CONCEPT

Cybersecurity Fundamentals, Threat Detection and Incident Response Training

21 – 25 November 2027
Riyadh - KAFD district five-star



Cybersecurity Fundamentals, Threat Detection and Incident Response Training

Ref: 1610_25698 **Date:** 21 – 25 November 2027 **Location:** Riyadh - KAFD district five-star **Fees:** 21450 SAR

Introduction:

Cybersecurity fundamentals, threat detection and incident response are the focus of this 1-week course for IT support, infrastructure and junior security staff, ending with a Security Baseline and Incident Response Starter Pack. Organisations lose time and data when basic controls are inconsistent, vulnerabilities stay unpatched and the first hour of an incident is handled without a clear procedure. Nominees already maintain systems, networks or user accounts but have little formal security training, and teaching is by hands-on lab with scanners, log tools and packet captures. CoreConcept Training Center delivers this cybersecurity fundamentals course.

Course Objectives:

- Explain common threats, attack techniques and security principles using NIST CSF 2.0 and MITRE ATT&CK terminology
- Select and apply baseline security controls for identities, networks, endpoints and web applications using CIS Controls v8.1
- Run vulnerability scans, interpret the findings and prioritise remediation with CVSS v4.0 scores
- Collect and examine endpoint logs and network traffic to identify suspicious activity
- Triage security alerts and carry out first-response containment following NIST SP 800-61 Rev. 3
- Produce a Security Baseline and Incident Response Starter Pack for the participant's own unit

Target Audience:

- IT support and infrastructure staff who maintain servers, endpoints and user accounts
- System and network administrators responsible for configuration, patching and access rights
- Junior security and monitoring staff who review alerts and escalate incidents
- Technical staff moving into security work from development, operations or service desk functions
- IT compliance and audit support staff who gather evidence that security controls operate

Course Outline:

Day 1: Threat Landscape, Security Principles and Asset Context

- CIA Triad and Defence in Depth Security Principles
- Threat Actor Types and Motivations Mapped to Attack Surface
- MITRE ATT&CK Overview of Phishing, Ransomware and Credential Theft
- NIST CSF 2.0 Functions for Organisational Security Posture
- CIS Controls v8.1 Asset Inventory and Data Classification

Day 2: Security Controls and Defensive Architecture

- CIS Controls v8.1 Implementation Groups and Safeguard Selection
- Identity and Access Management with Multi-Factor Authentication Enforcement
- Network Segmentation, Firewall Rules and Secure Remote Access Design
- Endpoint Protection, Hardening Baselines and Patch Policy Setting
- OWASP Top 10 Web Application Risks and Basic Defences

Day 3: Vulnerability Management and Security Monitoring

- Nmap Network Discovery and Open Port Enumeration
- OpenVAS Greenbone Vulnerability Scanning and Results Interpretation
- CVSS v4.0 Scoring for Vulnerability Prioritisation and Remediation
- Windows Event Viewer and Sysmon Log Collection
- Wireshark Packet Capture Analysis of Suspicious Traffic

Day 4: Threat Detection and Incident Response

- SIEM Search Queries for Alert Triage and Correlation
- Indicators of Compromise Identification in Logs and Endpoints
- NIST SP 800-61 Rev. 3 Incident Response Lifecycle and Roles
- Containment, Eradication and Recovery Steps for Ransomware Incidents
- Evidence Preservation and Incident Ticket Documentation Practice

Day 5: Lab Practice and the Security Baseline and Incident Response Starter Pack

- Lab Vulnerability Scan and Remediation Priority List Build
- Lab Phishing Incident Detection from Email Headers and Logs
- Lab Ransomware Containment Exercise Following a Response Checklist
- Post-Incident Review Using a Lessons Learned Template
- Security Baseline and Incident Response Starter Pack Completion

Skills You Will Gain:

- Threat Landscape Awareness
- Security Control Selection
- Vulnerability Prioritisation
- Endpoint Log Analysis
- Network Traffic Analysis
- Alert Triage
- Incident Containment
- Security Documentation

Why Attend This Course:

- Deliver a Security Baseline and Incident Response Starter Pack to the IT manager and the information security lead
- Decide whether an alert or scan finding needs immediate containment, a scheduled patch or escalation to specialists
- Avoid unpatched exposures, excessive access rights and a slow first response that turn minor events into costly outages
- Coach colleagues in IT support and operations on reporting suspicious activity and following the first-response checklist

Conclusion:

Back at work, the participant presents the Security Baseline and Incident Response Starter Pack to the IT manager and the information security lead, who use it to agree which baseline controls to enforce first, which vulnerabilities to remediate in the next patch cycle and who acts in the first hour of an incident. Support and operations teams use its checklists to report and contain suspicious activity consistently. After the first real alert or scheduled scan, the unit should review response times and remediation progress against the pack and update any checklist that did not work.

Frequently Asked Questions FAQ:

What should participants know before a cybersecurity fundamentals and incident response course?

Participants should be comfortable with operating systems, user accounts and basic networking such as IP addresses and ports. No previous security role is needed. Experience administering servers, endpoints or network devices helps participants move quickly through the lab exercises.

How does a cybersecurity fundamentals and incident response course differ from an advanced threat hunting course?

It builds the baseline: security principles, core controls, vulnerability scanning, log reading and first response. Advanced threat hunting and security operations courses assume this base and concentrate on hunting adversaries, writing detection rules and sharing intelligence within a mature monitoring team.

Why does threat detection depend on cybersecurity fundamentals such as asset inventory and logging?

Detection only works on what is known and recorded. Without an asset inventory, unknown devices go unmonitored, and without collected logs there is no evidence to search when an alert fires. Fundamentals therefore decide how quickly an incident is detected and contained.

What do participants take back from the cybersecurity fundamentals and incident response course?

Participants take back a Security Baseline and Incident Response Starter Pack: a prioritised control checklist, a vulnerability remediation list, a log review routine and a first-response checklist for common incidents, ready for review by their IT manager and security lead.