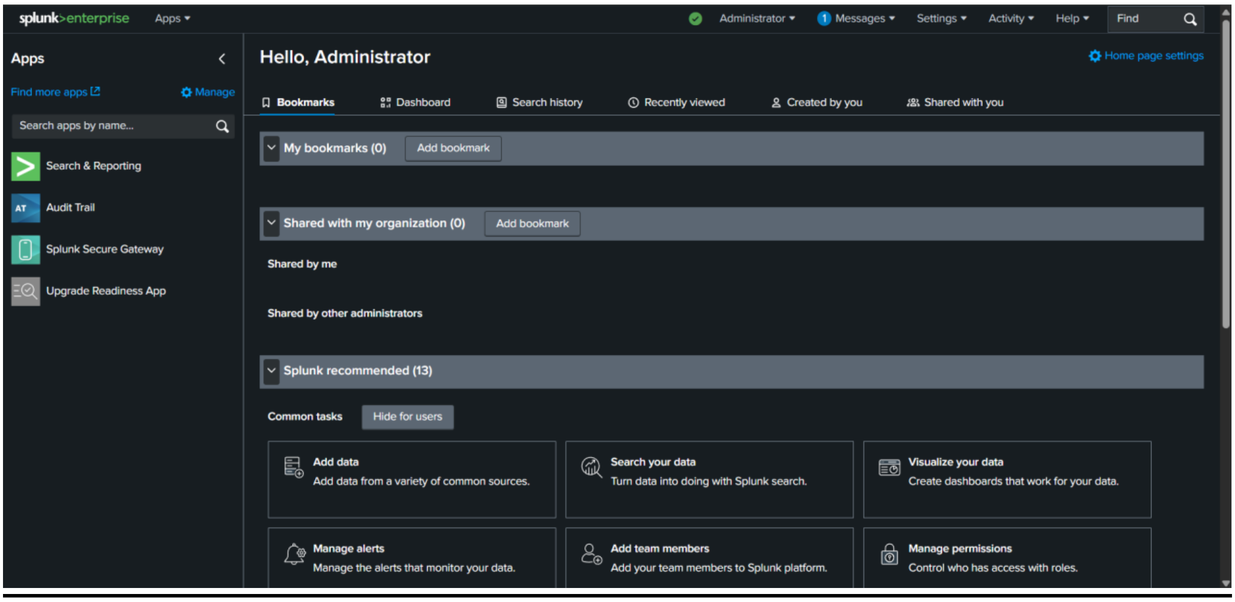
Security Alert Monitoring & Incident Response

About the Task:

This task simulates real-world SOC operations, involving the use of Splunk for detecting and investigating suspicious activities like malware alerts, brute-force logins, and risky user behaviour using simulated log data.

Objective:

- Upload sample security logs into Splunk
- Run meaningful detection queries
- Identify suspicious behaviour (malware, encoded PowerShell, etc.)
- Capture screenshots and analyse alerts
- Classify and respond to incidents
- Document findings in a professional SOC-style report



Add data from a variety of common sources.

Turn data into doing with Splunk search.

Create dashboards that work for your data.

Manage the alerts that monitor your data.

Add your team members to Splunk platform.

