Microsoft 365 Defender - Defender for Endpoint

Course code: GOC253

This three-day course covers in detail the deployment and management of Defender for Endpoint anti-malware technology on Windows-based computers, its configuration and customization, and the collection and monitoring of detection events in a cloud environment.

Affiliate	Duration	Course price	ITB

The prices are without VAT.

Course terms

Date	Duration	Course price	Type	Course language	Location

The prices are without VAT.

Prerequisites

Familiarity and basic knowledge corresponding to the courses listed in the Prerequisite Courses and Related Courses sections

Course Outline

- Overview and history of Microsoft Defender for Endpoint
- Requirements and capabilities for modern protection and detection of current threats
- Malware entry vectors and attack surface reduction
- Security differences between workstations and mobile computers
- Planning and preparing for Defender for Endpoint deployment
- Licensing, supported platforms, and architectural deployment options
- Distributing installation packages; monitoring installation and onboarding progress
- Onboarding methods using Intune, Group Policy, Configuration Manager, and scripts
- Ensuring and monitoring updates and compliance
- Basic Centralized configuration and tuning of performance and blocking strictness
- Configuration of Microsoft Defender Antivirus and cloud protection
- Attack Surface Reduction (ASR) rules and their deployment
- Web Protection, SmartScreen, and Network Protection
- Device Control – managing the use of USB and other peripherals
- Management of exclusions and their security implications
- Device Group management and role-based access control (RBAC)
- Asset tagging and device categorization based on criticality
- Detections, logging, and monitoring
- Handling alerts, incidents, and security event correlation
- Addressing false positives and responding to true positive detections
- Automated responses and options for isolating compromised devices
- Live Response and remote intervention on endpoints
- Endpoint Detection and Response (EDR) and EDR in Block Mode
- Analysis of processes, network connections, and forensic traces on devices
- Creating custom detection rules
- Optimizing detections for enterprise environments
- Microsoft Defender Vulnerability Management (MDVM)
- Software and vulnerability inventory and CVE tracking
- Security recommendations and remediation prioritization

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

- Secure Score for Devices and security posture assessment
- Threat intelligence and working with Indicators of Compromise (IOCs)
- Management of blocked and allowed items indicators (IP, URL, hash, certificates)
- Integration with Microsoft Defender XDR and other Microsoft security products
- Integration with Microsoft Sentinel and SIEM/SOAR scenarios
- Automation using APIs, PowerShell, and Logic Apps
- Reporting, dashboards, and security metrics for management
- Tips and tricks, vulnerability and threat databases
- Troubleshooting and endpoint remediation
- Common operational scenarios, best practices, and recommendations from real-world deployments

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved