Incident Escalation Practice

1. Objective

This report contains the details of the task includes Escalation Simulation, SITREP, and Workflow Automation. The goal of this task is to:

- Master workflows for escalating incidents and communicating with stakeholders effectively.

2. Introduction

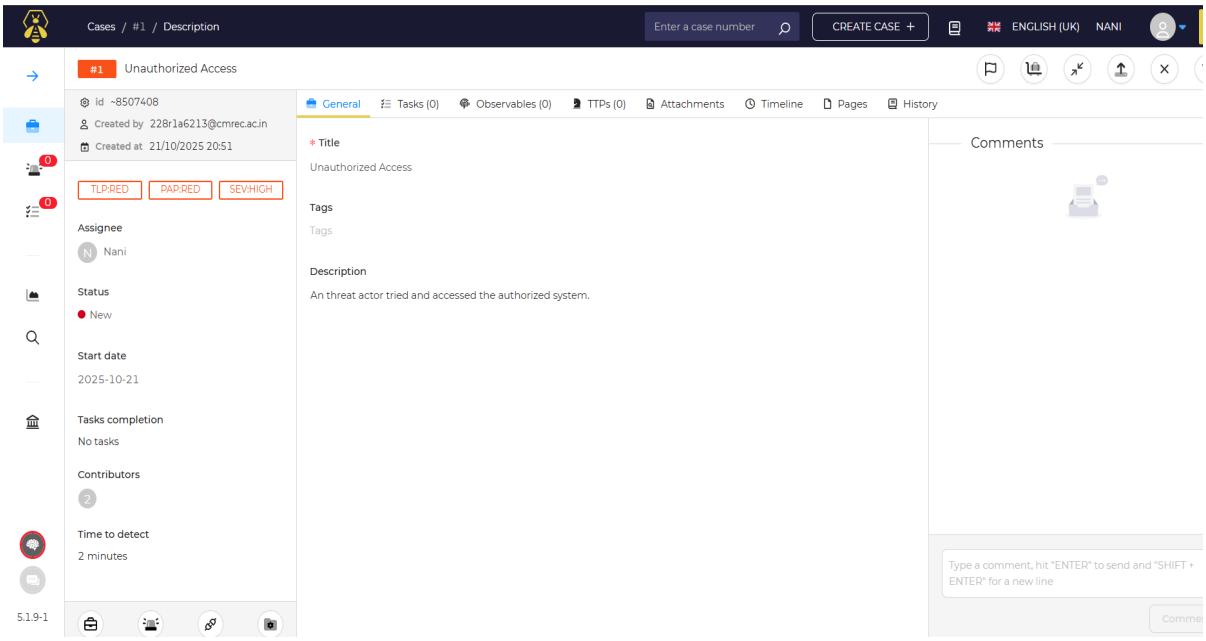
Incident Escalation Practice is a structured approach for handling an incident by sending it to higher authority like SOC L2 team when the current incident handler can't handle the event. For this practice it is required to know the escalation simulation process, Situation response Documentation, and automation of workflow that includes creation of playbook for sending the higher-alerts to Tier 2 teams.

3. Tools

- TheHive is a Security Incident Response Platform (SIRP) tool. Setup using TheHive documentation.
  https://docs.strangebee.com/thehive/installation/installation-guide-linux-standalone-server/
- Google docs

4. Escalation Simulation

Creating a TheHive case for a high-priority alert (e.g., unauthorized access). Escalating it to Tier 2 with a brief summary. This escalation simulation includes the following TheHive tool and Google docs. Creating a case for higher-priority for this simulating an alert then detailing about the incident as a brief summary and also informing about the TheHive tool because it contains the case details.



5. SITREP DRAFT

SITREP stands for Situation Report. Writing a situation report of the mock incident. SITREP is a structured update on an ongoing incident, threat, or security posture. Its purpose is to provide a clear and overview of the situation to both the technical and non-technical personnel. There are few steps to be taken to make the situation report and that steps includes Title, Summary, and Actions.

5.1 SITREP REPORT

1. Title

Title: Unauthorized Access on Server-Y

Incident ID: 100001

Date / Time of Report: 2025-10-16 13:30 UTC

Prepared by: Tier-1 Analyst (Escalated to Tier-2 SOC)

2. Execution Summary

Time	Event Description	Notes
13:00	Unauthorized access detected on Server-Y	Alerts triggered from SIEM correlation rule.

13:05	Alert verified by Tier-1 Analyst	Log analysis confirmed unauthorized RDP login.
13:13	Containment initiated	Server-Y isolated from network to prevent access.
13:22	Case created in TheHive	Incident recorded as high priority.
13:30	Escalation to Tier-2 SOC Team	Forensic Investigation assigned
13:35	SITREP drafted and distributed	Initial report sent to SOC management.

3. Actions

[13:00] SIEM alert triggered on unauthorized RDP login

[13:05] Analyst validated alert and initiated containment

[13:13] Server-Y isolated via firewall ACL

[13:30] TheHive case created and escalated to Tier-2

[13:35] SITREP drafted and distributed

6. Workflow Automation

Creating a simple Splunk Phantom playbook to auto-assign high-priority alerts to Tier2. Test with a mock alert. Workflow is the use of software to automate repetitive tasks and processes, reducing manual effort, errors, and time. It involves setting predefined rules to guide tasks, data, or file through a sequence of steps.

[DEBUG] **Playbook triggered for:** Unauthorized Access – Server-Y

[COMMENT] High-priority alert detected. Escalating to Tier 2 SOC.

[OWNER] Assigned to tier2_team

[STATUS] Set to open

[COMMENT] Case assigned to Tier 2 SOC and marked as Open.

[NOTIFY] **Sent to tier2@soc.local:**

High-Priority Alert Assigned to Tier 2:

Case: Unauthorized Access – Server-Y

ID: 100001

[DEBUG] Playbook completed for: Unauthorized Access – Server-Y

[DEBUG] Playbook triggered for: Suspicious Login Attempt

[COMMENT] No escalation required. Severity: medium

[DEBUG] Playbook completed for: Suspicious Login Attempt

[DEBUG] Playbook triggered for: Firewall Policy Update

[COMMENT] No escalation required. Severity: low

[DEBUG] Playbook completed for: Firewall Policy Update

6.1 Testing with mock alert

Testing with a mock alert whether it is escalating it or not to the higher authority.