Microsoft 365 Defender - Defender for Identity

Kód kurzu: GOC252

Třídenní kurz se detailně věnuje možnostem nasazení, logování, sledování, vyhodnocování a hlídání událostí, útoků a potenciálních slabých nastavení a hrozících situací souvisejících s identitami v hybridních prostředí Entra ID (cloud) a Active Directory, AD CS a ADFS (on-prem) a jejich přihlašováním a privilegovanými přístupy za pomoci Microsoft Defender for Identity.

Pobočka	Dnů	Cena kurzu	ITB

Uvedené ceny jsou bez DPH.

Termíny kurzu

Datum	Dnů	Cena kurzu	Typ výuky	Jazyk výuky	Lokalita

Uvedené ceny jsou bez DPH.

Předpokládané vstupní znalosti

Povědomí a základní znalosti v rozsahu kurzů uvedených v sekcích Předchozí kurzy a Související kurzy

Osnova kurzu

- přehled řešených scénářů jako jsou EntraID, PIM, Windows Server, Windows Client, ADDS DC Domain Controller, AD CS certifikační služby, ADFS, hybrid-join, EntraID join a EntraID registrace zařízení
- jaké bezpečnostní události se vůbec objevují v on prem security protokolech a jaké v cloud sign in protokolech
- cloudové aplikace, jejich identifikátory, non-human účty v EntraID (service principals) a jejich projevy v sign-in protokolech
- jak se v protokolech projevuje a vyšetřuje on prem přihlašování jako Kerberos, NTLM a Schannel, Windows Hello a Windows Hello for Business (WHB)
- jak se loguje práce lokálních adminů pod UAC i s Windows 11 novinkou Admin Protection
- protokoly o spouštění procesů a aplikací na Windows počítačích
- protokoly o TCP komunikaci a Windows Defender Firewall
- vyšetřování chyb přihlášení jako špatné heslo, zamčený a zakázaný účet apod. na stanicích, serverech, DC a v EntraID
- členství ve AD/EntraID skupinách a EntraID rolích a s tím související logy na zařízeních
- události související se změnou hesla, změnou MFA faktoru, TAP apod.
- události související se změnami členství v rolích a skupinách, PIM skupiny a JIT a approval
- události související s Entra Connect Cloud i Sync, technické účty a service principals
- události vyvolané přístupem cloud aplikací a jejich service principals, privilegované přístupy aplikací
- logování spouštění PowerShell scriptů a načítání PowerShell modulů
- projevy skenování EntraID útočníkem
- zavedení Defender for Identity na on prem řadičích ADDS DC
- zavedení Defender for Identity na on prem řadičích AD CS certifikačních autoritách
- zavedení Defender for Identity na on prem řadičích ADFS
- události produkované Defender for Identity pro ADDS DC, ADCS i ADFS
- detekce Kerberos útoků, golden ticket, pass the hash apod.
- projevy a detekce on-prem i cloud útoků jako jsou password-spraying, risky sign-in, brute-force, odcizené tokeny, MFA fraud, impossible travel
- detekce nevhodných AD nastavení jako RC4, LM hash, Kerberos delegation, nechráněné forest trusty apod.
- projevy a detekce skenování ADDS útočníkem, detekce a mapy lateral movement
- detekce a evidence privilegovaných účtů v doméně a na počítačích
- detekce a evidence účtů služeb (non-human) v doméně a na počítačích

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

- detekce a evidence účtů služeb v cloudovém prostředí (serivce 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