# Microsoft 365 Security Automation and Orchestration

SEC202

Scale your security operations without scaling headcount. Design, build, and operationalize powerful automation and orchestration workflows using Microsoft Sentinel, Logic Apps, Playbooks, and Defender XDR to respond to threats faster, reduce manual work, and run a more efficient SOC.

| | |
|---|---|
| **Modules** | 23 |
| **Lessons** | 222 |
| **Phases** | 4 |
| **Free preview** | Course Orientation (13 lessons) |

## The method

Automation in a SOC is a decision about what a machine may do without asking. This course runs the same loop for every playbook it builds, because the failure mode is not a playbook that breaks but one that acts confidently on a wrong input.

1. Automate the reading before the acting. Enrichment and evidence collection are safe, immediately valuable and reversible. Start there and the containment playbooks arrive with a track record behind them.

2. Define the trigger precisely. A playbook is only as good as the condition that fires it. Most bad automation is a good action on an over-broad trigger.

3. Decide what it may do unattended. Enrich, notify, contain. Each step outward needs a stated reason and a documented rollback, not a feature flag.

4. Test the failure path, not the happy one. What happens when the API is down, the identity is stale, the entity is missing. A playbook that has only been tested when everything works is untested.

5. Govern it as code. Version it, review changes and measure what it did. Automation nobody audits becomes automation nobody trusts, and then automation somebody disables.

## What this course assumes

No minimum experience and no prerequisite course. Logic Apps, the connector model and the Sentinel automation surface are explained from the first playbook.

What makes it go faster: an Azure subscription and a Sentinel workspace you can build in. Not required, and every playbook is shown as a definition you can read.

What this course does not cover: investigation technique, detection rule writing, and incident response process. This course automates the response those disciplines decide on.

# Full syllabus

## Phase 1: Foundations

### Course Orientation FREE PREVIEW

What Microsoft 365 Security Automation and Orchestration teaches: build Sentinel and Logic Apps playbooks that enrich alerts, collect evidence, and auto-contain threats across identity, endpoint, and cloud, so your SOC scales without scaling headcount.

1. 0.1 Why Most SOCs Don't Automate (And Why They Should)
2. 0.2 The Automation Spectrum
3. 0.3 The Three Automation Tiers
4. 0.4 The Confidence Threshold Problem
5. 0.5 The Blast Radius Assessment
6. 0.6 NE's Automation Landscape
7. 0.7 Sentinel Automation Architecture
8. 0.8 Defender XDR Automation Architecture
9. 0.9 The Automation Governance Framework
10. 0.10 The Automation Maturity Model
11. 0.11 Guided Walkthrough: Automation Assessment
12. Module Summary
13. Check My Knowledge

### Sentinel Automation Fundamentals

Build your first automation rule and your first Sentinel playbook.

1. 1.1 Automation Rules. The Lightweight Layer
2. 1.2 Playbooks. The Power Layer
3. 1.3 Your First Automation Rule
4. 1.4 Your First Playbook
5. 1.5 Authentication and Permissions
6. 1.6 Entity Extraction and Mapping
7. 1.7 Error Handling and Retry Logic
8. 1.8 Testing Automation Safely
9. 1.9 Monitoring Automation Health
10. 1.10 Cost Management
11. 1.11 Guided Walkthrough. Connecting the Automation Chain
12. Module Summary
13. Check My Knowledge

## Phase 2: Enrichment & Collection

### Alert Enrichment Automation

Build the enrichment pipeline that transforms every alert into an investigation-ready incident.

1. 2.1 The Enrichment Stack
2. 2.2 IP Reputation Enrichment Playbook
3. 2.3 User Risk Enrichment Playbook
4. 2.4 Device Compliance Enrichment Playbook
5. 2.5 Alert History and Pattern Enrichment
6. 2.6 Threat Intelligence Auto-Correlation
7. 2.7 Geo-Location and Impossible Travel Enrichment
8. 2.8 Combining Enrichments. The Enrichment Pipeline
9. 2.9 Watchlist-Driven Dynamic Enrichment
10. 2.10 Enrichment Performance Tuning
11. 2.11 Guided Walkthrough. Building the Production Enrichment Pipeline
12. Module Summary
13. Check My Knowledge

### Evidence Auto-Collection

Build the evidence collection pipeline that captures volatile data at alert time, before session tokens expire, before processes terminate, before containment modifies the environment.

