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

ID SC-5004 **Price** on request **Duration** 1 day

Prerequisites

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

You'll need to have access to a Microsoft 365 E5 Tenant with a Microsoft Defender for Endpoint P2 license to perform the exercises.

Course Content

Mitigate incidents using Microsoft Defender

Learn how the Microsoft Defender portal provides a unified view of incidents from the Microsoft Defender family of products.

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

Deploy the Microsoft Defender for Endpoint environment

Learn how to deploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security.

- Introduction
- Create your environment
- Understand operating systems compatibility and features
- Onboard devices
- Manage access
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features
- Knowledge check
- Summary and resources

Configure for alerts and detections in Microsoft Defender for Endpoint

Learn how to configure settings to manage alerts and notifications. You'll also learn to enable indicators as part of the detection process.

- Introduction
- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators
- Knowledge check
- Summary and resources

Configure and manage automation using Microsoft Defender for Endpoint

Learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.

- Introduction
- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices
- Knowledge check
- Summary and resources

Perform device investigations in Microsoft Defender for Endpoint

Microsoft Defender for Endpoint provides detailed device information, including forensics information. Learn about information available to you through Microsoft Defender for Endpoint that aids in your investigations.

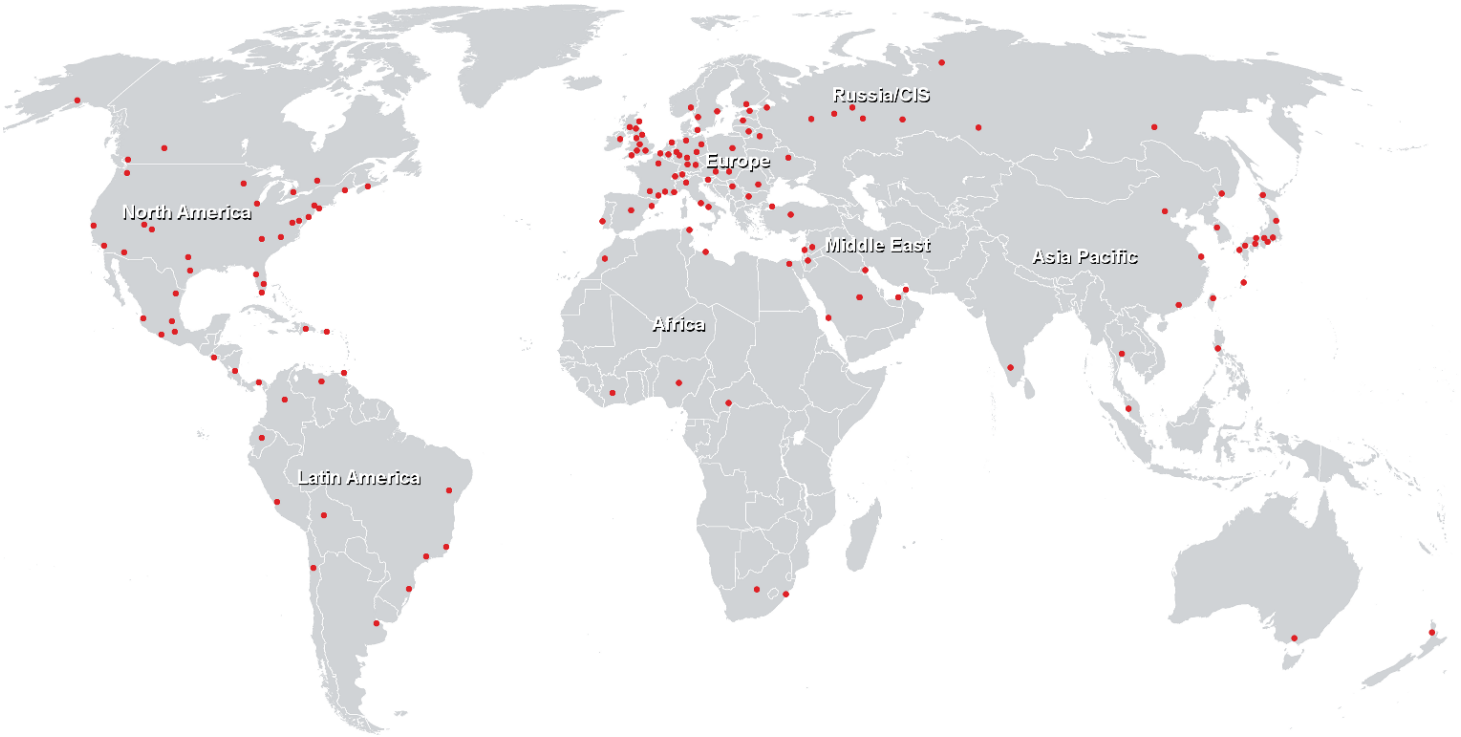
- Introduction
- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery
- Knowledge check
- Summary and resources

Defend against Cyberthreats with Microsoft Defender XDR lab exercises

In this module, you learned how to configure Microsoft Defender XDR, deploy Microsoft Defender for Endpoint, and onboard devices. You also configured policies, mitigated threats and responded to incidents with Defender XDR.

- Introduction
- Configure the Microsoft Defender XDR environment
- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks with Microsoft Defender for Endpoint
- Summary

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch