Roles and Responsibilities of L1, L2 and L3 Cybersecurity Analysts with Scenarios Examples v. 1.0

By Wojciech Ciemski

LN: https://www.linkedin.com/in/wojciech-ciemski/

PL: https://securitybeztabu.pl

EN: https://securitybeyondtaboo.com

Version	Date	Change Description
1.0	2025-01-28	Initial version of the document.

License and Disclaimer

Permission is hereby granted to copy and distribute this e-book under the following terms and conditions:

1. **Attribution**
   You must retain the author's name (or pseudonym) and the original title of the e-book on all copies. Any distribution must clearly attribute the work to the original author.

2. **No Modification**
   You may not alter, transform, or build upon the content of this e-book in any way. All copies must be distributed in their original, unmodified form, including this license text.

3. **Disclaimer of Liability**
   The author is not liable for any misuse of the information contained in this e-book. All material is provided for educational and informational purposes only. Any actions taken based on the content are solely at the reader's own risk.

4. **No Warranty**
   The e-book is provided "as is," without warranty of any kind, either expressed or implied. The author does not guarantee the accuracy, completeness, or applicability of the information herein, and shall not be held responsible for any errors, omissions, or potential damages resulting from its use.

5. **Governing Law and Dispute Resolution**
   Any disputes arising from or related to this license or the e-book itself shall be governed by the laws of the author's jurisdiction, unless superseded by mandatory legal provisions.

6. **Final Provisions**

   - This license aims to protect both the author's rights and the freedom of access to knowledge.
   - By using, copying, or distributing this e-book, you acknowledge and agree to be bound by these terms.

Table of Contents

1. Introduction

The Security Operations Center (SOC) often serves as the central nervous system of an organization's cybersecurity strategy. With the increasing frequency and sophistication of cyberattacks, many organizations have adopted a layered approach to incident detection and response—commonly referred to as the L1, L2, L3 model. This structure assigns clear roles and responsibilities to different analyst levels, ensuring that incidents are addressed swiftly and effectively.

1.1 Importance of Defining SOC Roles

A well-defined SOC hierarchy helps organizations respond to threats in a structured manner. When roles are clearly delineated, analysts at each level understand the scope of their responsibilities and the expectations set upon them. This clarity promotes efficient workflow and reduces confusion during high-pressure situations—such as identifying a zero-day exploit or managing a widespread ransomware event.

From a broader operational perspective, defining roles encourages cross-team collaboration. For example:

- **L1 analysts** can triage alerts rapidly, forwarding critical findings to higher-level analysts.
- **L2 analysts** handle detailed incident investigations, leveraging threat intelligence to correlate various alerts and determine the scope of an attack.
- **L3 analysts** focus on root cause analysis, advanced threat hunting, and strategic improvements to security posture.

A common pitfall in SOC environments arises when multiple analysts attempt to tackle the same incident without clear role definitions. By formalizing an L1–L2–L3 structure, organizations can avoid duplication of effort and ensure the necessary expertise is applied to each incident at the correct stage.

1.2 Overview of the L1, L2, L3 Model

The three-tier model segments tasks based on complexity and required expertise:

Level	Primary Focus	Key Activities	Required Skill Set
L1	Alert Monitoring & Basic Triage	Real-time monitoring, initial validation of alerts	Basic SIEM operation, knowledge of common threats
L2	In-Depth Analysis	Correlating events, incident investigation, threat intel	Advanced SIEM/EDR usage, scripting, security analytics
L3	Advanced Forensics & Strategy	Malware analysis, threat hunting, policy development	Reverse engineering, forensic tools, strategic planning

- **L1 (Level 1) – First Line of Defense**
  L1 analysts usually operate the Security Information and Event Management (SIEM) platform, reviewing alerts as they come in. Their primary responsibility is to identify false positives and escalate genuine threats. They also handle routine tasks like user security

awareness checks and may update basic firewall or endpoint security policies under supervision.

    - **Real-life example**: An L1 analyst notices repeated login attempts from a suspicious IP address and escalates the incident to L2 for deeper investigation.

- **L2 (Level 2) – In-Depth Analysis**
  L2 analysts dive into the technical details of potential incidents. Using threat intelligence feeds, Endpoint Detection and Response (EDR) tools, and various security analytics platforms, L2 analysts correlate alerts from multiple sources, looking for hidden patterns or indicators of compromise (IOCs). They also perform preliminary digital forensics—collecting logs, memory dumps, or malicious binaries for further analysis.

    - **Real-life example**: An L2 analyst cross-references file hashes flagged by the SIEM against a threat intel database, discovers them to be part of a known ransomware campaign, and initiates containment measures.

- **L3 (Level 3) – Advanced Forensics and Strategy**
  L3 analysts are typically seasoned experts who work on the most complex aspects of incident response. Their tasks may include reverse-engineering malware, conducting enterprise-wide threat hunts, and leading major investigations when sophisticated adversaries compromise the organization. Moreover, they assist in drafting and refining security policies to fortify defenses based on emerging threats.

    - **Real-life example**: An L3 analyst identifies a new variant of malware, writes custom YARA rules to detect it in the environment, and collaborates with threat intelligence teams to update the organization's defense strategies.

Bridging Theory and Practice

To translate this structure into day-to-day SOC operations, each level must be equipped with the right tools and training. SIEM dashboards, log management solutions, endpoint security platforms, and threat intelligence portals are shared across all levels, but the extent of usage and complexity of tasks vary:

- **L1** might rely heavily on SIEM dashboards for real-time alerting.
- **L2** could utilize scripting skills (e.g., **Python** or **PowerShell**) to automate log analysis or to parse suspicious payloads.
- **L3** might use advanced digital forensics software (e.g., **Volatility**, **Autopsy**) and threat modeling frameworks (e.g., **MITRE ATT&CK**).

In practical SOC environments, it is common to see individuals or small teams specializing in particular domains (e.g., cloud security, identity management) while still adhering to the L1–L2–L3 framework. For instance, an L3 analyst with expertise in cloud security might focus on analyzing unusual AWS or Azure logs, working closely with L2 analysts who escalate cloud-related alerts.

Below is a simplified schematic illustrating the alert flow in a three-tier SOC model:

Alert Origin -> SIEM (L1 Triages Alert) -> L2 Investigation -> Potential L3 Escalation

This linear representation serves as a guideline, but actual SOC processes may loop back or jump levels depending on the severity and nature of the incident. High-impact events might warrant immediate involvement of L3 analysts even before L2 completes a full investigation. Conversely, some minor incidents flagged by L1 can be resolved without further escalation.

2. Roles and Responsibilities

When security teams organize their work within a Security Operations Center (SOC), they often adopt a tiered approach that categorizes tasks and expertise into distinct levels—commonly referred to as L1, L2, and L3. This structure helps distribute responsibilities according to complexity and criticality, ensuring a clear workflow when responding to potential cyber incidents. The ultimate goal is to minimize incident impact by detecting threats early, containing them swiftly, and leveraging forensic insights to bolster the organization's defenses.

In practice, each level of analyst plays a unique role in this layered defense:

- **L1 (Level 1)** is usually the first point of contact when an alert or suspicious activity is detected. Analysts at this level focus on real-time monitoring, basic triage, and preliminary classification of events. Their role is often described as the "eyes on glass," since they typically watch dashboards, respond to alerts generated by tools such as SIEM (Security Information and Event Management) systems, and perform initial assessments. It is critical that L1 analysts maintain accuracy in logging incidents and escalating them. Mistakes at this stage can lead to missed threats or false alarms consuming valuable resources.
- **L2 (Level 2)** analysts step in when alerts exceed the basic triage threshold or require more in-depth investigation. They bring broader experience in correlating data across different sources—logs from firewalls, endpoint protection platforms, intrusion detection systems, and other security devices. L2 analysts dig into patterns, evaluate the threat's scope, and coordinate a more detailed response. They often have the mandate to pull additional forensic data or collaborate with IT teams to isolate suspicious hosts. In many SOCs, L2 analysts also perform limited threat hunting or test the validity of alerts against known attack techniques documented in frameworks like MITRE ATT&CK.
- **L3 (Level 3)** analysts handle the most complex tasks, ranging from advanced malware analysis to devising the overall response strategy. They often have deep expertise in digital forensics, reverse engineering, threat intelligence, and even secure software development practices. When an incident demands thorough investigation—such as when sophisticated persistent threats arise—L3 specialists take the lead, performing root-cause analysis, creating detection signatures, and recommending long-term architectural changes to strengthen security posture. They also coordinate with stakeholders outside the SOC, such as legal teams or external agencies. For guidance on incident handling best practices, SOCs frequently refer to documents like NIST SP 800-61.

Although the term "Level" might imply a strict hierarchy, effective SOCs view these roles as complementary. Collaboration is paramount—L1 cannot function without strong processes for escalation, L2 depends on thorough initial triage to avoid wasted effort, and L3 benefits greatly from the contextual information gathered by the previous tiers. In large organizations, each level may be staffed by separate teams. In smaller environments, a single analyst might span multiple levels. Regardless of size, the key is to ensure that escalation paths, communication protocols, and documentation practices are firmly in place.

On a practical level, these roles interact with various tooling ecosystems. For instance, an L1 analyst might use scripts to quickly parse logs:

```
# Example script snippet that L1 might use for log parsing
grep "SuspiciousActivity" /var/log/syslog | tail -n 50
```

Whereas an L3 analyst investigating advanced threats could rely on deeper forensic tooling, for example using Volatility to analyze memory captures:

```
# Memory analysis example for an L3 incident responder
volatility -f infected_memory_dump.vmem --profile=Win10x64 pstree
```

Such differences in tooling highlight how responsibility shifts as incidents move from preliminary assessment to intricate forensic analysis.

By understanding the core concepts behind these three levels—what each tier focuses on, how they collaborate, and the typical skills required—you set the foundation for a SOC that can respond more rapidly and with greater precision. The following sections explore each level in depth, offering both theoretical frameworks and real-world scenarios that illustrate the competencies needed at L1, L2, and L3.

2.1 L1 (Level 1) – First Line of Defense

L1 (Level 1) analysts form the backbone of a Security Operations Center (SOC) by serving as the first line of defense against potential threats. Their primary focus is real-time monitoring of security events, applying basic triage procedures, and escalating incidents that require deeper analysis. They deal with large volumes of alerts and must quickly determine which events are benign and which require immediate attention.

Core Duties

- **Alert Monitoring:** L1 analysts continuously observe dashboards and alert queues generated by SIEM (Security Information and Event Management) tools such as Splunk, IBM QRadar, or Azure Sentinel. Their job is to filter out noise, investigate anomalies, and ensure no critical events are missed.
- **Basic Triage:** Once an alert is identified, L1 analysts perform initial investigations. This includes verifying the alert's legitimacy by checking log data, threat intelligence feeds, or endpoint security console information. They typically follow SOC standard operating procedures (SOPs) and playbooks for categorizing and prioritizing incidents.
- **Documentation and Escalation:** If an event is confirmed to be suspicious, L1 analysts collect evidence (log files, screenshots, brief findings) and escalate the issue to Level 2 (L2) with a concise summary. Clear, accurate documentation is essential to facilitate a swift response.

Below is a simplified view of the types of alerts and common actions taken by L1 analysts:

Alert Type	Common Sources	Typical L1 Action
Malware Detection	Endpoint Protection (EDR/AV)	Verify file hash, isolate host if needed

Alert Type	Common Sources	Typical L1 Action
Phishing Email	Email Security Gateway, SIEM	Check sender domain, analyze attachments
Brute Force Attempt	Firewall, IDS/IPS, Authentication Logs	Validate user credentials, track IP origin
Suspicious Network Flow	Network Traffic Monitor, SIEM, IDS	Identify process/user involved, log details
Unauthorized Access	Windows Event Logs, Linux syslog, SIEM	Confirm account usage, gather host logs

Essential Skills and Tools

- **SIEM Mastery:** L1 analysts need a solid understanding of how to use SIEM platforms to filter, search, and tag alerts efficiently. A basic example in Splunk might be:

```
index=security sourcetype=win:security EventCode=4625
| stats count by SourceAddress, AccountName
```

Such a search helps L1 analysts identify repeated failed login attempts, which could indicate a brute force attack.

- **Knowledge of Common Attack Vectors:** Familiarity with top threats, such as phishing, ransomware, or web application exploits, helps L1 analysts recognize patterns quickly. Official resources like the MITRE ATT&CK framework provide extensive references on adversarial techniques and tactics.
- **Communication and Collaboration:** L1 analysts often work closely with other teams, including IT support and network operations, especially when a suspected intrusion involves immediate action like isolating a host or disabling a user account.
- **Ticketing and Case Management:** Proficiency in ticketing systems (e.g., ServiceNow, Jira, or custom in-house platforms) is important. Every alert that L1 analysts investigate should result in a well-documented ticket containing relevant details (time of incident, IP addresses, suspicious files, etc.).

Practical Example

Imagine an L1 analyst receiving an alert for a suspicious file download on a company workstation. The SIEM flags the event because the file's hash matches a known malicious signature on a threat intelligence list. The L1 analyst would:

1. **Check Endpoint Protection Logs:** Confirm whether endpoint protection quarantined the file and whether any other alerts are associated with the same user or host.
2. **Correlate with User Activity:** Investigate if the user was accessing external websites not typically associated with their role.

3. **Contain the Potential Threat:** Depending on internal policies, the L1 analyst might request that IT isolate the endpoint from the network to prevent lateral movement.
4. **Gather Evidence:** Document file hashes, download URL, user details, and attach any relevant log entries to the incident ticket.
5. **Escalate to L2:** If the alert remains suspicious or there is evidence of further compromise, the L1 analyst will hand off the incident to L2 for deeper investigation and remediation steps.

Real-World Considerations

- **High Volume, Rapid Decision-Making:** In large organizations, the SOC may receive thousands of alerts daily. L1 analysts must quickly spot the incidents that pose the greatest risk. Effective filtering rules and SIEM dashboards help streamline this process.
- **Incident Priority Levels:** L1 analysts often assign a severity level—e.g., Critical, High, Medium, Low—based on the organization's risk matrix or threat categorization. This ensures the most dangerous threats are addressed first.
- **Frequent Updates to Playbooks:** Threat landscapes evolve rapidly, so an L1 analyst's triage process and playbooks require continuous updates. Working closely with L2 and L3 teams helps ensure that detection rules and response steps remain relevant.

L1 analysts play an indispensable role in keeping organizations safe. By filtering out false positives, escalating legitimate threats, and maintaining thorough documentation, they enable the SOC to function efficiently and effectively. This foundational work sets the stage for deeper investigative efforts by L2 and L3 teams, ensuring a seamless escalation process that helps contain and mitigate security incidents before they escalate into full-blown crises.

2.2 L2 (Level 2) – In-Depth Analysis

An L2 analyst is responsible for the detailed investigation of security alerts and incidents that have been initially flagged or triaged by L1. This role requires a deeper understanding of threat landscapes, network architectures, and various toolsets to identify and contain incidents effectively. While L1 acts as the first filter, L2 analysts dive into the context and technical details, correlating data from multiple sources to assess the full scope and impact of a security event.

Key Responsibilities

1. **Incident Investigation and Correlation**
   L2 analysts use Security Information and Event Management (SIEM) platforms, Endpoint Detection and Response (EDR) solutions, and network monitoring tools to examine alerts that L1 has escalated. Their focus is on determining the root cause, potential affected systems, and the extent of compromise. This often involves:
   - Checking multiple log sources (firewall, IDS/IPS, endpoint logs) to see if there are common indicators of compromise (IoCs) such as IP addresses, file hashes, or domain names.
   - Using threat intelligence feeds to correlate known malicious patterns with current alerts.

- Building timelines to track attacker activities and pivot points within the environment.

2. **Escalation and Collaboration**
   Once an L2 analyst confirms that an incident is genuine and potentially severe, they collaborate with L3 or other specialized teams for further analysis and mitigation. This might include advanced malware analysis or digital forensics that go beyond L2's scope. Effective communication with L3 helps in refining detection logic and improving future prevention measures.

3. **Playbook Execution**
   Many Security Operations Centers (SOCs) follow predefined incident response playbooks to ensure consistency. L2 analysts are responsible for following these procedures in a more detailed manner than L1. For example, if L1 identifies a potential phishing attack, L2 might:
   - Retrieve full email headers.
   - Extract attachment samples and run them in a sandbox environment.
   - Check for similarities to known phishing campaigns.
   - Recommend or take initial containment steps, such as blocking malicious URLs on the proxy or quarantining endpoints.

4. **Quality Assurance**
   L2 analysts validate the findings and initial triage from L1. This includes confirming the severity level, ensuring the correct categorization of alerts, and verifying that the initial escalation notes are comprehensive. Where L1 might only note "Suspicious login from unknown IP," L2 will investigate if the IP belongs to a known threat actor or if it correlates with user activity patterns.

5. **Reporting and Documentation**
   While L1 typically creates brief alert tickets, L2 analysts expand on those with detailed incident reports. This documentation covers attacker Tactics, Techniques, and Procedures (TTPs), tools used, and all relevant IoCs. These reports become critical references for security posture reviews, audit requirements, and for L3 or threat hunting teams seeking broader patterns.

Technical Competencies

An L2 analyst must be proficient in multiple technical areas to conduct thorough investigations:

- **SIEM Query Mastery**
  Familiarity with query languages (e.g., Splunk's Search Processing Language, Elasticsearch's Query DSL) is essential for creating advanced correlation searches. Here is a simplified Splunk query example that an L2 analyst might use to investigate abnormal user logins:

```
index=authentication source="WinEventLog:Security"
(EventCode=4624 OR EventCode=4625)
| stats count by AccountName, IpAddress
| where count > 10
```

- In this example, an L2 analyst looks for users with more than ten login attempts from the same IP to spot potential brute-force or compromised accounts.

- **Endpoint Forensics**
  L2 analysts use EDR solutions (e.g., CrowdStrike, Microsoft Defender for Endpoint) or forensic tools (e.g., Volatility for memory analysis) to retrieve additional data from compromised hosts. They might investigate processes, registry changes, or suspicious executables.

- **Network Traffic Analysis**
  Understanding network protocols (TCP/IP stack, HTTP, DNS) and using tools like Wireshark or Zeek (formerly Bro) to dissect traffic patterns is central to identifying data exfiltration attempts or malicious connections.

- **Threat Intelligence Integration**
  Incorporating sources like MITRE ATT&CK, VirusTotal, or official vendor advisories helps L2 analysts enrich their findings. For example, if a malicious file hash appears in the logs, an L2 analyst might cross-reference it with VirusTotal to confirm its malicious nature and gather additional context:

```
curl --request GET \
     --url
https://www.virustotal.com/api/v3/files/<HASH_VALUE> \
     --header 'x-apikey: <YOUR_API_KEY>'
```

- **Scripting and Automation**
  Basic scripting knowledge in Python or PowerShell is valuable for parsing large log files or automating repetitive tasks, like extracting URLs from suspicious emails or bulk-checking domains against threat feeds.

Practical Examples from the Field

1. **Investigating Phishing Attachments**
   A user reports receiving an email with a suspicious PDF. L1 tags it as "Potential Phishing." An L2 analyst:
   - Downloads the PDF safely in a sandbox environment.
   - Runs a quick analysis using a script to extract embedded URLs or JavaScript.
   - Checks the extracted URLs against known blacklists and threat intel feeds.
   - Identifies that one URL is tied to a known phishing campaign targeting corporate O365 credentials.
   - Documents findings and escalates to L3 if deeper payload analysis is needed.
2. **Correlating Failed Logins with Suspicious File Modifications**
   L1 notices an increased number of failed SSH logins to a Linux server. L2 further investigates:
   - Queries SIEM for concurrent events from the same IP, discovering a pattern of repeated attempts over different user accounts.

- Cross-references logs from intrusion detection systems to see if the same IP triggered other alerts.
- Finds unusual file modifications in the /tmp directory after a successful login attempt.
- Concludes that the threat actor managed to log in using stolen credentials. L2 coordinates with remediation teams to reset credentials and block the attacker's IP range.

3. **Malware Outbreak Containment**
   When multiple machines trigger antivirus alerts for a specific malware signature, L1 escalates the event to L2. At this level:
   - Analysts examine whether the detected malware is part of a known family or if new variants are involved.
   - They cross-check software inventories to determine which machines are running vulnerable versions of operating systems or third-party applications.
   - If an advanced, previously unseen strain is suspected, L2 prepares a malware sample for deeper analysis and passes it to L3 or a dedicated malware lab.
   - L2 advises on rapid containment (e.g., isolating affected systems from the network) and partial remediation steps while awaiting more comprehensive guidance from L3.

Tools and Resources

Tool/Resource	Purpose	Official Reference
Splunk, IBM QRadar, or Azure Sentinel	SIEM platforms for log correlation and alerting	Splunk Docs, IBM QRadar, Azure Sentinel
CrowdStrike Falcon, Microsoft Defender	Endpoint telemetry and response	CrowdStrike Docs, Microsoft Defender
Wireshark, Zeek	Network traffic analysis	Wireshark Docs, Zeek
VirusTotal, AbuseIPDB	Threat intelligence lookups	VirusTotal, AbuseIPDB
MITRE ATT&CK	Framework mapping attacker TTPs	MITRE ATT&CK
NIST SP 800-61	Incident handling guidelines	NIST SP 800-61

These resources support L2 analysts in building a thorough picture of threats and responding effectively.

Importance to the Organization

Without L2 analysts, alerts could be misclassified or simply closed with insufficient follow-up, leaving potential threats unresolved. By performing in-depth analysis and correlation, they ensure a more accurate assessment of risks, prevent costly breaches, and maintain the smooth

functioning of the SOC. L2 forms the critical bridge between the broad, initial triage of L1 and the specialized, deep-dive capabilities of L3 teams.

2.3 L3 (Level 3) – Advanced Forensics and Strategy

An L3 analyst operates at the highest technical tier within a Security Operations Center (SOC). While L1 analysts focus on alert monitoring and basic triage, and L2 analysts handle in-depth investigations and correlation, L3 analysts go further by diving into complex forensics, advanced threat hunting, malware reverse engineering, and strategic security improvements. Their role often spans across both technical and managerial domains, balancing hands-on work with broader security initiatives such as policy updates and cross-team collaboration.

Core Responsibilities

1. **Advanced Digital Forensics**
   L3 analysts conduct detailed investigations that require specialized tooling and methodologies. This may involve memory analysis of compromised systems, deep dive into network traffic captures, or reconstruction of attacker timelines. The goal is to piece together a complete picture of an incident to understand the root cause, method of entry, and potential lateral movement within the environment.

2. **Malware Reverse Engineering**
   When dealing with novel or sophisticated malware, L3 analysts often reverse engineer samples to uncover hidden functionalities or capabilities. By understanding malware behavior at the assembly or code level, they provide valuable insights that can shape defensive strategies and detection rules.

3. **Threat Hunting**
   L3 analysts proactively search for threats that have not yet triggered standard alerts. They rely on indicators of compromise (IOCs), threat intelligence, and a deep familiarity with the organization's environment. The objective is to detect adversaries early in the kill chain before major damage occurs.

4. **Policy Updates and Security Strategy**
   After analyzing incidents and tracking threat trends, L3 analysts recommend updates to organizational security policies, processes, and technology stacks. They may assist in drafting new guidelines for endpoint protection, network segmentation, or user access controls based on their deep technical insight.

5. **Collaboration and Mentorship**
   As the most senior technical resource in the SOC, L3 analysts often mentor L1 and L2 team members. They may lead tabletop exercises, conduct training sessions on specialized tools, or serve as escalation points for high-severity incidents that surpass L2 capabilities.

Specialized Skill Sets

Skill	Description	Example Tools/References
Memory Forensics	Ability to capture and analyze volatile memory (RAM) to detect hidden processes, malicious drivers, or rootkits.	Volatility, Rekall
Malware Analysis	Expertise in static and dynamic analysis of malicious code, including familiarity with assembly language and sandboxing techniques.	x64dbg, Ghidra, IDA Pro, REMnux
Threat Intelligence	Proficient in consuming, correlating, and operationalizing threat intel from diverse sources.	MITRE ATT&CK, VirusTotal, Intel sharing forums
Network Analysis	In-depth knowledge of packet captures, flow logs, and network forensic artifacts to identify suspicious traffic patterns.	Wireshark, Zeek (Bro), Suricata, Cisco NetFlow
Incident Handling	Skilled in coordinating large-scale incident response, managing stakeholder communication, and orchestrating multi-team investigations.	NIST SP 800-61 (Computer Security Incident Handling Guide)
Programming/Scripting	Advanced scripting and automation skills to create custom detection rules or automate repetitive forensic tasks.	Python, PowerShell, Bash

The transition from L2 to L3 often requires additional training, hands-on practice in specialized labs, or certifications like GIAC Certified Forensic Analyst (GCFA) or GIAC Reverse Engineering Malware (GREM). L3 analysts also benefit from leadership competencies, as they often shape SOC strategy and drive large-scale changes.

Advanced Forensics in Practice

Memory Forensics Example

One common scenario involves investigating a compromised endpoint suspected of hosting memory-resident malware. L3 analysts might:

1. **Acquire Memory**: Use a trusted tool to create a memory dump. On Windows systems, tools like Magnet RAM Capture or Belkasoft Live RAM Capture are typical choices.
2. **Analyze with Volatility**: Employ the Volatility framework to run plugins such as pstree, malfind, or netscan.

```
# Example Volatility commands
volatility -f memory_dump.raw --profile=Win10x64 pstree
volatility -f memory_dump.raw --profile=Win10x64 malfind
```

3. **Identify Malicious Processes**: Investigate unusual processes, suspicious command lines, or code injections indicated by the tool's output.
4. **Extract and Reverse Engineer**: Dump suspicious process memory sections for offline reverse engineering using tools like x64dbg or IDA Pro.

By performing these steps, the L3 analyst uncovers hidden threats that conventional disk-based antivirus solutions might miss. Findings from memory analysis inform subsequent containment measures and guide the threat hunting process (for instance, searching for the same indicators across other systems).

Threat Hunting Methodologies

L3 analysts design and lead proactive hunting campaigns. Rather than waiting for an alert, they look for behavioral patterns or IOCs that might signal adversarial activity. Some key approaches include:

- **Hypothesis-Driven Hunts**: Start with a well-defined hypothesis, e.g., "Threat actors are using living-off-the-land binaries (LOLBins) for lateral movement." The analyst then queries logs and EDR solutions for suspicious use of tools like wmic.exe or rundll32.exe.
- **Machine Learning and Anomaly Detection**: Use behavioral analytics platforms to highlight deviations from normal baselines. L3 analysts refine detection rules to minimize false positives and accurately identify anomalies.
- **Custom Scripts**: Write scripts in Python or PowerShell to query SIEM data, parse system logs, or interrogate endpoints in bulk.
- **Threat Intelligence Correlation**: Cross-reference environment data against open-source or commercial threat intelligence feeds to see if any known malicious IPs, domains, or file hashes appear.

For references, the MITRE ATT&CK framework is widely used to categorize adversary techniques and map them to detection strategies. Many SOCs adopt MITRE ATT&CK to structure their threat hunting efforts and continuously improve coverage.

Malware Reverse Engineering: A Closer Look

While L2 analysts might extract file hashes or run malware in a sandbox, L3 analysts often go deeper:

1. **Static Analysis**: Examine the file's structure, strings, and metadata without executing it. They look for clues like embedded URLs, suspicious API calls, and obfuscated code segments.
2. **Dynamic Analysis**: Execute the malware in a tightly controlled environment (e.g., a virtual machine with network redirection) to observe its behavior. Tools like REMnux offer a Linux toolkit specifically designed for reverse engineering and malware analysis.
3. **Disassembly/Debugging**: Use debuggers (x64dbg, WinDbg) or disassemblers (IDA Pro, Ghidra) to step through code and uncover advanced functionalities, such as credential theft modules or data exfiltration routines.

4. **Indicators Extraction**: Document the malware's indicators (file paths, registry keys, network callbacks) and share them with the rest of the SOC to improve detection coverage.

These reverse engineering findings also inform long-term security strategies. For instance, if the malware exploits a particular Windows service, the L3 team can work with infrastructure teams to harden that service or apply custom access controls across the enterprise.

Developing Security Policy and Strategy

L3 analysts take their insights from deep investigations and translate them into tangible improvements:

- **Recommended Security Controls**: If an advanced threat bypassed existing defenses, L3 analysts might suggest implementing additional endpoint security layers or network segmentation to prevent similar breaches.
- **Policy Enhancement**: Based on discovered attack vectors, they update or create policies related to password complexity, multi-factor authentication, data access privileges, or log retention.
- **Training and Awareness**: When an attack succeeds due to user error (e.g., enabling macros in suspicious documents), L3 analysts might recommend more robust security awareness training or stricter email filtering policies.
- **Reporting to Stakeholders**: L3 analysts often participate in executive briefings or board-level updates. They must summarize complex threats in understandable terms, propose budget allocations for security tools, and align the security strategy with business goals.

Collaboration with L1 and L2

Although L3 analysts handle the most intricate technical problems, they rely on L1 and L2 to feed them accurate, contextual data. Once L3 completes a deep forensic investigation or reverse engineering task, they share actionable indicators and recommended countermeasures with L1 and L2 teams. These teams, in turn, update detection rules, refine triage processes, and ensure quick responses to future incidents.

Additionally, L3 analysts often review escalations from L2 and decide whether the incident demands threat hunting at scale, immediate IR (Incident Response) procedures, or policy revisions. Their advanced perspective ensures the SOC remains agile and anticipates sophisticated threats before they cause significant damage.

Real-World Example

Imagine an organization facing a targeted attack where an unknown threat actor deploys fileless malware via PowerShell scripts. The L2 team escalates the case because typical endpoint solutions fail to detect the malicious behavior. Here's how an L3 analyst intervenes:

1. **Collect Volatile Data**: Capture memory from an affected host and gather relevant PowerShell logs.
2. **Memory Analysis**: Use Volatility to spot suspicious code running under the powershell.exe process.

3. **Reverse Engineering**: Extract the memory-resident script and analyze it in a sandbox to pinpoint obfuscation and data exfiltration commands.
4. **Threat Hunting**: Search across the environment for similar PowerShell command patterns or the same malicious script block.
5. **Policy Update**: Propose restricting PowerShell usage to only signed scripts or implementing Constrained Language Mode for non-administrative users.
6. **Long-Term Strategy**: Recommend additional EDR capabilities that can monitor script usage in real time and block known malicious patterns.

This intervention not only resolves the immediate threat but also reduces the risk of future fileless attacks, showcasing the importance of L3 expertise in advanced forensics and overarching security strategy.

3. Practical Scenario Examples

Chapter 3 delves into realistic incident scenarios that illustrate how SOC teams operate under pressure, from the first moment an alert is triggered to the final stage of forensic analysis. The theory behind L1, L2, and L3 roles can feel abstract until it is grounded in actual events that demand swift action and collaboration. When facing phishing campaigns, ransomware attacks, or insider threats, every analyst's decision can significantly alter the outcome. This is why scenario-driven training and documentation are invaluable: they bridge the gap between textbook knowledge and day-to-day incident response.

In the sections that follow, you will see how each scenario unravels and how L1, L2, and L3 analysts coordinate their efforts. By observing concrete actions taken at every level, you can better understand not only the technical steps—such as analyzing phishing emails, quarantining malicious attachments, or performing forensic imaging—but also the strategic thinking that underpins each move. Monitoring dashboards, SIEM alerts, and endpoint logs might all point to suspicious activity, but it is the coordinated workflow across L1, L2, and L3 that ensures threats are identified, contained, and investigated properly.

The upcoming scenarios are designed to cover a wide range of common attack vectors:

- **Phishing Attack with Malware**: Showcasing how a single malicious email can serve as the gateway to data compromise and how deeper analysis can reveal hidden payloads.
- **Ransomware Outbreak**: Illustrating the critical need for rapid containment and cross-team communication when widespread encryption cripples an organization's infrastructure.
- **Insider Threat**: Highlighting the complexity of identifying abnormal behavior from privileged users and the investigative steps that go beyond simple log reviews.

Each scenario references industry-standard frameworks—such as MITRE ATT&CK for mapping adversary tactics and techniques, or guidelines from NIST Special Publication 800-61 on computer security incident handling—to ensure alignment with recognized best practices. Where relevant, analysts might use commands like curl -I http://suspicious-url.com to inspect response headers during phishing triage or rely on memory analysis tools like Volatility in insider threat investigations. Tools and approaches will vary, but the essential point is that every role in the SOC—L1, L2, and L3—contributes specialized expertise at different phases of an investigation.

Practical examples are not just about replication of steps; they help cultivate the analytical mindset needed to anticipate attacker behavior and adapt defensive strategies. Whether you are new to the field or already have some experience, these real-life scenarios will demonstrate how theoretical duties translate into hands-on procedures and decisions. By walking through each case study, you will gain clarity on why L1 focuses on quick response and basic triage, how L2 digs deeper for correlations and patterns, and how L3 brings advanced forensics and strategic oversight to the table.

3.1 Phishing Attack with Malware

In many organizations, phishing remains the most common and effective vector for delivering malware. Attackers craft emails or messages that appear to come from trusted sources,

enticing users to click a malicious link or open an infected attachment. Once a user interacts with the email, malware can be silently installed, potentially allowing the attacker to pivot inside the network. In this section, we examine how each Security Operations Center (SOC) tier—L1, L2, and L3—plays a role in managing a phishing incident that includes malware delivery.

L1: Detecting a Suspicious Email and Basic Triage

Typical Workflow and Responsibilities:

- **Monitoring Alerts and User Reports:** L1 analysts keep an eye on SIEM dashboards, spam filter alerts, and inbox traffic patterns. They often serve as the first point of contact when employees report suspicious emails.
- **Initial Investigation:** They gather basic information—such as the sender's address, email subject, and any suspicious links. L1 also checks against known phishing campaigns or newly discovered indicators of compromise (IOCs).
- **Basic Triage and Escalation:** If the email is identified as potentially malicious, L1 analysts escalate the incident to L2. This involves attaching relevant data (IP addresses, URLs, attachment hashes) for the next level's deeper investigation.

Example in Practice:

- An employee forwards an email with the subject line: *"Urgent: Invoice Overdue!"* to the SOC's mailbox.
- The L1 analyst inspects the sender domain, noticing a slight misspelling (e.g., @myco-accouts.com instead of @myco-accounts.com).
- After a quick review, the L1 analyst checks the attachment's hash against a threat intelligence database (e.g., VirusTotal). If the file is flagged, the analyst immediately tags the alert as *High Priority* and escalates.

Sample Command (Hash Check):

```
curl --request POST \
     --url https://www.virustotal.com/api/v3/files/<file_hash> \
     --header 'x-apikey: <API_KEY>'
```

(This is a simplified example; in many cases, this lookup happens automatically through SOC tooling rather than a raw API call.)

L2: Deep Analysis of Malicious Attachments

Core Activities:

- **Malware Analysis and Sandbox Testing:** L2 analysts examine suspicious attachments in a secure environment (sandbox). They observe file behavior, registry changes, processes spawned, and outbound connections.
- **Correlation of Additional Indicators:** By checking SIEM logs, endpoint detection solutions, and firewall data, L2 analysts attempt to see if this malware has affected other systems or if similar emails were sent to additional employees.

- **Coordinating with Incident Response Procedures:** Based on the findings, L2 analysts may trigger an official incident response playbook, working closely with IT teams to isolate infected systems or block known malicious IP addresses at the firewall.

Detailed Steps:

- The L2 analyst opens a sandbox environment (e.g., Cuckoo Sandbox) and uploads the suspicious attachment.
- The sandbox analysis reveals the file attempts to download an executable from a malicious URL or modifies certain registry keys associated with persistence.
- L2 searches the organization's endpoint logs to see if any hosts have called out to the same IP or domain. This correlation might uncover additional compromised machines.

Technical Example (Sandbox Analysis Output):

```
Threat Indicators:

- Suspicious network traffic to hxxp://malicious-example-
domain[.]com

- Creation of autorun key
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\malware.exe

- Dropping of secondary payload in
C:\Users\<User>\AppData\Roaming\malware.exe
```

After confirming these indicators, L2 updates the internal threat intelligence platform (e.g., MISP) with new IOCs—such as domains, IP addresses, file hashes—and coordinates any immediate containment measures like blocking the domain at the proxy level.

L3: Advanced Malware Forensics and Threat Hunting

Primary Objectives:

1. **Reverse Engineering and In-Depth Analysis:** L3 analysts perform full static and dynamic analysis on the malware sample, potentially deobfuscating code and extracting embedded configuration details (e.g., C2 server addresses).
2. **Threat Hunting Across the Enterprise:** Using EDR (Endpoint Detection and Response) tools or log analysis, L3 analysts search for traces of the same malware family or TTPs (Tactics, Techniques, and Procedures) that might indicate a broader compromise.
3. **Policy Updates and Strategic Countermeasures:** L3 reviews policies, email filtering configurations, and user training strategies to strengthen defenses. They might also recommend deploying new detection rules or Yara signatures to proactively catch similar threats.

In-Depth Reverse Engineering Example (Using a Disassembler):

```
1. Disassemble the binary with IDA Pro or Ghidra.

2. Inspect key functions calling Win32 APIs like "InternetOpenUrl"
or "CreateProcessA".
```

```
3. Identify encoded strings that reveal remote hosts or command-and-control infrastructure.

4. Extract embedded resources to see if there are hidden modules or secondary payloads.
```

This deeper analysis can help the SOC (and potentially law enforcement or other external parties) attribute the campaign to a known threat actor. It also informs the security architecture team about how to fine-tune detection signatures. For instance, L3 might create a custom Yara rule to detect the unique strings or file characteristics of this malware:

```
rule Malware_Phishing_Sample {

    meta:

        description = "Detects malicious attachments commonly used in phishing"

        author = "L3 SOC Analyst"

    strings:

        $a = "InternetOpenUrlA" nocase

        $b = "CreateProcessA" nocase

        $c = { 68 ?? ?? ?? ?? 8B ?? 55 ?? }

    condition:

        all of them

}
```

Threat Hunting Beyond the Initial Attack:

- L3 analysts pivot on newly discovered IOCs (domains, IP addresses, file hashes) across the enterprise environment using SIEM queries.
- If additional compromised endpoints are discovered, L3 communicates remediation steps to the Incident Response team, ensuring those endpoints are contained and cleaned.
- Patterns found during hunting (e.g., consistent registry modifications) might indicate advanced persistent threats or multiple infection attempts, leading to further investigation.

Collaborative Effort Across the Three Levels

Below is a simplified table showing key tasks associated with each level during a phishing-with-malware scenario:

Role	Key Tasks	Tools & Methods
L1	Identify suspicious emails, gather basic data, escalate	SIEM, ticketing system, AV logs

Role	Key Tasks	Tools & Methods
L2	Conduct deep file and behavioral analysis, correlate IOCs	Sandbox environments, EDR, threat intelligence feeds
L3	Perform reverse engineering, threat hunting, develop countermeasures	Disassemblers, Yara rules, enterprise-wide search

Though each level has distinct responsibilities, seamless communication and well-defined processes ensure rapid detection, thorough analysis, and effective remediation. In more sophisticated phishing campaigns—especially those using advanced social engineering and zero-day exploits—this multi-tiered approach is crucial for minimizing damage and preventing future attacks.

3.2 Ransomware Outbreak

Ransomware is a form of malware that encrypts files on a victim's system and demands payment (often in cryptocurrency) for the decryption key. Beyond causing direct financial damage, these attacks can severely disrupt regular business operations by locking critical data or systems. In many organizations, an outbreak will trigger a rapid, cross-functional response from the Security Operations Center (SOC). Below is a breakdown of how each SOC tier typically addresses a ransomware incident, including real-world perspectives and practical examples.

L1: Identifying Mass File Encryption and Escalating Alerts

Primary Detection and Alert Handling

- **Alert Monitoring**: The first clue might be a sudden spike in file I/O operations or security software notifications highlighting file modifications. Some next-generation antivirus (NGAV) solutions, such as Microsoft Defender or CrowdStrike, can flag anomalous activity when large numbers of files are encrypted in quick succession.
- **Basic Triage**: L1 analysts confirm whether these alerts are genuine. They look for patterns like unknown processes (e.g., encrypt.exe) or suspicious command-line executions that rename or delete file backups (for instance, using vssadmin commands to remove Volume Shadow Copies).

An example PowerShell command that might appear suspicious:

```
vssadmin delete shadows /all /quiet
```

This command deletes all Volume Shadow Copies, a known tactic used by many ransomware variants to prevent easy file recovery.

- **Gathering Initial Context**: L1 analysts review the user reports or any help desk tickets that come in with descriptions of locked files or pop-up ransom notes. They also verify which endpoints are affected and check whether multiple users are reporting similar symptoms.

Escalation Criteria

- High number of systems involved.

- Detection of known ransomware signatures in antivirus or EDR tools.
- Presence of a ransom note on the affected machines.

Once L1 sees a pattern indicating a large-scale encryption event rather than a false positive, they escalate to L2.

L2: Coordinating Incident Response and Containment

Deep Investigation and Scope Determination

- **Log Correlation**: L2 analysts collect logs from various sources—endpoint detection and response (EDR) platforms, firewalls, file servers—and correlate timestamps to pinpoint when the malicious activity started. They often use a SIEM (Security Information and Event Management) solution like Splunk, IBM QRadar, or the Elastic Stack to perform queries such as:

  ```
  index=endpoint sourcetype=edr process="*encrypt*" OR
  process="*ransom*"
  ```

  These queries help identify how many hosts have run suspicious processes.
- **Containment Measures**: L2 usually takes steps to limit the damage. This can include:
  - **Isolating Infected Machines**: Temporarily removing them from the network to prevent lateral movement. For instance, using an EDR console to isolate a host might involve a command like "Network Contain" or "Host Isolation."
  - **Blocking Threat Indicators**: If the ransomware communicates with a command-and-control (C2) server, L2 analysts might push firewall rules or modify proxy settings to block known malicious IPs or domains.
- **Communication and Coordination**: L2 often leads the internal incident response team, scheduling priority calls or coordinating chat channels where IT teams, management, and security staff can collaborate. They compile findings to ensure everyone understands the nature and severity of the outbreak.

Forensic Clues and Analysis

- **Entry Point Identification**: By looking at system event logs, L2 might discover that the ransomware was introduced via a phishing email that tricked a user into enabling macros in a malicious spreadsheet. Alternatively, an unpatched server could have been exploited as an initial foothold.
- **Malware Family Classification**: L2 analysts map the ransomware signature to known families such as Ryuk, LockBit, or WannaCry. Public resources like VirusTotal and CISA Alerts can assist in identifying the malware strain.

L3: Root Cause Analysis and Enterprise-Wide Mitigation Strategy

Advanced Threat Research and Recovery

- **Malware Reverse Engineering**: L3 analysts often deconstruct the malicious file using tools like REMnux or IDA Pro to see how the ransomware executes, what persistence

methods it might employ, and whether it has worm-like capabilities. This helps in creating specific detection rules (e.g., YARA rules) for future prevention.

- **Root Cause Analysis**: While L2 might have contained the immediate spread, L3 focuses on how the attackers entered the environment in the first place. If an unpatched RDP server was compromised, L3 will recommend disabling direct RDP access or enforcing multi-factor authentication (MFA).
- **Incident Post-Mortem**: L3 analysts conduct a detailed review of the entire incident workflow:
    - **Timeline Reconstruction**: Pin down the exact moment of infection, lateral movement steps, and escalation points.
    - **Gaps in Security Controls**: Identify which controls failed or were absent (e.g., missing patches, weak email filtering, insufficient network segmentation).
    - **Policy and Procedure Updates**: Recommend improvements to patch management, user awareness training, backup strategies, and logging capabilities.

Developing Future Safeguards

- **Long-Term Eradication**: L3 ensures compromised credentials are reset, all malicious binaries are removed, and any persistence mechanisms are neutralized. Tools like Volatility help analyze memory dumps for malicious processes that could have lingered.
- **Strategic Recommendations**: This may include segmenting critical servers from the rest of the corporate network, enforcing least privilege, and testing the organization's disaster recovery plan more frequently. Sometimes, L3 also leads the development of custom scripts or processes to automate detection and containment of similar threats in the future.