1. 3.1 The Collection Problem
2. 3.2 Cloud Evidence Auto-Collection
3. 3.3 Endpoint Evidence Auto-Collection
4. 3.4 Identity Evidence Auto-Collection
5. 3.5 Network Evidence Auto-Collection
6. 3.6 Evidence Packaging and Chain of Custody
7. 3.7 Collection Playbook for AiTM Incidents
8. 3.8 Collection Playbook for Endpoint Incidents
9. 3.9 Collection Playbook for Email Incidents
10. 3.10 Collection Timing and Retention
11. 3.11 Interactive Lab: Auto-Collection Pipeline
12. Module Summary
13. Check My Knowledge

### Notification and Escalation Automation

Build the notification pipeline that delivers the right information to the right people at the right severity, Teams adaptive cards for the SOC, escalation cascades for after-hours, MSSP coordination to prevent duplicate triage, regulatory flagging, fatigue prevention, and approval workflows...

1. 4.1 Who Needs to Know, and When
2. 4.2 Teams Channel Notifications
3. 4.3 Email Notifications
4. 4.4 On-Call Escalation Automation
5. 4.5 MSSP Notification and Coordination
6. 4.6 Management and Executive Notifications
7. 4.7 Ticketing Integration (ServiceNow/Jira)
8. 4.8 Regulatory Notification Triggers
9. 4.9 Notification Fatigue Prevention
10. 4.10 Approval Workflows
11. 4.11 Interactive Lab: Notification Pipeline
12. Module Summary
13. Check My Knowledge

## Phase 3: Response Automation

### Auto-Containment, Identity

Build the identity containment playbook that revokes sessions, surgically removes attacker MFA methods, activates emergency conditional access, revokes OAuth consents, and disables accounts, gated by confidence thresholds, VIP and service account safeguards, post-containment verification, and...

1. 5.1 The Auto-Containment Decision
2. 5.2 Session Revocation Automation
3. 5.3 MFA Reset Automation
4. 5.4 Conditional Access Emergency Policy
5. 5.5 OAuth App Revocation
6. 5.6 Account Disable with Safeguards
7. 5.7 Inbox Rule Remediation
8. 5.8 Password Reset Orchestration
9. 5.9 Identity Containment Verification
10. 5.10 Identity Containment Rollback
11. 5.11 Interactive Lab: Identity Auto-Containment
12. Module Summary
13. Check My Knowledge

### Auto-Containment, Endpoint

Build the endpoint containment playbook that isolates compromised devices through Defender for Endpoint, collects forensic evidence before isolation, blocks malicious files fleet-wide, and applies the workstation-versus-server-versus-DC decision logic that prevents production outages.

1. 6.1 Endpoint Isolation Decision Logic
2. 6.2 Defender for Endpoint Isolation Automation
3. 6.3 Automated Investigation Package Collection
4. 6.4 Automated Live Response Actions
5. 6.5 File Quarantine and Block
6. 6.6 Network Containment via Firewall API
7. 6.7 Endpoint Containment for Servers vs Workstations
8. 6.8 Multi-Endpoint Containment Coordination
9. 6.9 Endpoint Containment Verification
10. 6.10 Endpoint Containment Rollback
11. 6.11 Interactive Lab: Endpoint Containment Pipeline
12. Module Summary
13. Check My Knowledge

### Auto-Containment, Cross-Environment

Build the synchronized containment playbook that responds to attacks spanning cloud, endpoint, and network at once, parallel session revocation, device isolation, and IP blocking, with blast radius assessment, human approval gates, CHAIN-HARVEST and CHAIN-PRIVILEGE response, and breakout detection.

