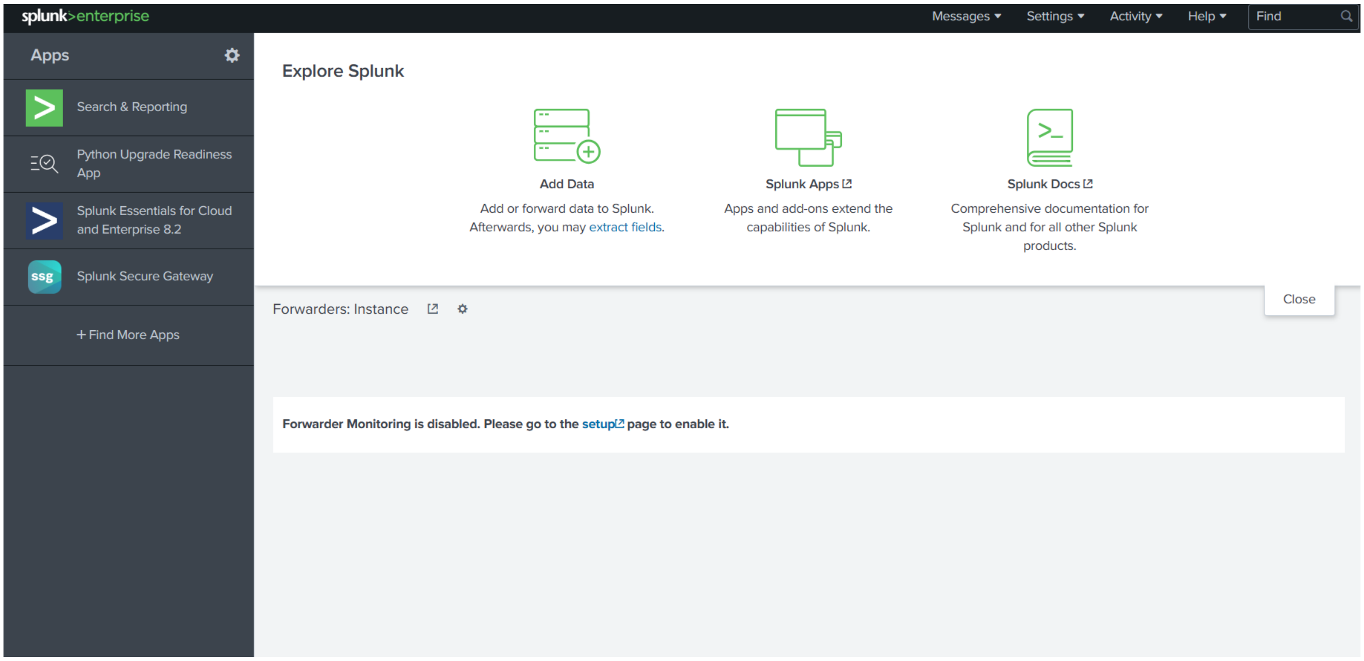
Splunk is one of the most widely used Security Information and Event Management (SIEM) solutions in the enterprise environment. It helps aggregate data from different data sources in the enterprise environment to help enhance security monitoring. However, sometimes, this data becomes too overwhelming for analysts. In this room, we will learn how an analyst can better organize the data in Splunk. Broadly, we will have the following learning objectives

Organizing data in Splunk

Splunk does a great job of aggregating the security-related data of an organization's assets in a single place. However, this data is huge, difficult to grasp, and make sense of. We will learn how to make sense of the data in this room.

When we open Splunk, this is the screen we might be greeted with after signing in.



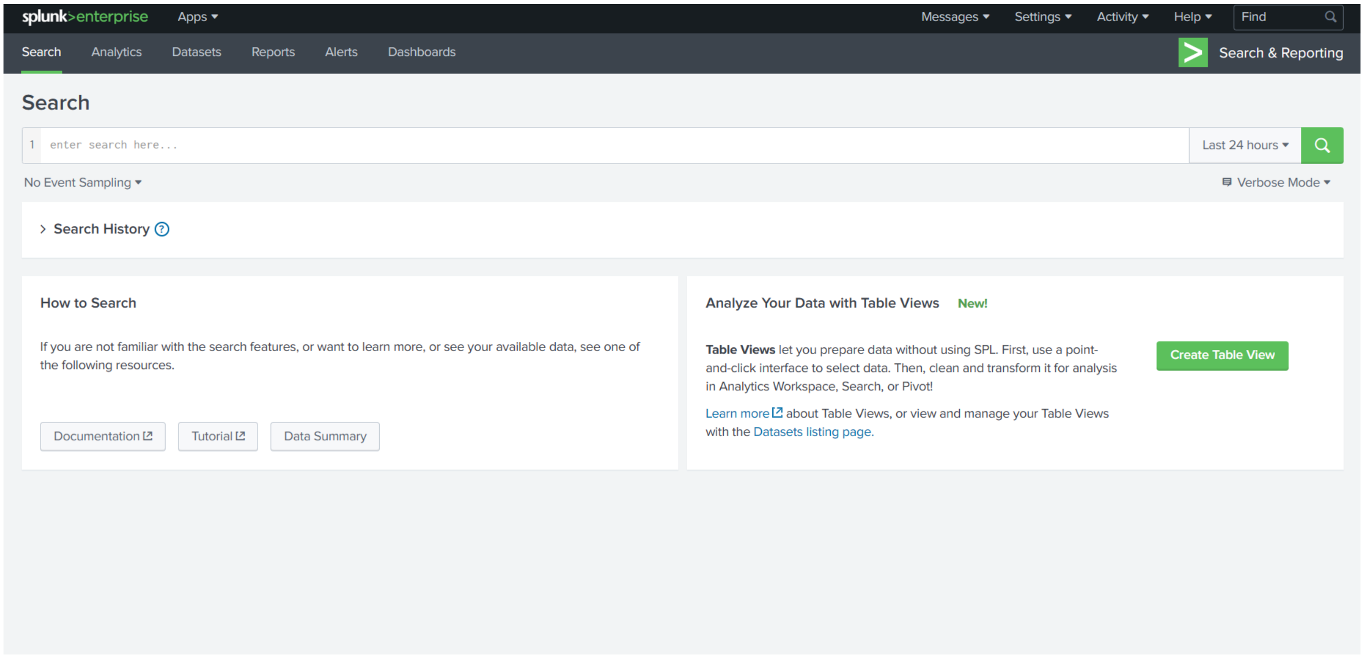
Add or forward data to Splunk. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk.

Comprehensive documentation for Splunk and for all other Splunk products.

Forwarder Monitoring is disabled. Please go to the setup page to enable it.

To move forward, go to the first tab on the left menu, **Search & Reporting**. Clicking that, we see the following interface.



How to Search

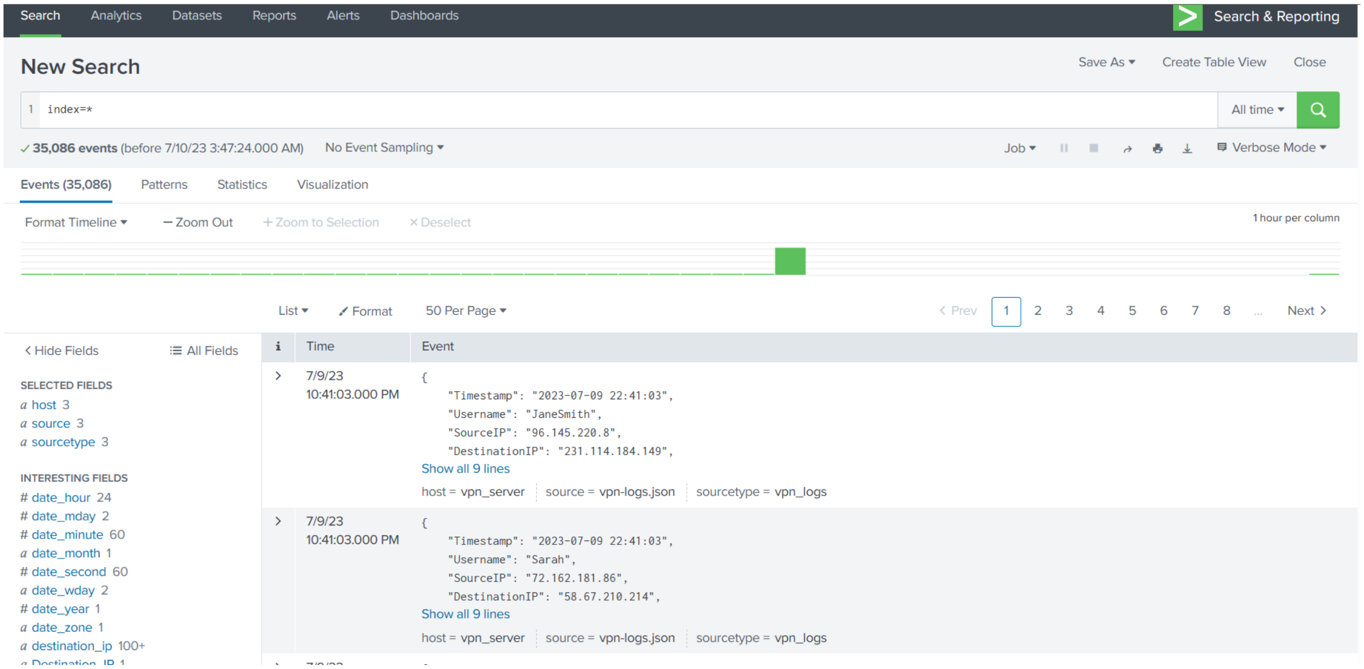
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views New!

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!

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

Now, we can see that we have an interface for the Search app. For starters, we can start a search with the search term `index=*` to see what data we have here. We have set the time window to 'all time' to see the data historically present here as well.



```
index=*
```

✓ 35,086 events (before 7/10/23 3:47:24.000 AM)

SELECTED FIELDS
a host 3
a source 3
a sourcetype 3

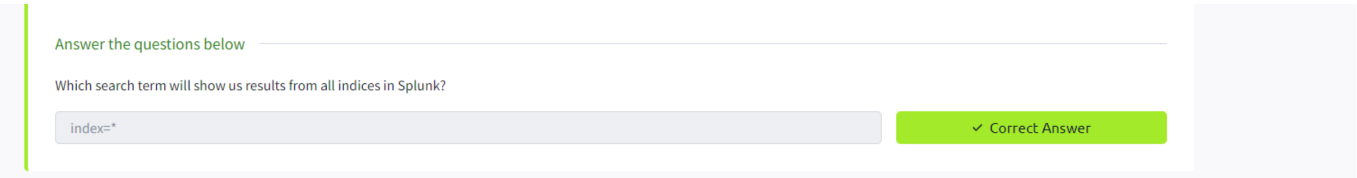
INTERESTING FIELDS
# date_hour 24
# date_mday 2
# date_minute 60
a date_month 1
# date_second 60
a date_wday 2
# date_year 1
a date_zone 1
a destination_ip 100+

```
7/9/23 10:41:03.000 PM
{
    "Timestamp": "2023-07-09 22:41:03",
    "Username": "JaneSmith",
    "SourceIP": "96.145.220.8",
    "DestinationIP": "231.114.184.149",
Show all 9 lines
host = vpn_server   source = vpn-logs.json   sourcetype = vpn_logs

7/9/23 10:41:03.000 PM
{
    "Timestamp": "2023-07-09 22:41:03",
    "Username": "Sarah",
    "SourceIP": "72.162.181.86",
    "DestinationIP": "58.67.210.214",
Show all 9 lines
host = vpn_server   source = vpn-logs.json   sourcetype = vpn_logs
```

Looking at the above screenshot, we can feel overwhelmed. There are more than 35000 events present in this data. If we are to sift through this data manually, it will make our lives difficult instead of making them easier. Therefore, looking at raw data is often not a good idea when our goal is to get an overview of an organisation's security posture. It also doesn't give us much information about the threats and attacks launched against the organization. Now this is just a sample of data in Splunk that we have added for this room. In production, we should avoid running searches for 'all time' as they can add undue load on the Splunk search head and make other searches difficult and slow.

The above-mentioned problems are bound to appear when we deal with a lot of data. Splunk is a data analysis platform that provides solutions for these problems. In the coming tasks, we will see how to aggregate and visualize this data to find answers to our problems.



Answer the questions below

Which search term will show us results from all indices in Splunk?

index=*

Creating reports for recurring searches

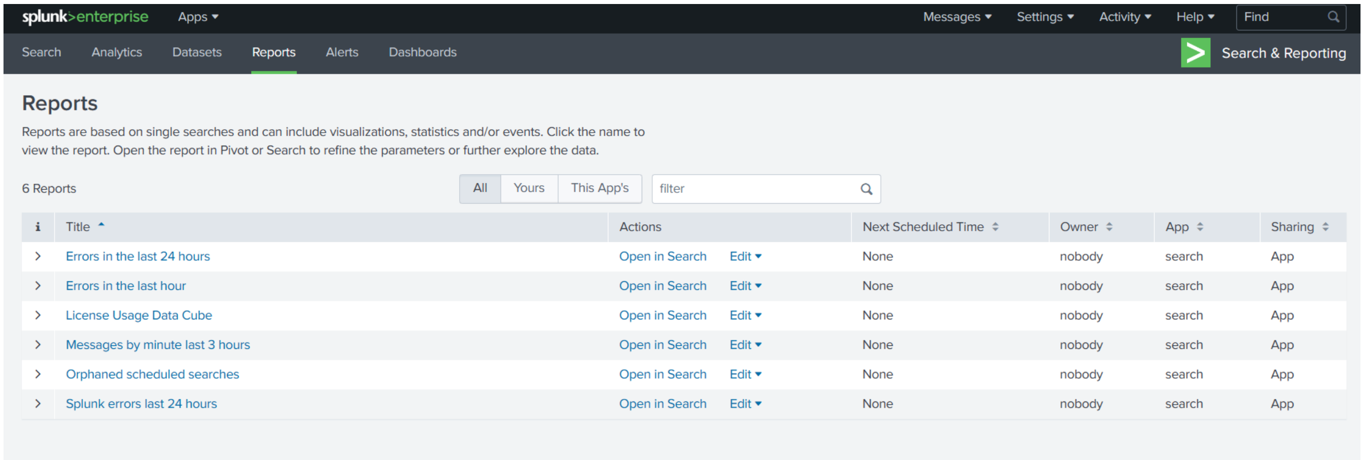
Until now, we have been using Splunk for broad searches mainly. However, we often need to run specific searches from time to time. For example, a certain organization might want to run a search every 8 hours when a new shift of SOC analysts arrives or is leaving. For this purpose, creating a report that will run at a specific time is efficient. Reports will then run the searches and save the results for viewing when the analysts for the incoming shift arrive.

Reports can also help reduce the load on the Splunk search head. For example, if multiple searches need to be run at the start of every shift, running them simultaneously can increase the search head's load and processing times. If searches are scheduled with 5 or 10-minute intervals, they will accomplish two tasks.

1. The searches will run automatically without any user interaction.
2. The searches will not run simultaneously, reducing the possibility of errors or inefficiency.

Before moving forward, please start the attached VM by clicking the **Start Machine** button on the top right corner. Once the IP address is visible, you can use the URL: http://10-10-99-1.p.thmlabs.com to access the Splunk instance. It might take 3-5 minutes for the Splunk instance to start. A VPN connection is not needed to access the Splunk instances.

Continuing from the previous task, move to the Reports tab to look at already saved reports in Splunk. We will see the following interface.



Reports

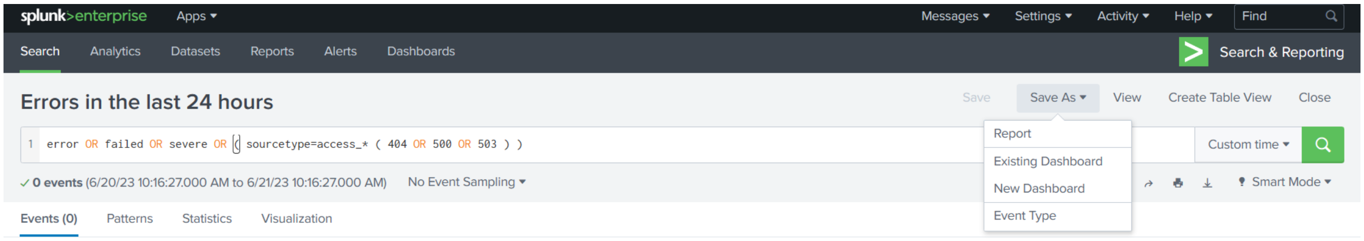
Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

6 Reports

i	Title ▴	Actions		Next Scheduled Time ⇕	Owner ⇕	App ⇕	Sharing ⇕
›	Errors in the last 24 hours	Open in Search	Edit ▾	None	nobody	search	App
›	Errors in the last hour	Open in Search	Edit ▾	None	nobody	search	App
›	License Usage Data Cube	Open in Search	Edit ▾	None	nobody	search	App
›	Messages by minute last 3 hours	Open in Search	Edit ▾	None	nobody	search	App
›	Orphaned scheduled searches	Open in Search	Edit ▾	None	nobody	search	App
›	Splunk errors last 24 hours	Open in Search	Edit ▾	None	nobody	search	App

Here, we see a list of reports already saved in Splunk. If we want to view the saved results of a report, we can click on the report's name. However, if we want to run a new search using the same query as the one in a report, we can use the 'Open in Search' option. The 'Edit' option allows us to edit the reports. The 'Next Scheduled Time' tab shows when the report will run again. We can also see the report's owner and its associated permissions. Please note that we have selected 'All' reports to be shown in the view above. There are options for viewing only the logged-in user's reports, as well as for viewing the reports added by the App.

To create a new report, we can run a search and use the Save As option to save the search as a report.

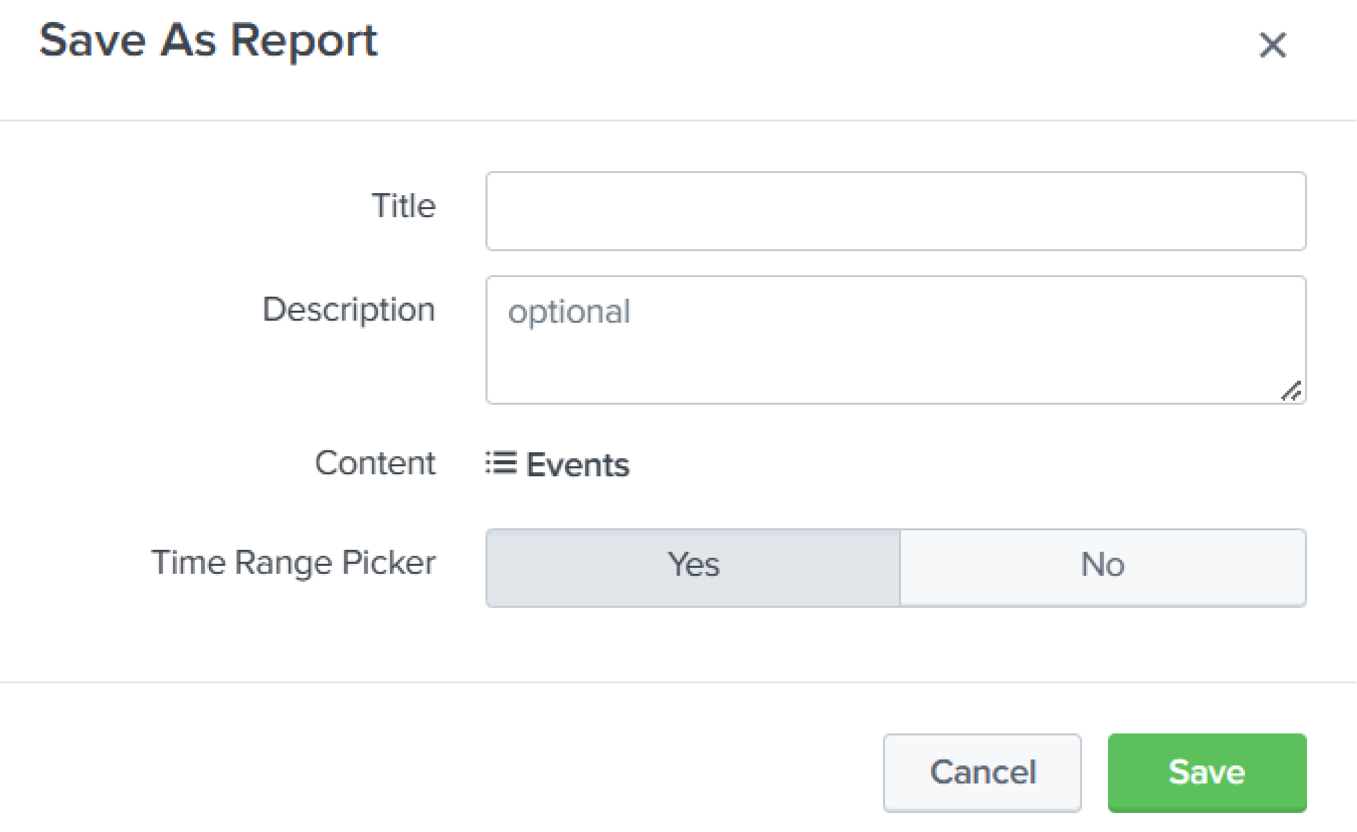


Errors in the last 24 hours

```
error OR failed OR severe OR ( sourcetype=access_* ( 404 OR 500 OR 503 ) )
```

✓ 0 events (6/20/23 10:16:27.000 AM to 6/21/23 10:16:27.000 AM)

Once we click the option to Save As Report, we see the following window.

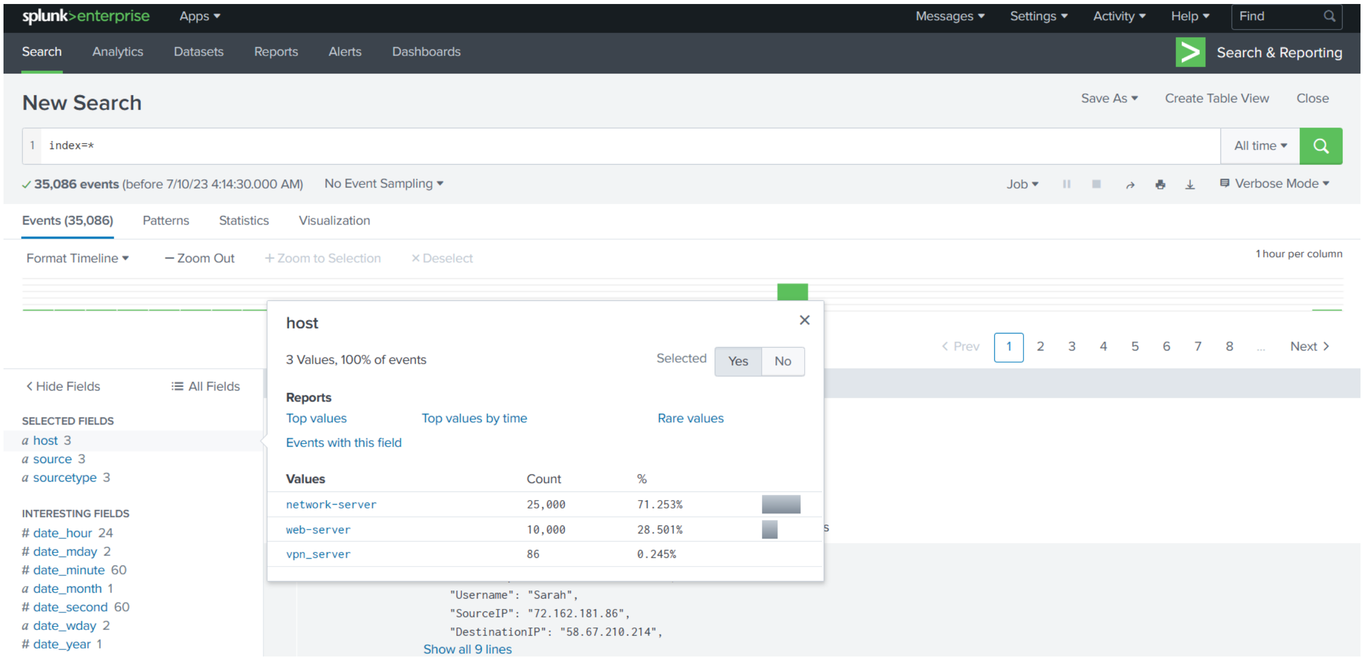


Save As Report

Title	
Description	optional
Content	☰ Events
Time Range Picker	[✓ Yes] No

Filling in the required data and clicking the 'Save' option here will save the search as a report.

Let's practice the same in the attached Splunk instance. We ran a search in the previous task. To create a report on a search, we will first have to understand the data. On the left tab, we will see some fields Splunk has identified that might interest us. Let's click on hosts to see the number of hosts sending logs to our Splunk instance.



New Search

```
index=*
```

✓ 35,086 events (before 7/10/23 4:14:30.000 AM) No Event Sampling

Events (35,086)

host

3 Values, 100% of events — Selected: Yes No

Reports: Top values · Top values by time · Rare values · Events with this field

Values	Count	%
network-server	25,000	71.253%
web-server	10,000	28.501%
vpn_server	86	0.245%

SELECTED FIELDS
- a host 3
- a source 3
- a sourcetype 3

INTERESTING FIELDS
- # date_hour 24
- # date_mday 2
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 2
- # date_year 1

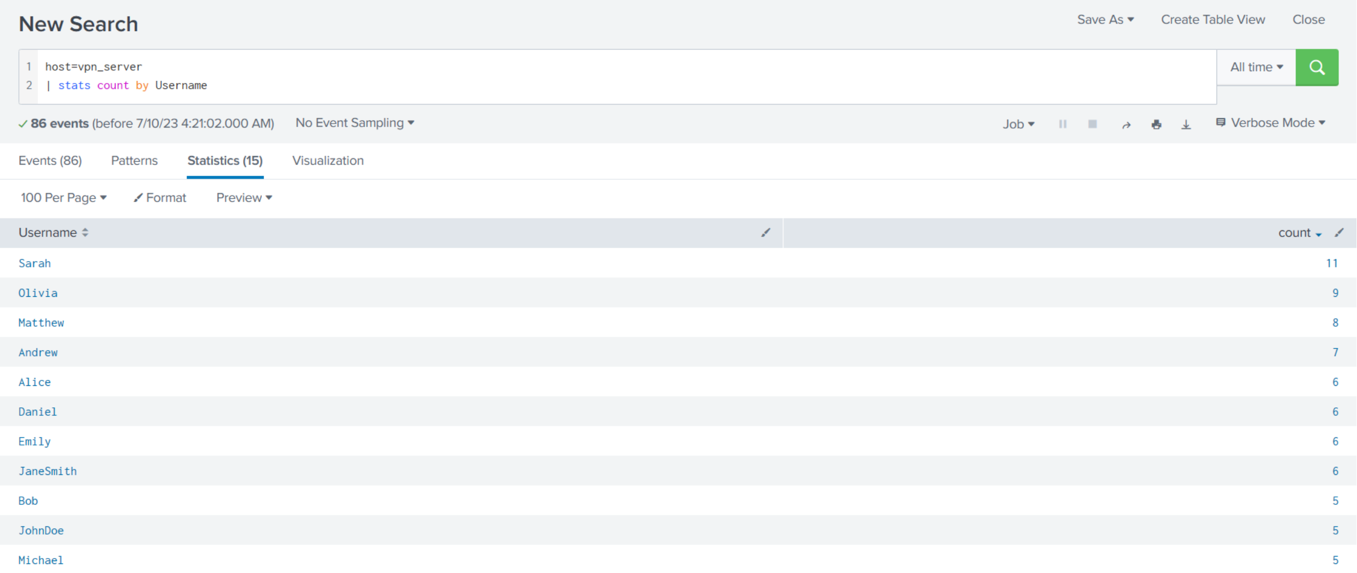
```
"Username": "Sarah",
"SourceIP": "72.162.181.86",
"DestinationIP": "58.67.210.214",
```

Show all 9 lines

So, we have 3 hosts; network-server, web-server, and vpn_server. They are all sending different numbers of events. If we are to determine the number of times each VPN user logged in during our given time window (which is 'all time' for this room), we will run the following query.

```
host=vpn_server | stats count by Username
```

This is what we get when we run this query in our instance.



New Search

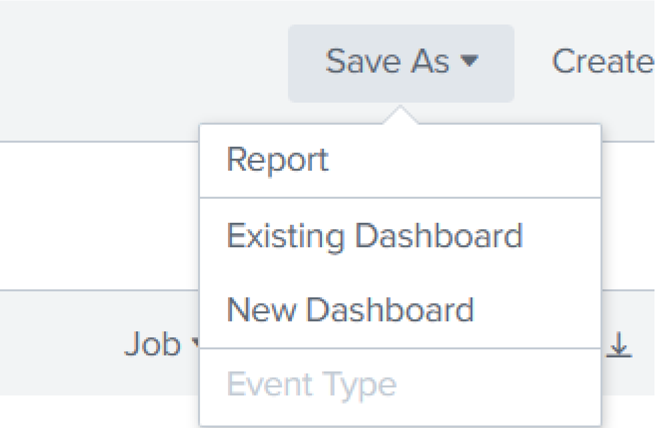
```
host=vpn_server
| stats count by Username
```

✓ 86 events (before 7/10/23 4:21:02.000 AM) No Event Sampling

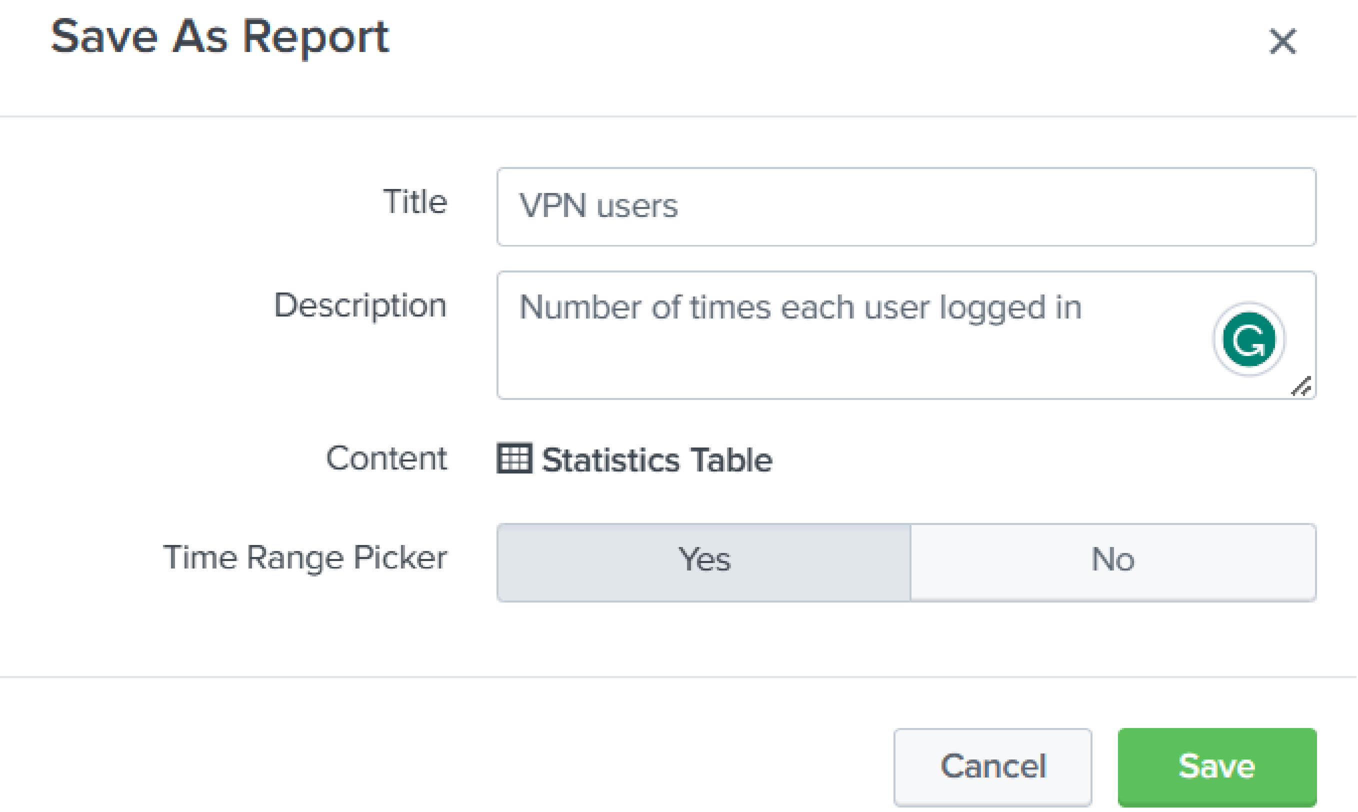
Statistics (15)

Username	count
Sarah	11
Olivia	9
Matthew	8
Andrew	7
Alice	6
Daniel	6
Emily	6
JaneSmith	6
Bob	5
JohnDoe	5
Michael	5

In a SOC environment, we might want to track users who logged in during a certain time window. This requirement might be repetitive. SOC analysts can create a report for this requirement that will run every few hours for ease of use. Let's practice that based on what we learned in this task. First, we click 'Save As' and select 'Report'.



We fill in the required information.



Save As Report

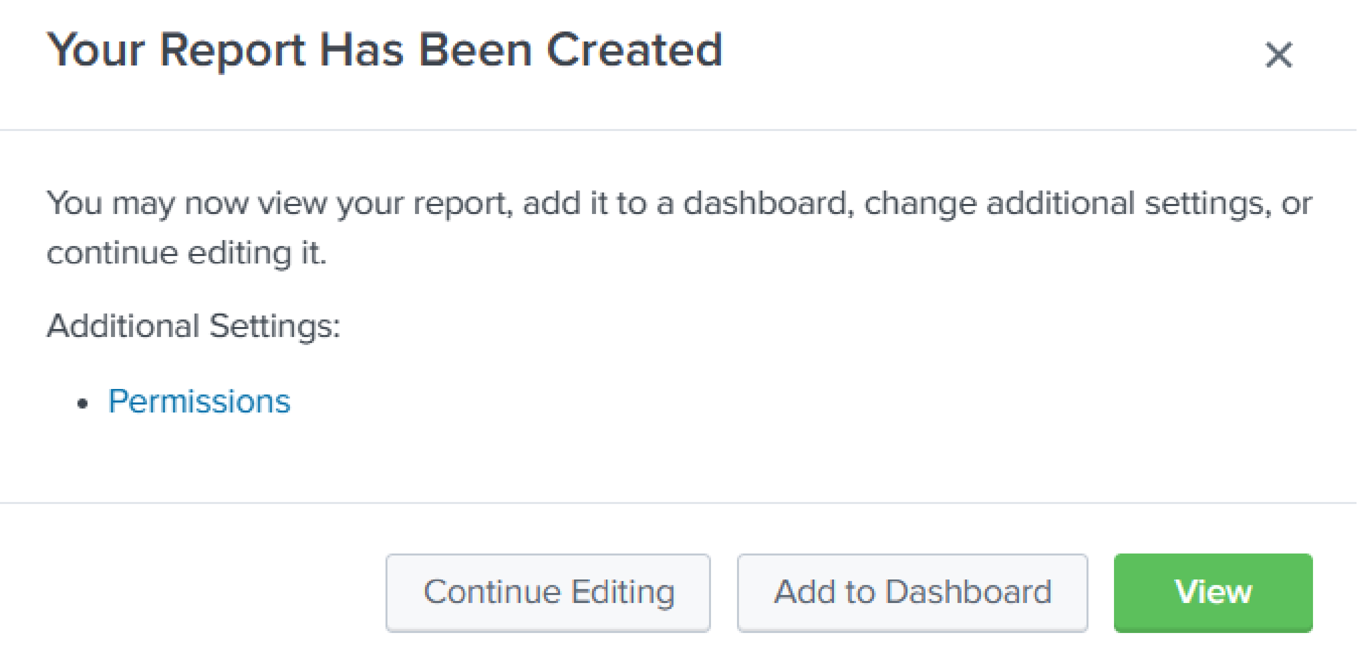
Title: VPN users

Description: Number of times each user logged in

Content: Statistics Table

Time Range Picker: [✓ Yes] No

Here, we can see the Content for this report will be a 'Statistics Table' because we used 'stats count' in our query. The 'Time Range Picker' has been set to 'Yes'. This means running the report will give us a time-range picker option. When we click 'Save', we get the following prompt, telling us the report has been created.



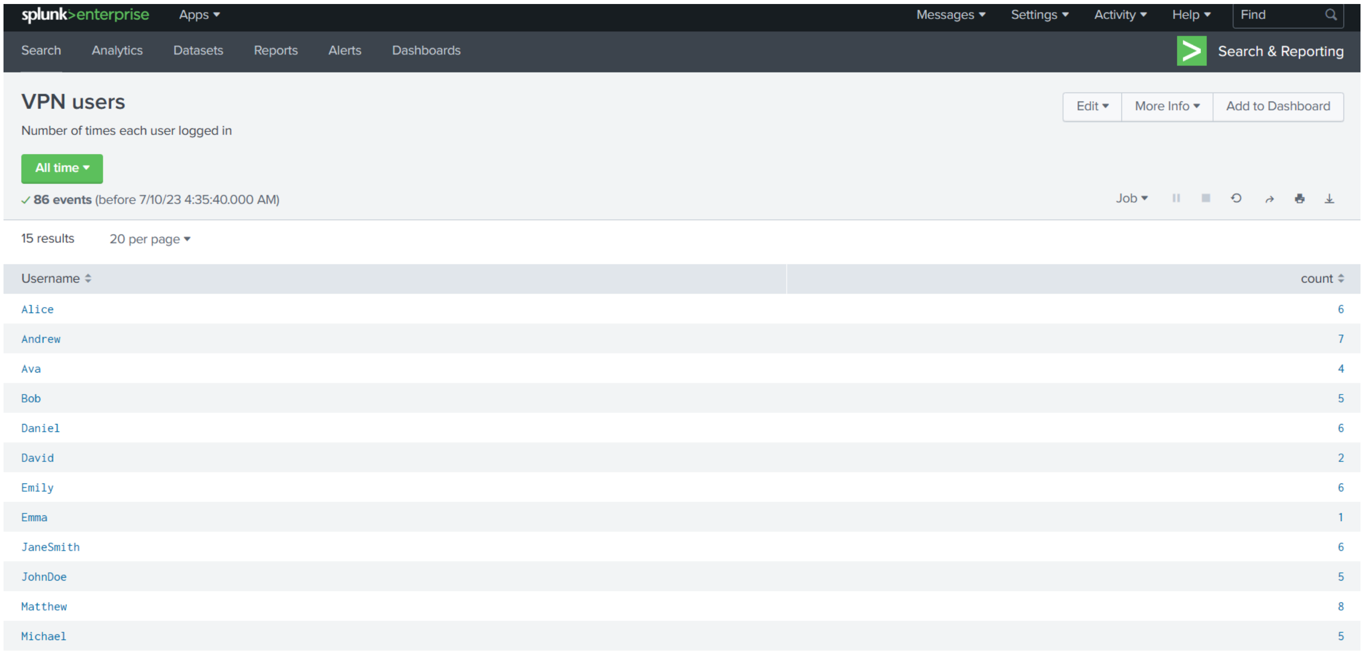
Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions

We can click the 'View' option to view our report. This is how it will look.



VPN users

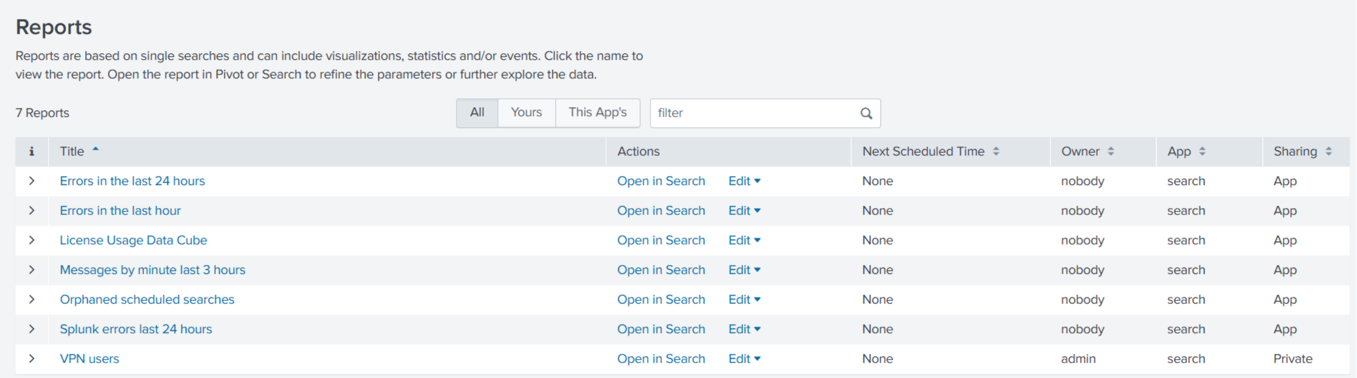
Number of times each user logged in

✓ 86 events (before 7/10/23 4:35:40.000 AM)

15 results

Username	count
Alice	6
Andrew	7
Ava	4
Bob	5
Daniel	6
David	2
Emily	6
Emma	1
JaneSmith	6
JohnDoe	5
Matthew	8
Michael	5

On the reports tab, we can see our report now.



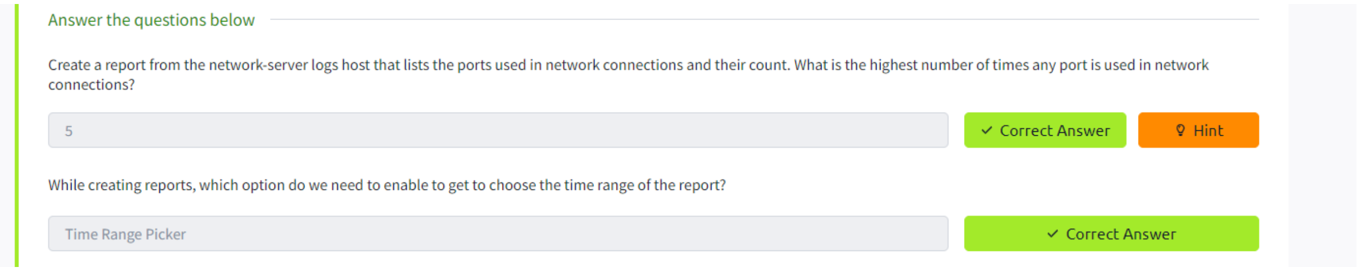
Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

7 Reports

i	Title	Actions		Next Scheduled Time	Owner	App	Sharing
>	Errors in the last 24 hours	Open in Search	Edit ▾	None	nobody	search	App
>	Errors in the last hour	Open in Search	Edit ▾	None	nobody	search	App
>	License Usage Data Cube	Open in Search	Edit ▾	None	nobody	search	App
>	Messages by minute last 3 hours	Open in Search	Edit ▾	None	nobody	search	App
>	Orphaned scheduled searches	Open in Search	Edit ▾	None	nobody	search	App
>	Splunk errors last 24 hours	Open in Search	Edit ▾	None	nobody	search	App
>	VPN users	Open in Search	Edit ▾	None	admin	search	Private

We see the owner of the report is 'admin', the logged-in user. The 'Sharing' is set to Private. This means that this report can only be accessed by admin. We can use the 'Edit' option to change the permissions and set it to be used by other users



Answer the questions below

Create a report from the network-server logs host that lists the ports used in network connections and their count. What is the highest number of times any port is used in network connections?

5

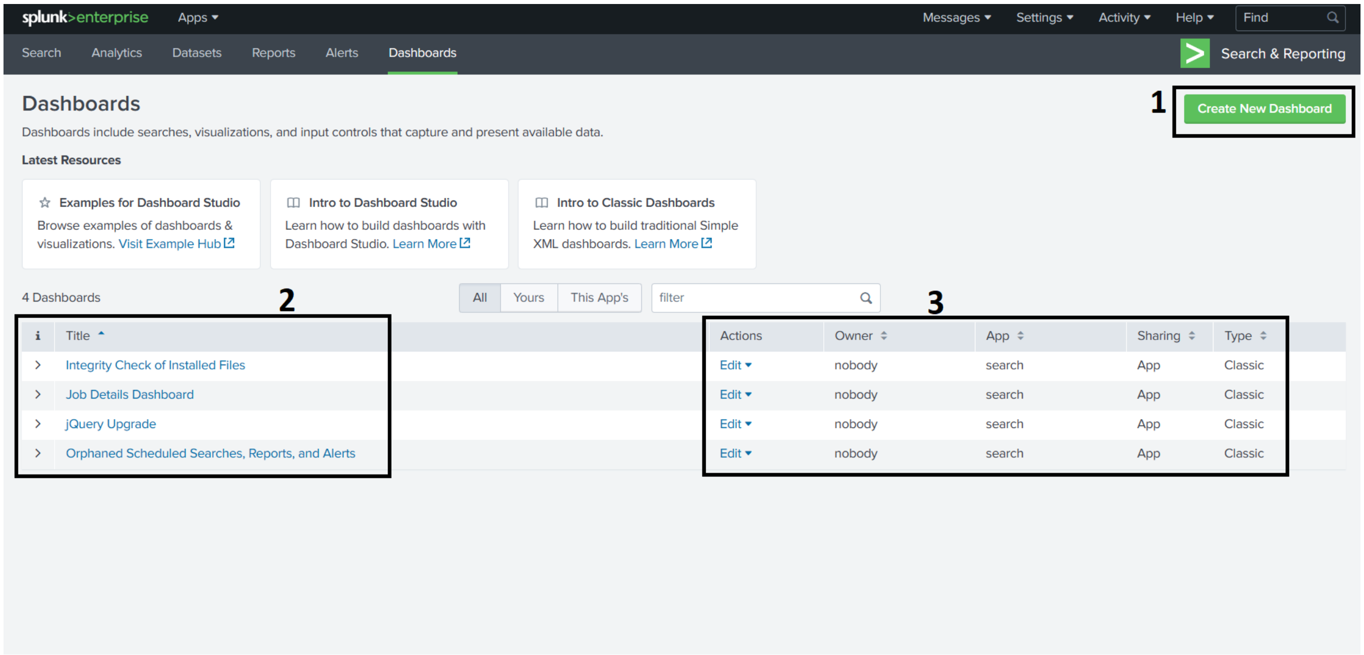
While creating reports, which option do we need to enable to get to choose the time range of the report?

Time Range Picker

Creating Dashboards for Summarizing reports

Splunk provides us with the ability to create dashboards and visualizations. These dashboards and visualizations provide a user with quick info about the data present in Splunk. Dashboards are often created to help give a brief overview of the most important bits of the data. They are often helpful in presenting data and statistics to the management, such as the number of incidents in a given time frame, or for SOC analysts to figure out where to focus, such as identifying spikes and drops in data sources, which might indicate a surge in, say, failed login attempts. The primary purpose of dashboards is to provide a quick visual overview of the available information.

To move forward, let's create a dashboard in the attached VM. To start, move to the Dashboards tab. We will see the below screen.



Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

☆ **Examples for Dashboard Studio**
Browse examples of dashboards & visualizations. Visit Example Hub

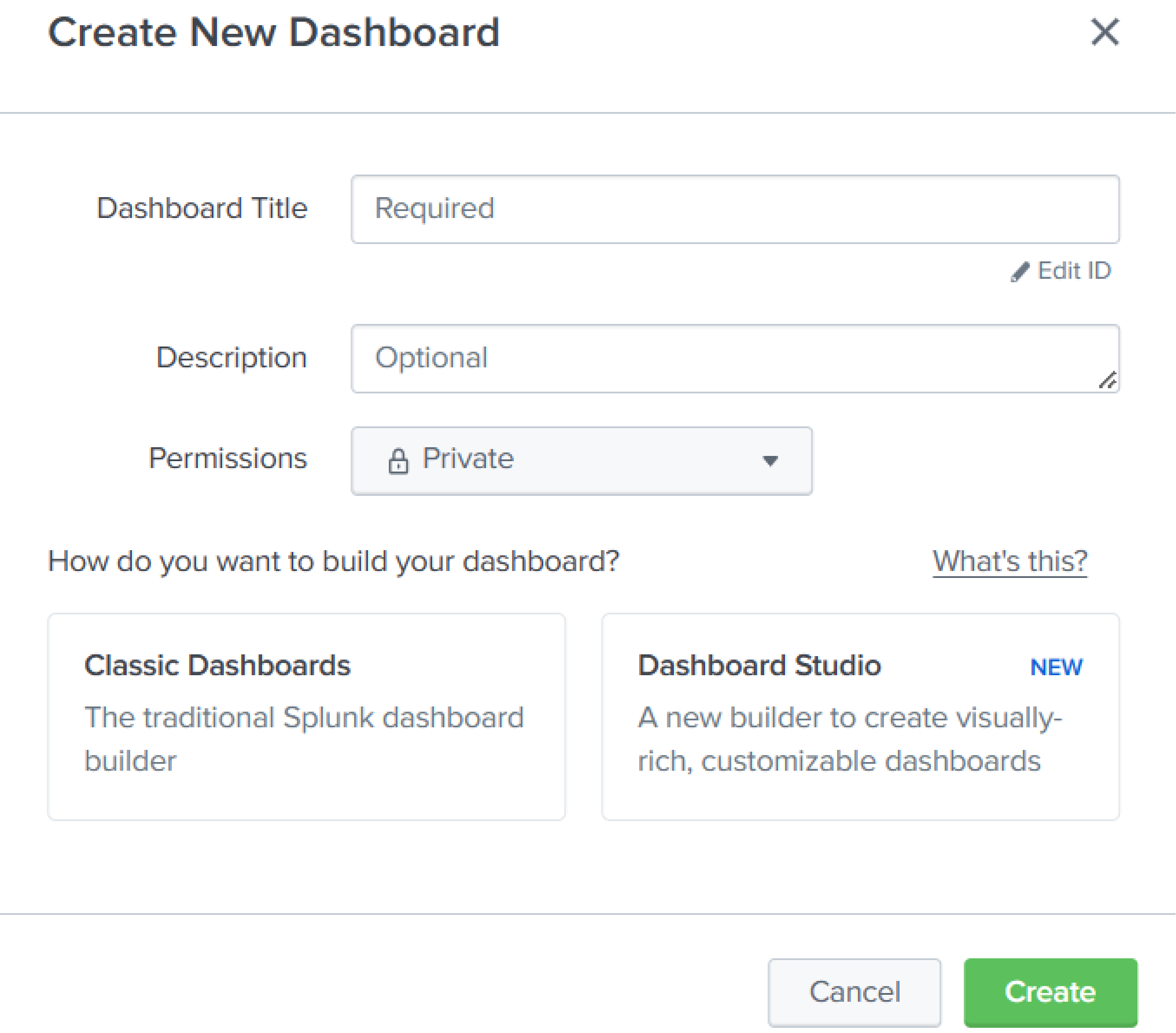
Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More

Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. Learn More

4 Dashboards

i	Title ▴	Actions	Owner ⇕	App ⇕	Sharing ⇕	Type ⇕
>	Integrity Check of Installed Files	Edit ▾	nobody	search	App	Classic
>	Job Details Dashboard	Edit ▾	nobody	search	App	Classic
>	jQuery Upgrade	Edit ▾	nobody	search	App	Classic
>	Orphaned Scheduled Searches, Reports, and Alerts	Edit ▾	nobody	search	App	Classic

In this screen, we see an option to create dashboards labeled as 1 in the screenshot. Labeled as 2 is a list of available dashboards. Please note that we have selected 'All' dashboards here instead of 'Yours' or 'This App's', which can show a different list of dashboards. Labeled as 3 is information about these dashboards, such as owner, permissions, etc. Here, we also find the option to Edit the dashboard's different properties, or set it as the home dashboard. We can also view a dashboard by clicking on the name of the dashboard. However, we don't have any dashboards yet. We can start by creating a dashboard. For that, let's click the **Create Dashboard** option to see the following window.



Create New Dashboard

Dashboard Title: Required

Edit ID

Description: Optional

Permissions: Private

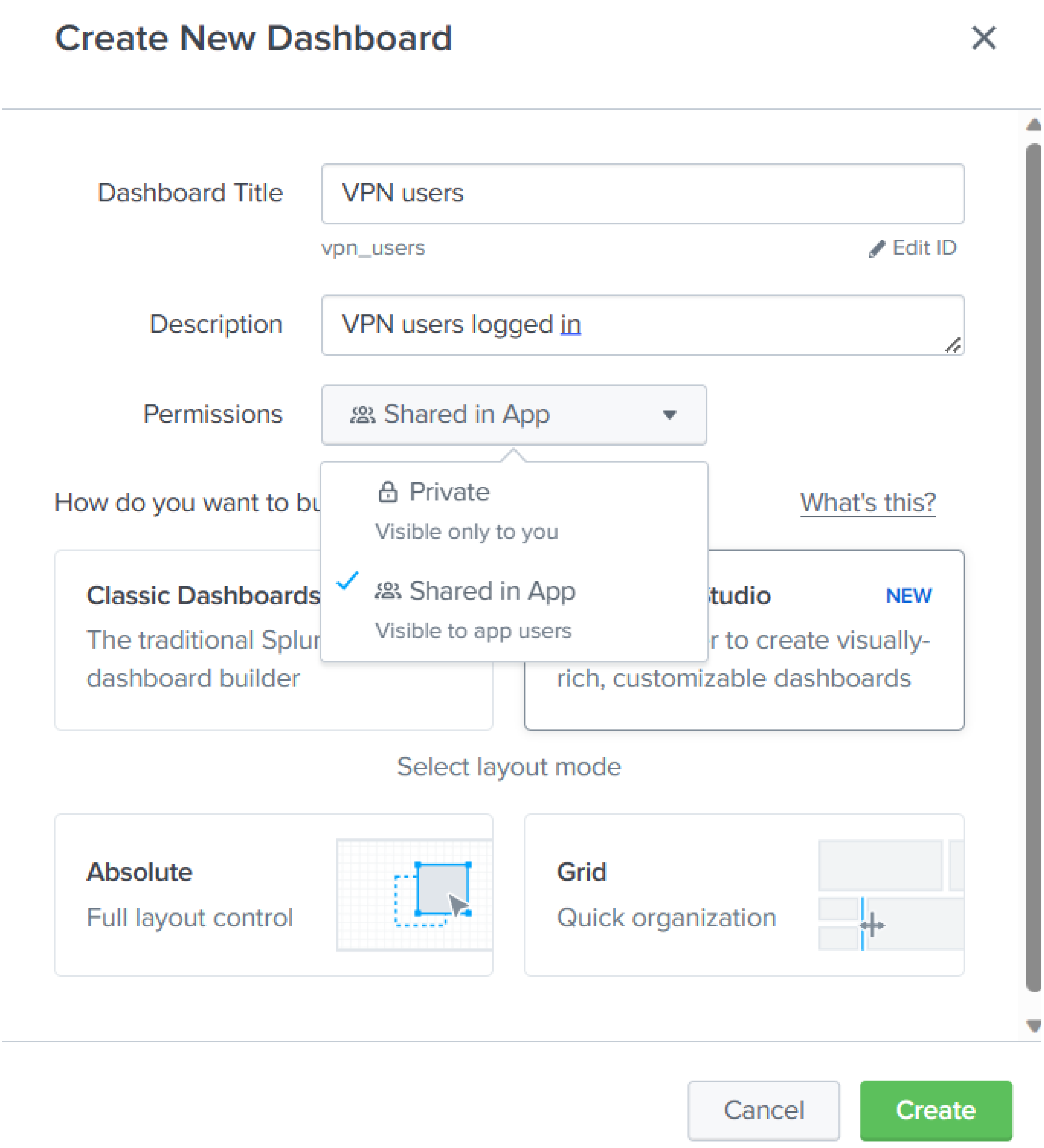
How do you want to build your dashboard?

What's this?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

After filling in the relevant details, such as the name and permissions, we can choose one of the two options for dashboard creation through Classic Dashboards or Dashboard Studio.



Create New Dashboard

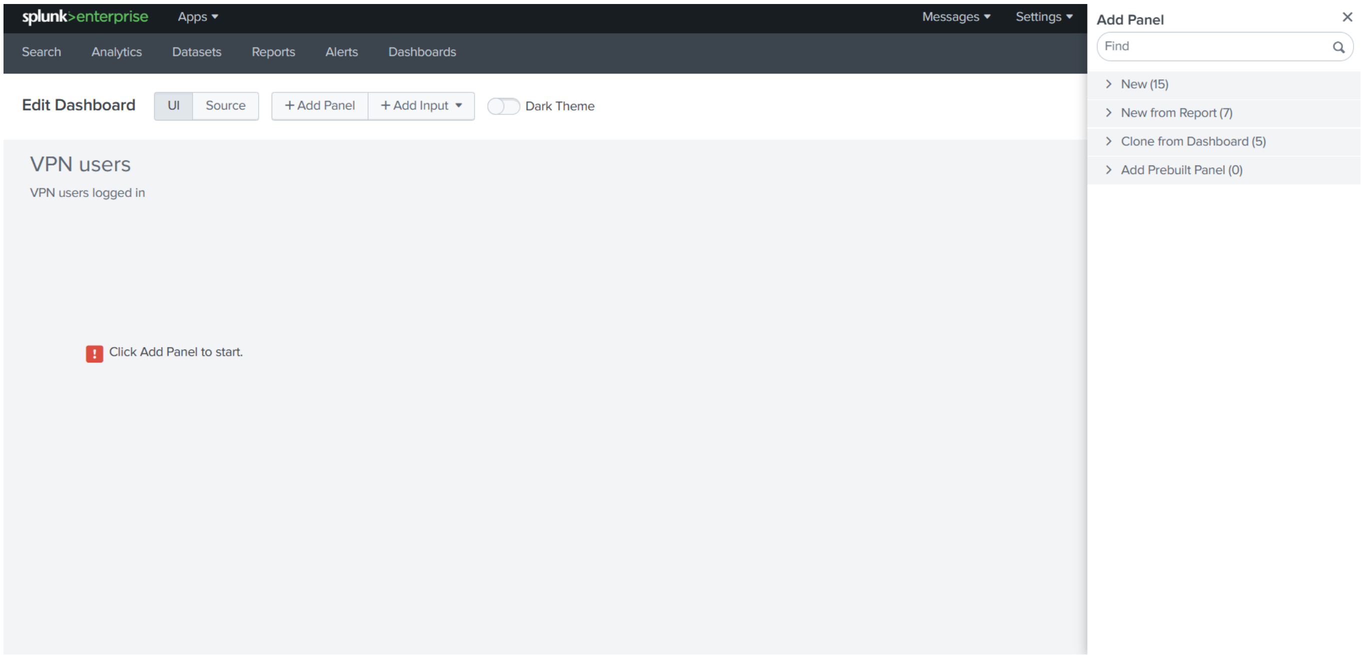
Dashboard Title: VPN users

vpn_users

Description: VPN users logged in

Permissions: Shared in App

We can see that we have set the permissions to 'Shared in App'. This will ensure that the dashboard is also visible to other users of Splunk. We will use the Classic Dashboard approach to create a dashboard for this room. Let's do that and click 'Create'. The Window tells us to 'Click Add Panel to Start'. When we click the 'Add Panel' option, we get the following menu on the right side.

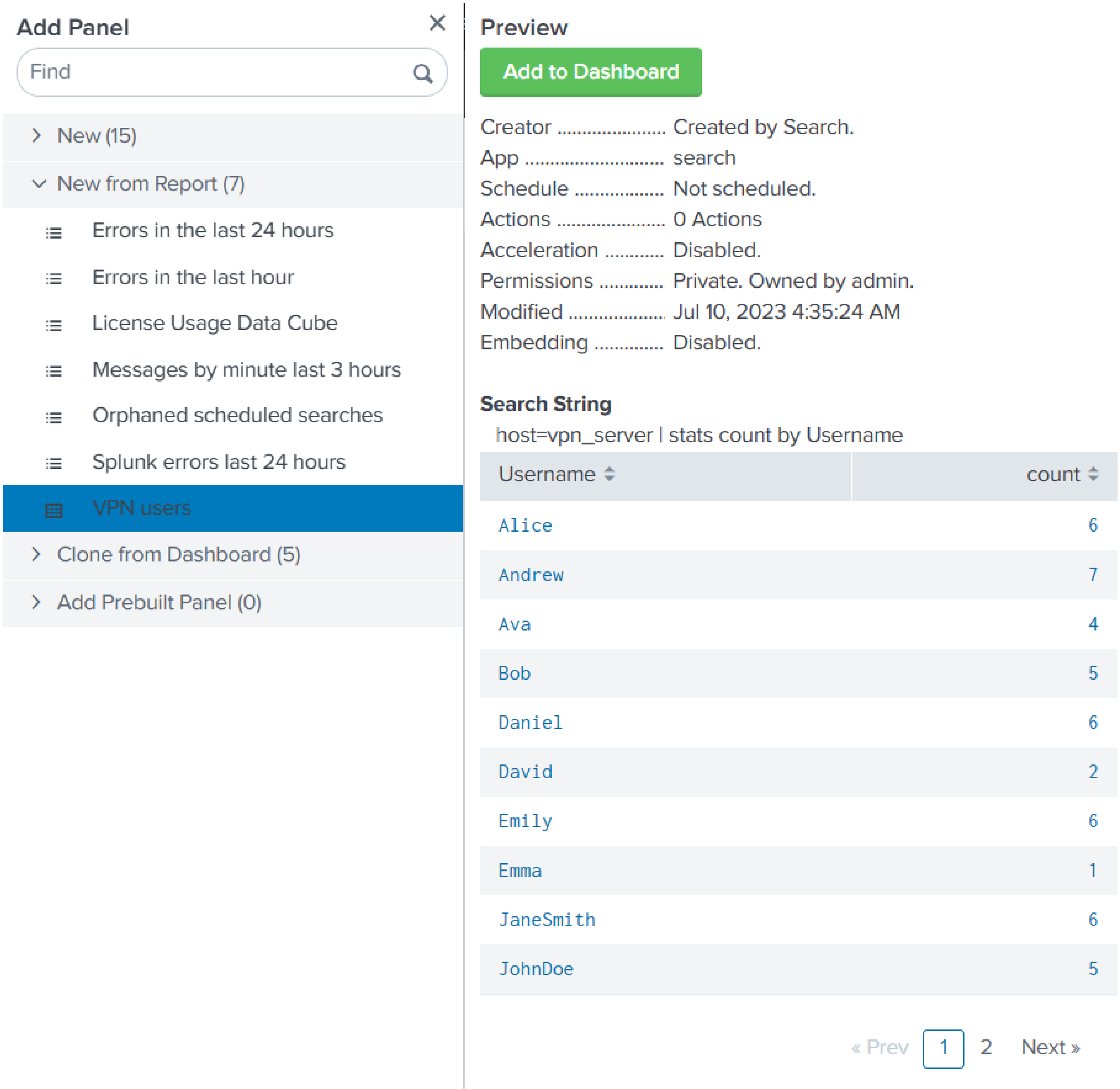


VPN users

VPN users logged in

Click Add Panel to start.

We want to add the results from our report to the Dashboard. We can select the 'New from Report' option to do that.



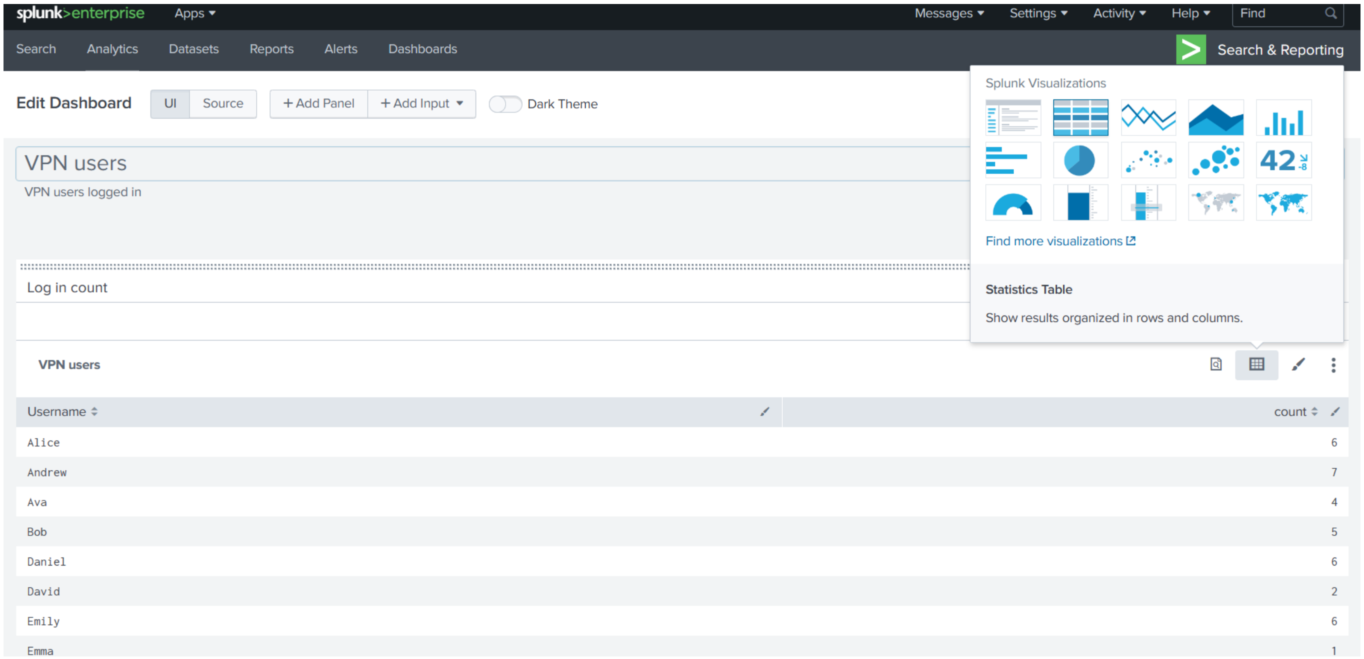
Creator .... Created by Search.
App .... search
Schedule .... Not scheduled.
Actions .... 0 Actions
Acceleration .... Disabled.
Permissions .... Private. Owned by admin.
Modified .... Jul 10, 2023 4:35:24 AM
Embedding .... Disabled.

Search String

```
host=vpn_server | stats count by Username
```

Username	count
Alice	6
Andrew	7
Ava	4
Bob	5
Daniel	6
David	2
Emily	6
Emma	1
JaneSmith	6
JohnDoe	5

The 'Add to Dashboard' option will add these results to our dashboard. However, we were already seeing the results as a report. What benefit will a dashboard provide us? The answer to that lies in visualizations. We can select a visualization from the menu, as shown below.



Statistics Table

Show results organized in rows and columns.

VPN users

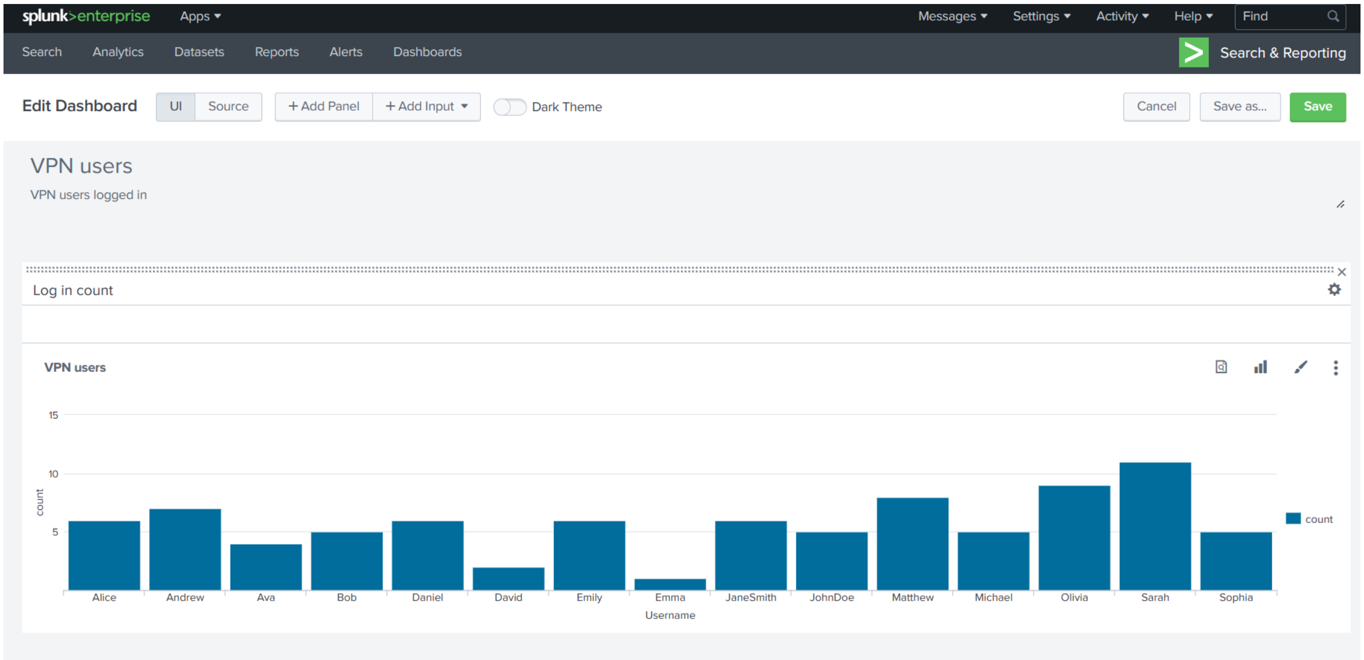
VPN users logged in

Log in count

VPN users

Username	count
Alice	6
Andrew	7
Ava	4
Bob	5
Daniel	6
David	2
Emily	6
Emma	1

Let's select the column chart visualization and check out the results.



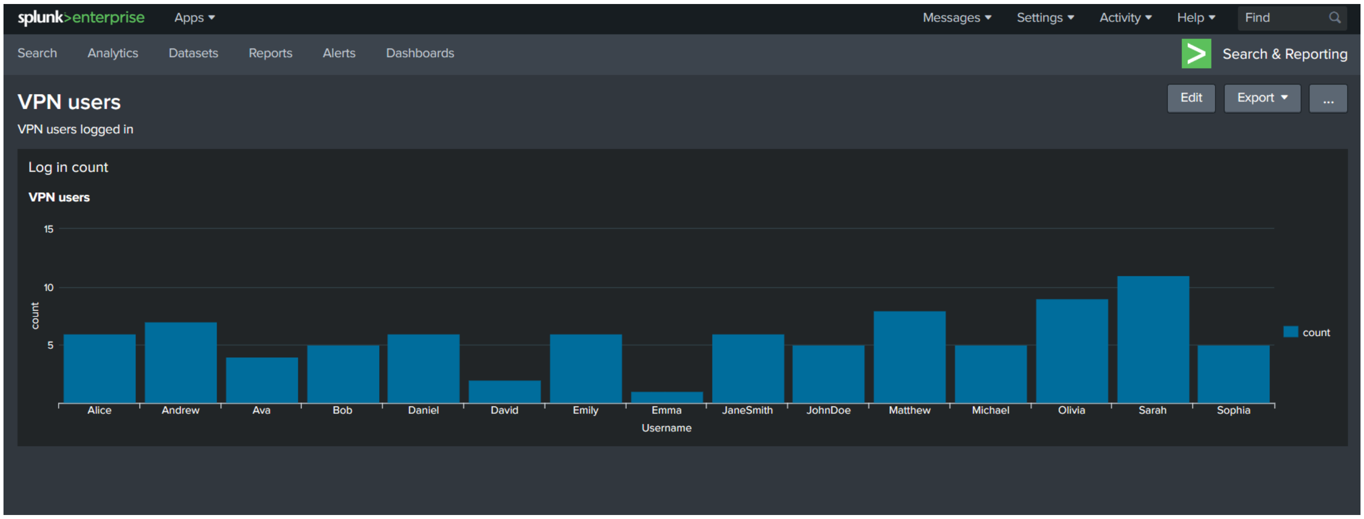
VPN users

VPN users logged in

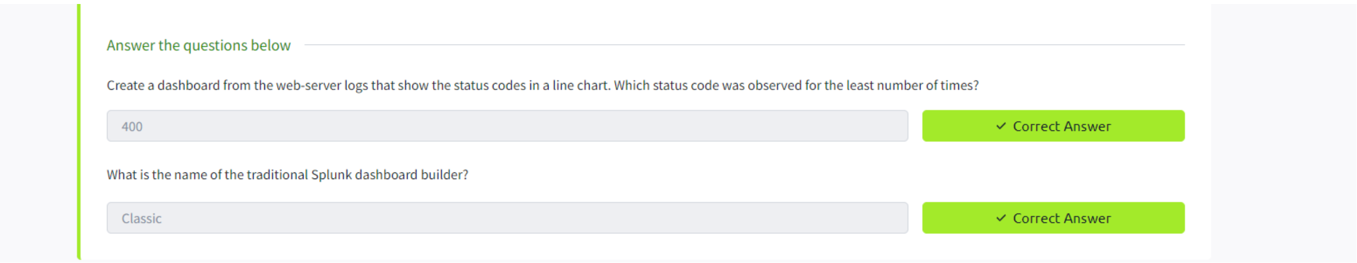
Log in count

VPN users

Doesn't it look nice? We can see on a cursory glance that Emma logged in the least amount of times, and Sarah logged in the most. This is the kind of information that a dashboard is helpful for. Another way dashboards can help is by adding multiple reports to a single dashboard. The process for that will be similar, as we still see the Add Panel option above. However, we will keep this task to a single report. We can flip the switch to the Dark theme and click 'Save' to save the dashboard if we like it. This is how it will look when finished.



Now, we can go to the Dashboards menu to see our newly created dashboard.



Answer the questions below

Create a dashboard from the web-server logs that show the status codes in a line chart. Which status code was observed for the least number of times?

400

✓ Correct Answer

What is the name of the traditional Splunk dashboard builder?

