

Endpoint Security Operations

SEC411

Operate and defend an endpoint estate you did not build. Write detections against endpoint telemetry, run a hunt that starts from a question, triage and contain a compromise under time pressure, and decide what to preserve before an investigation needs it.

Modules	17
Lessons	131
Phases	5
Free preview	Course Orientation (12 lessons)

The method

The course is organized around what an operator does with an estate rather than around the products they do it with.

1. The telemetry decides what is possible. Every detection and every hunt in this course is written against tables that exist, with the volume limits and retention windows named, because a rule against data you do not have is a rule that never fires.
2. Write the detection with its failure mode. A rule without a documented false positive profile and a stated data dependency is a rule somebody will disable during the first busy week.
3. Hunt from a hypothesis. A query with no question behind it produces results nobody can act on. Each hunt in this course states what it expects to find and what a null result would mean.
4. Triage to a disposition, not to a feeling. Every alert ends in escalate, contain or close, with the evidence that decided it recorded.
5. Decide collection before you need it. Forensic readiness is a set of configuration decisions taken while nothing is happening, and it is the phase that determines whether an investigation is possible at all.

The course closes on the adversary who knows which controls you deployed, and on wiring endpoint signal into the wider estate so that response happens without a person present.

What this course assumes

No minimum experience and no prerequisite course. Every concept is explained at first use, and the telemetry, the sensor model and the response surface are restated here rather than assumed from elsewhere.

What makes it go faster: access to a Defender for Endpoint tenant with advanced hunting, and an estate with enough activity in it to query. Neither is required to follow the material.

What this course does not cover: deploying and hardening the estate in the first place, which is ARC402 Endpoint Security Engineering; and deep artifact examination, which is FOR501 Windows Endpoint Investigation and FOR502 Endpoint Memory Forensic Investigation. This course stops at collection and preservation rather than analysis.

Full syllabus

Phase 1: What You Are Operating

Course Orientation [FREE PREVIEW](#)

What endpoint security operations is as a job, what this course assumes is already deployed, and how to establish it.

1. EO0.1 The Job This Course Is For
2. EO0.2 What Is Already Deployed
3. EO0.3 The Signal You Inherit
4. EO0.4 The Queue
5. EO0.5 Four Things That Go Wrong
6. EO0.6 The Estate You Are Operating
7. EO0.7 Detection, Hunting and Triage
8. EO0.8 What Good Looks Like
9. EO0.9 The Adversary You Operate Against
10. EO0.10 How This Course Is Ordered
11. EO0.11 See It Done: A Week on the Queue
12. Module Summary

The Telemetry You Are Operating

What endpoint telemetry actually is before you query it: where rows come from, what the pipeline does to them on the way, what each table can and cannot answer, and the eight properties that return a plausible wrong answer with nothing to indicate it.

1. EO1.1 What the Sensor Actually Records
2. EO1.2 From Action on Disk to Row in a Table
3. EO1.3 Process Events, and Their Blind Spots
4. EO1.4 The High-Volume Three
5. EO1.5 The Two That Answer Scope
6. EO1.6 What Your Own Controls Decided
7. EO1.7 Time, Ordering and Joins That Hold
8. EO1.8 Where the Sensor Cannot See
9. EO1.9 The EDR Surface You Inherited
10. EO1.10 Linux and macOS Change the Query
11. EO1.11 See It Done: One Intrusion, Six Tables
12. Module Summary

Phase 2: Hunting and Detection

EO2, KQL for Endpoint Hunting

Proactive threat hunting across MDE endpoint tables.

1. EO2.1 What Makes a Hunt a Hunt
2. EO2.2 Hunting the Process Table
3. EO2.3 Hunting Command and Control by Shape
4. EO2.4 What a Process Leaves Behind
5. EO2.5 How Far Did It Reach
6. EO2.6 Joins That Return What You Meant
7. EO2.7 Getting Inside the Field
8. EO2.8 Hunting Tools That Are Supposed to Be There
9. EO2.9 Ancestry Beyond Three Generations
10. EO2.10 A Library Somebody Else Can Run
11. EO2.11 See It Done: One Hunting Week
12. Module Summary

EO3, Detection Engineering for Endpoints

Building endpoint detection rules that fire: placement, table selection, the conversion from hunt to rule, technique detections for credential access, lateral movement and persistence, indicator value, automation by measured confidence, and proving a rule is capable of firing before trusting its...

1. EO3.1 Where a Detection Belongs
2. EO3.2 Which Table Can Carry a Detection
3. EO3.3 Writing a Query That Runs Forever
4. EO3.4 Detecting Credential Access
5. EO3.5 Detecting Lateral Movement
6. EO3.6 Detecting Persistence and Interference
7. EO3.7 What an Indicator Is Worth
8. EO3.8 Choosing What to Automate
9. EO3.9 Proving a Rule Can Fire
10. EO3.10 Detections as Production Code
11. EO3.11 See It Done: One Detection, One Week
12. Module Summary

Phase 3: Readiness and Response

EO4, Forensic Readiness & Artifact Collection

Decide what an investigation will be able to see, while nothing is wrong.

