SOC Analyst Fundamentals

Monitoring, Detecting, and Responding to Security Threats in Modern Environments

Preface

Every security breach that makes headlines shares something in common: somewhere, a SOC Analyst was either the first line of defense that stopped the attack—or the one who wasn't yet equipped to catch it in time. This book exists to ensure you become the former.

SOC Analyst Fundamentals: Monitoring, Detecting, and Responding to Security Threats in Modern Environments was written for one clear purpose—to give aspiring and early-career SOC Analysts the practical knowledge they need to perform confidently and effectively from day one. Whether you're preparing for your first role in a Security Operations Center, transitioning from another area of IT, or looking to solidify foundational skills you've been building on the job, this book is your comprehensive guide to the analyst craft.

Why This Book?

The cybersecurity industry faces a persistent challenge: organizations need skilled analysts *now*, but much of the available training is either too theoretical, too fragmented, or too advanced for someone stepping into the SOC analyst role for the first time. I wrote this book to bridge that gap. Every chapter is designed around what a SOC Analyst actually encounters—real alerts, real logs, real decisions—rather than abstract concepts disconnected from the daily workflow.

What You'll Find Inside

This book is structured to mirror the journey of a SOC Analyst, from understanding the role to mastering it.

Chapters 1–2 establish the foundation, exploring *what a SOC Analyst really does* and how the Security Operations Center is structured. You'll understand where analysts fit within the broader security ecosystem and what's expected at each tier.

Chapters 3–6 build the essential technical knowledge every analyst needs: networking fundamentals, operating system concepts, log source familiarity, and SIEM platforms. These aren't generic IT overviews—they're tailored specifically to the analyst's perspective, focusing on what matters when you're investigating alerts at 2 a.m.

Chapters 7–8 shift into the adversarial mindset, covering common attack techniques and indicators of compromise (IOCs). Understanding how threats manifest is the cornerstone of effective detection, and these chapters ensure you can recognize malicious activity when it crosses your screen.

Chapters 9–14 form the operational core of the book, walking you through the analyst's daily responsibilities: triaging alerts, investigating incidents, crafting SIEM queries, leveraging endpoint and network monitoring tools, executing containment actions, and producing clear documentation. This is where knowledge transforms into *capability*.

Chapters 15–16 round out the journey with SOC best practices, common pitfalls to avoid, and a forward-looking discussion on growing from SOC Analyst into a broader cybersecurity specialist role.

Finally, the **appendices** provide quick-reference materials you'll return to repeatedly—common ports and protocols, SIEM query examples, an incident response checklist, typical alert scenarios, and a career roadmap for analysts planning their next move.

How to Use This Book

Read it cover to cover for a structured learning experience, or use individual chapters as targeted references when you need to sharpen a specific skill. Either way, the content is designed to be *immediately applicable* to the analyst's workflow.

Acknowledgments

This book would not exist without the countless SOC Analysts I've had the privilege of working alongside—those who shared their war stories, their shortcuts, their hard-won lessons from the trenches. I'm also deeply grateful to the cybersecurity community at large, whose open commitment to knowledge sharing continues to elevate the profession. Special thanks to the technical reviewers who ensured accuracy and relevance throughout every chapter, and to my family for their patience during the many late nights that, fittingly, mirrored a SOC Analyst's own schedule.

The world needs more capable, confident SOC Analysts. Threats are growing in volume and sophistication, and the analyst sitting behind the console remains one of the most critical defenses any organization has. My hope is that this book gives you the foundation to be *that* analyst—the one who catches what others miss.

Let's get started.

Julien Moreau

Table of Contents

Chapter 1: What a SOC Analyst Really Does

The fluorescent lights never go off. Somewhere in a windowless room, rows of monitors cast a pale blue glow across the faces of professionals who sit with headsets on, eyes scanning dashboards that refresh every few seconds. A notification pops up on one screen, a yellow triangle warning of an anomalous login attempt from an IP address registered in a country where the organization has no employees. Within seconds, a SOC Analyst clicks into the alert, pulls up contextual logs, cross-references the IP against threat intelligence feeds, and begins the careful, methodical work of determining whether this is a genuine intrusion attempt or simply a false positive generated by an employee using a VPN on vacation. This is the reality of a Security Operations Center, and the analyst sitting at that desk is the first and most critical line of defense in modern cybersecurity.

Understanding what a SOC Analyst really does requires peeling back layers of misconception. Many people outside the cybersecurity field imagine the role as something cinematic, a lone hacker in a hoodie furiously typing commands to thwart a digital villain in real time. The truth is far more nuanced, more disciplined, and in many ways, more intellectually demanding. A SOC Analyst is not a single-purpose defender but a multifaceted professional who blends technical expertise with investigative thinking, communication skills, and an almost obsessive attention to detail. This chapter will walk you through the daily reality of the role, the core responsibilities that define it, the tools that make it possible, and the mindset that separates a competent analyst from an exceptional one.

The Security Operations Center as a Living Organism

Before we can understand what a SOC Analyst does, we need to understand where they do it. A Security Operations Center is a centralized function within an organization, sometimes a physical room, sometimes a distributed virtual team, that is responsible for continuously monitoring and improving an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. Think of it as the nervous system of an organization's digital body. Every signal, every packet, every authentication event flows through the SOC's awareness in some form.

The SOC operates around the clock. Threats do not observe business hours, and neither do the analysts who watch for them. Most SOCs run in shifts, typically following a follow-the-sun model for global organizations or a rotating 24/7 schedule for smaller teams. This means that at any given moment, day or night, weekend or holiday, there are analysts watching, waiting, and ready to act.

The SOC is structured in tiers, and understanding this hierarchy is essential to understanding the analyst's role within it.

Tier	Title	Primary Responsibility	Typical Experience Level
Tier 1	SOC Analyst (Junior/Associate)	Alert monitoring, initial triage, ticket creation, escalation of suspicious events to higher tiers	Entry level to 1-2 years
Tier 2	SOC Analyst (Senior/Incident Responder)	Deep-dive investigation, correlation of events, containment actions, detailed incident analysis	2-5 years

Tier 3	SOC Analyst (Threat Hunter/Subject Matter Expert)	Proactive threat hunting, advanced forensics, malware analysis, development of detection rules and playbooks	5+ years
SOC Manager	SOC Manager/Director	Team leadership, process improvement, reporting to executive leadership, strategic planning	7+ years with management experience

A Tier 1 Analyst is the front line. They are the ones who first see the alerts, who make the initial determination of whether something is worth investigating further, and who set the entire incident response process in motion. It is a role that demands speed, accuracy, and the humility to escalate when something exceeds your current capability. The work of a Tier 1 Analyst might seem repetitive to an outsider, reviewing hundreds of alerts per shift, but within that repetition lies the critical skill of pattern recognition. The analyst who catches the one genuinely malicious event hidden among 500 false positives is the analyst who prevents a breach.

A Day in the Life of a SOC Analyst

Let us walk through a realistic shift to ground these concepts in practical reality.

The shift begins with a handoff. The outgoing analyst briefs the incoming analyst on everything that happened during the previous shift: open investigations, ongoing incidents, any changes to the threat landscape, new detection rules that were deployed, and systems that are currently under maintenance and might generate expected noise. This handoff is sacred. A poor handoff can mean a missed indicator of compromise that was already partially investigated, forcing the new analyst to start from scratch or, worse, to miss it entirely.

Once seated, the analyst opens the primary tool of their trade: the SIEM, or Security Information and Event Management system. The SIEM is the central nervous system of the SOC itself. It aggregates logs from across the entire organization, firewalls, endpoint detection and response tools, email gateways, proxy servers, Active Directory, cloud platforms, and dozens of other sources. It normalizes this data into a common format and runs correlation rules against it to generate alerts.

The analyst's SIEM dashboard might look something like this in a typical environment:

```
SIEM Dashboard Summary - Shift Start
=====================================
Total Alerts (Last 8 Hours):        847
Critical Alerts:                      3
High Alerts:                         27
Medium Alerts:                      189
Low/Informational:                  628

Open Investigations:                  2
Pending Escalations:                  1

Top Alert Categories:
  - Failed Authentication Attempts:  312
  - Suspicious Outbound Traffic:      45
  - Malware Detection (Endpoint):     18
  - Policy Violation:                 94
  - Anomalous User Behavior:          12
```

Eight hundred and forty-seven alerts in eight hours. This is not unusual. In fact, for a medium-sized organization, this is relatively modest. The analyst's job is not to investigate every single one of these alerts individually. That would be physically impossible. Instead, the analyst uses a combination of automated filtering, prioritization logic built into the SIEM, and their own professional judgment to identify which alerts require human attention.

