

FUTURE_CS_02

Title: Security Event Monitoring and Analysis using Splunk

Intern: Meghan Diwate

Date: 14th September 2025

1. Introduction

This project demonstrates the use of Splunk for centralized log analysis, real-time monitoring, and threat detection. Custom security logs were ingested into Splunk to simulate real-world enterprise monitoring.

The objectives were to:

- Detect suspicious events from system logs.
- Classify alerts based on severity.
- Document incidents with a timeline, impact, and remediation steps.
- Build a dashboard to visualize the results in real time.

2. Objectives

- Collect and index custom logs into Splunk.
- Use SPL queries to detect suspicious activities such as login anomalies, malware detection, unauthorized file access, and unusual network connection attempts.
- Identify and classify 3–5 suspicious alerts by severity (High, Medium, Low).
- Build dashboards for security event visualization.
- Generate an incident response report.

3. Dataset Description

The dataset contained 47 security log entries, simulating real-world activities.

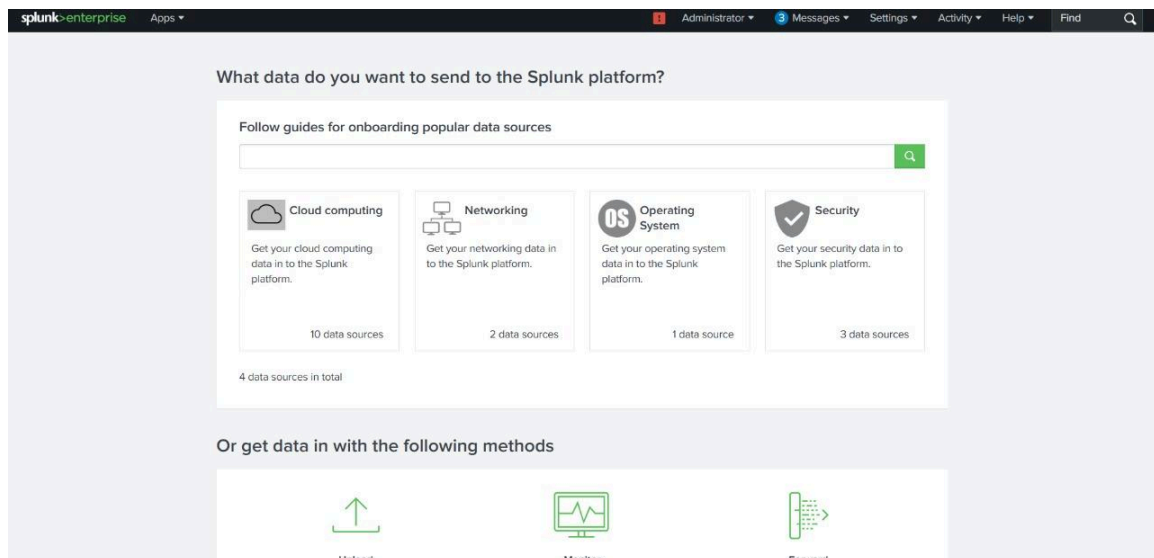
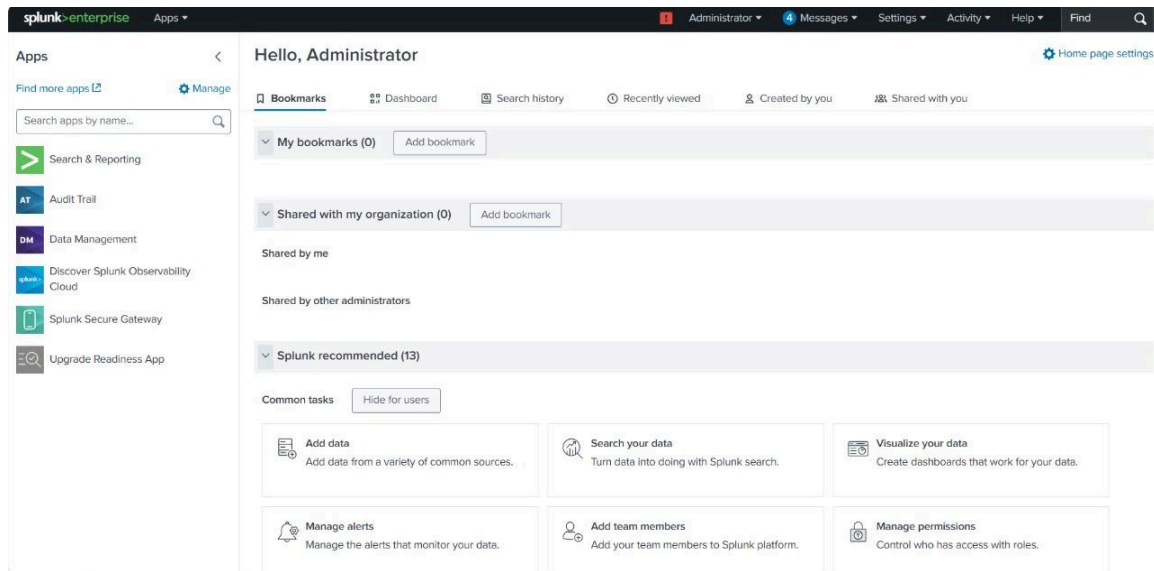
Log Fields:

- **Timestamp** – Event time
- **User** – Actor (alice, bob, charlie, david, eve)
- **IP Address** – Source of the event
- **Action** – Event performed
- **Threat** – Malware type

Examples:

- 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
- 2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
- 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior

4. Methodology



Step 1 – Data Ingestion

Logs were indexed in Splunk under index=internship.

The screenshot shows the 'Add Data' wizard in Splunk Enterprise. The 'Select Source' step is active, indicated by a green dot in the progress bar. The selected file is 'SOC_Task2_Sample_Logs.txt'. A 'Select File' button is visible. Below the file selection area, there is a large box with the text 'Drop your data file here' and 'The maximum file upload size is 500 Mb'. A green checkmark and the text 'File Successfully Uploaded' are displayed. An FAQ section is at the bottom with three questions: 'What kinds of files can the Splunk platform index?', 'What is a source?', and 'How do I get remote data onto my Splunk platform instance?'.

Add Data

Select Source Set Source Type Input Settings Review Done

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **SOC_Task2_Sample_Logs.txt**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

File Successfully Uploaded

FAQ

- > What kinds of files can the Splunk platform index?
- > What is a source?
- > How do I get remote data onto my Splunk platform instance?

The screenshot shows the 'Set Source Type' step in the 'Add Data' wizard. The progress bar shows 'Set Source Type' as the current step. The source is 'SOC_Task2_Sample_Logs.txt'. A 'Source type: default' dropdown menu is shown, along with a 'Save As' button. Below the dropdown, there are expandable sections for 'Event Breaks', 'Timestamp', and 'Advanced'. A 'View Event Summary' link is on the right.

Add Data

Select Source Set Source Type Input Settings Review Done

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **SOC_Task2_Sample_Logs.txt** [View Event Summary](#)

Source type: default **Save As**

- > Event Breaks
- > Timestamp
- > Advanced

_dsappevent	Edit	Delete	Disable	Events	SplunkDeploymentServ erConfig	1 MB	488.28 GB	0	—	—	\$\$SPLUNK_DB_dsappe ventdb	—	✓ Active
_dsclient	Edit	Delete	Disable	Events	SplunkDeploymentServ erConfig	1 MB	488.28 GB	0	—	—	\$\$SPLUNK_DB_dsclient ldb	—	✓ Active
_dsphonehome	Edit	Delete	Disable	Events	SplunkDeploymentServ erConfig	1 MB	488.28 GB	0	—	—	\$\$SPLUNK_DB_dsphon ehomeldb	—	✓ Active
_internal	Edit	Delete	Disable	Events	system	8 MB	488.28 GB	53.8K	2 days ago	a day ago	\$\$SPLUNK_DB_internal dbldb	—	✓ Active
_introspection	Edit	Delete	Disable	Events	system	33 MB	488.28 GB	15.7K	2 days ago	a day ago	\$\$SPLUNK_DB_introsp ectionldb	—	✓ Active
_metrics	Edit	Delete	Disable	Metrics	system	3 MB	488.28 GB	24.4K	2 days ago	a day ago	\$\$SPLUNK_DB_metrics ldb	—	✓ Active
_metrics_rolu p	Edit	Delete	Disable	Metrics	system	1 MB	488.28 GB	0	—	—	\$\$SPLUNK_DB_metrics _rollupldb	—	✓ Active
_telemetry	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0	—	—	\$\$SPLUNK_DB_telemet ryldb	—	✓ Active
_thefishbucke t	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0	—	—	\$\$SPLUNK_DB_fishbuck etldb	—	✓ Active
history	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0	—	—	\$\$SPLUNK_DB_historyd bldb	—	✓ Active
internship	Edit	Delete	Disable	Events	search	1 MB	500 GB	0	—	—	\$\$SPLUNK_DB_internshi pldb	—	✓ Active
main	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0	—	—	\$\$SPLUNK_DB_defaultd bldb	—	✓ Active
splunklogger	Edit	Delete	Enable	Events	system	0 B	488.28 GB	0	—	—	\$\$SPLUNK_DB_splunklo ggerldb	—	✗ Inactive
summary	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0	0 events	—	\$\$SPLUNK_DB_summary dbldb	—	✓ Active

splunk-enterprise Apps

Administrator 4 Messages Settings Activity Help Find

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

☒ Constant value
☐ Regular expression on path
☐ Segment in path

Host field value

DESKTOP-FG2ABKL

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index

internship Create a new index

FAQ

> How do indexes work?
> How do I know when to create or use multiple indexes?

Phone Link

splunk-enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Add Data

Select SourceSet Source TypeInput SettingsReviewDone

< BackSubmit>

Review

Input Type Uploaded File
File Name SOC_Task2_Sample_Logs.txt
Source Type soc_kv
Host DESKTOP-FG2ABKL
Index internship

Step 2 – Query Execution (SPL)

splunk-enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

Search

enter search here...

Time range: Last 24 hours

Q

No Event Sampling

Smart Mode

> Search History

How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

DocumentationTutorialData Summary

Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot! Create Table View

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

- Failed Logins → index=internship action="login failed"

The screenshot displays the Splunk Cloud interface with a search query: `Index=internship action=login "failed"`. The search results are shown in a table format, displaying 5 events. The table includes columns for Time, Event, and sourcetype. The events are filtered by the search query and show failed login attempts.

Search Query: `Index=internship action=login "failed"`

Time range: All time

Events (5):

Time	Event	sourcetype
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-06ae43f552a4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
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-06ae43f552a4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
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-06ae43f552a4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
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-06ae43f552a4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
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-06ae43f552a4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv

SELECTED FIELDS: host 1, source 1, sourcetype 1

INTERESTING FIELDS: action 1, date_hour 3, date_mday 1, date_minute 3, date_month 1, date_second 1, date_wday 1, date_year 1, date_zone 1, index 1, ip 4, linecount 1, punct 1, splunk_server 1, timeendpos 1, timestartpos 1, user 4

Timeline format: Timeline format, Zoom Out, Zoom to Selection, Deselect

Format: Format, Show: 20 Per Page, View: List

- Successful Logins → index=internship action="login success"

The screenshot shows the Splunk Cloud interface with a search query `index=internship action=login success`. The search results are displayed in a table format, showing 11 events. The table has columns for Time, Event, and sourcetype. The events are sorted by time, showing logins for users bob, alice, and charlie.

Time	Event	sourcetype
7/3/25 9:07:14.000 AM	2025-07-03 09:07:14 user=bob ip=203.0.113.77 action=login success host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 8:30:14.000 AM	2025-07-03 08:30:14 user=veve ip=172.16.0.3 action=login success host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 8:00:14.000 AM	2025-07-03 08:00:14 user=alice ip=198.51.100.42 action=login success host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 7:46:14.000 AM	2025-07-03 07:46:14 user=bob ip=10.0.0.5 action=login success host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 6:21:14.000 AM	2025-07-03 06:21:14 user=alice ip=203.0.113.77 action=login success host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 05:18:14	2025-07-03 05:18:14 user=charlie ip=172.16.0.3 action=login success	

- File Access → index=internship action="file accessed"

The screenshot shows the Splunk Cloud interface with a search query `index=internship action=file accessed`. The search results are displayed in a table format, showing 7 events. The table has columns for Time, Event, and sourcetype. The events are sorted by time, showing file access for users bob, charlie, veve, david, and bob.

Time	Event	sourcetype
7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=veve ip=172.16.0.3 action=file accessed host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=charlie ip=203.0.113.77 action=file accessed host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 8:31:14.000 AM	2025-07-03 08:31:14 user=veve ip=203.0.113.77 action=file accessed host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 7:57:14.000 AM	2025-07-03 07:57:14 user=david ip=10.0.0.5 action=file accessed host = si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt	log_sv
7/3/25 07:18:14	2025-07-03 07:18:14 user=bob ip=203.0.113.77 action=file accessed	

Format Show: 20 Per Page View: List		
< Hide Fields	All Fields	
SELECTED FIELDS		
a host 1		
a source 1		
a sourcetype 1		
INTERESTING FIELDS		
a action 1		
# date_hour 6		
# date_mday 1		
# date_minute 9		
a date_month 1		
# date_second 1		
a date_wday 1		
# date_year 1		
a date_zone 1		
a index 1		
a ip 4		
# linecount 1		
a punct 1		
a splunk_server 1		
# timeendpos 1		
# timestamppos 1		
a user 5		
+ Extract New Fields		
i	Time	Event
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=malware detected threat=Ransomware Behavior host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=eve ip=172.16.0.3 action=malware detected threat=Rootkit Signature host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=charlie ip=203.0.113.77 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 8:31:14.000 AM	2025-07-03 08:31:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:57:14.000 AM	2025-07-03 07:57:14 user=david ip=10.0.0.5 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:18:14.000 AM	2025-07-03 07:18:14 user=bob ip=203.0.113.77 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 6:10:14.000 AM	2025-07-03 06:10:14 user=david ip=203.0.113.77 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 6:01:14.000 AM	2025-07-03 06:01:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 5:44:14.000 AM	2025-07-03 05:44:14 user=bob ip=198.51.100.42 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 5:33:14.000 AM	2025-07-03 05:33:14 user=david ip=198.51.100.42 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 4:53:14.000 AM	2025-07-03 04:53:14 user=alice ip=203.0.113.77 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv

- Malware Detection → index=internship action="malware detected"





Format Show: 20 Per Page View: List		
< Hide Fields	All Fields	
SELECTED FIELDS		
a host 1		
a source 1		
a sourcetype 1		
INTERESTING FIELDS		
a action 1		
# date_hour 4		
# date_mday 1		
# date_minute 10		
a date_month 1		
# date_second 1		
a date_wday 1		
# date_year 1		
+ Extract New Fields		
i	Time	Event
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 user=eve ip=10.0.0.5 action=malware detected threat=Rootkit Signature host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:45:14.000 AM	2025-07-03 07:45:14 user=charlie ip=172.16.0.3 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 user=bob ip=10.0.0.5 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 5:45:14.000 AM	2025-07-03 05:45:14 user=david ip=172.16.0.3 action=malware detected threat=Trojan Detected host=si-i-06ae43f552a4e9d70.prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv

https://prd-p-otaj.splunkcloud.com/en-US/app/search/search?q=search%3Dindex%3Dinternship...&_t=03%2005%3A42%3A14%20user%3Deve%20ip%3D203.0.113.77%20action%3Dmalware%20detected%20threat%3DTrojan%20Detected

		Format	Show: 20 Per Page	View: List
		Time	Event	
< Hide Fields All Fields SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS a action 1 # date_hour 4 # date_mday 1 # date_minute 10 a date_month 1 # date_second 1 a date_wday 1 # date_year 1 a date_zone 1 a index 1 a ip 5 # linecount 1 a punct 2 a splunk_server 1 a threat 5 # timeendpos 1 # timestartpos 1 a user 5 + Extract New Fields	>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 user=eve ip=10.0.0.5 action=malware detected threat=Rootkit Signature host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 7:45:14.000 AM	2025-07-03 07:45:14 user=charlie ip=172.16.0.3 action=malware detected threat=Trojan Detected host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 user=bob ip=10.0.0.5 action=malware detected threat=Trojan Detected host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 5:45:14.000 AM	2025-07-03 05:45:14 user=david ip=172.16.0.3 action=malware detected threat=Trojan Detected host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 5:30:14.000 AM	2025-07-03 05:30:14 user=eve ip=192.168.1.101 action=malware detected threat=Trojan Detected host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14 user=bob ip=203.0.113.77 action=malware detected threat=Worm Infection Attempt host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 4:41:14.000 AM	2025-07-03 04:41:14 user=alice ip=172.16.0.3 action=malware detected threat=Spyware Alert host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 4:29:14.000 AM	2025-07-03 04:29:14 user=alice ip=192.168.1.101 action=malware detected threat=Trojan Detected host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 4:19:14.000 AM	2025-07-03 04:19:14 user=alice ip=198.51.100.42 action=malware detected threat=Rootkit Signature host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	

- **Connection Attempts** → index=internship action="connection attempt"

		Format	Show: 20 Per Page	View: List
		Time	Event	
< Hide Fields All Fields SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS a action 1 # date_hour 5 # date_mday 1 # date_minute 10 a date_month 1 # date_second 1 a date_wday 1 # date_year 1 a date_zone 1	>	7/3/25 8:21:14.000 AM	2025-07-03 08:21:14 user=david ip=172.16.0.3 action=connection attempt host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 8:20:14.000 AM	2025-07-03 08:20:14 user=charlie ip=192.168.1.101 action=connection attempt host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=192.168.1.101 action=connection attempt host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=203.0.113.77 action=connection attempt host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 7:38:14.000 AM	2025-07-03 07:38:14 user=charlie ip=172.16.0.3 action=connection attempt host = si-I06ae43f552e4e9d70.prd-p-otofj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv	
	>	7/3/25 7:36:14.000 AM	2025-07-03 07:36:14 user=david ip=10.0.0.5 action=connection attempt	



https://prd-p-ofoj.splunkcloud.com/en-US/app/search/search?q=search%20index%3Dinternship%20action%3Dconnection%20attempt&display.page.search.mode=smart&dispatch.sample...    


