Microsoft 365 SOC Engineering

SEC302

Build and run a high-performing Security Operations Center in Microsoft 365. Design, implement, and optimize modern SOC infrastructure, processes, and workflows using Microsoft Defender XDR, Microsoft Sentinel, Entra ID, and the full Microsoft security stack.

Modules	22
Lessons	182
Phases	4
Free preview	Course Orientation (8 lessons)

The method

A SOC is an engineering product: detections, playbooks, automation and the measurements that tell you whether any of it works. This course runs the same loop for every capability it builds.

1. Establish readiness before capability. Coverage, data sources, roles and escalation paths. Detections built on top of an unclear operating model produce alerts nobody owns.

2. Engineer detections by surface. Identity, email, endpoint, cloud. Each has its own telemetry, its own false positive profile and its own tuning problem.

3. Write the playbook the detection needs. An alert with no investigation path is an alert that gets closed on instinct.

4. Automate what the playbook proved repetitive. Automation built before the manual process is understood automates a guess.

5. Measure, then improve something specific. SOC metrics that nobody acts on are a reporting habit. The measurement exists to change a decision.

What this course assumes

No minimum experience and no prerequisite course. The detection model, the Sentinel surface and the operating concepts are built up from nothing.

What makes it go faster: a workspace you can build in and an alert queue you have seen. Neither is required.

What this course does not cover: forensics, architecture design and GRC. This course builds and runs the SOC as an engineering function.

Full syllabus

Phase 1: Foundation

Course Orientation FREE PREVIEW

What Microsoft 365 SOC Engineering teaches: how to build and run a security operation that detects, responds, and matures.

1. 0.1 What a SOC Actually Does
2. 0.2 The Four Security Operations Functions
3. 0.3 Where Most SOCs Fail
4. 0.4 The SOC Maturity Spectrum
5. 0.5 The Detection-and-Response Pipeline
6. 0.6 What This Course Builds
7. 0.7 Lab Environment and How to Study
8. Module Summary

SOC Foundations and Operational Readiness

The operational foundation that turns a team running on habits into a team running on documented, measurable process.

1. 1.1 SOC Operating Models
2. 1.2 Analyst Tiers and Role Architecture
3. 1.3 Shift Handover Design
4. 1.4 Escalation Framework
5. 1.5 The Triage Decision Framework
6. 1.6 Operational Metrics. Speed vs Quality
7. 1.7 The SOC Charter
8. 1.8 Tool Stack Integration
9. 1.9 SOC Maturity Assessment
10. 1.10 Incident Classification Framework
11. Module Summary
12. Check My Knowledge

Detection Engineering Methodology

Build the detection engineering methodology that governs every rule in the course, threat modeling, detection rule specifications, quality metrics, false positive management, detection-as-code practices, and the detection backlog that prioritizes what you build next.

1. 2.1 The Detection Engineering Lifecycle
2. 2.2 Threat Modeling for Detection Prioritization
3. 2.3 MITRE ATT&CK as a Detection Framework
4. 2.4 Writing Detection Rule Specifications
5. 2.5 Detection Rule Quality Metrics
6. 2.6 False Positive Management
7. 2.7 Detection-as-Code
8. 2.8 Building and Managing a Detection Backlog
9. Module Summary
10. Check My Knowledge

Phase 2: Detection Libraries

Building Identity & Access Detections

Build seven production detection rules for identity-based attacks in Entra ID, anomalous sign-ins, MFA fatigue, impossible travel, privileged role assignment, service principal credential abuse, Conditional Access modification, and password spray.

1. 3.1 SigninLogs Deep Dive. Schema, Fields, and Query Patterns
2. 3.2 Detection: Anomalous Sign-In from Unfamiliar Infrastructure
3. 3.3 Detection: MFA Fatigue and Push Notification Abuse
4. 3.4 Detection: Impossible Travel
5. 3.5 Detection: Privileged Role Assignment Outside PIM
6. 3.6 Detection: Service Principal Credential Manipulation
7. 3.7 Detection: Conditional Access Policy Modification
8. 3.8 Detection: Bulk Sign-In Failures Indicating Password Spray
9. Module Summary
10. Check My Knowledge

Building Email & Collaboration Detections

Build seven production detection rules for BEC operations in Microsoft 365, inbox forwarding, hiding rules, transport rule manipulation, bulk mailbox access, AiTM phishing, mailbox delegation, and outbound BEC execution.

