Defend against Cyberthreats with Microsoft Defender XDR (SC-5004)

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

- IT Security Professionals
- Security Operations Center (SOC) Analysts
- System and Network Administrators
- Cybersecurity Engineers
- Information Technology Professionals
- Security Consultants

Training objectives

- Understand Microsoft Defender XDR
- Threat detection and investigation
- Configure and manage Defender solutions
- Incident response techniques
- Integration with security operations
- Use advanced threat protection features
- Implement best practices

Summary

Deploy Microsoft Defender for Endpoint to manage devices, investigate endpoints, manage incidents with Defender XDR, and use Advanced Hunting with Kusto Query Language (KQL) to detect specific threats.

Course outline

- Mitigate incidents using Microsoft Defender
- Deploy Microsoft Defender for Endpoint environment

Copyright © 2026 AFI by Edgenda inc.

- Configure alerts and detections in Microsoft Defender for Endpoint
- Configure and manage automation using Microsoft Defender for Endpoint
- Perform device investigations in Microsoft Defender for Endpoint
- Defend against cyber threats with Microsoft Defender XDR lab exercises

Approach and methodology

Practical and structured approach combining focused theory and guided workshops.

Participants gradually protect themselves against cyber threats with Microsoft Defender XDR through real-world exercises inspired by professional scenarios, promoting immediate application of learnings. They learn how to detect, analyze, and respond to security incidents using a unified platform for extended protection and response.

Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to strengthen the security of environments in a professional context.

Prerequisites

- Experience using the Microsoft Defender portal
- Basic understanding of Microsoft Defender for Endpoint
- Basic understanding of Microsoft Sentinel
- Experience using the Kusto query language (KQL) in Microsoft Sentinel

Recommendations

Review:

- The basics of cybersecurity
- Common types of threats and attacks

Become familiar with:

- The Microsoft ecosystem (Microsoft 365, security)

Copyright © 2026 AFI by Edgenda inc.

Identify your needs:

- Threat detection
- Protection of users and systems
- Improvement of security posture

Copyright © 2026 AFI by Edgenda inc.