Incident Escalation Playbook

SOC Tier 1 – Incident Detection & Escalation Guide

Author: Dan Chui
Target Role: SOC Operations
Date: January 2026
Environment: Simulated SOC Lab

---

1. Purpose

This Incident Escalation Playbook defines the **standardized process** for detecting, triaging, classifying, and escalating security incidents within a Security Operations Center (SOC).

The objective is to ensure:

- Timely identification of security threats
- Consistent escalation decisions
- Proper handoff from SOC Tier 1 to Tier 2 / Incident Response (IR)
- Accurate documentation and auditability

This playbook is intended for **SOC Tier 1 analysts** handling initial alert triage.

---

2. Environment Overview

- Organization size: Mid-sized enterprise (~500 users)
- Centralized logging via SIEM
- Alerts generated from:
  - Network traffic monitoring
  - Endpoint security tools
  - Authentication and application logs
- SOC operates 24/7
- Incident Response team available on-call
- No SOAR automation assumed

---

3. Incident Severity Classification

Security events are classified into four severity levels based on **impact, scope, and confidence**.

Severity	Description	Example
Low	Informational or false positive	Benign scan, expected admin activity
Medium	Suspicious activity requiring investigation	Single malware alert
High	Confirmed malicious activity	Active command-and-control traffic
Critical	Severe business impact	Data exfiltration, ransomware

Severity determination guides **escalation urgency and response ownership**.

4. Detection & Initial Triage (SOC Tier 1)

When an alert is generated, the SOC Tier 1 analyst performs the following triage steps:

4.1 Alert Validation

- Confirm alert source and timestamp
- Validate alert context (host, user, IP)
- Check for known false positives

4.2 Initial Investigation

- Review correlated logs within SIEM
- Identify affected assets
- Check for repeated or related alerts
- Look for indicators of compromise (IOCs)

4.3 Preliminary Assessment

- Determine whether the activity is:
  - Benign
  - Suspicious
  - Clearly malicious

If the alert is confirmed as a false positive, it is documented and closed.

5. Escalation Decision Logic

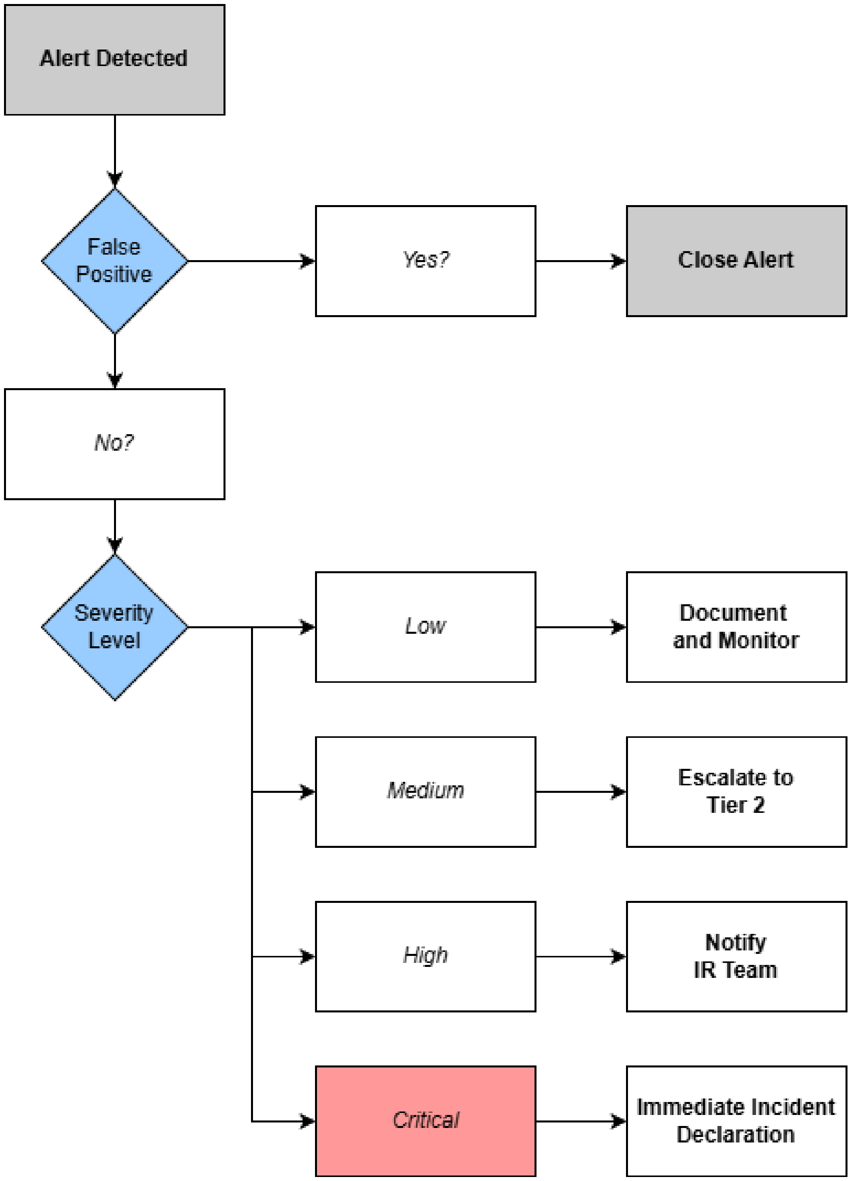
If an alert is **not a false positive**, escalation decisions follow this logic:

1. Identify severity level (Low / Medium / High / Critical)
2. Determine required escalation path

3. Notify appropriate team based on severity
4. Document actions taken

Escalation Flow Summary

- **Low:** Document and monitor
- **Medium:** Escalate to SOC Tier 2
- **High:** Notify Incident Response Lead
- **Critical:** Immediate incident declaration and executive notification



6. Escalation Matrix

Severity	Escalated To	Response SLA
Medium	SOC Tier 2 Analyst	Within 30 minutes
High	Incident Response Lead	Within 15 minutes
Critical	IR Team + Management	Immediate

Escalation may occur via ticketing system, email, or on-call notification depending on severity.

7. Evidence Collection & Handover

SOC Tier 1 analysts **do not remediate incidents**, but ensure proper handover.

Evidence to Collect

- Relevant logs (network, endpoint, authentication)
- Timestamps and event timeline
- Affected hosts and users
- Indicators of compromise (IPs, hashes, domains)

Preservation Guidelines

- Do not reboot affected systems
- Avoid altering system state
- Preserve logs and artifacts
- Maintain chain of custody

8. Documentation & Reporting

All incidents must be documented within the incident tracking system.

Required Documentation

- Alert summary
- Severity classification
- Timeline of actions taken
- Escalation details

- Evidence collected

Post-Incident

- Incident metrics captured (MTTD, MTTR)
- Lessons learned reviewed by SOC and IR teams
- Detection rules refined if necessary

---

9. Conclusion

This playbook ensures consistent and effective escalation of security incidents by SOC Tier 1 analysts.

By following defined severity levels, escalation paths, and documentation standards, the SOC maintains rapid response, accountability, and operational resilience.