1. 4.1 Email Data Sources in Sentinel. OfficeActivity, EmailEvents, and CloudAppEvents
2. 4.2 Detection: Inbox Forwarding Rule to External Domain After Anomalous Sign-In
3. 4.3 Detection: Inbox Rule Deleting or Moving Items to Hide Adversary Activity
4. 4.4 Detection: Mail Flow Transport Rule Manipulation
5. 4.5 Detection: Bulk Mailbox Access After Account Compromise
6. 4.6 Detection: Email Containing AiTM Phishing Indicators
7. 4.7 Detection: Mailbox Delegation and Permission Changes
8. 4.8 Detection: Suspicious Outbound Email Patterns Indicating BEC Execution
9. Module Summary
10. Check My Knowledge

Building Endpoint & Lateral Movement Detections

Build seven detection rules for endpoint attack surfaces, LOLBin execution chains, credential dumping, lateral movement, persistence mechanisms, ransomware pre-encryption, data staging and exfiltration, and PowerShell-based post-exploitation.

1. 5.1 Defender for Endpoint Data Sources. Schema and Query Patterns
2. 5.2 Detection: LOLBin Execution Chains
3. 5.3 Detection: Credential Dumping Indicators
4. 5.4 Detection: Lateral Movement via SMB, WinRM, and RDP
5. 5.5 Detection: Persistence via Scheduled Tasks, Services, and Registry
6. 5.6 Detection: Ransomware Pre-Encryption Indicators
7. 5.7 Detection: Data Staging and Exfiltration Indicators
8. 5.8 Detection: PowerShell and Script-Based Execution
9. Module Summary
10. Check My Knowledge

Building Cloud & SaaS Detections

Build seven detection rules for cloud and SaaS attack surfaces, OAuth consent phishing, shadow IT, Azure resource manipulation, storage exfiltration, cross-tenant access, application permission escalation, and cloud session anomalies.

1. 6.1 Cloud Application Data Sources
2. 6.2 Detection: Illicit OAuth Application Consent
3. 6.3 Detection: Shadow IT and Unsanctioned Application Usage
4. 6.4 Detection: Azure Resource Manipulation
5. 6.5 Detection: Storage Account Exfiltration Indicators
6. 6.6 Detection: Cross-Tenant Access Anomalies
7. 6.7 Detection: Application Permission Escalation
8. 6.8 Detection: Cloud Session Anomalies
9. Module Summary
10. Check My Knowledge

Phase 3: Investigation & Response

Building Investigation Playbooks

Structured investigation workflows for SOC analysts.

1. 7.1 Playbook Architecture. Structure, Standards, and Design Principles
2. 7.2 Evidence Collection and Preservation Standards
3. 7.3 Containment Decision Framework
4. 7.4 Playbook: AiTM Credential Phishing Investigation
5. 7.5 Playbook: BEC Financial Fraud Investigation
6. 7.6 Playbook: Ransomware Pre-Encryption Detection and Response
7. 7.7 Playbook Maintenance and Continuous Improvement
8. 7.8 Building Custom Playbooks for Your Environment
9. Module Summary
10. Check My Knowledge

Incident Response Documentation & Reporting

Formal incident response documentation from initial notification through post-incident review.

1. 8.1 The Incident Documentation Lifecycle
2. 8.2 Writing the Executive Incident Summary
3. 8.3 Building the Technical Investigation Timeline
4. 8.4 Evidence Documentation and Chain of Custody
5. 8.5 Regulatory Notification Assessment
6. 8.6 Third-Party and Stakeholder Communication
7. 8.7 Post-Incident Review Framework
8. 8.8 IR Report Template Pack
9. Module Summary
10. Check My Knowledge

Phase 4: Operational Maturity

Implementing Hardening Baselines

M365 tenant hardening checklists, Exchange Online protection baselines, Entra ID conditional access templates, endpoint security baselines, and validation KQL queries, the preventive controls that reduce your detection workload.

1. 9.1 The Relationship Between Hardening and Detection
2. 9.2 Entra ID Hardening Baseline
3. 9.3 Exchange Online Hardening Baseline
4. 9.4 Endpoint Security Baseline
5. 9.5 Cloud Application Hardening
6. 9.6 Hardening Validation Queries
7. 9.7 Hardening Change Management
8. 9.8 Hardening Checklist Pack
9. 9.9 Network Segmentation and Firewall Hardening
10. 9.10 SharePoint and OneDrive Hardening
11. Module Summary
12. Check My Knowledge

Building Sentinel Automation

Automation rules, playbook design patterns, SOAR integration, and notification workflows that accelerate SOC response.

1. 10.1 Automation Strategy. What to Automate and What to Keep Manual
2. 10.2 Sentinel Automation Rules
3. 10.3 Logic App Playbooks for Enrichment
4. 10.4 Logic App Playbooks for Notification
5. 10.5 Logic App Playbooks for Containment
6. 10.6 SOAR Integration Patterns
7. 10.7 Automation Testing and Monitoring
8. 10.8 Automation Runbook Pack
9. 10.9 Automated Enrichment Playbooks
10. Module Summary
11. Check My Knowledge

Measuring & Improving SOC Performance

KPI frameworks, Sentinel workbook dashboards, detection coverage tracking, SOC maturity scoring, and monthly reporting templates.

