

Offensive Security for Defenders

SEC403

Think like an attacker to defend like an expert. Learn offensive security techniques to understand real attacker campaigns, uncover detection gaps, and build resilient defenses that go far beyond alerts.

Modules	21
Lessons	198
Phases	2
Free preview	Course Orientation (6 lessons)

The method

This is an offensive course written for defenders, so every technique is taught with the artifact it leaves rather than the outcome it achieves. The loop is the same throughout.

1. Run the technique yourself. Reading about an attack tells you what it does. Running it tells you what it produces, and only the second is detectable.
2. Find what it wrote down. Every technique touches something: a process, a registry key, an authentication event, a network flow. That footprint is the detection surface.
3. Ask what the attacker can change and what they cannot. A tool name is changeable. The syscall the technique depends on is not. Detections built on the second survive.
4. Build the detection against the durable half. Then test it by running the technique again, which is the only proof that the rule works.
5. Try to defeat your own rule. If you can bypass it in ten minutes, so can somebody who does this for a living, and better to find out now.

What this course assumes

No minimum experience and no prerequisite course, and no offensive background assumed. The course teaches the attacker's technique to the depth a defender needs and not beyond it.

What makes it go faster: a lab you can break, virtual is fine, and comfort at a command line. Neither is required, and every technique is shown with the telemetry it produced.

What this course does not cover: penetration testing as a profession, exploit development, and red team operations. Offensive technique here is a means to a detection, and the course does not pretend otherwise.

Full syllabus

Phase 1: Offensive Foundations

Course Orientation [FREE PREVIEW](#)

What Offensive Security for Defenders teaches: learn the attacker's full campaign from the inside, recon, infrastructure, access, credentials, lateral movement, evasion, objectives, so you can build detection at every stage and turn real TTPs into production Sentinel and Defender XDR detections.

1. OD0.1 The Gap Between Alerts and Campaigns
2. OD0.2 How Attackers Think Differently from Defenders
3. OD0.3 The Pyramid of Pain. Why Operational Patterns Matter
4. OD0.4 What This Course Teaches and What It Doesn't
5. OD0.5 Course Roadmap, 12 Modules in Context
6. Module Summary

How Attackers Plan Operations

The offensive lifecycle from the attacker's perspective.

1. OD1.1 The Offensive Lifecycle. Planning to Objective
2. OD1.2 Target Selection and Objective Mapping
3. OD1.3 Constraint Analysis. Budget, Time, and Capability
4. OD1.4 Risk Tolerance and Operational Security
5. OD1.5 Passive Reconnaissance. What's Visible Before the Attack
6. OD1.6 Active Reconnaissance. Probing Without Being Caught
7. OD1.7 The Attacker's Decision Matrix
8. OD1.8 Operational Timing. Why Attacks Happen When They Do
9. OD1.9 Team Structures and Attacker Roles
10. OD1.10 Documented Campaigns. Ransomware Operations
11. OD1.11 Documented Campaigns. Espionage and Supply Chain
12. OD1.12 The Defender's Operational Profile
13. Module Summary
14. Check My Knowledge

Phase 2: The Campaign Lifecycle

Offensive Infrastructure, Build, Stage, Burn

How attackers build and manage C2 infrastructure: team servers, redirectors, domain fronting, CDN abuse, cloud-hosted C2, and disposable infrastructure.

1. OD2.1 Infrastructure as an Operational System
2. OD2.2 Command and Control Frameworks. Building and Detecting C2 Traffic
3. OD2.3 Redirectors, Domain Fronting, and CDN Abuse
4. OD2.4 Domain and Certificate Tradecraft
5. OD2.5 Cloud-Hosted Attack Infrastructure
6. OD2.6 Infrastructure Lifecycle. Build, Stage, Operate, Burn
7. OD2.7 Detecting Infrastructure Staging Before the Attack
8. OD2.8 Infrastructure Rotation. How Attackers Survive Your Blocking
9. OD2.9 Phishing Infrastructure. A Separate Operation
10. OD2.10 Exfiltration Channels. The Infrastructure You Haven't Found
11. OD2.11 Infrastructure Takedown. Dismantling vs Monitoring
12. OD2.12 Campaign Telemetry Exercise. Infrastructure Staging
13. Module Summary
14. Check My Knowledge

Payload Engineering and Delivery Tradecraft

How attackers build, obfuscate, and deliver payloads.

1. OD3.1 The Payload Decision Tree
2. OD3.2 Dropper and Loader Architecture. Multi-Stage Delivery
3. OD3.3 Obfuscation and Evasion. What Survives and What Doesn't
4. OD3.4 AMSI, ETW, and Runtime Evasion
5. OD3.5 Mark-of-the-Web Bypass and Trusted Binary Abuse
6. OD3.6 Delivery Method Selection. The Attacker's Routing Decision
7. OD3.7 Email-Based Delivery. From Crafted Phish to Mass Campaign
8. OD3.8 Web-Based Delivery. Watering Holes, Drive-Bys, and SEO Poisoning
9. OD3.9 Supply Chain and Trusted Relationship Delivery
10. OD3.10 Payload Testing. How Attackers QA Before Delivery
11. OD3.11 The Delivery-to-Execution Chain. Connecting the Artifacts
12. OD3.12 Campaign Telemetry Exercise. Payload Delivery
13. Module Summary
14. Check My Knowledge

Initial Access, The Attacker's Decision Tree

How attackers choose their initial access method based on the target's visible defenses.

