

Entra ID Security: Identity Controls & Attack Defense

ARC401

Read a Conditional Access estate the way an investigator does: what each control covers, which population it misses, and why a correctly configured policy still let the attack through.

Modules	18
Lessons	179
Phases	3
Free preview	Course Orientation (12 lessons)

The method

Identity is the control plane, and every attack in this course arrives through a successful authentication. The loop repeats for every control it builds.

1. Read the sign-in record properly. The result field and the risk fields answer different questions, and an investigation that reads one of them reaches the wrong conclusion confidently.
2. Fix the authentication method before the policy. A Conditional Access policy requiring multifactor is only as strong as the methods registered against the account it protects.
3. Design the policy set, then the policy. Every applicable policy is evaluated and the strictest control wins. Policies written one at a time acquire gaps no single review finds.
4. Validate in report-only against real sign-ins. Report-only tells you who would have been blocked using your own traffic. It is the cheapest verification here and the most skipped.
5. Close the application surface. Consent, credentials and service principals are identity too, and they survive every action taken against a user account.

What this course assumes

No minimum experience and no prerequisite course. Tokens, the evaluation model, risk detections and the application model are explained where they first matter.

What makes it go faster: a tenant with Entra ID P2, even a developer one, so you can build the policies alongside. Not required, and every configuration is shown with the portal path behind it.

What this course does not cover: identity governance and lifecycle, which is its own course, and incident response process. This is the identity control surface and defending it.

Full syllabus

Phase 1: Foundations

Course Orientation [FREE PREVIEW](#)

What Entra ID Security: Identity Controls & Attack Defense teaches: engineer Entra ID into the perimeter that stops account takeover, MFA fatigue, and token theft, using Conditional Access, Identity Protection, PIM, and token security.

1. 0.1 Why Identity Is the New Perimeter
2. 0.2 How Authentication Actually Works
3. 0.3 The Entra ID Security Stack
4. 0.4 Attack Patterns You Will Defend Against
5. 0.5 The Identity Kill Chain
6. 0.6 Zero Trust and Identity
7. 0.7 Real-World Identity Breaches
8. 0.8 The Defense Design Method
9. 0.9 Measuring Identity Security Posture
10. 0.10 The Lab Environment
11. Module Summary
12. Check My Knowledge

Sign-In Logs, Your Identity Telemetry

The sign-in log is the single most important data source for identity security.

1. 1.1 Anatomy of a Sign-In Log Entry
2. 1.2 Interactive vs Non-Interactive Sign-Ins
3. 1.3 Service Principal and Managed Identity Sign-Ins
4. 1.4 Authentication Details Deep Dive
5. 1.5 Conditional Access Evaluation in Sign-In Logs
6. 1.6 Risk Signals and Identity Protection
7. 1.7 Device and Location Signals
8. 1.8 KQL Fundamentals for Identity Security
9. 1.9 Advanced Query Patterns
10. 1.10 Cross-Table Joins and Correlation
11. 1.11 Building Your Sign-In Baseline
12. 1.12 The Identity Query Library
13. Module Summary
14. Check My Knowledge

Authentication Methods, Your First Line of Defense

Every identity attack either exploits weak authentication or bypasses strong authentication.

1. EI2.1 The Authentication Method Hierarchy
2. EI2.2 Passwords and Why They Fail
3. EI2.3 Microsoft Authenticator. Push and Number Matching
4. EI2.4 FIDO2 Security Keys
5. EI2.5 Passkeys in Microsoft Authenticator
6. EI2.6 Certificate-Based Authentication
7. EI2.7 Authentication Strength Policies
8. EI2.8 Passwordless Authentication and Temporary Access Pass
9. EI2.9 Planning the Migration to Phishing-Resistant Authentication
10. EI2.10 Deploying and Monitoring Authentication Changes
11. EI2.11 External Authentication Methods and Method Retirement
12. EI2.12 The Authentication Method Operations Playbook
13. Module Summary
14. Check My Knowledge

Phase 2: Conditional Access & Identity Protection

Conditional Access, Architecture and Design Principles

How to design a conditional access architecture that stops attacks without breaking productivity.

