Introduction

This document provides a framework for creating comprehensive documentation on **Security Operations Center (SOC) Advanced Practices,** focusing on structured methodologies and practical application for an internal audience.

1. Structure of the Document

The documentation is divided into two main sections: **Theoretical Knowledge** and **Practical Application**, followed by a comprehensive summary. Headings, subheadings, and bullet points are used throughout for improved **readability**.

1.1 Theoretical Knowledge

This section details the core concepts and learning resources for advanced SOC practices. Key terms are highlighted in **bold**.

- **Threat Hunting Methodologies**
  - **Core Concepts:** Focus on the distinction between **Proactive Threat Hunting** (e.g., hypothesis-driven hunting for TTPs like T1078 - Valid Accounts misuse) and reactive incident response. Study frameworks like **SqRR** (Search, Query, Retrieve, Respond) and **TaHiTI** (Targeted Hunting integrating Threat Intelligence). Learn to leverage diverse **Data Sources for Hunting** (EDR logs, network traffic, threat intelligence feeds).
  - **How to Learn:** Study SANS Threat Hunting papers, explore threat hunting case studies (e.g., APT29 via MITRE ATT&CK), and review Elastic's threat hunting guide.
- **Advanced SOAR Automation**
  - **Core Concepts:** Understand **SOAR Components**: orchestration (workflow integration), automation (e.g., auto-ticketing), and response (e.g., auto-containment). Learn **Playbook Development** for common incidents (e.g., phishing) and explore **Integration with SIEM/EDR** (Wazuh, Elastic).
  - **How to Learn:** Study SOAR concepts via Splunk SOAR documentation, review playbook examples in TheHive Project, and analyze automation case studies (e.g., phishing response automation via CISA's SOAR guide).

- **Post-Incident Analysis and Continuous Improvement**
  - **Core Concepts:** Master **Root Cause Analysis (RCA)** techniques (e.g., **5 Whys**, **Fishbone Diagram**) to identify incident causes. Understand the **Lessons Learned Process** and utilize SOC metrics like **Mean Time to Detect (MTTD)** and **Mean Time to Respond (MTTR)**.
  - **How to Learn:** Study RCA techniques via SANS Reading Room, review NIST SP 800-61 for post-incident activity, and explore SOC metrics via CISA's Cybersecurity Metrics. * **Adversary Emulation Techniques**
  - **Core Concepts:** Simulate attacker TTPs (e.g., T1566 - Phishing) using **Adversary Emulation** to test SOC capabilities. Study tools like **MITRE Caldera** for automated simulation and understand **Red-Blue Team Collaboration**.
  - **How to Learn:** Explore MITRE Caldera, study emulation case studies (e.g., APT28 via MITRE ATT&CK), and review Red Canary's emulation guide.
- **Security Metrics and Executive Reporting**
  - **Core Concepts:** Understand advanced metrics like **dwell time**, false positive rate, and incident resolution rate. Learn to present metrics to non-technical stakeholders using clear visualizations in **Executive Reporting**.
  - **How to Learn:** Study SOC metrics via SANS Reading Room, review CISA's Cybersecurity Metrics, and explore SANS Incident Response templates.

---

2. Practical Application

This section outlines practical activities, tools, and enhanced tasks to develop hands-on skills. Numbered lists are used for sequential steps and processes.

2.1 Threat Hunting Practice

1. **Hypothesis Development:** Formulate a hypothesis (e.g., "Unauthorized privilege escalation in domain accounts") and query **Elastic Security** for relevant events (e.g., Event ID 4672).
2. **Threat Intelligence Hunt:** Use **AlienVault OTX** for IOCs (e.g., suspicious IPs) and cross-reference with **Velociraptor** queries.

3. **Hunting Report:** Summarize findings, mapping to **MITRE ATT&CK** T1078.

Timestamp	**User**	**Event ID**	**MITRE TTP**	**Notes**
2025-08-18 15:00:00	testuser	4672	T1078 - Valid Accounts	Anomalous role assignment
2025-08-18 15:05:30	svc_account	5156	T1048 - Exfiltration	Suspicious outbound connection

2.2 SOAR Playbook Development

1. **Playbook Creation:** Create a **Splunk Phantom** playbook to auto-block IPs for phishing alerts. Steps include checking IP reputation, blocking via **CrowdSec**, and creating a **TheHive** ticket.
2. **Playbook Test:** Simulate a phishing alert in **Wazuh** and verify playbook execution.

2.3 Post-Incident Analysis

1. **Root Cause Analysis:** Use the **5 Whys** method for a mock incident (e.g., identifying weak email filtering as a cause for a phishing breach).
2. **Fishbone Diagram:** Create a **Fishbone Diagram** in **Draw.io** for the incident, identifying causes (e.g., process, technology).
3. **Metrics Calculation:** Calculate **MTTD** and **MTTR** for a mock incident.

2.4 Capstone Project: Comprehensive SOC Incident Response

This project integrates all advanced practices in a simulated complex attack.

1. **Attack Simulation & Emulation:** Exploit a vulnerability (e.g., Metasploit) and use **MITRE Caldera** to simulate a related TTP (e.g., **T1210** - Exploitation of Remote Services).
2. **Detection and Triage:** Configure **Wazuh** to alert and triage the incident in **TheHive**.
3. **Response and Containment:** Isolate the VM and block the attacker's IP with **CrowdSec**.
4. **SOAR Automation:** Automate IP blocking via a **TheHive** playbook.
5. **Post-Incident Analysis:** Conduct RCA and create a Fishbone Diagram.
6. **Metrics Reporting:** Calculate MTTD, MTTR, and dwell time in **Elastic Security**.

2.2 SOAR Playbook Development

1. **Playbook Creation:** Create a **Splunk Phantom** playbook to auto-block IPs for phishing alerts. Steps include checking IP reputation, blocking via **CrowdSec**, and creating a **TheHive** ticket.
2. **Playbook Test:** Simulate a phishing alert in **Wazuh** and verify playbook execution.

2.3 Post-Incident Analysis

1. **Root Cause Analysis:** Use the **5 Whys** method for a mock incident (e.g., identifying weak email filtering as a cause for a phishing breach).
2. **Fishbone**
3. **Diagram:** Create a **Fishbone Diagram** in **Draw.io** for the incident, identifying causes (e.g., process, technology).
4. **Metrics Calculation:** Calculate **MTTD** and **MTTR** for a mock incident.

2.4 Capstone Project: Comprehensive SOC Incident Response

This project integrates all advanced practices in a simulated complex attack.

1. **Attack Simulation & Emulation:** Exploit a vulnerability (e.g., Metasploit) and use **MITRE Caldera** to simulate a related TTP (e.g., **T1210** - Exploitation of Remote Services).
2. **Detection and Triage:** Configure **Wazuh** to alert and triage the incident in **TheHive**.
3. **Response and Containment:** Isolate the VM and block the attacker's IP with **CrowdSec**.

4. **SOAR Automation:** Automate IP blocking via a **TheHive** playbook.
5. **Post-Incident Analysis:** Conduct RCA and create a Fishbone Diagram.
6. **Metrics Reporting:** Calculate MTTD, MTTR, and dwell time in **Elastic Security**.

Conclusion/Summary

This documentation provides a comprehensive guide for advancing skills in **Threat Hunting**, **SOAR Automation**, **Post-Incident Analysis**, and **Adversary Emulation**. Adherence to the specified formatting guidelines, including **clear headings**, **consistent font styles** (Arial/Times New Roman, Size 11-12 body text) , and the strategic use of **visuals and bold text** for emphasis, ensures the document is professional, readable, and highly informative. The practical tasks, culminating in the **Capstone Project**, offer a structured path to mastering advanced SOC operations.