1. OD4.1 The Initial Access Decision
2. OD4.2 AiTM Phishing. The MFA Bypass
3. OD4.3 Device Code Phishing
4. OD4.4 OAuth Consent Phishing
5. OD4.5 Exploiting Public-Facing Applications
6. OD4.6 Trusted Relationship Abuse
7. OD4.7 What the Access Method Reveals
8. OD4.8 Containing Initial Access. Method-Specific Response
9. OD4.9 Pre-Access Staging Detection
10. OD4.10 Access Method Correlation Across Log Sources
11. OD4.11 Campaign Telemetry Exercise. Initial Access
12. OD4.12 Interactive Lab: Initial Access Classifier
13. Module Summary
14. Check My Knowledge

The First 30 Minutes, Post-Compromise Operations

What the attacker does immediately after landing and why they do it in a specific order.

1. OD5.1 The Post-Compromise Priority List
2. OD5.2 Discovery Command Sequences
3. OD5.3 Environment Profiling. What the Attacker Learns
4. OD5.4 Credential Harvesting Priorities
5. OD5.5 Persistence Decisions
6. OD5.6 C2 Establishment and Validation
7. OD5.7 Defense Evasion in the First Minutes
8. OD5.8 The 30-Minute Detection Window
9. OD5.9 Access-Method-Specific Post-Compromise Sequences
10. OD5.10 Automated vs Manual Post-Compromise
11. OD5.11 Containing the First 30 Minutes
12. OD5.12 Campaign Telemetry Exercise. The First 30 Minutes
13. Module Summary
14. Check My Knowledge

Credential Operations, The Keys to the Kingdom

How attackers think about credentials as operational resources, not individual passwords to steal, but an inventory of keys with different values, lifespans, and reuse potential.

1. OD6.1 Credentials as Operational Resources
2. OD6.2 Password and Hash Operations
3. OD6.3 Kerberos Abuse as an Operational System
4. OD6.4 Token and Session Operations
5. OD6.5 Certificate-Based Credential Abuse
6. OD6.6 Cloud Credential Operations
7. OD6.7 Credential Reuse Chains
8. OD6.8 Credential Tiering Failures
9. OD6.9 Credential Operation Detection at Campaign Scale
10. OD6.10 Defending the Credential Lifecycle
11. OD6.11 Campaign Telemetry Exercise. Credential Operations
12. OD6.12 Interactive Lab: Credential Chain Mapper
13. Module Summary
14. Check My Knowledge

Lateral Movement as Operational Maneuver

Not just 'T1021', how attackers decide WHERE to move, WHAT credentials to use, WHEN to move, and HOW FAST to move.

1. OD7.1 Movement as a Decision Problem
2. OD7.2 Target Prioritization. Where to Move and Why
3. OD7.3 Protocol Selection. How to Move
4. OD7.4 Movement Timing and Pacing
5. OD7.5 Trust Relationships as Movement Highways
6. OD7.6 Multi-Hop Movement Analysis
7. OD7.7 Cloud Lateral Movement
8. OD7.8 Lateral Movement Evasion
9. OD7.9 Movement Detection Across Log Sources
10. OD7.10 Containing Lateral Movement
11. OD7.11 Campaign Telemetry Exercise. Lateral Movement
12. OD7.12 Interactive Lab: Movement Path Reconstructor
13. Module Summary
14. Check My Knowledge

Defense Evasion at the Operational Level

How attackers think about your defenses, not as impenetrable barriers but as a landscape of controls to navigate.

1. OD8.1 The Evasion Mindset
2. OD8.2 EDR Evasion Philosophy
3. OD8.3 Log Awareness and Evidence Destruction
4. OD8.4 Timestomping and Anti-Forensics
5. OD8.5 Living Off the Land. Blending with the Environment
6. OD8.6 Detection Testing by the Attacker
7. OD8.7 Adapting Mid-Campaign
8. OD8.8 Cloud Evasion
9. OD8.9 The Meta-Signals of Evasion
10. OD8.10 Evasion-Aware Detection Design
11. OD8.11 Campaign Telemetry Exercise. Defense Evasion
12. OD8.12 Interactive Lab: Evasion Detection Challenge
13. Module Summary
14. Check My Knowledge

Objectives: Data Theft, Ransomware, Espionage, Sabotage

The endgame. Modules 4–8 taught the operational journey, initial access, post-compromise, credentials, lateral movement, evasion. Module 9 covers what happens when the attacker reaches the objective. Ransomware deploys through a specific operational sequence: backup destruction, shadow copy...

