Cybersecurity

Module 19 Challenge Submission File

Let's Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: The Need for Speed

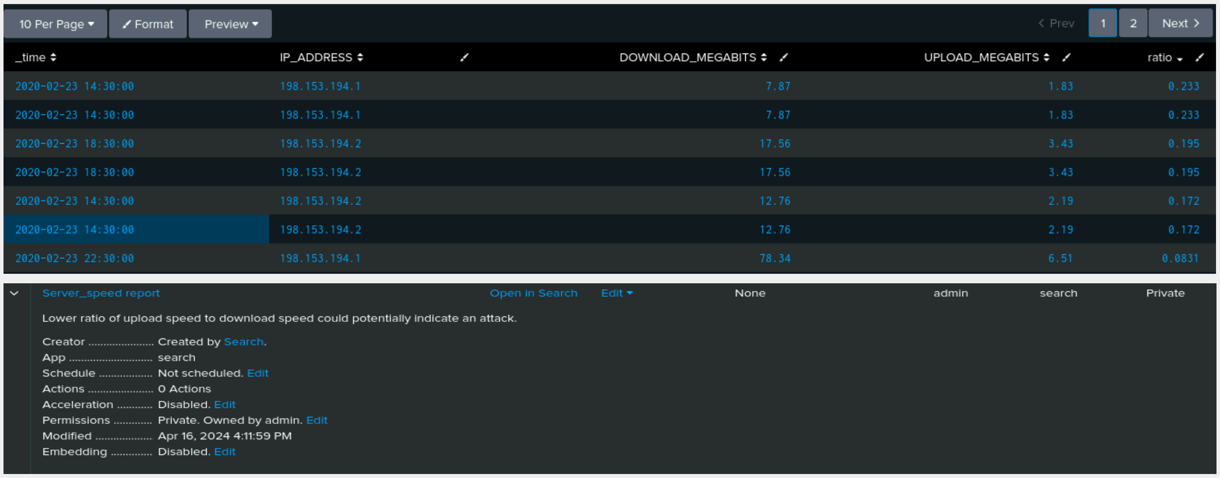
1. Based on the report you created, what is the approximate date and time of the attack?

2020-02-23 14:30:00

2. How long did it take your systems to recover?

So, there are 8 hours between 14:30 PM and 22:30 PM.

Provide a screenshot of your report:



_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831

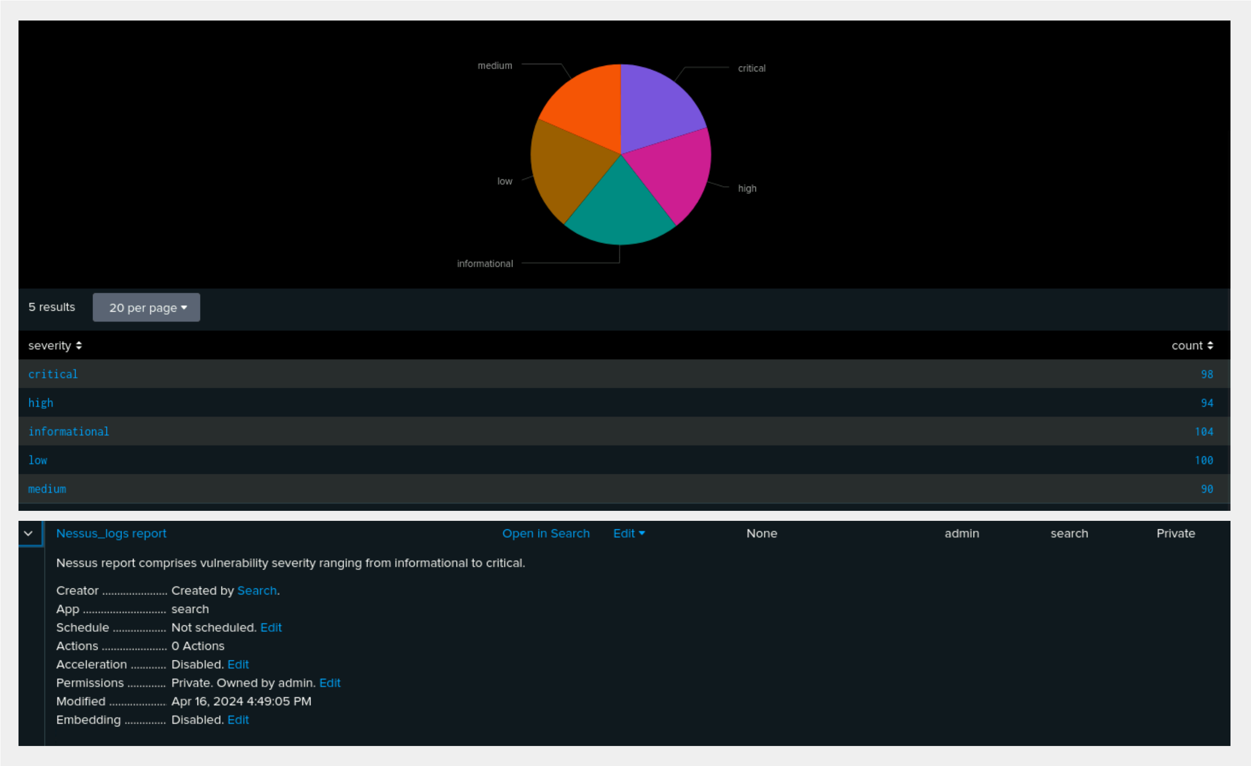
Server_speed report Open in Search Edit ▾ None admin search Private

Lower ratio of upload speed to download speed could potentially indicate an attack.

Creator .... Created by Search.
App .... search
Schedule .... Not scheduled. Edit
Actions .... 0 Actions
Acceleration .... Disabled. Edit
Permissions .... Private. Owned by admin. Edit
Modified .... Apr 16, 2024 4:11:59 PM
Embedding .... Disabled. Edit

Step 2: Are We Vulnerable?

Provide a screenshot of your report:



5 results | 20 per page ▾

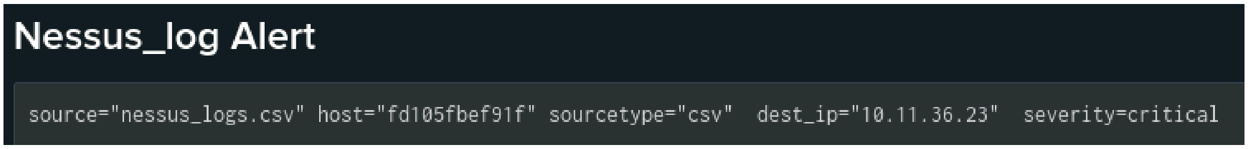
severity ⇕	count ⇕
critical	98
high	94
informational	104
low	100
medium	90

Nessus_logs report | Open in Search | Edit ▾ | None | admin | search | Private

Nessus report comprises vulnerability severity ranging from informational to critical.

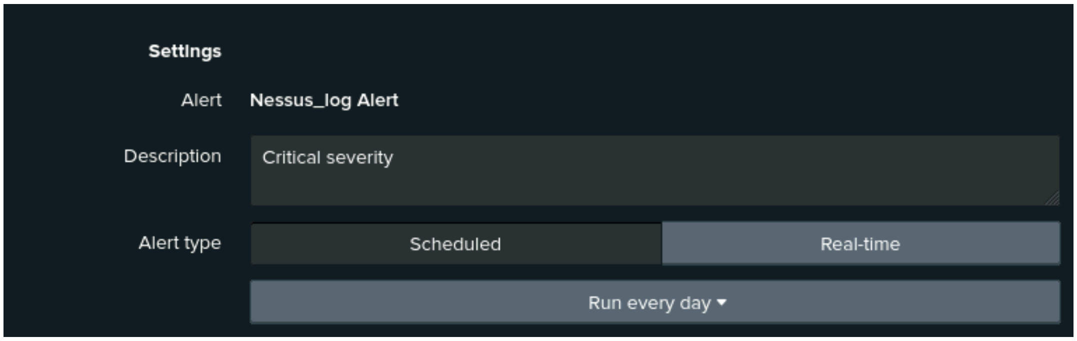
Creator .... Created by Search.
App .... search
Schedule .... Not scheduled. Edit
Actions .... 0 Actions
Acceleration .... Disabled. Edit
Permissions .... Private. Owned by admin. Edit
Modified .... Apr 16, 2024 4:49:05 PM
Embedding .... Disabled. Edit

Provide a screenshot showing that the alert has been created:



Nessus_log Alert

```
source="nessus_logs.csv" host="fd105fbef91f" sourcetype="csv"  dest_ip="10.11.36.23"  severity=critical
```



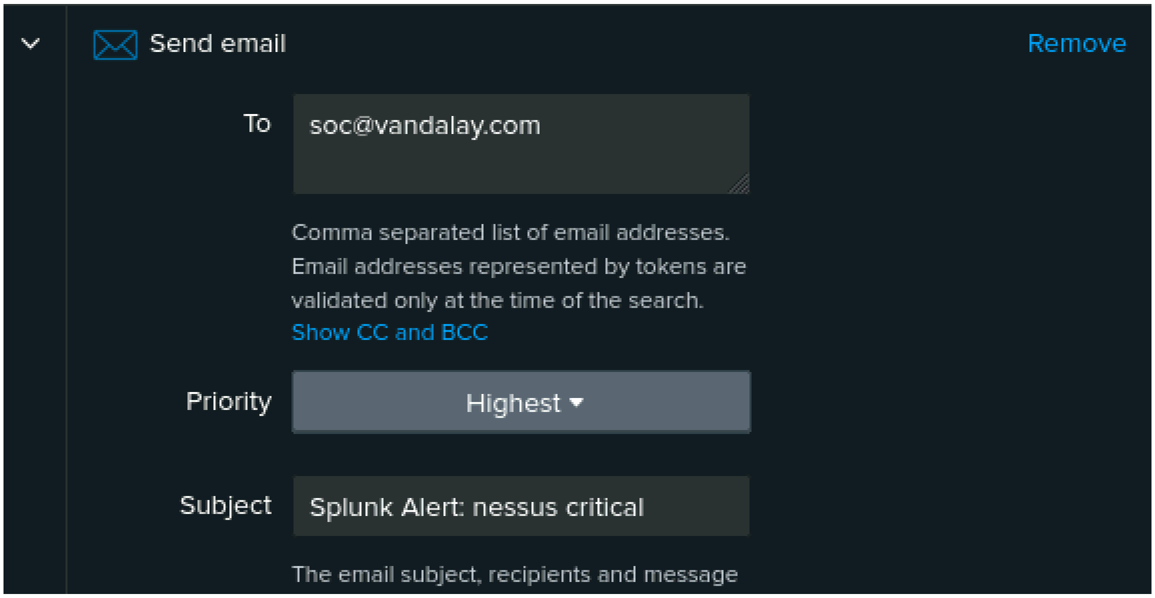
Settings

Alert: Nessus_log Alert

Description: Critical severity

Alert type: Scheduled | Real-time

Run every day ▾



Send email

Remove

To: soc@vandalay.com

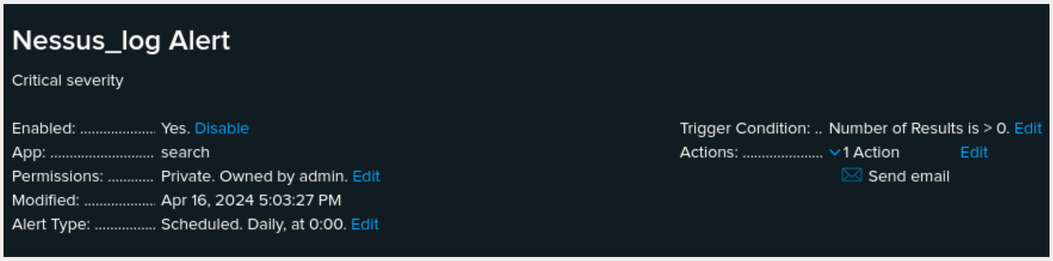
Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.

Show CC and BCC

Priority: Highest ▾

Subject: Splunk Alert: nessus critical

The email subject, recipients and message



Nessus_log Alert

Critical severity

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Apr 16, 2024 5:03:27 PM
Alert Type: .... Scheduled. Daily, at 0:00. Edit

Trigger Condition: .. Number of Results is > 0. Edit
Actions: .... 1 Action Edit
Send email

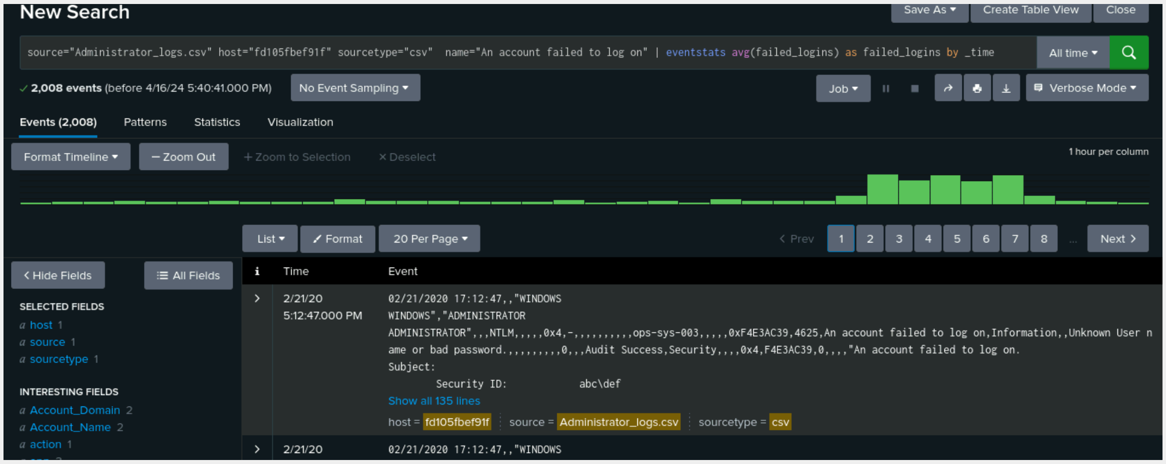
Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

```
The brute force attack occurred on February 21, 2020.
```

