

Entra ID Security: Identity Detection & Operations

ARC406

Detect identity attacks, govern the identities nobody owns, and operate Entra ID as a running system. Workload identity, external identities, lifecycle governance, detection engineering, monitoring, backup and recovery, and Defender XDR integration.

Modules	18
Lessons	153
Phases	5
Free preview	Course Orientation (11 lessons)

The method

This course is the operational half of identity security: detecting what got past the controls and recovering when it did. The loop repeats through every surface it covers.

1. Cover the identities that are not people. Workload identities, service principals and external accounts hold permissions and outnumber your users. Most identity programs monitor the humans.
2. Know which log holds the answer. Sign-ins, non-interactive sign-ins, service principal sign-ins, audit and Graph activity are five sources with five retentions and five schemas.
3. Write detections against the identity behavior. Consent grants, credential additions, role assignments and the token events that precede them, rather than against a signature.
4. Establish what you can still see. Retention differs by tier and by table, and routing decisions made once decide what every future investigation can reach.
5. Rehearse the recovery. Deleted objects, broken break-glass and a directory that will not authenticate. The identity plane is the one whose outage stops the response itself.

The course closes on one identity intrusion worked end to end.

What this course assumes

No minimum experience and no prerequisite course, and no requirement to have taken the identity controls course first. Each log source and object type is introduced where it first appears.

What makes it go faster: a tenant you can read the logs in, and any prior KQL. Neither is required, and every query is shown against data.

What this course does not cover: Conditional Access design in depth and identity governance, which are separate courses. This one is detection, monitoring and recovery.

Full syllabus

Foundations

Course Orientation [FREE PREVIEW](#)

What Entra ID Security: Identity Detection & Operations teaches: detect the identity attacks that get past Conditional Access, govern the workload and external identities no control reaches, and run the estate that produces the signal.

1. ID0.1 What This Course Is About
2. ID0.2 Where Identity Signal Comes From
3. ID0.3 What a Detection Actually Is
4. ID0.4 The Attacks You Will Detect
5. ID0.5 Why Most Identity Detections Cannot Tell You Anything Alone
6. ID0.6 The Identities Nobody Owns
7. ID0.7 Running an Identity Estate
8. ID0.8 The Portal, PowerShell and KQL
9. ID0.9 Measuring Detection Coverage
10. ID0.10 The Lab Environment
11. Module Summary

Phase 1: Workload and External Identity

Workload Identity Security

Most identities in a tenant are not people.

1. ID1.1 The Sign-In With Nobody In It
2. ID1.2 What Is Actually In Your Tenant
3. ID1.3 The Credential Decides the Blast Radius
4. ID1.4 The Identity With No Credential to Leak
5. ID1.5 Held Versus Granted
6. ID1.6 The One Policy Type That Reaches Them
7. ID1.7 The Only Record You Get
8. ID1.8 The Credential Nobody Asked For
9. ID1.9 Rotating One Without Breaking It
10. ID1.10 Proving the Inventory Still Describes the Tenant
11. ID1.11 See It Done End to End
12. Check My Knowledge

External Identities and B2B Security

A cross-tenant access configuration you can defend, inbound and outbound.

1. ID2.1 The Population You Have Before You Configure Anything
2. ID2.2 The Defaults You Inherited
3. ID2.3 The Inbound Decision
4. ID2.4 The Trust Decision
5. ID2.5 The Outbound Decision
6. ID2.6 Conditional Access Over Six Populations
7. ID2.7 Onboarding That Makes Review Possible
8. ID2.8 Direct Connect and Sync
9. ID2.9 The Review That Can Actually Remove Someone
10. ID2.10 Proving the Configuration Still Holds
11. ID2.11 See It Done End to End
12. Check My Knowledge

Phase 2: Governance and Detection

Identity Governance and Lifecycle Management

A permission arrives by one of four paths and only some of them record why.

1. ID3.1 Four Ways a Permission Arrives
2. ID3.2 The Paths That Record Nothing
3. ID3.3 The Rule That Stops Running
4. ID3.4 What an Access Package Actually Is
5. ID3.5 The Policy Decides, Not the Package
6. ID3.6 A Review That Can Say No, and What It Never Reaches
7. ID3.7 The Date the Workflow Depends On
8. ID3.8 Disable Is Not Offboarding
9. ID3.9 Joining Governance to Detection
10. ID3.10 Proving It Closed
11. ID3.11 See It Done End to End
12. Check My Knowledge

Identity Detection Engineering

Detection engineering is a development discipline.

1. ID4.1 Detection Engineering as a Development Discipline
2. ID4.2 From Hypothesis to Data Confirmation
3. ID4.3 The Detection Specification
4. ID4.4 Expressing the Rule
5. ID4.5 Blind Spots, Assumptions and False Positives
6. ID4.6 Test Cases and Validation
7. ID4.7 Response Guidance
8. ID4.8 The Repository and the Path to Production
9. ID4.9 Coverage That Means Something
10. ID4.10 The Library, Assembled
11. See It Done End to End
12. Check My Knowledge

Phase 3: Operations and Resilience

Identity Monitoring and Operations

Detections decay, configurations drift, and log sources stop without failing.

