CORSO SICUREZZA E HARDENING DELL'IDENTITÀ CON MICROSOFT ENTRA ID

Durata: 4 ore

PROGRAMMA

MODULO 1: FONDAMENTI E SUPERFICIE DI ATTACCO DI MICROSOFT ENTRA ID

- Entra ID vs AD on-prem (rebrand + modello di identità cloud)
- Superficie di attacco: utenti, workload identity (service principal / managed identity), app/OAuth, dispositivi, identità ibrida (Entra Connect / Cloud Sync)
- Enumerazione: OSINT, AADInternals, MSOLSpray + tooling moderno (ROADtools, GraphRunner, AzureHound)
- Threat landscape attuale come gancio: case study Midnight Blizzard (password spray su tenant legacy senza MFA + abuso app OAuth), Scattered Spider (social engineering help desk), Storm-0501 (ransomware ibrido cloud)

MODULO 2: TECNICHE DI ATTACCO E RILEVAMENTO

- Password spraying / brute force + MFA, Smart Lockout, number matching (ormai default), MFA fatigue / push bombing
- AiTM phishing & token theft (Evilginx, Tycoon 2FA, EvilProxy): il vettore dominante che bypassa l'MFA via reverse proxy + session hijacking
- Persistenza via service principal / app registration (aggiunta di credenziali agli SP, illicit consent grant) — il "backdoor" cloud moderno
- OAuth/consent abuse → workflow di protezione + app governance in Defender for Cloud Apps
- Privilege escalation: PIM, least privilege, [NUOVO] Restricted Management AU per i ruoli sensibili
- Attacchi ibridi: PRT theft, Golden SAML, abuso PHS/PTA/Seamless SSO
- Logging & detection: Sign-in logs, Entra ID Protection (ex Identity Protection), Defender for Identity

MODULO 3: HARDENING: IDENTITÀ E ACCESSI

- Da "MFA Everywhere" a "phishing-resistant MFA Everywhere": FIDO2 / passkey / Windows Hello for Business
- Conditional Access moderno: Authentication Strengths, Token Protection / Continuous Access Evaluation (CAE), device compliance + filters, Microsoft-managed
- Protezione account privilegiati: admin roles, break glass, PIM.

MODULO 4: DETECTION, RISPOSTA E AI NEL SOC

- Playbook Sentinel/Defender e automazioni SOAR
- Unified SecOps: Sentinel dentro il portale Defender, incident correlati identità+endpoint+cloud
- AI nel SOC: il Conditional Access Optimization Agent di Security Copilot
- Identità agentiche come superficie emergente

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO SICUREZZA E HARDENING DELL'IDENTITÀ CON MICROSOFT ENTRA ID

Durata: 4 ore

OVERVIEW DEL CORSO

Nel perimetro cloud-native, l'identità rappresenta la nuova e più critica frontiera della sicurezza aziendale. Questo Flash Training offre un percorso verticale e ad altissimo contenuto tecnico incentrato sulla protezione di Microsoft Entra ID, analizzando i vettori di compromissione moderni e le strategie di hardening più efficaci. In sole 4 ore, mapperemo la reale superficie d'attacco dei tenant cloud — analizzando minacce reali come il phishing AiTM bypass-MFA, il token theft e gli abusi sulle applicazioni OAuth — per poi implementare contromisure avanzate. Il programma approfondisce le più recenti evoluzioni di sicurezza del panorama Microsoft, inclusi i controlli per le identità agentiche, il supporto continuo di Continuous Access Evaluation (CAE) e l'ottimizzazione tramite Security Copilot.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Cloud Administrator e Identity Engineer
- Security Analyst e SOC Operator
- CISO e IT Manager

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- A mappare la superficie d'attacco di Microsoft Entra ID ed eseguire l'audit delle identità ibride e dei workload (Service Principal e Managed Identity).
- A identificare e intercettare minacce dominanti come il phishing basato su AiTM (Adversary-in-the-Middle) e le tecniche di persistenza tramite abusi di consensi OAuth.
- A implementare l'evoluzione dei modelli di Accesso Condizionato (Conditional Access) sfruttando Authentication Strengths, Token Protection e logiche di Continuous Access Evaluation (CAE).
- A segregare i privilegi amministrativi configurando Privileged Identity Management (PIM), account di Break Glass e le nuove Restricted Management Administrative Units.
- A sfruttare l'Intelligenza Artificiale nel SOC utilizzando il Conditional Access Optimization Agent di Security Copilot per identificare anomalie e ottimizzare i workflow di risposta (SOAR).

CONTATTI

info@nexsys.it

www.nexsys.it