

Cloud Incident Response

FOR401

Investigate, contain, and recover from security incidents across Microsoft 365, Entra ID, and Sentinel. From initial detection through forensic analysis, containment, regulatory notification, and post-incident improvement.

Modules	20
Lessons	164
Phases	5
Free preview	Course Orientation (5 lessons)

The method

Every module in this course runs the same six-step loop against a Microsoft 365 tenant. It is the habit the course is built to install, because it is the sequence that produces a claim somebody else can check rather than an account somebody has to take on trust.

1. Establish what the tenant recorded. Before any query, know which operations are collected at your license tier, how long they are kept, and what was never written down. An empty result means one of three things and only one of them is about the incident.
2. Scope from the record rather than from the alert. The alert is where the case reached you. The scope comes from reading the audit trail, both sign-in tables and the file and mail activity, and it is almost always larger than the alert suggested.
3. Preserve before you collect. Preservation stops a clock; collection takes a copy. Doing the second without the first means the material can expire between the decision and the export.
4. Contain across the four paths. Sessions, credentials, application identities and sharing links fail independently. Closing three properly still leaves the fourth open, and it is usually the one nobody looked at.
5. Verify that the action landed. Taking an action and proving it worked are separate pieces of work. Every check needs a positive control, because an empty result is a claim about your query as much as about the tenant.
6. State what the evidence supports, and what it does not. A figure without its basis is a figure somebody else will derive differently. A gap in the record is a finding with an owner rather than an apology.

Recovery closes the loop and does not undo it. What can be restored, in what order, and why the copy that already left is unaffected by any of it.

What this course assumes

No minimum experience and no prerequisite course. Every concept is explained where it is first used, including the ones a syllabus like this would normally assume: what the unified audit log is, why there are two sign-in tables, what a refresh token does. If you have never opened the Defender portal, start at module zero and nothing will be missing.

What does make it go faster: a Microsoft 365 tenant you can read, even a developer one, and enough comfort with a command line to run a PowerShell cmdlet and read what comes back. Neither is required.

Every query in the course can be practiced against the Practice Hub instead, which holds populated tables and known answers, and the lab module walks through building a tenant from nothing if you want one.

What the course does not cover, deliberately: endpoint forensics beyond what Microsoft 365 reaches, memory analysis, and malware reverse engineering. Those are separate disciplines with their own courses, and a cloud investigation that pretends to teach them alongside teaches neither properly.

Full syllabus

Phase 1: Orientation and Foundations

Course Orientation [FREE PREVIEW](#)

What a Microsoft 365 investigation can physically reach, how to work through the course, the estate every example runs on, where the evidence lives, and the toolkit.

1. IR0.1 What This Course Covers, and What It Does Not
2. IR0.2 How to Work Through This Course
3. IR0.3 The Estate This Course Runs On
4. IR0.4 Where the Evidence Lives
5. IR0.5 The Toolkit, and Where to Practice

Foundations of M365 Incident Response

Who owns the evidence in a Microsoft 365 tenant, what it can and cannot establish, the deadlines that run regardless, and what a responder can defensibly claim.

1. IR1.1 The Shared Responsibility Model, and the Half Nobody Logs For You
2. IR1.2 Identity Is the Perimeter, and What That Costs an Investigation
3. IR1.3 The Threat Landscape: Attacks That Collect Authentication Rather Than Break It
4. IR1.4 The Framework Stopped Telling You How
5. IR1.5 Where the Framework Stops Describing a Tenant
6. IR1.6 The Clock Starts at Awareness, Not at Certainty
7. IR1.7 How You Find Out Decides What Is Left
8. IR1.8 The Questions a Tenant Cannot Answer at Any Speed
9. IR1.9 What You Can Defend, and at What Confidence
10. IR1.10 The Access You Need Before You Need It
11. IR1.11 See It Done: One Case, End to End
12. IR1.12 The Two Hunting Surfaces
13. Check My Knowledge

Preparation and Readiness

The tenant configuration that decides whether an investigation is possible: log export, the two retention systems, what to switch on, and who can reach it.

