

Threat Detection Engineering

SEC401

Design, build, and operationalize advanced detection capabilities that stop modern threats across on-prem and cloud environments. Write KQL detection rules against real attacker techniques, measure ATT&CK coverage, manage false positives systematically, and run a detection-as-code pipeline.

Modules	22
Lessons	200
Phases	3
Free preview	Course Orientation (11 lessons)

The method

A detection is a claim that a technique is visible in your data. This course runs the same loop for every rule it builds, and the loop is what makes a rule library into a detection program.

1. Model the threat before writing anything. Which techniques matter to your organization, against your data sources, is a prioritization question. A backlog assembled from a framework rather than from a threat model is a backlog with no order in it.
2. Establish the data source can see it. A rule against a field your estate does not collect is inert and looks identical to a rule that never fires because nothing happened.
3. Write against the durable artifact. The thing the technique cannot avoid doing, rather than the tool that happened to do it this time.
4. Test positively and negatively. Fire the technique and confirm the rule catches it. Run it across normal activity and count what came back. Skipping the second is how alert fatigue is manufactured.
5. Manage it as a lifecycle. Rules decay. Schemas change underneath them, environments change around them, and a rule nobody has re-validated is a coverage claim rather than a control.

The course closes on a ninety-day detection program: not a rule set, an operating model with coverage measured and reviewed.

What this course assumes

No minimum experience and no prerequisite course. KQL, the Sentinel rule model and the ATT&CK framework are all introduced where they first matter.

What makes it go faster: a Sentinel workspace with real data, and any prior query-language exposure. Neither is required, and every rule in the course is written against data the course provides.

What this course does not cover: incident response process, forensics, and SIEM administration. This course builds the detections; investigating what they catch is a separate discipline.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

What Threat Detection Engineering teaches, the detection rules and pipeline you walk away with, the Microsoft detection surface you build against, and how the course is structured.

1. DE0.1 Detection Engineering. What It Is and Why It Is Important
2. DE0.2 Why Organizations Need Detection Engineers
3. DE0.3 The Detection Coverage, The Gap, The Illusion
4. DE0.4 The Microsoft Detection Surface
5. DE0.5 Measuring Detection
6. DE0.6 Walking CHAIN-HARVEST
7. DE0.7 The Six Attack Chains in Detail
8. DE0.8 MITRE ATT&CK
9. DE0.9 The Detection Engineering Discipline
10. DE0.10 Tools and Capabilities
11. DE0.11 Creating a Detection Engineering Baseline

Detection Rule Architecture in Microsoft Sentinel

How detection rules work architecturally in Sentinel and Defender XDR.

1. DE1.1 Sentinel Analytics Rule Types
2. DE1.2 Anatomy of a Scheduled Rule
3. DE1.3 Entity Mapping and Alert Enrichment
4. DE1.4 Severity, MITRE Mapping, and Documentation
5. DE1.5 NRT Rules and Defender XDR Custom Detections
6. DE1.6 Alert Grouping and Incident Architecture
7. DE1.7 The Rule Specification Template and Common Mistakes
8. Module Summary
9. Check My Knowledge

Phase 2: Detection Library

Threat Modeling for Detection Prioritization

The methodology module. Before building detection rules, you decide which rules to build first. Crown jewel analysis, threat actor profiling, ATT&CK coverage assessment, risk-based gap scoring, detection backlog, sprint planning, and the 90-day roadmap that DE3 through DE8 execute against.

1. DE2.1 Why Threat Modeling Before Rules
2. DE2.2 Crown Jewel Analysis
3. DE2.3 Threat Actor Profiling and Technique Relevance
4. DE2.4 Current Detection Coverage Baseline
5. DE2.5 Risk-Based Gap Scoring and Data Availability
6. DE2.6 Building the Detection Backlog
7. DE2.7 Sprint Planning and the 90-Day Roadmap
8. DE2.8 Communicating the Program to Leadership
9. DE2.9 Maintaining and Evolving the Backlog
10. DE2.10 Threat Intelligence Integration
11. Module Summary
12. Check My Knowledge

Detecting Initial Access

Nine production detection rules for the techniques attackers use to enter your environment.

1. DE3.1 The Initial Access Detection Challenge
2. DE3.2 Phishing Detection Beyond Safe Links
3. DE3.3 Sender Reputation and Email Anomaly Detection
4. DE3.4 Password Spray and Distributed Evasion
5. DE3.5 Token Theft and Session Hijacking
6. DE3.6 Drive-By Download and Watering Hole Detection
7. DE3.7 USB and Removable Media Detection
8. DE3.8 Valid Account Compromise Detection
9. DE3.9 Attachment Phishing and Public-Facing Exploits
10. DE3.10 Cross-Chain Correlation and Deployment Strategy
11. Module Summary
12. Check My Knowledge

Detecting Credential Attacks and Identity Threats

Identity-layer detection. MFA fatigue, MFA registration anomalies, impossible travel that works with VPN, token replay beyond AiTM, PIM role activation abuse, service principal threats, client secret anomalies, and LSASS credential dumping. Eight production KQL rules targeting the techniques...

