Enhance endpoint security with Microsoft Intune and Microsoft Security Copilot (MD-4011)

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

This course is designed for Endpoint Administrators and Security Analysts proficient in basic device management and security operations.

Training objectives

By

the end of this course, students will be able to:

- Configure Microsoft Entra ID roles, licensing, and tenant settings for device management
- Enroll and validate devices across Windows, iOS, iPadOS, and Android platforms
- Create and deploy configuration profiles and compliance policies using Microsoft Intune
- Implement app protection policies and conditional access for data loss prevention
- Deploy security baselines and onboard devices to Microsoft Defender for Endpoint
- Configure attack surface reduction rules and monitor security posture
- Leverage Microsoft Security Copilot for AI-powered incident investigation and device troubleshooting

Summary

This Course will empower IT professionals and security analysts with the expertise to utilize Microsoft Intune and Microsoft Security Copilot effectively in device management and security operations. This course directs learners towards optimizing Intune for enhanced security and integrating Security Copilot to strengthen their organization's security stance.

Course outline

Learning Path 1: Enhance endpoint security with Microsoft Intune and Microsoft Security Copilot

- Module 1: Prepare Microsoft Entra ID and Intune for device management
- Module 2: Enroll and validate devices with Microsoft Intune
- Module 3: Configure and secure devices with Microsoft Intune policies
- Module 4: Protect data and control access with Microsoft Intune and Conditional Access
- Module 5: Harden endpoints and monitor security with Microsoft Intune and Defender for Endpoint
- Module 6: Accelerate endpoint remediation and response with Microsoft Security Copilot

Approach and methodology

Practical and structured approach combining focused theory with guided security oriented workshops. Participants progressively strengthen their expertise in endpoint protection by applying Microsoft Intune and Microsoft Security Copilot to real world operational scenarios.

Through hands on exercises, they learn how to optimize device security configurations, analyze relevant security signals, and integrate Copilot into incident investigation workflows to enhance response efficiency.

Led by a Microsoft Certified Trainer (MCT), the training emphasizes interactivity, practical demonstrations, and the development of immediately transferable skills for modern endpoint security operations.

Prerequisites

Students

should have the following knowledge and experience before attending this course:

- Strengthen endpoint security using Microsoft Intune’s advanced configuration and compliance capabilities
-

Integrate Microsoft Security Copilot into endpoint security workflows to enhance incident analysis and response

- Optimize Intune policies to improve device protection and reduce organizational risk
- Analyze security signals and alerts relevant to endpoint protection using Microsoft 365 security tools

  A
- pply Zero Trust principles to device management and endpoint hardening strategies
- Use Security Copilot to investigate threats, summarize incidents, and generate actionable security insights
- Implement secure device onboarding and lifecycle management aligned with organizational security requirements
- Evaluate and improve an organization’s endpoint security posture using Intune and Copilot driven recommendations

Recommendations

- Basic understanding of IT security principles.
- Familiarity with Microsoft Intune.
- Experience managing devices in an enterprise environment.
- Knowledge of Microsoft Entra ID.
- Access to Microsoft Intune and Copilot tools for security for hands-on exercises