

Incident Escalation Report

1. Executive Summary

This exercise focused on simulating an incident escalation workflow using TheHive for case management and Splunk Phantom for automation. The objective was to practice Tier-based escalation, and demonstrate automated handling of High-priority alerts.

2. Environment

- TheHive: Incident response and case management.
- Splunk Phantom (SOAR): Workflow automation.
- MITRE ATT&CK Threat technique: T1078 – Valid Accounts.

3. Incident Details

Field	Value
Incident Title	Unauthorized Access on Server-Y
Detection Time	2025-12-18 13:00
Severity	High
Source IP	192.168.1.200
Affected Asset	Server-Y
MITRE ATT&CK	T1078 – Valid Accounts
Initial Handler	SOC L1
Escalated To	SOC L2

Table 1: Incident Details

4. Escalation

A High-priority incident case was created in TheHive following detection of unauthorized access activity and escalated to SOC L2.

An unauthorized access alert was detected on Server-Y at 2025-12-18 13:00 originating from IP address 192.168.1.200. Analysis suggests potential misuse of valid credentials, aligning with MITRE ATT&CK technique T1078 (Valid Accounts). Initial triage confirmed abnormal login behavior deviating from baseline activity. As a containment action, Server-Y was isolated



from the network. Due to the high severity and risk of credential compromise, the incident has been escalated to SOC L2 for deeper investigation, credential validation, and assessment of possible lateral movement across the environment.

5. TheHive Case Tasks

Five investigation and response tasks were created and tracked within the TheHive case:

Task No.	Task Name	Status
1	Initial Alert Triage	Completed
2	Validate Unauthorized Access	Completed
3	Containment and Isolation	Completed
4	Evidence Collection	Completed
5	Escalation Decision	Completed

Table 2: Case Task

7. Situation Report

Situation report is documented in another doc named Situation Report.

8. Workflow Automation – Splunk Phantom Playbook

Workflow is documented in another document named WorkFlow.

9. Summary

This incident escalation practice successfully demonstrated structured incident handling using TheHive, effective L1 to L2 escalation, clear and professional incident documentation, and automated escalation through Splunk Phantom SOAR. The workflow aligned with MITRE ATT&CK techniques and established SOC best practices, accurately reflecting real world SOC operations and strengthening operational readiness for handling high severity security incidents.