Workshop: AI Azure Incident Response

Course code: WAIAZIR

The AI Azure Cloud Incident Response Skill Building workshop is designed to help you build on job skills for responding to various incidents. This outline ensures a comprehensive and hands-on approach to mastering Azure incident response over a structured three-day period. Each participant will get 1 month access to Azure labs. The workshop is conducted in-person only. The number of seats is limited. You can also purchase the workshop in a package together with the Hackerfest conference, which follows immediately after.

Who is the course for

- Cyber Security engineers / analysts
- Network and system administrators
- Drone, &Robotic Engineers &Developers
- Drone Operators
- Digital Forensics Investigators
- Penetration Testers
- Cloud computing personnel
- Cloud project managers
- Operations support looking for career advancement

Course outline

Day 1: Introduction to Azure Security and Incident Response

Morning Session: Foundations and Overview

1. Welcome and Introduction

o Overview of the workshop goals and agenda

o Importance of incident response in cloud environments

2. Azure Security Fundamentals

o Introduction to Microsoft Defender for Cloud

o Overview of Azure security architecture and key concepts

3. Incident Response Basics

o Incident response lifecycle: preparation, detection, analysis, containment, eradication, recovery, and post-incident activity

o Key roles and responsibilities in incident response

Afternoon Session: Tools and Preparation

1. Azure Security Tools and Services

o Deep dive into Microsoft Defender for Cloud, Microsoft Sentinel, and Azure Monitor

o Configuring and managing security alerts

2. Setting Up Your Incident Response Environment

o Configuring a secure Azure environment for incident response

o Setting up and utilizing Azure Log Analytics

3. Practical Lab: Initial Setup

o Hands-on lab: Configure Microsoft Defender for Cloud and Microsoft Sentinel

o Setting up security policies and alert rules

Day 2: Detection and Analysis

Morning Session: Advanced Detection Techniques

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

1. Threat Detection in Azure

o Understanding threat detection methodologies in Azure

o Utilizing Microsoft Sentinel for threat detection

2. Log Analysis and Monitoring

o Collecting and analyzing logs from various Azure services

o Using Kusto Query Language (KQL) for advanced log analysis

3. Practical Lab: Detecting Incidents

o Hands-on lab: Configuring log sources and setting up detection rules

o Running KQL queries to identify potential incidents

Afternoon Session: Incident Analysis and Investigation

1. Incident Analysis Techniques

o Investigating security alerts and incidents in Azure

o Leveraging Microsoft Sentinel workbooks and playbooks for analysis

2. Forensics in Azure

o Introduction to cloud forensics

o Capturing and analyzing evidence in Azure

3. Practical Lab: Incident Investigation

o Hands-on lab: Investigating a simulated incident

o Performing root cause analysis and identifying the scope of the breach

Day 3: Containment, Eradication, and Recovery

Morning Session: Containment and Eradication

1. Containment Strategies

o Techniques for containing incidents in Azure

o Isolating affected resources and mitigating further impact

2. Eradication Techniques

o Removing malicious artifacts and backdoors

o Ensuring the environment is clean and secure

3. Practical Lab: Containment and Eradication

o Hands-on lab: Containing a live incident

o Eradicating malicious components from the environment

Afternoon Session: Recovery and Post-Incident Activities

1. Recovery Procedures

o Restoring affected systems and services

o Validating the integrity of restored systems

2. Post-Incident Review

o Conducting post-incident reviews and lessons learned sessions

o Updating incident response plans and security controls based on findings

3. Practical Lab: Recovery and Review

o Hands-on lab: Recovering from an incident and validating the environment

o Conducting a mock post-incident review and updating response strategies

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Workshop: AI Azure Incident Response

Using Azure AI and other 3rd party tools

By integrating Azure AI and third-party tools into your Incident Response process, organizations can streamline operations, reduce manual effort, and improve overall security posture by responding faster and more effectively to cyber threats. This approach not only enhances security resilience but also frees up resources to focus on strategic initiatives and proactive threat mitigation.

Conclusion and Q&A

o Wrap-Up

o Summary of key takeaways and skills acquired

o Open floor for questions and discussion

o Feedback

o Providing completion certificates

o Gathering participant feedback for continuous improvement

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk