FUTURE_CS_02

Security Alert Monitoring & Incident Response

Name Aditya Khonde
Intern Domain :- Cyber Security Intern
Tools Used :-Splunk Cloud and sample log file

Introduction

Cybersecurity threats are constantly evolving, and organizations must be prepared to detect, monitor, and respond to security incidents in real time. **Security Alert Monitoring and Incident Response (IR)** are core functions of a Security Operations Center (SOC) that help in minimizing risk, ensuring compliance, and maintaining business continuity.

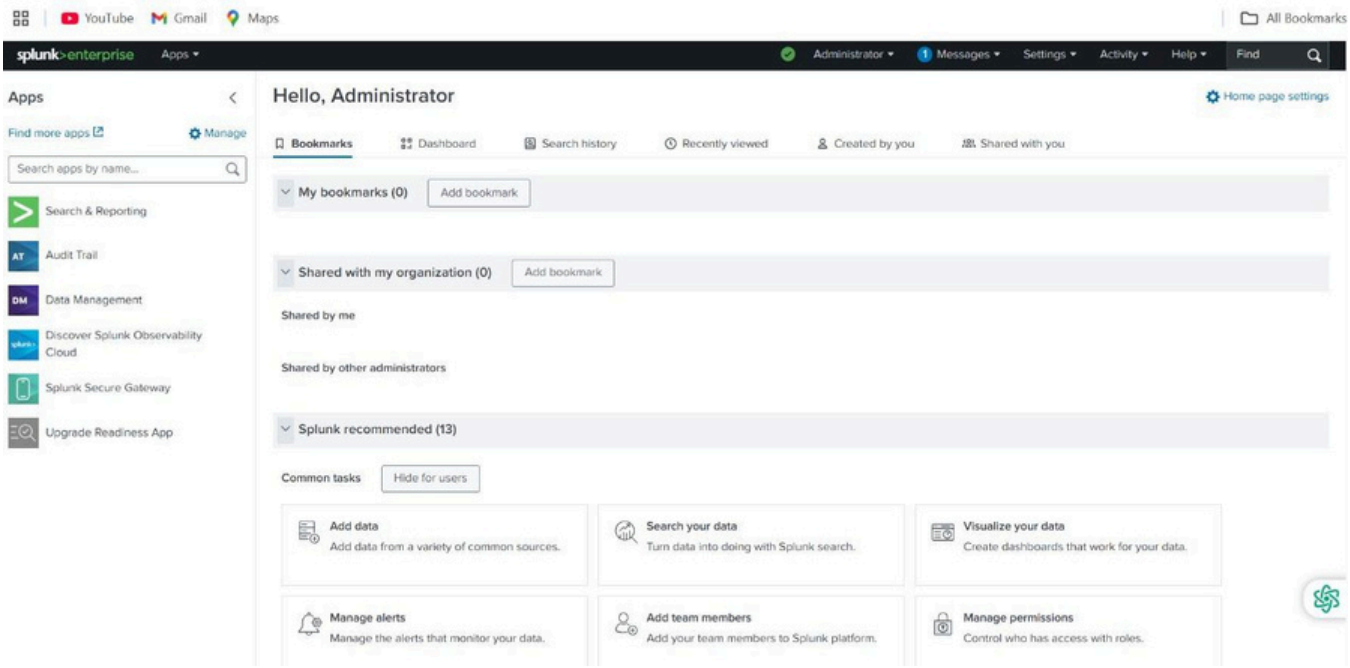
This report demonstrates the use of **Splunk Cloud (Free Trial)** to ingest and analyze logs for security alert monitoring, with a focus on malware detection, failed logins, brute-force attempts, and suspicious IP activity.

Objective

- Ingest and analyze sample security logs using Splunk Cloud.
- Detects abnormal patterns such as multiple failed login attempts, malware infections, and brute-force attacks.
- Configure alerts for suspicious activities.

Tools & Environment

- **Splunk Cloud Free Trial**: Used for log ingestion, queries, dashboards, and alerts.
- **Custom SecurityLogs** : Simulated authentication events, brute-force attempts, and malware detections.



