

Microsoft 365 Security Operations

SEC301

Configure, operate, and optimize the full Microsoft Security stack to run a modern, effective Security Operations Center. Detect, investigate, respond to, and recover from threats across Microsoft 365, Entra ID, Defender XDR, Sentinel, Intune, and Purview.

Modules	26
Lessons	234
Phases	4
Free preview	Course Orientation (8 lessons)

The method

This course covers the Microsoft security stack as an operator uses it, and then works five real intrusions through it end to end. The loop is the same for each.

1. Know what each product actually sees. Defender XDR, Defender for Endpoint, Purview, Defender for Cloud and Sentinel overlap and disagree. Knowing which one holds the answer is most of the speed.
2. Get the data in before writing the query. Connectors, workspace design and retention decide what a hunt can reach. Configuration is not the boring part; it is the ceiling.
3. Query for a question you can state. KQL against a hypothesis rather than a table full of everything.
4. Investigate the intrusion, not the alert. The five worked investigations, adversary-in-the-middle, business email compromise, token replay, consent phishing and insider threat, each start where an alert did and end somewhere else.
5. Turn the finding into a rule and a document. An investigation that changes nothing has produced one closed ticket.

What this course assumes

No minimum experience and no prerequisite course. Every product surface and KQL itself are introduced from the beginning.

What makes it go faster: a tenant with Defender and Sentinel, and any prior query experience. Neither is required; the investigations run against data the course provides.

What this course does not cover: architecture and design decisions, which are a separate course, and deep forensics. This is operating the stack and investigating in it.

Full syllabus

Phase 1: Foundations

Course Orientation [FREE PREVIEW](#)

What Microsoft 365 Security Operations teaches: operate the full Microsoft security stack, Defender XDR, Sentinel, Purview, Defender for Cloud, and Security Copilot, as one SOC, running the detect, investigate, respond, and recover lifecycle and finishing on real investigation scenarios.

1. 0.1 Mission, Course Structure, and Who This Is For
2. 0.2 SC-200 Exam Overview and Study Strategy
3. 0.3 How to Learn from This Course
4. 0.4 Lab Setup: M365 E5 Developer Tenant
5. 0.5 Lab Setup: Azure Subscription and Sentinel Workspace
6. 0.6 Lab Setup: Sample Data and Validation
7. Module Summary
8. Check My Knowledge

Mitigate Threats Using Microsoft Defender XDR

Operate the unified Microsoft Defender XDR platform as an integrated investigation and response tool.

1. 1.1 Introduction to Microsoft Defender XDR Threat Protection
2. 1.2 Mitigate Incidents Using Microsoft Defender XDR
3. 1.3 Remediate Risks with Microsoft Defender for Office 365
4. 1.4 Manage Microsoft Defender for Endpoint Investigations
5. 1.5 Mitigate Threats Using Microsoft Defender for Identity
6. 1.6 Secure Cloud Apps with Microsoft Defender for Cloud Apps
7. 1.7 Unified Portal Operations: Daily SOC Workflow
8. 1.8 Cross-Product Incident Correlation
9. Module Summary
10. Check My Knowledge

Mitigate Threats Using Microsoft Defender for Endpoint

Deploy, configure, and operate Microsoft Defender for Endpoint as a preventive and investigative platform.

1. 2.1 MDE Architecture and Deployment Planning
2. 2.2 Onboarding Devices Across Platforms
3. 2.3 Attack Surface Reduction Rules
4. 2.4 Next-Generation Protection and EDR Configuration
5. 2.5 Device Investigation: Timelines, Forensics, and Evidence Collection
6. 2.6 Response Actions and Live Response
7. 2.7 Automated Investigation and Response (AIR)
8. 2.8 Threat and Vulnerability Management
9. Module Summary
10. Check My Knowledge

Phase 2: Microsoft Security Stack

Mitigate Threats Using Microsoft Purview

Investigate DLP alerts, insider risk incidents, audit log anomalies, and eDiscovery content searches.