1. IR2.1 The Export That Has No Retroactive Fix
2. IR2.2 Two Retention Systems, Not One
3. IR2.3 Choosing Where the Records Go
4. IR2.4 Retention Per Record Type
5. IR2.5 Turning On What Is Off
6. IR2.6 The Permissions Your Rota Needs
7. IR2.7 Alerting on the Durable Artifacts
8. IR2.8 Practicing the Collection
9. IR2.9 Documenting What the Tenant Records
10. IR2.10 What You Can Now Promise
11. IR2.11 Simulating the Attack You Prepared For

Phase 2: Detection, Investigation, and Containment

Detection and Analysis

Where a case reaches you from, what each source can tell you when it arrives, and how the records in a Microsoft 365 tenant turn a signal into a scoped incident.

1. IR3.1 Detection Sources in Microsoft 365
2. IR3.2 Unified Audit Log Fundamentals
3. IR3.3 Entra ID Sign-in and Risk Analysis
4. IR3.4 Email Threat Detection with Defender for Office 365
5. IR3.5 Defender XDR Incidents and Alert Correlation
6. IR3.6 Mailbox and Exchange Forensic Signals
7. IR3.7 OAuth Apps, Consent Grants and Persistence Detection
8. IR3.8 SharePoint, OneDrive and Teams Activity Analysis
9. IR3.9 Advanced Hunting with KQL
10. IR3.10 Triage, Scoping and Investigation Timeline Building
11. IR3.11 See It Done: One Case, Ten Surfaces
12. Check My Knowledge

Evidence Collection

Evidence taken in a way that will hold. What you cannot image, what preservation buys, the index that omits without telling you, and the package somebody else will rely on.

1. IR4.1 What You Cannot Image
2. IR4.2 Preserve Before You Collect
3. IR4.3 The Tool That Replaced Three
4. IR4.4 The Index That Quietly Omits
5. IR4.5 Exporting the Audit Record
6. IR4.6 Capture Before Removal
7. IR4.7 What a Hash Proves
8. IR4.8 Custody Without Custody
9. IR4.9 What You Can Notify On
10. IR4.10 The Package Somebody Else Reads
11. IR4.11 See It Done: The Same Week, From the Collection Side
12. Check My Knowledge

Forensics

What the tenant can still tell you, and what it never recorded.

1. IR5.1 Evidence Inventory, Collection Planning, and What You Can Claim
2. IR5.2 Entra ID Forensic Artifacts
3. IR5.3 Mailbox and Exchange Forensics
4. IR5.4 SharePoint, OneDrive, and Teams Forensics
5. IR5.5 OAuth, Tokens, and Application Forensics
6. IR5.6 Graph Activity Logs: What the Token Did
7. IR5.7 Collection Tooling and Automation
8. IR5.8 Timeline Reconstruction and Cross-Source Correlation
9. IR5.9 M365 Anti-Forensic Techniques
10. IR5.10 Hybrid Identity Forensics
11. IR5.11 See It Done: A Question Four Months Late
12. Check My Knowledge

Containment and Eradication

An attacker removed, and the removal verified.

1. IR6.1 Containment Without Infrastructure
2. IR6.2 Revocation, and the Four Populations It Misses
3. IR6.3 The Policy You Write Under Pressure and Delete Afterwards
4. IR6.4 Disabled, Contained, or Left Running
5. IR6.5 The Reset That Leaves a Method Behind
6. IR6.6 Application and Workload Identity Containment
7. IR6.7 The Mailbox Footholds, and the Limits on Removing Them
8. IR6.8 Sharing Links Outlive Identity
9. IR6.9 Proving It Landed
10. IR6.10 The Sync Boundary
11. IR6.11 See It Done: The Morning It Was Already Contained
12. Check My Knowledge

Phase 3: Responding by Attack Type

Responding by Attack Type

The same lifecycle behaves differently depending on what the attacker came for.

1. IR7.1 The Window Between Access and Containment
2. IR7.2 When the Session Is What Was Stolen
3. IR7.3 Consent Phishing and the App That Stays
4. IR7.4 Business Email Compromise
5. IR7.5 Ransomware Without an Endpoint
6. IR7.6 When the Subject Works Here
7. IR7.7 When the Compromise Is the Vendor's
8. IR7.8 When the Identity Is an AI
9. IR7.9 The Identity That Leaves Your Tenant
10. IR7.10 When Two of These Are Running at Once
11. IR7.11 See It Done: One Campaign, Four Playbooks
12. Check My Knowledge

Phase 4: Hunting and the Aftermath

Threat Hunting

Asking a question no rule was written for.