The three critical alerts demand immediate attention. The analyst clicks into the first one. It reads:

```
Alert: Potential Data Exfiltration Detected
```

```
Severity: Critical
Timestamp: 2024-03-15 02:47:33 UTC
Source Host: WORKSTATION-FIN-042
Source User: j.martinez
Destination IP: 185.220.101.34
Protocol: HTTPS
Data Volume: 2.4 GB transferred in 23 minutes
Threat Intel Match: IP associated with known C2 infrastructure
(Cobalt Strike)
```

The analyst's pulse quickens, but their training takes over. They do not panic. They do not immediately call the incident response team. They investigate. This is the triage phase, and it is where the analyst's value is most clearly demonstrated.

The first step is to validate the alert. Is this a true positive or a false positive? The analyst begins pulling contextual information. They check the user profile for j.martinez. Is this a real employee? What department are they in? Finance, according to Active Directory. What is their normal work pattern? Typically active between 08:00 and 18:00 local time, not at 02:47 in the morning. That is the first red flag confirmed.

Next, the analyst examines the destination IP. They query it against multiple threat intelligence platforms:

```
Threat Intelligence Query: 185.220.101.34
==========================================
VirusTotal:       14/89 vendors flagged as malicious
AbuseIPDB:        Confidence of Abuse: 97%
AlienVault OTX:   Associated with Cobalt Strike C2, APT29
campaigns
Shodan:           Open ports: 443, 8443 | SSL Certificate: Self-
signed
First Seen:       2024-01-22
Last Reported:    2024-03-14
Geolocation:      Moscow, Russia
ASN:              AS12345 - Suspicious Hosting Provider
```

Multiple independent sources confirm the IP is associated with command and control infrastructure. The second red flag is confirmed.

The analyst then pivots to the endpoint. Using the organization's EDR (Endpoint Detection and Response) tool, they pull the process tree from WORKSTATION-FIN-042 around the time of the alert:

```
Process Tree - WORKSTATION-FIN-042
===================================
explorer.exe (PID: 1204)
  └── outlook.exe (PID: 3847)
        └── winword.exe (PID: 5102)
              └── cmd.exe (PID: 6233)
                    └── powershell.exe (PID: 6891)
                          └── rundll32.exe (PID: 7104)
                                └── svchost.exe (PID: 7302)
[SUSPICIOUS]
                                      └── Connection to
185.220.101.34:443
```

This process chain tells a story. The user opened Outlook, received an email, opened a Word document, which spawned a command prompt, which launched PowerShell, which used rundll32 to load a DLL, which created a suspicious svchost.exe process that made the outbound connection. This is a textbook phishing attack leading to a Cobalt Strike beacon deployment.

The analyst now has enough evidence to make a confident determination. This is not a false positive. This is a genuine security incident. The analyst documents their findings in a structured format, following the organization's incident response playbook, and escalates to Tier 2 with all the evidence gathered. Depending on the organization's policies and the analyst's authority level, they might also take immediate containment actions, such as isolating the endpoint from the network using the EDR tool:

```
EDR Command: Isolate Host
==========================
Target: WORKSTATION-FIN-042
Action: Network Isolation (Allow SOC communication only)
Initiated By: analyst.thompson
Timestamp: 2024-03-15 03:12:45 UTC
Status: Isolation Confirmed
```

This entire process, from alert to escalation, took approximately 25 minutes. That is 25 minutes of focused, methodical investigation that potentially prevented a significant data breach from the finance department. And there are still two more critical alerts waiting, plus 27 high-severity alerts that need review before the shift is over.

Core Responsibilities Beyond Alert Triage

While alert triage is the most visible and time-consuming activity, it is far from the only responsibility of a SOC Analyst. The role encompasses several critical functions that together form a comprehensive defensive capability.

