CONCEPT

Endpoint Security and EDR: Device Hardening, Alert Triage and Host Isolation

14 – 18 June 2027
London - Central London four-star



Endpoint Security and EDR: Device Hardening, Alert Triage and Host Isolation

Ref: 902_21166 **Date:** 14 – 18 June 2027 **Location:** London - Central London four-star **Fees:** 25300 SAR

Introduction:

Endpoint security fails quietly when laptops leave the office unpatched, local administrator rights spread, USB drives carry data out and EDR alerts pile up with nobody sure whether to isolate the device. This Core Concept course gives administrators a vendor-neutral method for protecting laptops, desktops, servers and mobile devices: hardening baselines, patch cadence, application allow-listing, device control, disk encryption and EDR telemetry triage, through to isolating a compromised host and passing a clean case to the SOC. Participants build an Endpoint Security Baseline and EDR Alert Playbook for a case organisation.

Course Objectives:

- Map the endpoint attack surface of an organisation's laptops, desktops, servers and mobile devices and rank exposure by device group
- Configure and verify a secure configuration baseline derived from consensus hardening benchmarks, with documented deviations
- Run an endpoint patch and vulnerability cycle that prioritises fixes by exploitability and asset criticality
- Enforce application allow-listing, device control, disk encryption and least-privilege local administrator rights across device groups
- Triage EDR alerts from process, file, registry and network telemetry, then isolate, remediate and hand confirmed incidents to the SOC
- Produce an Endpoint Security Baseline and EDR Alert Playbook with policies, exceptions and coverage metrics for a case organisation

Target Audience:

- Endpoint and desktop administration functions that build, configure and maintain corporate laptops and workstations
- Server administration functions responsible for agent coverage, hardening and patch status on Windows and Linux hosts
- IT security operations functions that run endpoint protection consoles, policies and exception requests
- Mobile device administration functions that enrol, restrict and wipe smartphones and tablets
- Infrastructure support functions that respond first when an endpoint agent raises a detection

Course Outline:

Day 1: Endpoint Attack Surface and the Protection Stack

- Endpoint Inventory Types: Laptops, Desktops, Servers, Mobile and Virtual Desktops
- Initial Access Paths: Phishing Payloads, Exploited Browsers, Stolen Credentials and USB Media
- EPP, EDR and XDR Layering: Prevention, Detection and Cross-Domain Correlation
- Agent Coverage Gap Analysis: Unmanaged, Offline and Unsupported Operating Systems
- Endpoint Exposure Scorecard for a Mixed Device Estate

Day 2: Hardening Baselines, Secure Configuration and Patch Cadence

- Consensus Hardening Benchmarks: Level Profiles, Scored Controls and Recommended Values
- Baseline Deviation Register: Business Justification, Compensating Controls and Expiry
- Configuration Drift Scanning and Conformance Reporting per Device Group
- Enterprise Patch Management Planning: Identify, Prioritise, Deploy and Verify
- Vulnerability Prioritisation by Exploit Availability, Asset Criticality and Exposure

Day 3: Application Control, Device Control, Encryption and Privilege

- Application Allow-Listing Rules: Publisher, Path and Hash Methods with Audit Mode Rollout
- Device Control Policy for USB Storage, Printers, Bluetooth and Removable Media
- Full-Disk Encryption Deployment, Recovery Key Escrow and Lost Laptop Procedure
- Local Administrator Rights Removal, Just-in-Time Elevation and Rotating Local Passwords
- Mobile Device Enrolment, Compliance Rules, Containerisation and Remote Wipe

Day 4: EDR Telemetry, Alert Triage, Isolation and Remediation

- EDR Telemetry Sources: Process Trees, Command Lines, File Writes, Registry and Network Connections
- Alert Triage Worksheet: True Positive, Benign Positive and False Positive Verdicts
- Host Isolation, Process Kill, File Quarantine and Persistence Removal Actions
- SOC Escalation Package: Timeline, Indicators, Affected Hosts and Actions Taken
- Endpoint Security at Scale: Policy Inheritance, Device Groups, Exclusions and Tuning

Day 5: Lab: Endpoint Security Baseline and EDR Alert Playbook

- Case Organisation Briefing: Device Estate, Business Units and Current Controls
- Lab: Build a Workstation and Server Hardening Baseline with Deviation Register
- Lab: Triage Three Staged EDR Detections from Credential Theft to Ransomware Precursor
- Endpoint Security Metrics Set: Agent Coverage, Patch Latency, Baseline Conformance and Dwell Time
- Endpoint Security Baseline and EDR Alert Playbook Presentation and Peer Review

Skills You Will Gain:

- Endpoint Attack Surface Mapping
- Secure Configuration Baselining
- Endpoint Patch Prioritisation
- Application Allow-Listing
- Removable Media Control
- Privileged Access Reduction
- EDR Alert Triage
- Compromised Host Containment

Why Attend This Course:

- Return with an Endpoint Security Baseline and EDR Alert Playbook built during lab work on a case organisation
- Decide within minutes whether an EDR detection needs isolation, remediation or closure, and record why
- Cut the number of devices running with local administrator rights, unencrypted disks or open USB ports
- Compare endpoint practice with administrators from banking, healthcare, energy and public service device estates

Conclusion:

Endpoints are where most intrusions start and where the evidence of them is recorded. The week moves from mapping the endpoint attack surface and the EPP, EDR and XDR stack, through hardening baselines, deviation handling and patch cadence, to application allow-listing, device control, disk encryption, local privilege and mobile enrolment, then EDR telemetry, alert triage, isolation and SOC escalation. The final day applies each control in the lab and produces an Endpoint Security Baseline and EDR Alert Playbook with a set of coverage and conformance metrics.