Endpoint Security Professional

Official Course Syllabus

Duration: **4 Weeks** | Live Instructor-led | Hands-on Labs | Capstone Project

Course Overview

Master enterprise endpoint protection using Microsoft Defender for Endpoint and CrowdStrike Falcon. Learn endpoint security, EDR/XDR, threat hunting, incident response and endpoint hardening through hands-on enterprise labs.

Module 1 – Endpoint Security Fundamentals

- Introduction to Endpoint Security
- Endpoint Protection Platform (EPP)
- Endpoint Detection & Response (EDR)
- Extended Detection & Response (XDR)
- Common Endpoint Threats
- MITRE ATT&CK; Framework
- Enterprise Endpoint Security Architecture
- Hands-on: Windows Security Overview, Event Viewer

Module 2 – Windows Security Fundamentals

- Windows Security Architecture
- Windows Registry
- Windows Services
- User Account Control
- Windows Firewall
- BitLocker
- Secure Boot
- Microsoft Defender Antivirus

Module 3 – Endpoint Detection & Response (EDR)

- Endpoint Telemetry
- Detection Techniques
- Behavioral Analytics
- IOC vs IOA
- Detection Workflow

Module 4 – Microsoft Defender for Endpoint

- Microsoft Defender Portal
- Device Inventory
- Vulnerability Management
- Live Response
- Advanced Hunting (KQL)
- Threat Analytics
- Device Isolation

Module 5 – CrowdStrike Falcon

- Falcon Platform
- Sensor Deployment
- Host Management
- RTR
- Falcon Intelligence
- Threat Investigation

Module 6 – Threat Hunting & Incident Response

- Threat Hunting
- Threat Intelligence
- KQL
- Containment
- Recovery
- MITRE ATT&CK;
- Ransomware Investigation

Module 7 – Endpoint Hardening & Enterprise Security

- CIS Benchmarks
- Microsoft Security Baselines
- ASR Rules
- Application Control
- USB Restrictions
- Patch Management
- Endpoint Compliance
- Zero Trust for Endpoints

Module 8 – Capstone Project

- Deploy Microsoft Defender for Endpoint
- Investigate Malware
- Threat Hunting
- Incident Response

- Executive Security Report

Tools Covered

Microsoft Defender for Endpoint, Microsoft Defender XDR, CrowdStrike Falcon, PowerShell, Event Viewer, Sysinternals Suite, Microsoft Security Portal.

Career Opportunities

- Endpoint Security Engineer
- Microsoft Security Engineer
- SOC Analyst
- Security Operations Engineer
- Cybersecurity Analyst
- Blue Team Analyst
- Endpoint Administrator