1. 3.1 Microsoft Purview for Security Operations
2. 3.2 Data Loss Prevention: Policy Architecture and Alert Pipeline
3. 3.3 Investigating DLP Alerts in the Defender Portal
4. 3.4 Insider Risk Management: Policies, Indicators, and Risk Signals
5. 3.5 Investigating Insider Risk Alerts and Managing Cases
6. 3.6 Microsoft Purview Audit: Standard vs Premium
7. 3.7 Investigating with Audit Log Search
8. 3.8 eDiscovery: Content Search for Security Investigations
9. 3.9 Cross-Product Investigation: Purview + Defender XDR + Sentinel
10. Module Summary
11. Check My Knowledge

Mitigate Threats Using Microsoft Defender for Cloud

Plan, deploy, and operationally manage Microsoft Defender for Cloud across Azure, hybrid, and multi-cloud environments.

1. 4.1 Defender for Cloud Architecture and Foundational Concepts
2. 4.2 Enabling and Connecting Azure Resources
3. 4.3 Connecting Hybrid and Multi-Cloud Environments
4. 4.4 Cloud Security Posture Management (CSPM)
5. 4.5 Defender for Servers: Workload Protection
6. 4.6 Defender for Storage, SQL, and App Service
7. 4.7 Defender for Containers and Kubernetes
8. 4.8 Security Alerts: Investigation and Remediation
9. 4.9 Regulatory Compliance and Security Standards
10. 4.10 Cross-Product Investigation: Defender for Cloud + Sentinel + XDR
11. Module Summary
12. Check My Knowledge

Mitigate Threats Using Microsoft Security Copilot

Use Microsoft Security Copilot to accelerate incident investigation, generate KQL queries, summarize complex alerts, perform guided threat hunting, and automate routine SOC analysis.

1. 5.1 Generative AI for Security Operations
2. 5.2 Security Copilot Architecture and Setup
3. 5.3 Prompting Security Copilot: Techniques and Promptbooks
4. 5.4 Embedded Copilot in Defender XDR
5. 5.5 Embedded Copilot in Sentinel
6. 5.6 Embedded Copilot in Entra, Purview, and Defender for Cloud
7. 5.7 Incident Investigation with Security Copilot
8. 5.8 Threat Hunting and KQL Generation with Copilot
9. 5.9 Copilot Governance, Plugins, and Data Security
10. 5.10 Cross-Product Investigation: Copilot-Assisted Workflow
11. Module Summary
12. Check My Knowledge

Create Queries for Microsoft Sentinel Using Kusto Query Language (KQL)

Learn to write KQL from scratch, from your first query to complex multi-table investigation joins.

1. 6.1 Construct KQL Statements for Microsoft Sentinel
2. 6.2 Analyze Query Results Using KQL
3. 6.3 Build Multi-Table Statements Using KQL
4. 6.4 Work with String Data in KQL
5. 6.5 Security-Specific KQL Patterns
6. 6.6 Building an Investigation Query Library
7. 6.7 KQL Performance Optimization and Query Debugging
8. 6.8 Real-World Query Building Exercises
9. Module Summary
10. Check My Knowledge

Configure Your Microsoft Sentinel Environment

Design, deploy, and operationally manage a Microsoft Sentinel workspace from scratch.

1. 7.1 Microsoft Sentinel: SIEM + SOAR Architecture
2. 7.2 Workspace Architecture and Design Decisions
3. 7.3 Creating and Configuring a Sentinel Workspace
4. 7.4 Log Types: Analytics, Basic, and Archive Tiers
5. 7.5 Data Retention and Cost Management
6. 7.6 Key Tables and Schema for Security Operations
7. 7.7 Watchlists: Named Data for KQL Enrichment
8. 7.8 Threat Intelligence in Sentinel
9. 7.9 Integrating Defender XDR with Sentinel
10. 7.10 Content Hub and Solutions
11. 7.11 Workspace Health and Operational Monitoring
12. 7.12 RBAC, Multi-Workspace, and Governance
13. Module Summary
14. Check My Knowledge

Connect Logs to Microsoft Sentinel

Connect every data source in your environment to Sentinel, Microsoft first-party services, Defender XDR, Windows hosts, third-party devices via Syslog and CEF, and custom applications via API ingestion.

1. 8.1 Ingestion Strategy and Connector Architecture
2. 8.2 Microsoft First-Party Connectors
3. 8.3 Connecting Microsoft Defender XDR
4. 8.4 Connecting Windows Hosts to Sentinel
5. 8.5 Common Event Format (CEF) Connectors
6. 8.6 Syslog Data Sources
7. 8.7 Data Collection Rules: Filter, Transform, Route
8. 8.8 Custom Logs and API Ingestion
9. 8.9 Connector Troubleshooting and Validation
10. 8.10 Ingestion Cost Optimization at the Connector Level
11. 8.11 Building the Complete Ingestion Pipeline
12. Module Summary
13. Check My Knowledge

Defender for Office 365 Policies & Protection

Configure anti-phishing, Safe Links, Safe Attachments, ZAP, email authentication, transport rules, and Threat Explorer, the complete email protection stack for a Microsoft 365 environment.

1. 9.1 Email Threat Landscape and Architecture
2. 9.2 Anti-Phishing Policies
3. 9.3 Safe Links Policies
4. 9.4 Safe Attachments Policies
5. 9.5 Zero-Hour Auto Purge (ZAP)
6. 9.6 Email Authentication: SPF, DKIM, DMARC
7. 9.7 Transport Rules for Security
8. 9.8 Threat Explorer Deep Dive
9. 9.9 Automated Investigation and Response for Email
10. Module Summary
11. 9.11 Module Assessment

Phase 3: Detection & Hunting

Create Detections and Perform Investigations Using Microsoft Sentinel

Build the detection and investigation layer that turns raw data into actionable security incidents.

1. 10.1 Analytics Rules: Architecture and Rule Types
2. 10.2 Creating Scheduled Analytics Rules
3. 10.3 Near-Real-Time (NRT) and Microsoft Security Rules
4. 10.4 Entity Mapping and Alert Enrichment
5. 10.5 Incident Management and Investigation Workflow
6. 10.6 Automation Rules
7. 10.7 Playbooks with Logic Apps
8. 10.8 User and Entity Behavior Analytics (UEBA)
9. 10.9 Workbooks and Security Reporting
10. 10.10 ASIM Parsers and Data Normalization
11. 10.11 Detection Engineering Lifecycle
12. Module Summary
13. Check My Knowledge

Perform Threat Hunting in Microsoft Sentinel

Move from reactive detection to proactive threat discovery.

1. 11.1 Threat Hunting Concepts and Methodology
2. 11.2 The Sentinel Hunting Experience
3. 11.3 Writing Effective Hunting Queries
4. 11.4 Hypothesis-Driven Hunting
5. 11.5 Hunting Bookmarks and Evidence Collection
6. 11.6 Livestream: Real-Time Hunting
7. 11.7 Search Jobs and Archived Data
8. 11.8 Hunt Management and Collaboration
9. 11.9 MITRE ATT&CK-Driven Hunting
10. 11.10 Hunting with Notebooks
11. 11.11 Building a Hunting Program
12. Module Summary
13. Check My Knowledge

Phase 4: Investigation Scenarios

Investigating AiTM Credential Phishing

Full incident response on a real five-wave AiTM phishing campaign.

1. 12.1 Understanding AiTM Attack Mechanics
2. 12.2 Incident Briefing: INC-NE-2026-0227-001
3. 12.3 Investigation Setup and Scoping
4. 12.4 Email Analysis: Tracing the Phishing Campaign
5. 12.5 Sign-In Log Investigation
6. 12.6 Post-Compromise Activity Assessment
7. 12.7 Containment
8. 12.8 Eradication
9. 12.9 Campaign Tracking Across Waves
10. 12.10 Scope Assessment: Who Else Was Hit?
11. 12.11 CISO Report
12. 12.12 Hardening Recommendations
13. 12.13 Detection Engineering
14. 12.14 Lessons Learned and Post-Incident Review
15. Module Summary
16. 12.16 Check My Knowledge

Investigating BEC and Financial Fraud

Full investigation of a business email compromise leading to a vendor payment diversion attempt.

1. 13.1 Understanding BEC Attack Mechanics
2. 13.2 Incident Briefing: INC-NE-2026-0315-002
3. 13.3 Mailbox Compromise Assessment
4. 13.4 Email Thread Analysis
5. 13.5 The Fraudulent Email
6. 13.6 Financial Impact Assessment
7. 13.7 Containment and Evidence Preservation
8. 13.8 Law Enforcement and Banking Coordination
9. 13.9 Eradication
10. 13.10 Detection Engineering
11. 13.11 Hardening Against BEC
12. Module Summary
13. 13.13 Check My Knowledge

Investigating Token Replay and Session Hijacking

Deep investigation of post-authentication token abuse, the persistence technique that survives password resets and MFA re-registration.

