JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Cyber Incident First Responder Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Cyber Incident First Responder Training Course

Cyber Incident First Responder is a 2-week training course for SOC analysts, incident responders and IT security officers who handle the first hours of an attack, and it ends with a tested incident handling runbook. Intrusions now move from initial foothold to data theft in hours, so the quality of first response decides how much an organisation loses. Jupiter Prime Training delivers this course for responders who must act with evidence, speed and restraint.

Why Cyber Incident First Responder Matters Now

Three forces shape first response today: ransomware crews that encrypt and extort within a single shift, hybrid estates where cloud, endpoint and identity logs sit in separate consoles, and executives who expect a clear account of impact before the facts are settled. A responder who triages well limits dwell time, preserves admissible evidence and keeps recovery orderly; a poor first move can wipe volatile memory or alert the intruder. The course rests on the incident handling life cycle of NIST Special Publication 800-61 NIST SP 800-61, from preparation to post-incident activity.

Who Gains Most from Cyber Incident First Responder

- Security operations staff who watch alerts, tune detections and escalate suspected intrusions
- Incident handlers who scope compromises, contain hosts and coordinate eradication
- IT security officers who own endpoint, server and identity hardening after an attack
- Network defenders who read packet captures, flow records and firewall logs during a breach
- Threat intelligence contributors who enrich indicators and track adversary behaviour

A security operations centre that sends its analysts, handlers and network defenders together gains most, because the shared runbook removes hand-off delays between shifts.

Cyber Incident First Responder Capabilities

Participants leave able to move from a single alert to a contained, documented incident without losing evidence or time.

- Assess alert fidelity using threat intelligence and log correlation — escalation decisions for the shift lead
- Analyse network traffic and packet captures for command-and-control patterns — containment scope for network owners
- Apply endpoint triage to memory, processes and persistence points — host isolation decisions
- Preserve digital evidence with a documented chain of custody — legal counsel and investigators
- Specify containment, eradication and recovery steps for each incident class — system owners and service managers
- Communicate incident status, impact and lessons learned — executives and the incident commander

Key Cyber Incident First Responder Terms

- Indicator of compromise — An observable artefact, such as a file hash, domain or IP address, that signals a system may have been breached.
- Dwell time — The period between an intruder's first access and the moment defenders detect the intrusion.
- Triage — The rapid sorting of alerts and affected assets by severity so scarce responders act on the most urgent first.
- Chain of custody — The documented record of who collected, handled and stored each piece of evidence, and when.
- Containment — Actions that stop an incident spreading, such as isolating hosts, disabling accounts or blocking traffic, while evidence is kept.
- Lateral movement — Techniques an attacker uses to move from the first compromised host to other systems inside the network.

Cyber Incident First Responder Day by Day

Day 1: The Threat Landscape a Responder Faces

- Ransomware and Extortion Tactics — Response Urgency and Business Impact
- Attack Chain Models — Where Detection Can Interrupt an Intrusion
- NIST SP 800-61 Life Cycle — Roles Across Preparation and Recovery
- Incident Severity Matrix — Escalation Thresholds and On-Call Triggers
- Responder Toolkit Inventory — Gaps Before the Next Alert

Day 2: Threat Intelligence for First Response

- Intelligence Feeds and Sharing Communities — Source Reliability and Relevance
- Indicator Enrichment Workflow — Alert Confidence and False Positive Rates
- Adversary Behaviour Profiles — Likely Next Moves After Initial Access
- Threat Hunting Hypotheses — Proactive Searches Ahead of Alerts
- Intelligence Requirements Register — Questions Leadership Needs Answered

Day 3: Log Sources and Event Correlation

- Windows Event Logs and Sysmon — Process and Logon Visibility
- Linux Audit and Authentication Logs — Privilege Abuse Detection
- SIEM Correlation Rules — Alert Volume Versus Coverage Trade-Offs
- Cloud Audit Trails and Identity Logs — Tenant-Wide Compromise Scope
- Log Retention and Time Synchronisation — Reliability of the Incident Timeline