Splunk Cloud Tool :- Splunk Cloud is a cloud-based SIEM (Security Information and Event Management) and data analytics platform provided by Splunk. Instead of installing and managing Splunk on your own servers, you use Splunk as a hosted service on the cloud.

Use Cases

- **Security Monitoring** (SIEM) → Detect brute-force, malware, suspicious IPs.
- **IT Operations** → Monitor system logs, uptime, and errors.
- **DevOps** → Debugging application logs, performance monitoring.
- **Business Analytics** → User behavior tracking, fraud detection.

Methodology

1. Log Collection

A sample dataset (samplesplunklog.csv) was created containing events such as:

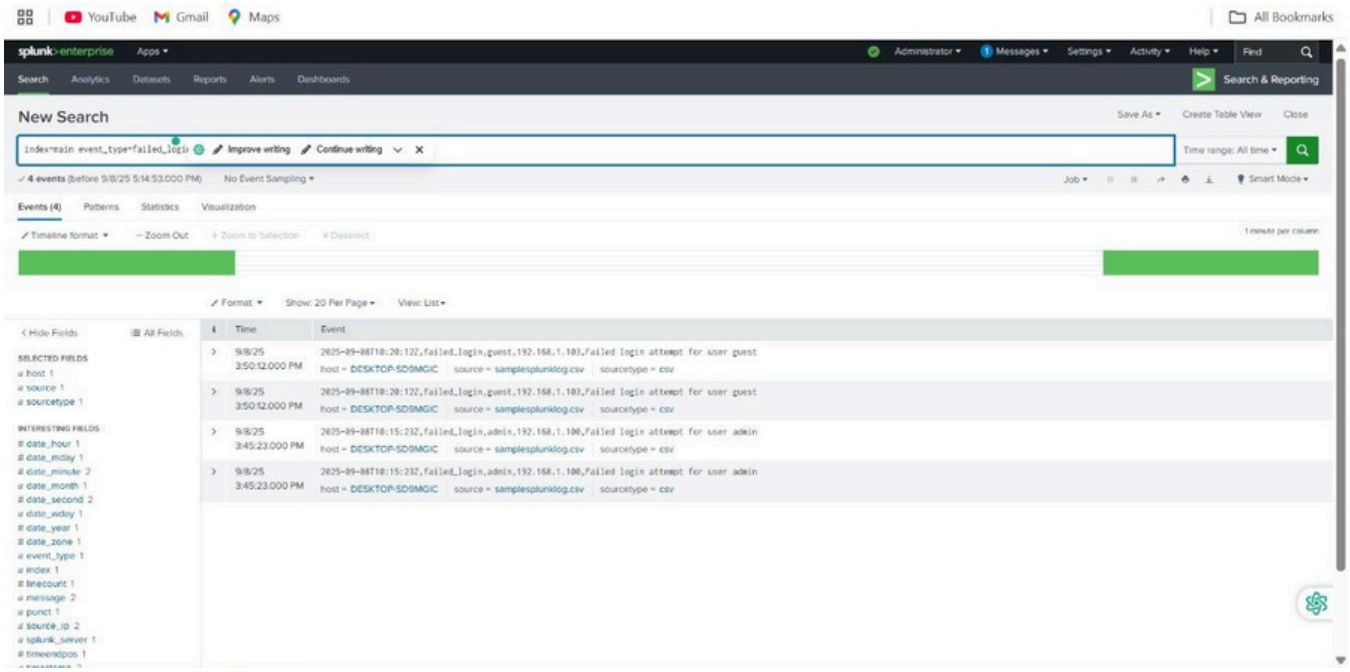
- Failed logins
- Successful logins
- Brute-force attempts
- Malware detections (Trojan, Worms, Ransomware, etc.)

The dataset was uploaded into Splunk Cloud using the**Add Data** → **Upload File** option.