1. DE4.1 The Credential Access Challenge
2. DE4.2 MFA Fatigue and Push Bombing Detection
3. DE4.3 MFA Registration from Suspicious Context
4. DE4.4 Impossible Travel That Works with VPN
5. DE4.5 Token Replay Beyond AiTM
6. DE4.6 PIM Role Activation Anomalies
7. DE4.7 Role-to-Action Correlation
8. DE4.8 Service Principal Threat Detection
9. DE4.9 Client Secret and Certificate Anomalies
10. DE4.10 LSASS Credential Dumping Detection
11. DE4.11 Cross-Technique Credential Attack Correlation
12. DE4.12 Credential Attack Deployment and Monitoring
13. Module Summary
14. Check My Knowledge

Detecting Persistence and Execution

Post-access detection. Mailbox rules, OAuth consent grants, scheduled tasks, autorun persistence, PowerShell anomalies, local account creation, WMI event subscriptions, file-drop persistence, and execution anomalies.

Nine production detection rules across the persistence and execution surface...

1. DE5.1 The Persistence and Execution Challenge
2. DE5.2 Mailbox Rule Persistence
3. DE5.3 OAuth Consent Grant Persistence
4. DE5.4 Scheduled Task and Service Persistence
5. DE5.5 Autorun Persistence
6. DE5.6 PowerShell Execution Anomaly
7. DE5.7 Local Account Creation
8. DE5.8 WMI Event Subscription Persistence
9. DE5.9 File-Drop Persistence
10. DE5.10 Execution Anomaly
11. DE5.11 Cross-Technique Correlation
12. DE5.12 Deployment and Monitoring
13. Module Summary
14. Check My Knowledge

Detecting Discovery and Defense Evasion

Mid-chain detection. Reconnaissance command sequences, LDAP enumeration, file and system discovery, Defender tampering, event log clearing, mailbox audit manipulation, security configuration drift, process masquerading, and LOLBin proxy execution. Nine production KQL rules targeting the...

1. DE6.1 The Discovery and Defense Evasion Challenge
2. DE6.2 Reconnaissance Command Sequence Detection
3. DE6.3 LDAP and Directory Enumeration
4. DE6.4 File and System Discovery Detection
5. DE6.5 Security Tool Tampering Detection
6. DE6.6 Event Log Clearing and Audit Manipulation
7. DE6.7 Mailbox Audit Log Manipulation
8. DE6.8 Security Configuration Drift Monitoring
9. DE6.9 Process Masquerading Detection
10. DE6.10 LOLBin Proxy Execution Detection
11. DE6.11 Cross-Technique Discovery and Evasion Correlation
12. DE6.12 Deployment and Monitoring
13. Module Summary
14. Check My Knowledge

Detecting Collection and Exfiltration

Objective-phase detection. Email collection, SharePoint bulk download, network share access, USB exfiltration, cloud storage upload, time-series anomaly detection, BEC outbound email, C2 beaconing, external sharing abuse, data staging, and archive compression. Eleven production KQL rules...

1. DE7.1 The Collection and Exfiltration Challenge
2. DE7.2 Email Collection Detection
3. DE7.3 SharePoint and OneDrive Bulk Download Detection
4. DE7.4 Network Share Bulk Access Detection
5. DE7.5 USB Data Exfiltration Detection
6. DE7.6 Cloud Storage Exfiltration Detection
7. DE7.7 Time-Series Anomaly Detection
8. DE7.8 BEC Outbound Email Detection
9. DE7.9 C2 Beaconing and Data Exfiltration Detection
10. DE7.10 External Sharing Abuse Detection
11. DE7.11 Local Data Staging Detection
12. DE7.12 Archive and Compression Detection
13. DE7.13 Cross-Technique Collection Correlation
14. DE7.14 Deployment and Monitoring
15. Module Summary
16. Check My Knowledge

Detecting Lateral Movement and Impact

End-chain detection. RDP first-access lateral movement, WMI remote execution, WinRM and PSRemoting, SMB admin share file deployment, cross-site SD-WAN traversal, ransomware pre-encryption indicators, mass file encryption, SSH lateral movement, and service disruption. Nine production KQL rules...

1. DE8.1 The Lateral Movement and Impact Challenge
2. DE8.2 RDP First-Access Lateral Movement
3. DE8.3 WMI Remote Execution Detection
4. DE8.4 WinRM and PSRemoting Detection
5. DE8.5 SMB Admin Share Lateral Movement
6. DE8.6 Cross-Site SD-WAN Traversal Detection
7. DE8.7 Ransomware Pre-Encryption Indicators
8. DE8.8 Mass File Encryption Detection
9. DE8.9 SSH Lateral Movement to Linux Systems
10. DE8.10 Critical Service Stop Detection
11. DE8.11 Cross-Technique Lateral Movement and Impact Correlation
12. DE8.12 Deployment and Monitoring
13. Module Summary
14. Check My Knowledge

Phase 3: Operations

Detection Testing, Tuning, and Lifecycle Management

The operational discipline module. Pre-deployment testing against historical data, attack simulation for detection validation, threshold optimization, false positive classification, watchlist and exclusion management, exclusion governance, rule health metrics, the monthly tuning review cadence...

