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

ID SC-5004 **Price** CHF 690.—(excl. VAT) **Duration** 1 days

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

Course Content

Mitigate incidents using Microsoft Defender

- 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 with the Security Copilot Threat Intelligence Briefing Agent
- Analyze reports
- Configure the Microsoft Defender portal
- Module assessment
- Summary and resources

Deploy the Microsoft Defender for Endpoint environment

- 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
- Module assessment
- Summary and resources

Configure for alerts and detections in Microsoft Defender for Endpoint

- Introduction
- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators
- Module assessment
- Summary and resources

Configure and manage automation using Microsoft Defender for Endpoint

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

Perform device investigations in Microsoft Defender for Endpoint

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

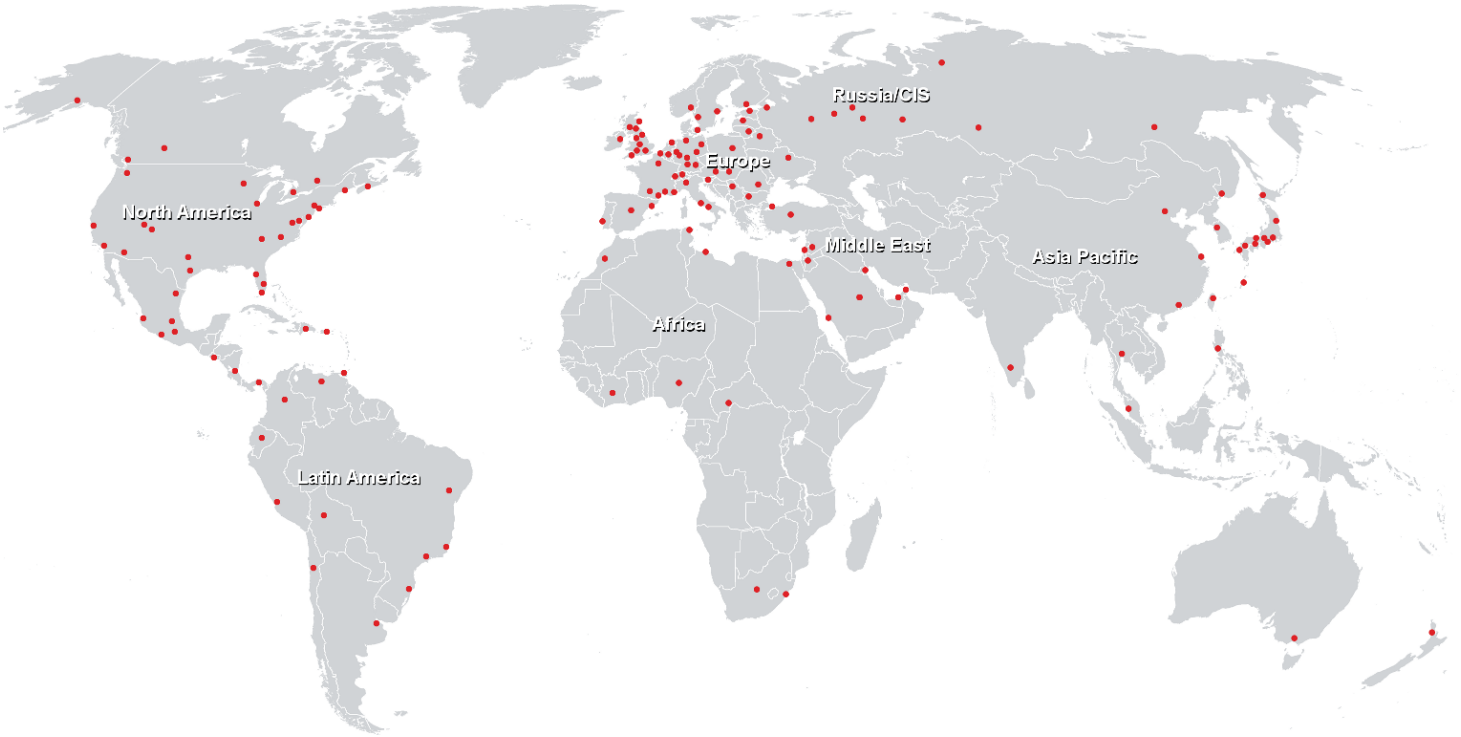
Defend against Cyberthreats with Microsoft Defender XDR lab exercises

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

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

Microsoft Solutions Partner
Microsoft Cloud Training Services

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