SOC Incident Detection & Analysis using SIEM (Splunk)

Objective

To simulate a real-world Security Operations Center (SOC) environment by collecting Windows security logs, detecting brute-force login attempts, creating alerts, and documenting the incident using Splunk SIEM.

Tools and Technologies Used

- SIEM Tool: Splunk Enterprise (Free Version)
- Operating System: Windows 10 Pro
- Log Source: Windows Security Event Logs
- Framework: MITRE ATT&CK

Project Environment

Component	Details
Machine Type	Personal laptop
OS	Windows 10 Professional
SIEM	Splunk Enterprise Free
Data Source	Local Windows Security Logs

Data Collection Setup

1. Installed Splunk Enterprise on Windows.
2. Logged into Splunk web interface.
3. Navigated to:
4. Settings → Add Data → Monitor
5. Selected:
6. Local Event Logs → Security
7. Enabled collection of Windows security events.

Result:

Splunk started collecting login-related events.

Attack Simulation

To simulate a brute-force scenario:

1. Locked the system using:
2. Windows + L
3. Entered incorrect password multiple times.
4. Generated:
    - EventCode 4625 (failed login attempts)
5. Logged in successfully once:
    - EventCode 4624 (successful login)

Log Analysis in Splunk

Failed Login Detection

Query used:

index=main Event Code=4625

Result:

- Multiple failed login events detected.

Successful Login Detection

Query used:

index=main EventCode=4624

Result:

- Successful login event detected after failures.

Suspicious Account Identification

Query used:

index=main EventCode=4625

| stats count by Account_Name

Result:

- Identified accounts with multiple failed attempts.

Brute-Force Detection Rule

Query used:

index=main EventCode=4625

| stats count by Account_Name

| where count > 5

Result:

- Detected suspicious account with more than 5 failed logins.

Alert Configuration

1. Converted detection query into an alert.
2. Alert settings:

Parameter	Value
Alert Name	Brute Force Detection
Alert Type	Scheduled
Trigger Condition	If results > 0
Severity	Medium
Action	Add to Triggered Alerts

Incident Investigation

Observed:

Field	Value (Example)
Account Name	Moorthy
EventCode	4625
Failed Attempts	18
Time Range	Short interval

Field	Value (Example)
Source Network Address	127.0.0.1

Conclusion:

- Multiple failed logins detected.
- Indicates brute-force attempt.

MITRE ATT&CK Mapping

Category	Value
Tactic	Credential Access
Technique ID	T1110
Technique Name	Brute Force

Reason:

- Multiple failed login attempts indicate password-guessing activity.

Incident Summary

A brute-force login attempt was detected on a user account.
Multiple failed login attempts were observed within a short time frame, indicating suspicious credential access activity.

Severity Assessment

Severity Level: Medium

Reason:

- Multiple failed login attempts detected.
- No confirmed system compromise.

Recommended Actions

- Reset affected user password.
- Enable account lockout policy.
- Enable multi-factor authentication (MFA).
- Monitor login attempts continuously.

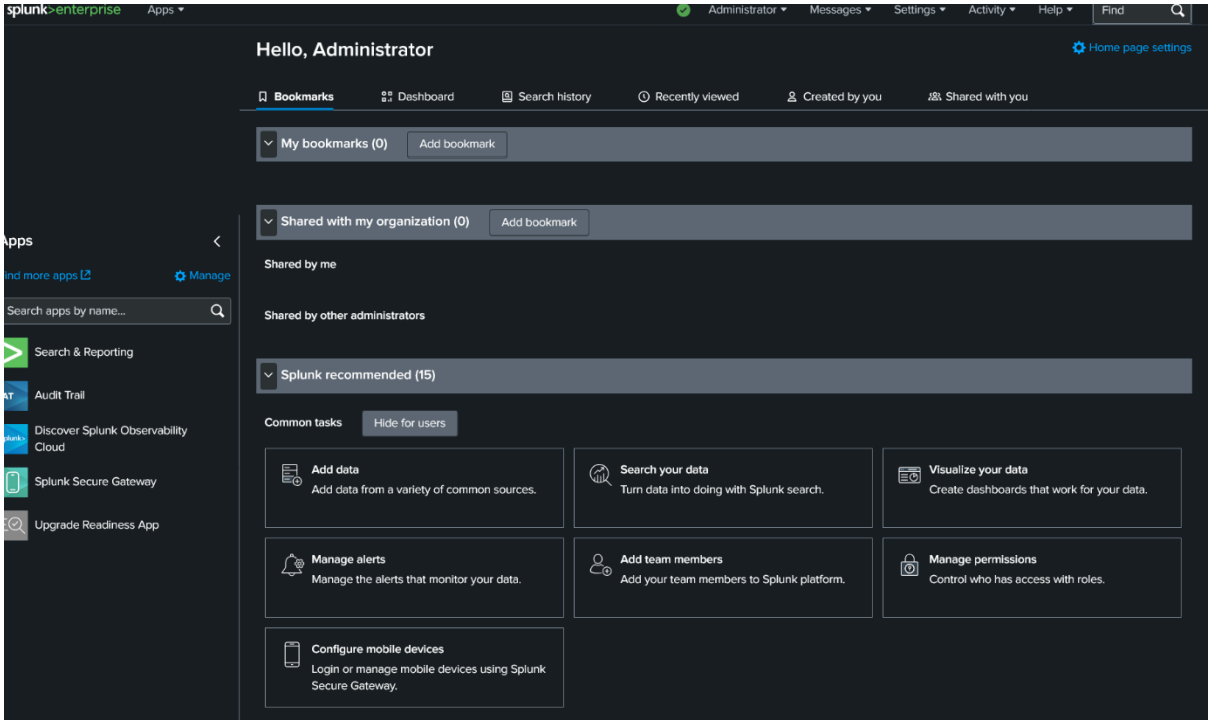
Conclusion

This project demonstrated:

- Log collection using Splunk SIEM
- Detection of brute-force login attempts
- Alert creation and monitoring
- Incident investigation
- MITRE ATT&CK mapping

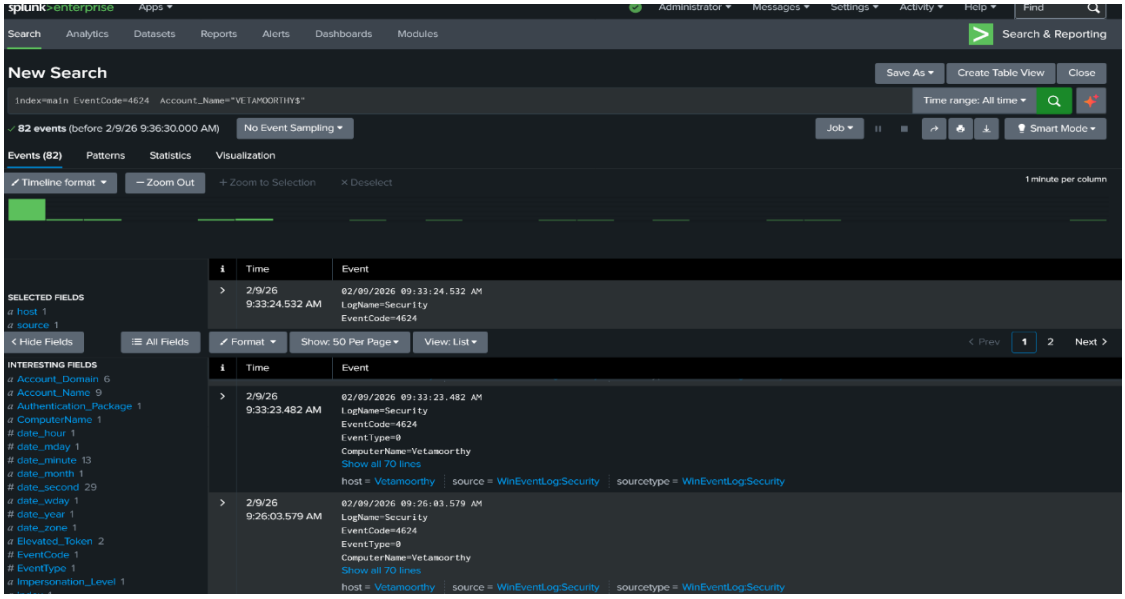
The project simulated a real SOC workflow for entry-level security operations.

Splunk Dashboard



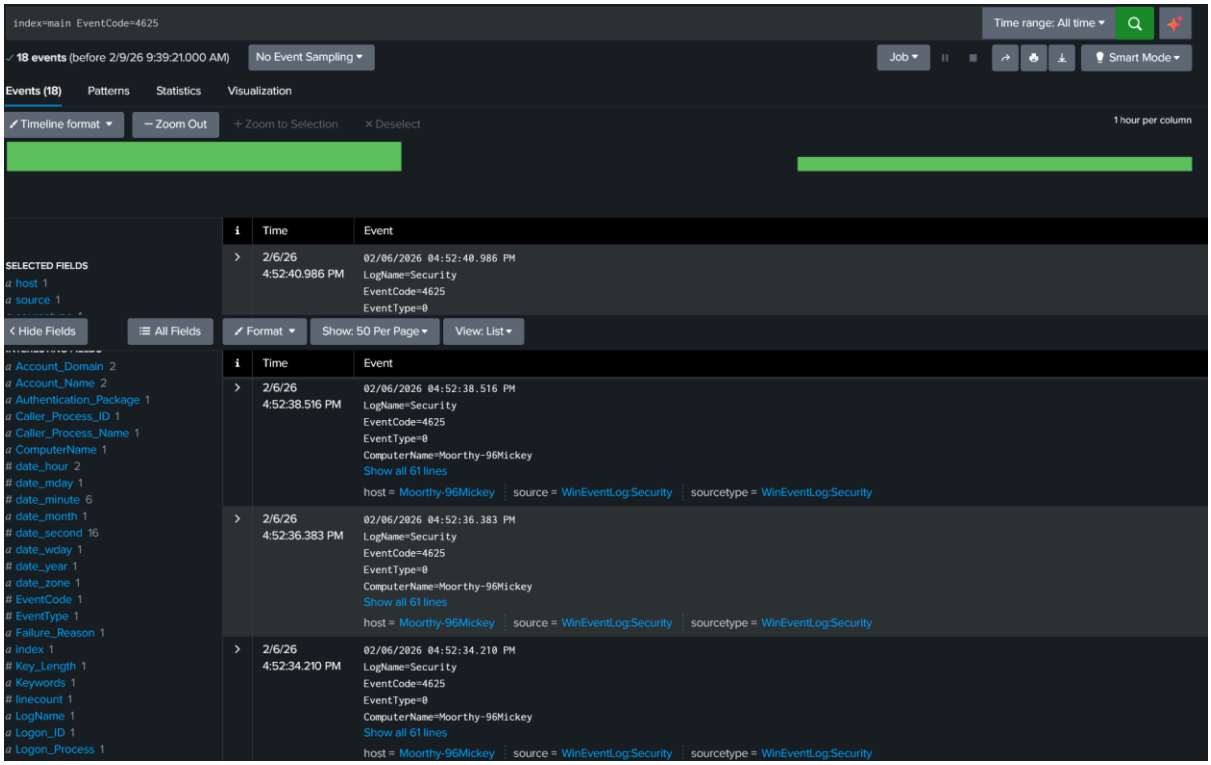
Displaying the Splunk Dashboard.

