# How to Use This Handbook

This handbook is your daily companion as a SOC analyst. It covers exactly what to do from the moment an alert fires to the moment you close the ticket — no guesswork, no gaps. Every step, every tool, every decision point is spelled out.

**📋 WHAT'S INSIDE**

- Phase-by-phase triage process
- Severity scoring matrix
- Real-world investigation queries
- Escalation decision framework
- Shift handover checklist

**🎯 WHO IT'S FOR**

- Junior SOC analysts (Tier 1–2)
- Analysts joining a new SOC team
- Security engineers rotating into SOC
- Team leads standardizing processes
- Anyone sick of ad-hoc triage

# Alert Severity Scoring Matrix

Before you investigate anything, you score it. This prevents wasting 2 hours on a P4 while a real P1 sits in the queue.

| SEV | LEVEL | EXAMPLES | RESPOND WITHIN | ACTION |
|---|---|---|---|---|
| P1 | CRITICAL | Active ransomware / lateral movement confirmed / domain admin compromise / data exfil in progress | 15 minutes | Page IR lead. Contain NOW. War room. |
| P2 | HIGH | Malware detected on endpoint / successful phishing / brute force with successful auth / C2 beacon detected | 1 hour | Escalate to Tier 2. Begin containment. Notify supervisor. |
| P3 | MEDIUM | Multiple failed logins / suspicious script execution / new admin account / AV detection (low confidence) / unauthorized software install | 4 hours | Investigate during shift. Document findings. Escalate if evidence grows. |
| P4 | LOW | Policy violation / single failed login / scan detected / informational IOC / user reported suspicious email (no click) | 24 hours | Log and monitor. Resolve same shift if possible. |

**⚡ UPGRADE RULE — When to bump severity immediately:**

If ANY of the following appear during investigation, upgrade severity by one level: evidence of lateral movement, PII or financial data access, privileged account involved, persistence mechanism found (scheduled task, registry run key, service), C2 communication detected, attacker still active/connected.

# The 5-Phase Triage Process

Every alert — from a simple AV detection to a full ransomware incident — runs through this same 5-phase framework. Do not skip phases. Do not change the order.

## PHASE 1 — Initial Alert Review (5 min)

*Open the alert. Do not touch the endpoint yet. Read before you act.*

1. Read the full alert title, description, and source system (SIEM / EDR / email gateway).
2. Identify the key entities: hostname, username, source IP, destination IP, process name, file path, parent process.
3. Record these in your ticket before doing anything else — they are your anchors for the rest of the investigation.
4. Assign initial severity using the matrix in Section 2.
5. Check: have we seen this alert or these entities before? Search the SIEM for the hostname and username over the past 30 days.

## PHASE 2 — Context Gathering (10–20 min)

*Build the story around the alert. Alerts without context are meaningless.*

| USER CONTEXT | ENDPOINT CONTEXT | NETWORK CONTEXT |
|---|---|---|
| Is account active? | OS / patch level? | Internal or external IP? |
| Normal working hours? | Managed or BYOD? | IP reputation (VirusTotal)? |
| On PTO / offboarding? | Last seen / check-in time? | Geo-location expected? |
| Admin / privileged? | Previous alerts on this host? | Reverse DNS lookup? |
| Any recent password reset? | Is it critical / server / workstation? | Seen in threat intel feeds? |

## PHASE 3 — Evidence Collection (15–45 min)

*Collect before you contain. Evidence disappears once you isolate. Document everything with timestamps.*

6. Pull process creation logs: Look for the parent-child process chain. Suspicious patterns: Word.exe → cmd.exe → powershell.exe, explorer.exe → mshta.exe, svchost.exe spawning an unexpected child.
7. Pull network connection logs: Look for connections to new/unknown external IPs, especially on unusual ports (4444, 1337, 8080, 443 to non-CDN IPs).
8. Pull authentication logs: Failed logins, successful logins from new locations, MFA bypass attempts, token-based auth from new devices.