AI TACTICAL SKILLS:

AZURE CLOUD INCIDENT RESPONSE

This AI training is designed to help you build on job skills for responding to various incidents.

3 DAYS | Online / In person / Hybrid | ALL LEVELS

Learn to Leverage AI technology with Azure Sentinel for Incident Response, detection and mitigation. A practical, 3-day hands-on class designed to empower cybersecurity professionals with the skills to utilize artificial intelligence effectively in threat detection and response.

TARGET AUDIANCE

- 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

CYBER2 LABS

Build your AI Tactical Skills

WWW.CYBER2LABS.COM

INFO@CYBER2LABS.COM

AI TACTICAL SKILLS:

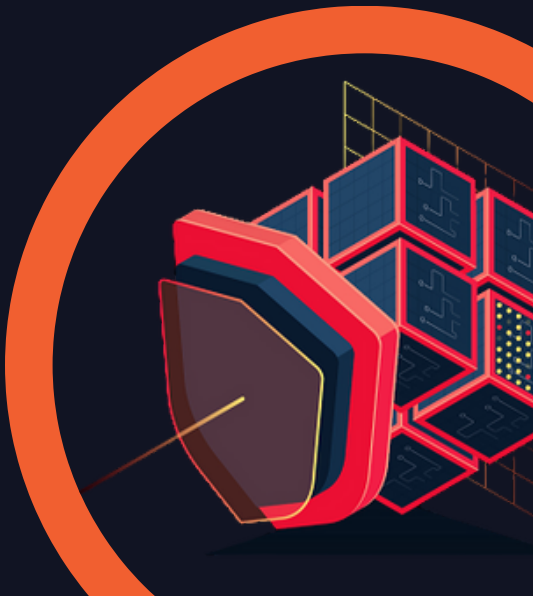
AZURE CLOUD INCIDENT RESPONSE

COURSE OUTLINE

This outline ensures a comprehensive and hands-on approach to mastering Azure incident response over a structured 3-day period. 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.

AI

- BUILD
- HACK
- DETECT
- DEFEND



CYBER2 LABS

WWW.CYBER2LABS.COM
INFO@CYBER2LABS.COM

AI TACTICAL SKILLS:

AZURE CLOUD INCIDENT RESPONSE

Day 1: **Introduction to Azure Security and Incident Response**

Foundations and Overview

- Welcome and Introduction
  - Overview of the workshop goals and agenda
  - Importance of incident response in cloud environments
- Azure Security Fundamentals
  - Introduction to Microsoft Defender for Cloud
  - Overview of Azure security architecture and key concepts
- Incident Response Basics
  - Incident response lifecycle: preparation, detection, analysis, containment, eradication, recovery, and post-incident activity
  - Key roles and responsibilities in incident response

Tools and Preparation

- Azure Security Tools and Services
  - Deep dive into Microsoft Defender for Cloud, Microsoft Sentinel, and Azure Monitor
  - Configuring and managing security alerts
- Setting Up Your Incident Response Environment
  - Configuring a secure Azure environment for incident response
  - Setting up and utilizing Azure Log Analytics
- Practical Lab: Initial Setup
  - Hands-on lab: Configure Microsoft Defender for Cloud and Microsoft Sentinel
  - Setting up security policies and alert rules

CYBER2 LABS

WWW.CYBER2LABS.COM

INFO@CYBER2LABS.COM

Build your AI Tactical Skills

AI TACTICAL SKILLS:

AZURE CLOUD INCIDENT RESPONSE

Day 2: **Detection and Analysis**

Advanced Detection Techniques

- Threat Detection in Azure
  - Understanding threat detection methodologies in Azure
  - Utilizing Microsoft Sentinel for threat detection
- Log Analysis and Monitoring
  - Collecting and analyzing logs from various Azure services
  - Using Kusto Query Language (KQL) for advanced log analysis
- Practical Lab: Detecting Incidents
  - Hands-on lab: Configuring log sources and setting up detection rules
  - Running KQL queries to identify potential incidents

Incident Analysis and Investigation

- Incident Analysis Techniques
  - Investigating security alerts and incidents in Azure
  - Leveraging Microsoft Sentinel workbooks and playbooks for analysis
- Forensics in Azure
  - Introduction to cloud forensics
  - Capturing and analyzing evidence in Azure
- Practical Lab: Incident Investigation
  - Hands-on lab: Investigating a simulated incident
  - Performing root cause analysis and identifying the scope of the breach

AI TACTICAL SKILLS:

AZURE CLOUD INCIDENT RESPONSE

Day 3: **Containment, Eradication, and Recovery**

Containment and Eradication

- Threat Detection in Azure
  - Techniques for containing incidents in Azure
  - Isolating affected resources and mitigating further impact
- Eradication Techniques
  - Removing malicious artifacts and backdoors
  - Ensuring the environment is clean and secure
- Practical Lab: Containment and Eradication
  - Hands-on lab: Containing a live incident
  - Eradicating malicious components from the environment

Recovery and Post-Incident Activities

- Recovery Procedures
  - Restoring affected systems and services
  - Validating the integrity of restored systems
- Post-Incident Review
  - Conducting post-incident reviews and lessons learned sessions
  - Updating incident response plans and security controls based on findings
- Practical Lab: Recovery and Review
  - Hands-on lab: Recovering from an incident and validating the environment
  - Conducting a mock post-incident review and updating response strategies