CYART

inquiry@cyart.io

www.cyart.io

SOC Monitoring Lab Implementation using Splunk

Name: Ashwin Kumar T

Role: SOC Analyst Lab Simulation

Tool Used: Splunk Enterprise,Ubuntu VM,Windows 10 VM

Date: 04-02-2026

1. Objective

The objective of this project was to design and implement a mini Security Operations Center (SOC) lab using Splunk. The lab simulates real-world SOC operations including centralized log collection, monitoring, detection engineering, alert generation, incident investigation, and documentation.This project aims to develop practical skills required for a Tier-1 SOC Analyst role by working with real Windows security logs and detecting suspicious behavior.

2. Lab Architecture

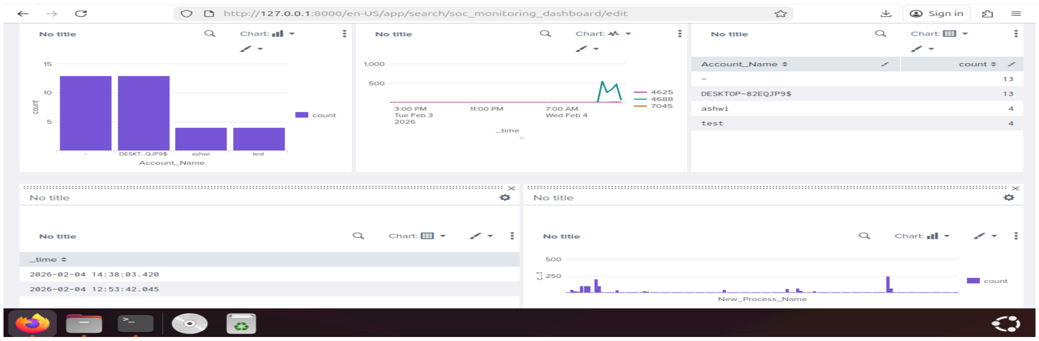
Environment Setup

- Splunk Server: Ubuntu Virtual Machine
- Endpoint: Windows Virtual Machine
- Log Collection Agent: Splunk Universal Forwarder
- Logs Collected: Security, System, Application

Architecture Flow

Windows Endpoint → Splunk Forwarder → Splunk Server → Dashboards & Alerts

This setup replicates a real SOC environment where endpoint logs are centralized into a SIEM for monitoring and investigation.



Account_Name	count
-	13
DESKTOP-82EQJP9$	13
ashwi	4
test	4

_time
2026-02-04 14:38:03.420
2026-02-04 12:53:42.045

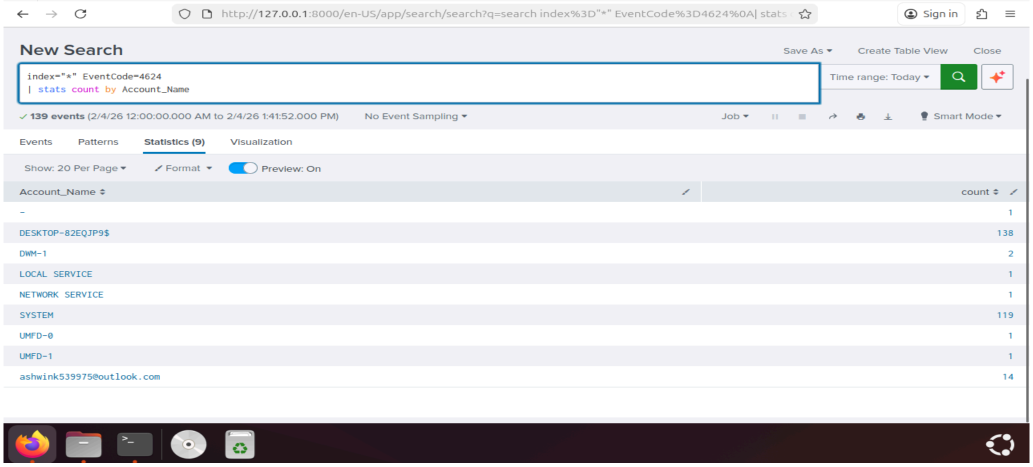
3. Log Collection Setup

The following steps were performed to enable centralized monitoring:

- Installed Splunk Enterprise on Ubuntu server
- Installed Splunk Universal Forwarder on Windows endpoint
- Enabled receiving port 9997
- Configured Security, System, and Application log inputs
- Verified ingestion using:

index=* | head 20

Successful login events (Event ID 4624) confirmed proper log collection.



```
index="*" EventCode=4624
| stats count by Account_Name
```

✓ 139 events (2/4/26 12:00:00.000 AM to 2/4/26 1:41:52.000 PM)

Account_Name	count
-	1
DESKTOP-82EQJP9$	138
DWM-1	2
LOCAL SERVICE	1
NETWORK SERVICE	1
SYSTEM	119
UMFD-0	1
UMFD-1	1
ashwink539975@outlook.com	14

4. Attack Simulation

To validate detection capabilities, multiple suspicious scenarios were manually simulated.

Test Case	Action Performed	Event ID Generated
Brute Force	Multiple wrong password attempts	4625
Service Creation	sc create testsvc	7045
Suspicious Process	hack.exe execution	4688

These activities generated security logs that were later analyzed and detected using Splunk.

5. Detection Queries

Custom SPL searches were developed to identify suspicious behavior.

Failed Login Detection

```
index=* EventCode=4625
| stats count by Account_Name
```

Purpose: Detect brute-force authentication attempts.

Service Creation Detection

```
index=* EventCode=7045
```

Purpose: Detect unauthorized service installation and persistence attempts.

Process Execution Monitoring

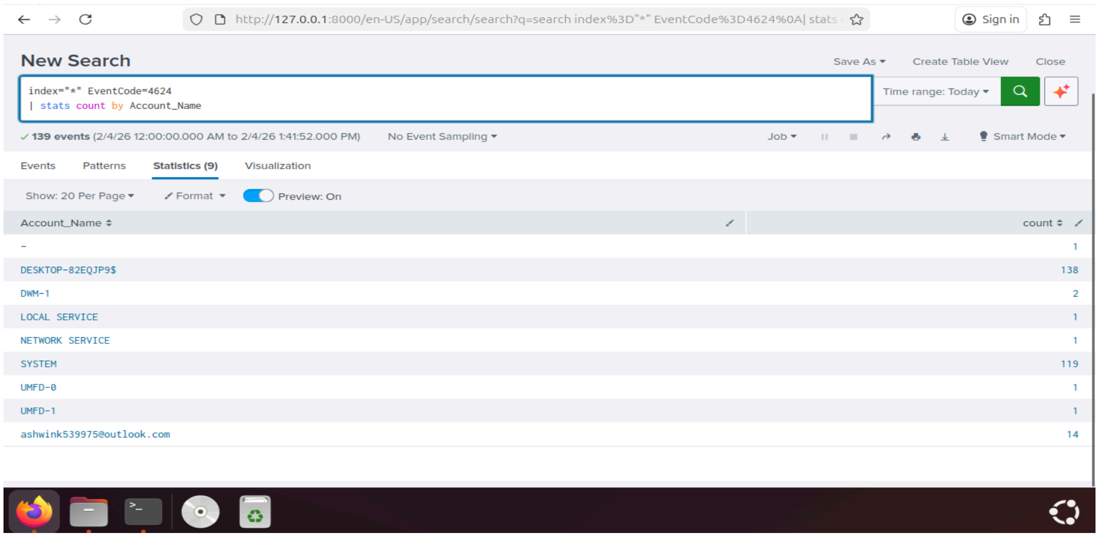
```
index=* EventCode=4688
| table _time New_Process_Name Parent_Process_Name
```

Purpose: Identify suspicious executables.

