# Microsoft 365 Defender - Defender for Identity

Kód kurzu: GOC252

Trojdňový kurz sa detailne venuje možnostiam nasadenia, logovania, sledovania, vyhodnocovania a stráženia udalostí, útokov a potenciálnych slabých nastavení a hroziacich situácií súvisiacich s identitami v hybridných prostrediach Entra ID (cloud) a Active Directory, AD CS a ADFS (on-prem) a ich prihlasovaním a privilegovanými prístupmi.

## Predpokladané vstupné znalosti

Povedomie a základné znalosti v rozsahu kurzov uvedených v sekciách Predchádzajúce kurzy a Súvisiace kurzy

## Osnova kurzu

- prehľad riešených scenárov ako sú EntraID, PIM, Windows Server, Windows Client, ADDS DC Domain Controller, AD CS certifikačné služby, ADFS, hybrid-join, EntraID join a EntraID registrácia zariadenia
- aké bezpečnostné udalosti sa vôbec objavujú v on prem security protokoloch a aké v cloud sign in protokoloch
- cloudové aplikácie, ich identifikátory, non-human účty v EntraID (service principals) a ich prejavy v sign-in protokoloch
- ako sa v protokoloch prejavuje a vyšetruje on prem prihlasovanie ako Kerberos, NTLM a Schannel, Windows Hello a Windows Hello for Business (WHB)
- ako sa loguje práca lokálnych adminov pod UAC aj s Windows 11 novinkou Admin Protection
- protokoly o spúšťaní procesov a aplikácií na Windows počítačoch
- protokoly o TCP komunikácii a Windows Defender Firewall
- vyšetrovanie chýb prihlásení ako zlé heslo, zamknutý a zakázaný účet a pod. na staniciach, serveroch, DC av EntraID
- členstvo v AD/EntraID skupinách a EntraID roliach as tým súvisiace logy na zariadeniach
- udalosti súvisiace so zmenou hesla, zmenou MFA faktora, TAP a pod.
- udalosti súvisiace so zmenami členstva v rolách a skupinách, PIM skupiny a JIT a approval
- udalosti súvisiace s Entra Connect Cloud a Sync, technické účty a servisné prvky
- udalosti vyvolané prístupom cloud aplikácií a ich service principals, privilegované prístupy aplikácií
- logovanie spúšťania PowerShell scriptov a načítanie PowerShell modulov
- prejavy skenovania EntraID útočníkom
- zavedenie Defender for Identity na on prem radičoch ADDS DC
- zavedenie Defender for Identity na on prem radičoch AD CS certifikačných autoritách
- zavedenie Defender for Identity na on prem radičoch ADFS
- udalosti produkované Defender for Identity pre ADDS DC, ADCS aj ADFS
- detekcia Kerberos útokov, golden ticket, pass the hash a pod.
- prejavy a detekcia on-prem aj cloud útokov ako sú password-spraying, risky sign-in, brute-force, odcudzené tokeny, MFA fraud, impossible travel
- detekcia nevhodných AD nastavení ako RC4, LM hash, Kerberos delegation, nechránené forest trusty a pod.
- prejavy a detekcia skenovania ADDS útočníkom, detekcia a mapy lateral movement
- detekcia a evidencia privilegovaných účtov v doméne a na počítačoch
- detekcia a evidencia účtov služieb (non-human) v doméne a na počítačoch
- detekcia a evidencia účtov služieb v cloudovom prostredí (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