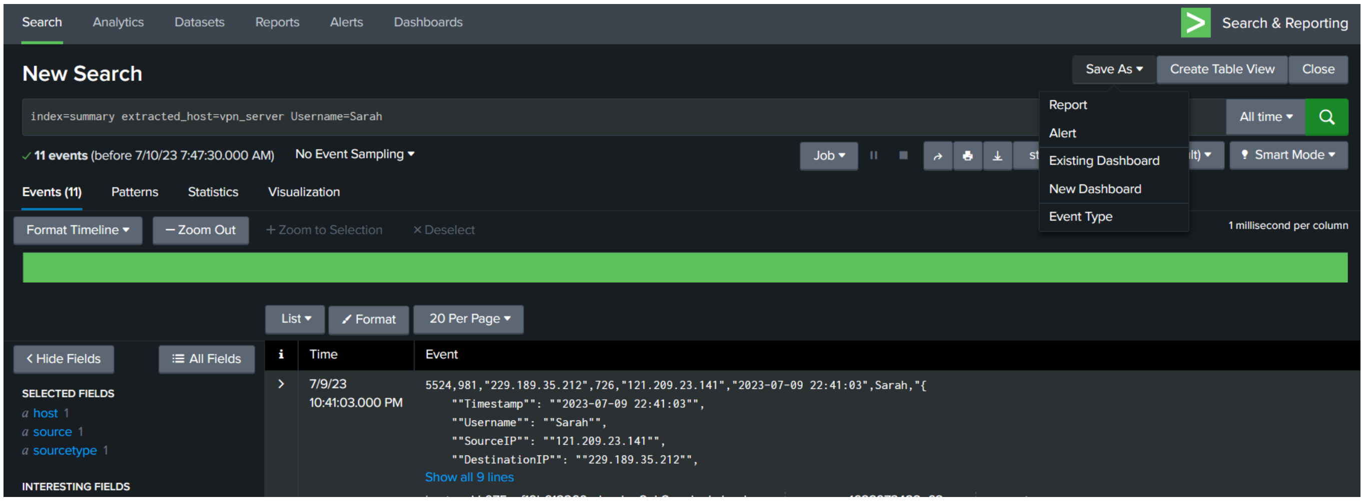
Classic

✓ Correct Answer

Alerting on high priority events

In the previous tasks, we practiced creating reports and dashboards. We understood that when we need to run a search repetitively, we can use reports, and if we want to club a few reports together or make visualizations, we can use dashboards. However, reports and dashboards will only be viewed by users at set time intervals. Sometimes, we want to be alerted if a certain event happens, such as, if the amount of failed logins on a single account reaches a threshold, it indicates a brute force attempt, and we would like to know as soon as it happens. In this task, we will learn how to set up alerts. Unfortunately, we cannot practice setting up alerts on the attached instance because of licensing issues. However, we will explain how to set up an alert in this task.

First, we will run a search for our required search term. In the 'Save As' drop-down, we will see an option for saving as an alert. In the previous task, we identified that the user Sarah logged in the most during our time range. Therefore, let's narrow down our search to all the login events of the user Sarah.



New Search

```
index=summary extracted_host=vpn_server Username=Sarah
```

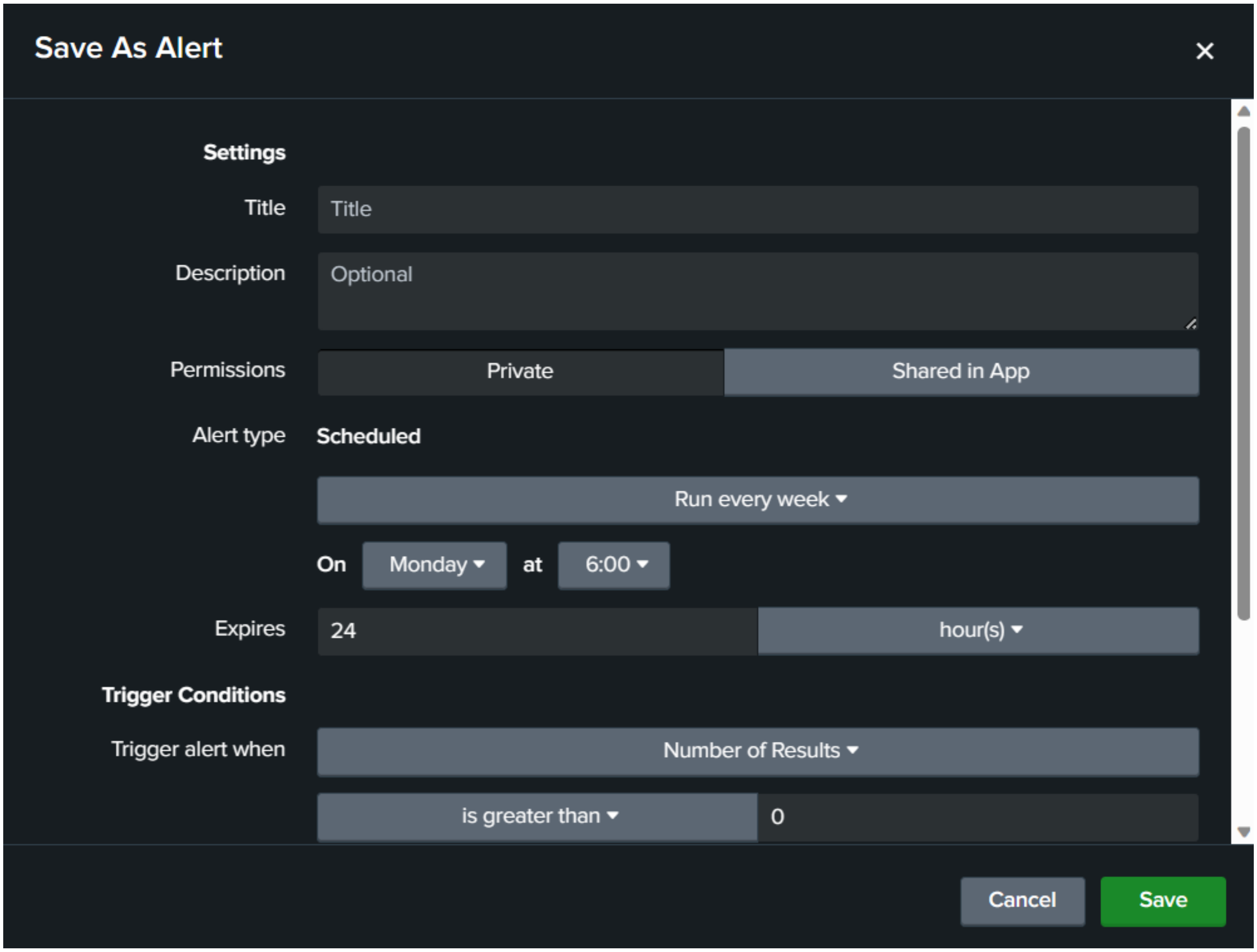
✓ 11 events (before 7/10/23 7:47:30.000 AM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

i	Time	Event
>	7/9/23 10:41:03.000 PM	5524,981,"229.189.35.212",726,"121.209.23.141","2023-07-09 22:41:03",Sarah,"{ ""Timestamp"": ""2023-07-09 22:41:03"", ""Username"": ""Sarah"", ""SourceIP"": ""121.209.23.141"", ""DestinationIP"": ""229.189.35.212"",

When we click 'Alert' in the 'Save As' menu, we are asked to configure the alert's parameters.



Save As Alert

Settings

Title: Title

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled

Run every week ▾

On Monday ▾ at 6:00 ▾

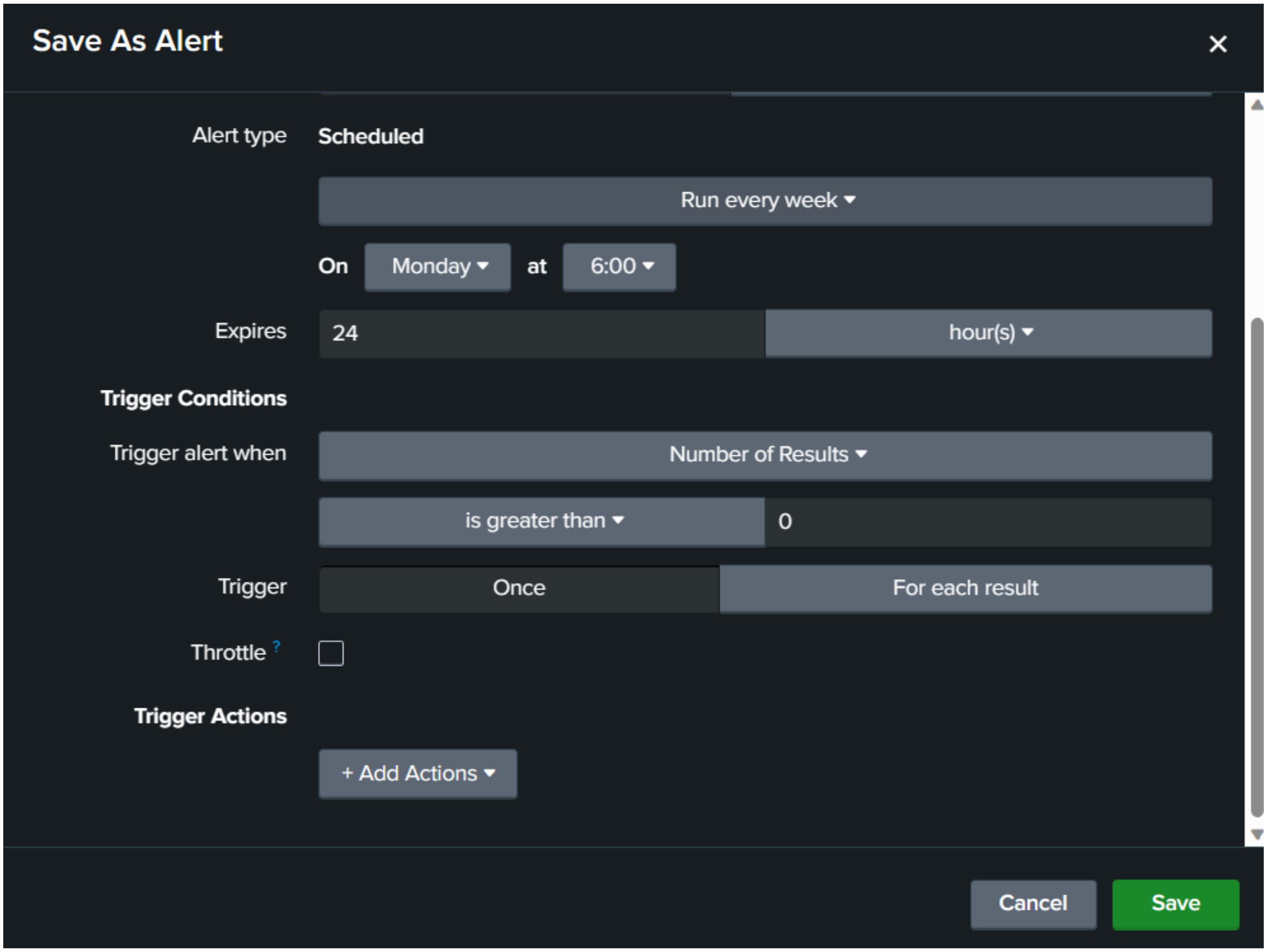
Expires: 24 hour(s) ▾

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ 0

We see the usual settings such as Title, Description and Permissions. In addition to that, we have some more options specific to alerts. The alert type we are setting up is scheduled. This means that Splunk will run this search as per the schedule, and if the trigger condition is satisfied, an alert will be raised. Depending on the license and configuration for your Splunk instance, you might get an option for scheduling Real-time alerts. Next, we have trigger conditions.



