# Microsoft 365 Defender - configuration, management, and incident detection

Course code: GOC250

The five-day advanced course is designed for security specialists, administrators, blue team analysts, and SOCs who want to effectively use the entire Microsoft Defender ecosystem as a unified platform for preventing, detecting, investigating, and responding to security incidents. The course covers the complete Microsoft Defender XDR stack, including Defender for Endpoint, Defender for Office 365, Defender for Cloud, and Defender for Cloud Apps. The course provides a detailed overview of the configuration and management of individual Microsoft Defender XDR components, their mutual integration, and practical use in detecting modern cyber threats. Participants will gain a deeper understanding of attacks targeting identities, endpoints, email, and cloud applications and learn how to mitigate or detect these attacks early using Microsoft Defender technologies. The course also includes incident investigation analysis and advanced hunting.

## Assumed entry knowledge

Awareness and basic knowledge in the scope of the courses listed in the Previous courses and Related courses sections

## Course outline

Microsoft Defender XDR

- Microsoft Defender XDR architecture
- Integration of individual Defender components
- RBAC and Access Control

Defender for Endpoint

- Deployment and Configuration
- Endpoint Detection and Response (EDR)
- Attack Surface Reduction
- Vulnerability Management
- Device Investigation
- Automated Investigation and Remediation

Defender for Office 365

- Email Protection
- Anti-Phishing and Anti-Spam Protection
- Safe Links and Safe Attachments
- Threat Explorer

Defender for Cloud

- Architecture and Configuration
- CSPM and Secure Score
- Cloud Workload Protection
- Integration with Defender XDR
- Detection and Investigation Cloud Threats

Defender for Cloud Apps

- SaaS Security
- Shadow IT and Discovery
- App Risk Assessment
- Access and Session Policies
- Cloud Threat Detection
- Investigating Compromised Cloud Applications

Threat Detection &Incident Response

**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

- Incident Investigation
- KQL Basics
- Advanced Hunting
- Response Actions and Remediation

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