

GENESIS ITU

Security Operations Center Analyst Course Textbook

A foundation text for entry-level SOC analysts
Definitions · Process · Practice · Professional style

Instructor of Record: Marcus “Talon” Wade

Zarco AI Systems LLC · Genesis ITU

Student Edition

How to Use This Book

This textbook is written for students preparing for Security Operations Center (SOC) analyst work. It is designed to be read chapter by chapter, either with an instructor video or as a standalone course text. Each chapter includes formal definitions, explanation, examples, a short style note where relevant, review questions, and practice prompts.

Read the definitions carefully. They are the language you will use on the job and in interviews. Complete the end-of-chapter exercises before moving on. Pause the teaching video whenever you need time to write.

Table of Contents

Chapter 1 What a Security Operations Center Is

Chapter 2 Logs, Telemetry, and Evidence

Chapter 3 Alert Triage for Level-1 Analysts

Chapter 4 Documentation, Notes, and Escalation

Chapter 5 MITRE ATT&CK; for SOC Analysts

Chapter 6 SIEM Fundamentals and Purposeful Search

Chapter 7 Incident Response and the Analyst's Place in It

Chapter 8 Practice Path, Labs, and Professional Next Steps

Appendix A SOC Writing Style Guide

Appendix B Glossary of Core Terms

Appendix C Answer Key (Selected Review Items)

Chapter 1 — What a Security Operations Center Is

Learning objectives. After this chapter you should be able to: define a SOC; explain the role of process; describe common analyst tiers; state the core mission sequence; and list a practical day-one alert workflow.

1.1 Definition and purpose

Security Operations Center (SOC)

A Security Operations Center is an organizational function—people, processes, and technology—charged with continuous monitoring for cybersecurity threats, investigation of security events and alerts, and coordinated response when harmful activity is confirmed or strongly suspected.

A SOC is not merely a room of screens. It is a capability. The value of a SOC comes from consistent process: how alerts are received, how context is gathered, how decisions are recorded, and how serious issues are escalated. Technology supports that process; it does not replace it.

Organizations operate SOCs to reduce the time between intrusion and detection, to limit damage when incidents occur, and to create an auditable record of security operations. For the analyst, that means every shift is built around observation, judgment, and clear communication.

1.2 Analyst tiers

Many SOCs organize work by tier. Titles vary by employer, but the following model is widely understood and useful for learning.

Tier	Primary responsibility
Level 1 (L1)	Initial alert handling, triage, basic investigation, documentation, and escalation when required.
Level 2 (L2)	Deeper investigation, correlation across sources, confirmation or dismissal of complex cases, support to L1.
Level 3 / specialists	Threat hunting, advanced malware or forensics support, major incident leadership, detection engineering.

Most SOC careers begin at Level 1. That is expected. L1 work trains pattern recognition, documentation discipline, and the judgment to know when a case is beyond current tools or authority. Excellence at L1 is a professional skill, not a holding pattern.

1.3 The core mission sequence

SOC mission sequence (operational)

Detect → Understand → Contain → Recover → Document. This sequence describes the analytical and operational arc of security monitoring work, from noticing anomalous activity through recording what was done.

Phase	Meaning for the analyst
Detect	Notice anomalous activity through alerts, hunts, or reports.
Understand	Determine nature, scope, and severity using available evidence.
Contain	Limit spread or impact according to authority and runbooks (often escalated).
Recover	Support return to a known-good state (often multi-team).
Document	Record facts, decisions, and rationale so others can trust and continue the work.

Level 1 analysts spend most of their time in Detect, Understand, and Document. Containment and recovery frequently require higher authority or specialized teams. Knowing where you stop—and how you hand off—is part of professional practice.

1.4 Day-one alert workflow

On the first day, perfection is not the standard. A repeatable process is. The following four-step workflow is the foundation of L1 practice:

1. **See** the alert — read title, severity, time, affected asset or identity, and rule or detection name.
2. **Check** context — who or what is involved; whether the activity is expected; recent tickets or change windows.
3. **Decide** — close as false or benign, monitor, or escalate.
4. **Write** notes another analyst can trust without redoing your work from scratch.

Key idea

Shifts exist because attacks do not wait for business hours. Many SOC's operate nights, weekends, or follow-the-sun coverage. Reliability of process matters more than heroic individual effort.

1.5 Chapter review

1. Define Security Operations Center in your own words using the formal definition as a base.
2. Contrast L1 and L2 responsibilities in two sentences.
3. List the five elements of the mission sequence and give a one-line meaning for each.
4. State the four steps of the day-one alert workflow in order.
5. Why is documentation treated as part of the mission rather than optional paperwork?

Chapter 2 — Logs, Telemetry, and Evidence

Learning objectives. Define telemetry and logs; identify major log source categories; explain the role of a SIEM; and describe a disciplined habit for turning an alert into evidence.

2.1 Definitions

Telemetry

Telemetry is the set of signals generated by systems, networks, applications, identities, and cloud services that describe activity in an environment. It is the raw observational material of security monitoring.

Log

A log is a recorded entry or stream of entries that captures events—such as authentication attempts, process starts, network connections, or configuration changes—usually with timestamps and identifying fields.

Without telemetry, monitoring is guesswork. Without retained and searchable logs, investigation is incomplete. Analysts do not “feel” their way to conclusions; they support or refute hypotheses with recorded evidence.

2.2 Common source categories

Category	Typical contents
Endpoint	EDR telemetry, operating system logs, process and file events
Network	Firewall, proxy, IDS/IPS, DNS, flow data
Identity	Authentication, MFA, SSO, account lifecycle events
Cloud	Control-plane audit logs (e.g., CloudTrail), resource activity, API calls

After a suspicious login alert, an analyst often starts with identity logs, then expands to endpoint and network sources if the case remains open. Source selection follows the question you are trying to answer.

2.3 The SIEM

SIEM (Security Information and Event Management)

A SIEM is a platform that collects, normalizes, and stores security-relevant logs and alerts, and provides search, correlation, and alerting capabilities so analysts can investigate from a central interface.

A SIEM is a tool. It does not replace analytical questions. Poor questions produce noisy searches; clear questions produce usable evidence. Treat the SIEM as a library with a powerful index, not as an oracle.

2.4 From alert to evidence

A practical habit: when an alert appears, ask what log would prove or disprove the implied claim. Retrieve that evidence. Build a short timeline. Only then decide. This habit prevents random clicking and keeps investigations focused.

Practice habit

Alert → What evidence would prove or disprove this? → Retrieve it → Build a short timeline → Decide and document.

2.5 Chapter review

1. Distinguish telemetry from logs in one or two sentences each.
2. Name four source categories and one example from each.
3. Define SIEM and state one limitation of relying on tools without questions.
4. Write the alert-to-evidence habit as a four-part sequence.

Chapter 3 — Alert Triage for Level-1 Analysts

Learning objectives. Define triage; apply a standard triage sequence; use precise decision language; and identify appropriate grounds for escalation.

3.1 Definition

Triage (SOC context)

Triage is the initial assessment of a security alert or event to determine priority, likely validity, and next action—such as closure, continued monitoring, or escalation—without performing a complete forensic investigation.

Triage is sorting, not solving. The goal is a defensible next step. Over-investigating every alert at L1 creates backlog; under-investigating creates missed incidents. Process protects both speed and quality.

3.2 Standard triage sequence

Step	Analyst action
1. Read the alert	Capture title, severity, timestamp, asset or identity, detection or rule name.
2. Establish context	Is the activity expected? Change window? Known travel or business process?
3. Gather minimum evidence	Pull only the logs needed to support or refute the alert's claim.
4. Decide	False positive, benign true positive, watch, or escalate.
5. Document	Record what was checked, the decision, and the rationale.

3.3 Decision language

False positive

The detection fired, but investigation shows no genuine security issue matching the intended detection logic.

Benign true positive

The detection correctly identified a real event, but the event is expected, authorized, or otherwise not malicious in context.

True positive

The detection correctly identified activity that represents a security concern requiring action, monitoring, or escalation.

Precise language prevents confusion in handoffs. Calling everything a “false positive” when some events are real but authorized trains bad habits and misleads metrics.

3.4 Escalation judgment

Escalate when potential impact is high, required access or tools are unavailable, the pattern aligns with known attack behavior, or your notes would not allow another analyst to continue without restarting. Seeking help is professional behavior, not failure.

3.5 Chapter review

1. Define triage in the SOC sense.
2. List the five triage steps in order.
3. Contrast false positive and benign true positive with a short example of each.

4. Give two appropriate reasons to escalate a case.

Chapter 4 — Documentation, Notes, and Escalation

Learning objectives. Explain why documentation is operational work; apply a minimum note structure; and assemble a clear escalation handoff.

4.1 Why documentation is the job

If the next analyst cannot reconstruct your reasoning, the investigation effectively restarts. Documentation creates continuity across shifts, supports management and audit needs, and protects both the organization and the individual analyst. It is not clerical busywork; it is part of the control system.

4.2 Minimum note structure

Field	Content
What	Alert or event name and brief description
When	Event time and time of analyst work
Who / asset	User, host, IP address, or cloud resource
Evidence	Brief reference to searches or log findings
Decision	False positive, benign, watch, or escalate
Next	Required follow-up, if any

Standard
A note another trained analyst can trust should answer: what happened, what you checked, what you decided, and why—without requiring a meeting to decode it.

4.3 Escalation packets

An escalation is a handoff, not a dump of raw alerts. Include a short summary, estimated severity or business impact, evidence already collected, hypotheses ruled out, and a clear request for Level 2 or incident response. Quality of handoff is a measure of L1 competence.

4.4 Worked scenario

Alert: multiple failed logins followed by a successful login from a new country. The user is a salesperson known to travel. MFA succeeded on the successful login. A careful note would record the alert details, travel context if known, MFA result, identity log findings, and a decision such as benign true positive with monitoring—or escalation if policy requires review of all geographic anomalies.

4.5 Chapter review

1. Why is documentation treated as operational work?
2. List the six fields of a minimum note.
3. What should a good escalation packet include?
4. Draft a short note for the travel-login scenario using the six fields.

Chapter 5 — MITRE ATT&CK; for SOC Analysts

Learning objectives. Define ATT&CK; distinguish tactics from techniques; explain why SOCs use the framework; and formulate investigation questions using ATT&CK; language.

5.1 Definitions

MITRE ATT&CK;

MITRE ATT&CK; is a publicly available knowledge base of adversary tactics and techniques based on real-world observations. It provides a common language for describing how attackers operate across enterprise, mobile, and other technology domains.

Tactic

A tactic is the adversary's tactical goal—the reason for an action (for example, Credential Access or Lateral Movement).

Technique

A technique is the method used to achieve a tactic (for example, Brute Force under Credential Access). Sub-techniques further refine methods where applicable.

ATT&CK; does not replace vendor detections or local runbooks. It organizes thinking. When an analyst can name a likely tactic and technique, searches become more targeted and communication with peers becomes clearer.

5.2 Why SOC teams use ATT&CK;

Teams use ATT&CK; to map alerts to known behaviors, to discover gaps in detection coverage, to structure threat hunts, and to report in language that security engineers and leaders understand. For L1, the immediate value is vocabulary: you can say what you think you are seeing and what evidence would confirm it.

5.3 Starter tactics

Familiarize yourself with these tactic names: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. You are not required to memorize every technique identifier. Learn to navigate the matrix and look up techniques when cases demand it.

5.4 Investigation questions

After an alert, useful questions include: What tactic might this represent? Which technique is the best fit? What data source would show that technique? What would a competent adversary likely do next? These questions connect monitoring work to adversary models without requiring advanced hunting skill on day one.

Exercise

Visit attack.mitre.org. Open Credential Access. Select one technique. Record its ID, name, and one data source listed for detection.

5.5 Chapter review

1. Define MITRE ATT&CK;, tactic, and technique.
2. Give one reason SOC analysts use ATT&CK; in daily work.
3. Write two investigation questions you could ask after a suspicious authentication alert.

Chapter 6 — SIEM Fundamentals and Purposeful Search

Learning objectives. Restate the role of a SIEM; form investigation questions before searching; scope time and assets appropriately; and define “good enough” evidence for L1 decisions.

6.1 Role of the SIEM

In many environments the SIEM is both the alert console and the primary search interface for historical logs. It centralizes visibility. It does not invent answers. Analysts who search without a question generate noise; analysts who search with a question generate timelines.

6.2 Search with a question

Before opening a search window, write the question. Examples: Which accounts authenticated from this IP in the last twenty-four hours? What process executed on this host at the alert timestamp? When did this user last succeed prior to the failure sequence? Questions of who, what, when, and where keep work bounded.

6.3 Scope and time range

Begin with a narrow scope—specific host or user and a short time window around the event—then expand if the hypothesis remains open. Excessively wide ranges increase cost, slow queries, and bury relevant events. Discipline in scope is a professional skill.

6.4 Good enough evidence

Level 1 does not require exhaustive collection of every possible log. It requires sufficient evidence to support or reject the alert’s claim and to write a decision another analyst can defend. When evidence is incomplete and impact may be high, escalate rather than invent certainty.

6.5 Chapter review

1. Why is a written question useful before a SIEM search?
2. Why start with a narrow time range and asset scope?
3. What does “good enough” evidence mean for an L1 decision?
4. Draft one SIEM question for an alert about a new local administrator account.

Chapter 7 — Incident Response and the Analyst’s Place in It

Learning objectives. Name major incident response phases; locate L1 triage within that lifecycle; state limits on unilateral containment; and explain how notes support lessons learned.

7.1 Lifecycle overview

Incident response (IR) lifecycle (common model)

Preparation → Detection and Analysis → Containment → Eradication → Recovery → Post-Incident Activity (Lessons Learned). Organizations adapt NIST and related guidance to local policy; the phase names teach sequence and responsibility.

The operational mission sequence taught in Chapter 1 (Detect → Understand → Contain → Recover → Document) fits inside this broader lifecycle. L1 work concentrates on detection and analysis, with documentation feeding later phases.

7.2 Where Level 1 operates

Phase	Typical L1 connection
Preparation	Know tools, runbooks, contacts, and escalation paths.
Detection & Analysis	Triage alerts, retrieve evidence, first decision, escalate when required.
Containment and beyond	Usually L2, IR, or engineering under approved authority.
Lessons learned	Quality L1 notes improve detections, runbooks, and training.

7.3 Containment discipline

Isolating systems or disabling accounts can stop an attacker—and can also interrupt business operations or destroy evidence if done incorrectly. Unless a documented runbook and your authority explicitly allow an action, escalate with impact notes rather than improvising containment.

7.4 Lessons learned

After significant incidents, teams examine what worked, what failed, and what should change in detection or process. Analyst notes are primary source material for those reviews. Vague notes produce weak improvements.

7.5 Chapter review

1. List the major IR phases in order.
2. In which phase does most L1 triage occur?
3. Why is unilateral “shut it off” often the wrong first action?
4. How do L1 notes support lessons learned?

Chapter 8 — Practice Path, Labs, and Professional Next Steps

Learning objectives. Summarize core competencies gained; construct a thirty-day practice plan; identify free laboratory resources; and describe evidence of readiness for further training or entry-level roles.

8.1 Competencies from this course

A student who completes this text with honest practice can explain what a SOC is; operate within tier expectations; apply a mission and triage sequence; use precise decision language; write minimum viable notes; escalate cleanly; apply basic ATT&CK; vocabulary; search with purpose; and locate L1 work inside incident response.

8.2 Thirty-day practice plan

Focus	Activity
Recall	Re-answer Chapter 1–4 review questions from memory once per week.
Labs	Fifteen to twenty minutes on TryHackMe or CyberDefenders, three sessions per week.
ATT&CK;	One technique per week: read, note data sources, write one detection idea.
Writing	One practice triage note per week from a sample or lab alert.

8.3 Recommended free resources

- TryHackMe — beginner blue-team and SOC-oriented rooms
- CyberDefenders — defensive challenges and labs
- MITRE ATT&CK; — attack.mitre.org
- NIST SP 800-61 — Computer Security Incident Handling Guide
- CISA — public incident response and cybersecurity materials

8.4 Readiness and career direction

Readiness is demonstrated by process fluency and practice evidence—not by memorizing tool screenshots alone. Maintain a small portfolio of anonymized practice notes and lab completions. When pursuing roles, lead with skills and judgment. Within the Genesis ecosystem, career tools such as NodePath and REACH may support job search after foundational skills are in place.

8.5 Chapter review

1. List three competencies you can demonstrate after this course.
2. Write a three-line personal practice plan for the next month.
3. Name the first lab resource you will open and why.
4. What evidence would show a hiring manager you understand L1 process?