1. EI3.1 How Conditional Access Evaluation Works
2. EI3.2 Assignments: Users, Groups, and Roles
3. EI3.3 Target Resources: Applications and Authentication Context
4. EI3.4 Conditions: Location, Device Platform, and Client Apps
5. EI3.5 Named Locations and Network Context
6. EI3.6 Device Conditions and Compliance
7. EI3.7 Grant Controls: MFA, Auth Strength, Device, Terms of Use
8. EI3.8 Session Controls: Sign-In Frequency, Token Protection, and CAAC
9. EI3.9 The Zero Trust Policy Framework
10. EI3.10 Emergency Access and Break-Glass Accounts
11. EI3.11 Policy Design Patterns for Common Scenarios
12. EI3.12 Conditional Access Architecture as Code
13. Module Summary
14. Check My Knowledge

Conditional Access, Stopping Real Attacks

Specific real-world attack techniques and the conditional access policy combinations that stop each one.

1. EI4.1 The Attack-to-Defense Methodology
2. EI4.2 Blocking Legacy Authentication
3. EI4.3 Stopping Password Spray
4. EI4.4 Defending Against AiTM Credential Phishing
5. EI4.5 Preventing MFA Fatigue Attacks
6. EI4.6 Token Theft and Session Replay Defense
7. EI4.7 Consent Phishing and Illicit OAuth Grant Defense
8. EI4.8 Blocking Unauthorized Device Types and Platforms
9. EI4.9 Defending Against Credential Stuffing
10. EI4.10 Insider Threat Through Identity Controls
11. EI4.11 Attack Chain Defense: Multi-Stage Attack Scenarios
12. EI4.12 The Defense Verification Playbook
13. EI4.13 Defending Privileged Role Escalation
14. EI4.14 Workload Identity Attacks and Service Principal Abuse
15. Module Summary
16. Check My Knowledge

Identity Protection, Risk-Based Defense

How Identity Protection detects risk, how to configure risk policies, and how to operationalize risk signals for prevention and detection.

1. EI5.1 How Identity Protection Works
2. EI5.2 Sign-In Risk Detections
3. EI5.3 User Risk Detections
4. EI5.4 Configuring Risk-Based Conditional Access
5. EI5.5 Risk Remediation and Self-Service
6. EI5.6 The Risky Users Investigation Workflow
7. EI5.7 The Risky Sign-Ins Investigation Workflow
8. EI5.8 Tuning Identity Protection
9. EI5.9 Attack Disruption and Automatic Response
10. EI5.10 Identity Protection in Sentinel
11. EI5.11 Operationalizing Risk Signals
12. EI5.12 Advanced Risk Scenarios
13. EI5.13 Building a Risk Posture Dashboard
14. Module Summary
15. Check My Knowledge

Privileged Identity Management

Just-in-time, just-enough-access for administrative roles.

1. EI6.1 Why Standing Privileges Are Dangerous
2. EI6.2 PIM for Entra ID Roles. Eligible vs Active
3. EI6.3 Configuring PIM Role Settings
4. EI6.4 PIM for Azure Resource Roles
5. EI6.5 PIM Activation Security
6. EI6.6 Access Reviews for Privileged Roles
7. EI6.7 PIM Monitoring and Detection
8. EI6.8 Emergency Access and PIM
9. EI6.9 Designing a Privileged Access Strategy
10. EI6.10 PIM for Groups
11. EI6.11 PIM Operational Procedures
12. EI6.12 Advanced PIM Scenarios
13. Module Summary
14. Check My Knowledge

Token Security and Session Management

Tokens are the currency of identity. Token types and lifecycle, how tokens are stolen, token protection deployment, continuous access evaluation, session lifetime controls, and protecting the Primary Refresh Token.

1. EI7.1 Token Types and Lifecycle
2. EI7.2 Where Tokens Live
3. EI7.3 How Tokens Are Stolen: Proxy-Based Attacks
4. EI7.4 How Tokens Are Stolen: Device-Based Attacks
5. EI7.5 How Tokens Are Stolen: Infrastructure Attacks
6. EI7.6 Token Protection Deployment
7. EI7.7 Continuous Access Evaluation (CAE)
8. EI7.8 Session Lifetime and Sign-In Frequency
9. EI7.9 Protecting the Primary Refresh Token
10. EI7.10 Token Theft Detection
11. EI7.11 Token Theft Response
12. EI7.12 Browser Session Security
13. EI7.13 Token Security for Non-Interactive Sign-Ins
14. EI7.14 Building the Token Security Architecture
15. Module Summary
16. Check My Knowledge

Conditional Access Validation and Troubleshooting

You deployed conditional access policies.