Incident documentation is a responsibility that many new analysts underestimate. Every action taken during an investigation must be recorded with precision. The notes an analyst writes during triage become the foundation for incident reports, forensic investigations, legal proceedings, and lessons-learned sessions. Poor documentation can undermine an otherwise excellent investigation. A well-documented incident ticket includes the initial alert details, every investigative step taken, every tool queried, every finding discovered, the analyst's reasoning for their conclusions, and the actions taken or recommended.

Threat intelligence consumption is another ongoing responsibility. A SOC Analyst must stay current with the evolving threat landscape. This means reading threat intelligence reports, understanding new attack techniques documented in frameworks like MITRE ATT&CK, reviewing indicators of compromise shared by industry peers, and understanding how these threats might apply to their specific organization. An analyst who only reacts to alerts without understanding the broader threat context is operating at a significant disadvantage.

Playbook and runbook execution is the structured methodology that brings consistency to the SOC's operations. A playbook defines the step-by-step process for handling specific types of alerts or incidents. For example, a phishing playbook might include the following steps:

Step	Action	Details
1	Validate the alert	Confirm the email was delivered and opened by the recipient
2	Analyze email headers	Check sender reputation, SPF/DKIM/DMARC results, originating IP
3	Analyze attachments or URLs	Submit to sandbox, check against threat intelligence
4	Determine scope	Identify all recipients of the same email across the organization
5	Check for interaction	Determine if any recipients clicked links or opened attachments
6	Endpoint investigation	For users who interacted, check endpoints for indicators of compromise
7	Containment	Block sender, remove emails from all mailboxes, isolate compromised endpoints
8	Documentation	Record all findings and actions in the incident management system
9	Communication	Notify affected users and relevant stakeholders
10	Lessons learned	Update detection rules if the phishing email bypassed existing controls

Tuning and feedback is a responsibility that directly improves the SOC's effectiveness over time. When an analyst repeatedly encounters false positives from a particular detection rule, they document the pattern and recommend tuning adjustments. This might mean adding exclusions for known-good behavior, adjusting thresholds, or refining the correlation logic. An analyst who simply closes false positives without providing feedback is allowing the same noise to waste their colleagues' time on future shifts.

The Analyst Mindset

Technical skills can be taught. Tools can be learned. But the mindset of an effective SOC Analyst is something that must be cultivated deliberately. It is a combination of several intellectual qualities that work together to produce consistently sound investigative outcomes.

Healthy skepticism is the foundation. An analyst must question everything. An alert says a connection is malicious, but is it really? A log shows a user authenticated successfully, but was it truly that user? The analyst lives in a world where attackers deliberately try to make malicious activity look normal and where legitimate activity sometimes looks suspicious. The ability to hold judgment in suspension while gathering evidence is essential.

Contextual thinking separates good analysts from great ones. A single log entry means almost nothing in isolation. A failed login attempt is meaningless on its own. But a failed login attempt from a foreign IP, followed by a successful login from the same IP two minutes later, followed by the creation of a new mailbox forwarding rule, followed by access to sensitive SharePoint documents, tells the story of a compromised account being exploited. The analyst must constantly ask: what happened before this event, what happened after, and what is the broader context?

Composure under pressure is non-negotiable. When a critical alert fires and the evidence suggests an active intrusion, the analyst cannot afford to panic. Panic leads to skipped investigative steps, premature conclusions, and poorly communicated escalations. The playbook exists precisely for these moments, providing a structured path forward when the adrenaline starts flowing.

Continuous learning is not optional in this field. The threat landscape evolves daily. New vulnerabilities are discovered, new attack techniques are developed, new tools are released, and new threat actors emerge. An analyst who stops learning becomes less effective with each passing month. Reading threat reports, practicing in lab environments, pursuing certifications, and engaging with the broader security community are all essential habits.

Note on Professional Development

It is worth emphasizing that the SOC Analyst role is not a dead end. It is a launchpad. The skills developed in the SOC, log analysis, network traffic interpretation, endpoint forensics, threat intelligence, incident response, and structured investigative methodology, are foundational to nearly every advanced cybersecurity role. Former SOC Analysts go on to become incident response leads, threat hunters, security engineers, detection engineers, malware analysts, and chief information security officers. The breadth of exposure that the SOC provides is unmatched in the cybersecurity field.

Practical Exercise: Alert Triage Walkthrough

To reinforce the concepts covered in this chapter, work through the following exercise. Read the alert below and answer the investigation questions that follow.

```
Alert: Suspicious PowerShell Execution
Severity: High
Timestamp: 2024-03-16 14:22:17 UTC
Source Host: SERVER-DC-01
Source User: svc_backup (Service Account)
Process: powershell.exe -enc
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQA...
Parent Process: services.exe
Detection Rule: Encoded PowerShell command execution on domain
controller
```

Investigation questions to consider:

Question Number	Investigation Question
1	Why is encoded PowerShell execution on a domain controller concerning?
2	What is the significance of the parent process being services.exe?
3	What would you check first to determine if this is legitimate or malicious?
4	What does the service account svc_backup normally do, and how would you verify its expected behavior?
5	If you determined this was malicious, what would be the immediate risk given that the target is a domain controller?
6	What containment challenges exist when the compromised system is a domain controller?

Working through exercises like this builds the investigative muscle memory that every SOC Analyst needs. The goal is not to memorize specific answers but to develop the habit of asking the right questions in the right order, every single time.

The SOC Analyst role is demanding, sometimes monotonous, occasionally intense, and always essential. It is the role where cybersecurity theory meets operational reality, where textbook knowledge is tested against live adversaries, and where the decisions of a single individual can determine whether an organization suffers a minor security event or a catastrophic breach. Understanding what a SOC Analyst really does is the first step toward becoming one, and the chapters that follow will equip you with the specific technical skills, tools knowledge, and procedural expertise to do it well.

Chapter 2: Security Operations Center Structure

The Security Operations Center, commonly referred to as the SOC, serves as the central nervous system of an organization's cybersecurity defense strategy. It is the physical or virtual environment where security analysts gather, monitor, and respond to threats that target the organization's digital assets. Understanding the structure of a SOC is not merely an academic exercise for a SOC analyst; it is foundational knowledge that shapes how an analyst operates daily, communicates with peers, escalates incidents, and ultimately contributes to the security posture of the entire enterprise. This chapter provides a thorough exploration of the SOC's architecture, its tiered analyst model, the roles and responsibilities that define each position, the tools and technologies that empower the analyst, and the workflows that bind everything together into a cohesive defense mechanism.

The Purpose and Mission of a Security Operations Center

Before examining the structural components, it is essential to understand why a SOC exists in the first place. Organizations face a relentless barrage of cyber threats ranging from commodity malware and phishing campaigns to advanced persistent threats orchestrated by nation-state actors. The SOC exists to provide continuous monitoring, detection, analysis, and response to these threats. Its mission is to reduce the time between when a threat enters the environment and when it is detected and neutralized. This metric, often described as "dwell time," is one of the most critical indicators of a SOC's effectiveness.

A SOC analyst sits at the heart of this mission. Every alert that fires, every log that is ingested, and every incident that is investigated passes through the hands of an analyst at some stage. The structure of the SOC determines how efficiently this process flows, how effectively knowledge is shared, and how rapidly threats are contained.

The Tiered Analyst Model

The most widely adopted SOC structure follows a tiered model. This model organizes analysts into distinct levels based on their experience, skill set, and the complexity of the tasks they handle. While organizations may customize this model to suit their specific needs, the general framework remains remarkably consistent across industries.

Tier	Role Title	Primary Responsibility	Typical Experience Level
Tier 1	SOC Analyst (Junior/Associate)	Alert monitoring, initial triage, and classification of security events	0 to 2 years of experience
Tier 2	SOC Analyst (Senior/Incident Responder)	Deep dive investigation, correlation of events, and incident containment	2 to 5 years of experience

Tier 3	SOC Analyst (Threat Hunter/Advanced Analyst)	Proactive threat hunting, malware analysis, forensic investigation, and threat intelligence integration	5 or more years of experience
Tier 4	SOC Manager/Director	Strategic oversight, team management, process improvement, and reporting to executive leadership	7 or more years of experience with management skills

This tiered approach is not arbitrary. It is designed to ensure that the most common and straightforward alerts are handled quickly by a larger pool of Tier 1 analysts, while more complex and nuanced threats are escalated to increasingly skilled analysts who have the time and expertise to conduct thorough investigations. The analyst at each tier plays a distinct but interconnected role, and the success of the SOC depends on the seamless collaboration between these tiers.