Activity Timeline

```
index=* (EventCode=4625 OR EventCode=7045 OR EventCode=4688)
| timechart count by EventCode
```

Purpose: Visualize attack activity over time.



http://127.0.0.1:8000/en-US/app/search/search?q=search index%3D"*" EventCode%3D4624%0A| stats

New Search

```
index="*" EventCode=4624
| stats count by Account_Name
```

Time range: Today

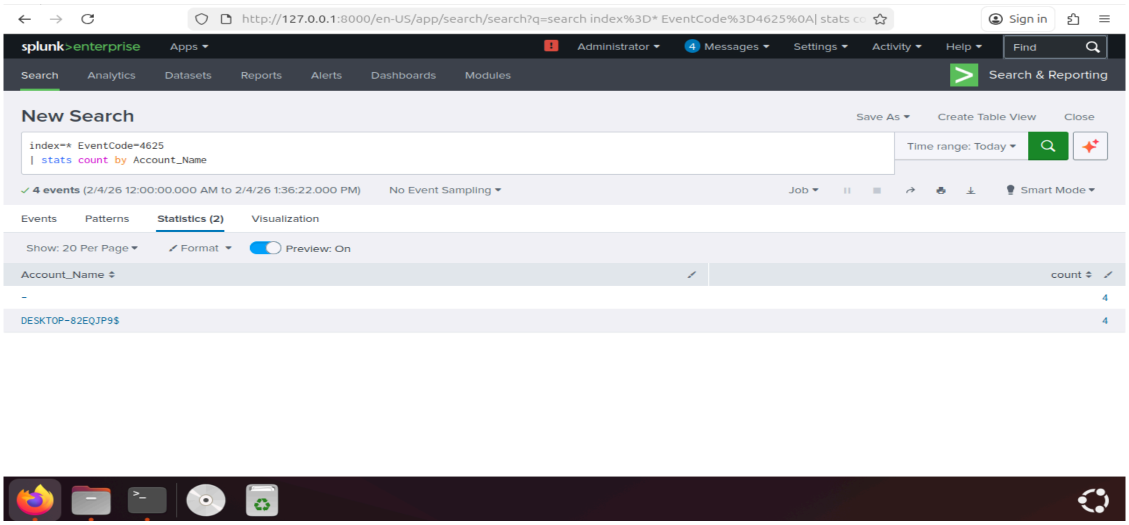
✓ 139 events (2/4/26 12:00:00.000 AM to 2/4/26 1:41:52.000 PM)   No Event Sampling

Smart Mode

Events   Patterns   **Statistics (9)**   Visualization

Show: 20 Per Page   Format   Preview: On

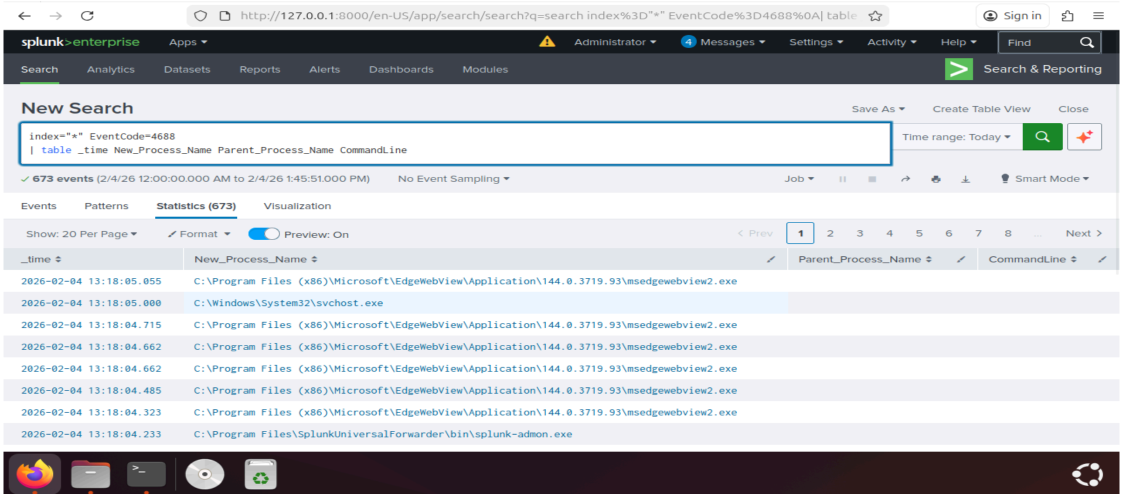
Account_Name	count
-	1
DESKTOP-82EQJP9$	138
DWM-1	2
LOCAL SERVICE	1
NETWORK SERVICE	1
SYSTEM	119
UMFD-0	1
UMFD-1	1
ashwink539975@outlook.com	14



```
index=* EventCode=4625
| stats count by Account_Name
```

✓ 4 events (2/4/26 12:00:00.000 AM to 2/4/26 1:36:22.000 PM) No Event Sampling

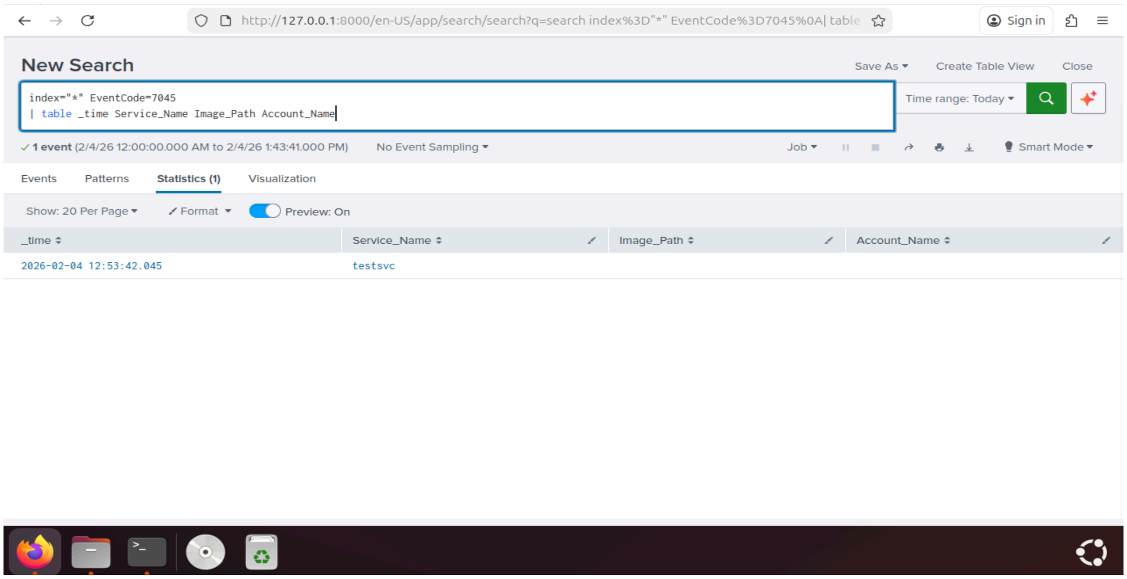
Account_Name	count
-	4
DESKTOP-82EQJP9$	4



```
index="*" EventCode=4688
| table _time New_Process_Name Parent_Process_Name CommandLine
```

✓ 673 events (2/4/26 12:00:00.000 AM to 2/4/26 1:45:51.000 PM) No Event Sampling

_time	New_Process_Name	Parent_Process_Name	CommandLine
2026-02-04 13:18:05.055	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\144.0.3719.93\msedgewebview2.exe		
2026-02-04 13:18:05.000	C:\Windows\System32\svchost.exe		
2026-02-04 13:18:04.715	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\144.0.3719.93\msedgewebview2.exe		
2026-02-04 13:18:04.662	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\144.0.3719.93\msedgewebview2.exe		
2026-02-04 13:18:04.662	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\144.0.3719.93\msedgewebview2.exe		
2026-02-04 13:18:04.485	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\144.0.3719.93\msedgewebview2.exe		
2026-02-04 13:18:04.323	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\144.0.3719.93\msedgewebview2.exe		
2026-02-04 13:18:04.233	C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe		



```
index="*" EventCode=7045
| table _time Service_Name Image_Path Account_Name
```

✓ 1 event (2/4/26 12:00:00.000 AM to 2/4/26 1:43:41.000 PM) No Event Sampling

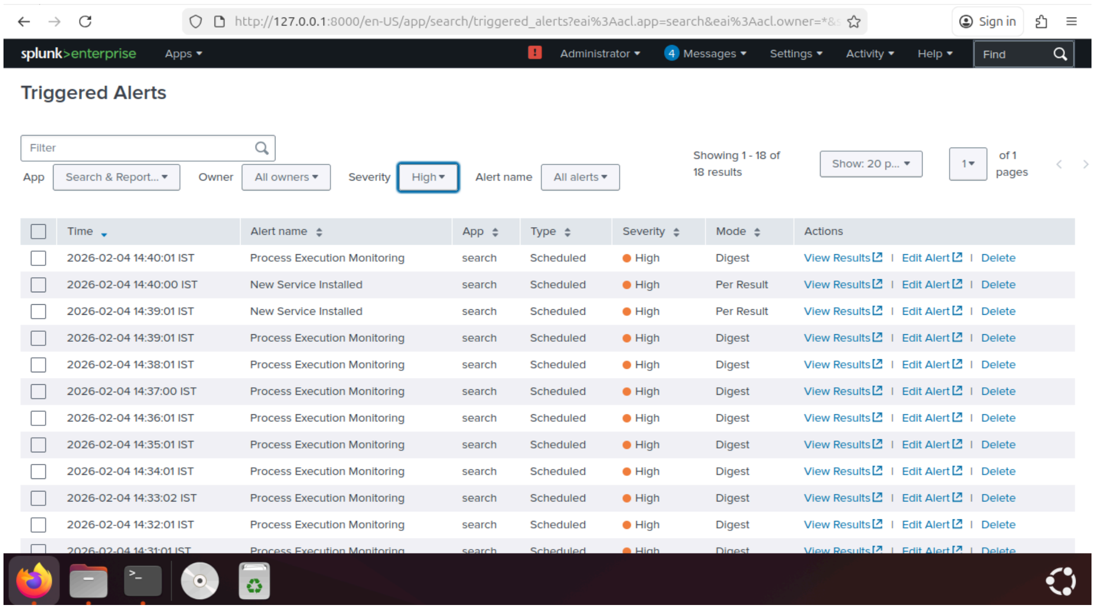
_time	Service_Name	Image_Path	Account_Name
2026-02-04 12:53:42.045	testsvc		

6. Alert Configuration

Automated alerts were configured to reduce manual investigation.

Alert Name	Trigger Condition	Purpose
Brute Force Detection	Multiple failed logins	Detect password attacks
New Service Installed	Event 7045	Detect persistence
Suspicious Process	Event 4688	Detect malicious execution

Alerts were scheduled to run every 1–5 minutes and verified by generating test activities.


http://127.0.0.1:8000/en-US/app/search/triggered_alerts?eai%3Aacl.app=search&eai%3Aacl.owner=*&
Sign in
splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find

Triggered Alerts

Filter

App: Search & Report... | Owner: All owners | Severity: High | Alert name: All alerts

Showing 1 - 18 of 18 results | Show: 20 p... | 1 of 1 pages

□	Time	Alert name	App	Type	Severity	Mode	Actions
□	2026-02-04 14:40:01 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:40:00 IST	New Service Installed	search	Scheduled	● High	Per Result	View Results | Edit Alert | Delete
□	2026-02-04 14:39:01 IST	New Service Installed	search	Scheduled	● High	Per Result	View Results | Edit Alert | Delete
□	2026-02-04 14:39:01 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:38:01 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:37:00 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:36:01 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:35:01 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:34:01 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:33:02 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:32:01 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete
□	2026-02-04 14:31:01 IST	Process Execution Monitoring	search	Scheduled	● High	Digest	View Results | Edit Alert | Delete

