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

ID SC-5004 **Price** 690.— €(excl. tax) **Duration** 1 day

Course Overview

Implement the Microsoft Defender for Endpoint environment to manage devices, perform investigations on endpoints, manage incidents in Defender XDR, and use Advanced Hunting with Kusto Query Language (KQL) to detect unique threats.

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

About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Worldwide Presence
with high-end training centers around the globe

Multiple Awards
from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

Experienced SMEs
with over 19.000 combined certifications

Germany
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Austria
ITLS GmbH
(Partner of Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Switzerland
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch