Microsoft Defender for Endpoint and Intune Deep Dive

Duration: 32 hours

Day 1: Endpoint Security Foundations & Defender for Endpoint Core

Module 1: Microsoft Defender for Endpoint

- Role and Capabilities
- Architecture
- Threat Detection Capabilities
- Additional Benefits
- Requirements and Onboarding Steps
- Managing Defender for Endpoint Features
- Troubleshooting

Module 2: Threat & Vulnerability Management (LAB)

- Next-gen Threat Capabilities
- Dashboard Overview
- Understanding Configuration Score
- Threat Exposure Scenarios
- Reducing Threat Exposure
- Improving Security Configuration

Day 2: Attack Surface & Response Mechanisms

Module 3: Attack Surface Reduction (LAB)

- Hardware-based Isolation
- Application Isolation
- System Integrity & Requirements
- Application Control
- Exploit Protection & Network Protection
- Credential Guard
- Controlled Folder Access
- Attack Surface Reduction Rules
- Network Firewall Configuration

Module 4: Endpoint Detection and Response (LAB)

- Security Operations Dashboard
- Incident & Alert Management
- Managing Machine Groups & Tags
- Response Actions: AV Scan, Restrict Apps, Action Center
- Quarantining and Stopping Malicious Files

Day 3: Automation, Hunting & Intune Integration

Module 5: Automated Investigation and Remediation (LAB)

- Investigation Overview
- Investigation Flow and Expansion
- Threat Remediation Details

Module 6: Advanced Hunting

- Introduction to KQL and Hunting Interface
- Writing Queries and Exploring Schema
- Hunting Best Practices
- Creating and Managing Custom Detection Rules

Module 7: Intune Device Enrollment

- Benefits and Prerequisites for Co-management
- Azure AD Join Concepts
- Overview of Microsoft Intune
- Device Enrollment and Inventory Management
- Practice Lab: Device Enrollment and Management

Day 4: Device & Identity Management with Intune

Module 8: Configuring Profiles

- Device Profile Types
- Built-in vs. Custom Profiles
- Profile Assignment to Azure AD Groups
- Monitoring Devices and Reporting
- Practice Lab: Managing Profiles

Module 9: Managing Authentication in Azure AD

- Azure AD Overview
- Identity and Directory Synchronization
- Identity Protection (MFA, Hello for Business)
- Managing Device Authentication
- Practice Lab: Azure AD Object & Authentication Management

Module 10: Managing Device Access and Compliance

- Compliance Policies and Conditional Access
- Always On VPN and Secure Resource Access
- Monitoring Devices
- Practice Lab: Access & Compliance Management

Module 11: Integration with SCCM (Demo Only)

- SCCM Roles and Agents
- Defender and Intune Policy Integration
- Demo and Q&A