KOENIG SOLUTIONS · COURSE OUTLINE

# Attacking and Defending Azure & M365

Learn to attack and defend Azure and Microsoft 365, from reconnaissance and credential theft to persistence and defense evasion.

**9** MODULES

**110** TOPICS

## COURSE OVERVIEW

This course provides a deep dive into security threats targeting Azure and Microsoft 365 environments. Participants will explore reconnaissance, credential theft, lateral movement, privilege escalation, and persistence techniques used by attackers. Each module covers attack methods, detection strategies, and mitigation techniques, ensuring a comprehensive understanding of both offensive and defensive security practices.

## WHO THIS COURSE IS FOR

- **Security Analysts**
- **Penetration Testers**
- **Incident Responders**
- **Cloud Security Engineers**
- **Threat Hunters**
- **SOC Analysts**

## PREREQUISITES

Required Prerequisites

- Basic understanding of Azure and Microsoft 365
- Familiarity with cybersecurity concepts and attack techniques
- Experience with identity and access management (IAM)
- Knowledge of security monitoring and log analysis tools.

## LEARNING OBJECTIVES

- Identify reconnaissance and enumeration techniques against Azure/M365
- Apply password spraying and OAuth abuse initial access techniques
- Analyse credential theft methods such as Golden SAML and skeleton keys
- Assess lateral movement techniques such as Pass the PRT and Pass the Cookie
- Evaluate privilege escalation through Azure AD and RBAC role abuse
- Explain persistence techniques such as federated backdoors and service principals
- Describe defense evasion methods such as audit disabling and log spoofing
- Plan detection and mitigation strategies across the attack lifecycle

COURSE SYLLABUS

# 9 Modules, 110 Topics

01

## Introduction

TOPICS

Overview of Azure/M365 · Updates to ENTRA ID

02

## Setting Up Your Environment

TOPICS

SOF-ELK Overview and Setup · Log Analysis Using SOF-ELK

03

## Reconnaissance & Enumeration

TOPICS

- ATTACK - Enumerate Users and Domains
- DETECT - Enumerate Users and Domain
- ATTACK - Post Exploitation Reconnaissance
- DETECT - Post Exploitation Reconnaissance
- ATTACK - Access Packages (Insider) NEW
- DETECT - Access Packages (Insider) NEW
- MITIGATE - Access Packages (Insider

04

## Initial Access Techniques

TOPICS

- ATTACK - Password Spraying M365
- DETECT - Password Spraying M365
- MITIGATE - Password Spraying M365
- ATTACK - OWA Password Spraying
- DETECT - OWA Password Spraying
- MITIGATE - OWA Password Spraying
- ATTACK - OAuth Abuse
- DETECT - OAuth Abuse
- MITIGATE - OAuth Abuse
- ATTACK - Device Code Authentication Abuse
- DETECT - Device Code Authentication Abuse
- MITIGATE - Device Code Authentication Abuse
- ATTACK - M365 Business Email Compromise
- DETECT - M365 Business Email Compromise
- MITIGATE - M365 Business Email Compromise
- ATTACK - Bypassing MFA and CA
- DETECT - Bypassing MFA and CA
- MITIGATE - Bypassing MFA and CA

05

## Credential Theft

TOPICS

- ATTACK - Golden SAML Attack
- DETECT - Golden SAML Attack
- MITIGATE - Golden SAML Attack
- ATTACK - Attacking Key Vaults
- DETECT - Attacking Key Vaults
- MITIGATE - Attacking Key Vaults
- ATTACK - Skeleton Keys (PTA Abuse)
- DETECT - Skeleton Keys (PTA Abuse)
- MITIGATE - Skeleton Keys (PTA Abuse)
- ATTACK - Stealing Access Tokens from Office Apps
- DETECT - Stealing Access Tokens from Office Apps
- MITIGATE - Stealing Access Tokens from Office Apps
- ATTACK - Extract Passwords from Automation Accounts
- DETECT - Extract Passwords from Automation Accounts
- MITIGATE - Extract Passwords from Automation Account
- ATTACK - Hunting Credentials in Previous Deployment
- DETECT - Hunting Credentials in Previous Deployment

06

## Lateral Movement Techniques

TOPICS

- ATTACK - Pass the PRT
- DETECT - Pass the PRT
- MITIGATE - Pass the PRT
- ATTACK - Pass the Cookie
- DETECT - Pass the Cookie
- MITIGATE - Pass the Cookie
- ATTACK - Abusing Managed Identities
- DETECT - Abusing Managed Identities
- MITIGATE - Abusing Managed Identities
- ATTACK - Virtual Machine Abuse
- DETECT - Virtual Machine Abuse
- MITIGATE - Virtual Machine Abuse
- ATTACK - Azure Lighthouse
- DETECT - Azure Lighthouse
- MITIGATE - Azure Lighthouse
- ATTACK - Microsoft Intune
- DETECT - Microsoft Intune
- MITIGATE - Microsoft Intune
- ATTACK - Azure Arc Custom Script Extension
- DETECT - Azure Arc Custom Script Extension
- MITIGATE - Azure Arc Custom Script Extension

07

## Privilege Escalation

TOPICS

- Abusing Azure AD / RBAC Roles
- ATTACK - Cloud Administrator Abuse
- DETECT - Cloud Administrator Abuse
- MITIGATE - Cloud Administrator Abuse
- ATTACK - User Administrator Abuse
- DETECT - User Administrator Abuse
- MITIGATE - User Administrator Abuse
- ATTACK - Abusing Family of Client IDs
- DETECT - Abusing Family of Client IDs
- MITIGATE - Abusing Family of Client IDs

08

## Persistence Techniques

TOPICS

- ATTACK - AAD Federated Backdoor
- DETECT - AAD Federated Backdoor
- MITIGATE - AAD Federated Backdoor
- ATTACK - Malicious MFA Takeover
- DETECT - Malicious MFA Takeover
- MITIGATE - Malicious MFA Takeover
- ATTACK - Service Principal Abuse
- DETECT - Service Principal Abuse
- MITIGATE - Service Principal Abuse
- ATTACK - Automation Account Abuse
- DETECT - Automation Account Abuse
- MITIGATE - Automation Account Abuse
- ATTACK - Compromising Azure Blobs & Storage Accounts
- DETECT - Compromising Azure Blobs & Storage Accounts
- MITIGATE - Compromising Azure Blobs & Storage Accounts
- ATTACK - Malicious Device Join
- DETECT - Malicious Device Join
- MITIGATE - Malicious Device Join
- ATTACK - Directory Synchronization Accounts
- DETECT - Directory Synchronization Accounts
- MITIGATE - Directory Synchronization Accounts
- ATTACK - Cross Tenant Synchronization
- DETECT - Cross Tenant Synchronization
- MITIGATE - Cross Tenant Synchronization

09

## Defense Evasion

TOPICS

- ATTACK - Disabling Auditing
- DETECT - Disabling Auditing
- MITIGATE - Disabling Auditing
- ATTACK - Spoofing Azure Sign-in Logs
- DETECT - Spoofing Azure Sign-in Logs
- MITIGATE - Spoofing Azure Sign-in Logs
- ATTACK - Registering Fake Agents for Log Spoofin
- DETECT - Registering Fake Agents for Log Spoofing
- MITIGATE - Registering Fake Agents for Log Spoofing

WHAT IS INCLUDED

## Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

## Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

## Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

### Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com