SOC L1 Alert Triage:

Knowing how to handle it properly ultimately decides whether a security breach is detected and prevented, or missed and devastating.

First, an **event** must occur, like user login, process launch, or file download. Then, the system, like your OS, a firewall, or a cloud provider must **log the event.** After that, all **system logs must be shipped to a security solution** like **SIEM or EDR.**

Alert, a **notification** generated by a **security solution** when a specific event or sequence of events occurs, is what saves **SOC analysts from manual log review.**

With alerts, analysts triage just dozens of alerts per day instead of **millions of raw logs.**

While EDR and NDR provide their own alert dashboards, **it is preferred to use SIEM or SOAR**

SOAR (Security Orchestration, Automation, and Response)
Bigger SOC teams can use SOAR to aggregate and centralise alerts from multiple solutions

ITSM = Information Technology Service Management , refers to managing IT services, incidents, and workflows.

Alert Properties:

1. **Alert Time**
   When the alert was created.
   The system usually generates the alert a few minutes *after* the real event.

2. **Alert Name**
   A short title that tells you what the alert is about.
   Example: “Unusual Login Location”, “RDP Bruteforce”.

3. **Alert Severity**
   How urgent or dangerous the alert is.
   Low → Medium → High → Critical.

4. **Alert Status**
   Shows whether anyone is working on the alert.
   New → In Progress → Resolved.

5. **Alert Verdict**
   The analyst's final decision on the alert.
   True Positive = real threat.
   False Positive = harmless/no threat.

6. **Alert Assignee**
   The analyst responsible for investigating that alert.

7. **Alert Description**
   A text explanation that tells you:
   Tells you *why the rule triggered*, *why it may be suspicious*, and sometimes *how to investigate it*.

   – Human-readable guidance.

8. **Alert Fields**
   The technical details that triggered the alert.
   Examples: hostname, username, command line, IP address, file hash.

   The technical data. Shows the *exact values* that triggered the alert (IP, hostname, command line, username, etc.). Machine-generated event details.

Alert Prioritisation:

The process of deciding which to take is called **Alert Prioritisation**, and it is crucial to ensure timely detection of a threat, especially with many alerts in the queue.

Every SOC team decides on its own prioritisation rules and usually automates them by setting the appropriate alert sorting logic in SIEM or EDR

Most Commonly Used Approach for Handling Alerts

1. **Filter the Alerts**
    - Only take alerts that are **new, unseen, and unresolved**.
    - Avoid alerts that other analysts have **already reviewed** or that are **currently being investigated by a teammate.**
2. **Sort by Severity**
    - Prioritize alerts in this order: **Critical** → **High** → **Medium** → **Low**.
    - Critical alerts are more likely to **indicate real, high-impact threats,** as **detection engineers design rules to reflect potential impact.**
3. **Sort by Time**
    - Review the **oldest alerts first**, then move to the newest.
    - Rationale: if **two alerts** relate to **breaches**, the **older breach may already be causing damage, while the newer one may just be starting.**

Note that the alert review by SOC analysts can also be called alert triage, alert handling, alert processing, alert investigation, or alert analysis.

The initial steps are designed to ensure that you take ownership of the assigned alert and avoid interfering with alerts being handled by other analysts, then familiarising yourself with the alert details like its name, description, and key indicators.

Investigation

apply your technical knowledge and experience to understand the activity and properly analyse its legitimacy in SIEM or EDR logs. some teams develop **Workbooks** (also known as playbooks or runbooks) - instructions on how to investigate the specific category of alerts.

Key Recommendations Without Workbooks

1. Identify the **target** (user, host, network, cloud, or website).
2. Note the **action described in the alert** (suspicious login, malware, phishing).
3. Check **surrounding events shortly after or before the alert** for related suspicious activity.
4. Use **threat intelligence** to verify and support your findings.

Final Actions:

First, decide if the alert you investigated is **malicious (True Positive) or not (False Positive).** Then, prepare your **detailed comment** explaining your analysis steps and verdict reasoning, return to the dashboard and move it to the **Closed** status.

Severity takes precedence over time because high-severity alerts are more likely to indicate a real, impactful threat.
Time is used as a secondary factor **within the same severity level**.

SOC L1 Alert Reporting:

L1 analysts may be uncertain about how to classify the alert, requiring senior support or information from the system owner.
Most of the alerts are closed as False Positives or are handled on L1 level, but complex and threatening ones are sent to L2 that remediate most breaches.

And to send the alerts further, you need to learn three new terms: reporting, escalation, and communication.

Alert Reporting:

Before closing or passing the alert to L2, **you might have to report it** . you can be required to document your **investigation in detail, ensuring all relevant evidence is included.**This is especially important for **True Positives, which require escalation.**

Alert Escalation:

That's where your alert report comes in handy since **L2 will use it to get the initial context and spend less on the analysis from scratch.**

Communication:

You may also need to communicate **with other departments during or after the analysis.** For example, ask the IT team if they confirm granting administrative privileges to some users or contact HR to get more information about the newly hired employee.

Reporting Guide:

It is essential to clarify why anyone would want L1 analysts to write reports in addition to marking them as True or False Positives and why this topic can not be underestimated. Having L1 analysts write alert reports serves several key purposes:

Purpose of an Alert Report

1. **Provide Context for Escalation**
    - **Helps L2 analysts** quickly understand the situation and saves time during escalation.
2. **Save Findings for Records**
    - Raw SIEM logs are temporary (3–12 months), but **alerts are stored indefinitely;** keeping **context in the report ensures** information is preserved.
3. **Improve Investigation Skills**

- **Writing clear reports reinforces understanding** and helps L1 analysts **strengthen their skills by summarizing alerts effectively.**

Five Ws Approach for an Alert Report

1. **Who** – *Who performed the action?*
    - Example: `User: john.doe@example.com`
2. **What** – *What exactly happened?*
    - Example: `Downloaded a suspicious executable file from GitHub and ran it`
3. **When** – *When did the activity occur?*
    - Example: `Start: Mar 21, 2025, 13:02 | End: Mar 21, 2025, 13:05`
4. **Where** – *Which system or network was involved?*
    - Example: `Host: JD-Laptop-01 | IP: 192.168.1.45`
5. **Why** – *Reasoning behind your verdict (most important)*
    - Example: `The file matches known malware hash and triggered endpoint protection → Verdict: True Positive`

SPF (Sender Policy Framework)

- Checks if the sending **mail server is allowed** to send emails for a domain.

- Think: **“Is this server allowed to send emails on behalf of example.com?”**
- Works at the **server level**.

2. DKIM (DomainKeys Identified Mail)

- Adds a **digital signature** to the email.
- Ensures the **email was not altered** and really **came from the claimed domain.**
- Works at the **message/content level**.

3. DMARC (Domain-based Message Authentication, Reporting & Conformance)

- Uses **SPF + DKIM results** to decide what to do with emails that fail authentication.
- Policies: `none` (just report), `quarantine`, or `reject`.
- Provides **reports** back to the domain owner.

When to Escalate Alerts

1. The alert indicates a **major cyberattack** needing deeper investigation or DFIR.
2. **Remediation actions** are required (e.g., malware removal, host isolation, password reset).
3. **Communication** with customers, partners, management, or law enforcement is necessary.
4. You **do not fully understand** the alert and need guidance from senior analysts.

Once everything is clear, the L2 analyst will typically research the alert details further, validate if the alert is indeed a True Positive, communicate with other departments if needed, and, for major incidents, start a formal Incident Response process.

It is generally fine for L1 to request senior support if something is unclear. Especially in **your first months,** it's always better to discuss the alert and clarify SOC procedures than to blindly close the alert you don't understand yourself.

SOC Dashboard Escalation

1. Write an alert report and provide your verdict; move the alert to **In Progress** status
2. Assign the alert **to your L2** on shift. L2 will receive a notification and start from your report

SOC Crisis Communication

In an ideal scenario, the SOC team has Crisis Communication procedures.

1. **L2 Unavailable:**

If an urgent alert cannot be escalated, follow the chain of emergency contacts: L2 → L3 → Manager.

2. **Compromised User Accounts:**

Validate with the user via alternative methods (e.g., phone), not through the breached chat.

3. **High Alert Volume:**

Prioritize alerts using the workflow and inform L2 about the situation.

4. **Misclassified Alerts:**

If an alert was likely misclassified earlier by you , immediately notify L2 to prevent potential impact.

5. **Incomplete Triage due to SIEM Issues:**

Investigate what is possible and report the parsing/log issue to L2 or SOC engineer; **do not skip the alert.** Action: Investigate what you can and report the issue to your L2 or SOC engineer. Reason: **You should never skip an alert entirely, even if logs are incomplete.**

SOC Workbooks and Lookups:

Identity inventory gives context about **who** is doing what, when, and why, which helps you decide whether the **alert is normal or suspicious.**

A **catalogue of all users and system accounts**, including:

1. **User accounts** (employees)
2. **Machine accounts** (servers, services)
3. **Details**: privileges, roles, contact info, and department

Purpose:
Helps analysts **quickly check if a user or access is legitimate**.

Example in scenario: Using the inventory, you can see that G.Baker is a finance analyst and R.Lund is a manager who is allowed to access financial reports.

Asset Inventory

Definition:

- A list of all **computing resources** (servers, workstations) in an organization.
- Focus here is on **hardware assets** like PCs and servers, **not software or employees.**

Purpose:

- Provides context about a system when investigating alerts.
- Example: Helps understand the **HQ-FINFS-02 server** in your alert scenario.

Why Network Diagrams Matter:

- Show **connections between subnets, servers, and services**.

- Help **visualize attack paths** and spot unusual activity.
- Map internal IPs to **subnets** using **asset inventory.**

- Understand why traffic to certain subnets may be suspicious.

✅ **In short:** The network diagram allows SOC analysts to **reconstruct the attack path** and understand the threat actor's moves inside the network

Workbooks Theory:

Some alerts are simple, but complex alerts may require many steps to avoid missing critical details

By using **playbooks, inventories, network diagrams, and proper documentation**, you ensure a thorough and repeatable alert analysis process.

SOC workbook, also called **playbook, runbook, or workflow**, is a structured document that defines the **steps required to investigate and remediate specific threats efficiently and consistently**. s**enior analysts often prepare workbooks** to support their less experienced teammates

L1 analysts are recommended and sometimes even required to triage the alerts precisely according to workbooks to avoid mistakes and streamline the analysis.

Typical Workflow:

1. **Enrichment:**
    - Check **identity inventory** and **threat intelligence** to gather info about the user and login source.

2. **Investigation:**
    - Analyze SIEM logs and other data to determine if the login is **expected or suspicious**.
3. **Escalation:**
    - If suspicious: escalate to **L2** or contact the user for verification.
    - If normal: close the alert

SOC Metrics and Objectives

The main goal of a SOC is to protect an organization's digital assets by ensuring:

Confidentiality, Integrity, Availability (CIA).

Alerts Count (AC)

Formula:

```
AC = Total Alerts Received
```

What it measures:

- The workload of SOC analysts.
- 80 unresolved alerts in the queue → overwhelming, higher chance of missing real threats.
- 0 alerts for a week → suspicious; maybe your monitoring is broken or visibility is poor.

Target:

- ~5–30 alerts per day per L1 analyst (depends on company size).

Insight:

- Too many alerts = high stress, prone to mistakes.
- Too few alerts = possible undetected threats.

False Positive Rate (FPR)

Formula:

```
FPR = False Positives / Total Alerts
```

What it measures:

- The “noise” level in alerts.
- Out of 80 alerts, 75 are false positives → FPR = 75/80 = 94%.
- Analysts may become fatigued and treat all alerts as spam → dangerous.

Target:

- 0% is ideal but unrealistic.
- FPR > 80% → serious problem, usually fixed by tuning detection rules or SIEM.

Alert Escalation Rate (AER)

Formula:

```
AER = Escalated Alerts / Total Alerts
```

What it measures:

- How experienced and independent L1 analysts are.

Example:

- L1 escalates too many alerts → might not understand what's actionable.
- L1 escalates too few → might miss threats.

Target:

- Usually <50%, ideally <20%.

Insight:

- Balance is key: escalate real threats, filter out noise

Threat Detection Rate (TDR)

Formula:

```
TDR = Detected Threats / Total Threats
```

What it measures:

- How reliable the SOC team is at catching threats.

Example:

- 6 attacks occurred: SOC detected 4, missed 2 → TDR = 4/6 = 67% → BAD.

Target:

- 100% → every threat must be detected.

Insight:

- Missing threats can lead to severe consequences: ransomware, data loss, breaches.

Metric	Formula	Target / Insight
Alerts Count (AC)	Total Alerts	5–30 per analyst/day
False Positive Rate (FPR)	False Positives / Total Alerts	<80%, lower is better
Alert Escalation Rate(AER)	Escalated Alerts / Total Alerts	<50%, ideally <20%
Threat Detection Rate(TDR)	Detected Threats / Total Threats	

Triage Metrics:

An **alert by itself will not stop the breach**, and it is important to timely receive the alert, triage it, and respond to the attack before the attackers achieve their goals

The requirements to ensure a quick detection and remediation of the threat are commonly grouped into a **Service Level Agreement (SLA)** - a document signed between the internal SOC team and its company management, or by the managed SOC provider (MSSP) and its customers

🕵️ Mean Time to Detect (MTTD)

MTTD measures how long it takes the SOC to **detect a threat after it first occurs**. It begins the moment malicious activity starts on a system and ends when the security tool or monitoring system generates an alert.

A low MTTD means threats are spotted quickly, reducing the time attackers have to cause damage.

In simple terms, it shows how quickly your detection mechanisms and visibility tools, like SIEM or EDR, can recognize abnormal or harmful behavior.

Malware runs on host at 10:00 → Alert appears in SIEM at 10:10 → **MTTD = 10 min**

👩‍💻 Mean Time to Acknowledge (MTTA)

MTTA measures how long it takes an **L1 analyst to acknowledge or take ownership** of an alert after it appears in the SOC dashboard. It starts when the alert is generated and ends when an analyst begins investigating it or changes its status to “In Progress.”

Alert appears at 10:10 → Analyst picks it up at 10:15 → MTTA = 5 min

🧯 Mean Time to Respond (MTTR)

MTTR measures the time required to **contain, remediate, and recover** from a confirmed security incident. It begins once the alert has been acknowledged and continues until the issue is fully resolved

MTTR indicates how effectively the SOC and IT teams coordinate during incident response. A lower MTTR means the organization can control and eliminate threats rapidly, minimizing impact and downtime

Mttr: (MTTA + internal response)

In Simple Terms:

- **MTTD: How fast we *notice* the problem.**
- **MTTA: How fast we *react* to the alert.**
- **MTTR: How fast we *fix* the problem.**

First, you should understand that metrics **were built to make the SOC more efficient** and, therefore, to make the **attacks far less successful.**
Second, the metrics are often used t**o evaluate your performance, and good results lead** to career growth and a raise **to more senior positions like L2 analyst.**

Issues and remedy:

False Positive Rate
over 80% :

Exclude trusted activities from **detection rules**; use SOAR or **automation to handle common alerts.**

Mean Time to Detect (MTTD):

Optimize detection **rules for faster runs;** ensure **real-time log collection** in SIEM.

Mean Time to Acknowledge (MTTA):
Enable **instant alert notifications**; **balance alert load** among analysts.

Mean Time to Respond (MTTR):
Escalate threats promptly to L2; **maintain clear, documented response procedures.**