

TASK 2 | FUTURE INTERNS | Security Alert Monitoring & Incident Response.

INCIDENT RESPONSE REPORT- Security log analysis using Splunk.

NAME- IZUGBARA CHIOMA BENITA.

DATE- 31ST JULY, 2025.

TOOLS USED- SPLUNK CLOUD PLATFORM TRAIL, GOOGLE DOCS.

SIEM TASK-LOG ANALYSIS & THREAT DETECTION.

OBJECTIVE

The purpose of this task was to simulate the role of a SOC analyst by reviewing and analyzing security logs to identify suspicious activity, prioritize threats and provide a documented response by using an SIEM tool (Splunk). This report summarizes my findings which includes *failed login attempts, malware alerts*.

SET UP AND DATA UPLOAD

- Tools Used - Splunk search and reporting app
- Data Source - Sample log file, provided by internship coordinator.
- Upload Method- Data was uploaded via Add data > Upload in the Splunk Dashboard.
- Source Types Selected- Network logs, Malware alerts.

Fig 1: splunk cloud

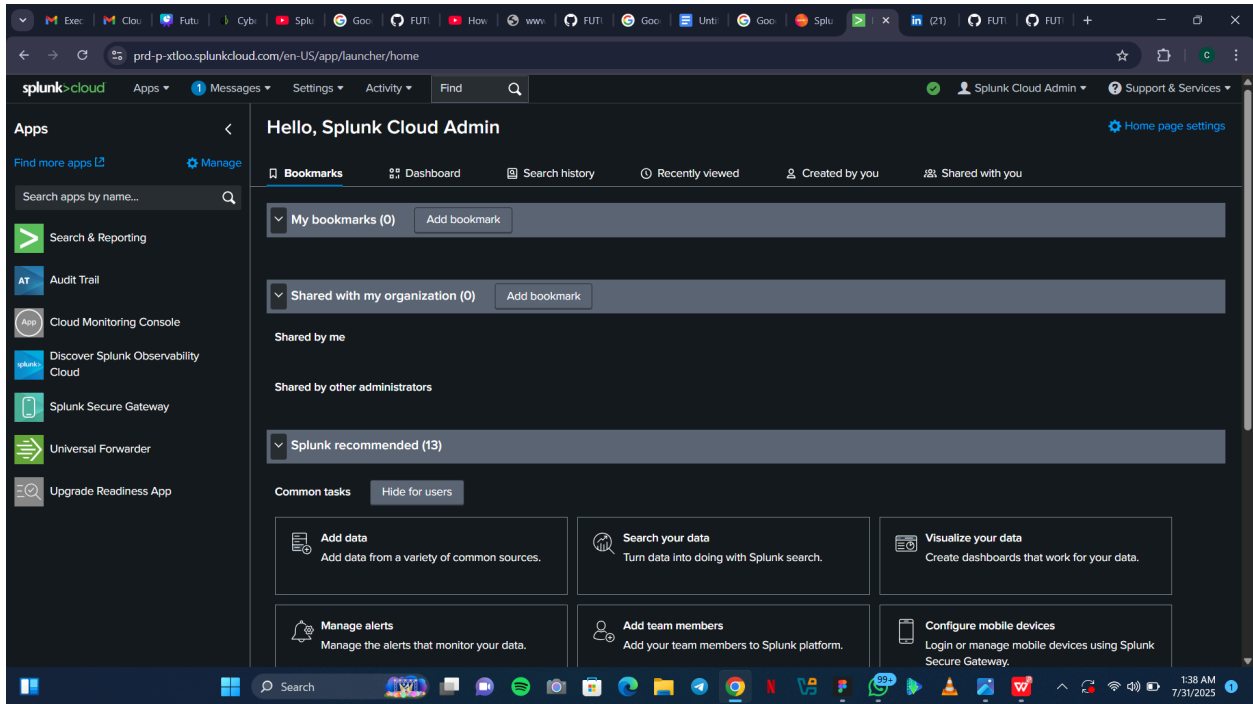


Fig 2: the log file

Time	Event	sourcetype
2025-07-03 03:44:14	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=file accessed	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=malware detected threat=Trojan Detected	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=file accessed	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=connection attempt	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=file accessed	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=login success	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=malware detected threat=Ransomware Behavior	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=file accessed	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=malware detected threat=Worm Infection Attempt	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=login success	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=file accessed	access_combined
7/30/25 11:57:44.000 PM	host = si-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com action=login failed	access_combined

IDENTIFIED INCIDENTS— INCIDENT 1 | MULTIPLE FAILED LOGIN ATTEMPTS DETECTED.

