SOC LEVEL 1 ESSENTIALS – PART C: ALERTS AND INCIDENT HANDLING (POST 21-28)

From Alert to Action: Essential Practices for SOC Level 1 Analysts

JULY 16, 2025

INAAM KABBARA
Security Analyst | Cybersecurity Content Creator | EPITA MSc Graduate

Table of Contents

1- SOC Level 1 Responsibilities – A Day in the Life

What does a typical day look like for a SOC Level 1 Analyst?
As a Level 1 Analyst, you're the frontline defender—the eyes and ears of the security operations center. You play a vital role in the early detection and escalation of threats, ensuring rapid response to security incidents before they escalate.

🔎 Your daily routine often includes:
📊 Monitoring SIEM dashboards (e.g., ELK, Splunk, QRadar) for real-time alerts
🛑 Triage and prioritization of security events based on severity
🧩 Initial investigation to distinguish between false positives and real threats
🚨 Escalation of high-risk incidents to Level 2/3 teams
📝 Documenting every step taken in a ticketing system (e.g., ServiceNow, Jira)
🤝 Collaborating with IT teams for containment or verification

💡 Pro Tip: A strong L1 analyst doesn't just react—they look for context. Learn to read between the logs, correlate multiple alerts, and always ask why this alert matters.

❓ What part of the SOC workflow excites you the most—monitoring, triaging, or escalation?

Responsabilités d'un Analyste SOC Niveau 1 – Une Journée Type

En tant qu'analyste SOC de niveau 1, vous êtes le premier rempart de la cybersécurité. Vous assurez une détection rapide, une analyse initiale et une escalade efficace des incidents, jouant un rôle crucial dans la protection des systèmes d'information.

🔎 Vos missions quotidiennes incluent souvent :
📊 Surveillance des alertes via des outils SIEM (ELK, Splunk, QRadar, etc.)
🛑 Analyse et hiérarchisation des événements de sécurité
🧩 Première investigation pour distinguer les faux positifs des véritables menaces
🚨 Escalade des incidents critiques aux analystes N2/N3
📝 Documentation rigoureuse dans un outil de ticketing (ServiceNow, Jira…)
🤝 Collaboration avec les équipes IT pour valider ou contenir l'incident
💡 Astuce : Un bon analyste L1 ne se contente pas de réagir. Il cherche à comprendre le contexte, à corréler plusieurs sources et à questionner la pertinence de chaque alerte.

❓ Quelle partie du workflow SOC vous motive le plus : la surveillance, l'analyse ou l'escalade ?

SOC LEVEL 1 RESPONSIBILITIES
A DAY IN THE LIFE

WHAT DOES A TYPICAL DAY LOOK LIKE FOR A SOC LEVEL 1 ANALYST

- MONITORING SIEM DASHBOARDS (E.G., ELK, SPLUNK, QRADAR)
- TRIAGE AND PRIORITIZATION OF SECURITY EVENTS
- INITIAL INVESTIGATION TO DISTINGUISH BETWEEN FALPOITIVES AND REAL THREATS
- ESCALATION OF HIGH-RISK INCIDENTS TO LEVEL 2/3 TEAMS
- DOCUMENTING EVERY STEP TAKEN IN A TICKETING S-STEM (E.G., SERVICENO, JIRA)

INAAM

2- Incident Lifecycle According to NIST

Why is the incident lifecycle important for SOC operations?
NIST (National Institute of Standards and Technology) defines a standardized incident response lifecycle in its SP 800-61 publication. This lifecycle is crucial for SOC analysts because it ensures that every security incident is handled consistently, efficiently, and with proper documentation.

🔎 The 4 stages of the NIST incident lifecycle are:
1️⃣ Preparation – Establishing response tools, procedures, access, and training
2️⃣ Detection & Analysis – Identifying, validating, and analyzing suspicious activity
3️⃣ Containment, Eradication & Recovery – Isolating the threat, removing it, and restoring services
4️⃣ Post-Incident Activity – Lessons learned, reporting, documentation, and improving defenses

💡 Pro Tip: Even if you're L1, you must understand the entire lifecycle. You're most active in Detection & Analysis, but your reports and logs directly support the Containment and Post-Incident phases.

❓ Which stage do you think is most often underestimated—and why?

Cycle de Vie d’un Incident selon le NIST

Pourquoi le cycle de vie des incidents est-il essentiel dans un SOC ?
Le NIST (National Institute of Standards and Technology) définit un cycle de réponse aux incidents en 4 étapes dans sa publication SP 800-61. Ce cadre aide les analystes SOC à gérer les incidents de manière structurée, rapide et traçable.

🔎 Les 4 phases du cycle de vie selon le NIST sont :
1️⃣ Préparation – Mise en place des outils, procédures et formations
2️⃣ Détection & Analyse – Identification, validation et analyse des activités suspectes
3️⃣ Confinement, Éradication & Rétablissement – Isolement de la menace, suppression et restauration
4️⃣ Activités Post-Incident – Retour d'expérience, documentation et amélioration continue

💡 Astuce : Même si vous êtes analyste L1, il est essentiel de comprendre tout le cycle. Vous intervenez surtout dans la détection, mais votre travail impacte directement le traitement et les activités post-incident.

❓ Selon vous, quelle étape est la plus négligée dans un incident ?

INCIDENT LIFECYCLE ACCORDING TO NIST

PREPARATION

Establishing response tools, procedures, access, and training

DETECTION & ANALYSIS

Identifying, validating, and analyzing suspicious activity

CONTAINMENT, ERADICATION & RECOVERY

Isolating the threat, removing it, and restoring services

POST-INCIDENT ACTIVITY

Lessons learned, reporting, documentation, and improving defenses

INAAM

3- How to Triage an Alert Efficiently

Why is triage such a critical skill in a SOC?
In a real-world SOC, analysts face hundreds of alerts per day. Efficient triage helps determine what truly matters and ensures the right incidents are escalated quickly, avoiding alert fatigue and missed threats.

🔎 A structured triage approach includes:
1️⃣ Check severity & classification
➡️ Is it critical? Is it related to malware, access attempt, privilege escalation?
2️⃣ Correlate with other logs or alerts
➡️ Is this alert part of a larger pattern? Is there supporting evidence?
3️⃣ Validate context
➡️ Who is the user/IP? Is this behavior normal for this time, machine, or asset?
4️⃣ Decide on action
➡️ Escalate, close as false positive, or document for further investigation

💡 Pro Tip: Don't rush triage. A well-documented triage helps the whole SOC team. Always leave a trail that explains your reasoning.

❓ What's your go-to checklist when reviewing a new alert?

Comment Traiter une Alerte Efficacement

Pourquoi la capacité à trier les alertes est-elle si cruciale dans un SOC ?
Dans un SOC opérationnel, les analystes traitent des centaines d'alertes chaque jour. Une bonne gestion permet d'identifier les vraies menaces, d'éviter la fatigue liée aux alertes, et d'agir rapidement sur les incidents critiques.

🔎 Une approche structurée de triage comprend :
1. Vérifier la sévérité et le type
➡️ Est-ce critique ? Lié à un malware, une tentative d'accès, une élévation de privilèges ?
2. Corréler avec d'autres logs ou alertes
➡️ Cette alerte fait-elle partie d'un schéma plus large ? Y a-t-il des éléments qui confirment ?
3. Valider le contexte
➡️ Qui est l'utilisateur/l'IP ? Ce comportement est-il habituel à cette heure ou sur cette machine ?
4. Décider de l'action
➡️ Escalade, clôture comme faux positif, ou documentation pour suivi

💡 Astuce : Ne vous précipitez pas. Un triage bien documenté aide toute l'équipe SOC. Laissez toujours une trace claire de votre raisonnement.

❓ Quelle est votre checklist personnelle lors du tri d’une alerte ?

4- Escalation Process – When and Why It’s Needed

Why is escalation critical in a SOC?
Not every alert can or should be resolved by a Level 1 analyst. Escalation ensures that complex or high-impact threats are handed over to more experienced analysts (L2/L3), allowing timely and effective incident response.

🔎 Common reasons to escalate an alert:
🚨 The alert involves critical assets or sensitive data
🧠 You lack access, tools, or authorization to proceed
📚 The incident pattern is unclear or too complex
📈 There's evidence of lateral movement, malware persistence, or privilege escalation
🛠️ The incident requires containment actions beyond your permissions

💡 Pro Tip: Always include detailed notes, timestamps, and your analysis in the ticket before escalating. Escalation is not failure—it’s collaboration.

❓ What’s the most important detail to include when escalating an alert in your opinion?

Processus d’Escalade – Pourquoi et Quand C’est Nécessaire

Pourquoi l’escalade est-elle essentielle dans un SOC ?
Toutes les alertes ne peuvent pas (ou ne doivent pas) être traitées par un analyste L1. L’escalade permet de transférer les incidents critiques ou complexes aux niveaux supérieurs (L2/L3) pour une réponse rapide et appropriée.

🔎 Raisons fréquentes d’escalader une alerte :
🚨 L’alerte concerne des actifs critiques ou des données sensibles
🧠 Vous n’avez pas les accès, outils ou autorisations nécessaires
📚 Le schéma d’attaque est flou ou trop complexe
📈 Présence de mouvements latéraux, de malware persistant ou d’escalade de privilèges
🛠️ L’incident nécessite des actions de remédiation au-delà de vos droits

💡 Astuce : Avant d’escalader, documentez bien votre analyse, les timestamps, et les éléments observés. L’escalade n’est pas un échec — c’est du travail d’équipe.

❓ Quel élément est, selon vous, indispensable à inclure dans un ticket d’escalade ?

ESCALATION PROCESS WHEN AND WHY IT' NEEDED

The alert involves critical assets or sensitive data

You lack access, tools, or authorization to proceed

The incident pattern is unclear or too complex

There's evidence of lateral movement, malware persistence, or privilege escalation

The incident requires containment actions beyond your permissions

INAAM

5- How to Document an Incident Professionally

Why does documentation matter so much in SOC operations?
In a SOC, documentation isn't optional — it's critical. Every step you take must be traceable, reproducible, and understandable by other analysts or auditors. Your notes tell the story of the incident and guide future actions.

🔎 What should your incident documentation include?
🕒 Timestamps for detection, triage, escalation, and resolution
👤 Actors involved – Usernames, IPs, assets impacted
🔍 Actions taken – Investigation steps, queries used, alerts reviewed
📌 Decisions made – Why you escalated, closed, or took specific actions
🛠️ Response outcomes – Was it contained? What was remediated?

💡 Pro Tip: Use clear, structured sentences. Avoid jargon. Write as if the person reading has no context. Documentation may be reviewed weeks later—or during an audit.

❓ What template or structure do you follow when writing incident reports?

Comment Documenter un Incident de Manière Professionnelle

Pourquoi la documentation est-elle si importante dans un SOC ?
Dans un SOC, tout doit être documenté avec rigueur. Vos notes servent à reconstituer les faits, à guider les collègues et à fournir des preuves en cas d'audit ou d'investigation future.

🔎 Une documentation d'incident doit inclure :
🕒 Horodatages pour chaque étape (détection, analyse, escalade, résolution)
👤 Acteurs concernés – IPs, utilisateurs, machines affectées
🔍 Actions menées – Recherches effectuées, alertes analysées, outils utilisés
📌 Décisions prises – Raisons des choix faits (escalade, clôture, etc.)
🛠️ Résultats obtenus – Contention réussie ? Éléments remédiés ?

💡 Astuce : Soyez clair, précis et structuré. Rédigez comme si le lecteur n'a aucun contexte technique. Les rapports peuvent être relus longtemps après l'incident.

❓ Quel modèle ou format utilisez-vous pour vos rapports d'incidents ?


HOW TO DOCUMENT AN INCIDENT PROFESSIONALLY
CAPTURE DETAILS
DOCUMENT THOROUGHLY
MAINTAIN CONSISTENCY
ENSURE CLARITY
INAAM

6- Alert Fatigue – What It Is and How to Manage It

Why is alert fatigue a real risk in SOC environments?
SOC analysts face thousands of alerts daily, most of which are false positives. Over time, this volume can cause mental overload, reduce reaction time, and lead to dangerous oversight of real threats. This is known as alert fatigue.

🔎 Common causes of alert fatigue:
🔁 Too many repetitive false positives
⚙️ Poorly tuned detection rules or thresholds
💭 Lack of context behind alerts (no enrichment)
👥 Small team size or understaffed SOC
⏱️ Long hours on monitoring without rotation

🧠 How to manage it as a SOC L1:
🛠️ Fine-tune rules (with your team's help) to reduce noise
📚 Use enrichment sources (threat intel, asset context)
✅ Create suppression rules for benign events
🤝 Rotate duties across the team to reduce monotony
📝 Give feedback to improve SIEM logic continuously

💡 Pro Tip: Alert fatigue isn't just a personal issue—it's a system issue. Advocate for smarter automation and better triage workflows.

❓ Have you ever experienced alert fatigue? What helped you recover or stay sharp?

Fatigue face aux Alertes – Définition et Solutions

Pourquoi la fatigue face aux alertes est-elle un risque dans un SOC ?
Un analyste SOC peut recevoir des centaines d'alertes par jour, souvent des faux positifs. Ce flot constant finit par user l'attention, ralentir les réponses et parfois même laisser passer de vraies menaces : c'est la fatigue face aux alertes.

🔎 Causes fréquentes :
🔁 Trop de faux positifs répétés
⚙️ Règles de détection mal configurées
💭 Manque de contexte (alertes non enrichies)
👥 Équipe trop réduite
⏱️ Heures prolongées sans rotation

🧠 Comment y faire face en tant que L1 :
🛠️ Aider à l'ajustement des règles pour réduire le bruit

📚 Utiliser des sources de CTI ou d’inventaire réseau pour contextualiser
✅ Mettre en place des règles de suppression pour les alertes bénignes
🤝 Alterner les tâches pour garder la concentration
📝 Donner du feedback pour améliorer les règles SIEM

💡 Astuce : La fatigue n’est pas une faiblesse individuelle, c’est souvent un signal d’alerte sur les processus internes. Proposez des améliorations constructives.

❓ Avez-vous déjà ressenti cette fatigue ? Qu’est-ce qui vous a aidé à la surmonter ?

7- Working with Shift Teams in a 24/7 SOC

In a 24/7 Security Operations Center (SOC), continuous monitoring is non-negotiable. This is made possible by working in shift-based teams, where effective communication, documentation, and handover practices are essential to maintain security posture around the clock.

🔁 Why shift work matters in a SOC:
Threat actors don't follow business hours.
Incidents can evolve rapidly and must be tracked across shifts.
Every alert or investigation must be handed over clearly and accurately.

🧰 Best practices for shift-based SOC work:
🕒 Maintain a clear shift schedule with minimal overlap gaps
📋 Use standardized handover templates or tickets (Jira, ServiceNow)
📞 Hold quick debrief meetings (if possible) to ensure clarity
📓 Document incomplete investigations or observations in detail
🤝 Build trust and shared ownership with your teammates across shifts

💡 Pro Tip: Your shift handover note might be the only information your teammate has to continue the investigation. Write it like you won't be there to explain it.

❓ How do you ensure nothing gets lost between SOC shifts in your team?

Travailler en Équipes de Rotation dans un SOC 24/7

Dans un SOC opérationnel 24/7, la surveillance continue est essentielle. Cela repose sur un travail par équipes en rotation, où la communication, la transmission des consignes et la documentation sont clés pour assurer une couverture efficace en continu.

🔁 Pourquoi le travail en shifts est indispensable :
Les cyberattaques ne s'arrêtent pas le soir ou le week-end
Un incident peut s'aggraver si la relève n'a pas toutes les infos
Chaque alerte ou enquête doit être documentée et transmise avec rigueur

🧰 Bonnes pratiques pour le travail en shifts :
🕒 Respecter un planning de rotation sans zones grises
📋 Utiliser des modèles de passation normalisés (tickets, rapports)
📞 Prévoir des points de transmission oraux si possible
📓 Bien documenter les investigations en cours ou observations clés
🤝 Créer une culture de confiance et de collaboration entre équipes

💡 Astuce : Agissez comme si votre collègue n'avait aucune autre info que votre note de passation. Soyez précis et clair.

❓ Quelles pratiques utilisez-vous pour éviter les pertes d’info entre deux shifts ?

8- Common Mistakes to Avoid as a Junior SOC Analyst

Starting out in a SOC is an incredible opportunity, but the learning curve can be steep. Here are key mistakes that can slow your progress—and how to avoid them.

🔎 Top Mistakes

1️⃣ Focusing only on alert title — always check logs and context
2️⃣ Poor documentation — weakens handovers and team support
3️⃣ Skipping root cause — don't stop at symptoms
4️⃣ Escalating too fast — understand triage thresholds
5️⃣ Ignoring threat intel — enrich alerts with CTI (e.g., OTX)
6️⃣ Not asking for help — SOC is a team job
7️⃣ Skipping SOPs — follow the playbooks
8️⃣ Burnout from alert overload — learn to prioritize

💡 Pro Tip: Strong habits = faster growth. Document clearly, collaborate often, and stay curious.

❓ Which mistake helped you grow the most?

Erreurs à Éviter en tant qu'Analyste SOC Junior

Commencer dans un SOC est une belle opportunité, mais il y a des pièges fréquents à éviter pour progresser efficacement.

🔎 Erreurs Fréquentes

1. Se fier uniquement à l'alerte — analyser aussi les logs
2. Documentation floue — impacte le travail d'équipe
3. Oublier la cause racine — pas seulement les symptômes
4. Escalade trop rapide — comprendre les critères
5. Oublier le renseignement — enrichir via CTI (ex: OTX)
6. Travailler seul — poser des questions est vital
7. Ignorer les SOP — suivez les procédures
8. Surchauffe — prioriser les alertes importantes

💡 Astuce : Les bonnes habitudes font toute la différence. Rédiger, partager, progresser.

❓ Quelle erreur vous a le plus appris ?

COMMON MISTAKES TO AVOID AS A JUNIOR SOC ANALYST

ALERT-ONLY FOCUS
Don't rely solely on the alert title.

POOR DOCUMENTATION
Capture clear, complete ticket details.

SKIPPING ROOT CAUSE
Don't stop at the symptom.

ESCALATING WITHOUT CLARITY
Know your triage criteria.

NEGLECTING THREAT INTEL
Use internal & external CTI feeds

WORKING IN ISOLATION
SOC is collaborative

IGNORING SOPs
Follow your playbooks

INAAM