



Vulnerability Management Programme and Attack Surface Management Course



Vulnerability Management Programme and Attack Surface Management Course

Introduction:

Vulnerability Management Programme and Attack Surface Management is a 5-day course for security operations, infrastructure and patch management teams that ends with a Vulnerability Management Programme Plan for a case organisation. Organisations carry large backlogs of open scanner findings, miss internet-facing assets that nobody registered and patch by severity score alone, so actively exploited weaknesses stay open for months. Nominees already run scans, own servers or schedule patch cycles, and they work in a lab with scan data, an asset inventory, EPSS feeds and a remediation tracker. CoreConcept Training Center delivers this vulnerability management course as a programme-building exercise.

Course Objectives:

- Define the scope, ownership and governance of a vulnerability management programme using a charter and a RACI matrix
- Reconcile asset inventories and map the external attack surface so that scanning reaches every internal and internet-facing system
- Design authenticated scanning coverage across agents, network scanners and cloud interfaces
- Prioritise findings by combining CVSS, EPSS and KEV catalogue data with asset criticality tiers
- Set remediation SLA tiers, exception approvals and patch orchestration in line with NIST SP 800-40 planning practice
- Report exposure metrics to leadership and produce a Vulnerability Management Programme Plan for a case organisation

Target Audience:

- Security operations staff responsible for running vulnerability scans and triaging findings
 - Infrastructure and server teams responsible for applying patches and configuration fixes
 - Patch and release coordinators responsible for maintenance windows and change approvals
 - Cloud and network engineers responsible for internet-facing services and their exposure
 - IT risk and governance staff responsible for remediation SLAs, exceptions and reporting
-

Course Outline:

Day 1: Vulnerability Management Programme Foundations and Current-State Review

- Vulnerability Management Lifecycle from Identification to Remediation Verification
- CVE, CWE and NVD Records as Programme Data Sources
- Programme Charter, Scope and Asset Ownership Model Definition
- RACI Matrix for Security, IT Operations and System Owners
- Current-State Maturity Assessment of Scanning and Patching Practice

Day 2: Asset Discovery, Attack Surface Mapping and Scanning Architecture

- Asset Inventory Reconciliation Across CMDB, Cloud and Directory Sources
- External Attack Surface Mapping of Domains, Certificates and IP Ranges
- Authenticated Versus Unauthenticated Scanning Coverage and Credential Handling
- Agent-Based, Network and Cloud API Scanner Placement Design
- SBOM and Software Composition Data for Third-Party Components

Day 3: Risk-Based Prioritisation and Remediation Workflow

- CVSS Base Scores Versus Environmental and Threat Context
- EPSS Exploitation Probability Scores for Remediation Ranking
- KEV Catalogue Matches as Fast-Track Remediation Triggers
- Asset Criticality Tiers and Business Context Weighting Model
- Remediation Ticket Routing to Owning Teams Through Service Management

Day 4: Patch Orchestration, Exceptions and Continuous Exposure Management

- NIST SP 800-40 Enterprise Patch Management Planning Practice
- Patch Rings, Maintenance Windows and Rollback Plan Design
- Remediation SLA Tiers and Risk Exception Approval Workflow
- Compensating Controls for Legacy and Unpatchable Systems
- CTEM Scoping, Discovery, Prioritisation, Validation and Mobilisation Stages

Day 5: Lab Case Work and the Vulnerability Management Programme Plan

- Lab Case Asset Inventory and External Exposure Register Build
 - Lab Case Prioritised Remediation Queue Using CVSS, EPSS and KEV
 - Lab Case SLA and Exception Register Drafting Exercise
 - Exposure Metrics Dashboard with Mean Time to Remediate
 - Vulnerability Management Programme Plan Completion and Peer Review
-

Skills You Will Gain:

- Asset Inventory Reconciliation
- External Attack Surface Mapping
- Authenticated Scan Design
- Exploit-Likelihood Prioritisation
- Remediation SLA Governance
- Patch Ring Planning
- Risk Exception Handling
- Exposure Metrics Reporting

Why Attend This Course:

- Deliver a Vulnerability Management Programme Plan to the chief information security officer and the head of IT operations, setting scope, SLA tiers and metrics
- Decide which findings to fast-track, schedule for the next patch ring or accept under a documented exception
- Avoid breaches through exploited weaknesses left open on unregistered internet-facing assets
- Coach infrastructure and application teams on reading prioritised queues and meeting remediation SLA tiers

Conclusion:

Back at work, the participant presents the Vulnerability Management Programme Plan to the chief information security officer and the head of IT operations, who use it to approve scanning scope, remediation SLA tiers and the exception process before the next patch cycle. Asset owners then receive prioritised remediation queues instead of raw scanner exports. After the first monthly reporting cycle, the unit should review mean time to remediate, scan coverage and open exceptions against the plan and adjust any threshold that produced too many or too few fast-track items.

Frequently Asked Questions FAQ:

What should participants know before a vulnerability management programme and attack surface management course?

Participants should understand networking, operating systems and how patches are deployed in their organisation. Experience running a scanner or handling remediation tickets helps. No coding is needed, and the first day reviews CVE, CWE and NVD records before programme design begins.

How does a vulnerability management programme and attack surface management course differ from a penetration testing course?

This course builds the continuous process of discovering assets, scanning, prioritising and patching across the whole estate. A penetration testing course runs a time-boxed, authorised attack against a defined scope to show how weaknesses can be exploited, then reports those findings.

Why does a vulnerability management programme combine EPSS and KEV catalogue data with CVSS scores?

CVSS rates technical severity, not the likelihood of attack. EPSS estimates the probability that a vulnerability will be exploited, and the KEV catalogue lists vulnerabilities already exploited in the wild. Combining them lets teams fix the findings that matter first.

What do participants take back from the vulnerability management programme and attack surface management course?

Participants take back a Vulnerability Management Programme Plan: an asset and external exposure register, a prioritisation model, remediation SLA tiers with an exception register, a patch ring schedule and a leadership metrics set, ready for review by security and IT operations leaders.