Example Comparison Table of Responsibilities

Activity	L1	L2	L3
Alert Identification	Monitors SIEM/EDR alerts for ransomware	Validates alerts and correlates across multiple systems	Oversees advanced threat detection strategies
Basic Triage	Checks for false positives or duplicates	Confirms impact and scope of the outbreak	Informs on the latest TTPs to refine triage steps
Isolation and Containment	Assists in isolating single endpoints	Coordinates mass isolation efforts across infrastructure	Advises on enterprise-wide quarantine protocols
Investigation & Analysis	Collects initial logs and user feedback	Correlates data, identifies the threat family	Conducts reverse engineering, hunts for hidden indicators

Activity	L1	L2	L3
Remediation	Supports re-imaging of infected hosts	Deploys remediation scripts and updates endpoint policies	Designs strategic fixes, updates incident response and security policies

By understanding how each SOC tier responds during a ransomware outbreak, teams can orchestrate a swift containment and limit the disruption to business operations. Each level plays a complementary role: L1 quickly identifies and escalates, L2 thoroughly investigates and coordinates, and L3 ensures a comprehensive eradication plan and strengthened policies to guard against future attacks.

3.3 Insider Threat

Insider threats remain one of the most complex challenges within any organization. They can originate from disgruntled employees, well-intentioned staff who make mistakes, or malicious actors who have established insider access through compromised credentials. Detecting and mitigating insider threats requires continuous monitoring of user behavior, in-depth investigation of anomalies, and sophisticated digital forensics capabilities. Below is a closer look at how L1, L2, and L3 analysts handle these scenarios in a Security Operations Center (SOC).

L1: Monitoring Unusual User Activity

Primary Focus

L1 analysts act as the first line of defense against potential insider threats by monitoring security dashboards, alert queues, and system logs. Their role involves identifying deviations in user behavior, such as unexpected login times, abnormal data transfers, or suspicious account usage.

Typical Tasks

1. **Alert Verification**: L1 analysts receive alerts from automated systems that flag out-of-norm user actions. For example, a data loss prevention (DLP) system might generate an alert if sensitive files are attached to personal email accounts.
2. **Basic Triage**: Once an alert is triggered, L1 analysts review relevant information—user ID, source IP, time of activity—to decide whether the event is a genuine threat or a false positive.
3. **Initial Documentation**: L1 analysts document the suspected insider threat incident, adding context about the user's department or role if known.
4. **Escalation**: If the indicator seems serious—like unauthorized access to critical systems—L1 escalates to L2 with supporting evidence.

Example in Practice

An L1 analyst notices an unusually large file transfer via a secure file transfer protocol (SFTP) going to an external IP address. The security platform's user behavior analytics (UBA) module raises an alert due to the volume of data sent. The analyst quickly reviews the user's recent login history and sees multiple late-night sessions. This anomaly is outside the employee's normal

work hours and job function, so the analyst escalates the alert with screenshots from the monitoring console and relevant log entries.

Relevant Tools and Commands

- **Splunk Query Example**:

  ```
  index=main source="windows:event:security" user="<username>"
  | stats count by EventCode
  | where count > 50
  ```

  This query could help identify a user generating an unusual number of login events or permission changes within a short timeframe.

- **DLP Solutions**: McAfee DLP, Forcepoint DLP, or Symantec DLP for policy-based alerts regarding sensitive data movement.

L2: Investigating Privileged Account Misuse

Primary Focus
L2 analysts handle detailed investigations into potential insider threats. When L1 flags a suspicious user action, L2 correlates logs from multiple sources to see if there is a broader pattern of misuse, particularly involving privileged or administrative accounts.

Key Activities

1. **Contextual Analysis**: L2 analysts combine endpoint logs, network traffic, and identity management alerts to reconstruct the user's actions and timeline. They look for sequences of events—such as privilege escalation followed by data exfiltration.
2. **Deep Dive into Access Controls**: Investigations often involve checking Active Directory (AD) logs or cloud IAM (Identity and Access Management) reports to see if the user's role-based access was changed or abused.
3. **Collaboration with HR and Legal**: In the case of a serious insider threat, L2 may coordinate with human resources and legal teams to gather background information on the user's role, performance issues, or any history of policy violations.
4. **Evidence Collection**: L2 analysts ensure logs are preserved in a forensically sound manner, labeling them with timestamps and user details for further analysis by L3 or legal teams.

Real-Life Example
A L2 analyst investigates an engineer who accessed a Git repository containing proprietary code outside normal business hours. By correlating firewall logs, the analyst notices connections to the repository from a personal VPN service. Cross-referencing HR data reveals the engineer has recently accepted a position at a competitor. This pattern indicates possible data exfiltration, prompting a deeper investigation and swift escalation to L3.

Useful Tools

- **SIEM Correlation Rules**: Correlate suspicious AD logins with file share access logs and identity management alerts.

- **PowerShell for Windows Event Log Review**:

```
Get-WinEvent -LogName Security |
  Where-Object { $_.Id -eq 4624 -and $_.Properties[5].Value -
eq "Domain Admins" }
```

  This helps identify logins tied to privileged groups like Domain Admins.

- **Incident Tracking Platforms**: ServiceNow, Jira, or TheHive allow structured workflows for insider threat investigations.

L3: Digital Forensics, Policy Review, and Improvements

Primary Focus

When an insider threat escalates to L3, it usually involves confirmed misuse of privileged accounts or large-scale data exfiltration. L3 analysts are responsible for performing advanced forensics on compromised systems, reviewing and refining security policies, and implementing measures to prevent future incidents.

Critical Responsibilities

1. **In-Depth Digital Forensics**: L3 analysts collect and analyze disk images, memory dumps, and network packet captures. For instance, they might use tools like EnCase or Autopsy to identify hidden files, track data transfers, and uncover attempts to delete or obfuscate activity.
2. **Threat Hunting**: Using Indicators of Compromise (IoCs) derived from the forensic investigation, L3 analysts proactively search across the enterprise environment to uncover additional systems or accounts that may be compromised by the same insider or associated threat actor.
3. **Policy and Procedure Updates**: If a gap in access control or a lapse in monitoring enabled the insider threat, L3 analysts recommend updates to security policies, such as stricter access review cycles or better endpoint logging configurations.
4. **Technical Remediation and Strategic Guidance**: Working closely with management, L3 analysts propose steps to fortify the environment: implementing Just-In-Time (JIT) privilege for critical systems, adding multi-factor authentication (MFA) for high-risk roles, or creating new detection rules in the SIEM.

Practical Example

A manufacturing company discovers that a senior engineer downloaded a large number of proprietary design documents. L3 analysts perform a forensic image of the engineer's workstation, retrieve deleted files, and confirm the use of encrypted external media. They also review the network traffic logs for suspicious outbound connections. With these findings, the SOC team updates policies by limiting access to design documents, enforcing geoblocking, and requiring encryption keys to be stored in a secure vault.

Comparing Roles for Insider Threats

Below is a brief comparison of how L1, L2, and L3 analysts each contribute to handling insider threats:

Role	Typical Actions	Tools/Techniques	Outcome
L1	- Monitor dashboards - Basic triage - Escalate alerts	- SIEM dashboards - Basic log analysis	Quick detection of anomalies; ensures potential insider threats are not overlooked
L2	- Correlate multiple data sources - Investigate privileged misuse - Collaborate with HR/Legal	- SIEM correlation rules - AD reports - Incident tracking platforms	Deep dive investigations to confirm an insider threat and gather evidence
L3	- Perform full forensics - Update policies - Implement advanced threat hunting	- Forensic imaging tools - Threat hunting frameworks - Policy revision	Thorough root-cause analysis; strategic changes to prevent similar incidents

Insider threats often demand collaboration across multiple departments, not just different SOC tiers. By combining L1's vigilant monitoring, L2's investigative rigor, and L3's deep forensics and strategic oversight, organizations stand a better chance of uncovering and mitigating insider risks before they escalate into major incidents.