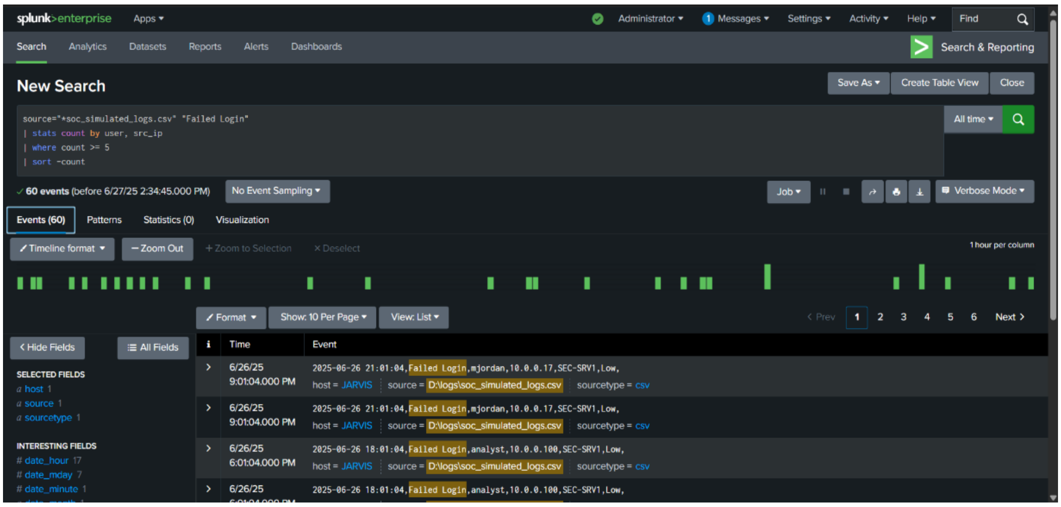
Control who has access with roles.

Tools Used:

- Splunk Cloud Trial
- Sample Log File: soc_simulated_logs.csv
- MS Word

Methodology:

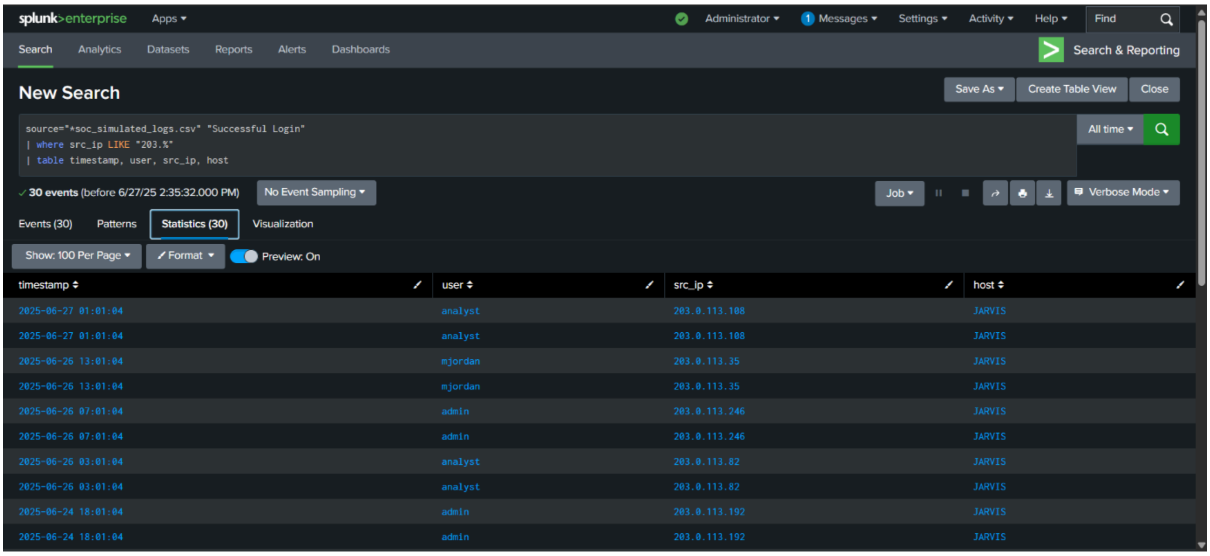
1. Upload Data:
   Uploaded soc_simulated_logs.csv to Splunk Cloud via “Add Data”.
2. Run Queries:
   Used Splunk search queries to detect and analyze:
   a. Failed login floods
   b. Successful logins from public IPs
   c. Malware detections
   d. Lateral movement patterns
   e. Encoded PowerShell execution
3. Screenshots Taken:
   Captured visual evidence of alerts (6 screenshots total).



```
source="*soc_simulated_logs.csv" "Failed Login"
| stats count by user, src_ip
| where count >= 5
| sort -count
```

