



**3 ore. Un obiettivo. Una competenza chiave.**

# **Corso Entra ID Security**

## **Protezione di identità e accessi cloud**

---



**3 ore.**  
**Un obiettivo.**  
**Una competenza chiave.**





## Corso Entra ID Security: protezione di identità e accessi cloud

Rilevare, mitigare e rispondere agli attacchi alle identità cloud

Questo TechShot ti porta dentro il mondo degli attacchi alle identità cloud e ti mostra come difendere utenti, amministratori e applicazioni in Entra ID. Scoprirai le tecniche reali che gli attaccanti usano, imparerai a rilevare segnali di compromissione e ad applicare contromisure operative immediate, riducendo il rischio per la tua infrastruttura cloud.

**ISCRIVITI**

### Dettagli del corso

-  6 maggio 2026 dalle 9.30 - 12.30
-  Online Live
-  €99+IVA a partecipante
-  Posti limitati

### Cosa è incluso nel corso

-  Open Badge
-  Registrazione per 3 mesi
-  Materiale didattico

### La tua skill in 3 ore

L'obiettivo è comprendere le tecniche di attacco e applicare contromisure pratiche per proteggere identità, accessi e applicazioni cloud in Entra ID.

Alla fine del corso sarai in grado di:

- Identificare i principali vettori di attacco in Entra ID e Azure AD
- Applicare MFA, Conditional Access e PIM per ridurre i rischi
- Rilevare attività sospette e rispondere rapidamente agli incidenti
- Proteggere account privilegiati e configurare ambienti sicuri per gli utenti

---

## **Corso Entra ID Security: protezione di identità e accessi cloud**

Rilevare, mitigare e rispondere agli attacchi alle identità cloud

---

### **Prerequisiti di partecipazione**

- Conoscenze di base di Azure e familiarità con concetti di autenticazione (MFA, OAuth)

### **Programma del corso**

#### **Modulo 1: Fondamenti e Superficie di Attacco Cloud**

- Cos'è Azure AD (Entra ID) e differenze con AD on-prem
- Superficie di attacco: identità, accessi, applicazioni, dispositivi
- Tecniche di enumerazione Azure AD (OSINT, AADInternals, MSOLSpray)
- Indicatori precoci di attacco e best practice introduttive

#### **Modulo 2: Tecniche di Attacco e Rilevamento**

- Password spraying, brute force e contromisure (MFA, Smart Lockout)
- Token theft e session hijacking: rilevamento e mitigazione
- Abuso di applicazioni e permessi OAuth: workflow di protezione
- Enumerazione privilegi e escalation: PIM e least privilege
- Logging e alert: Sign-in logs, Identity Protection, Defender for Identity

#### **Modulo 3: Hardening & Best Practice Difensive**

- MFA Everywhere: MFA anche su account di servizio
- Conditional Access avanzato: location-based, device compliance
- Protezione account privilegiati: admin roles, break glass, gestione sicura
- Monitoraggio e risposta: playbook Sentinel/Defender, automazioni SOAR