

---

# Master Class: Microsoft Defender for Endpoint (MDE)

**ID** MDE **Price** on request **Duration** 4 days

## Who should attend

SecOps team members, device administrators and all interested responsible.

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

## 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

### Additional configurations

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

### Advanced Hunting

- KQL primer
- Important MDE queries

### Endpoint DLP (if time permits)

# Master Class: Microsoft Defender for Endpoint (MDE)

---

## 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>