2. Log Analysis (SPL Queries)

Some example Splunk SPL queries used for analysis:

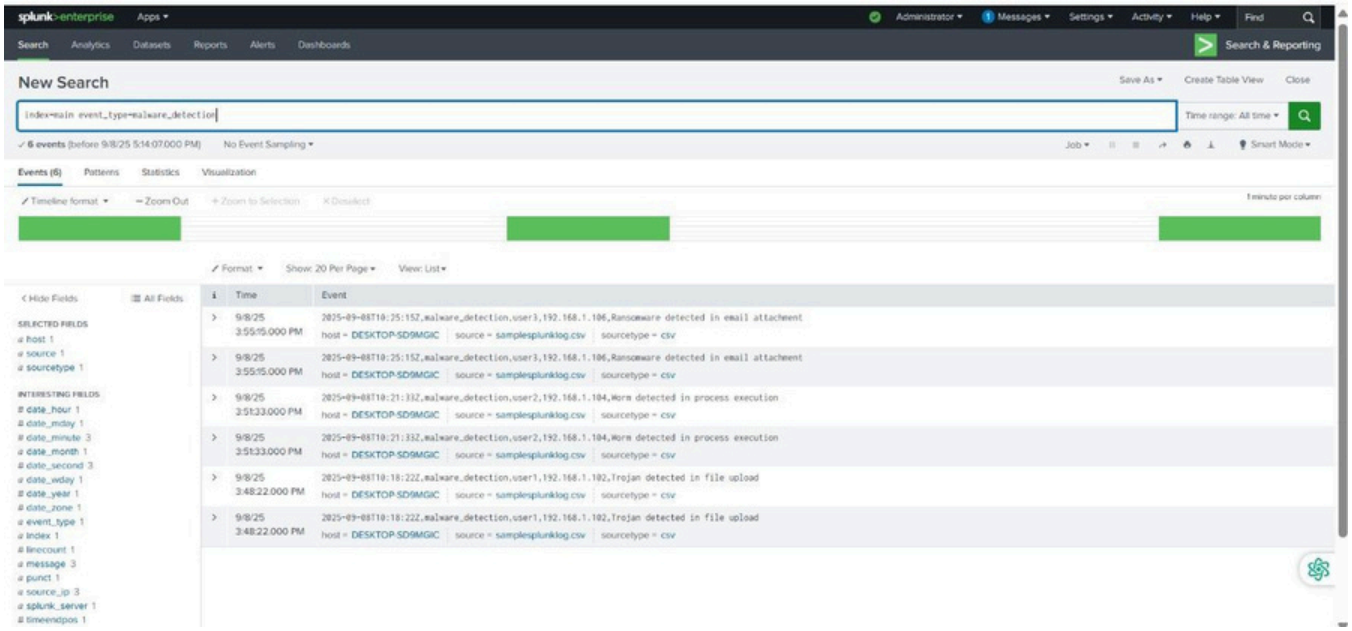
- **Detect multiple failed logins from the same IP.** (Bruteforce attack Possibility)




```
index=main action="login" status="failed"
| stats count by user, src_ip
| where count > 5
```

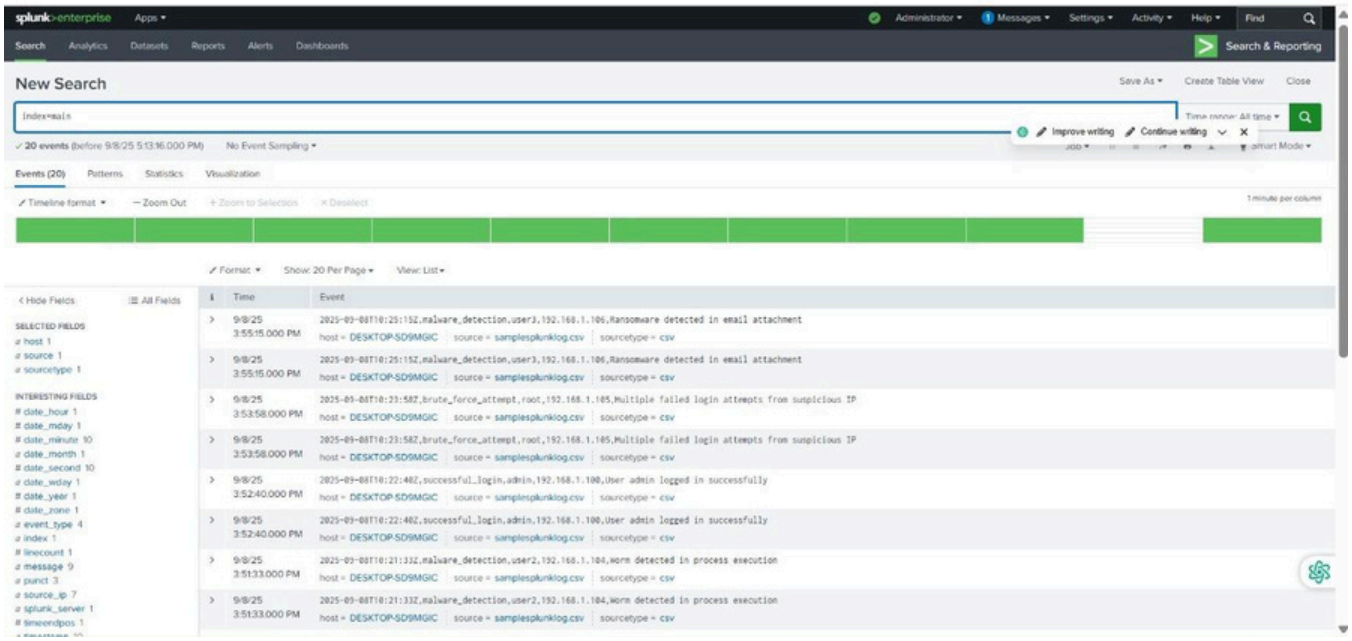
- **List all malware detections**:

  index=main action="malware_detection"
  | stats count by src_ip, signature, severity



- **Show all logs**

  index=”main”



Steps to Create an Alert in Splunk

1. **RunaSearch / SPL Query**
    - Go to **Search &Reporting** app.

Enter your SPL query (e.g., failed logins in the last 10 minutes):

```
 index=security_logs action="login" status="failed"
| stats count by src_ip, user
| where count > 5
```

    - This query finds users or IPs with more than 5 failed login attempts.
    - **Save As Alert**
    - After running the query → click **Save As** → select **Alert**.

2. **Configure Alert Settings**

    - **Title**: e.g., *Brute Force Login Alert*
    - **Description**: "Triggered when more than 5 failed logins are detected from the same IP within 10 minutes."
    - **Permissions**: Private or shared with the team.

3. **Define Alert Type**

    - **Scheduled Alert** → Runs on a fixed interval (e.g., every 5 minutes, every hour).
    - **Real-Time Alert** → Fires as soon as matching events occur.
      (Forsecurity monitoring,scheduledalertsevery5–15minutesarecommonto reduce noise.)

5. **Set Trigger Conditions**
    - Trigger when **Number of Results > 0**
    - Or when **Custom Condition is Met** (e.g., `count > 5`).

6. **Add Actions**
    - You can configure Splunk to:
        - **Send Email** to your SOC team
          Webhook/Script (e.g., notify Slack, Microsoft Teams, PagerDuty)
        - **Add to Incident Dashboard**

7. **Save & Test**
    - Save the alert.
    - Trigger it with test data (e.g., insert multiple failed login events).

3. Incident Response Workflow

- **Detection**: Alert triggered for multiple failed logins.
- **Analysis**: Investigated IPs using Splunk dashboards.
- **Containment**: Blocked malicious IP addresses at the firewall.
- **Eradication**: Reset compromised accounts and enforced MFA.
- **Recovery**: Monitored logs for reoccurrence and tuned Splunk alerts.

Conclusion

This task demonstrated how **Splunk Cloud** can be leveraged for **Security Alert Monitoring & Incident Response**. By simulating real-world attack patterns, it showcased:

- Proactive detection of threats.
- Streamlined incident response.
- The importance of automation in modern SOC environments.

Even with a trial environment and synthetic logs, Splunk provided valuable insights, proving its utility for both learning and enterprise-level defense

What I Learned

- How to **set up and use Splunk Cloud** (free trial) for log ingestion and analysis.
- The importance of **structured log data** (CSV format) for effective search and visualization.
- Writing **SPL queries** to detect failed logins, brute-force attempts, and malware infections.
- The step-by-step process of **Incident Response**: Detection → Analysis → Containment → Eradication → Recovery.
- Gained practical understanding of how a **SOC team monitors security events** in real time.
- Learned the value of **proactive monitoring and automation** in strengthening cybersecurity defenses.