

KOENIG SOLUTIONS • COURSE OUTLINE

Microsoft Defender Endpoint

Learn to deploy and manage Microsoft Defender ATP alongside Intune and Azure AD to detect, investigate and remediate threats.

11

MODULES

60

TOPICS

11

HANDS-ON ACTIVITIES

COURSE OVERVIEW

This course covers Windows Defender ATP, including its architecture, capabilities and management, followed by Threat and Vulnerability Management and Attack Surface Reduction features such as application isolation, exploit protection and network firewall. It then addresses Endpoint Detection and Response, Automated Investigation and Remediation, and Advanced Hunting using custom detection rules. The course continues with Intune device enrollment, configuring device profiles, managing authentication and identity protection in Azure AD, and managing device access and compliance policies. It concludes with integration between Microsoft Defender ATP, Intune and SCCM roles and agents.

WHO THIS COURSE IS FOR

Security Operations Analysts

Endpoint Administrators

Identity Administrators

Systems Administrators

IT Security Engineers

LEARNING OBJECTIVES

- Explain the role and architecture of Windows Defender ATP
- Configure Threat and Vulnerability Management to reduce exposure
- Implement Attack Surface Reduction controls such as network protection
- Manage incidents, alerts and response actions in EDR
- Describe how Automated Investigation and Remediation handles threats
- Apply Advanced Hunting queries and create custom detection rules
- Configure Intune device enrollment and device profiles
- Manage identity protection and device compliance in Azure AD

11 Modules, 60 Topics

01

Windows Defender ATP

TOPICS

- The Role of Windows Defender ATP
- Windows Defender ATP Architecture
- How Windows Defender ATP helps detect sophisticated threats?
- What Else Can Windows Defender ATP Do for Us?
- Requirements and initial steps
- Manage Windows Defender ATP capabilities
- Troubleshoot Windows Defender ATP

02

Threat & Vulnerability Management

LAB

TOPICS

- Next-generation capabilities
- Dashboard Overview and what it means for my organization
- Configuration score
- Scenarios
- Reduce your Threat and Vulnerability Exposure Tamp
- Improve your Security Configuration

03

Attack Surface Reduction

LAB

TOPICS

- Hardware-based isolation
- Application isolation
- System requirements
- System integrity
- Application control
- Exploit protection
- Network protection
- Controlled folder access
- Credential Guard
- Attack surface reduction
- Network firewall

04**LAB**

Endpoint Detection and Response

TOPICS

- Security operations dashboard
- Manage incidents
- Manage alerts
- Manage machine group and tags
- Take response actions on a machine
- Run antivirus scan
- Restrict app execution
- Check activity details in Action center
- Stop and quarantine files in your network

05**LAB**

Automated Investigation and Remediation

TOPICS

- Overview of Automated investigations
- Understand the Automated investigation flow
- Details of an Automated investigation
- How an Automated investigation expands its scope
- How threats are remediated

06

Advanced Hunting

TOPICS

- Overview of advanced hunting
- Query data using Advanced hunting
- Advanced hunting reference
- Advanced hunting query language best practices
- Custom detections
- Create custom detections rules

07**Practice Lab**

Intune Device Enrollment

In this module, students will examine the benefits and prerequisites for co-management and learn how to plan for it. This module will also cover Azure AD join and will be introduced to Microsoft Intune, as well as learn how to configure policies for enrolling devices. The module will conclude with an overview of device inventory in Intune and reporting using the Intune console, Power BI and Microsoft Graph.

TOPICS

Device management and Tamper Protection · Microsoft Intune Overview · Manage Intune device enrollment and inventory · Managing devices with Intune

08**Practice Lab**

Configuring Profiles

This module dives deeper into Intune device profiles including the types of device profiles and the difference between built-in and custom profiles. The student will learn about assigning profiles to Azure AD groups and monitoring devices and profiles in Intune. The module will conclude with an overview of using Windows Analytics for health and compliance reporting.

TOPICS

- Configuring and controlling device by using profiles
- Managing user profiles
- Monitoring devices

09**Practice Lab**

Managing Authentication in Azure AD

In this module, students will be introduced to the concept of directory in the cloud with Azure AD. Students will learn the similarities and differences between Azure AD and Active Directory DS and how to synchronize between the two. Students will explore identity management in Azure AD and learn about identity protection using Windows Hello for Business, as well as Azure AD Identity Protection and multi-factor authentication.

TOPICS

Azure AD Overview · Managing identities in Azure AD · Protecting identities in Azure AD · Managing device authentication

10**Practice Lab**

Managing Device Access and Compliance

In this module, students will be introduced to managing device security. The module will cover securely accessing corporate resources and introduce concepts such as Always On VPN and remote connectivity in Windows 10. Students will learn how to create and deploy compliance policies and use compliance policies for conditional access. The module concludes with monitoring devices enrolled in Intune.

TOPICS

Microsoft Intune Overview · Implement device compliance policies

11**3 Demo Onlies**

Integration with SCCM

TOPICS

- Understanding SCCM Roles
- Understanding SCCM Agents
- Defender ATP and Intune based Policy Integration

Practise What You Learn

#	MODULE	ACTIVITY
02	Threat & Vulnerability Management	LAB: Threat & Vulnerability Management
03	Attack Surface Reduction	LAB: Attack Surface Reduction
04	Endpoint Detection and Response	LAB: Endpoint Detection and Response
05	Automated Investigation and Remediation	LAB: Automated Investigation and Remediation
07	Intune Device Enrollment	Practice Lab: Device Enrollment and Management
08	Configuring Profiles	Practice Lab: Managing profiles
09	Managing Authentication in Azure AD	Practice Lab: Managing objects and authentication in Azure AD
10	Managing Device Access and Compliance	Practice Lab: Managing Access and Compliance
11	Integration with SCCM	DEMO ONLY ■ Understanding SCCM Roles ■ Understanding SCCM Agents ■ Defender ATP and Intune based Policy Integration

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

✉ info@koenig-solutions.com