1. EO4.1 What You Can Collect Is Decided in Advance
2. EO4.2 Audit Policy, and the Half That Is Usually Missing
3. EO4.3 PowerShell Logging, and the Engine That Ignores It
4. EO4.4 Sysmon, and the Two Filter Rules That Catch Everyone
5. EO4.5 Getting the Log Off the Machine
6. EO4.6 Collection You Run During an Incident
7. EO4.7 Memory, and the Decisions That Decide Whether You Get Any
8. EO4.8 Investigating a Host You Have Contained
9. EO4.9 Asking the Estate a Question
10. EO4.10 The Control That Stops One Machine Becoming All of Them
11. EO4.11 Lab: The Readiness Nobody Owns
12. Module Summary

EO5, Alert Triage, Investigation & Containment

Operationalize the detection layer. Triage MDE alerts in 60 minutes, investigate using device timeline and process tree analysis, execute containment at scale, and apply incident-type-specific playbooks for ransomware, commodity malware, and living-off-the-land attacks.

1. EO5.1 The Queue Is Not the Incident
2. EO5.2 The 60-Minute Endpoint Triage Rule
3. EO5.3 Device Timeline Exploration
4. EO5.4 Process Tree Analysis
5. EO5.5 Investigation Playbook: Ransomware on Endpoint
6. EO5.6 Investigation Playbook: Commodity Malware
7. EO5.7 Investigation Playbook: Living-off-the-Land
8. EO5.8 Evidence Collection Without Breaking Chain of Custody
9. EO5.9 Containment at Scale
10. EO5.10 Decision Trees: Ransomware, Commodity and Living off the Land
11. EO5.11 Interactive Lab: Endpoint Investigation and Containment
12. Module Summary

Phase 4: Advanced

EO6, Advanced Evasion, Anti-Forensics & Threat Intelligence

Understand what attackers do to bypass the endpoint security stack, process injection, AMSI bypass, ETW tampering, EDR evasion, anti-forensics, from the defender's perspective.

1. EO6.1 Why Defenders Need to Understand Evasion
2. EO6.2 Process Injection Techniques
3. EO6.3 AMSI Bypass and Script-Level Evasion
4. EO6.4 ETW Tampering and Blind Spots
5. EO6.5 EDR Evasion: What Attackers Do
6. EO6.6 Anti-Forensics on Endpoints
7. EO6.7 Defense Evasion and Living off the Land at Scale
8. EO6.8 Validation: Red Team and Purple Team
9. EO6.9 Threat Intelligence Driven Defense
10. EO6.10 Building Resilient Detections
11. EO6.11 Interactive Lab: Evasion-Aware Defense
12. Module Summary

EO7, Zero Trust, Integration & Automation

Connect the endpoint security architecture to the broader security ecosystem.

1. EO7.1 What Compliant Actually Asserts
2. EO7.2 Retention Tiers, and What They Remove
3. EO7.3 The Session That Survives Isolation
4. EO7.4 Servers, Cloud Workloads and the Device Population
5. EO7.5 Joining the Endpoint to Email and Identity
6. EO7.6 What Is Safe to Automate
7. EO7.7 Automation That Crosses a Boundary
8. EO7.8 Working Through the API
9. EO7.9 What Leaves the Tenant
10. EO7.10 The Seams Between Systems
11. EO7.11 Interactive Lab: One Night, Three Seams
12. Module Summary

Phase 5: Capstone

EO8, Capstone: Running Endpoint Defense

One estate, seven phases, and two documents somebody can be held to.

1. EO8.1 Capstone Briefing
2. EO8.2 Phase 1: The Telemetry You Have
3. EO8.3 Phase 2: The Hunt Cycle
4. EO8.4 Phase 3: The Detection Portfolio
5. EO8.5 Phase 4: Collection Decided in Advance
6. EO8.6 Phase 5: The Triage Hour
7. EO8.7 Phase 6: Assuming It Was Read
8. EO8.8 Phase 7: Proving the Arrangements
9. EO8.9 Validation: What You Can Prove
10. EO8.10 The Operations Runbook
11. EO8.11 Interactive Lab: The Quarter Reviewed
12. Module Summary

Phase 0: Course Resources

Cheatsheets

Subject-area sheets for endpoint operations: the question, the query that settles it, the fields that carry the decision, and what the answer does not prove.

1. Which Table Answers the Question
2. Hunting Patterns That Hold
3. Reading a Detection Rule
4. Collecting From a Host
5. Taking an Alert to a Disposition
6. What Stopped Reporting

Cookbooks

Four procedures an endpoint operator repeats: running a hunt cycle, shipping a detection, working an alert to a closure, and collecting from a host under time pressure.

1. Running a Hunt Cycle
2. Shipping a Detection
3. Working an Alert to a Closure
4. Collecting Under Time Pressure

Lab Setup

A complete operations lab: tenant, licensing, endpoints, onboarding, the activity worth hunting, and the checks that prove it works.

1. Tenant and Licensing
2. Building the Endpoints
3. Onboarding and Telemetry
4. Generating Activity Worth Hunting
5. Verify and Limits

Walkthroughs

Worked operations 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 Hunt That Could Not Have Found It
2. The Closure That Was Reopened
3. The Timeline That Inverted

Playbooks

Three operations events with a procedure each: prerequisites, a pre-flight that validates the sources, a numbered sequence, tiered disposition and a worked handoff.

1. A Class Went Quiet
2. An Alert Class Is Producing Volume
3. A Host Is Confirmed Compromised Out of Hours

Playground

Where to practice the operations work in this course against populated data, and where your own lab is still the only option.

Operational Reference

Every command, query and recurring check from the Endpoint Security Operations course, consolidated for the working moment rather than for learning.

1. The Operational Cadence

Course Completion

Course Exam

Endpoint Security Operations 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. Endpoint Security Operations

Generated 2026-09-10 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/endpoint-security-operations/