
Cyber Incident Response Leadership: Detection, Containment and Recovery Training Course

1 – 5 February 2027
Tokyo





Cyber Incident Response Leadership: Detection, Containment and Recovery Training Course

Ref: 98_13810 Date: 1 – 5 February 2027 Location: Tokyo Fees: 6900 GBP

Programme Summary

Cyber incident response leadership is a five-day training course for security leaders at managerial and strategic level, culminating in an incident response plan and playbook set for their own organisation. Ransomware, data theft and supply chain intrusions now test every organisation, yet many response plans are untested and roles become unclear under pressure. The approach covers preparation, detection, containment, forensics, recovery and lessons learned. Mars Training Centre UK delivers this programme in cyber incident response leadership.

The Business Case

The cost of a cyber incident depends on how quickly it is detected and contained and how well the organisation communicates. Slow escalation, lost evidence and improvised decisions turn a contained event into a prolonged outage. A prepared, rehearsed response capability limits each of these.

- Time to Detect and Contain: Shortens as monitoring, triage criteria and containment playbooks are agreed in advance.
- Service Downtime and Recovery Cost: Fall as recovery priorities, backups and restoration steps are tested before an attack.
- Regulatory and Reputational Exposure: Reduces as evidence handling, notification and stakeholder communication follow a defined process.

Principles and Evidence Base

- NIST SP 800-61 Revision 3: Links incident response to cybersecurity risk management and structures the capability review in Session 1.
- NIST Cybersecurity Framework 2.0: Provides the govern, identify, protect, detect, respond and recover functions used to map responsibilities across Sessions 1 to 4.
- ISO/IEC 27035 Information Security Incident Management: Frames the incident management process, team roles and evidence handling in Sessions 2 and 3.
- SANS Six-Step Incident Response Process: Gives the preparation-to-lessons-learned sequence rehearsed in the Session 5 exercise.

Intended Participants

- Leaders accountable for an organisation's cyber defence and incident response capability.
- Managers who run security operations, monitoring and incident handling teams.
- Directors responsible for IT services, infrastructure recovery and business continuity.
- Senior staff who coordinate legal and communications responses to breaches.



The programme serves banks and insurers, government entities, energy and utilities, and telecommunications and healthcare providers.

Learning Outcomes

1. Participants will be able to evaluate the maturity of their incident response capability against NIST SP 800-61 Revision 3.
2. Participants will be able to design triage criteria, severity levels and escalation paths for the security operations centre.
3. Participants will be able to prioritise containment and eradication actions using threat intelligence on attacker techniques.
4. Participants will be able to justify evidence handling and forensic procedures that preserve investigative and legal options.
5. Participants will be able to construct a ransomware response and recovery sequence for critical services.
6. Participants will be able to formulate notification, communication and lessons-learned processes after a major incident.

Programme Structure

Day 1: Foundations of Cyber Incident Response Leadership

What does an effective response capability require, and how mature is it today?

- Ransomware, Data Theft and Supply Chain Threats
- NIST SP 800-61 Revision 3 and Cybersecurity Risk Management
- NIST CSF 2.0 Functions and Response Responsibilities
- Incident Response Team Models, Roles and Authority
- Capability Maturity Assessment and Gap Analysis

Day 2: Detection, Triage and Threat Intelligence

How are real incidents found quickly and separated from noise?

- Security Operations Centre Monitoring and Use Cases
- Alert Triage, Severity Classification and Escalation
- Threat Intelligence Sources and Attacker Techniques
- ISO/IEC 27035 Incident Management Process
- Incident Logging, Tracking and Situation Reporting

Day 3: Containment, Eradication and Digital Forensics

How is an intrusion stopped without destroying the evidence needed to understand it?



- Containment Strategies for Endpoints, Networks and Cloud
- Eradication of Persistence and Compromised Accounts
- Digital Forensics Triage and Evidence Collection
- Chain of Custody and Legal Considerations
- Working With External Responders and Law Enforcement

Day 4: Ransomware, Recovery and Communication

How are services restored and stakeholders informed during a major attack?

- Ransomware Response Decisions and Extortion Scenarios
- Backup Integrity, Restoration Priorities and Recovery Testing
- Business Continuity Links and Crisis Management Interfaces
- Regulatory Notification and Data Breach Obligations
- Executive, Staff, Customer and Media Communication

Day 5: Applying Cyber Incident Response Leadership

How are capability, playbooks and decisions tested together before a real attack?

- Full-Cycle Tabletop Exercise Using the SANS Six Steps
- Playbook Drafting for Priority Incident Types
- Lessons-Learned Review and Improvement Tracking
- Peer Challenge of Incident Response Plans
- Incident Response Plan and Playbook Presentation

Methodology

The programme is built around simulation and case analysis. Participants work through incidents drawn from banking, government, healthcare and industrial settings and make decisions as new facts emerge before applying each tool to their own environment.

- Suggested activity: Classifying and escalating a stream of security alerts in a simulated operations centre.
- Suggested activity: Deciding containment steps for a compromised domain administrator account.
- Suggested activity: Leading the first hours of a ransomware incident.

Capstone Output

Each participant completes an incident response plan and playbook set for their organisation. It contains team roles and authority, severity and escalation criteria, playbooks for priority incident types, evidence handling rules, recovery priorities, a communication and notification matrix and an exercise schedule, ready for executive approval.



Frequently Asked Questions

Is cyber incident response leadership suitable for IT directors without a security operations background?

Yes. It suits CISOs, security operations heads, incident response managers and IT directors. It assumes familiarity with IT operations but not hands-on forensic or analyst experience.

Which standards underpin cyber incident response leadership?

It draws on NIST SP 800-61 Revision 3, the NIST Cybersecurity Framework 2.0, ISO/IEC 27035 for incident management and the SANS six-step incident response process.

How is the cyber incident response plan and playbook set used at work?

You take back a plan and playbooks your executives can approve and your team can exercise, with clear roles, escalation criteria and recovery priorities.

How does cyber incident response leadership differ from general cybersecurity awareness programmes?

It focuses on what happens once an attack is under way: detection, containment, forensics, recovery and notification, rather than general security awareness or policy.