Cybersecurity Analyst: Core Skills and Investigation

SEC208

The security analyst's job from the first record to the handover: read what systems record, query it, triage alerts, investigate endpoints, identities, mail, networks and AI systems, contain what you find and check that it held, and write it up for the people who act on it.

Modules	19
Lessons	140
Phases	5
Free preview	Cybersecurity Analyst: Core Skills and Investigation (10 lessons)

The method

Every module is an investigation you work yourself, in your browser, from the records. Every lesson reads real records in the tool an analyst would use to read them: the portal, the query console, Event Viewer, Wireshark, a terminal, an AI assistant. The loop is the same throughout.

1. Start from the question. What the alert or the report claims, what would settle it, and what you are allowed to do about it.

2. Read the records. Run the queries in the page against the case's own data, and open the lab pack's files with free tools on your own machine.

3. Test the explanation. Write the prediction first, then run the query that could prove it wrong, including the ordinary explanation you'd rather not have to rule out.

4. Keep the claims honest. A fact is not an inference, an account is not a person, and a quiet result means nothing until the source is shown to be collecting.

5. Hand it over. Every practical ends with a disposition, the actions within your authority, and a handover the next person can act on without re-running your queries.

What this course assumes

Comfort using a computer and a web browser, and a general idea of what a network and an account are. Every system, record and tool is explained the first time the course uses it.

What makes it go faster: some time in IT support or administration, and having seen an event log or a firewall log before. Module 0 has one short lesson for each module, so you can see what each one expects before you start it.

What this course does not cover in depth: forensic imaging and memory analysis, malware reverse engineering, writing detections as a discipline, and offensive testing. Each has its own course in the catalog.

Full syllabus

Module 0: Foundations

Cybersecurity Analyst: Core Skills and Investigation FREE PREVIEW

Module 0 of Cybersecurity Analyst: what security analysis is, one foundation lesson for each module, from reading a record to writing for a reader, the twelve cases the course works, and whether the course is for you.

1. 0.1 Reading a Record
2. 0.2 One Person, Many Names
3. 0.3 Finding What You Need in Data
4. 0.4 Behavior in Records
5. 0.5 Windows Events and Processes
6. 0.6 Sign-ins, Mail and Cloud Audit
7. 0.7 Packets, Flows and Exposure
8. 0.8 How Assistants and Agents Work
9. 0.9 Response and Detection Basics
10. 0.10 Writing for a Reader

Phase 1: Foundations, Systems and Telemetry

Analyst Foundations and Investigative Judgment

Module 1 of Cybersecurity Analyst: what the analyst is responsible for and where their authority ends, what the business runs on, how an enterprise is put together, how events become cases, how to frame questions and test explanations, how to keep facts apart from inferences, how to handle...

1. 1.1 The Analyst's Responsibilities and Limits of Authority
2. 1.2 Business Services, Critical Assets and Operational Impact
3. 1.3 Enterprise Environments: Endpoints, Networks, Identity, Cloud and SaaS
4. 1.4 Events, Alerts, Cases and Incidents
5. 1.5 Investigation Questions, Hypotheses and Alternative Explanations
6. 1.6 Facts, Inferences, Confidence and Unsupported Claims
7. 1.7 Evidence Handling, Privacy and Professional Conduct
8. 1.8 Case Notes, Ownership and Escalation
9. 1.9 Using the Investigation Environment and Checking Its Data
10. 1.10 Practical: Validate an Alert and Document the Next Steps

Systems, Networks and Identity

Module 2 of Cybersecurity Analyst: how Windows and Linux run programs and record what they do, how addresses, ports, DNS, HTTP and TLS carry traffic, what firewalls, proxies, VPNs and NAT change, and how identity, authentication, tokens and privileged accounts work, each taught on the records it...

1. 2.1 Windows Processes, Services and Scheduled Tasks
2. 2.2 Windows Files, Registry, Permissions and Event Logs
3. 2.3 Linux Processes, Permissions, Services and Authentication Logs
4. 2.4 IP Addresses, Ports, Connections and Routing
5. 2.5 DNS, HTTP, TLS and Certificates
6. 2.6 Firewalls, Proxies, VPNs and NAT
7. 2.7 Active Directory, Entra ID and Enterprise Identity
8. 2.8 Authentication, Authorization, MFA, Tokens and Sessions
9. 2.9 Privileged Accounts, Service Accounts and Application Identities
10. 2.10 Practical: Explain a User's Activity Across Host, Network and Identity Records

Security Telemetry, Querying and Data Handling

Module 3 of Cybersecurity Analyst: what each kind of log records, schemas and identifiers, event and ingestion time, coverage and gaps, KQL where a query is needed, and free tools (jq, DuckDB, PowerShell 7, Python) for exported files, hashes and small repeatable scripts.

