

CyberSec First Responder: Incident Response Mastery Course

2027 000000 18 - 14
Online

UK Traininig

PARTNER



CyberSec First Responder: Incident Response Mastery Course

~~R20222425~~ ~~19880514~~ ~~Detention~~: Online Fees: 2700 GBP

Why This Course

Cybersecurity incidents can escalate quickly, causing operational disruption, data loss, financial damage, and reputational harm. Effective incident response requires more than technical knowledge; it requires preparation, structured processes, clear roles, rapid threat analysis, evidence handling, recovery planning, and continuous improvement.

This intensive 5-day Cybersecurity Incident Response Training program equips IT professionals with the practical skills needed to identify, assess, contain, eradicate, and recover from cyber incidents. The course covers incident response planning, threat detection, log analysis, containment strategies, malware handling, digital forensics, evidence preservation, post-incident reporting, and tabletop simulations. Through hands-on exercises and real-world scenarios, participants will learn how to coordinate incident response activities and strengthen organizational resilience.

What You'll Learn and Practice

By joining this program, you will:

- Understand the cybersecurity incident response lifecycle and key frameworks.
- Develop and implement comprehensive incident response plans.
- Build and organize an effective incident response team.
- Identify common cyber threats, attack vectors, and indicators of compromise.
- Apply network and endpoint monitoring techniques.
- Analyze logs and security events to detect suspicious activity.
- Use threat intelligence to support investigation and response.
- Apply containment strategies for different incident types.
- Support malware analysis, eradication, and system recovery procedures.
- Perform digital forensics and evidence collection activities.
- Preserve evidence using proper chain of custody practices.
- Conduct post-incident analysis, reporting, and continuous improvement activities.

UK Training

PARTNER

A graphic of a chessboard with several chess pieces (a king, a queen, a rook, and a pawn) positioned on it. The board is checkered, and the pieces are in gold and silver.

The Program Flow

Day 1: Foundations of Incident Response

- Understand the purpose and importance of cybersecurity incident response.
- Explore the incident response lifecycle and recognized response frameworks.
- Identify key roles and responsibilities within an incident response team.
- Develop incident response plans aligned with organizational needs.
- Apply preparation practices that improve readiness before incidents occur.

Day 2: Threat Detection and Analysis

- Identify common cyber threats, attack techniques, and attack vectors.
- Apply network and endpoint monitoring methods to detect suspicious behavior.
- Analyze logs, alerts, and security events for signs of compromise.
- Use security information management practices to support investigations.
- Apply threat intelligence and indicators of compromise to improve detection and response.

Day 3: Incident Containment and Eradication

- Apply containment strategies based on incident type and business impact.
- Use network segmentation and access control to limit incident spread.
- Understand malware analysis and eradication techniques.
- Plan system recovery and data restoration procedures.
- Coordinate containment, eradication, and recovery actions while minimizing disruption.

Day 4: Digital Forensics and Evidence Handling

- Understand the principles and purpose of digital forensics.
- Collect and preserve digital evidence using proper procedures.
- Conduct forensic analysis of systems, endpoints, and networks.
- Maintain chain of custody and documentation standards.
- Understand legal considerations related to evidence handling and incident investigations.

Day 5: Post-Incident Activities and Continuous Improvement

- Conduct post-incident analysis to identify root causes and lessons learned.
- Prepare clear incident reports for technical and management audiences.
- Improve incident response processes based on findings.
- Implement security enhancements to reduce future risk.
- Participate in tabletop exercises and simulations to test response readiness.

A graphic featuring the text 'UK Training PARTNER' in black, with 'PARTNER' in a larger, bold font. The text is positioned above a chessboard with several chess pieces (a king, a queen, and a pawn) and concentric circles emanating from behind them.

Individual Impact

- Build confidence in responding to cybersecurity incidents effectively.
- Strengthen skills in threat detection, analysis, containment, and recovery.
- Gain practical awareness of digital forensics and evidence handling.
- Improve the ability to coordinate with incident response teams and stakeholders.
- Develop stronger reporting, communication, and post-incident analysis capabilities.

Work Impact

- Improve organizational readiness for cybersecurity incidents.
- Reduce incident impact through faster detection, containment, and recovery.
- Strengthen coordination between IT, security, legal, management, and business teams.
- Improve evidence handling, reporting, and compliance readiness.
- Enhance security posture through lessons learned and continuous improvement.

Training Methodology

This program combines incident response concepts with practical application through:

- Real-world cybersecurity incident scenarios and case studies.
- Hands-on threat detection and log analysis exercises.
- Incident containment, eradication, and recovery simulations.
- Digital forensics and evidence preservation activities.
- Tabletop exercises for incident coordination and decision-making.
- Post-incident reporting and lessons-learned workshops.

Beyond the Course

Upon completion, participants will be able to:

- Create and implement a customized incident response plan.
- Detect, analyze, and respond to different types of cyber threats.
- Apply containment, eradication, and recovery strategies effectively.
- Collect and preserve digital evidence using proper forensic procedures.
- Conduct post-incident analysis and prepare clear incident reports.
- Lead or support incident response teams during cybersecurity events.

A decorative graphic in the bottom right corner featuring a chessboard with several chess pieces (a king, a queen, and a pawn) and concentric circles radiating from behind them.

UK Training
PARTNER