Incident Escalation Practice Report

Introduction

Incident escalation is a critical SOC process used to ensure security incidents are handled by the appropriate response tier. High-priority alerts that indicate potential compromise are escalated from Tier 1 analysts to Tier 2 or Tier 3 for deeper investigation. Proper escalation improves response time, reduces risk, and ensures effective communication with stakeholders.

Escalation Simulation – TheHive Case

A High-priority alert indicating unauthorized access was detected during routine SOC monitoring. Based on the severity and potential impact, the incident was escalated from Tier 1 to Tier 2 using TheHive case management workflow.

TheHive Case Details

Case Title:
[High] Unauthorized Access on Server-Y

Severity:
High

Status:
Escalated

Assigned Team:
Tier 2 SOC

Description:
Unauthorized access activity was detected on Server-Y. The alert indicated suspicious login behavior associated with MITRE ATT&CK technique T1078 (Valid Accounts).

This incident was escalated to Tier 2 SOC due to confirmed unauthorized access activity on Server-Y. The alert was detected at 13:00 IST and originated from IP address 192.168.1.200. Analysis mapped the activity to MITRE ATT&CK technique T1078, indicating potential misuse of valid credentials. The affected server was isolated as a containment measure, and initial log review was completed. Further forensic analysis and credential validation are required to determine the scope and impact of the compromise.

Situation Report (SITREP)

Title:
Unauthorized Access on Server-Y

Summary:
An unauthorized access incident was detected on 18 August 2025 at 13:00 IST. The suspicious activity originated from IP address 192.168.1.200 and was mapped to MITRE ATT&CK technique T1078 (Valid Accounts).

Actions Taken:
- Affected server was isolated from the network
- Alert was escalated from Tier 1 to Tier 2 SOC
- Initial log review was performed

Current Status:
Incident under investigation by Tier 2 SOC team.

Escalation Workflow Automation

Automation can significantly improve incident escalation efficiency in SOC environments. A Splunk Phantom playbook was designed to automate escalation of High-priority alerts.

Playbook Logic:
1. Trigger when alert severity = High
2. Automatically assign case to Tier 2 SOC
3. Enrich alert with threat intelligence
4. Notify Tier 2 team via ticketing system

Testing was performed using a mock High-priority alert, and the playbook successfully assigned the case to Tier 2.

Conclusion

This task demonstrated the importance of structured escalation workflows, clear communication, and automation in SOC operations. Using TheHive for case management, SITREPs for communication, and SOAR platforms for automation ensures faster response and consistent handling of high-impact security incidents.