Defending Entra ID

ARC407

Defending Microsoft Entra ID from the record: how each attack works, from password spray and stolen sessions to consent, escalation through applications, roles and agents, persistence and the hybrid seam, the evidence it leaves, the control that stops it, and a response proved step by step, with Copilot's answers checked throughout.

Modules	14
Lessons	107
Phases	5
Free preview	Defending Entra ID (10 lessons)

The method

Portal, PowerShell and the record. Each of the 106 lessons shows the admin center and the Microsoft Graph PowerShell for the task it teaches, and proves each finding from the sign-in and audit records. Queries run in the page against the SecOps Range, a month of a tenant's records with real attacks in it. Every product behavior a lesson relies on comes from a Microsoft page it names, with the date it was read.

Copilot, checked. Every lesson delegates work to Copilot and checks its answer against the record, and every practice scenario asks which of an assistant's claims fails and on what. The course treats an assistant as a fast colleague whose work is verified before it becomes a finding.

One case, end to end. The capstone works one intrusion across the edge, an identity, an attacker-built application and an agent: its scope widened from an address to its range, a response in one window, every step proved, and a report with exposure kept apart from loss.

Full syllabus

Phase 1: Foundations, Tokens and Sessions

Defending Entra ID FREE PREVIEW

Module 0 of Defending Entra ID: what Entra ID is and why attackers want it, its users, groups, applications, devices and roles, how a sign-in works, how attacks on it have changed, what it gives a defender, working with Copilot and its agents, and the evidence a defender reads.

1. 0.1 What Entra ID Is and Why Attackers Want It
2. 0.2 Users and Groups
3. 0.3 Applications and Service Principals
4. 0.4 Devices
5. 0.5 Roles and Privileged Access
6. 0.6 How a Sign-In Works
7. 0.7 How Attacks on Entra ID Have Changed
8. 0.8 What Entra ID Gives a Defender
9. 0.9 Working With Copilot and Entra's Agents
10. 0.10 The Evidence a Defender Reads

Tokens, Sessions and Protocols

Module 1 of Defending Entra ID: OAuth 2.0 and OpenID Connect, the flows and their traces, the claims inside a token, lifetimes, browser sessions, the PRT, session controls, and following a session across the sign-in logs.

1. 1.1 OAuth 2.0 and OpenID Connect in Entra ID
2. 1.2 The Flows and Their Traces
3. 1.3 Inside a Token
4. 1.4 Lifetimes and the Policies That Set Them
5. 1.5 Browser Sessions
6. 1.6 The Primary Refresh Token in Depth
7. 1.7 Session Controls in Force
8. 1.8 Following a Session Across the Logs

Phase 2: Attacks on Sign-in

Password Attacks and MFA Abuse

Module 2 of Defending Entra ID: password spray, stuffing and brute force, smart lockout and password protection, finding a spray in the logs, MFA methods and strengths, push fatigue, registration and recovery abuse, Identity Protection, and the response.

1. 2.1 How Passwords Are Attacked
2. 2.2 Smart Lockout and Password Protection
3. 2.3 Finding a Spray in the Logs
4. 2.4 MFA Methods and Their Strength
5. 2.5 MFA Fatigue and Push Abuse
6. 2.6 Abusing Registration and Recovery
7. 2.7 Identity Protection for Password and MFA Attacks
8. 2.8 Responding to a Compromised Password

Conditional Access as Defense

Module 3 of Defending Entra ID: how Conditional Access evaluates a sign-in, the baseline set, exclusions and emergency access, device and location conditions, resource targeting and its gaps, changing policy safely, and finding sign-ins a policy missed.

1. 3.1 How a Policy Is Evaluated
2. 3.2 The Baseline Set
3. 3.3 Exclusions and Emergency Access
4. 3.4 Device-Based Access
5. 3.5 Locations and Their Limits
6. 3.6 Resources, Apps and Gaps
7. 3.7 Changing Policy Safely
8. 3.8 Finding Who a Policy Missed

Phishing for Sessions

Module 4 of Defending Entra ID: adversary-in-the-middle phishing and how to find it, phishing-resistant methods, device code phishing, consent phishing, consent settings and AI apps, and responding to a phished session or consent.

1. 4.1 How Adversary-in-the-Middle Works
2. 4.2 Finding an AiTM Sign-in
3. 4.3 Phishing-Resistant Methods
4. 4.4 Device Code Phishing
5. 4.5 Consent Phishing
6. 4.6 Consent Settings and AI Apps
7. 4.7 Responding to Phished Sessions and Consents
8. 4.8 A Phishing Case End to End

Token Theft and Replay

Module 5 of Defending Entra ID: how session cookies, refresh tokens and the PRT are stolen, finding a replayed session, ID Protection token detections, the PRT under attack, token protection, CAE in a theft case, sessions Entra cannot end, and a case end to end.

