

KOENIG SOLUTIONS • COURSE OUTLINE

Defender for Endpoint & Intune: EDR & KQL Hunting

Learn to deploy Defender for Endpoint, hunt threats with KQL, and manage devices with Intune.

4 Days

32 HOURS

11

MODULES

51

TOPICS

4

HANDS-ON ACTIVITIES

COURSE OVERVIEW

This course covers Microsoft Defender for Endpoint, including its architecture, threat and vulnerability management, attack surface reduction, and endpoint detection and response. It then addresses automated investigation and remediation, advanced hunting with KQL, and creating custom detection rules. The course also covers Intune device enrollment, configuring device profiles, managing authentication in Azure AD, and managing device access and compliance, concluding with integration between Defender, Intune, and SCCM.

WHO THIS COURSE IS FOR

Security Operations Analysts

Endpoint Security Engineers

Systems Administrators

Intune Administrators

Identity and Access Administrators

LEARNING OBJECTIVES

- Explain the architecture and capabilities of Defender for Endpoint
- Identify and reduce threat exposure using vulnerability management tools
- Configure attack surface reduction features such as Application Control
- Manage incidents, alerts, and response actions in the security dashboard
- Analyse automated investigations and threat remediation details
- Write KQL queries and create custom detection rules for hunting
- Plan Intune device enrollment and co-management with Azure AD
- Configure device profiles and compliance policies in Intune

11 Modules, 51 Topics

DAY 1**Endpoint Security Foundations & Defender for Endpoint Core****01****Microsoft Defender for Endpoint****TOPICS**

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

02**Threat & Vulnerability Management (LAB)****TOPICS**

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

DAY 2**Attack Surface & Response Mechanisms****03****Attack Surface Reduction (LAB)****TOPICS**

- 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

04**Endpoint Detection and Response (LAB)****TOPICS**

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

05

Automated Investigation and Remediation (LAB)

TOPICS

Investigation Overview · Investigation Flow and Expansion · Threat Remediation Details

06

Advanced Hunting

TOPICS

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

07

Intune Device Enrollment

Practice Lab

TOPICS

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

08

Practice Lab

Configuring Profiles

TOPICS

Device Profile Types · Built-in vs. Custom Profiles · Profile Assignment to Azure AD Groups · Monitoring Devices and Reporting

09

Practice Lab

Managing Authentication in Azure AD

TOPICS

Azure AD Overview · Identity and Directory Synchronization · Identity Protection (MFA, Hello for Business) · Managing Device Authentication

10

Practice Lab

Managing Device Access and Compliance

TOPICS

Compliance Policies and Conditional Access · Always On VPN and Secure Resource Access · Monitoring Devices

11

Integration with SCCM (Demo Only)

TOPICS

SCCM Roles and Agents · Defender and Intune Policy Integration

Practise What You Learn

#	MODULE	ACTIVITY
07	Intune Device Enrollment	Device Enrollment and Management
08	Configuring Profiles	Managing Profiles
09	Managing Authentication in Azure AD	Azure AD Object & Authentication Management
10	Managing Device Access and Compliance	Access & Compliance Management

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

[Visit koenig-solutions.com](https://www.koenig-solutions.com)[✉ info@koenig-solutions.com](mailto:info@koenig-solutions.com)