Successful Login



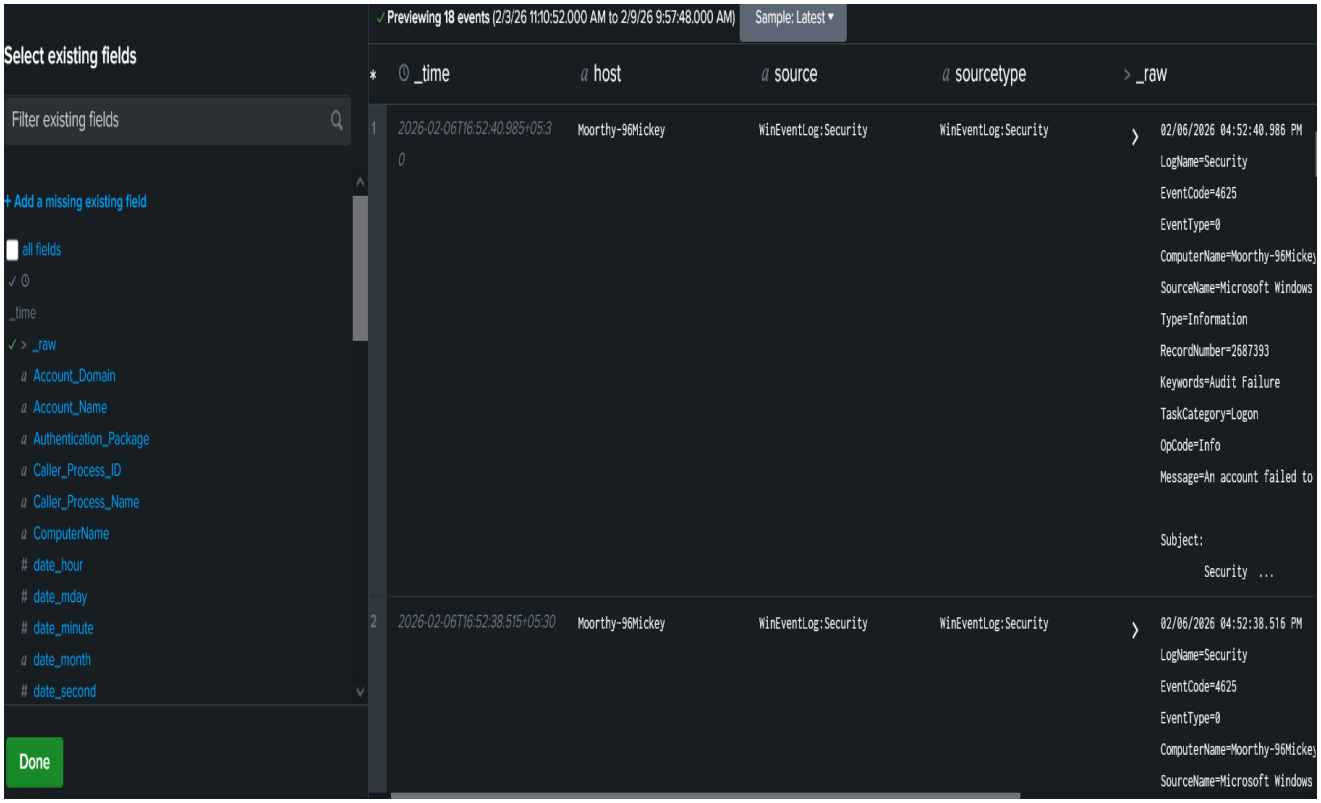
The user's successful login logs are displayed on the page.

Failed Login



This picture shows the Failed Login logs on the given page.

Failed Login table



This image shows the Failed logs on the table format.