1. 5.1 How Tokens Are Stolen
2. 5.2 Finding a Replayed Session
3. 5.3 Token Detections in ID Protection
4. 5.4 The PRT Under Attack
5. 5.5 Token Protection
6. 5.6 CAE in a Theft Case
7. 5.7 Sessions Entra Cannot End
8. 5.8 A Token Theft Case End to End

Phase 3: Escalation and Agents

Escalation Through Applications

Module 6 of Defending Entra ID: how applications escalate, adding a credential, creating an app and granting it, what an app did, a leaked workload credential, workload identity detections, governing ownership and permissions, and a case end to end.

1. 6.1 How Applications Escalate
2. 6.2 Adding a Credential
3. 6.3 Creating an App and Granting It
4. 6.4 What the App Did
5. 6.5 A Leaked Workload Credential
6. 6.6 Detections for Workload Identities
7. 6.7 Governing Ownership and Permissions
8. 6.8 An Application Escalation Case End to End

Escalation Through Roles and Groups

Module 7 of Defending Entra ID: how roles escalate, reading role assignments, assignments outside PIM, groups as a route, PIM settings that hold, restricting who manages whom, from Entra into Azure, and a case end to end.

1. 7.1 How Roles Escalate
2. 7.2 Reading Role Assignments
3. 7.3 Assignments Outside PIM
4. 7.4 Groups as a Route
5. 7.5 PIM Settings That Hold
6. 7.6 Restricting Who Can Manage Whom
7. 7.7 From Entra into Azure
8. 7.8 A Role Escalation Case End to End

Agents as Identities

Module 8 of Defending Entra ID: what an agent is in Entra, the agent inventory, what an agent can reach, reading agent activity, a blueprint credential added and used, detecting a risky agent, controls for agents, and a case end to end.

1. 8.1 What an Agent Is in Entra
2. 8.2 The Agent Inventory
3. 8.3 What an Agent Can Reach
4. 8.4 Reading Agent Activity
5. 8.5 A Blueprint Credential Added and Used
6. 8.6 Detecting a Risky Agent
7. 8.7 Controls for Agents
8. 8.8 An Agent Case End to End

Phase 4: Persistence and the Hybrid Seam

Persistence and Evasion

Module 9 of Defending Entra ID: what survives a response, methods as persistence, federation backdoors, cross-tenant access and sync, turning off the lights, the agents' own audit trail, controls for the control plane, and the persistence sweep.

1. 9.1 What Survives a Response
2. 9.2 Methods as Persistence
3. 9.3 Federation Backdoors
4. 9.4 Cross-Tenant Access and Synchronization
5. 9.5 Turning Off the Lights
6. 9.6 The Agents' Own Audit Trail
7. 9.7 Controls for the Control Plane
8. 9.8 The Persistence Sweep

The Hybrid Seam

Module 10 of Defending Entra ID: where the directories meet, the synchronization accounts, password hash sync, pass-through authentication agents, seamless SSO, soft and hard match, cloud-only administrators, and a hybrid case end to end.

1. 10.1 Where the Directories Meet
2. 10.2 The Synchronization Accounts
3. 10.3 Password Hash Sync
4. 10.4 Pass-Through Authentication Agents
5. 10.5 Seamless SSO
6. 10.6 Soft and Hard Match
7. 10.7 Cloud-Only Administrators
8. 10.8 A Hybrid Case End to End

Phase 5: Response and Capstone

Response

Module 11 of Defending Entra ID: the response order, the Identity Risk Management Agent, containing users, containing applications and agents, rotating secrets, recovering configuration, proving the response held, and a response end to end.

1. 11.1 The Response Order
2. 11.2 The Identity Risk Management Agent
3. 11.3 Containing Users
4. 11.4 Containing Applications and Agents
5. 11.5 Rotating Secrets
6. 11.6 Recovering Configuration
7. 11.7 Proving It Held
8. 11.8 A Response End to End

Capstone

Module 12 of Defending Entra ID, the capstone: one intrusion from the first alert through the edge, the identity, the cloud backdoor and the agent, to its scope, response and report.

1. 12.1 The First Alert
2. 12.2 The Edge and the Credential
3. 12.3 The Identity
4. 12.4 The Cloud Backdoor
5. 12.5 The Agent
6. 12.6 Scope
7. 12.7 The Response
8. 12.8 The Report

Course Completion

Course Exam

Defending Entra ID end-of-course exam: 40 questions in four parts, from tokens and sessions to response, ending on a case study.

1. Course Completion. Defending Entra ID

Generated 2026-11-18 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/defending-entra-id/