Attacking and Defending Azure & M365

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.

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.

Table of contents

- ATTACK - Post Exploitation Reconnaissance
- DETECT - Post Exploitation Reconnaissance
- ATTACK - Access Packages (Insider) NEW
- DETECT - Access Packages (Insider) NEW
- MITIGATE - Access Packages (Insider

Module 4: Initial Access Techniques

- 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 Abus
- 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

Module 5: Credential Theft

- 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

Module 6: Lateral Movement Techniques

- 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

Module 7: Privilege Escalation

- 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

Module 8: Persistence Techniques

- 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

Module 9: Defense Evasion

- 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