Tier 1: The First Line of Defense

The Tier 1 SOC analyst is the first human being to lay eyes on a security alert. This role is often the entry point for professionals beginning their careers in cybersecurity, and it is arguably the most demanding in terms of volume and pace. A Tier 1 analyst may review hundreds of alerts in a single shift, making rapid decisions about which events are benign, which require further investigation, and which represent genuine threats that must be escalated immediately.

The daily workflow of a Tier 1 analyst typically involves monitoring the Security Information and Event Management (SIEM) console, reviewing alerts generated by intrusion detection systems, endpoint detection and response tools, and firewall logs. The analyst must quickly assess the context of each alert, determine its severity, and decide on the appropriate course of action.

Consider a practical example. A Tier 1 analyst notices an alert indicating that a user account has attempted to authenticate to a server 47 times within a two-minute window, with all attempts failing. The analyst must determine whether this is a brute-force attack, a misconfigured application, or a user who has forgotten their password. To make this determination, the analyst checks the source IP address, reviews the user's recent activity, and examines whether the targeted server contains sensitive data. If the evidence suggests a legitimate attack, the analyst documents the findings and escalates the alert to Tier 2.

A common command that a Tier 1 analyst might use when investigating such an alert in a SIEM environment like Splunk would be:

```
index=auth_logs sourcetype=windows_security EventCode=4625
| stats count by src_ip, dest_host, user
| where count > 20
| sort -count
```

This query searches for failed authentication events (Windows Event Code 4625), groups them by source IP, destination host, and user, filters for cases where the count exceeds 20, and sorts the results in descending order. Understanding how to write and interpret such queries is a fundamental skill for any SOC analyst, and it is a skill that is refined continuously throughout one's career.

Note: Tier 1 analysts should never dismiss an alert without documenting their reasoning. Even if an alert is determined to be a false positive, the documentation serves as a record that can be reviewed later if a similar pattern emerges as part of a larger campaign.

Tier 2: The Investigative Engine

When a Tier 1 analyst escalates an alert, it lands on the desk of a Tier 2 analyst. This is where the investigation deepens significantly. The Tier 2 analyst takes the initial findings provided by Tier 1 and conducts a comprehensive analysis that may involve correlating data from multiple sources, examining network traffic captures, reviewing endpoint telemetry, and consulting threat intelligence feeds.

The Tier 2 analyst is expected to answer more complex questions. Returning to the brute-force example, the Tier 2 analyst would investigate whether the attacking IP address has been observed in other malicious activity, whether any of the authentication attempts were successful, whether lateral movement has occurred from the targeted server, and whether the attack is part of a broader campaign targeting multiple accounts or systems.

A Tier 2 analyst might use packet capture analysis tools to examine the network traffic associated with the attack. For example, using tcpdump to capture traffic from a suspicious IP:

```
sudo tcpdump -i eth0 host 192.168.1.105 -w
suspicious_traffic.pcap
```

This command captures all network traffic to and from the IP address 192.168.1.105 on the eth0 interface and writes the output to a file called suspicious_traffic.pcap. The analyst would then open this file in a tool like Wireshark to examine the packet contents in detail.

Command Component	Explanation
sudo	Executes the command with elevated privileges, which is required for packet capture
tcpdump	The packet capture utility being invoked
-i eth0	Specifies the network interface to monitor

host 192.168.1.105	Filters traffic to capture only packets involving this specific IP address
-w suspicious_traffic.pcap	Writes the captured packets to a file for later analysis

The Tier 2 analyst also plays a critical role in incident containment. If the investigation confirms that a genuine compromise has occurred, the Tier 2 analyst may take immediate containment actions such as isolating an affected endpoint from the network, disabling a compromised user account, or blocking a malicious IP address at the firewall. These actions require a solid understanding of the organization's network architecture and the potential impact of containment measures on business operations.

Note: Containment decisions must be made carefully. Isolating a critical production server without coordination can cause significant business disruption. Tier 2 analysts should follow established incident response procedures and communicate with relevant stakeholders before taking containment actions.

Tier 3: The Advanced Threat Specialist

The Tier 3 analyst represents the most technically advanced role within the SOC's analyst hierarchy. These professionals are not primarily reactive; they are proactive. While Tier 1 and Tier 2 analysts respond to alerts and investigate incidents as they occur, the Tier 3 analyst actively hunts for threats that may have evaded automated detection mechanisms.

