SOC Operations Documentation

1. Introduction

This document outlines the operations, workflows, tools, and procedures within a Security Operations Center (SOC). It demonstrates proficiency in using essential SOC tools, with a primary focus on **Elasticsearch** as a SIEM solution. It also includes detailed procedures for alert handling, incident response, and shift transitions.

2. Essential SOC Tools Overview

2.1 SIEM System: Elasticsearch

Purpose: Elasticsearch, as part of the Elastic Stack (ELK Stack), is a powerful, open-source search and analytics engine used for log aggregation and real-time security monitoring.

Function:

- Ingests log data from multiple sources (firewalls, endpoints, servers).
- Enables real-time search, analysis, and visualization of log data.
- Supports alert generation through Kibana and Watcher.
- Allows security teams to identify suspicious patterns and anomalies.

Operational Concepts:

- Indexing of logs for quick searchability.
- Use of Kibana for dashboard visualization.
- Use of Elastic Security for detection rules and threat hunting.

2.2 Ticketing Platform: ServiceNow

Purpose: Central platform for tracking incidents, requests, and changes in an IT environment.

Function:

- SOC analysts log, update, and resolve incidents.
- Tickets are assigned based on severity and team roles.
- Enables consistent documentation and compliance.**2.3 Monitoring Solution: Zabbix**

Purpose: Open-source monitoring tool for tracking the status of servers, network devices, and applications.

Function:

- Collects metrics (CPU, memory, disk, etc.) from systems.
- Sends alerts when thresholds are crossed.
- Helps correlate system health with security alerts.

3. SOC Workflow: Alert Handling and Escalation Path

```
graph TD
A[Alert Generated by Elasticsearch] --> B[Initial
Triage by Tier 1 Analyst]
B --> C[Log Incident in ServiceNow]
C --> D[Analyze Indicators in Kibana]
D --> E{Is Escalation Needed?}
```

```
E -- Yes --> F[Escalate to Tier 2 Analyst]
F --> G[Deep Dive Investigation]
G --> H[Mitigate and Contain Threat]
H --> I[Update Ticket and Notify Stakeholders]
E -- No --> J[Perform Basic Mitigation]
J --> I
I --> K[Close Ticket and Document Lessons Learned]
```

4. Shift Transition Procedures

Handover Requirements:
• Summary of all open incidents and alerts.
• Status of ongoing investigations.
• Noteworthy events or patterns observed.
• Pending actions or follow-ups.
Shift Handoff Process:1. Outgoing analyst reviews open tickets and updates documentation.
2. Brief handover meeting (or documented email) is conducted.
3. Incoming analyst verifies all relevant information has been received.
4. Both parties sign off in the shift log.
Tools Used:
• Shift log document (e.g., Excel, Google Sheets, or internal tool).
• Communication platform (Slack, MS Teams, or email).

5. Incident Handling (Template-Based Example)

Incident Title: Suspicious Login from Foreign IP
Detection: Alert generated by Elastic Security: multiple failed logins followed by a successful one from an unusual IP.
Triage: Tier 1 confirmed the anomaly and created a ticket in ServiceNow.
Investigation:
• Checked Kibana logs: multiple failed logins from IP 182.78.x.x
• User's account accessed outside of working hours.
• Correlated login with IP geolocation data.
Containment:
• Temporarily disabled user account.
• Blocked the suspicious IP in the firewall.
Eradication:
• Required password reset.
• Verified no lateral movement or exfiltration.
Recovery:
• Re-enabled account post-verification.• Monitored for recurrence.
Lessons Learned:
• Implemented geofencing for sensitive accounts.
• Added login alerts for off-hours access.

6. Initial Response Protocols (for a designated security incident type)

Incident Type Chosen:
Malware Infection on Workstation

Initial Response Actions:

- **Detection:**
    - SIEM alert triggered for malicious executable download.
- **Triage:**
    - Validate alert severity and confirm the asset involved.
- **Containment:**
    - Immediately isolate the affected workstation from the network.
    - Notify system owner/user and SOC team lead.
- **Preservation:**
    - Capture volatile data (RAM image, running processes).
    - Secure copies of relevant logs (endpoint, SIEM, proxy).

2. Case Management System Components and Operational Purpose

Case Management System:

- **ServiceNow** is used as the central case management platform.

Key Components:

- **Ticket Creation:** Document the incident with all available details (time, asset, indicators).
- **Assignment:** Assign to appropriate analyst tier depending on incident severity.
- **Work Notes:** Analysts log their activities in real time.
- **Escalation Path:** If required, escalate to Tier 2 or Incident Response Team (IRT).

- **Closure:** Ensure full documentation of containment, eradication, recovery steps, and lessons learned.
- **Post-Incident Review:** Linked to continuous improvement processes (update detection rules, new playbooks).

3. Escalation Criteria and Communication Protocols

Decision Point	Action	Who to Notify
Malware spreads to multiple hosts	Escalate to Tier 2	SOC Lead and Incident Response Manager
Malware attempts outbound C2 traffic	Escalate to Incident Response Team (IRT)	CISO and IT Network Team
Data exfiltration suspected	Notify Legal/Compliance	Legal Counsel, CISO,
Regulatory breach potential (e.g., PII loss)	Notify External Authorities (as required)	Legal, Communications Team

Communication Methods:

- Internal: ServiceNow updates, Slack, MS Teams.
- External (if required): Encrypted email or phone calls following escalation matrix.

4. Incident Response Documentation Template

Section	Details
Incident Title	Malware Infection on Workstation
Detection Method	SIEM alert (malicious file hash detected)
Triage Details	Verified malware hash via VirusTotal and endpoint logs
Asset Affected	Workstation (user: marketing_dept01)
Containment Steps	Isolated device from network
Investigation Findings	Malicious executable, initiated outbound traffic attempts
Eradication Measures	Performed full malware removal and reimaged the device
Recovery Actions	Reconnected device after thorough revalidation
Lessons Learned	Added new hash signatures to EDR blocklist, updated detection rules for early identification
Post-Incident Actions	Conducted team review, tuned SIEM correlation rules

✅ **Summary:**

- **Initial Response Protocols:** Documented.
- **Case Management Components:** Explained for ServiceNow.
- **Escalation Criteria and Communication:** Detailed with decision points.
- **Incident Response Template:** Completed in a structured format.
- **Methodologies:** Demonstrated understanding of principles with clear explanations.

7. Conclusion

This documentation showcases the operational maturity of a SOC environment, covering essential tools such as Elasticsearch, ServiceNow, and Zabbix. It demonstrates structured alert handling, escalation, incident response, and effective shift transitions to ensure continuous coverage and rapid response to security events.