Severity: High.

Source: Authentication logs.

Repeated failed log in attempts were detected in the logs for several user accounts.

DETAILS

Username	IP Address	Date	Time.
David	203.0.113.77	7/3/25	9;02;14 AM
Alice	203.0.113.77	7/3/25	7;02;14 AM
Bob	10.0.0.5, 172.16.0.2	7/3/25	4:47;14, 4;23;14
Charlie	198.51.100.42	7/3/25	4;23;14 AM

These log in attempts happened within a short time frame, which may indicate a brute-force attempt or scripted attack.

Fig 3: log data showing failed login attempts for four users

>	7/3/25 4:47:14.000 AM	2025-07-03 04:47:14 user=bob ip=10.0.0.5 action=login failed host = si-i-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = linux_secure
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14 user=bob ip=172.16.0.3 action=login failed host = si-i-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14 user=charlie ip=198.51.100.42 action=login failed host = si-i-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 9:02:14.000 AM	2025-07-03 09:02:14 user=david ip=203.0.113.77 action=login failed host = si-i-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = linux_secure
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14 user=alice ip=203.0.113.77 action=login failed host = si-i-0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = syslog

MITIGATION

- Investigate accounts activity.
- Implement use of MFA.
- Lock accounts with excessive failures.

INCIDENT 2 | MALWARE ALERTS IN LOGS.

Trojan Detected.

User: Charlie.

Date: 7/3/2025

IP Address: 172.16.0.3

Threat: Trojan

Severity: High

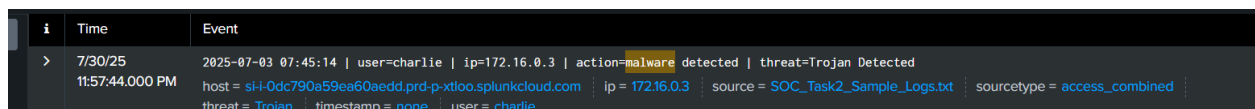
RISKS

- Steal user data.
- Damage files.
- Create backdoor for further attackers.

MITIGATION

- Install a reputable anti-virus software.
- Keep all softwares up to date with the latest patches.

Fig 4: trojan horse alert



The screenshot shows a security alert log with the following details:

i	Time	Event
>	7/30/25 11:57:44.000 PM	2025-07-03 07:45:14 user=charlie ip=172.16.0.3 action=malware detected threat=Trojan Detected host = si-l-0dc790a59ea60aedd-prd-p-xtloo.splunkcloud.com ip = 172.16.0.3 source = SOC_Task2_Sample_Logs.txt sourcetype = access_combined threat = Trojan timestamp = none user = charlie

Ransomware Behavior.

User: Bob

Date: 7/3/2025

IP Address: 172.16.0.3

Threat: Ransomware

Severity: High

RISKS

- Encryption of files.

- Data loss.
- Data Breach.

MITIGATION.

- Backup data.
- Increase security.

Fig 5: ransomware behavior detected.

>	7/30/25 11:57:44.000 PM	2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = si-I0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com ip = 172.16.0.3 source = SOC_Task2_Sample_Logs.bt sourcetype = access_combined threat = Ransomware timestamp = none user = bob
---	----------------------------	---

Rootkit

User: Eve.

Date: 7/3/2025

IP Address: 10.0.0.2

Threat: Rootkit

Severity: Critical.

RISKS

- To launch DDoS attacks.

