# Defend against cyberthreats with Microsoft Defender XDR (SC-5004)

## Description

### Protect Your Organization Against Cyber Threats

Cyberattacks are becoming increasingly sophisticated and can compromise your company’s security in an instant. Mastering detection and incident response tools is essential to ensure effective protection. With the SC-5004 training, you will learn how to use Microsoft Defender XDR to monitor, analyze, and neutralize threats in real time.

### Master Microsoft Defender XDR and Enhance Your Security

This training enables you to deploy and configure Microsoft Defender for Endpoint, investigate alerts, and automate incident response. You will discover how to manage devices, analyze logs, and use the Kusto Query Language (KQL) to identify targeted attacks. Through structured learning and hands-on exercises, you will develop operational cybersecurity skills.

Designed for security analysts, this in-depth training will equip you with the knowledge to fully leverage Microsoft Defender and strengthen your organization’s resilience against cyber threats.

**Course Content**
**Module 1: Mitigate incidents using Microsoft Defender**

- Use the Microsoft Defender portal
- Manage incidents and investigate alerts
- Investigate incidents with Microsoft Defender XDR
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics and reports
- Configure the Microsoft Defender portal

**Module 2: Deploy the Microsoft Defender for Endpoint environment**

- Create and configure the security environment
- Understand operating systems compatibility and features
- Onboard and manage devices
- Manage access and roles
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features

**Module 3: Configure for alerts and detections in Microsoft Defender for Endpoint**

- Configure advanced security features
- Manage alert notifications
- Administer alert suppression
- Enable and manage detection indicators

**Module 4: Configure and manage automation using Microsoft Defender for Endpoint**

- Configure automation settings in Microsoft Defender
- Manage automation upload and folder settings
- Configure automated investigation and remediation
- Block high-risk devices

**Module 5: Perform device investigations in Microsoft Defender for Endpoint**

- Use the device inventory list
- Investigate device behavior and security risks
- Apply behavioral blocking techniques
- Detect and manage devices through device discovery

**Module 6: Defend against cyber threats with Microsoft Defender XDR**

- Configure the Microsoft Defender XDR environment
- Deploy Microsoft Defender for Endpoint
- Mitigate attacks using Microsoft Defender for Endpoint

**Lab / Exercises**

- Ce cours vous donne un accès exclusif au laboratoire officiel Microsoft, vous permettant de mettre en pratique vos compétences dans un environnement professionnel.

**Documentation**

- Accès à Microsoft Learn, la plateforme d'apprentissage en ligne Microsoft, offrant des ressources interactives et des contenus pédagogiques pour approfondir vos connaissances et développer vos compétences techniques.

**Participant profiles**

- Security operations analysts
- Cybersecurity experts
- System and network administrators
- Incident management professionals

**Prerequisites**

- Experience with the Microsoft Defender portal
- Basic knowledge of Microsoft Defender for Endpoint
- Fundamental understanding of Microsoft Sentinel

**Objectives**

- Use the Microsoft Defender portal to manage incidents
- Deploy and configure Microsoft Defender for Endpoint
- Set up alerts and threat detections

- Automate incident and device management
- Analyze threats and leverage connection logs
- Use Kusto Query Language (KQL) to investigate attacks

**Description**
Defend against cyberthreats with Microsoft Defender XDR (SC-5004)
**Niveau**
Intermédiaire
**Classroom Registration Price (CHF)**
900
**Virtual Classroom Registration Price (CHF)**
850
**Duration (in Days)**
1
**Reference**
SC-5004