Introduction

This document outlines essential guidelines for writing effective technical documentation, focusing on clear and professional documentation is crucial for conveying complex technical information, and consistent application of formatting and structural rules ensures readability for a wide audience, which in this case includes Security Operations Center (SOC) personnel. The structure, Language, and formatting provided herein serve as the foundation for creating high-quality, professional reports and guides.

1. Theoretical Knowledge

This section details the core concepts, objectives, and learning methodologies for advancing skills in key security domains.

1.1. Advanced Log Analysis

The core concepts focus on transforming raw logs into actionable intelligence.

- **Core Concepts:**
    - **Log Correlation:** Understanding how to link logs from diverse sources (e.g, firewall, endpoint, application) to identify comprehensive attack patterns, such as connecting failed logins (Events ID 4625) with suspicious outbound traffic.
    - **Anomaly Detection:** Techniques (statistical or rule-based) used to spot unusual activity like high-volume data transfers or abnormal login times.
    - **Log Enrichment:** The process of adding context to logs, such as mapping IPs to their geolocation or assigning user roles, to enhance analysis.

- **Key Objectives:** Develop the capability to analyze and correlate logs effectively to uncover complex threats and significantly reduce the number of false positives.
- **How to Learn:** Study log correlation methods via SANS Reading Room resources, explore anomaly detection through Elastic's documentation, and review historical case studies (e.g., Equifax breach) to understand real-world log correlation.

1.2. Threat Intelligence Integration

This domain focuses on leveraging external data to improve detection and hinting capabilities.

- **Core Concepts:**
  - **Threat Intelligence Types:** Distinguishing between Indicators of Compromise (**IOCs**) (e.g., malicious IPs, hashes), **TTPs** (Tactics, Techniques, and Procedures), and standardized threat feeds (e.g., STIX/TAXII).
  - **Integration in SOC:** Learning to embed threat intelligence into SIEM systems for automated alert enrichment, such as matching a suspicious IP against a known Command and Control (C2) server.
  - **Threat Hunting with Intelligence:** Proactively searching for threats using intelligence, for instance, hunting for the MITRE ATT&CK technique T1078 (Valid Accounts misuse).

- **Key Objectives:** Build expertise in integrating and applying threat intelligence to significantly enhance detection and response efficiency.
- **How to Learn:** Explore the MITRE ATT&CK framework for TTPs, study STIX/TAXII standards through OASIS Cyber Threat Intelligence, and review practical threat feed examples on platforms like AlienVault OTX.

1.3. Incident Escalation Workflows

Mastering the process for handling and communicating high-severity incidents.

- **Core Concepts:**
  - **Escalation Tiers:** Understanding the SOC structure (Tier 1: Triage, Tier 2: Investigation , Tier 3: Advanced Analysis) and defining clear criteria for escalation based on severity and complexity.
  - **Communication Protocols:** Learning structured communication formats like **SITREP** (Situation Reports) for effective stakeholder briefings.
  - **Automation in Escalation :** Utilizing **SOAR** (Security Orchestration, Automation, and Response) tools to automate tasks like ticket assignment and alert enrichment during the escalation process.

- **Key Objectives:** Master reliable workflows for escalating incidents and ensuring effective, structured communication with all stakeholders.

- **How to Learn:** Study incident escalation workflows in **NIST SP800-61,** review the SANS Incident Handler's Handbook for communication templates, and explore SOAR concepts using documentation like Splunk SOAR's

2. Practical Application

This section details the hands-on tasks and corresponding tables used to document the outcomes for skill validation.

2.1. Advanced Log Analysis

Timestamp	Event ID	Source IP	Destination IP	Notes
2025-08-18 12:00:00	4625	192.168.x.x	192.168.x.x	Suspicious DNS request correlating with failed login
2025-08-18 12:00:00	5156	192.168.x.x	192.168.x.x	Outbound connection attempt following failed authentication.

2.2. Threat Intelligence Integration

Alert ID	IP	Reputation	Notes
003	192.168.x.x	Malicious (OTX)	Linked to known C2
005	192.168.x.x	Benign	Internal DNS server

4. Alert Triage with Threat Intelligence

Alert ID	Description	Source IP	Priority	Status
004	Suspicious PowerShell Execution	192.168.x.x	High	Open
006	Failed Brute Force Attempt	192.168.x.x	Medium	In Progress

5. Evidence Preservation and Analysis

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-Y Dump for malware analysis	SOC Analyst	2025-08-18	*72A6F3C8A67B…..A194B5E*
Hard Drive Image	Full image of Compromised Workstation-Z	Forensic Lead	2025-08-18	*E9D4C2B1F0A8….D876C5A*

6. Capstone Project

Timestamp	Source IP	Alert Description	MITRE Technique
2025-08-18 14:00:00	192.168.x.x	Samba usermap_script exploit attempt	T1210
2025-08-18 14:00:00	192.168.x.x	High-volume file write to /tmp	T1105

Summary

This program successfully structures the development of advanced SOC analyst skills, clearly separating the conceptual **Theoretical Knowledge** from the necessary **Practical Application.** The practical section provides structured, verifiable tasks using industry tools, complete with mandatory tables for documentation, which aligns with the goal of creating clear, concise , and structured material, Mastery of these skills is crucial for moving from reactive monitoring to proactive threat hunting and structured incident response, all to be completed by the **Friday 5:30 PM deadline.**