Threat hunting is a hypothesis-driven activity. A Tier 3 analyst might begin with a hypothesis such as "An attacker may be using DNS tunneling to exfiltrate data from our environment." The analyst would then design and execute queries to search for evidence supporting or refuting this hypothesis. For example:

```
index=dns_logs
```

```
| eval query_length=len(query)
| where query_length > 50
| stats count by src_ip, query
| where count > 100
| sort -count
```

This query searches DNS logs for unusually long DNS queries, which can be an indicator of DNS tunneling. Legitimate DNS queries are typically short, so queries exceeding 50 characters in length warrant investigation. The analyst groups the results by source IP and query string, filters for high-frequency occurrences, and sorts the results to identify the most suspicious patterns.

Tier 3 analysts also perform malware analysis, which may involve both static and dynamic analysis techniques. Static analysis involves examining a malicious file without executing it, looking at its code structure, embedded strings, and metadata. Dynamic analysis involves executing the malware in a controlled sandbox environment and observing its behavior, such as what network connections it establishes, what files it creates or modifies, and what registry keys it alters.

A Tier 3 analyst examining a suspicious file might use the strings command to extract readable text from a binary:

```
strings suspicious_file.exe | grep -i "http"
```

This command extracts all readable strings from the executable and filters for those containing "http," which could reveal command-and-control server URLs embedded in the malware.

Analysis Type	Description	Tools Commonly Used
Static Analysis	Examining malware without execution, reviewing code, strings, and metadata	strings, PEStudio, IDA Pro, Ghidra
Dynamic Analysis	Executing malware in a sandbox and observing behavior	Cuckoo Sandbox, Any.Run, Joe Sandbox

Memory Analysis	Examining the contents of system memory for artifacts of malicious activity	Volatility, Rekall
Network Analysis	Analyzing network traffic for indicators of compromise	Wireshark, Zeek, NetworkMiner

Supporting Roles Within the SOC

While the tiered analyst model forms the backbone of the SOC, several supporting roles contribute to its overall effectiveness. These roles do not replace the analyst but rather enhance the analyst's ability to perform their duties.

The **Threat Intelligence Analyst** gathers, processes, and disseminates intelligence about emerging threats, adversary tactics, and indicators of compromise. This intelligence feeds directly into the work of SOC analysts at all tiers, enabling them to recognize and respond to threats more effectively.

The **Security Engineer** is responsible for deploying, configuring, and maintaining the tools and technologies that SOC analysts rely upon. When a SIEM requires a new data source integration, when detection rules need to be tuned to reduce false positives, or when a new endpoint detection tool needs to be deployed, the security engineer handles these tasks so that analysts can focus on monitoring and investigation.

The **Incident Response Lead** coordinates the response to major security incidents, ensuring that all necessary parties are engaged, that communication flows smoothly, and that the incident is managed according to established procedures. During a significant breach, the incident response lead serves as the central point of coordination, while analysts at various tiers contribute their investigative findings.

Role	Primary Focus	Relationship to SOC Analyst
Threat Intelligence Analyst	Gathering and analyzing threat intelligence	Provides context and indicators that analysts use during investigations
Security Engineer	Tool deployment, configuration, and maintenance	Ensures that the tools analysts depend on are functioning optimally
Incident Response Lead	Coordinating response to major incidents	Directs and organizes analyst efforts during significant security events
Compliance Analyst	Ensuring adherence to regulatory requirements	Works with SOC analysts to ensure that monitoring and response activities meet compliance obligations

The SOC Workflow: From Alert to Resolution

Understanding the workflow that connects all of these roles and tiers is essential for any SOC analyst. The workflow represents the lifecycle of a security event from the moment it is detected to the moment it is fully resolved and documented.

The process begins with **data collection**. Logs and telemetry from across the organization's infrastructure are collected and ingested into the SIEM. This data includes firewall logs, endpoint logs, authentication logs, email gateway logs, DNS logs, proxy logs, and many other sources.

Next comes **detection**. The SIEM applies correlation rules, statistical models, and threat intelligence to the ingested data, generating alerts when suspicious patterns are identified. These alerts populate the queue that Tier 1 analysts monitor.