✓ 60 events (before 6/27/25 2:34:45.000 PM)

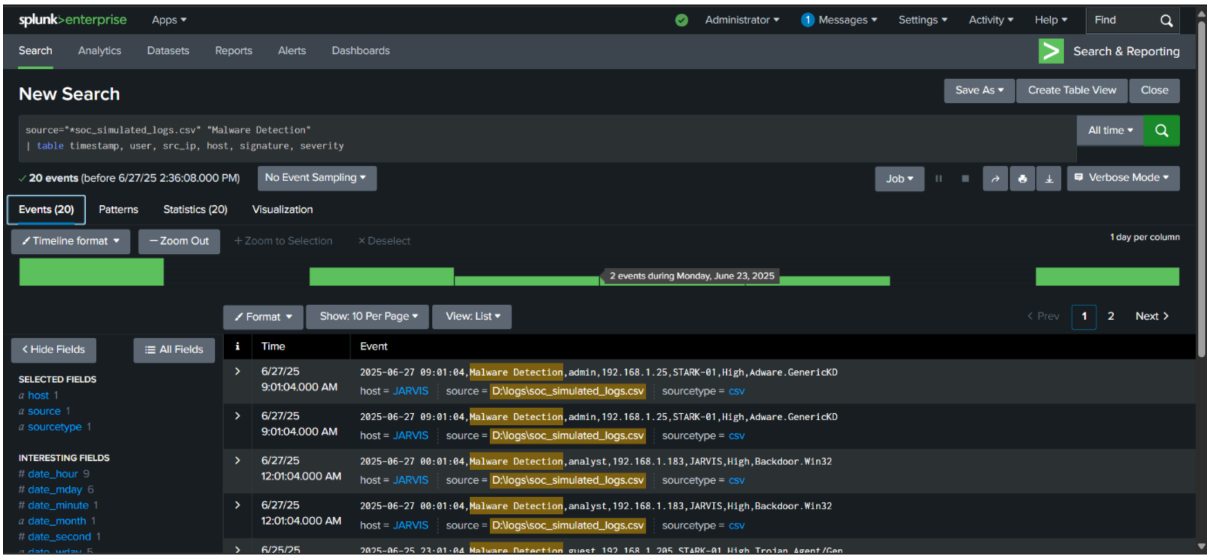
i	Time	Event
>	6/26/25 9:01:04.000 PM	2025-06-26 21:01:04,Failed Login,mjordan,10.0.0.17,SEC-SRV1,Low, host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
>	6/26/25 9:01:04.000 PM	2025-06-26 21:01:04,Failed Login,mjordan,10.0.0.17,SEC-SRV1,Low, host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
>	6/26/25 6:01:04.000 PM	2025-06-26 18:01:04,Failed Login,analyst,10.0.0.100,SEC-SRV1,Low, host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
>	6/26/25	2025-06-26 18:01:04,Failed Login,analyst,10.0.0.100,SEC-SRV1,Low,



```
source="*soc_simulated_logs.csv" "Successful Login"
| where src_ip LIKE "203.%"
| table timestamp, user, src_ip, host
```

✓ **30 events** (before 6/27/25 2:35:32.000 PM)

timestamp	user	src_ip	host
2025-06-27 01:01:04	analyst	203.0.113.108	JARVIS
2025-06-27 01:01:04	analyst	203.0.113.108	JARVIS
2025-06-26 13:01:04	mjordan	203.0.113.35	JARVIS
2025-06-26 13:01:04	mjordan	203.0.113.35	JARVIS
2025-06-26 07:01:04	admin	203.0.113.246	JARVIS
2025-06-26 07:01:04	admin	203.0.113.246	JARVIS
2025-06-26 03:01:04	analyst	203.0.113.82	JARVIS
2025-06-26 03:01:04	analyst	203.0.113.82	JARVIS
2025-06-24 18:01:04	admin	203.0.113.192	JARVIS
2025-06-24 18:01:04	admin	203.0.113.192	JARVIS



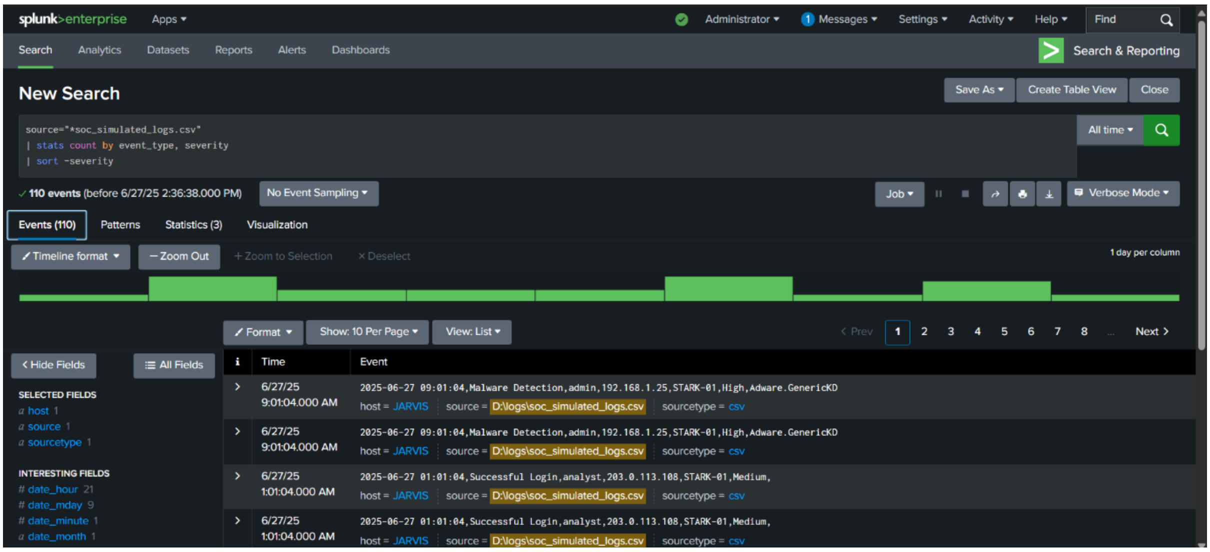
```
source="*soc_simulated_logs.csv" "Malware Detection"
| table timestamp, user, src_ip, host, signature, severity
```

✓ **20 events** (before 6/27/25 2:36:08.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 9
# date_mday 6
# date_minute 1
a date_month 1
# date_second 1
a date_wday 5

i	Time	Event
›	6/27/25 9:01:04.000 AM	2025-06-27 09:01:04,Malware Detection,admin,192.168.1.25,STARK-01,High,Adware.GenericKD host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
›	6/27/25 9:01:04.000 AM	2025-06-27 09:01:04,Malware Detection,admin,192.168.1.25,STARK-01,High,Adware.GenericKD host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
›	6/27/25 12:01:04.000 AM	2025-06-27 00:01:04,Malware Detection,analyst,192.168.1.183,JARVIS,High,Backdoor.Win32 host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
›	6/27/25 12:01:04.000 AM	2025-06-27 00:01:04,Malware Detection,analyst,192.168.1.183,JARVIS,High,Backdoor.Win32 host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
›	6/25/25	2025-06-25 23:01:04,Malware Detection,guest,192.168.1.205,STARK-01,High,Trojan.Agent/Gen



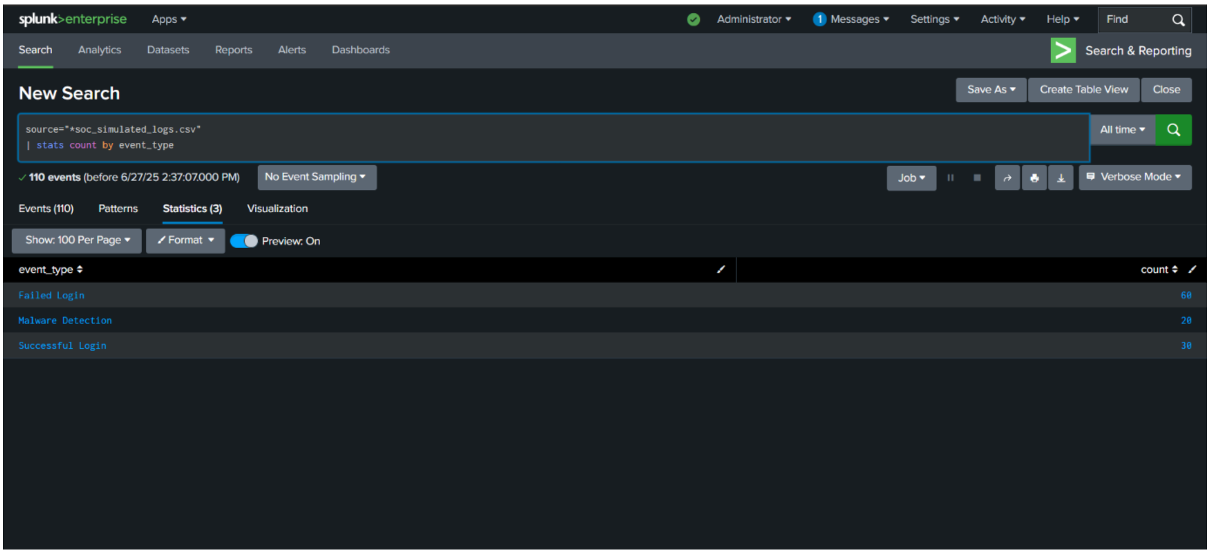
```
source="*soc_simulated_logs.csv"
| stats count by event_type, severity
| sort -severity
```

✓ **110 events** (before 6/27/25 2:36:38.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 21
# date_mday 9
# date_minute 1
a date_month 1

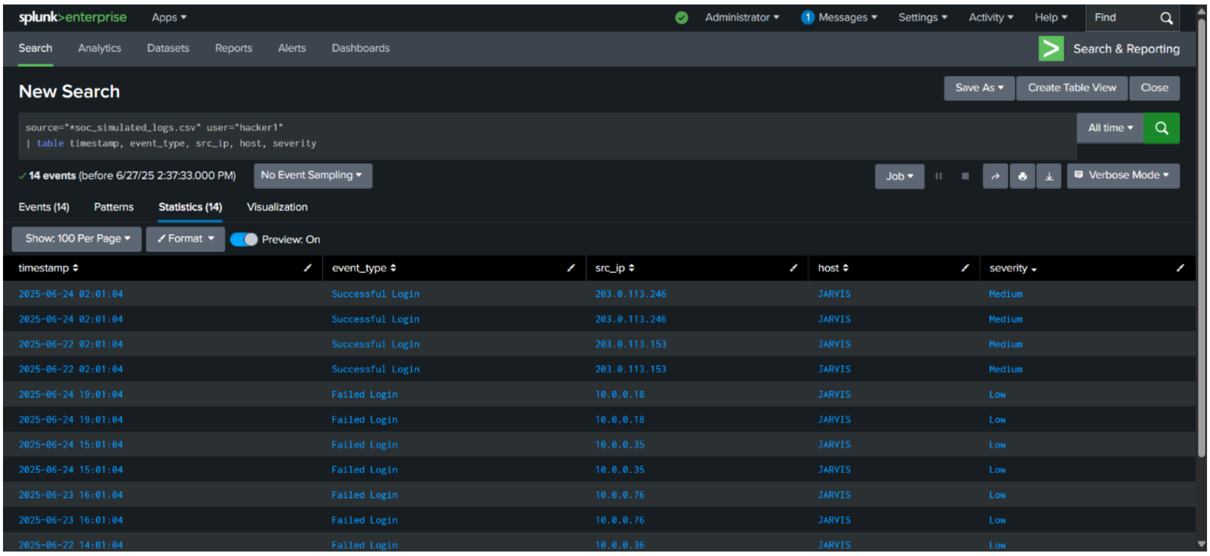
i	Time	Event
›	6/27/25 9:01:04.000 AM	2025-06-27 09:01:04,Malware Detection,admin,192.168.1.25,STARK-01,High,Adware.GenericKD host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
›	6/27/25 9:01:04.000 AM	2025-06-27 09:01:04,Malware Detection,admin,192.168.1.25,STARK-01,High,Adware.GenericKD host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
›	6/27/25 1:01:04.000 AM	2025-06-27 01:01:04,Successful Login,analyst,203.0.113.108,STARK-01,Medium, host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv
›	6/27/25 1:01:04.000 AM	2025-06-27 01:01:04,Successful Login,analyst,203.0.113.108,STARK-01,Medium, host = JARVIS source = D:\logs\soc_simulated_logs.csv sourcetype = csv



```
source="*soc_simulated_logs.csv"
| stats count by event_type
```