1. EI8.1 Report-Only Mode: How It Works
2. EI8.2 Analyzing Report-Only Results
3. EI8.3 The What-If Tool and Policy Simulation
4. EI8.4 Policy Validation Queries
5. EI8.5 Conditional Access Gap Analysis
6. EI8.6 Troubleshooting Access Failures
7. EI8.7 Common Misconfigurations
8. EI8.8 Conditional Access Change Management
9. EI8.9 Policy Drift Detection
10. EI8.10 Validating Token Protection and Session Controls
11. EI8.11 Testing Break-Glass and Emergency Access
12. EI8.12 Building the CA Validation Dashboard
13. Module Summary
14. Check My Knowledge

Phase 3: Application Identity

Application Registration Security

Application registrations are the most overlooked attack surface in Entra ID.

1. EI9.1 The Dual-Object Model
2. EI9.2 How Application Authentication Works
3. EI9.3 Client Secrets: The Application Password Problem
4. EI9.4 Certificate-Based Application Authentication
5. EI9.5 Workload Identity Federation
6. EI9.6 Permission Governance: Delegated vs Application
7. EI9.7 The Consent Framework
8. EI9.8 Admin Consent Workflow
9. EI9.9 Publisher Verification and App Governance
10. EI9.10 Application Lifecycle Security
11. EI9.11 Detecting Malicious Application Activity
12. EI9.12 Application Security Queries
13. EI9.13 Securing Application Registrations
14. EI9.14 Building the Application Governance Framework
15. Module Summary
16. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

Subject-area sheets for identity work: where the control lives in the portal, the query that answers the question at scale, and what the answer does not prove.

1. Reading a Sign-In, and Tokens
2. Authentication Methods and MFA
3. Conditional Access
4. Identity Protection and Risk
5. Privileged Access and PIM
6. Applications and Workload Identity
7. Tables, Codes and Limits

Cookbooks

Seven runbooks for the procedures an identity engineer repeats: deploying a policy, retiring a method, migrating to PIM, onboarding a partner, and getting a tenant back.

1. Deploying a Conditional Access Policy
2. Rolling Out Phishing-Resistant Authentication
3. Retiring an Authentication Method
4. Migrating a Role to PIM
5. Onboarding an External Partner
6. Responding to a Risky User
7. Recovering a Locked-Out Tenant

Lab Setup

A complete build for an identity lab: tenant, workspace, telemetry, a population, a partner tenant, and the checks that prove it works.

1. Getting a Tenant
2. Wiring the Telemetry
3. Building a Population
4. The Second Tenant
5. Verify and Troubleshoot

Walkthroughs

Worked identity investigations end to end, including the wrong turns, the queries that looked right and were not, and what would have changed each answer.

1. The Travel That Was Not Impossible
2. The Policy That Covered Nobody
3. The Token That Survived the Revocation
4. The Consent That Was Not Phishing
5. The Admins the Query Could Not See
6. The MFA That Was Already Satisfied
7. The Spray That Found One Door

Playbooks

Seven configuration and governance events that fire at an identity engineer, each with the clearing check, what escalates it, and how to reverse it.

1. A Conditional Access Policy Changed
2. A Break-Glass Account Signed In
3. A Permanent Role Assignment Appeared
4. A Credential Landed on an Application
5. PIM Settings Were Weakened
6. A Guest Entered a Privileged Group
7. Legacy Authentication Came Back

Playground

Where to practice the identity work in this course against real data, without a tenant of your own.

References & Further Reading

External sources this course draws on: Microsoft Entra documentation, attack research, frameworks and community identity security material.

Course Completion

Course Exam

Entra ID Security: Identity Controls & Attack Defense end-of-course exam: a three-phase simulation testing whether you can apply the method to a situation the course did not walk through.

1. Course Completion. Entra ID Security: Identity Controls & Attack Defense

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/entra-id-security/