1. 11.1 From Metrics to Dashboards
2. 11.2 Building the SOC Operations Workbook
3. 11.3 Detection Coverage Dashboard
4. 11.4 Monthly SOC Report Template
5. 11.5 Quarterly SOC Maturity Review
6. 11.6 Continuous Improvement Cycle
7. 11.7 Benchmarking Against Industry Standards
8. 11.8 Reporting to Non-Technical Stakeholders
9. Module Summary
10. Check My Knowledge

Building a Threat Intelligence Program

Threat intelligence program design, indicator lifecycle management, STIX/TAXII feed integration, hunting hypothesis generation from TI, and the operational workflow that converts intelligence into detection and response improvements.

1. 12.1 Threat Intelligence Fundamentals for SOC Analysts
2. 12.2 Building a TI Collection Program
3. 12.3 Indicator Lifecycle Management
4. 12.4 STIX/TAXII Integration with Sentinel
5. 12.5 Converting TI into Detection Hypotheses
6. 12.6 TI-Driven Threat Hunting
7. 12.7 TI Operations Playbook
8. 12.8 TI Maturity Assessment
9. Module Summary
10. Check My Knowledge

Copilot for Security in SOC Operations

Using Microsoft Copilot for Security as the AI layer across the SOC operational model, incident investigation, KQL generation, threat hunting, promptbook automation, agent-driven triage, and the governance framework that keeps humans in control of AI-assisted security decisions.

1. 13.1 What Copilot for Security Is (and Isn't)
2. 13.2 Embedded Experience: Incident Investigation
3. 13.3 Natural Language to KQL
4. 13.4 AI-Augmented Threat Hunting
5. 13.5 Promptbooks for SOC Workflows
6. 13.6 Copilot Agents and Automation
7. 13.7 Governance, Cost, and Limitations
8. 13.8 Building AI-Augmented SOC Operations
9. Module Summary
10. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

Subject-area sheets carrying the detection in both forms this course teaches, with the fields that carry the decision and the limits on each.

1. Identity Detections
2. Email and Collaboration Detections
3. Endpoint and Lateral Movement Detections
4. Cloud and SaaS Detections
5. Writing a Detection That Survives
6. Investigation and Response
7. Hardening and Baselines
8. Automation, Metrics and Threat Intelligence
9. Formats, Tables and Limits

Cookbooks

Seven procedures a SOC engineer repeats: building a detection, tuning it, deploying it to both surfaces, and the cycles around them.

1. Building a Detection
2. Tuning a Noisy Rule
3. Working an Incident to a Report
4. Onboarding a Log Source
5. Running a Detection Sprint
6. Retiring a Detection
7. The Monthly Reporting Cycle

Lab Setup

A complete SOC lab: tenant, workspace, Sentinel, connectors, detectable activity, and the cost controls that stop it running away.

1. Workspace and Sentinel
2. Connecting the Sources
3. Generating Detectable Activity
4. Deploying and Proving a Rule
5. Verify, Costs and Limits

Walkthroughs

Worked detection engineering cases end to end, including the wrong turns, the queries that looked right and were not, and what would have changed each answer.

1. The Rule That Fired on Everything
2. The Rule That Missed It
3. The Alert Nobody Could Work
4. The Quarter That Looked Good
5. Three Incidents That Were One
6. The Rule That Did Not Translate
7. The Fix That Broke the Detection

Playbooks

Seven events that arrive at a SOC engineer with a decision attached, each with prerequisites, a pre-flight, a numbered sequence and a worked handoff.

1. A Rule Stopped Firing
2. A Connector Degraded
3. An Incident Was Missed
4. An Automation Took a Wrong Action
5. A Threat Advisory Arrived
6. Somebody Asked If We Are Covered
7. The Workspace Bill Jumped

Playground

Where to practice the detection engineering in this course against populated data and real deployment surfaces.

Resources

References

The quick reference and field manual for this course: the queries, configuration steps and procedures, organized for use during live work.

1. Microsoft 365 SOC Engineering Quick Reference
2. References & Further Reading
3. Microsoft 365 SOC Engineering Field Manual

Course Completion

Course Exam

Microsoft 365 SOC Engineering end-of-course exam, a simulation-based assessment testing your ability to triage, investigate, and respond to a multi-stage incident using the skills built across all 14 modules.

1. Course Completion. Microsoft 365 SOC Engineering

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/m365-soc-engineering/