JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Network Threat Hunting and Detection Tuning Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Network Threat Hunting and Detection Tuning Training Course

Network Threat Hunting and Detection Tuning is a 2-week advanced training course for network security engineers and SOC analysts who must find intruders hiding in ordinary traffic, and it produces a network defence and hunting plan for an enterprise network. Attackers now live off legitimate protocols and encrypted sessions, so untuned sensors drown analysts in alerts while real intrusions pass quietly. Jupiter Prime Training runs this Network Threat Hunting and Detection Tuning course.

Why Network Threat Hunting and Detection Tuning Matters Now

Three forces shape network detection today. Most traffic is now encrypted, so analysts must read metadata such as flow records, certificate details and connection timing rather than payloads. Hybrid estates stretch east-west traffic across data centres, cloud subnets and remote sites, widening the blind spots between sensors. SOC teams also face alert fatigue, where noisy signatures hide genuine lateral movement. Organisations that hunt proactively shorten attacker dwell time and contain breaches before data leaves; those relying on default rules learn of intrusions from outsiders. The course draws on public adversary-technique knowledge bases and recognised incident-handling lifecycles, described in general terms.

Who Gains Most from Network Threat Hunting and Detection Tuning

- Engineers who deploy and maintain intrusion detection sensors and packet brokers
- SOC analysts who triage network alerts and escalate suspicious sessions
- Specialists who design segmentation zones and firewall rule bases
- Hunters who build hypotheses and query flow and protocol logs
- Responders who isolate compromised hosts and preserve network evidence

The greatest gain comes when sensor engineers and SOC analysts from the same security operations centre attend together and agree one shared tuning and escalation rhythm.

Network Threat Hunting and Detection Tuning Capabilities

Participants move from waiting for alerts to deliberately searching packet, flow and protocol records for adversary behaviour.

- Assess sensor placement and visibility gaps across segments — SOC leads funding new taps
- Design segmentation zones and internal choke points — network architects approving changes
- Calibrate intrusion detection signatures and thresholds to cut false positives — analyst shift leads
- Build hypothesis-driven hunts on flow, DNS and TLS metadata — threat intelligence owners
-

Apply containment playbooks that isolate hosts without breaking services — incident commanders
- Communicate hunt findings as new detection rules — detection engineering owners

Key Network Threat Hunting and Detection Tuning Terms

- Threat Hunting — A proactive search for adversary activity that existing alerts missed, driven by a testable hypothesis.
- Flow Record — A summary of a network conversation listing endpoints, ports, byte counts and duration, without the packet contents.
- Lateral Movement — Techniques an intruder uses to pivot from one compromised host to others inside the network.
- Beaconing — Regular, timed outbound connections from an infected host to an attacker's command server.
- Signature Tuning — Adjusting detection rules, thresholds and suppressions so alerts fire on real threats rather than benign traffic.
- Microsegmentation — Dividing a network into small zones with explicit allow rules so a breach in one cannot spread freely.

Network Threat Hunting and Detection Tuning Day by Day

Day 1: The Modern Network Attack Surface

- Adversary Technique Knowledge Bases — Mapping Network Behaviours To Attacker Goals
- Encrypted Traffic Realities — What Metadata Still Reveals To Defenders
- Hybrid Estate Visibility Mapping — Locating Blind Spots Between Sites And Cloud
- Dwell Time And Breach Cost Drivers — Why Early Detection Pays Back
- Case Contrasts From Energy And Banking — Lessons From Late Discovery

Day 2: Segmentation and Internal Choke Points

- Zone And Conduit Models — Grouping Assets By Trust And Function
- Microsegmentation Policies — Limiting East-West Paths Between Workloads
- Firewall Rule Base Hygiene — Removing Shadowed And Overly Broad Rules
- Jump Host And Bastion Design — Controlling Administrative Access Routes
- Segmentation Testing — Proving Zones Block What They Should

Day 3: Perimeter and Internal Sensor Architecture

- Tap And Span Placement — Choosing Where Sensors See Most Traffic
- Packet Broker Filtering — Balancing Capture Depth Against Storage Cost
- Proxy And DNS Logging — Capturing Outbound Requests For Later Hunts
- Cloud Traffic Mirroring — Extending Visibility Into Virtual Networks
- Sensor Health Monitoring — Detecting Dropped Packets And Silent Failures

Day 4: Intrusion Detection Tuning

- Signature Rule Anatomy — Reading Conditions, Thresholds And Flow Options
- False Positive Root Cause Review — Deciding To Suppress, Modify Or Keep
- Baseline-Aware Thresholds — Adjusting Alerts To Normal Business Rhythms
- Custom Rule Writing — Encoding Local Threats Into New Detections
- Rule Lifecycle Records — Tracking Changes, Owners And Review Dates

