Master Class: Microsoft Defender and Microsoft Sentinel for Hybrid Cloud (HYBSEC)

ID HYBSEC **Price** 5,990.— €(excl. tax) **Duration** 5 days

Course Overview

Today, IT environments (VMs, apps and data platforms) are not only hosted on premises nor only in the cloud. Working with both world is the reality for a variety of reasons. This affects a lot of processes, design decisions but also security monitoring.

Monitoring must be established, and the collected data has to be investigated and evaluated. In this Master Class we dive deep into Microsoft Cloud Security whether on-prem or cloud-based systems. We will focus on Microsoft Defender for Cloud, Defender for Identity and Microsoft Sentinel. These services are able to monitor and secure you hybrid environment.

Who should attend

Administrators with experience of at least 5 years in administering Windows Active Directory Domain Services, Azure Active Directory and Azure resources.

Course Content

Defender for Cloud

- Overview of Defender for Cloud
- Prerequisites and implementation
- Securing Azure workloads
- Securing on-premises workloads
- Cloud Security Posture Management overview
- Use automation to respond to alerts
- Mastering Azure Policy guest configuration

Defender for Identity

- Overview of MS Defender for Identity
- Planning MS Defender for Identity Deployment (Architecture, Prerequisites)+
- Implement Defender for Identity
- Investigate alerts/detections
  - Reconnaissance Alerts
  - Compromised Credential Alerts
  - Lateral Movement Alerts
  - and some more

KQL Primer

- Basic operators for querying tables and formatting output
- Working with variables
- Advance operators and functions
  - Extending tables
  - Querying and filtering property bags
  - Aggregate records and
  - Create custom functions
- working with multiple tables and external data

Microsoft Sentinel

- Data collectors Implementation
- Creating Analytic rules
- Use automation to respond to Incidents
- Automatically enrich incident information
- Investigate Incidents
- Perform threat hunting
- Create workbooks
- Investigate with UEBA

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