4. Conclusion

4.1 Summary of Role Interdependence

In a well-structured SOC, the L1, L2, and L3 roles function like interlocking gears. Each level depends on the accuracy, thoroughness, and timeliness of the others. When an L1 analyst flags suspicious indicators—perhaps a repetitive login failure or an unusual process spawning on multiple endpoints—L2 picks up the initial triage data and builds a more in-depth picture. This deeper analysis often involves correlating information from SIEM tools, threat intelligence feeds, and even raw network captures. L2 must trust that L1's preliminary checks are solid, because any gap or oversight at the first level can undermine more complex incident investigations.

Once a case escalates to L3, the potential scope grows larger. L3 teams operate at a level of advanced forensic analysis and threat hunting that can be decisive in understanding not just the immediate compromise, but also the adversary's motivations and potential pivot techniques. For example, during a ransomware outbreak, if L2 analysts identify indicators of compromise (IoCs) and notice that the threat spreads through a Windows service vulnerability, the L3 team might replicate the scenario in a controlled environment. They could run detailed memory forensics using tools like **Volatility** or **Rekall**, dissect malicious binaries with **Ghidra**, and trace lateral movement patterns. This advanced insight then feeds back into L2's standard operating procedures and L1's alert logic, creating a continuous feedback loop of improvement.

Here is a simplified diagram showing the interaction:

Level	Primary Focus	Key Tools	Dependencies
L1	Alert Monitoring, Basic Triage	SIEM Dashboards, Ticketing Systems	Relies on L2 escalation paths
L2	In-Depth Investigation	Correlation Engines, Threat Feeds, Sandbox Environments	Relies on L1 data, L3 guidance
L3	Advanced Forensics, Strategy	Memory Forensics, Malware Analysis Frameworks, Policy Setting	Relies on L1 and L2 findings as input

In practice, the synergy among these levels ensures that even if an adversary tries to bypass standard controls, each line of defense has the awareness and capability to catch the threat at some point along the kill chain.

4.2 Importance of Continuous Training and Collaboration

Cybersecurity threats evolve at a rapid pace, making ongoing learning essential. L1 analysts need periodic refreshers on new SIEM functionalities, updated correlation rules, and the latest common attack vectors. A typical training session might involve analyzing logs from a newly released worm to sharpen triage skills. L2 analysts benefit from deeper training in incident handling frameworks like **NIST SP 800-61** or **MITRE ATT&CK** tactics. These frameworks guide them in mapping detected threats to known adversarial tactics, techniques, and procedures (TTPs). L3 analysts often require specialized courses in reverse engineering or advanced digital forensics to stay proficient in dissecting sophisticated malware variants.

Collaboration within and across levels is the backbone of a resilient SOC. Regular tabletop exercises and cross-functional drills bring everyone onto the same page, showing how L1's alerting, L2's correlation efforts, and L3's investigative deep dives converge to form a cohesive defense. One illustrative example is a quarterly "purple team" exercise, where a red team simulates an attack and the blue team—comprising L1, L2, and L3—must detect, respond, and report in real time. This not only hones technical abilities but also fosters clear communication channels and an atmosphere of trust.

Below is a simplified example of how training objectives might be planned:

1. **L1 Focus**
    - Objective: Quick recognition of phishing emails with advanced evasion techniques.
    - Methods: Practice on curated sets of real-life phishing samples, combined with automated sandbox scans.
    - Expected Outcome: Faster response times and higher accuracy in initial triage.
2. **L2 Focus**
    - Objective: Enhanced skill in pivot analysis and event correlation.
    - Methods: Workshops on correlating endpoint detections with network flow data (e.g., using **Zeek** logs or **Suricata** alerts).
    - Expected Outcome: More accurate incident scoping and a reduced false-positive rate.
3. **L3 Focus**
    - Objective: Mastery of advanced malware dissection and memory forensics.
    - Methods: Deep dives into memory dump analysis, advanced debugging sessions in **WinDbg**, or code review of obfuscated malicious scripts.
    - Expected Outcome: Creation of refined detection signatures and proactive threat hunting strategies.

As these examples show, continuous learning and structured collaboration translate directly into stronger security postures. By sharing experiences and refining processes, each level not only improves its own efficacy but also bolsters the capabilities of the entire team. This comprehensive approach ensures that when new threats emerge, the SOC is ready to respond collectively, minimizing damage and shortening recovery time.

Bibliography

- NIST Special Publication 800-61: Computer Security Incident Handling Guide - https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- MITRE ATT&CK Framework - https://attack.mitre.org
- CISA Ransomware Guidance - https://www.cisa.gov/stopransomware
- ISO/IEC 27001: Information Security Management Systems - https://www.iso.org/standard/54534.html
- Cyber Kill Chain (Lockheed Martin) - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- Splunk Documentation - https://docs.splunk.com
- Elastic Stack Documentation (Elasticsearch, Kibana) - https://www.elastic.co/guide
- IBM QRadar Documentation - https://www.ibm.com/docs/en/qradar
- CrowdStrike Falcon Platform Documentation - https://www.crowdstrike.com
- Microsoft Defender for Endpoint Documentation - https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint
- Cuckoo Sandbox Documentation - https://cuckoosandbox.org
- Volatility Framework Documentation - https://volatilityfoundation.org
- Ghidra Reverse Engineering Tool - https://ghidra-sre.org
- Wireshark Official Site - https://www.wireshark.org
- Zeek (formerly Bro) Network Security Monitor - https://zeek.org
- YARA Rules Framework - https://virustotal.github.io/yara/
- VirusTotal - https://www.virustotal.com
- AbuseIPDB: IP Threat Intelligence - https://www.abuseipdb.com
- MISP Threat Intelligence Platform - https://www.misp-project.org
- AlienVault Open Threat Exchange (OTX) - https://otx.alienvault.com
- FireEye Threat Research - https://www.fireeye.com/current-threats.html
- SANS Digital Forensics and Incident Response - https://www.sans.org/digital-forensics-incident-response
- Microsoft Cybersecurity Reference Architectures - https://aka.ms/cybersecurityreferencearchitectures
- NCSC Incident Response and Management Guidelines - https://www.ncsc.gov.uk/collection/incident-management
- REMnux Linux Toolkit for Malware Analysis - https://remnux.org
- IDA Pro Disassembler - https://hex-rays.com/ida-pro/
- x64dbg Debugger - https://x64dbg.com
- Magnet Forensics Tools - https://www.magnetforensics.com
- Autopsy Digital Forensics - https://www.sleuthkit.org/autopsy
- Rekall Memory Forensics - https://github.com/google/rekall
- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- OWASP Top Ten Security Risks - https://owasp.org/www-project-top-ten
- CIS Controls and Benchmarks - https://www.cisecurity.org/controls
- PhishMe (Cofense) Anti-Phishing Training - https://cofense.com/phishme
- KnowBe4 Security Awareness Training - https://www.knowbe4.com
- GIAC Certified Incident Handler (GCIH) - https://www.giac.org/certifications/incident-handler-gcih/
- Certified Information Systems Security Professional (CISSP) - https://www.isc2.org/certifications/CISSP

- GIAC Reverse Engineering Malware (GREM) - https://www.giac.org/certifications/reverse-engineering-malware-grem/
- Insider Threat Program Best Practices (CERT) - https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636261
- Data Loss Prevention Guidelines (DLP) - https://www.forcepoint.com/data-loss-prevention
- McAfee DLP Resources - https://www.mcafee.com/enterprise/en-us/solutions/data-loss-prevention.html
- Purple Team Exercises (Attack/Defend) - https://www.redcanary.com/blog/purple-team-exercises/
- Living-off-the-Land Binaries (LOLBins) - https://lolbas-project.github.io
- Cyber Threat Hunting Playbooks (CrowdStrike) - https://www.crowdstrike.com/resources/threat-hunting-playbook/