1. OD9.1 Objective Execution as the Culmination of Operations
2. OD9.2 Ransomware as an Operational Sequence
3. OD9.3 Data Theft and Exfiltration Operations
4. OD9.4 Double Extortion Operations
5. OD9.5 Espionage Operations. The Long Game
6. OD9.6 Business Email Compromise Operations
7. OD9.7 Sabotage and Destructive Operations
8. OD9.8 Cloud-Native Objective Execution
9. OD9.9 Detecting Objective Staging
10. OD9.10 Objective-Informed Containment
11. OD9.11 Campaign Telemetry Exercise. Objective Execution
12. OD9.12 Interactive Lab: Objective Classifier
13. Module Summary
14. Check My Knowledge

Campaign Reconstruction

The capstone defensive skill. Three alerts arrive across three systems over six hours: a suspicious PowerShell execution, an unusual logon, and a new scheduled task. Each triggers a rule. Each is triaged independently. Each is closed as low-severity. Together, they're a credential-access...

1. OD10.1 From Alerts to Narrative
2. OD10.2 Campaign Timeline Construction
3. OD10.3 Multi-Source Correlation Techniques
4. OD10.4 Behavioral Clustering
5. OD10.5 Kill Chain Reconstruction
6. OD10.6 Filling the Gaps
7. OD10.7 Attribution at the Operational Level
8. OD10.8 Building Campaign-Level Detection Rules
9. OD10.9 Confidence Scoring and Alternative Hypotheses
10. OD10.10 The Investigation Brief
11. OD10.11 Campaign Telemetry Exercise, 72-Hour CHAIN-HARVEST
12. OD10.12 Interactive Lab: Campaign Reconstruction Tool
13. Module Summary
14. Check My Knowledge

Threat-Informed Defense

The final module. Modules 0–10 taught you how attackers think, plan, execute, evade, and achieve their objectives, and how defenders detect, correlate, and reconstruct campaigns. Module 11 translates that understanding into program-level decisions. Attacker economics: hash values and IPs are...

1. OD11.1 From Understanding to Strategy
2. OD11.2 Attacker Economics. What's Cheap and What's Expensive
3. OD11.3 Threat Modeling from the Attacker's Perspective
4. OD11.4 Detection Coverage Mapping
5. OD11.5 Prioritizing Detection Investment
6. OD11.6 The Detection Portfolio
7. OD11.7 The Program Rhythm
8. OD11.8 Measuring Detection Program Effectiveness
9. OD11.9 The Threat-Informed Detection Roadmap
10. OD11.10 Threat Model Exercise. Build the NE Detection Roadmap
11. OD11.11 Interactive Lab: Detection Portfolio Assessor
12. Module Summary
13. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

Detection sheets organized by attacker stage, each rule carrying how durable it is against the operator adapting.

1. Infrastructure and Staging
2. Initial Access
3. The First Thirty Minutes
4. Credential Operations
5. Lateral Movement
6. Defense Evasion
7. Objectives and Impact
8. Campaign Reconstruction
9. Threat-Informed Defense
10. Stages, Tables and Anchors

Cookbooks

Seven procedures for converting attacker understanding into detection capability, each with a state to reach.

1. Raising a Detection's Anchor Tier
2. Scoping an Intrusion From One Alert
3. Choosing Containment by Objective
4. Validating a Detection Against the Technique
5. Running a Purple Team Exercise
6. Building a Campaign-Level Detection
7. Auditing the Detection Portfolio

Lab Setup

An isolated lab for running attacker techniques safely, and the telemetry to observe them from the defender's side.

1. Isolation and Safety
2. The Domain and Hosts
3. Telemetry
4. Tooling and the First Technique
5. Verify and Limits

Walkthroughs

Worked cases where understanding the operator's constraints changes the answer, including the wrong turns.

1. The Rule That Stopped Working
2. The Purple Team That Found Nothing
3. The Beacon That Was a Backup Agent
4. The Containment That Cost Us the Operator
5. The Advisory We Were Not Affected By
6. The Rule That Could Never Have Fired
7. The Campaign We Only Saw the End Of

Playbooks

Seven events that arrive with an offensive question attached, each with prerequisites, a pre-flight, a numbered sequence and a worked handoff.

1. A Behavioral Detection Fired
2. An Operator Appears to Be Adapting
3. A Technique Fired With No Playbook
4. A Third Party Told Us
5. Somebody Is Testing Our Detections
6. A Red Team Engagement Is Starting
7. A Rule We Rely On Went Silent

Playground

Where to practice reading attacker telemetry, and which half of this course a simulator cannot teach.

Operational Reference

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

1. Campaign Detection Quick Reference
2. Offensive-to-Defensive Field Manual

References & Further Reading

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

Course Completion

Course Exam

Offensive Security for Defenders 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. Offensive Security for Defenders

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