1. DE9.1 The Tuning Imperative
2. DE9.2 Testing Before Deployment
3. DE9.3 Attack Simulation and Validation
4. DE9.4 Threshold Optimization
5. DE9.5 False Positive Classification
6. DE9.6 Watchlists and Exclusions
7. DE9.7 Exclusion Governance
8. DE9.8 Rule Health Metrics
9. DE9.9 The Monthly Tuning Review
10. DE9.10 Tuning Case Studies
11. DE9.11 The Tuning Lifecycle
12. Module Summary
13. Check My Knowledge

Detection as Code and Program Management

The engineering maturity module. Portal governance failures, detection-as-code with Git, rule specification standards, CI/CD deployment pipelines, branch strategy and PR review, automated ATT&CK coverage reporting, detection engineering sprints, cross-team collaboration, program metrics...

1. DE10.1 The Portal Governance Problem
2. DE10.2 Detection-as-Code with Git
3. DE10.3 The Rule Specification Standard
4. DE10.4 CI/CD for Detection Rules
5. DE10.5 Branch Strategy and Pull Request Review
6. DE10.6 Coverage Reporting and ATT&CK Heatmaps
7. DE10.7 The Detection Engineering Sprint
8. DE10.8 Cross-Team Collaboration
9. DE10.9 Program Metrics and Executive Reporting
10. DE10.10 The Detection Engineer Operational Cadence
11. DE10.11 SIGMA Rule Portability
12. DE10.12 Sentinel Cost Optimization
13. Module Summary
14. Check My Knowledge

Capstone: The 90-Day Detection Program

The capstone module. You run a complete 90-day detection engineering program as Rachel Okafor, NE's CISO, threat modeling, three detection sprints (credential, persistence/movement, collection/impact), ATT&CK coverage assessment, board reporting, a simulated triage day, gap retrospective, and...

1. DE11.1 Capstone Briefing: The Board Mandate
2. DE11.2 Phase 1: Credential Attack Detection Sprint
3. DE11.3 Phase 2: Persistence and Movement Sprint
4. DE11.4 Phase 3: Collection, Exfiltration, and Config Sprint
5. DE11.5 Full Coverage Assessment
6. DE11.6 The 90-Day Board Report
7. DE11.7 Triage Day: The Full Alert Queue
8. DE11.8 The Detection Gap Retrospective
9. DE11.9 Program Sustainability and Handover
10. Module Summary
11. Check My Knowledge

AI-Accelerated Detection Engineering

AI as a detection engineering accelerator.

1. DE12.1 The AI Acceleration Thesis
2. DE12.2 Threat Advisory to Detection Hypothesis
3. DE12.3 KQL Development and Debugging with AI
4. DE12.4 Rule Specification Generation
5. DE12.5 FP Analysis and Tuning Acceleration
6. DE12.6 AI-Assisted SIGMA Conversion
7. DE12.7 AI-Assisted Attack Simulation Planning
8. DE12.8 AI-Assisted Coverage Gap Analysis
9. DE12.9 The AI-Augmented Detection Workflow
10. DE12.10 AI Limitations and the Human Judgment Boundary
11. Module Summary
12. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

Detection queries by subject area, each with the fields that carry the decision and what the rule will not catch.

1. Rule Mechanics
2. Prioritization
3. Initial Access
4. Credential and Identity
5. Persistence and Execution
6. Discovery and Evasion
7. Collection and Exfiltration
8. Lateral Movement and Impact
9. AI-Assisted Detection
10. Tables, Codes and Coverage

Cookbooks

The established way to do the recurring things: build a rule, test it, tune it, measure coverage, run a sprint, ship as code, report.

1. Building a Rule
2. Testing Before Deployment
3. Tuning a Noisy Rule
4. Measuring Coverage
5. Running a Detection Sprint
6. Shipping Rules as Code
7. The Quarterly Report

Lab Setup

Building an environment you can deploy, test and tune detections in, and the constraint that makes tuning unpracticisable in a clean lab.

1. Building the Environment

Walkthroughs

Rules built end to end, including the ones that never fired, fired too much, or reported as coverage while broken.

1. The Rule That Never Fired
2. The Threshold From One Incident
3. The Backtest That Lied
4. The Coverage Number That Was Wrong
5. The Rule That Broke Silently
6. The Draft That Looked Right
7. The Finding That Did Not Earn a Rule

Playbooks

The established way to get coverage for a threat: the rule set in chain order, what validates it, and where the set is thin.

1. Ransomware
2. Account Takeover
3. Business Email Compromise
4. Insider Data Theft
5. Lateral Movement
6. A Newly Published Technique

Playground

Resources for building detections and using them at work: a query console, graded investigations, a production detection library, and a DFIR toolkit.

Operational Reference

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

1. Detection Rule Quick Reference
2. Detection Engineering Field Manual

References & Further Reading

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

Course Completion

Course Exam

Threat Detection Engineering end-of-course exam: a three-phase simulation testing whether you can apply the method to a case the course did not walk through.

1. Course Completion. Threat Detection Engineering

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