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.

Predpokladané vstupné znalosti

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

Osnova kurzu

- Prehľad a história Microsoft Defender for Endpoint
- Požiadavky a možnosti moderných ochrán a detekcií aktuálnych hrozieb
- Cesty prenikania malware na počítače a obmedzenie povrchu na ich útoky
- Rozdiely z bezpečnostného pohľadu medzi stanicami a mobilnými počítačmi
- Plánovanie a príprava nasadenia Defender for Endpoint
- Licencovanie, podporované platformy a architektonické možnosti nasadenia
- Distribúcia inštalačných balíčkov, sledovanie postupu inštalácie a on-boardingu
- Metódy on-boardingu pomocou Intune, Group Policy, Configuration Manageru a skriptov
- Zabezpečenie a sledovanie aktualizácií a compliance
- Základné centrálne nastavenie a ladenie výkonu a striktnosti blokácií
- Konfigurácia Microsoft Defender Antivirus a cloudovej ochrany
- Attack Surface Reduction (ASR) pravidlá a ich nasadenie
- Web Protection, SmartScreen a Network Protection
- Device Control – riadenie použitia USB a ďalších periférií
- Správa výnimiek (Exclusions) a ich bezpečnostné dopady
- Správa skupín zariadení (Device Groups) a role-based access control (RBAC)
- Asset tagging a kategorizácia zariadení podľa kritickosti
- Záchyty a ich protokolovanie a sledovanie
- Práca s alertami, incidentmi a koreláciou bezpečnostných udalostí
- Riešenie false-positive a reakcie na skutočne pozitívne záchyty
- Automatizované reakcie a možnosti izolácie napadnutých zariadení
- Live Response a vzdialený zásah na koncových bodoch
- Endpoint Detection and Response (EDR) a EDR v Block Mode
- Analýza procesov, sieťových spojení a forenzných stôp na zariadení
- Tvorba vlastných detekčných pravidiel (Custom Detection Rules)
- Optimalizácia detekcií pre podnikovú prevádzku
- Microsoft Defender Vulnerability Management (MDVM)
- Inventarizácia softvéru, zraniteľností a sledovanie CVE
- Security Recommendations a prioritizácia nápravných opatrení
- Secure Score for Devices a vyhodnotenie úrovne zabezpečenia
- Threat Intelligence a práca s indikátormi kompromitácie (IOC)
- Správa blokovaných a povolených indikátorov (IP, URL, hash, certifikáty)
- Integrácia s Microsoft Defender XDR a ďalšími bezpečnostnými produktmi Microsoftu
- Integrácia s Microsoft Sentinel a SIEM/SOAR scenáre
- Automatizácia pomocou API, PowerShellu a Logic Apps
- Reporting, dashboardy a bezpečnostné metriky pre manažment
- Tipy a triky, databázy zraniteľností a hrozieb
- Riešenie problémov a zásah na koncových bodoch

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

- Najčastejšie prevádzkové scenáre, best practices a odporúčania z reálnych nasadení

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