Appendix A — SOC Writing Style Guide

This style guide sets expectations for case notes, escalations, and professional communication in SOC work and in this course.

A.1 Principles

- Prefer facts over adjectives. Write what was observed, not how dramatic it felt.
- Use standard decision terms: false positive, benign true positive, true positive, escalate, monitor.
- Record time in a consistent form and include time zone when policy requires it.
- Name systems and users as they appear in authoritative logs; avoid nicknames in formal notes.
- Separate observation from interpretation. “Login failed ten times” is observation; “likely brute force” is interpretation—label it as such if used.

A.2 Minimum note checklist

What · When · Who/asset · Evidence · Decision · Next step

A.3 Escalation tone

Be concise and respectful. State what you need: review, containment authority, deeper malware analysis, or policy exception. Do not apologize for escalating when criteria are met. Do not demand action without evidence summary.

A.4 Example — weak vs strong note

Weak: “Looks bad. User might be hacked. Escalating.”

Strong: “Alert: impossible travel / new country success after failures. User: j.smith. 14 failed then 1 success, MFA passed, 18:40–18:52 UTC. Identity logs show prior travel pattern last quarter. Decision: benign true positive pending UEBA policy; monitoring 24h. Next: none unless repeat.”

A.5 Language to avoid

Avoid slang, blame, speculation presented as fact, and absolute claims when evidence is partial. Prefer “consistent with,” “suggests,” and “based on available logs.”

Appendix B — Glossary of Core Terms

Alert. A notification generated by a detection rule or system indicating activity that may require analyst review.

Benign true positive. A correctly detected real event that is authorized or non-malicious in context.

Containment. Actions taken to limit the spread or impact of an incident.

Detection. The identification of potentially malicious or policy-violating activity through tooling or analysis.

Escalation. Transfer of a case to a higher tier or specialized team with sufficient context for continued work.

False positive. A detection that fired without a genuine issue matching the detection's intent.

Incident. A violation or imminent threat of violation of security policies or standard security practices.

Log. A recorded record of events, typically timestamped and attributable to systems or identities.

MITRE ATT&CK.; A knowledge base of adversary tactics and techniques based on real-world observations.

Runbook. A documented procedure for handling a class of alerts or incidents.

SIEM. Security Information and Event Management system for log collection, search, and alerting.

SOC. Security Operations Center — function for monitoring, investigation, and response.

Tactic. In ATT&CK;, the adversary's tactical goal.

Technique. In ATT&CK;, the method used to achieve a tactic.

Telemetry. Signals describing activity across systems, networks, identities, and cloud services.

Triage. Initial assessment of an alert to determine priority and next action.

True positive. A detection that correctly identifies activity of security concern.

Appendix C — Answer Key (Selected Review Items)

Answers are indicative. Full-sentence student responses that capture the same meaning are acceptable.

Chapter 1. SOC = organizational function for monitoring, investigation, response. L1 triage vs L2 deeper investigation. Mission: Detect, Understand, Contain, Recover, Document. Workflow: See, Check context, Decide, Write. Documentation enables continuity and trust.

Chapter 2. Telemetry = signals; logs = stored event records. Sources include endpoint, network, identity, cloud. SIEM centralizes search; questions drive value. Habit: alert → required evidence → retrieve → timeline.

Chapter 3. Triage = initial assessment for priority and next action. Steps: read, context, evidence, decide, document. FP vs benign TP as defined in chapter. Escalate on impact, access limits, attack patterns, or weak standalone notes.

Chapter 4. Documentation is operational continuity. Six fields: what, when, who/asset, evidence, decision, next. Escalation includes summary, impact, evidence, ruled-out items, request. Scenario notes should apply the six fields.

Chapter 5. ATT&CK; = adversary behavior knowledge base; tactics = goals; techniques = methods. Used for common language and mapping. Questions: tactic, technique, data source, next adversary step.

Chapter 6. Question-first search reduces noise. Narrow scope improves signal. Good enough = enough to decide and document, else escalate.

Chapter 7. Phases as listed in chapter. L1 primarily Detection & Analysis. Unilateral shutdown risks business impact and evidence. Notes feed lessons learned.

Chapter 8. Competencies and plans are personal; quality requires specific practice and lab evidence.