SOC Fundamentals and Operations

Purpose of a SOC (Security Operations Center):

A SOC is a dedicated unit that continuously monitors, detects, investigates, and responds to cybersecurity incidents.
Its goal is to protect an organization's assets through **proactive threat detection, incident response, and continuous monitoring.**

Key Functions:

Log Analysis: Reviewing collected logs for anomalies or suspicious activities.

Alert Triage: Prioritizing and investigating security alerts.

Threat Intelligence Integration: Using external data sources to identify new and emerging threats.

Incident Response: Taking immediate actions to contain and remediate attacks.

Reporting and Documentation: Maintaining detailed records of incidents and resolutions.

Roles in a SOC:

Role	Responsibility
Tier 1 Analyst (L1)	Monitors alerts, performs initial triage, and escalates true positives.
Tier 2 Analyst (L2)	Conducts deeper investigations, performs correlation and threat hunting.
Tier 3 Analyst (L3)	Handles advanced incidents, malware analysis, and forensic investigations.
SOC Manager	Oversees SOC operations, ensures KPIs are met, and reports to management.
Threat Hunter	Proactively searches for undetected threats using advanced analytics and threat intelligence.

SOC team structure diagram

The image part with relationship ID rId7 was not found in the file.

2. Security Monitoring Basics:

Objectives:

Detect anomalies and unauthorized access.

Identify malware infections or suspicious behaviors.

Monitor compliance and detect policy violations.

Key Metrics:

False Positive: An alert that looks malicious but isn't.

False Negative: A missed alert that was actually malicious.

MTTD (Mean Time to Detect): Average time to identify a threat.

MTTR (Mean Time to Respond): Average time to contain and resolve a threat.

1 Setup in Splunk

1.1 Open Splunk Web → **Add Data** → **Upload Files**

1.2Upload these 3 logs one by one:

windows_security.log

firewall.log

web_access.log

1.3 Assign:

Source type → log

Index → practice

Host → lab1

Click **Start Searching**

Step 2: Basic Detection Queries (SPL)

2.1 Detect Anomalies — multiple failed logins

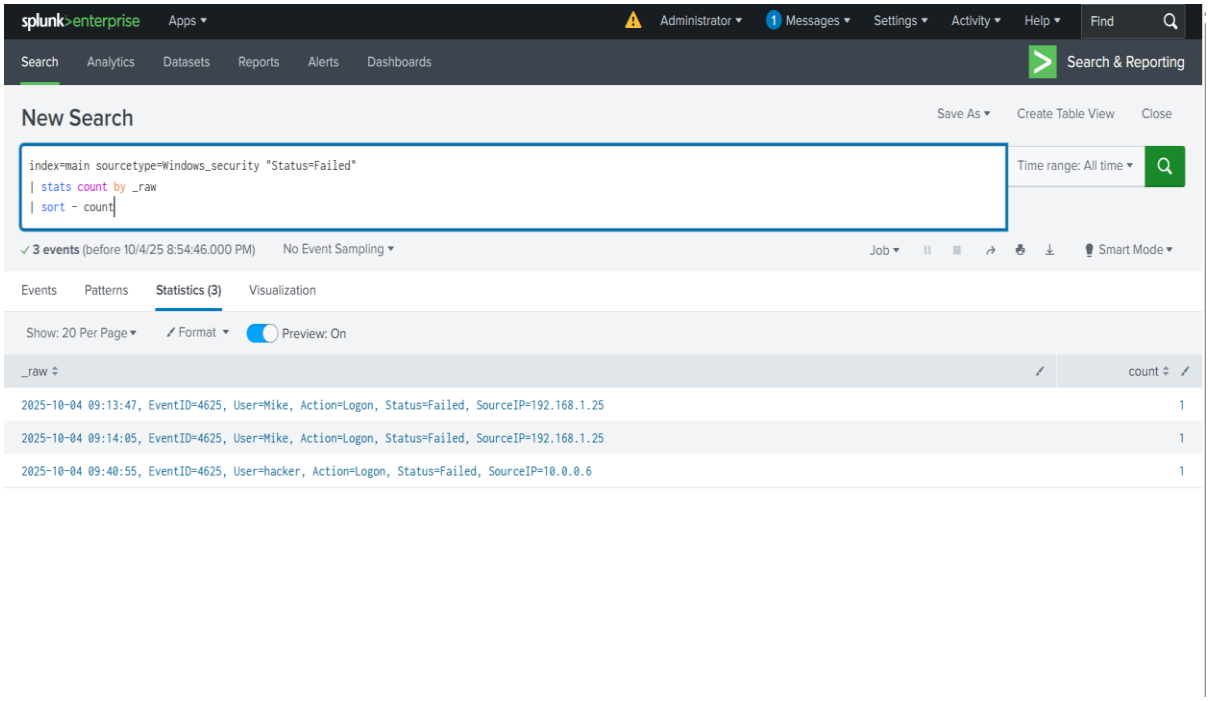
CMD:

index=practice "Status=Failed" OR 401

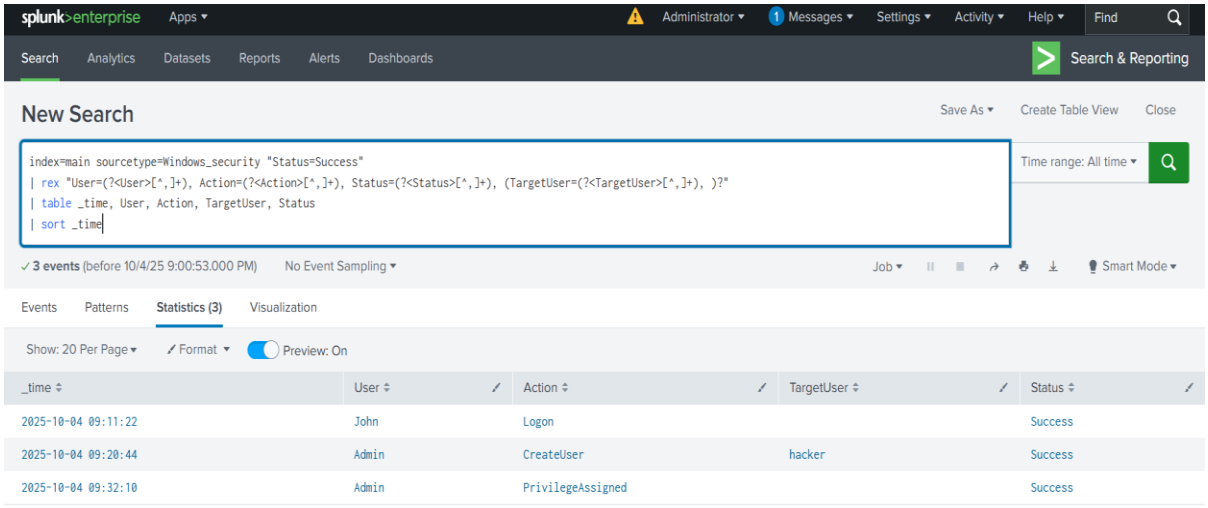
| stats count by User, SourceIP

| where count > 3

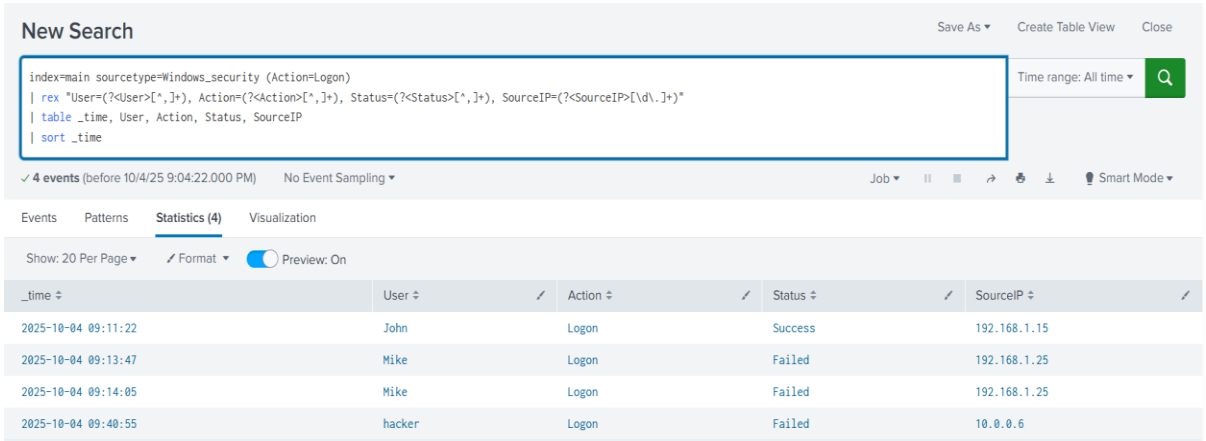
Screenshot:



2.2 Detect Successful Admin Actions



2.3 Detect All Logons



Log Management Fundamentals:

1.1 Objective

To understand how logs are collected, normalized, stored, retained, and analyzed in a SIEM (Splunk).
This task demonstrates the **log lifecycle**, **types of logs**, and **practical querying techniques**.

