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:

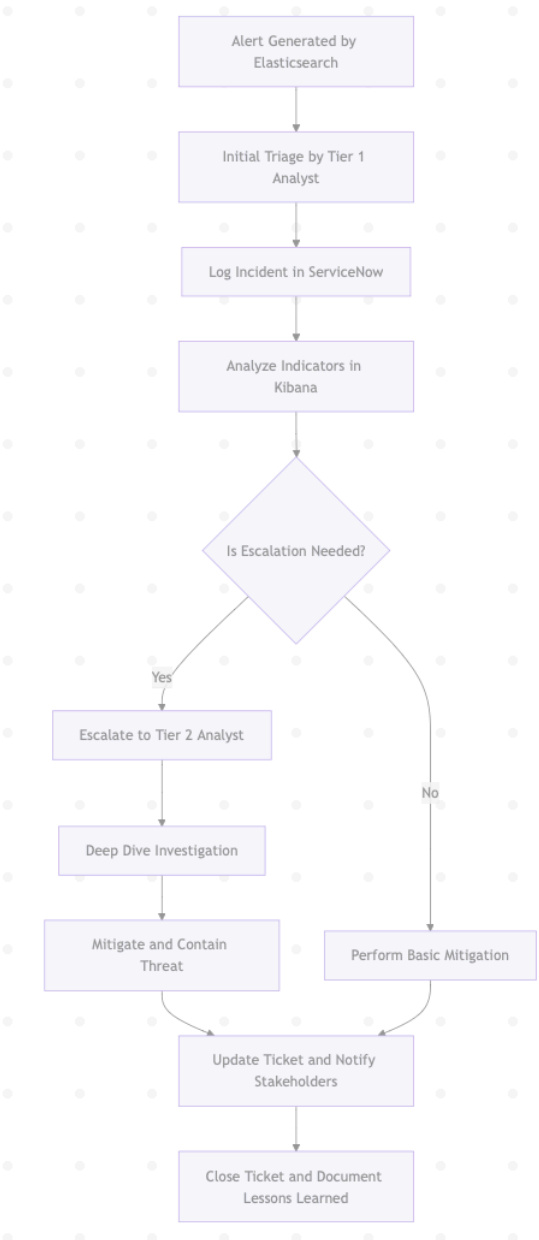
- Re-enabled account post-verification.

- Monitored for recurrence.

Lessons Learned:

- Implemented geofencing for sensitive accounts.
- Added login alerts for off-hours access.

6. Conclusion



Caption

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.