1. 3.1 What Endpoint, Identity, Network and Application Logs Record
2. 3.2 Schemas, Stable Identifiers and Data Types
3. 3.3 Event Time, Ingestion Time and Time-Zone Normalization
4. 3.4 Collection Coverage, Retention and Missing Data
5. 3.5 KQL Filtering, String Matching and Field Selection
6. 3.6 Aggregation, Baselines and Distinct Counts
7. 3.7 Parsing Dynamic Fields and Correlating Tables
8. 3.8 PowerShell for Targeted Collection and Data Processing
9. 3.9 CSV, JSON, Hashing and Small Repeatable Analysis Scripts
10. 3.10 Practical: Build and Validate a Query-Backed Timeline

Phase 2: Triage and Investigation

Attacker Behavior and Alert Triage

Module 4 of Cybersecurity Analyst: how intrusions behave from initial access to exfiltration, read in real recorded events, then how to read detection logic, prioritize by context and validate benign explanations before choosing a disposition for each alert in a mixed queue.

1. 4.1 Initial Access and Social Engineering
2. 4.2 Execution and Abuse of Trusted Utilities
3. 4.3 Discovery and Credential Access
4. 4.4 Privilege Escalation and Persistence
5. 4.5 Lateral Movement and Remote Administration
6. 4.6 Command and Control, Collection and Exfiltration
7. 4.7 Reading Detection Logic and Supporting Evidence
8. 4.8 Prioritizing by Context, Exposure and Business Impact
9. 4.9 Validating Benign Explanations and Selecting a Disposition
10. 4.10 Practical: Triage a Mixed Queue of Malicious, Legitimate and Inconclusive Alerts

Endpoint Investigation

Module 5 of Cybersecurity Analyst: determining what executed on a Windows endpoint, how it arrived and what happened afterward, from process ancestry, files, scripts, persistence, logons and connections, with live collection, scoping across devices and a Linux comparison.

1. 5.1 Planning an Endpoint Investigation
2. 5.2 Process Ancestry, Command Lines and Execution Context
3. 5.3 File Origin, Creation, Modification and Execution
4. 5.4 PowerShell and Script Activity
5. 5.5 Services, Tasks and Registry Persistence
6. 5.6 Accounts, Logons and Remote Sessions
7. 5.7 Process-to-Network Correlation
8. 5.8 Targeted Artifact Collection and Volatile Evidence
9. 5.9 Scoping Related Devices and Recognizing Collection Limits
10. 5.10 Practical: Investigate Suspicious Execution and Establish Its Scope

Identity, Email and Cloud Investigation

Module 6 of Cybersecurity Analyst: following access and activity across sign-ins, sessions and MFA, account and application changes, mail headers, clicks and mailbox rules, and cloud audit and storage records, then correlating them where each service names the same person and session differently.

1. 6.1 Investigating Sign-In and Authentication Records
2. 6.2 MFA Results, Sessions and Conditional Access Context
3. 6.3 Account Changes, Privileged Activity and Persistence
4. 6.4 Application Consent and Workload Identities
5. 6.5 Email Headers, Authentication and Delivery Evidence
6. 6.6 URLs, Attachments and User Interaction
7. 6.7 Mailbox Rules, Forwarding and Account Abuse
8. 6.8 Cloud Audit Records, Resource Changes and Storage Access
9. 6.9 Correlating Identity, Email, Endpoint and Cloud Activity
10. 6.10 Practical: Investigate Phishing Followed by Suspicious Account Activity

Network, Data Exposure and Vulnerability Analysis

Module 7 of Cybersecurity Analyst: choosing between packets, flows, DNS, proxy and firewall records; reading captures in Wireshark; telling scans, beacons and uploads from their legitimate lookalikes; tying an address to a device through NAT, VPN and DHCP; and ranking vulnerabilities by...

1. 7.1 Selecting Packet, Flow, DNS, Proxy and Firewall Evidence
2. 7.2 Wireshark Filters, Conversations and Streams
3. 7.3 DNS and Web Activity Investigation
4. 7.4 Encrypted Traffic and Metadata Limitations
5. 7.5 Scanning, Beaconing and Legitimate Lookalikes
6. 7.6 NAT, VPN and Device Attribution
7. 7.7 Data Staging, Uploads and Potential Exfiltration
8. 7.8 Vulnerability, Exploitability and Asset Exposure
9. 7.9 Prioritizing Remediation and Assessing Compensating Controls
10. 7.10 Practical: Assess a Suspicious Transfer and the Exposure That Enabled It

Phase 3: AI, Response and Improvement

AI Systems Investigation

Module 8 of Cybersecurity Analyst: investigating LLM applications, copilots and agents from their traces, tool calls, approvals and the Microsoft 365 records their actions leave; prompt injection, data disclosure and unauthorized actions; containing an agent; and using AI on an investigation...