1. ID5.1 What the Platform Reports, and What It Cannot
2. ID5.2 Choosing What to Watch
3. ID5.3 Alerting on Your Own Machinery
4. ID5.4 What You Can Honestly Promise
5. ID5.5 Drift in the Control Plane
6. ID5.6 Credential and Secret Hygiene
7. ID5.7 What Makes an Identity Alert Different
8. ID5.8 Toil, and What to Automate Away
9. ID5.9 Ownership, Escalation and Handover
10. ID5.10 The Operations You Inherited
11. See It Done End to End
12. Check My Knowledge

Identity Recovery and Resilience

The platform now backs your tenant up and keeps seven days of it.

1. ID6.1 What the Platform Backs Up, and for How Long
2. ID6.2 Two Different Restores Wearing One Word
3. ID6.3 The Control Plane Is the Unit of Recovery
4. ID6.4 What Does Not Come Back
5. ID6.5 Hard Delete, and Protected Actions
6. ID6.6 Break-Glass, the Account Everything Assumes
7. ID6.7 The Baseline You Keep Yourself
8. ID6.8 Rehearsing It
9. ID6.9 The Tenant You Cannot Log Into
10. ID6.10 The Dependencies You Did Not Know You Had
11. See It Done End to End
12. Check My Knowledge

Identity in the Defender XDR Ecosystem

An identity-only view sees one segment of an attack.

1. ID7.1 What Identity Alone Cannot See
2. ID7.2 The Prerequisite Chain Nobody Reads
3. ID7.3 What Defender for Identity Actually Adds
4. ID7.4 The Entra Connect Seam
5. ID7.5 The Identity Tables, and What Joins Them
6. ID7.6 Disruption, and What It Does Not Do
7. ID7.7 Predictive Shielding Is Not Disruption
8. ID7.8 The Join Identity Cannot Make Alone
9. ID7.9 What the Unified Queue Changes About Triage
10. ID7.10 What the Integration Does Not Solve
11. See It Done End to End
12. Check My Knowledge

Phase 4: Architecture and Capstone

Log Routing, Tiers and Retention

The seam the rest of the course depends on.

1. ID8.1 The Setting That Turns the Lights On
2. ID8.2 The Category Is Not the Table
3. ID8.3 What Each Category Is Worth, and What It Costs
4. ID8.4 Free Is Not Free
5. ID8.5 Analytics and Data Lake
6. ID8.6 The Retention You Have, and the One You Think You Have
7. ID8.7 Getting Old Data Back
8. ID8.8 The Cost Decision That Removes a Detection
9. ID8.9 Proving the Pipeline Still Runs
10. ID8.10 The Routing You Inherited
11. See It Done End to End
12. Check My Knowledge

Capstone: One Identity Intrusion, End to End

One attack that Conditional Access did not stop, worked from the alert to the routing decision to the detection to the response, in a tenant that cannot currently see half of it.

1. ID9.1 The Brief, and What the Tenant Can Currently See
2. ID9.2 The Attack That Got Through
3. ID9.3 What the Evidence Does Not Contain
4. ID9.4 The Routing Decision Comes First
5. ID9.5 Writing It
6. ID9.6 What It Costs to Run
7. ID9.7 The Response You Can Actually Perform
8. ID9.8 Handover
9. 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 Workload Identity Sign-In
2. The Four Identity Tables
3. Grant Paths and What Each Records
4. Credential Types and Their Limits
5. Workload Identity Policy Scope
6. Retention and What Expires When
7. External Identities and B2B
8. Governance and Lifecycle
9. Detection and Monitoring
10. Backup, Recovery and Resilience

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. Rotating a Credential Without an Outage
2. Removing a Credential Somebody Added
3. Finding What a Leaver Left Behind
4. Replacing a Retiring Membership Rule
5. Building the Workload Identity Inventory
6. Scoping a Review That Can Remove
7. Routing Identity Logs for Retention

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 Sign-In With Nobody In It
2. The Rule That Stopped Running
3. The Package That Took Ownership
4. The Review That Removed Three
5. The Eleven Nobody Offboarded
6. The Secret That Outlived the Account
7. Two Alerts, One Differing Field

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 Credential Landed on a Service Principal
2. A Workload Identity Signed In From a New Address
3. A Membership Rule Stopped Processing
4. An Access Package Assignment Expired Unexpectedly
5. A Leaver Account Is Still Enabled
6. Consent Granted an Application Permission
7. Graph Activity With No Matching Sign-In

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, detection guidance, frameworks and community research.

Course Completion

Course Completion

You've reached the end of Identity Detection & Operations.

1. Course Completion. Identity Detection & Operations

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