1. IR8.1 Hunting Without an Alert
2. IR8.2 A Hypothesis You Can Be Wrong About
3. IR8.3 How Far Back You Can Actually Look
4. IR8.4 The Identity Tables and the Date in October
5. IR8.5 Hunting What the Response Left Behind
6. IR8.6 When Nothing Was Added
7. IR8.7 A Result Is Not Yet a Finding
8. IR8.8 From a Hunt to a Rule That Runs Without You
9. IR8.9 The Rule You Wrote a Year Ago
10. IR8.10 When the Hunt Finds Nothing
11. IR8.11 See It Done: One Hypothesis, Start to Finish
12. Check My Knowledge

Post-Incident and Communication

A report, a notification and a control change.

1. IR9.1 The Report That Outlives the Evidence
2. IR9.2 Where the Causal Chain Actually Stops
3. IR9.3 What the Collection Lets You Notify
4. IR9.4 Three Clocks, One Incident
5. IR9.5 The Numbers Somebody Will Check
6. IR9.6 Privilege Over an Export
7. IR9.7 Four Readers, One Set of Facts
8. IR9.8 The Metric That Improves as Your Evidence Gets Worse
9. IR9.9 Findings Into Tenant Changes
10. IR9.10 What Closed Actually Means
11. IR9.11 See It Done: From a Statement to a Verified Change
12. Check My Knowledge

Phase 5: Recovery

Recovery

Getting the tenant back, and being able to say so.

1. IR10.1 Recovery Is Not Undo
2. IR10.2 The Order That Stops a Restore Reinviting the Actor
3. IR10.3 Mail: The One Window You Control
4. IR10.4 Files: Two Safety Nets, and One Is a User Setting
5. IR10.5 The Identity You Deleted
6. IR10.6 Teams: There Is No Restore
7. IR10.7 When Retention Fights Recovery
8. IR10.8 What Cannot Be Recovered
9. IR10.9 Proving It Came Back
10. IR10.10 Who Declares It Over
11. IR10.11 See It Done: A Library, a Setting, and Four Days
12. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

Investigation and response queries organized by lifecycle stage, each carrying whether the finding would survive challenge.

1. Evidence Acquisition and Forensics
2. Threat-Specific Response
3. From Alert to Eradication
4. Coverage, Before and After
5. The Capability Around the Incident
6. Legal, Compliance and Communications
7. Tables, Retention and Clocks
8. Recovery Windows and Limits

Cookbooks

Eight procedures, from working an incident through to the report and the review, each with the branches and the record it has to leave.

1. Working an Incident to Scope
2. Containing Without Losing the Evidence
3. Proving Eradication Rather Than Declaring It
4. Writing the Investigation Report
5. Collecting Evidence You Can Rely On Later
6. Preparing the Notification Input
7. Running the Post-Incident Review
8. Restoring Without Reinviting the Actor

Lab Setup

Five pages to a tenant you can respond in, including what it costs and when, and how to produce an incident worth investigating.

1. The Tenant, and What It Costs
2. The Endpoint and Server Layers
3. Producing an Incident to Respond To
4. Practicing Containment Safely
5. Verify, and What the Lab Cannot Teach

Walkthroughs

Seven worked cases where the investigation was competent and the conclusion did not hold.

1. The Finding the Report Could Not Carry
2. The Containment That Held Nothing
3. The Scope That Stopped Where the Logs Did
4. The Clean Check That Could Not Fail
5. Two Incidents That Read as One
6. The Clock That Started Before Anybody Noticed
7. The Evidence That Could Not Be Used

Response Playbooks

Eight playbooks for responding under a constraint: a running clock, expiring evidence, a live actor, a failed eradication, a filed report that changed.

1. The Clock Is Running and the Scope Is Open
2. The Evidence Is Expiring While You Work
3. The Actor Is Still Moving
4. A Closed Incident Was Never Eradicated
5. The Facts Changed After the Report Went Out
6. A Supplier Tells You They Were Breached
7. A Legal Hold Arrives Mid-Response
8. A Restore Brought the Damage Back

Playground

Where to practice responding, and the two things about this discipline no practice surface can give you.

Operational Reference

The consolidated lookup and the step-by-step procedures from this course, in one place.

1. Investigation Quick Reference
2. Incident Response Field Manual

References & Further Reading

External sources this course draws on: vendor documentation, frameworks, standards, and research.

Course Completion

Course Exam

Cloud Incident Response end-of-course exam, a simulation-based assessment testing your ability to triage, investigate, contain, and report on a multi-stage Microsoft 365 incident using the skills built across all ten modules.

1. Course Completion. Cloud Incident Response

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