SELECTED FIELDS		INTERESTING FIELDS	
a host 1	a source 1	a action 1	a date_hour 5
a source 1	a sourcetype 1	# date_minute 1	# date_mday 1
		# date_month 1	# date_second 1
		# date_wday 1	# date_year 1
		# date_zone 1	a index 1
		a ip 4	# linecount 1
		a punct 1	a splunk_server 1
		# timeendpos 1	# timestartpos 1
		a user 3	

+ Extract New Fields

i	Time	Event
>	7/3/25 8:20:14.000 AM	2025-07-03 08:20:14 user=charlie ip=192.168.1.101 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=192.168.1.101 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=203.0.113.77 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:38:14.000 AM	2025-07-03 07:38:14 user=charlie ip=172.16.0.3 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:36:14.000 AM	2025-07-03 07:36:14 user=charlie ip=10.0.0.5 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 7:22:14.000 AM	2025-07-03 07:22:14 user=charlie ip=192.168.1.101 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 6:13:14.000 AM	2025-07-03 06:13:14 user=charlie ip=10.0.0.5 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 5:49:14.000 AM	2025-07-03 05:49:14 user=charlie ip=192.168.1.101 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 5:27:14.000 AM	2025-07-03 05:27:14 user=charlie ip=203.0.113.77 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 4:27:14.000 AM	2025-07-03 04:27:14 user=charlie ip=172.16.0.3 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 4:19:14.000 AM	2025-07-03 04:19:14 user=charlie ip=10.0.0.5 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv


Show details





splunkcloud Apps Messages Settings Activity Find  Splunk Cloud Admin  Support & Services

Search Analytics Datasets Reports Alerts Dashboards  Search & Reporting

New Search

Save As Create Table View Close

index=internship NOT (ip="10.*" OR ip="172.*" OR ip="192.168.*") Time range: All time 

✓ 23 events (before 9/9/25 8:35:28.000 AM) No Event Sampling Job     Policy-Based Pool Smart Mode

Events (23) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect 1 hour per column

SELECTED FIELDS		INTERESTING FIELDS	
a host 1	a source 1	a action 4	# date_hour 6
a source 1	a sourcetype 1	# date_minute 1	# date_mday 1
		# date_month 1	# date_second 1
		# date_wday 1	# date_year 1
		a date_zone 1	

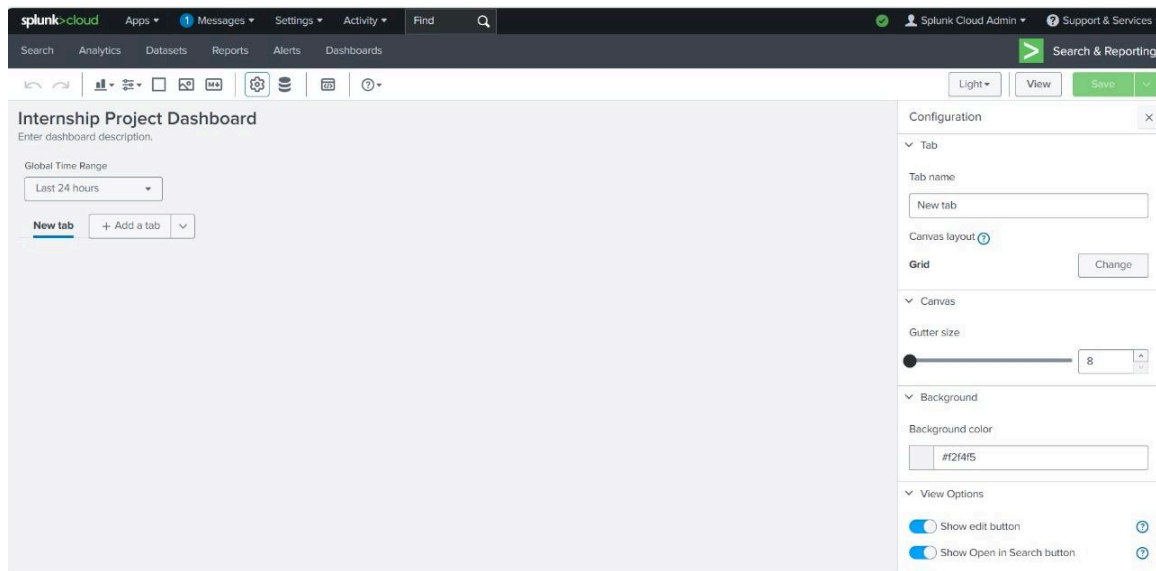
+ Extract New Fields

i	Time	Event
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 9:07:14.000 AM	2025-07-03 09:07:14 user=eve ip=203.0.113.77 action=login success source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 9:02:14.000 AM	2025-07-03 09:02:14 user=charlie ip=203.0.113.77 action=login failed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=charlie ip=203.0.113.77 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 8:31:14.000 AM	2025-07-03 08:31:14 user=eve ip=203.0.113.77 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv
>	7/3/25 8:00:14.000 AM	2025-07-03 08:00:14 user=alice ip=198.51.100.42 action=login success source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv

< Hide Fields	All Fields	Format	Show: 20 Per Page	View: List	< Prev	1	2	Next >
# date_hour 0								
# date_mday 1								
# date_minute 17								
# date_month 1								
# date_second 1								
# date_wday 1								
# date_zone 1								
# index 1								
# ip 2								
# linecount 1								
# punct 3								
# splunk_server 1								
# timeendpos 1								
# timestartpos 1								
# user 5								
1 more field								
+ Extract New Fields								
i	Time	Event						
	8:42:14.000 AM	host = si-i-06ae43f552a4e9d70-prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 8:31:14.000 AM	2025-07-03 08:31:14 user=reve ip=203.0.113.77 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 8:00:14.000 AM	2025-07-03 08:00:14 user=alice ip=198.51.100.42 action=login success source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=203.0.113.77 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 7:18:14.000 AM	2025-07-03 07:18:14 user=bob ip=203.0.113.77 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14 user=alice ip=203.0.113.77 action=login failed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 6:21:14.000 AM	2025-07-03 06:21:14 user=alice ip=203.0.113.77 action=login success source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 6:10:14.000 AM	2025-07-03 06:10:14 user=david ip=203.0.113.77 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:44:14.000 AM	2025-07-03 05:44:14 user=bob ip=198.51.100.42 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=reve ip=203.0.113.77 action=malware detected threat=Trojan Detected source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:33:14.000 AM	2025-07-03 05:33:14 user=david ip=198.51.100.42 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:27:14.000 AM	2025-07-03 05:27:14 user=david ip=203.0.113.77 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						

< Hide Fields	All Fields	Format	Show: 20 Per Page	View: List	< Prev	1	2	Next >
# user 5								
1 more field								
+ Extract New Fields								
i	Time	Event						
	8:42:14.000 AM	host = si-i-06ae43f552a4e9d70-prd-p-otaj.splunkcloud.com source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 6:21:14.000 AM	2025-07-03 06:21:14 user=alice ip=203.0.113.77 action=login success source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 6:10:14.000 AM	2025-07-03 06:10:14 user=david ip=203.0.113.77 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:44:14.000 AM	2025-07-03 05:44:14 user=bob ip=198.51.100.42 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=reve ip=203.0.113.77 action=malware detected threat=Trojan Detected source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:33:14.000 AM	2025-07-03 05:33:14 user=david ip=198.51.100.42 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:27:14.000 AM	2025-07-03 05:27:14 user=david ip=203.0.113.77 action=connection attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:12:14.000 AM	2025-07-03 05:12:14 user=alice ip=198.51.100.42 action=login success source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14 user=bob ip=203.0.113.77 action=malware detected threat=Worm Infection Attempt source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 4:53:14.000 AM	2025-07-03 04:53:14 user=alice ip=203.0.113.77 action=file accessed source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 4:53:14.000 AM	2025-07-03 04:53:14 user=david ip=203.0.113.77 action=login success source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						
>	7/3/25 4:46:14.000 AM	2025-07-03 04:46:14 user=david ip=203.0.113.77 action=login success source = SOC_Task2_Sample_Logs.txt sourcetype = log_sv						

Step 3 – Dashboard Creation



All queries were saved as panels, and a dashboard was created with:

- Failed Logins

Edit data source

Data source name

Failed Login Attempts

☐ Access search results or metadata [?](#)

SPL query

[Open in search](#)

```
index=internship "action=login failed"  
| stats count AS failed_logins
```

Time range

Default

Time range set by dashboard source default value

\$global_time.earliest\$ - \$global_time.latest\$

Configure in source editor

Event Sampling

Cancel

Apply and close

- Successful Logins

Edit data source

Data source name

Successful Logins

☐ Access search results or metadata [?](#)

SPL query

[Open in search](#)

```
index=internship "action=login success"
| stats count AS successful_logins
```

Time range

Default

Time range set by dashboard source default value

\$global_time.earliest\$ - \$global_time.latest\$

Configure in source editor

i 1 visualization will be updated

Cancel

Apply and close

splunk-cloud

Apps

Messages

Settings

Activity

Find

Splunk Cloud Admin

Support & Services

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Reporting

Light

View

Save

Internship Project Dashboard

Enter dashboard description.

Global Time Range

All time

New tab

New tab

+ Add a tab

Successful Logins

11

Configuration

Tab

Tab name

New tab

Canvas layout

Grid

Change

Canvas

Gutter size

8

Background

Background color

#121415

View Options

Show edit button

Show Open in Search button

- File Access Events

Edit data source

Data source name

File Accessed

☐ Access search results or metadata [?](#)

SPL query

[Open in search](#)

```
index=internship "action=file accessed"  
| stats count AS file_access_attempts
```

Time range

Default

Time range set by dashboard source default value

\$global_time.earliest\$ - \$global_time.latest\$

Configure in source editor

i 1 visualization will be updated

Cancel

Apply and close

- Malware Types Detected

Edit data source

Data source name

Malware_Detection

☐ Access search results or metadata [?](#)

SPL query

[Open in search](#) [↗](#)

```
index=internship action="malware detected"
| stats count AS malware_events
```

Time range

Default ▼

Time range set by dashboard source default value

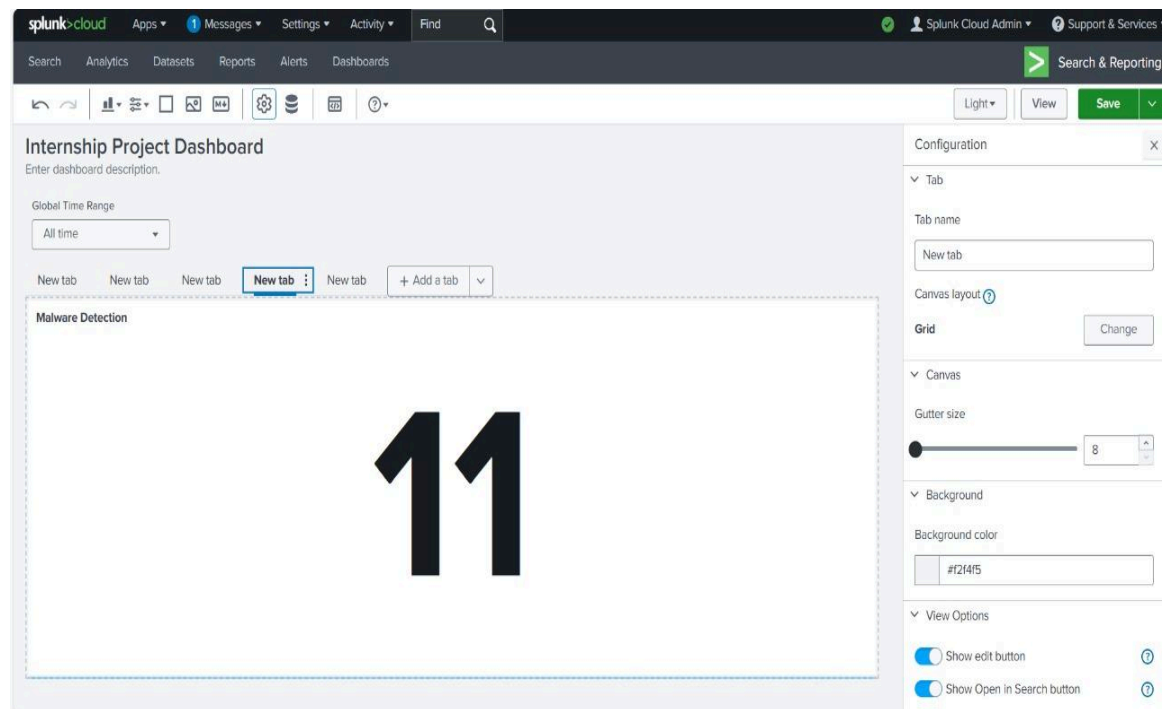
\$global_time.earliest\$ - \$global_time.latest\$

Configure in source editor

Event Sampling

Cancel

Apply and close



- Connection Attempts by User

Edit data source

Data source name

Susoicious IP

☐ Access search results or metadata [?](#)

SPL query

[Open in search](#)

```
index=internship (ip="203.0.113.*" OR ip="198.51
.100.*")
| stats count AS suspicious_ip_events
```

Time range

Default

Time range set by dashboard source default value

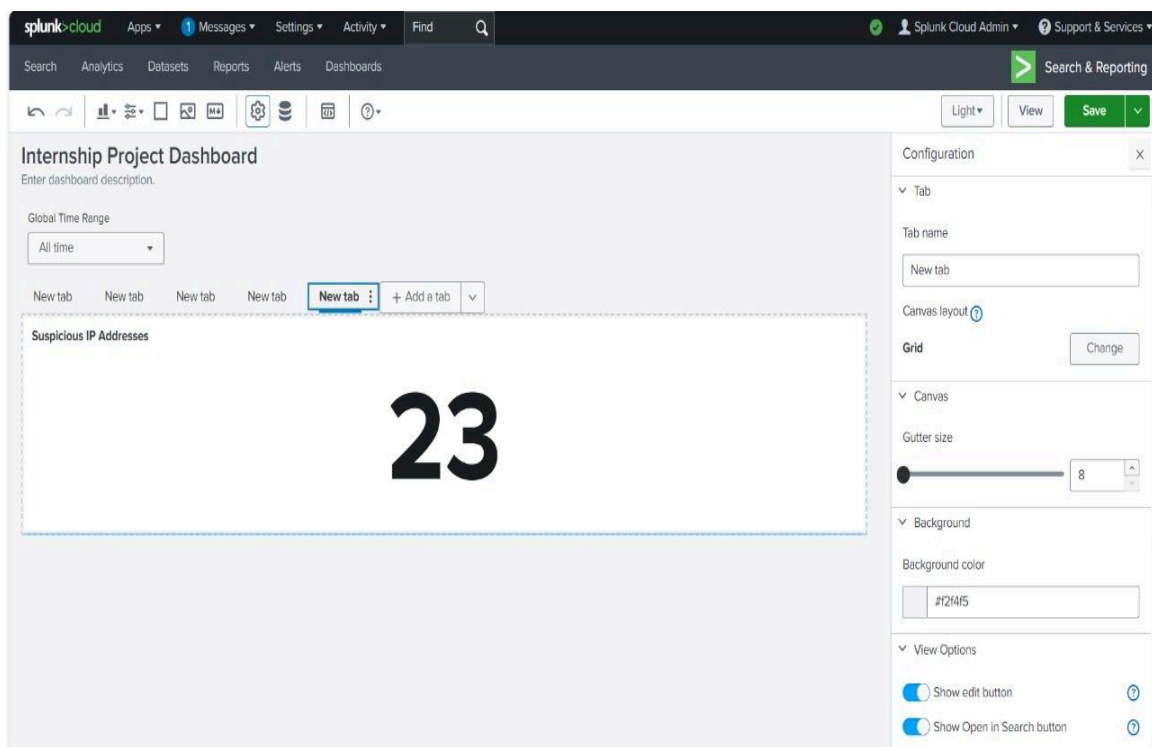
\$global_time.earliest\$ - \$global_time.latest\$

Configure in source editor

Event Sampling

Cancel

Apply and close



-Events By User

Edit data source

Data source name

Events_By_User

☐ Access search results or metadata [?](#)

SPL query

[Open in search](#)

```
index=internship
| stats count BY user
| sort - count
```