1. 7.1 The Coordinated Containment Problem
2. 7.2 Synchronized Containment Playbook
3. 7.3 Containment Sequence Prioritization
4. 7.4 Blast Radius Assessment Automation
5. 7.5 Human Approval Gates for High-Impact Actions
6. 7.6 Automation for CHAIN-HARVEST Response
7. 7.7 Automation for CHAIN-PRIVILEGE Response
8. 7.8 Partial Automation Patterns
9. 7.9 Containment Monitoring and Breakout Detection
10. 7.10 Post-Containment Automation
11. 7.11 Interactive Lab: Cross-Environment Response
12. Module Summary
13. Check My Knowledge

## Phase 4: Operational Mastery

### Defender XDR Automation

Build automation native to Microsoft Defender XDR, custom detection rules with auto-actions, Automated Investigation and Response, attack disruption, custom indicators, and the per-workload automation across MDO, MDI, and MDCA, plus the coordination model that keeps XDR and Sentinel from...

1. 8.1 Custom Detection Rules with Auto-Actions
2. 8.2 Auto Investigation and Response (AIR)
3. 8.3 Attack Disruption Configuration
4. 8.4 MDE Custom Indicators for Automated Blocking
5. 8.5 Defender for Office 365 Automation
6. 8.6 Defender for Identity Auto-Response
7. 8.7 Defender for Cloud Apps Automation
8. 8.8 Unified XDR + Sentinel Automation
9. 8.9 XDR Automation Monitoring
10. 8.10 XDR Automation at Scale
11. 8.11 Interactive Lab: XDR Custom Detection and Auto-Response
12. Module Summary
13. Check My Knowledge

## KQL-Driven Automation

Engineer KQL as the control layer for automation, queries as triggers, dynamic watchlists for runtime control, suppression with audit cycles, multi-signal correlation that composes confidence, health monitoring, hunting automation, evidence collection that avoids truncation, and the query...

1. 9.1 KQL as Automation Trigger
2. 9.2 Dynamic Watchlists for Automation Control
3. 9.3 KQL-Based Alert Suppression
4. 9.4 KQL Correlation Rules for Multi-Signal Automation
5. 9.5 KQL for Automation Health Monitoring
6. 9.6 KQL-Driven Hunting Automation
7. 9.7 KQL for Evidence Collection Queries
8. 9.8 Advanced KQL Patterns for Automation
9. 9.9 KQL Alert Tuning for Automation Confidence
10. 9.10 Building a KQL Automation Query Library
11. 9.11 Interactive Lab: KQL-Driven Automation
12. Module Summary
13. Check My Knowledge

## Azure Functions for Security Automation

Build Azure Functions for automation that exceeds Logic Apps, TI enrichment with caching and retry, bulk remediation with dry-run safety, custom IOC feed processing with deduplication and expiry, evidence packaging with chain of custody, secure least-privilege architecture, and async Sentinel...

1. 10.1 When Logic Apps Are Not Enough
2. 10.2 Azure Function Architecture for Security
3. 10.3 Building a TI Enrichment Function
4. 10.4 Building a Bulk Remediation Function
5. 10.5 Building a Custom IOC Feed Processor
6. 10.6 Building an Evidence Packager
7. 10.7 Error Handling and Observability
8. 10.8 Security Considerations for Functions
9. 10.9 Testing and Deployment
10. 10.10 Connecting Functions to Sentinel
11. 10.11 Interactive Lab: Azure Functions for Security Automation
12. Module Summary
13. Check My Knowledge

## Automation Testing and Governance

Build the discipline that keeps automation trustworthy, the testing framework, staging workspace, safe containment testing, version control, change management, operational runbooks, audit trails, false positive impact analysis, and continuous improvement that prevent the untested playbook from...

1. 11.1 The Case for Automation Testing
2. 11.2 The Testing Framework
3. 11.3 The Staging Workspace
4. 11.4 Testing Containment Automation Safely
5. 11.5 Version Control for Automation
6. 11.6 Change Management for Production Automation
7. 11.7 Automation Runbooks
8. 11.8 Automation Audit Trail
9. 11.9 False Positive Impact Analysis
10. 11.10 Continuous Improvement
11. 11.11 Interactive Lab: Testing and Governing the Automation Stack
12. Module Summary
13. Check My Knowledge

### Building the Automation Program

Turn automation capability into a sustained program, a dependency-ordered roadmap, leverage-based candidate selection, a team structure that survives turnover, business metrics, playbook library governance, MSSP coordination, compliance evidence, cost-benefit analysis, and the path to a mature...