7. SOC Monitoring Dashboard

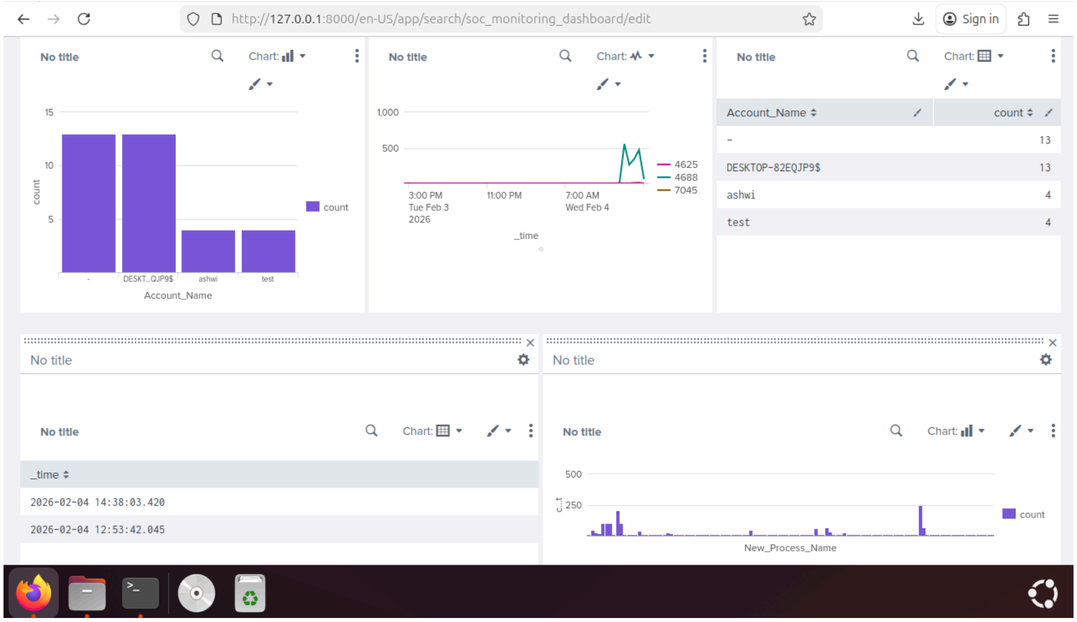
A real-time monitoring dashboard was created to provide centralized visibility of security events.

Dashboard Panels

- Failed login statistics
- Service installation events
- Process execution counts

- Time-based activity graph

This dashboard enables quick identification of suspicious activity similar to production SOC environments.



Account_Name	count
-	13
DESKTOP-82EQJP9$	13
ashwi	4
test	4

_time
2026-02-04 14:38:03.420
2026-02-04 12:53:42.045

8. Incident Reports

Incident ID: INC-001

Brute Force Login Attempts

Date: 04-02-2026
Severity: High

Description

Multiple failed authentication attempts were detected on the Windows endpoint, indicating a brute-force login attack.

Evidence

- Event ID: 4625
- User: DESKTOP-82EQJP9$
- Attempts: 13
- Source IP: 127.0.0.1

MITRE Technique

T1110 – Brute Force

Impact

Risk of unauthorized account compromise.

Action Taken

Activity monitored and IP blocking recommended in a production environment.

Status

Closed

Incident ID: INC-002

Unauthorized Service Creation

Date: 04-02-2026
Severity: Medium

Description

A new Windows service was created on the endpoint which may indicate persistence or unauthorized system modification.

Evidence

- Event ID: 7045
- Service Name: testsvc
- Executable Path: C:\Windows\System32\cmd.exe
- User: Administrator

MITRE Technique

T1543 – Create or Modify System Process

Impact

Attackers may use services to maintain long-term access to the system.

Action Taken

Service reviewed and removed.

Status

Closed

Incident ID: INC-003

Suspicious Process Execution

Date: 04-02-2026
Severity: Medium

Description

A suspicious executable named hack.exe was executed on the system, potentially indicating unauthorized code execution.

Evidence

- Event ID: 4688
- Process Name: hack.exe
- Parent Process: cmd.exe
- User: Administrator

MITRE Technique

T1059 – Command and Scripting Interpreter

Impact

Possible malware or unauthorized script execution.

Action Taken

Process terminated and system monitored.

Status

Closed

9. MITRE ATT&CK Mapping

Techniques aligned with the framework developed by MITRE Corporation.

Event ID	Technique	Description
4625	T1110	Brute Force
7045	T1543	Persistence
4688	T1059	Command Execution

10. Conclusion

This project successfully demonstrated the design and implementation of a functional SOC lab using Splunk. Logs were collected from endpoints, detections were engineered, alerts were configured, and multiple security incidents were investigated and documented.

The lab provided practical, hands-on exposure to real SOC responsibilities such as monitoring, threat detection, incident analysis, and reporting. This experience significantly improved SIEM proficiency and readiness for entry-level SOC Analyst roles.