Incident Escalation Practice

Objective

To practice incident escalation procedures, draft a Situation Report (SITREP), and demonstrate basic workflow automation for handling high-priority security alerts.

Tools Used

- TheHive
- Google Docs
- Splunk Phantom
- MITRE ATT&CK

1. Escalation Simulation (High-Priority Alert)

A mock high-priority security alert indicating unauthorized access was simulated. A case was created in TheHive and escalated to Tier 2 for further investigation and response.

Escalation Summary

A high-priority alert indicating unauthorized access activity was detected on a monitored server. Initial analysis identified suspicious authentication behavior associated with a valid user account, suggesting potential credential misuse. The incident was classified as high severity due to the risk of lateral movement and privilege abuse. Immediate containment actions were recommended, including isolating the affected system and reviewing authentication logs. The case was escalated to Tier 2 analysts for in-depth investigation, validation of compromise indicators, and coordination of remediation actions. All relevant artifacts, timestamps, and indicators were documented to support efficient incident handling.

2. SITREP Draft (Mock Incident)

Title

Unauthorized Access on Server-Y

Summary

Unauthorized access activity was detected on Server-Y at 2025-08-18 13:00 originating from IP address 192.168.1.200. The activity aligns with MITRE ATT&CK technique T1078 (Valid Accounts), indicating possible misuse of legitimate credentials.

Actions Taken

- Server-Y was isolated from the network
- The incident was escalated to Tier 2 analysts
- Relevant logs and indicators were preserved for investigation

3. Workflow Automation (SOAR)

A simple workflow automation was designed using Splunk Phantom to improve incident response efficiency.

Playbook Description

The playbook automatically assigns High-priority alerts to the Tier 2 response team upon detection. This reduces manual effort and ensures timely escalation of critical incidents.

Mock Test Performed

A mock high-priority alert was generated to validate the workflow. The playbook successfully executed and auto-assigned the alert to Tier 2 analysts, confirming correct automation behavior.

Conclusion

This task was completed as a mock simulation to demonstrate incident escalation, SOC communication, and workflow automation concepts. The exercise reflects real-world SOC practices while ensuring no production systems or live environments were impacted.