# Masterclass: Incident Response in the Cloud

**Duration: 4 Days** **Course Code: IRC** **Delivery Method: Virtual Learning**

## Overview:

This immersive training delivers a complete, hands-on journey through Azure security, identity abuse, threat detection, and cloud incident response. Students begin by establishing core foundations – Azure architecture, governance, logging, and the security stack, before progressing into the full Azure Cyber Kill Chain. Participants will perform real-world attacks across identity, compute, storage, and control-plane layers, including token theft, AiTM phishing, privilege escalation, service principal compromise, misconfigurations, and persistence techniques unique to Azure.

## Target Audience:

The course is perfect for security architects, Entra ID administrators, security administrators, and security auditors.
Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

## Objectives:

- Understand Azure security and cloud incident response fundamentals.
- Detect, investigate, and respond to attacks targeting Azure, Entra ID, and hybrid environments.
- Analyze identity, infrastructure, and network-based threats in cloud environments.
- Use KQL, Microsoft Sentinel, and Graph API for threat hunting and incident investigation.
- Apply incident response processes aligned with the National Institute of Standards and Technology framework.
- Implement remediation, hardening, and cloud security best practices.
- Gain hands-on experience through practical labs and real-world attack scenarios.

## Prerequisites:

- To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5 years in the field is recommended. All attendees should have experience with Active Directory Domain Services (AD DS) administration.

## Testing and Certification

- After completing the course, participants will receive a CQURE Certificate of Completion and will also be eligible for CPE points.

## Content:

Module One: Azure Security and Incident Response Fundamentals

Module Two: Deep Dive into Entra ID and Governance

Module Three: Core Controls, Benchmarks, and Logging

Module Four: Reconnaissance and Initial Access

Module Five: Infrastructure and Network Attacks

Module Six: Execution and Privilege Escalation

Module Seven: Advanced Identity Attacks and Credential Access

Module Eight: Persistence Technique

Module Nine: Exfiltration and Impact

Module Ten: KQL for Incident Response

Module Eleven: Advanced Hunting and Detection

Module Twelve: Graph API for Incident Response

Module Thirteen: Responding to Azure Attacks (NIST)

Module Fourteen: Remediation and Strategic Hardening

Module Fifteen: Advanced and Strategic Best Practices

## Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE