Microsoft 365 Defender - Defender for Identity

Course code: GOC252

This three-day course provides an in-depth look at deployment, logging, monitoring, evaluation, and the detection of events, attacks, potential configuration weaknesses, and emerging threats related to identities—as well as associated sign-ins and privileged access—within hybrid environments comprising Entra ID (cloud) and Active Directory, AD CS, and ADFS (on-premises), utilizing Microsoft Defender for Identity.

Prerequisites

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

Course Outline

- Overview of scenarios such as Entra ID, PIM, Windows Server, Windows Client, AD DS Domain Controller, AD CS Certificate Services, ADFS, hybrid join, Entra ID join, and Entra ID device registration
- Security events appearing in on-premises security logs versus cloud sign-in logs
- Cloud applications, their identifiers, non-human accounts in Entra ID (service principals), and their representation in sign-in logs
- How on-premises sign-in methods—such as Kerberos, NTLM, Schannel, Windows Hello, and Windows Hello for Business (WHB)—appear in logs and how to investigate them
- Logging of local administrator activity under UAC, including the new Windows 11 Admin Protection feature
- logs of process and application execution on Windows computers

TCP communication and Windows Defender Firewall logs

investigation of login errors such as incorrect passwords, locked or disabled accounts, etc., on workstations, servers, Domain Controllers (DCs), and Entra ID

AD/Entra ID group and Entra ID role memberships and associated device logs

events related to password changes, MFA factor changes, TAP (Temporary Access Pass), etc.

events related to changes in role and group memberships, PIM groups, JIT (Just-In-Time) access, and approvals

events related to Entra Connect (Cloud and Sync), technical accounts, and service principals

events triggered by cloud application access and their service principals, as well as privileged application access

logging of PowerShell script execution and module loading

indicators of Entra ID scanning by attackers

deployment of Defender for Identity on on-premises AD DS domain controllers

deployment of Defender for Identity on on-premises AD CS certification authorities

deployment of Defender for Identity on on-premises AD FS servers

events generated by Defender for Identity for AD DS DCs, AD CS, and AD FS

detection of Kerberos attacks, Golden Ticket, Pass-the-Hash, etc.

indicators and detection of on-premises and cloud attacks such as password spraying, risky sign-ins, brute-force attacks, stolen tokens, MFA fraud, and impossible travel

detection of insecure AD configurations such as RC4, LM hash, Kerberos delegation, unprotected forest trusts, etc.

indicators and detection of AD DS scanning by an attacker; detection and mapping of lateral movement

detection and inventory of privileged accounts within the domain and on computers

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

detection and inventory of service accounts (non-human) within the domain and on computers

detection and inventory of service accounts in cloud environments (service identities)

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