MITIGATION

- Keep systems updated

Fig 6: rootkit signature detected

>	7/30/25 11:57:44.000 PM	2025-07-03 07:51:14 user=eve ip=10.0.0.5 action=malware detected threat=Rootkit Signature host = si-I0dc790a59ea60aedd.prd-p-xtloo.splunkcloud.com ip = 10.0.0.5 source = SOC_Task2_Sample_Logs.bt sourcetype = access_combined threat = Rootkit timestamp = none user = eve
---	----------------------------	--

Alert Type	Affected IP	Date/Time	Severity	Description	Action Taken
Malware Detected.	172.16.0.3	7/30/25, 07:45:40	High	Trojan malware activity detected	Removed malware and logged
Malware Detected	172.16.0.3	7/30/25, 09:10:14	High	Ransomware alert on internal host	Disconnected host and reported
Malware Detected	10.0.0.5	7/3/25, 07:51:14	Critical	Rootkit malware detected on host	Isolated and scanned systems
Failed Login Attempt	David (203.0.113.7)	7/3/25, 9:02:14 AM	Medium	Multiple failed log in by David	Account lock out triggered.
Failed Login Attempt	Alice (203.0.113.7)	7/3/25, 7:02:14 AM	Medium	Failed log ins from Alice.	Investigated and notified user.
Failed Login Attempt	Bob (10.0.0.5, 172.16.0.2)	7/3/25, 4:47:14, 4:23:14	Medium	Repeated failed logins from Bob	Notified SOC team.

Fig 7: showing IP Addresses of Malware detected on a pie chart.

