYB6188_89492

Course Introduction / Overview:

The escalating sophistication of ransomware attacks poses a significant and persistent threat to organizations worldwide, capable of causing catastrophic operational disruption and financial loss. This course provides a comprehensive, end-to-end framework for building robust cyber resilience against these advanced threats. Moving beyond basic prevention, this program delves into the complete lifecycle of ransomware incident management, from proactive defense mechanisms to strategic recovery and post-incident analysis. We will explore the tactical methodologies employed by modern threat actors, as detailed in works like "The Art of Invisibility" by Kevin Mitnick, to better understand and counter their strategies. Participants will learn to develop and implement multi-layered security controls, create effective incident response plans, and master data recovery techniques that ensure business continuity. BIG BEN Training Center has designed this curriculum to empower professionals with the practical skills and strategic foresight needed to protect critical assets, manage crises effectively, and minimize the impact of a ransomware event, transforming their organization's posture from reactive to resilient. This training is an essential investment in safeguarding your organization's future against the evolving landscape of cyber extortion.

Target Audience / This training course is suitable for:

- Information Technology (IT) Managers and Directors.
- Cybersecurity Analysts and Engineers.
- Incident Response Team Members.
- System and Network Administrators.
- Security Operations Center (SOC) Staff.
- Risk and Compliance Officers.
- Business Continuity and Disaster Recovery Planners.
- IT Auditors and Consultants.
- Chief Information Security Officers (CISOs).

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceutical.
- Government and Public Sector Agencies.
- Manufacturing and Industrial Control Systems.
- Energy and Critical Infrastructure.
- Retail and E-commerce.
- Telecommunications and Technology.
- Education and Research Institutions.
- Legal and Professional Services.

Target Organizations Departments:

- Information Technology (IT) and Infrastructure.
- Cybersecurity and Information Security.
- Risk Management and Compliance.
- Internal Audit.
- Legal and General Counsel.
- Operations Management.
- Crisis Management and Communications.
- Business Continuity Planning.

Course Offerings:

By the end of this course, the participants will have able to:

- Analyze the modern ransomware threat landscape, including attack vectors and threat actor motivations.
- Develop and implement a multi-layered ransomware prevention strategy.
- Conduct vulnerability assessments and patch management programs effectively.
- Create a comprehensive and actionable ransomware incident response plan.
- Master techniques for containing an active ransomware infection to prevent lateral movement.
- Evaluate and implement robust data backup and recovery solutions.
- Execute data restoration procedures to meet Recovery Time Objectives (RTOs).
- Understand the legal and regulatory obligations following a data breach.
- Improve organizational cyber resilience through post-incident analysis and lessons learned.
- Effectively manage communications during a cybersecurity crisis.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring participants can apply their learning directly to their professional roles. This course moves beyond theoretical lectures by integrating a variety of dynamic learning techniques. A cornerstone of our approach is the extensive use of real-world case studies, which deconstruct recent, high-profile ransomware attacks to analyze attacker tactics, defensive failures, and successful response strategies. Participants will engage in collaborative group exercises and workshops, such as developing a mock incident response plan for a hypothetical organization, fostering teamwork and critical thinking. Interactive sessions, including Q&A panels and expert-led discussions, encourage active participation and knowledge sharing. The curriculum incorporates simulated ransomware scenarios and tabletop exercises where participants must make critical decisions under pressure, reinforcing their understanding of containment, eradication, and recovery processes. Continuous feedback from the instructor ensures that participants grasp complex concepts and can confidently implement these advanced defense and recovery strategies within their own operational environments.

Course Agenda (Course Units):

Unit One: The Modern Ransomware Threat Landscape

- Understanding the Evolution of Ransomware.
- Anatomy of a Ransomware Attack Chain.
- Key Threat Actor Groups and Their Tactics, Techniques, and Procedures (TTPs).
- The Ransomware-as-a-Service (RaaS) Ecosystem.
- Analysis of Initial Access Vectors: Phishing, RDP, and Software Vulnerabilities.
- The Role of Initial Access Brokers (IABs).
- Double and Triple Extortion Tactics.
- Recent Trends and Future Predictions in Ransomware.

Unit Two: Proactive Defense and Prevention Strategies

- Implementing a Defense-in-Depth Security Architecture.
- Advanced Endpoint Protection (EDR/XDR) and Antivirus Configuration.
- Network Segmentation and Zero Trust Principles.
- Securing Identity and Access Management (IAM) and Privileged Accounts.
- Effective Email Security and Anti-Phishing Controls.
- Developing a Robust Vulnerability and Patch Management Program.
- Application Whitelisting and Control.
- Building a Strong Security Awareness and Training Culture.

Unit Three: Incident Detection and Response Planning

- Building a Ransomware-Specific Incident Response (IR) Plan.
- Defining Roles and Responsibilities for the Cyber Incident Response Team (CIRT).
- Establishing Threat Intelligence and Threat Hunting Capabilities.
- Key Indicators of Compromise (IOCs) for Early Detection.
- Developing a Crisis Communication Plan for Internal and External Stakeholders.
- Legal and Regulatory Considerations Before, During, and After an Attack.
- Engaging with Law Enforcement and External IR Forensics Teams.
- Conducting Tabletop Exercises and IR Plan Drills.

Unit Four: Containment, Eradication, and Recovery Operations

- Executing the Incident Response Plan: First Steps.
- Isolating Infected Systems and Network Segments to Prevent Spread.
- Evidence Preservation and Forensic Data Collection.
- Strategies for Eradicating Malware from the Environment.
- The Ransom Payment Decision: A Framework for Evaluation.
- Designing and Implementing a Resilient Backup and Recovery Strategy (The 3-2-1 Rule).
- Data Recovery Techniques: Restoring from Clean Backups.
- System Validation and Post-Recovery Security Hardening.

Unit Five: Post-Incident Activities and Building Cyber Resilience

- Conducting a Thorough Post-Incident Review and Root Cause Analysis.
- Documenting Lessons Learned and Creating an Action Plan for Improvement.
- Reporting Requirements: Cyber Insurance, Regulatory Bodies, and Data Protection Authorities.
- Managing Reputational Damage and Stakeholder Trust.
- Integrating Business Continuity and Disaster Recovery (BCDR) with Cybersecurity.
- Continuously Monitoring and Improving Security Controls.
- Developing Metrics to Measure and Report on Cyber Resilience.
- Final Course Review and Capstone Simulation Exercise.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Considering the ethical dilemma and the potential for encouraging future attacks, under what circumstances, if any, could paying a ransom be a strategically justifiable decision for an organization?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by adopting a holistic, strategy-first approach to ransomware resilience, moving beyond a narrow focus on specific software tools or technical fixes. While many programs concentrate solely on prevention, our curriculum provides a complete, 360-degree view of the entire incident lifecycle, from proactive defense and threat hunting to crisis management, strategic recovery, and long-term resilience building. We emphasize the critical intersection of technology, policy, and people, ensuring participants understand not just the 'how' of technical implementation but the 'why' of strategic decision-making. The content is uniquely structured around real-world attacker methodologies and business impact, rather than abstract technical concepts. Through advanced tabletop exercises and case study deconstructions, participants are challenged to make critical decisions in a simulated crisis environment, honing skills that are directly transferable to their organizations. This focus on practical application, strategic thinking, and integrating cybersecurity with broader business continuity objectives provides a level of depth and preparedness that is essential for confronting the sophisticated, multi-faceted nature of modern ransomware threats.