Day 4: Network Traffic Analysis

- Packet Capture with Wireshark — Evidence of Exfiltration and Beaconing
- NetFlow and Connection Records — Lateral Movement Paths
- DNS and Proxy Log Review — Command-and-Control Domain Detection
- Intrusion Detection Signatures — Tuning Against Benign Traffic
- Encrypted Traffic Metadata — Inspection Limits and Privacy Trade-Offs

Day 5: Endpoint Triage and Volatile Data

- Order of Volatility — What to Collect Before Isolation
- Memory Acquisition and Process Review — Malicious Code in Running Systems
- Persistence Mechanisms and Scheduled Tasks — Eradication Completeness
- Endpoint Detection and Response Telemetry — Host Isolation Decisions
- Live Response Scripts — Speed Versus Evidence Integrity

Day 6: Digital Evidence and Forensic Handling

- Disk Imaging and Hash Verification — Admissibility of Collected Evidence
- Chain of Custody Forms — Accountability for Every Artefact
- Timeline Reconstruction — Sequence of Attacker Actions
- Malware Sample Handling and Sandboxing — Safe Behavioural Insight
- Legal Hold and Evidence Storage — Counsel and Insurer Expectations

Day 7: Containment and Eradication Decisions

- Short-Term Versus Long-Term Containment — Business Continuity Impact
- Account Disablement and Credential Resets — Identity Compromise Scope
- Network Segmentation and Blocking Rules — Attacker Visibility Risk
- Root Cause Identification — Vulnerability or Misconfiguration to Close
- Eradication Verification Checks — Confidence Before Reconnection

Day 8: Recovery and Incident Coordination

- System Restoration from Trusted Backups — Reinfection Prevention
- Incident Command Structure — Decision Rights During a Crisis
- Stakeholder Communication Templates — Executive, Staff and Customer Messages
- Third-Party and Supplier Coordination — Shared Responsibility in Response
- Monitoring After Recovery — Signs the Attacker Has Returned

Day 9: Reporting and Lessons Learned

- Incident Report Structure — Facts, Impact and Open Questions
- After-Action Review Facilitation — Blame-Free Improvement Findings
- Response Metrics and Mean Time to Contain — Capability Investment Priorities
- Detection Gap Analysis — New Rules and Telemetry Sources
- Healthcare and Financial Services Case Reviews — Sector Response Patterns

Day 10: Practising the Incident Handling Runbook

- Live Intrusion Simulation from First Alert — Triage Under Time Pressure
- Applied Log, Traffic and Endpoint Analysis — Scoping the Simulated Breach
- Evidence Collection Drill — Chain of Custody in Practice
- Containment and Briefing Exercise — Executive Update Within One Hour
- Incident Handling Runbook Completion — Steps, Owners and Escalation Paths

Applying Cyber Incident First Responder After the Course

- Run a tabletop exercise on a ransomware scenario using the severity matrix and containment options practised in the course
- Audit log sources and retention against the correlation and timeline needs identified during traffic and endpoint analysis

Cyber Incident First Responder Questions FAQ

What is cyber incident first responder work and why does it matter now?

Cyber incident first responder work is the detection, triage and containment of an attack in its first hours. It matters now because intruders move quickly, and early decisions on evidence and isolation set the cost and length of recovery.

Which roles gain most from cyber incident first responder training?

SOC analysts, incident handlers, IT security officers and network defenders gain most. You benefit if you receive alerts, scope compromises or contain hosts, and the gain is larger when several members of one response team attend together.

How does cyber incident first responder training differ from a digital forensics course?

It covers the whole first response, from alert to lessons learned, rather than deep laboratory forensics. Evidence handling is taught to the level a responder needs to preserve artefacts for specialists, alongside intelligence, traffic analysis and containment.

What do you bring back from cyber incident first responder training?

You bring back a tested runbook for handling incidents in your environment. It sets out triage steps, evidence collection, containment choices, escalation contacts and reporting formats that your team can adopt the following week.

Cyber Incident First Responder: The Way Forward

The incident handling runbook first informs how the next high-severity alert is escalated and who isolates the affected host. Shift analysts, incident handlers and the incident commander use it during live events, and service owners use it during recovery. After its first real use, revisit the containment thresholds and evidence steps, since early incidents show where speed and preservation pull against each other.