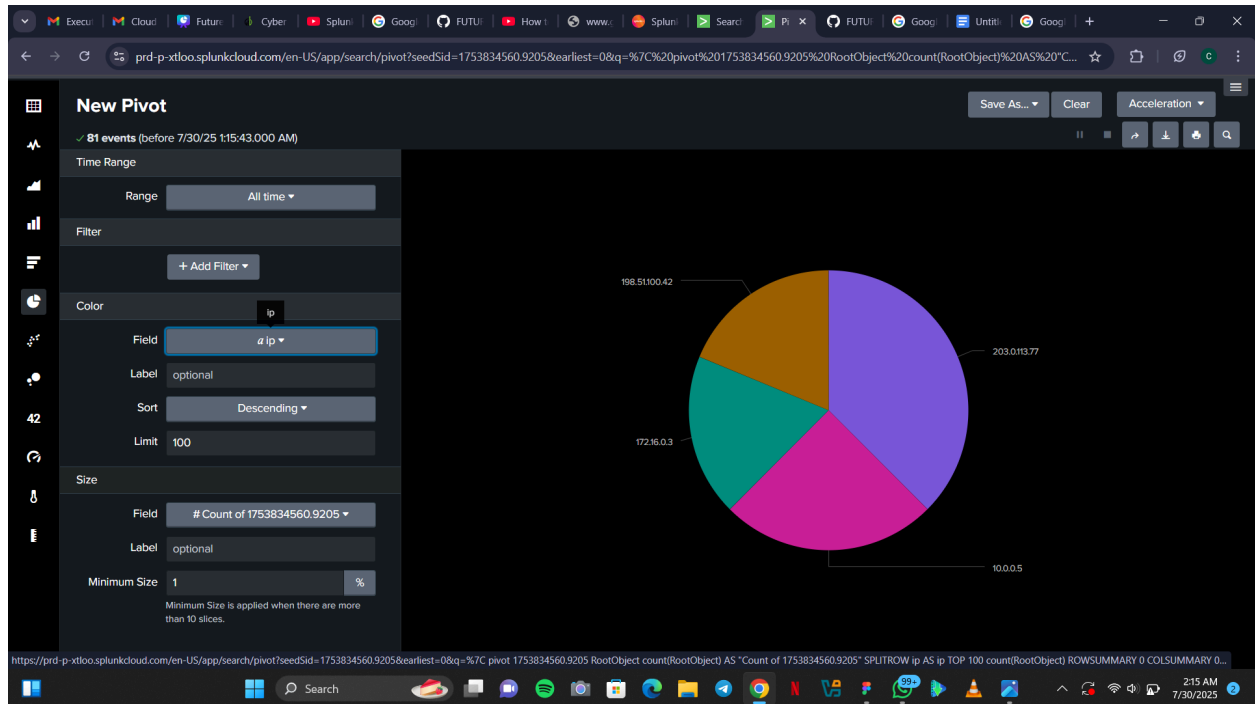
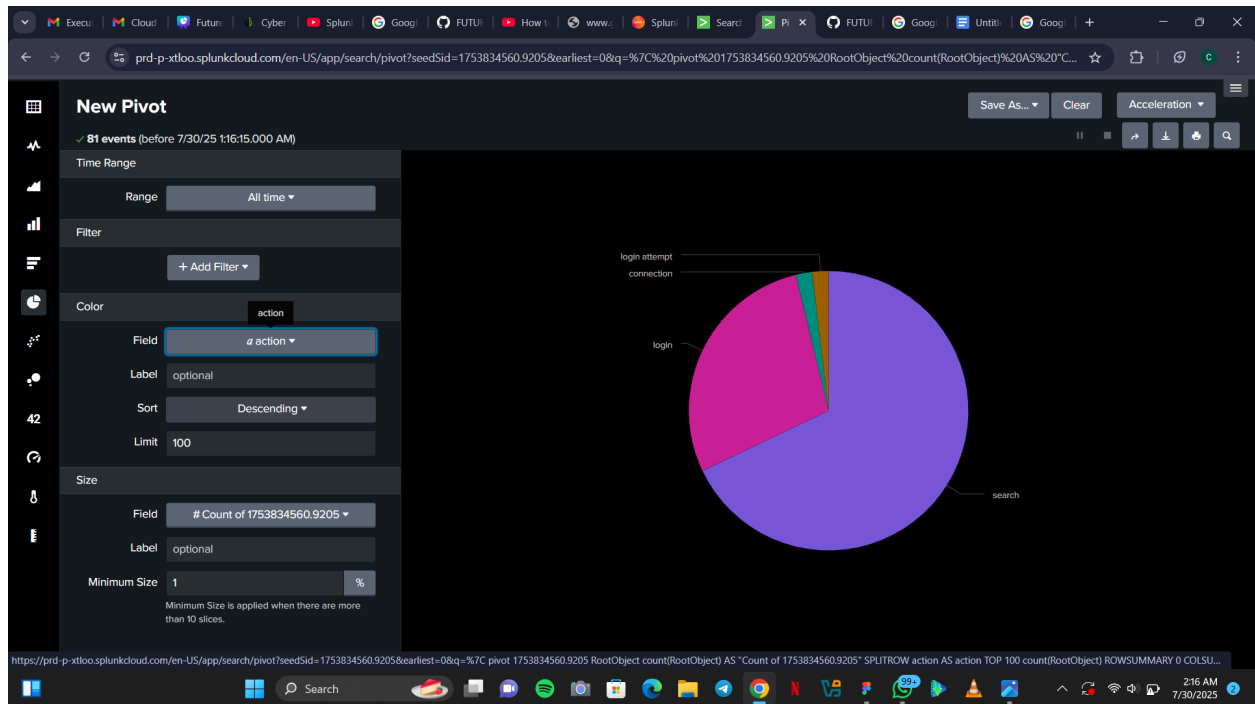


Fig 8: pie chart displaying failed log in attempts



STAKEHOLDER COMMUNICATION (SIMULATED)

Subject: Summary of Security Incident Findings.

Following the review of recent system logs using a SIEM tool (Splunk), multiple failed login attempts were detected from several user accounts, alongside malware alerts identifying Rootkiy, Trojan and Ransomware threats.

According to these findings, we have drafted some ***Suggested Next Steps***:

- Review affected user accounts and enforce password resets that includes MFA.
- Investigate and isolate endpoints showing malware alerts.
- Apply relevant patches and updates to vulnerable systems.
- Continue monitoring for suspicious activity using the SIEM dashboards.
- Schedule a follow-up assessment to verify remediation.

Please refer to the full incident report for detailed analysis.

—SOC Analyst, Future Interns Security Team.