Incident Escalation Practice

Objective

This task focuses on **incident escalation procedures** within a Security Operations Center (SOC). The goal is to practice **escalation decision-making, situation reporting (SITREP), and basic workflow automation** to ensure timely response and effective communication between SOC tiers.

Tools Used

- **TheHive** – Incident and case management
- **Google Docs** – SITREP and incident documentation
- **Splunk Phantom (SOAR)** – Workflow automation (conceptual)

Task Overview

1. Escalation Simulation (TheHive Case)

Purpose:
Practice escalating a **High-priority security incident** from Tier 1 to Tier 2.

Mock Incident:

- Incident Type: Unauthorized Access
- Affected Asset: Server-Y
- Source IP: 192.168.1.200
- MITRE Technique: **T1078 – Valid Accounts**

TheHive Case Details:

- **Title:** `[High] Unauthorized Access on Server-Y`
- **Severity:** High
- **Status:** Open
- **Assignee:** SOC Analyst – Tier 1

Escalation Action:
Case escalated to **Tier 2** for deeper investigation due to potential credential compromise.

Escalation Summary (100 Words – Tier 2)

A high-priority unauthorized access alert was detected on Server-Y at 2025-08-18 13:00. The activity originated from IP address 192.168.1.200 and maps to MITRE ATT&CK technique T1078 (Valid Accounts), indicating possible credential misuse. Initial triage confirmed suspicious login behavior outside normal patterns. As a containment measure, Server-Y was isolated from the network. No confirmed lateral movement observed at this stage. The incident is escalated to Tier 2 for advanced log analysis, credential validation, and scope determination.

2. SITREP Draft (Situation Report)

Purpose:
Communicate incident status clearly to technical and management stakeholders.

SITREP Document

Title:
Unauthorized Access on Server-Y

Summary:
Unauthorized access activity was detected on Server-Y at **2025-08-18 13:00**. The source IP **192.168.1.200** was identified, and the activity aligns with **MITRE ATT&CK T1078 (Valid Accounts)**, suggesting possible credential compromise.

Actions Taken:

- Server-Y isolated from the network
- Alert escalated to SOC Tier 2
- Investigation initiated for credential misuse

3. Workflow Automation (Splunk Phantom)

Purpose:
Reduce response time by automating alert assignment.

Automation Logic (Conceptual Playbook):

```
IF alert.priority == "High"
THEN assign case to Tier 2
```

Playbook Actions:

1. Trigger on High-priority alert
2. Update incident owner to Tier 2
3. Add escalation note automatically

Test Result:

- Mock High-priority alert successfully auto-assigned to Tier 2

SOC Benefit:
Automation ensures faster escalation, reduces analyst workload, and enforces consistent response workflows.

Summary (50 Words)

Incident escalation practice demonstrated effective SOC workflows by creating a high-priority TheHive case, drafting a structured SITREP, and escalating to Tier 2. Automation using a SOAR playbook ensured rapid assignment of critical alerts, improving response time, communication, and operational efficiency.