JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Cyber Forensics and Incident Response Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Cyber Forensics and Incident Response Training Course

Cyber Forensics and Incident Response is a 1-week training course for incident responders, SOC analysts and forensic technicians who contain live attacks without destroying evidence, and it produces a forensic-ready incident response playbook. Ransomware crews and intruders now move within hours, so responders who capture memory, logs and network traces early decide both recovery speed and what the organisation can later prove. Jupiter Prime Training delivers this cyber forensics and incident response course.

Why Cyber Forensics and Incident Response Matters Now

Attackers increasingly live off built-in system utilities, run malicious code only in memory and wipe logs before leaving. At the same time insurers, auditors and legal teams expect a defensible account of what happened. Responders who isolate a host too early can lose the volatile traces needed to scope an intrusion; those who wait too long let it spread. The course balances both pressures, linking the Detect, Respond and Recover functions of the NIST Cybersecurity Framework 2.0 NIST CSF 2.0 with the incident management controls of ISO/IEC 27001:2022.

Who Gains Most from Cyber Forensics and Incident Response

- Responders who lead triage and containment during live security incidents
- Analysts in security operations centres who escalate alerts into investigations
- Technicians who capture memory, packet and log evidence from affected systems
- Threat hunters who search for persistence and lateral movement across networks
- Engineers who restore systems and must confirm attackers have been removed

Security operations teams in telecommunications and energy gain most when analysts and responders attend together, because they agree one evidence-first escalation path.

Cyber Forensics and Incident Response Capabilities

Participants learn to treat every containment action as both a defensive move and an evidential event, choosing what to capture before what to block.

- Assess alert severity and scope using correlated log and endpoint signals — incident commander
- Apply memory acquisition and analysis to expose hidden processes and injected code — forensic lead
- Analyse packet captures and flow records to trace command-and-control channels — network operations
- Test suspicious files through static and sandbox triage to extract indicators — threat intelligence
- Weigh containment options against evidence loss and business disruption — service owners

- Design playbook steps that preserve evidence at each response phase — security operations manager

Key Cyber Forensics and Incident Response Terms

- Order of volatility — the sequence for collecting evidence from most to least short-lived, starting with memory.
- Memory image — a capture of a system's RAM revealing running processes, network sockets and code that never touches disk.
- Indicator of compromise — an observable artefact, such as a hash, domain or registry key, that signals malicious activity.
- Command-and-control channel — the communication path attackers use to send instructions to compromised hosts.
- Containment strategy — the chosen method of limiting an attacker's reach, from network isolation to account suspension.
- Forensic readiness — the prior arrangement of logging, tools and procedures that lets evidence be gathered quickly and soundly.

Cyber Forensics and Incident Response Day by Day

Day 1: The Intrusion Landscape and Response Lifecycle

- Attacker Tradecraft Review — Recognising Living-off-the-Land and Fileless Techniques
- Response Lifecycle Phases — Aligning Detect, Respond and Recover with NIST CSF 2.0
- Order of Volatility — Sequencing Collection Before Containment Actions
- Severity Classification Matrix — Deciding Escalation Levels and Responders
- Forensic Readiness Checklist — Confirming Logging Coverage Before an Incident

Day 2: Memory Forensics

- Live Memory Acquisition — Capturing RAM Without Alerting the Intruder
- Process Tree Analysis — Spotting Parent-Child Anomalies and Masquerading
- Injected Code Detection — Identifying Hollowed and Reflective Payloads
- Network Socket Inspection — Linking Processes to Remote Connections
- Credential Theft Traces — Assessing Exposure of Cached Secrets

Day 3: Log and Network Evidence

- Log Source Prioritisation — Choosing Authentication, Proxy and DNS Records
- SIEM Correlation Queries — Reconstructing Attacker Movement Across Hosts
- Packet Capture Review — Extracting Payloads and Session Details
- Flow Record Analysis — Revealing Beaconing and Data Exfiltration Patterns
- Incident Controls Mapping — Linking Evidence Needs to ISO/IEC 27001:2022

Day 4: Malware Triage and Containment Decisions

- Static File Triage — Extracting Strings, Hashes and Signatures Safely
- Sandbox Behaviour Analysis — Observing Persistence and Network Callbacks
- Indicator Packaging — Sharing Compromise Markers with Detection Teams
- Containment Option Matrix — Weighing Isolation, Blocking and Account Suspension
- Eradication Verification — Confirming Removal Before Restoring Services

Day 5: Practising the Forensic-Ready Incident Response Playbook

- Volatility-First Collection Steps — Embedding Day Two Memory Capture
- Network Evidence Triggers — Applying Day Three Log and Packet Rules
- Containment Decision Gates — Inserting Day Four Option Matrix Approvals
- Simulated Ransomware Exercise — Testing Steps Under Time Pressure
- Forensic-Ready Incident Response Playbook — Finalising Roles, Triggers and Evidence Steps

Applying Cyber Forensics and Incident Response After the Course

- Run a memory acquisition drill on a test host and record the time and tools needed.
- Add order-of-volatility collection steps to the first three actions of the current ransomware runbook.

Cyber Forensics and Incident Response Questions FAQ

What is cyber forensics and incident response and why does it matter now?

It is the practice of containing security incidents while capturing the evidence that explains them. It matters now because attackers work in memory and erase logs, so evidence lost during response cannot be recovered later.

Which roles gain most from cyber forensics and incident response training?

Incident responders, SOC analysts and forensic technicians gain most. Threat hunters and recovery engineers also benefit, since they rely on the same memory, log and network evidence to scope and close incidents.

How does cyber forensics and incident response differ from a computer forensic investigation course?

This course works during live incidents, focusing on memory, network evidence and containment choices. A computer forensic investigation course examines seized disks after the event, building detailed timelines and reports for legal proceedings.

What do you bring back from cyber forensics and incident response training?

You bring back a forensic-ready incident response playbook tested in a simulated ransomware exercise, with collection steps, containment gates and roles, ready to adapt to your own security operations centre.

Cyber Forensics and Incident Response: The Way Forward

The forensic-ready incident response playbook first informs the next decision to isolate an infected host. Responders, SOC leads and service owners use it to agree what is captured and who approves containment. After its first live use, revisit whether any containment gate delayed action unnecessarily, and adjust triggers where evidence was still lost.