Microsoft 365 Defender - Defender for Endpoint

Kód kurzu: GOC253

Třídenní kurz se detailně věnuje nasazení a správě antimalware technologie Defender for Endpoint na počítače s Windows operačními systémy, jeho konfiguraci a přizpůsobení, sběru událostí o záchytech a jejich sledování v cloudovém prostředí.

Předpokládané vstupní znalosti

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

Osnova kurzu

- Přehled a historie Microsoft Defender for Endpoint
- Požadavky a možnosti moderních ochran a detekcí aktuálních hrozeb
- Cesty pronikání malware na počítače a omezení povrchu na jejich útoky
- Rozdíly z bezpečnostního pohledu mezi stanicemi a mobilními počítači
- Plánování a příprava nasazení Defender for Endpoint
- Licencování, podporované platformy a architektonické možnosti nasazení
- Distribuce instalačních balíčků, sledování postupu instalace a on-boardingu
- Metody on-boardingu pomocí Intune, Group Policy, Configuration Manageru a skriptů
- Zajištění a sledování aktualizací a compliance
- Základní centrální nastavení a ladění výkonu a striktnosti blokací
- Konfigurace Microsoft Defender Antivirus a cloudové ochrany
- Attack Surface Reduction (ASR) pravidla a jejich nasazení
- Web Protection, SmartScreen a Network Protection
- Device Control – řízení použití USB a dalších periferií
- Správa výjimek (Exclusions) a jejich bezpečnostní dopady
- Správa skupin zařízení (Device Groups) a role-based access control (RBAC)
- Asset tagging a kategorizace zařízení podle kritičnosti
- Záchyty a jejich protokolování a sledování
- Práce s alerty, incidenty a korelací bezpečnostních událostí
- Řešení false-positive a reakce na skutečně pozitivní záchyty
- Automatizované reakce a možnosti izolace napadených zařízení
- Live Response a vzdálený zásah na koncových bodech
- Endpoint Detection and Response (EDR) a EDR in Block Mode
- Analýza procesů, síťových spojení a forenzních stop na zařízení
- Tvorba vlastních detekčních pravidel (Custom Detection Rules)
- Optimalizace detekcí pro podnikový provoz
- Microsoft Defender Vulnerability Management (MDVM)
- Inventarizace software, zranitelností a sledování CVE
- Security Recommendations a prioritizace nápravných opatření
- Secure Score for Devices a vyhodnocení úrovně zabezpečení
- Threat Intelligence a práce s indikátory kompromitace (IOC)
- Správa blokovaných a povolených indikátorů (IP, URL, hash, certifikáty)
- Integrace s Microsoft Defender XDR a dalšími bezpečnostními produkty Microsoftu
- Integrace s Microsoft Sentinel a SIEM/SOAR scénáře
- Automatizace pomocí API, PowerShellu a Logic Apps
- Reporting, dashboardy a bezpečnostní metriky pro management
- Tipy a triky, databáze zranitelností a hrozeb
- Řešení potíží a zásah na koncových bodech

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

- Nejčastější provozní scénáře, best practices a doporučení z reálných nasazení

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