Time range

Default

Time range set by dashboard source default value

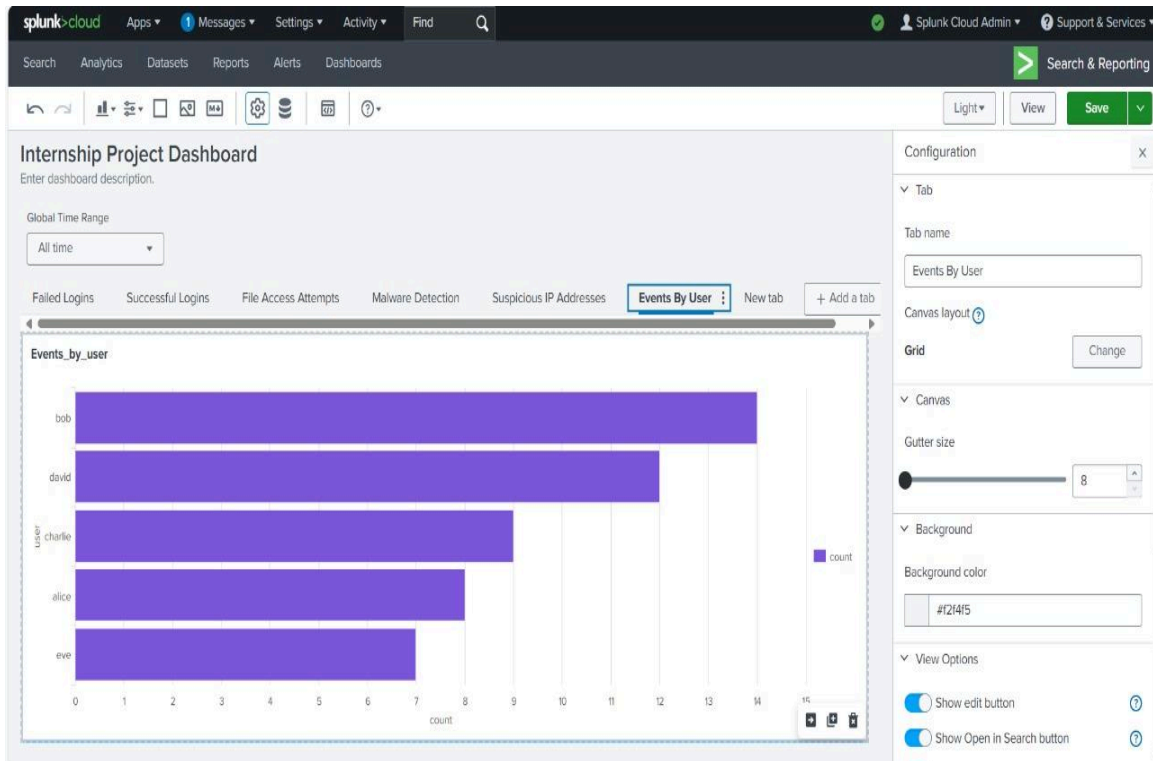
\$global_time.earliest\$ - \$global_time.latest\$

Configure in source editor

Event Sampling

Cancel

Apply and close



-Events Over Time

New data source

Data source name

☐ Access search results or metadata [?](#)

SPL query

[Open in search](#) [↗](#)

```
index=internship  
| timechart count BY action
```

Time range

Default ▼

Time range set by dashboard source default value

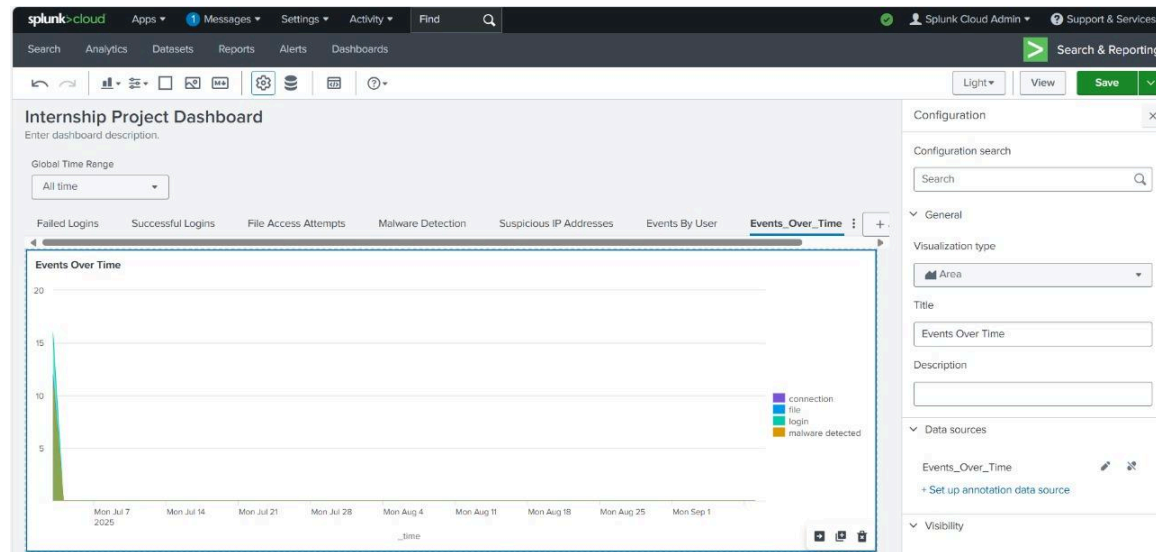
\$global_time.earliest\$ - \$global_time.latest\$

Configure in source editor

i 1 visualization will be updated

Cancel

Apply and close



5. Incident Findings & Classification

5.1 Login Activity

- **Successful logins:** 12 (Alice: 3, Bob: 4, Charlie: 1, David: 2, Eve: 2)

- **Failed logins:** 4 (Alice: 1, Bob: 2, Charlie: 1, David: 1)

⚠ **Suspicious Alert #1 (Medium):** Bob had multiple failed and successful logins, indicating potential brute-force or weak password usage.

5.2 File Access

- **Total events:** 11

- **Users:** Bob (4), David (3), Eve (2), Alice (1), Charlie (1)

⚠ **Suspicious Alert #2 (Medium):** Bob accessed files immediately after failed logins — may indicate persistence attempts.

5.3 Malware Detection

- **Total malware events:** 11

- **Types detected:** Trojan (5), Rootkit (2), Spyware (1), Worm (1), Ransomware (1)

- **Users flagged:** Bob, Alice, David, Eve, Charlie

⚠ **Suspicious Alert #3 (High):** Bob flagged for Trojan and Ransomware → critical compromise risk.

