SOC Fundamentals and Practical Training

Introduction

This document provides a structured guide for learning and practicing **Security Operations Center (SOC)** fundamentals and operations.
It is designed for cybersecurity trainees, SOC interns, and entry-level analysts aiming to build hands-on skills in **threat detection, incident response, and monitoring** using industry-standard tools and frameworks.
The purpose is to blend theoretical knowledge with practical exercises for building readiness in real-world SOC environments.

1. SOC Fundamentals and Operations

1.1 Purpose of a SOC

- **Proactive Threat Detection** – Identify potential threats before they cause damage.
- **Incident Response** – Mitigate attacks through quick action.
- **Continuous Monitoring** – 24/7 vigilance over network and system activities.

1.2 SOC Roles

- **Tier 1 Analyst:** Initial alert triage.
- **Tier 2 Analyst:** Deep investigation and threat hunting.
- **Tier 3 Analyst:** Complex incident handling, malware reverse engineering.
- **SOC Manager:** Team leadership, process improvement.
- **Threat Hunters:** Proactive search for unknown threats.

1.3 Key Functions

- Log analysis
- Alert triage
- Threat intelligence integration

How to Learn:

1. Study SOC frameworks: **NIST**, **MITRE ATT&CK**.
2. Watch SOC case studies: *IBM SOC*, *Microsoft SOC*.
3. Practice workflows with **Splunk Phantom** or other SOAR tools.

2. Security Monitoring Basics

2.1 Objectives

- Detect anomalies
- Identify unauthorized access attempts
- Monitor for policy violations

2.2 Tools

- **SIEM:** Splunk, Elastic SIEM
- **Network Analyzers:** Wireshark

2.3 Key Metrics

- **False Positives/Negatives**
- **Mean Time to Detect (MTTD)**

How to Learn:

1. Set up a **lab environment** with Elastic SIEM.

2. Analyze **sample network traffic logs** for suspicious activity.
3. Use pre-recorded attack datasets like **Boss of the SOC**.

3. Log Management Fundamentals

3.1 Log Lifecycle

1. Collection
2. Normalization
3. Storage
4. Retention
5. Analysis

3.2 Common Log Types

- Windows Event Logs
- Syslog
- HTTP Server Logs

Practical Tasks:

- **Log Collection Pipeline:** Install Fluentd on Ubuntu to collect Syslog, forward to Elastic SIEM.
- **KQL Query Practice:**
- **source = "security-login-*" EventID = 4625 | stats count by SourceIP**
- **Normalization Exercise:** Convert Apache access logs to JSON using Logstash.

4. Security Tools Overview

Key Tools

- **SIEM:** Splunk, QRadar
- **EDR:** CrowdStrike
- **IDS/IPS:** Snort
- **Vulnerability Scanner:** Nessus

Practical Tasks:

1. **Snort Rule Testing:** Detect HTTP requests to malicious.com.
2. **Nessus Scan:** Identify top vulnerabilities on Metasploitable2.
3. **Osquery Monitoring:** Query processes and simulate suspicious activity.

5. Basic Security Concepts

- **CIA Triad:** Confidentiality, Integrity, Availability
- **Threat vs Vulnerability vs Risk**
- **Defense-in-Depth & Zero Trust**

6. Security Operations Workflow

1. **Detection:** Alerts from SIEM/EDR
2. **Triage:** Severity prioritization
3. **Investigation:** IOC hunting
4. **Response:** Containment, eradication

7. Incident Response Basics

- **Lifecycle:** Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned
- **Framework:** NIST SP 800-61

8. Documentation Standards

- Incident Reports
- SOPs & Runbooks
- Post-Mortems

Practical Application

1. Log Analysis

- Filter Windows Event ID 4625 (failed logins)
- Identify brute-force attack patterns
- Analyze Chrome history with **Eric Zimmerman's tools**

2. Security Event Documentation

Date/Time	Source IP	Event ID	Description	Action Taken
2025-08-14 14:25	192.168.1.10	4625	Multiple failed logins	Account locked

3. Monitoring Dashboards

- Top 10 source IPs
- Event frequency charts

4. Alert Rules

- Elastic SIEM: Detect 5+ failed logins in 5 minutes
- Wazuh: Detect 3+ failed SSH logins in 2 minutes

Conclusion

This report outlines the **foundational learning path** for SOC operations, blending theory with hands-on practice.

By following this structured approach, a beginner can progress to an operational SOC analyst level, capable of managing alerts, performing investigations, and documenting incidents effectively.

References

- NIST SP 800-61
- MITRE ATT&CK Framework
- Elastic SIEM Documentation
- SANS Incident Handler's Handbook