1. 14.1 How M365 Tokens Work
2. 14.2 Incident Briefing: INC-NE-2026-0320-003
3. 14.3 Identifying Token Replay in Sign-In Logs
4. 14.4 Tracing Token Lifecycle
5. 14.5 Non-Interactive Sign-In Deep Dive
6. 14.6 Token-Specific Containment
7. 14.7 Continuous Access Evaluation (CAE)
8. 14.8 Token Protection (Token Binding)
9. 14.9 Detection Engineering
10. Module Summary
11. 14.11 Check My Knowledge

Investigating Consent Phishing and Illicit OAuth Grants

Investigate malicious OAuth application consent, the attack that grants an attacker persistent API access to mailboxes, files, and directory data without stealing any credential.

1. 15.1 How OAuth Consent Works in M365
2. 15.2 Incident Briefing: INC-NE-2026-0325-004
3. 15.3 Identifying Malicious Consent Grants
4. 15.4 Assessing What the Application Accessed
5. 15.5 Revocation and Cleanup
6. 15.6 Tenant-Wide Consent Audit
7. 15.7 Preventive Controls
8. 15.8 Detection Engineering
9. Module Summary
10. 15.10 Check My Knowledge

Investigating Insider Threats

Investigate data exfiltration by an authorized user, the investigation type that involves HR, legal, and evidence standards that external-attacker incidents do not.

1. 16.1 Insider Threat Fundamentals
2. 16.2 Incident Briefing: INC-NE-2026-0401-005
3. 16.3 Activity Reconstruction
4. 16.4 Identifying Exfiltration Channels
5. 16.5 Evidence Preservation
6. 16.6 HR and Legal Coordination
7. 16.7 Containment Without Tipping Off
8. 16.8 Detection Engineering
9. Module Summary
10. 16.10 Check My Knowledge

Phase 0: Course Resources

Cheatsheets

The KQL, the workspace, the connectors and the investigation pivots, one sheet per part of the stack.

1. KQL That Holds Up
2. Defender XDR and the Endpoint
3. The Workspace and What Reaches It
4. Purview, DLP and the Audit Log
5. Email Security and Phishing
6. Detection Rules That Work
7. Hunting With a Hypothesis
8. AiTM, Token Replay and Session Theft
9. BEC, Consent Phishing and Insider Threat
10. Cloud Posture and Copilot
11. Metrics and Reporting

Cookbooks

Ordered procedures for the work an M365 security operations analyst does: shift start, triage, investigation, containment, deployment and reporting.

1. Starting a Shift
2. Triageing an Incident
3. Containing a Compromised Identity
4. Investigating Across Workloads
5. Deploying a Detection Rule
6. Running a Threat Hunt
7. Writing the Monthly Report

Lab Setup

A trial tenant with real telemetry, the connectors that matter, and every silent failure produced on purpose.

1. Building the Tenant
2. Producing the Silent Failures
3. Verify, and What the Lab Cannot Teach

Walkthroughs

Six investigations reasoned end to end, including the ones where the answer was that the evidence did not exist.

1. The Impossible Travel That Was a VPN
2. The Mailbox Nobody Could Scope
3. The Application Nobody Revoked
4. The Rule That Never Could Have Fired
5. The Departure Nobody Could Prove
6. The One That Was Real

Playbooks

What to do when an identity alert fires, a phishing campaign lands, a rule goes quiet, or somebody asks what was exposed.

1. An Identity Alert Fires
2. A Phishing Campaign Lands
3. A Rule Has Gone Quiet
4. Somebody Asks What Was Exposed
5. The Queue Has Filled Up
6. An Application You Do Not Recognize
7. HR Asks About an Employee

Playground

Four Incident Lab scenarios, a three-part exam, a lab pack and your own tenant, with what each one is good for.

Operational Reference

The commands, queries and configuration references from this course in one place, organized for lookup during live work.

1. Operational Quick Reference

References & Further Reading

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

1. References & Further Reading

Course Completion

Course Exam

Microsoft 365 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. Microsoft 365 Security Operations

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