5.4 Connection Attempts

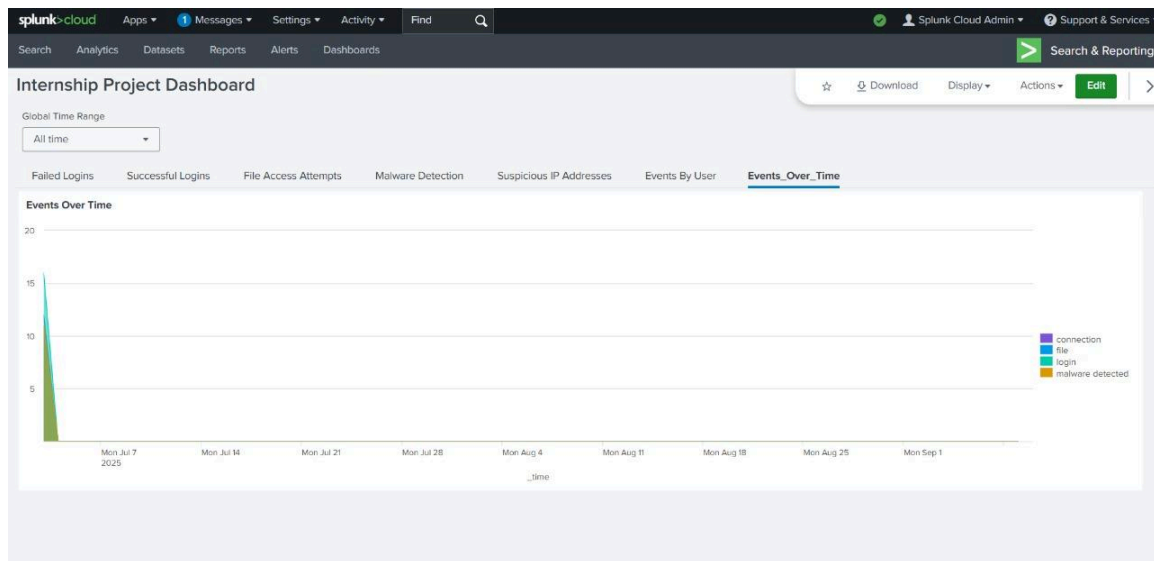
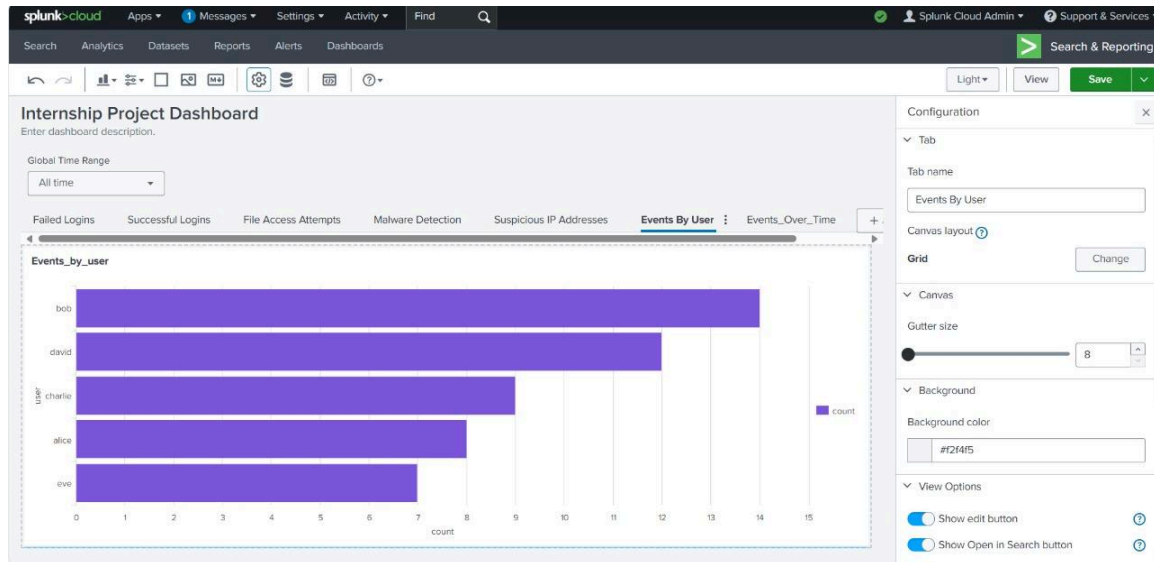
- **Total:** 9

- **Users:** Charlie (4), David (3), Bob (2)

⚠ **Suspicious Alert #4 (High):** Charlie initiated multiple connection attempts from varying IPs → possible reconnaissance/scanning activity.

5.5 Dashboard Overview

A Splunk Dashboard was created with panels displaying trends in logins, malware detections, file accesses, and connection attempts for real-time SOC monitoring.



6. Incident Timeline (Sample)

Timestamp	User	Event Type	Severity	Notes
2025-07-03 05:48:14	Bob	Malware – Trojan	High	First Trojan detection
2025-07-03 07:02:14	Alice	Login Failed	Low	Possible mistyped password
2025-07-03 09:10:14	Bob	Malware – Ransomware	High	Critical infection detected
2025-07-03 09:15:22	Bob	File Accessed	Medium	Suspicious access after failed login
2025-07-03 10:05:14	Charlie	Connection Attempt	High	Multiple IPs used – scanning suspected

7. Impact & Remediation

Impacts Identified:

- Brute-force risk from repeated login failures.
- Malware spread across multiple users (especially Bob).
- Unauthorized/suspicious file access.
- Possible reconnaissance via multiple connection attempts.

Recommended Remediation Steps:

- High Alerts (Bob & Charlie): Immediate account isolation, malware scan, and password reset.
- Medium Alerts (File Access): Monitor activity, enforce access controls.
- General: Apply endpoint protection, enforce MFA, block suspicious IPs, and strengthen user training.

8. Conclusion

The project successfully simulated a Security Operations Center (SOC) workflow:

- Suspicious events were identified.
- Alerts were classified by severity.
- Incidents were documented with timelines, impact, and remediation.
- A Splunk dashboard was built for continuous monitoring.

Final Outcome: Splunk effectively detected malicious behavior (brute-force attempts, malware infections, unauthorized file access, and scanning). This confirms its role as a powerful SIEM tool for real-world enterprise security monitoring.

Prepared By:

Meghan Diwate

SOC Analyst / Ethical Hacker