1. 8.1 LLM Applications, Retrieval, Copilots and Agents
2. 8.2 AI Data Access, Identities, Tools and Permissions
3. 8.3 Prompt Injection and Untrusted Retrieved Content
4. 8.4 Sensitive-Data Disclosure and Unauthorized Actions
5. 8.5 AI Traces, Tool Calls, Approvals and Downstream Audit Records
6. 8.6 Reconstructing an AI-Related Incident
7. 8.7 Containment of Affected Agents, Connectors and Credentials
8. 8.8 Using AI to Explain Records, Draft Queries and Summarize Evidence
9. 8.9 Verifying AI Output and Protecting Investigation Information
10. 8.10 Practical: Investigate an Agent Action Nobody Asked For

Incident Response and Detection Improvement

Module 9 of Cybersecurity Analyst: declaring and scoping an incident, deciding what to collect before evidence is lost, containing across endpoint, network, identity and application, coordinating with the business, verifying containment and finding remaining access, closing on criteria, and...

1. 9.1 Incident Declaration, Scope and Severity
2. 9.2 Collection Priorities and Evidence-Loss Decisions
3. 9.3 Endpoint, Network, Identity and Application Containment
4. 9.4 Approval, Business Dependencies and Coordinated Action
5. 9.5 Verifying Containment and Identifying Remaining Access
6. 9.6 Recovery, Monitoring and Closure Criteria
7. 9.7 Developing a Bounded Hunt from an Investigation
8. 9.8 Detection Objectives, Telemetry Requirements and Testing
9. 9.9 Safe Automation, Failure Handling and Analyst Oversight
10. 9.10 Practical: Contain a Developing Incident and Validate One Detection Improvement

Phase 4: Independent Investigation

Independent Investigation and Professional Reporting

Module 10 of Cybersecurity Analyst: taking an unfamiliar case from brief to handover on your own, with a plan, an evidence inventory, tested hypotheses, a reconstruction across endpoint, identity, email and cloud, a timeline with confidence, verified response decisions, three kinds of report and...

1. 10.1 Case Briefing, Scope and Investigation Plan
2. 10.2 Evidence Inventory and Coverage Assessment
3. 10.3 Independent Querying and Hypothesis Testing
4. 10.4 Endpoint and Identity Reconstruction
5. 10.5 Network, Email, Cloud and AI Correlation Where Relevant
6. 10.6 Timeline, Affected Assets and Confidence Assessment
7. 10.7 Response Decisions and Verification Evidence
8. 10.8 Technical Report, Management Update and Shift Handover
9. 10.9 Quality Review, Feedback and Corrective Work
10. 10.10 Capstone: Submit and Defend an Investigation Portfolio

Phase 0: Course Resources

Cheatsheets

Six subject sheets and a lookup page: the question, the lesson's query on its case, what to read and what it does not prove.

1. Sign-ins and Identity
2. Email, Mailbox and Cloud Apps
3. Endpoint: Process, File and Network
4. Windows Security Events
5. Network and Firewall
6. Response, Verification and Case Writing
7. Lookup Values

Cookbooks

Six procedures run end to end: validating an alert, one user across sources, account compromise, execution, phishing and containment.

1. Validate an Alert
2. Explain a User's Activity Across Sources
3. Account Compromise
4. Suspicious Execution
5. Phishing to Mailbox
6. Containment, Verification and Closure

Lab Setup

The browser workspace and its twelve cases, the lab pack, the free tools the lessons use, and checking it all works.

1. The Browser Workspace
2. The Lab Pack
3. Local Tools
4. Verify the Lab

Walkthroughs

Four investigations worked end to end, wrong turns included: an encoded command, a midnight sign-in, a failed containment and an agent's share.

1. An Encoded Command from the Deployment Agent
2. A Director's Account at Midnight
3. Contained on Tuesday, Back on Thursday
4. An Agent Shared the Wrong File

Playbooks

Six playbooks, one per alert type: a risky sign-in, an inbox rule, a server logon or service, an upload, a phish and an AI agent action.

1. Risky Sign-in or Anomalous Token
2. Suspicious Inbox Rule
3. New Service or Remote Desktop Logon on a Server
4. Unusual Upload Volume
5. Reported Phishing or URL Click
6. Unexpected Action by an AI Agent

Playground

Every case workspace in one place, with an inventory query and an open question for each, and every lesson's practice.

1. The Case Workspaces and Every Practice

References

The sources behind the course: pages read for each module, and the public datasets with their licenses.

1. References by Module

Course Completion

Course Exam

Cybersecurity Analyst end-of-course exam: 40 questions in three parts, from records and triage to response and reporting, ending on a case study.

1. Course Completion. Cybersecurity Analyst

Generated 2026-11-27 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/cybersecurity-analyst/