1. 12.1 The Automation Roadmap
2. 12.2 Identifying Automation Candidates
3. 12.3 Building the Automation Team
4. 12.4 Automation Metrics Dashboard
5. 12.5 The Playbook Library
6. 12.6 MSSP Automation Coordination
7. 12.7 Automation for Compliance
8. 12.8 Cost-Benefit Analysis
9. 12.9 Scaling Automation
10. 12.10 The Mature Automation Operation
11. 12.11 Interactive Lab: Building the Program Roadmap
12. Module Summary
13. Check My Knowledge

### Capstone, The Automated SOC

Assemble the entire course into one working system, six automation phases from enrichment through governance, run a realistic multi-stage attack end to end, expose the bugs only integration testing reveals, measure the performance gain, and produce the reference architecture and business case...

1. 13.1 Capstone Briefing
2. 13.2 Phase 1: Enrichment Automation
3. 13.3 Phase 2: Collection Automation
4. 13.4 Phase 3: Notification Automation
5. 13.5 Phase 4: Containment Automation
6. 13.6 Phase 5: Cross-Environment Orchestration
7. 13.7 Phase 6: Monitoring and Governance
8. 13.8 Integration Testing
9. 13.9 Metrics and Business Case
10. 13.10 The Complete Automation Architecture
11. 13.11 Interactive Lab: Running the Full Stack
12. Module Summary
13. Check My Knowledge

## Phase 0: Course Resources

### Cheatsheets

Automation patterns organized by what they do, each carrying the risk tier that decides whether it runs unattended.

1. Enrichment Automation
2. Evidence Collection Automation
3. Notification and Escalation
4. Identity Containment
5. Endpoint Containment
6. Cross-Environment Containment
7. Defender XDR Automation
8. KQL-Driven Automation
9. Functions and Custom Logic
10. Testing, Governance and Measurement
11. Tiers, Triggers and Limits

### Cookbooks
Seven procedures for getting automation into production and keeping it there, each with a state to reach.

1. Assigning a Tier to a New Automation
2. Debugging a Playbook That Reports Success
3. Promoting an Automation to Unattended
4. Recovering From a Wrong Automated Action
5. Moving a Playbook to a Function
6. Retiring an Automation
7. Building an Enrichment Pipeline That Stays Fast

### Lab Setup
A lab with disposable targets, so containment automation can be tested without locking you out of the tenant running it.

1. Workspace and Logic Apps
2. Disposable Targets
3. Your First Playbook
4. Testing Containment Safely
5. Verify and Limits

### Walkthroughs
Worked automation failures end to end, including the wrong turns and what would have made each answer different.

1. The Playbook That Reported Success
2. The Approval Queue Nobody Read
3. The Loop That Disabled Thirty-Four Accounts
4. The Enrichment That Slowed Triage Down
5. The Tier One Automation That Was Not
6. The Function That Lost Half Its Work
7. The Hours That Were Never Spent

### Playbooks
Response procedures for when the automation is the incident, with dispositions and a handoff artifact.

1. An Automation Is Acting Wrongly
2. The Automation Identity May Be Compromised
3. The Containment Did Not Fire
4. The Automation Is Being Throttled
5. An Approval Has Been Sitting Unanswered
6. Automation Was Disabled and Nobody Said
7. An Automation Acted During a Freeze

### Playground
Where to practice building automation, and the one thing about this discipline no practice surface can give you.

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

1. Automation Quick Reference
2. Security Automation Field Manual

### References & Further Reading
External sources this course draws on: vendor documentation, frameworks, standards, and research.

## Course Completion

## Course Exam

Security Automation end-of-course exam, a simulation-based assessment testing whether you can diagnose, contain, and remediate an automation failure under pressure, using the engineering and judgment built across all 14 modules.

1. Course Completion. Security Automation

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