

# Workshop: AI Azure Incident Response

Kód kurzu: WAI AZIR

Workshop AI Azure Cloud Incident Response Skill Building je navržen tak, aby vám pomohl rozvíjet pracovní dovednosti potřebné k reakci na různé incidenty. Jeho osnova zajišťuje komplexní a praktický přístup k zvládnutí reakce na incidenty Azure během 3 dnů. Každý účastník získá 30denní přístup k praktickým cvičením Azure. Celý workshop je veden pouze v anglickém jazyce. Pro účast na workshopu je nezbytně nutné, aby si každý účastník přinesl svůj notebook a monitor či tablet pro práci s laby. Workshop probíhá pouze prezenčně. Počet míst omezen. Workshop si také můžete zakoupit v balíčku společně s konferencí Hackerfest, která na něj bezprostředně navazuje.

## Workshop probíhá v anglickém jazyce!

### Pro koho je workshop určen

- Inženýři / analytici kybernetické bezpečnosti
- Správci sítí a systémoví administrátoři
- Inženýři a vývojáři dronů a robotiky
- Operátoři dronů
- Vyšetřovatelé digitální forenzní analýzy
- Penetrační testéři
- Pracovníci v oblasti cloud computing
- Manažeři projektů v cloudu
- Podpora provozu se zájmem o kariérní postup

### Osnova

#### Den 1: Úvod do bezpečnosti a reakce na incidenty v Azure

Ranní část: Základy a přehled

1. Úvod a představení
  - Přehled cílů workshopu a program
  - Význam reakce na incidenty v cloudových prostředích
2. Základy bezpečnosti v Azure
  - Úvod do Microsoft Defender pro Cloud
  - Přehled architektury bezpečnosti v Azure a klíčové koncepty
3. Základy reakce na incidenty
  - Životní cyklus reakce na incidenty: příprava, detekce, analýza, zadržení, vyhlazení, obnova a činnosti po incidentu
  - Klíčové role a odpovědnosti při reakci na incidenty

Odpolední část: Nástroje a příprava

1. Nástroje a služby pro bezpečnost v Azure
  - Důkladné zkoumání Microsoft Defender pro Cloud, Microsoft Sentinel a Azure Monitor
  - Nastavení a správa bezpečnostních výstrah
2. Nastavení vašeho prostředí pro reakci na incidenty
  - Nastavení bezpečného prostředí v Azure pro reakci na incidenty
  - Nastavení a využívání Azure Log Analytics
3. Praktické cvičení: Počáteční nastavení
  - Nastavení Microsoft Defender pro Cloud a Microsoft Sentinel
  - Nastavení bezpečnostních politik a pravidel výstrah

#### Den 2: Detekce a analýza

Ranní část: Pokročilé techniky detekce

#### GOPAS Praha

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

#### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

#### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved

# Workshop: AI Azure Incident Response

1. Detekce hrozeb v Azure
  - Porozumění metodologiím detekce hrozeb v Azure
  - Využití Microsoft Sentinel pro detekci hrozeb
2. Analýza logů a monitoring
  - Sběr a analýza logů z různých služeb v Azure
  - Použití jazyka Kusto Query Language (KQL) pro pokročilou analýzu logů
3. Praktické cvičení: Detekce incidentů
  - Konfigurace zdrojů logů a nastavení pravidel detekce
  - Spouštění KQL dotazů k identifikaci potenciálních incidentů

Odpolední část: Analýza a vyšetřování incidentů

1. Techniky analýzy incidentů
  - Vyšetřování bezpečnostních výstrah a incidentů v Azure
  - Využití sešitů a playbooků služby Microsoft Sentinel pro analýzu
2. Forenzní analýza v Azure
  - Úvod do forenzní analýzy v cloudu
  - Zachycování a analýza důkazů v Azure
3. Praktické cvičení: Vyšetřování incidentu
  - Vyšetřování simulovaného incidentu
  - Provádění analýzy příčin a identifikace rozsahu porušení

## Den 3: Zadržení, vyhlazení a obnova

Ranní část: Zadržení a vyhlazení

1. Strategie zadržení
  - Techniky pro zadržení incidentů v Azure
  - Izolace postižených zdrojů a minimalizace dalšího dopadu
2. Techniky vyhlazení
  - Odstranění škodlivých artefaktů a zadních vrat
  - Zajištění, že prostředí je čisté a zabezpečené
3. Praktické cvičení: Zadržení a vyhlazení
  - Zadržení probíhajícího incidentu
  - Vyhlazení škodlivých složek z prostředí

Odpolední část: Obnova a činnosti po incidentu

1. Postupy obnovy
  - Obnovení postižených systémů a služeb
  - Ověření integrity obnovených systémů
2. Kontrola po incidentu
  - Provádění recenzí po incidentu a sezení k získání zkušeností
  - Aktualizace plánů reakce na incidenty a bezpečnostních kontrol na základě zjištění
3. Praktické cvičení: Obnova a kontrola
  - Obnova po incidentu a ověření prostředí
  - Provádění simulované recenze po incidentu a aktualizace strategií reakce

## Použití Azure AI a nástrojů třetích stran

Integraci Azure AI a nástrojů třetích stran do procesu reakce na incidenty mohou organizace zefektivnit provoz, snížit manuální úsilí a zlepšit celkovou bezpečnostní pozici tím, že rychleji a efektivněji reagují na kybernetické hrozby. Tento přístup nejenže zvyšuje odolnost bezpečnosti, ale také uvolňuje zdroje pro zaměření na strategické iniciativy a proaktivní zmírnění hrozeb.

**GOPAS Praha**  
Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Brno**  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved

# Workshop: AI Azure Incident Response

## Závěr, otázky a odpovědi

- Závěr
- Shrnutí klíčových poznatků a získaných dovedností
- Prostor pro otázky a diskuzi
- Zpětná vazba
- Vydávání certifikátů o dokončení kurzu
- Sběr zpětné vazby účastníků pro neustálé zlepšování

**GOPAS Praha**  
Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Brno**  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved