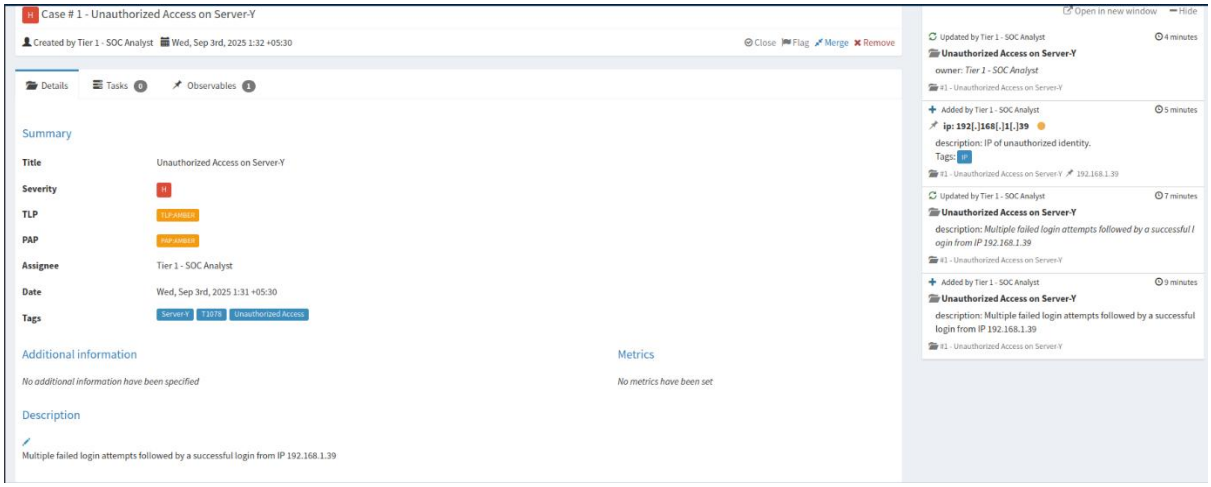
INCIDENT ESCALATION PRACTICE

Introduction

This document outlines the incident escalation practice exercise carried out using TheHive for case and alert management. The exercise simulated a high-priority alert involving unauthorized access to a server. It covered case creation, alert ingestion via API, initial triage, escalation to Tier 2, and drafting a Situation Report (SITREP). A simple Splunk Phantom playbook was created to auto-assign High-priority alerts to Tier 2, tested with a mock alert.

Case Creation In TheHive

- Logged into TheHive web interface.
- Manually created a new case titled: “Unauthorized Access on Server-Y.”
- Case served as a container for documentation and escalation simulation.
- Note: Case was not directly linked to alert (mock simulation allowed treating them separately).



1: TheHive Case - Unauthorized Access

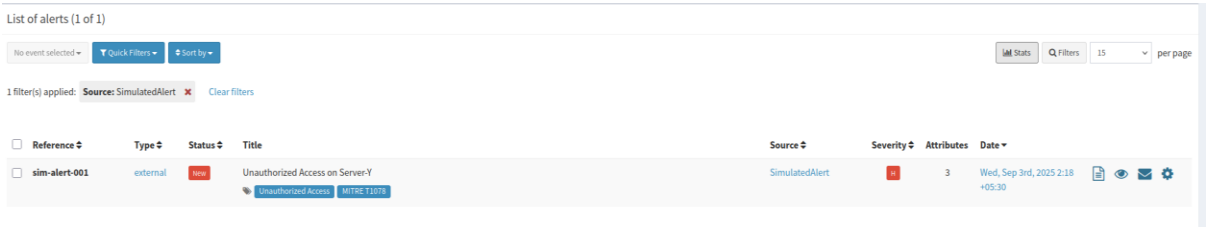
Alert Ingestion via API

- **Created a JSON file (unauthorized_mockalert.json) with alert details:**

```
{
 "title": "Unauthorized Access on Server-Y",
 "description": "Detected unauthorized login attempt on Server-Y from IP 192.168.1.39",
 "severity": 3,
 "tags": ["Unauthorized Access", "MITRE T1078"],
 "artifacts": [
  {"dataType": "ip", "data": "192.168.1.39", "message": "Observed source IP"},
  {"dataType": "hostname", "data": "Server-Y", "message": "Affected host"},
  {"dataType": "user", "data": "admin", "message": "Compromised account"}
 ],
 "source": "SimulatedAlert",
 "sourceRef": "sim-alert-001"
}
```

- **Ingested the alert via cURL:**

```
curl -X POST http://192.168.1.35:9000/api/alert \
-H "Authorization: Bearer <API_KEY>" \
-H "Content-Type: application/json" \
-d @unauthorized_mockalert.json
```



2: Generated Alert

Alert successfully ingested and confirmed in TheHive with status New and artifacts attached.

Initial Triage (Tier 1 Actions)

- Reviewed artifacts: IP 192.168.1.39, Host Server-Y, User admin.
- Simulated containment: Server-Y isolated from the network.
- Reviewed logs: Authentication and firewall logs checked.
- Added notes in alert: Documented findings and containment actions.

Escalation to Tier 2

Prepared a 100-word escalation summary for Tier 2 analysts.

Escalation Summary (100 words):

A high-priority alert was triggered for unauthorized access on Server-Y, detected at 2025-09-03 01:31 from IP 192.168.1.39 (MITRE T1078 – Valid Accounts). Initial triage was performed by Tier 1: Server-Y was isolated from the network to prevent lateral movement, authentication and firewall logs were reviewed, and artifacts including the source IP, affected hostname, and compromised user account were documented. Tier 2 is requested to conduct a detailed forensic analysis, assess potential credential compromise, check for malware or backdoors, and implement remediation measures. All findings should be logged in the alert for further review.

SITREP Draft in Google Docs

Title: Unauthorized Access on Server-Y

Summary: Detected at 2025-09-03 01:31, IP: 192.168.1.39, MITRE T1078

Actions: Isolated server, escalated to Tier 2

The SITREP includes:

1. Incident Overview

An unauthorized login attempt was detected on Server-Y, originating from IP 192.168.1.39. This activity aligns with MITRE ATT&CK technique T1078 (Valid Accounts).

The alert was classified as High severity due to the potential for credential misuse and lateral movement.

2. Triage Actions

Tier 1 analysts performed initial triage: Server-Y was isolated from the network to contain potential spread, logs were reviewed for suspicious authentication attempts, and the affected user account (admin) was flagged for further investigation.

3. Escalation Summary

A structured 100-word escalation report was drafted and shared with Tier 2. It highlighted the detection timestamp, affected host, source IP, compromised account, and containment steps. Tier 2 was tasked with deeper forensic analysis and remediation.

4. Recommended Next Steps

Tier 2 should validate whether credentials were stolen, scan the server for persistence mechanisms or malware, and review authentication logs across other servers. Password resets and additional monitoring should be enforced.

5. Notes (mock simulation context)

This SITREP was created as part of a training exercise. No real-world systems were compromised. The workflow focused on practicing escalation procedures and structured reporting using TheHive and Google Docs.

Workflow Automation: Auto-Assign High-Priority Alerts to Tier 2

To demonstrate automation of the incident escalation process, a simple Python script was used to simulate a Splunk Phantom (SOAR) playbook. The script automatically assigns high-priority alerts to Tier 2 analysts, allowing the SOC to streamline response workflows without manual intervention.

Python Script Example:

phantom_playbook_auto_assign.py

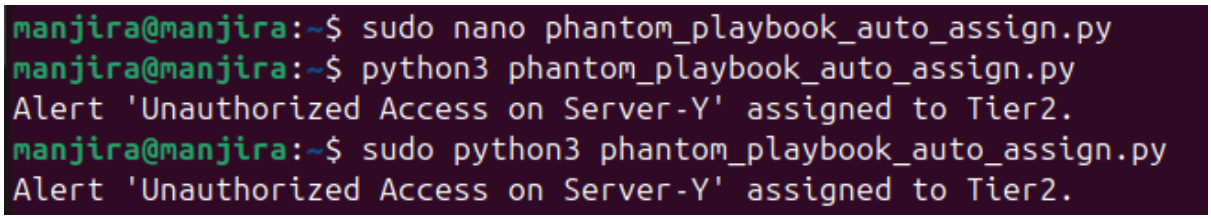
```
alert = {
    "title": "Unauthorized Access on Server-Y",
    "severity": 3
}
tier_assigned = "Tier2"

# Simulate automation broker/playbook assignment
print(f"Alert '{alert['title']}' assigned to {tier_assigned}.")
```

Execution and Result:

python3 phantom_playbook_auto_assign.py

Alert 'Unauthorized Access on Server-Y' assigned to Tier2.



3: Playbook Python Script

Attempts to use Automation Broker CLI also failed due to lack of access to the required Docker images and package installation issues in the current environment.

As a result, the Python script was used as a mock simulation to represent the workflow logic of auto-assigning alerts to Tier 2 analysts.

Troubleshooting

- Could not link alert to case in TheHive (limitation of current setup).
- Workaround: treated case and alert as related but independent objects.
- Alert ingestion required correcting JSON structure (severity as integer, artifacts instead of observables, sourceRef mandatory).
- Pre-deploy checks failing due to insufficient disk space (required ≥500 GiB, only 29 GiB available).
- Errors with systemd daemon reload during installation.

References

- TheHive Project Documentation: https://docs.strangebee.com
- MITRE ATT&CK Technique T1078 – Valid Accounts: https://attack.mitre.org/techniques/T1078/
- Splunk SOAR (Phantom): https://www.splunk.com/en_us/software/soar.html