Master Class: Microsoft Defender for Endpoint (MDE)

ID MDE **Price** 3,995.— €(excl. tax) **Duration** 4 days

Course Overview

Users must access and work with a lot of files and applications in their daily business. To do this, they use devices that are in turn attacked by attackers very often. To prevent the success of these attacks, administrators have to deploy many security settings and also have to monitor activities.

Microsoft Defender for Endpoint (MDE) offers comprehensive threat protection by detecting, investigating, and responding to threats in real-time, making it a crucial tool for any organization. Its seamless integration with the Microsoft ecosystem ensures a unified security experience. The platform's robust Endpoint Detection and Response (EDR) capabilities provide detailed insights into sophisticated threats, while automated investigation and remediation reduce the workload on security teams.

Learn in this course how to activate MDE, onboard devices, reduce attack surface, enable next-generation protection, control automated investigation and monitor all security related aspects of devices.

Who should attend

SecOps team members, device administrators and all interested responsible.

Course Content

Microsoft Defender XDR

- Overview of MS Defender XDR
- MDE overview and licensing
- MDE vs. Microsoft Intune
- Zero Trust and MDE

Microsoft Defender for Endpoint

- MDE architecture
- MDE portal
- MDE activation
- MDE roles and permissions

Onboarding/Offboarding

- Windows devices via local script, MS Intune and Group policies
- MacOS devices via local script and MS Intune
- Linux and Windows Server via Azure Arc
- Troubleshoot onboarding issues
- Offboard devices

Endpoint protection – Attack surface reduction

- Service to Service connection to Microsoft Intune
- Attack surface reduction rules
- Controlled folder access
- Device control

Endpoint protection – Next-generation protection

- Cloud protection
- Behavior monitoring
- Real-time protection
- EDR in block mode

Endpoint detection and response

- Alerts and Incidents management
- Automated investigation and response (AIR)
- Remediation actions
- Device investigation
- Device response actions

Additional configurations

- Advanced features
- Indicators
- Web content filtering
- Vulnerability Management

Advanced Hunting

- KQL primer
- Important MDE queries

Endpoint DLP (if time permits)

About Fast Lane

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