Microsoft 365 Defender - konfigurace, správa a detekce incidentů

Kód kurzu: GOC250

Pětidenní pokročilý kurz je určen bezpečnostním specialistům, administrátorům, blue team analytikům a SOC, kteří chtějí efektivně využívat celý ekosystém Microsoft Defender jako jednotnou platformu pro prevenci, detekci, vyšetřování a reakci na bezpečnostní incidenty. Kurz pokrývá kompletní Microsoft Defender XDR stack včetně Defender for Endpoint, Defender for Office 365, Defender for Cloud a Defender for Cloud Apps. Kurz detailně rozebírá konfiguraci a správu jednotlivých komponent Microsoft Defender XDR, jejich vzájemnou integraci a praktické využití při detekci moderních kybernetických hrozeb. Účastníci získají hlubší porozumění útokům zaměřeným na identity, endpointy, elektronickou poštu a cloudové aplikace a naučí se, jak pomocí Microsoft Defender technologií tyto útoky mitigovat nebo včas detekovat. Součástí kurzu je také analýza vyšetřování incidentů a advanced hunting.

Předpokládané vstupní znalosti

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

Osnova kurzu

Microsoft Defender XDR

- Architektura Microsoft Defender XDR
- Integrace jednotlivých Defender komponent
- RBAC a řízení přístupu

Defender for Endpoint

- Nasazení a konfigurace
- Endpoint Detection and Response (EDR)
- Attack Surface Reduction
- Vulnerability Management
- Device Investigation
- Automated Investigation and Remediation

Defender for Office 365

- Ochrana elektronické pošty
- Anti-Phishing a Anti-Spam ochrana
- Safe Links a Safe Attachments
- Threat Explorer

Defender for Cloud

- Architektura a konfigurace
- CSPM a Secure Score
- Ochrana cloudových workloadů
- Integrace s Defender XDR
- Detekce a vyšetřování hrozeb v cloudu

Defender for Cloud Apps

- SaaS Security
- Shadow IT a Discovery
- App Risk Assessment
- Access a Session Policies
- Cloud Threat Detection
- Vyšetřování kompromitovaných cloudových aplikací

Threat Detection &Incident Response

- Vyšetřování incidentů
- KQL základy

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

- Advanced Hunting
- Response Actions a Remediation

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