Save As Alert

Alert type: Scheduled

Run every week

On Monday at 6:00

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results

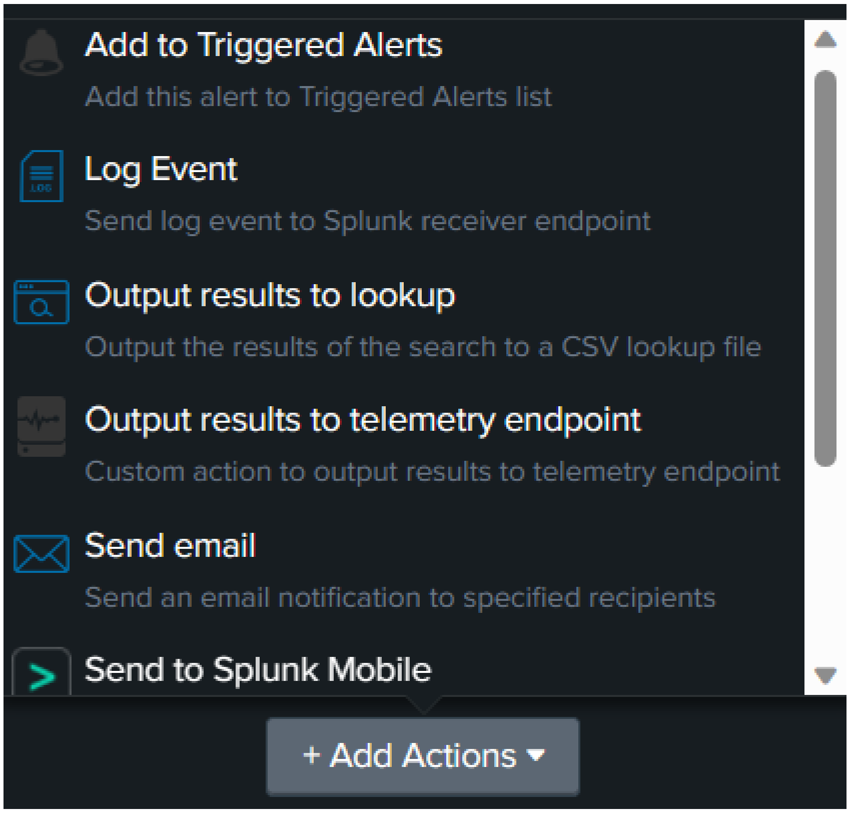
is greater than 0

Trigger: Once | For each result

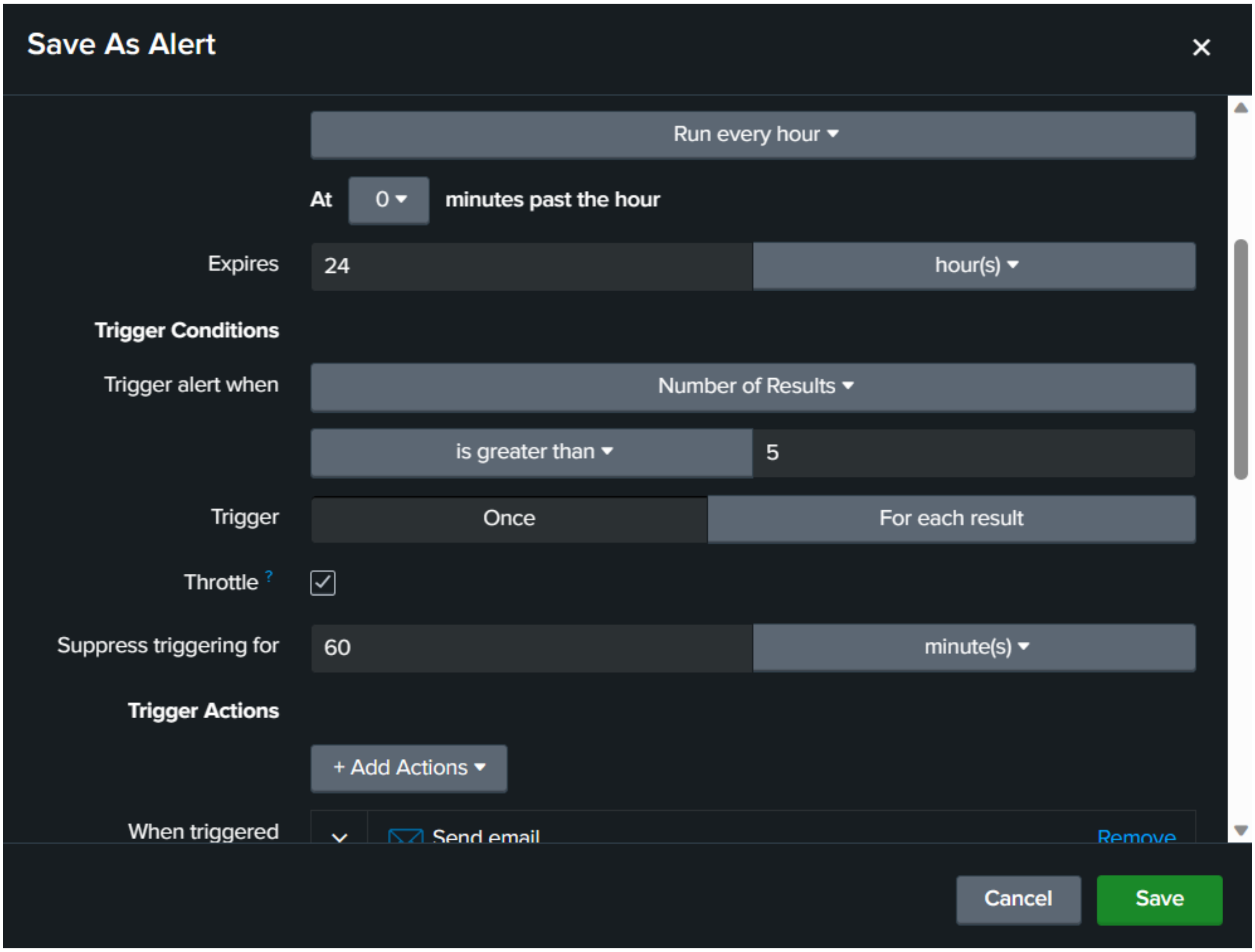
Throttle ☐

Trigger Actions

Trigger conditions define the conditions when the alert will be raised. Here, let's say we raise the alert when the login count of our user is more than 5. In that case, we will use the 'Number of Results' option and set the 'is greater than' option to 5. We can trigger 5 alerts for the 5 login times, or we can just trigger a single alert for exceeding this count. The 'Throttle' option lets us limit the alerts by not raising an alert in the specified time period if an alert is already triggered. This can help reduce alert fatigue, which can overwhelm analysts when there are too many alerts. The final option here is for Trigger Actions. This option allows us to define what automated steps Splunk must take when the alert is triggered. For example, we might want Splunk to send an email to the SOC email account in case of an alert.


Add to Triggered Alerts
Add this alert to Triggered Alerts list
Log Event
Send log event to Splunk receiver endpoint
Output results to lookup
Output the results of the search to a CSV lookup file
Output results to telemetry endpoint
Custom action to output results to telemetry endpoint
Send email
Send an email notification to specified recipients
Send to Splunk Mobile
+ Add Actions

Below, we can see the configured alert. We have configured it to run every hour if Sarah logs in more than 5 times. The email will only be sent once every 60 minutes.



Save As Alert

Run every hour

At 0 minutes past the hour

Expires 24 hour(s)

Trigger Conditions

Trigger alert when Number of Results

is greater than 5

Trigger Once For each result

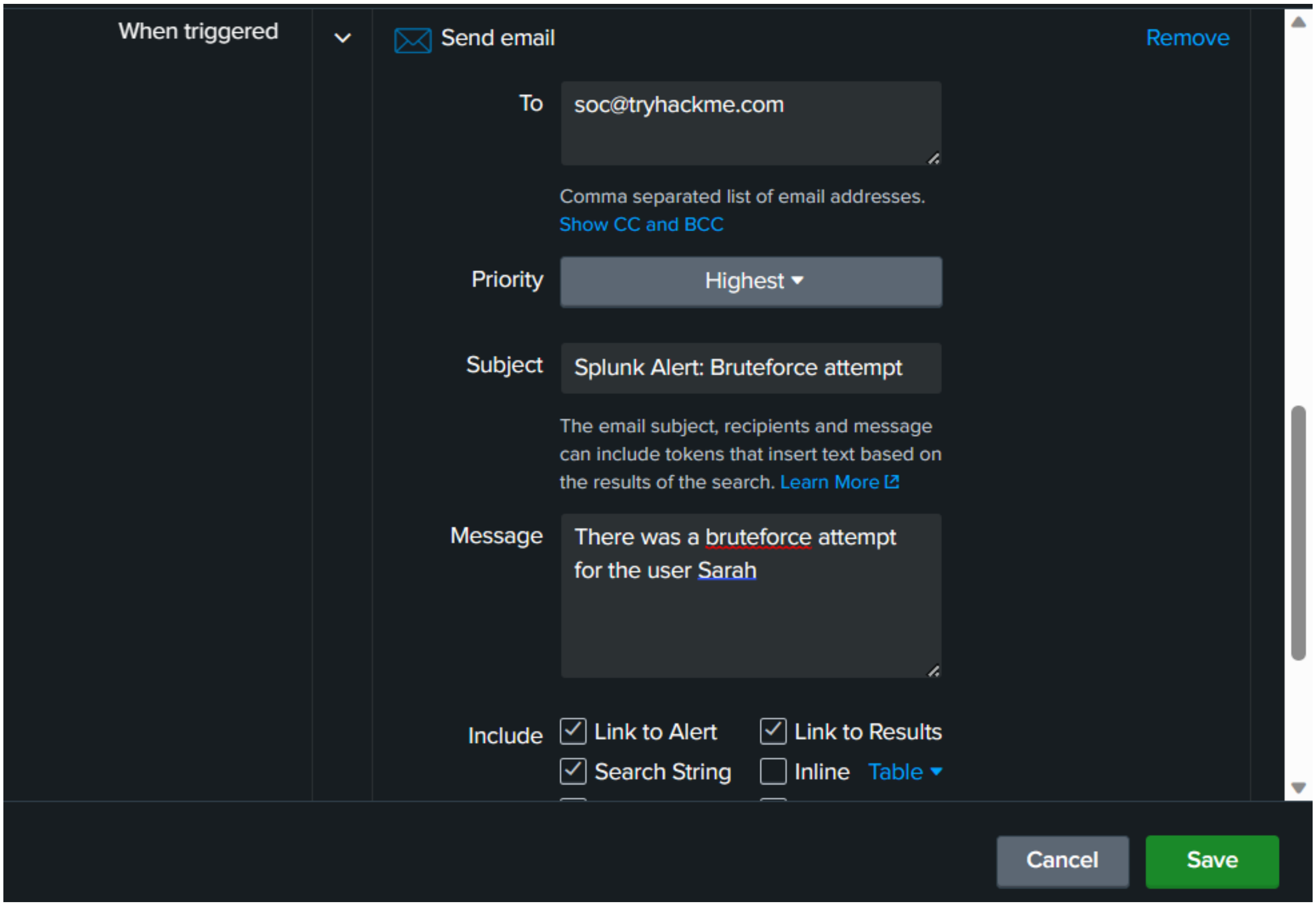
Throttle ? ☑

Suppress triggering for 60 minute(s)

Trigger Actions

When triggered Send email

If the alert is triggered, Splunk will send an email to soc@tryhackme.com.



To: soc@tryhackme.com

Comma separated list of email addresses.

Priority: Highest

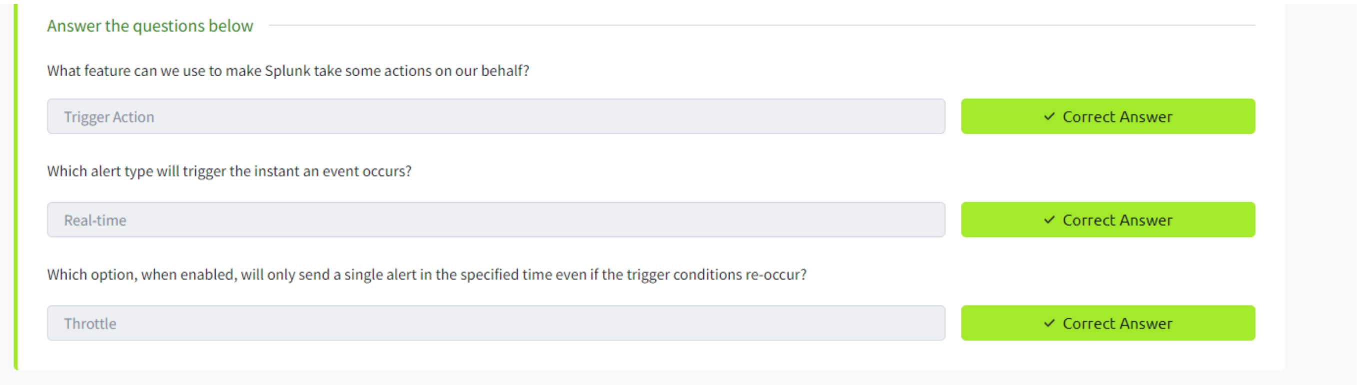
Subject: Splunk Alert: Bruteforce attempt

The email subject, recipients and message can include tokens that insert text based on the results of the search.

Message: There was a bruteforce attempt for the user Sarah

Include: ☑ Link to Alert ☑ Link to Results ☑ Search String □ Inline Table

The email will be sent with the highest priority, and it will include the Subject and message mentioned above.



Answer the questions below

What feature can we use to make Splunk take some actions on our behalf?

Trigger Action

✓ Correct Answer

Which alert type will trigger the instant an event occurs?

Real-time

✓ Correct Answer

Which option, when enabled, will only send a single alert in the specified time even if the trigger conditions re-occur?

Throttle

✓ Correct Answer