Log Types Used :

Log File	Description	Source Type
windows_security.log	Windows Event Logs (logons, privilege changes)	Windows_security
web_Acess.log	Web server access logs (HTTP requests)	web_Acess
firewall.log	Network firewall activity logs	firewall

1.2 Normalization in Splunk (Field Extraction):

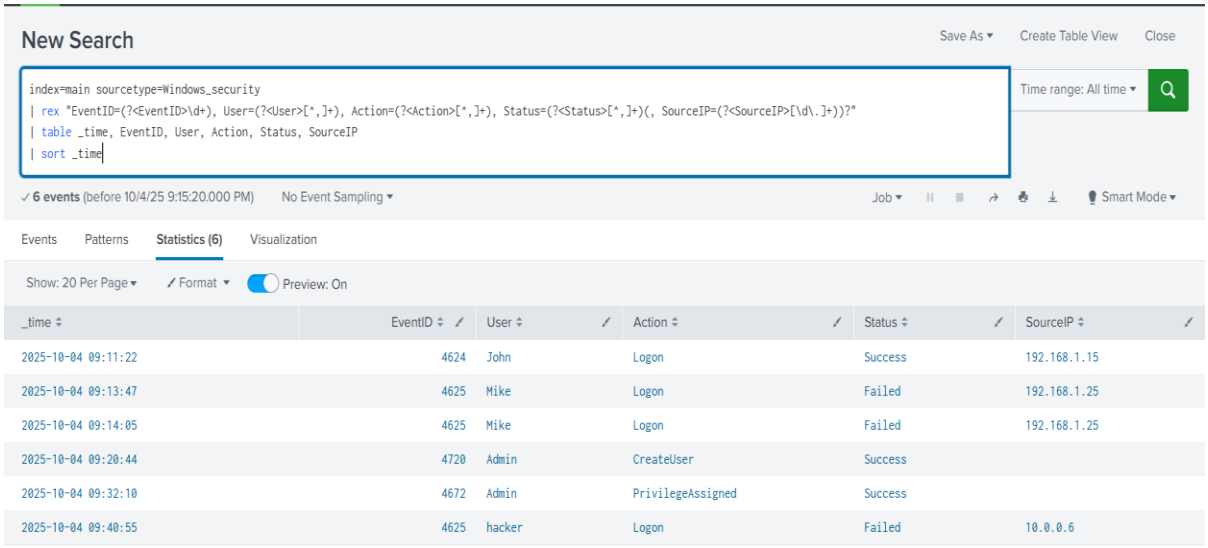
To structure Windows log data into readable columns:

CMD:

```
index=main sourcetype=Windows_security

| rex "EventID=(?<EventID>\d+), User=(?<User>[^,]+), Action=(?<Action>[^,]+), Status=(?<Status>[^,]+)(, SourceIP=(?<SourceIP>[\d\.]+))?"

| table _time, EventID, User, Action, Status, SourceIP

| sort _time
```

This extracts Event ID, User, Action, and Status from raw log text.

Screenshot: Normalized field output in Splunk



1.3 Failed Logins Detection (KQL Equivalent in SPL)

CMD:

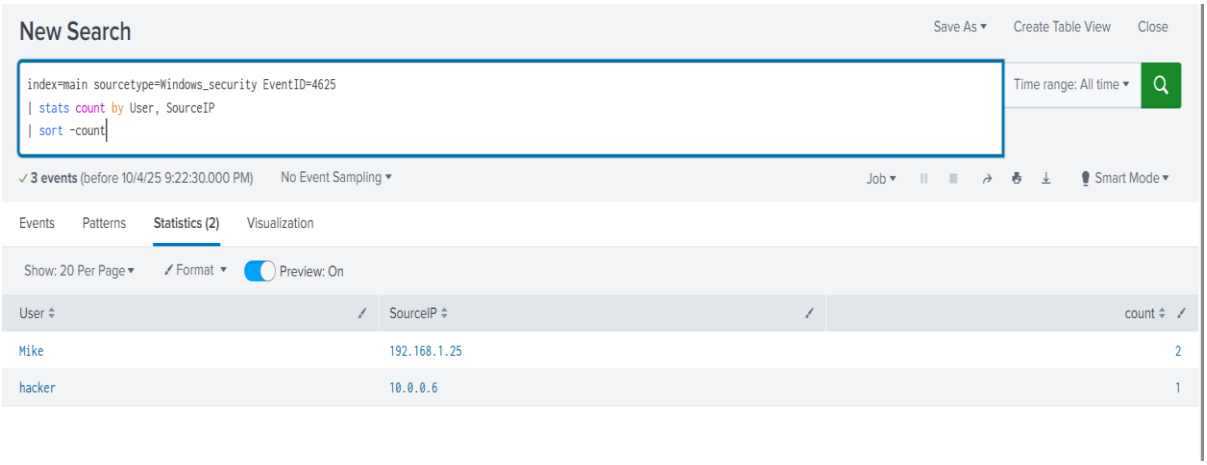
index=main sourcetype=Windows_security EventID=4625

| stats count by User, SourceIP

| sort -count

Detects repeated failed logins from same user/IP.

Screenshot: Failed login count table



1.4 Successful Admin Actions (Policy Violations Example)

Query to find privilege changes or new user creation:

CMD:

index=main sourcetype=Windows_security (Action=CreateUser OR Action=PrivilegeAssigned)

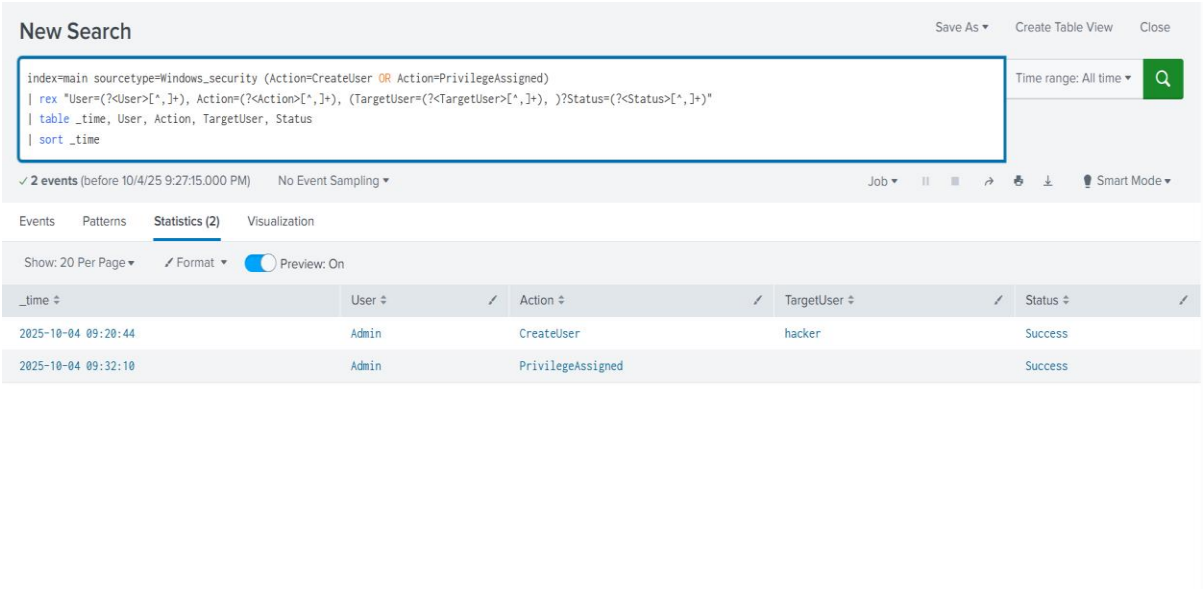
| rex "User=(?<User>[^,]+), Action=(?<Action>[^,]+), (TargetUser=(?<TargetUser>[^,]+),)?Status=(?<Status>[^,]+)"

| table _time, User, Action, TargetUser, Status

| sort _time

Shows when an Admin creates or modifies users (potential policy violation).

Screenshot: Query results for privilege changes



1.5 Web Access Log Analysis

Extract client IP and HTTP method:

CMD:

index=main sourcetype=web_Acess

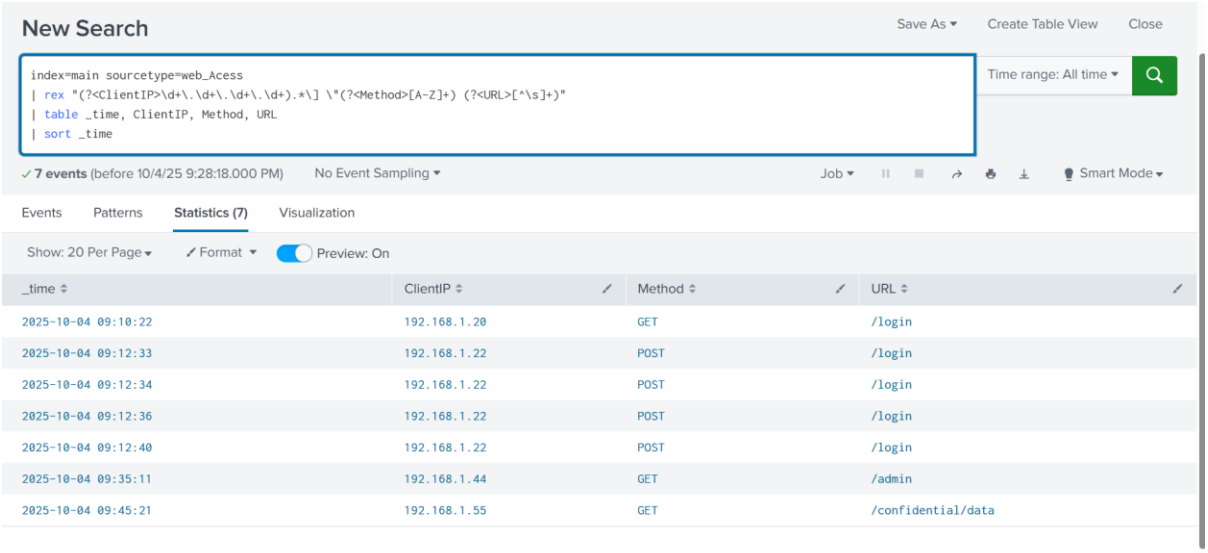
| rex "(?<ClientIP>\d+\.\d+\.\d+\.\d+).*\] \"(?<Method>[A-Z]+) (?<URL>[^\s]+)"

| table _time, ClientIP, Method, URL

| sort _time

Displays which IPs accessed which URLs on your web server.

Screenshot: Web access log output



1.6 Firewall Log Analysis

Check for blocked connections:

CMD:

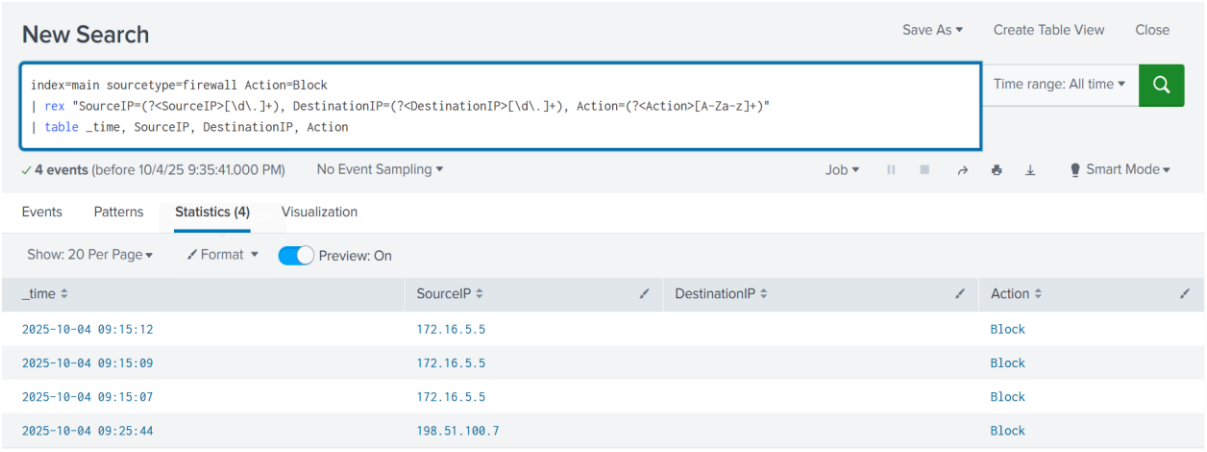
index=main sourcetype=firewall Action=Block

| rex "SourceIP=(?<SourceIP>[\d\.]+), DestinationIP=(?<DestinationIP>[\d\.]+), Action=(?<Action>[A-Za-z]+)"

| table _time, SourceIP, DestinationIP, Action

Identifies blocked IPs and traffic sources.

Screenshot: Firewall log search results



Outcome:

Understood how logs are collected, normalized, and analyzed in Splunk.

Learned how to extract fields and detect suspicious activity using SPL queries.

Practiced with real log samples representing Windows, Web, and Firewall data.