

# SOC L1: OPERATIONS & INVESTIGATION

Date: 09/01/2026 | Revision No: 02

## 1. SOC TEAM STRUCTURE

---

### – Level 1 (The Gatekeepers)

- Constant monitoring of SIEM dashboard.
- **Triage Alerts**: Sorting real threats from noise.
- Identify **False Positives** ASAP to save time.
- If suspicious but complex → **Escalate!**

### – Level 2 (The Incident Responders)

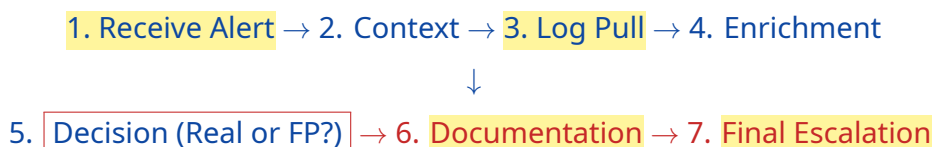
- Deep dive into logs & correlation.
- Goal: **Containment** & Eradication.

### – Level 3 (The Hunters)

- **Threat Hunting**: Looking for what SIEM missed.
- Reverse engineering malware & Tuning SIEM.

## 2. DAY-TO-DAY WORKFLOW OF L1

---



### Memory Trick

**R-C-L-E-D**: Receive, Context, Logs, Enrich, Decide

## 3. CORE RESPONSIBILITIES & TOOLKIT

---

### Core Responsibilities

- ✓ Continuous Monitoring
- ✓ Initial Investigation
- ✓ **Threat Validation**
- ✓ Documentation
- ✓ Escalation

### L1 Analyst Toolkit

- ☐ **SIEM** (Splunk/Sentinel)
- ☐ **EDR** (CrowdStrike/Defender)
- ☐ **Intel** (VirusTotal/Talos)
- ☐ Wireshark (Network)
- ☐ ServiceNow/Jira

## 4. DEMO: URL INVESTIGATION (VIRUSTOTAL)

---

**Target URL:** mp3raid.com/music/krizz\_kaliko.html

### Investigation Findings

Checking this on VirusTotal (VT) yields critical data:

1. **Detection Ratio:** Indicates how many engines flagged the URL (e.g., 5/90).
2. **Threat Categories:** Helps identify if the site is Malware, Phishing, or PUA.
3. **Reputation:** Community votes and historical data regarding the domain.

**Final Verdict:** Precision is more important than speed, but Documentation is more important than both.

*Stay vigilant. Happy Hunting!*