✓ 110 events (before 6/27/25 2:37:07.000 PM)

event_type	count
Failed Login	60
Malware Detection	20
Successful Login	30



```
source="*soc_simulated_logs.csv" user="hacker1"
| table timestamp, event_type, src_ip, host, severity
```

✓ 14 events (before 6/27/25 2:37:33.000 PM)

timestamp	event_type	src_ip	host	severity
2025-06-24 02:01:04	Successful Login	203.0.113.246	JARVIS	Medium
2025-06-24 02:01:04	Successful Login	203.0.113.246	JARVIS	Medium
2025-06-22 02:01:04	Successful Login	203.0.113.153	JARVIS	Medium
2025-06-22 02:01:04	Successful Login	203.0.113.153	JARVIS	Medium
2025-06-24 19:01:04	Failed Login	10.0.0.18	JARVIS	Low
2025-06-24 19:01:04	Failed Login	10.0.0.18	JARVIS	Low
2025-06-24 15:01:04	Failed Login	10.0.0.35	JARVIS	Low
2025-06-24 15:01:04	Failed Login	10.0.0.35	JARVIS	Low
2025-06-23 16:01:04	Failed Login	10.0.0.76	JARVIS	Low
2025-06-23 16:01:04	Failed Login	10.0.0.76	JARVIS	Low
2025-06-22 14:01:04	Failed Login	10.0.0.36	JARVIS	Low

Summary of Detected Alerts:

Timestamp	Source IP	Username	Event Description	Severity
2025-06-26	203.0.113.90	someone@corp.local	PowerShell encoded command (MITRE T1059.001)	High
2025-06-26	10.0.0.45	hacker1	Multiple failed login attempts	High
2025-06-26	203.0.113.45	admin	Successful login from suspicious public IP	Medium
2025-06-26	192.168.1.15	jdoe	Malware alert triggered	High

Incident Classification Table:

Alert Type	Description	Severity	Reasoning
Encoded PowerShell	Attempt to execute obfuscated script	High	Bypasses detection, possible malware drop
Brute Force Login	5+ failed logins from 1 IP (hacker1)	High	Brute-force credentials
Public IP Login	Successful login from 203.x.x.x	Medium	Unusual login location
Malware Alert	Detected trojan via log inspection	High	Confirmed malicious signature

Mitigation Recommendations:

Threat	Recommended Action
PowerShell Abuse	Block encoded commands, enable logging
Brute Force Login	Add IP rate limiting, enable MFA
Public IP Logins	Geo-blocking, alert on unfamiliar regions
Malware Alert	Quarantine host, scan all endpoints

Conclusion:

This task helped me understand how SOC teams monitor, analyze, and respond to threats using Splunk. I investigated real patterns like PowerShell misuse and brute-force login attempts, and documented my findings through screenshots and alert classifications.