

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

The screenshot shows the Splunk Enterprise dashboard. At the top, it says "Hello, Administrator". Below the header are navigation links: Bookmarks, Dashboard, Search history, Recently viewed, Created by you, and Shared with you. A "Find" search bar is also present. On the left, there's a sidebar titled "Apps" with sections for "Search & Reporting" (Audit Trail, Discover Splunk Observability Cloud, Splunk Secure Gateway, Upgrade Readiness App), "Find more apps", and a "Manage" link. The main content area is titled "Splunk recommended (15)" and contains several cards: "Add data" (Add data from a variety of common sources.), "Search your data" (Turn data into doing with Splunk search.), "Visualize your data" (Create dashboards that work for your data.), "Manage alerts" (Manage the alerts that monitor your data.), "Add team members" (Add your team members to Splunk platform.), and "Configure mobile devices" (Login or manage mobile devices using Splunk Secure Gateway.).

Displaying the Splunk Dashboard.

Successful Login

The screenshot shows the Splunk Enterprise interface with a search titled "Successful Login". The search bar contains the query "index=main EventCode=4624 Account_Name='VETAMOORTHY\$'". The results table has three columns: Time, Event, and a third column which is partially visible. The first event is selected, showing details: Time is 2/9/26 09:33:24.532 AM, LogName=Security, EventCode=4624. The second event shows similar details: Time is 2/9/26 09:33:23.482 AM, LogName=Security, EventCode=4624. The third event shows: Time is 2/9/26 09:26:03.579 AM, LogName=Security, EventCode=4624. The interface includes a sidebar with "SELECTED FIELDS" and "INTERESTING FIELDS" sections, and a bottom navigation bar with tabs like Events (82), Patterns, Statistics, and Visualization.

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

Failed Login

The screenshot shows a Splunk search interface with the following details:

- Time range:** All time
- Events (18):** (before 2/9/26 9:39:21.000 AM)
- No Event Sampling:** No sampling is applied.
- Event Fields:** The table lists several event fields:
 - SELECTED FIELDS:** host, source
 - Available Fields:** Account_Domain, Account_Name, Authentication_Package, Caller_Process_ID, Caller_Process_Name, ComputerName, date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year, date_zone, ErrorCode, EventCode, EventType, Failure_Reason, index, Key_Length, Keywords, lincount, LogName, Logon_ID, Logon_Process.
- Event Data:** The table displays 18 events, each with a timestamp, event type, and detailed log information. The first few events are:
 - 2/6/26 4:52:40.986 PM: LogName=Security, EventCode=4625, EventType=0, ComputerName=Moorthy-96Mickey, host = Moorthy-96Mickey, source = WinEventLog:Security, sourcetype = WinEventLog:Security
 - 2/6/26 4:52:38.516 PM: LogName=Security, EventCode=4625, EventType=0, ComputerName=Moorthy-96Mickey, host = Moorthy-96Mickey, source = WinEventLog:Security, sourcetype = WinEventLog:Security
 - 2/6/26 4:52:36.383 PM: LogName=Security, EventCode=4625, EventType=0, ComputerName=Moorthy-96Mickey, host = Moorthy-96Mickey, source = WinEventLog:Security, sourcetype = WinEventLog:Security

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

Failed Login table

Previewing 18 events (2/3/26 11:10:52.000 AM to 2/9/26 9:57:48.000 AM) Sample: Latest ▾					
Select existing fields	*	_time	host	source	sourcetype
Filter existing fields	<input type="text"/>	1 2026-02-06T16:52:40.985+05:30	Moorthy-98Mickey	WinEventLog:Security	WinEventLog:Security
+ Add a missing existing field		0			
<input type="checkbox"/> all fields					> 02/06/2026 04:52:40.986 PM
✓ ①					LogName=Security
_time					EventCode=4625
✓ > _raw					EventType=0
a Account_Domain					ComputerName=Moorthy-98Mickey
a Account_Name					SourceName=Microsoft Windows
a Authentication_Package					Type=Information
a Caller_Process_ID					RecordNumber=2887393
a Caller_Process_Name					Keywords=Audit Failure
a ComputerName					TaskCategory=Logon
# date_hour					OpCode=Info
# date_mday					Message=An account failed to
# date_minute		2 2026-02-06T16:52:38.515+05:30	Moorthy-98Mickey	WinEventLog:Security	Subject:
a date_month					Security ...
# date_second					
Done					

This image shows the Failed logs on the table format.