Day 5: Flow and Protocol Telemetry

- Flow Export And Collection — Selecting Fields That Support Investigation
- Protocol Log Analysis — Reading HTTP, DNS And TLS Session Details
- Certificate And Fingerprint Inspection — Spotting Unusual Encrypted Clients
- Traffic Volume Profiling — Separating Backups From Bulk Exfiltration
- Telemetry Retention Planning — Keeping Enough History For Late Hunts

Day 6: Hypothesis-Driven Hunting

- Hunt Hypothesis Framing — Turning Intelligence Into Testable Questions
- Beaconing Detection Methods — Finding Periodic Callbacks In Flow Data
- DNS Tunnelling And Rare Domain Hunts — Exposing Covert Channels
- Lateral Movement Hunts — Tracing Remote Administration And File Share Abuse
- Hunt Documentation Templates — Recording Queries, Findings And Gaps

Day 7: Correlation and Detection Engineering

- Event Correlation Rules — Linking Network Signals With Endpoint Alerts
- Detection As Code Practices — Versioning And Testing Rules Before Release
- Attack Simulation Replays — Validating Detections Against Known Techniques
- Alert Enrichment Pipelines — Adding Asset And Threat Context Automatically
- Coverage Heatmaps — Showing Which Techniques Remain Undetected

Day 8: Containment and Network Response

- Containment Decision Trees — Isolate, Monitor Or Block Choices
- Dynamic Quarantine Controls — Moving Hosts Into Restricted Segments
- Sinkholing And Egress Blocking — Cutting Command Channels Safely
- Network Evidence Preservation — Capturing Packets Before Changes Erase Traces
- Incident Handling Lifecycles — Aligning Containment With Eradication And Recovery

Day 9: Measuring Detection Performance

- Detection Quality Indicators — Precision, Coverage And Time To Detect
- Analyst Workload Modelling — Matching Alert Volume To Shift Capacity
- Purple Team Exercises — Joint Attack And Defence Validation Sessions
- Hunt Outcome Reporting — Turning Findings Into Leadership Decisions
- Healthcare And Manufacturing Examples — Detection Priorities In Sensitive Networks

Day 10: Practising the Network Defence and Hunting Plan

- Visibility Gap Synthesis — Applying Day Three Sensor Reviews To A Case
- Segmentation Change Proposals — Applying Zone Models To A Sample Estate
- Tuning Backlog Prioritisation — Ranking Rule Fixes By Analyst Impact
- Hunt Calendar Design — Scheduling Recurring Hypotheses And Owners
- Network Defence And Hunting Plan — Final Peer-Reviewed Plan For SOC Sign-Off

Applying Network Threat Hunting and Detection Tuning After the Course

- Run a false positive root cause review on the noisiest ten intrusion detection rules and present suppress, modify or keep decisions to the SOC lead.
- Lead one beaconing hunt across a month of flow records, document the queries used and convert any confirmed pattern into a new detection rule.

Network Threat Hunting and Detection Tuning Questions FAQ

What is Network Threat Hunting and Detection Tuning and why does it matter now?

Network Threat Hunting and Detection Tuning is the practice of proactively searching traffic for hidden intruders while calibrating sensors to cut noise. It matters now because encryption, hybrid estates and alert fatigue let attackers stay unnoticed for long periods.

Which roles gain most from Network Threat Hunting and Detection Tuning?

Network security engineers and SOC analysts gain most. That includes sensor engineers, alert triage analysts, segmentation specialists, threat hunters and incident responders who work with packet, flow and protocol records every day.

How does Network Threat Hunting and Detection Tuning differ from a secure network design course?

Network Threat Hunting and Detection Tuning focuses on operating and improving detection rather than building the network. A design course plans architecture; this course concentrates on sensor tuning, telemetry hunts, correlation and containment once the network is running.

What do you bring back from Network Threat Hunting and Detection Tuning training?

You bring back a peer-reviewed plan covering visibility gaps, segmentation changes, a ranked tuning backlog, a recurring hunt calendar and containment steps, ready to present to your SOC leadership.

Network Threat Hunting and Detection Tuning: The Way Forward

The network defence and hunting plan first informs which sensor gaps and noisy rules to fix in the coming quarter. SOC leads, sensor engineers and hunters use it to schedule work and share ownership. After its first use, the perspective worth revisiting is coverage: which adversary techniques still produce no alert once the backlog is cleared.