2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

```
Establish the threshold at 20. This setup will notify you if the count of
failed login attempts surpasses the typical peak, potentially signaling a
brute force attack.
A baseline of normal activity is between 10 and 15.
```



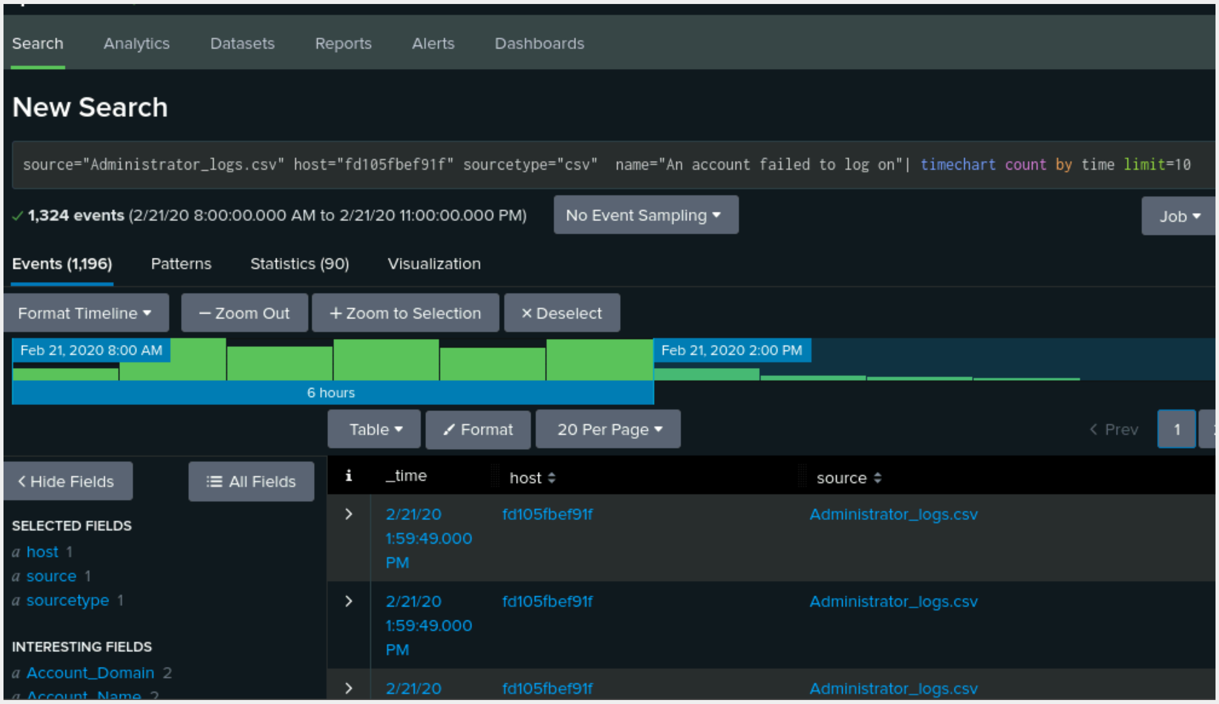
```
source="Administrator_logs.csv" host="fd105fbef91f" sourcetype="csv"  name="An account failed to log on" | eventstats avg(failed_logins) as failed_logins by _time
```

✓ **2,008 events** (before 4/16/24 5:40:41.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2
a Account_Name 2
a action 1

i	Time	Event
>	2/21/20 5:12:47.000 PM	02/21/2020 17:12:47,,"WINDOWS WINDOWS","ADMINISTRATOR ADMINISTRATOR",,,NTLM,,,,,0x4,-,,,,,,,,,,ops-sys-003,,,,,0xF4E3AC39,4625,An account failed to log on,Information,,Unknown User name or bad password.,,,,,,,,,0,,,Audit Success,Security,,,,0x4,F4E3AC39,0,,,,"An account failed to log on. Subject: Security ID: abc\def Show all 135 lines host = fd105fbef91f source = Administrator_logs.csv sourcetype = csv
>	2/21/20	02/21/2020 17:12:47,,"WINDOWS



```
source="Administrator_logs.csv" host="fd105fbef91f" sourcetype="csv"  name="An account failed to log on"| timechart count by time limit=10
```

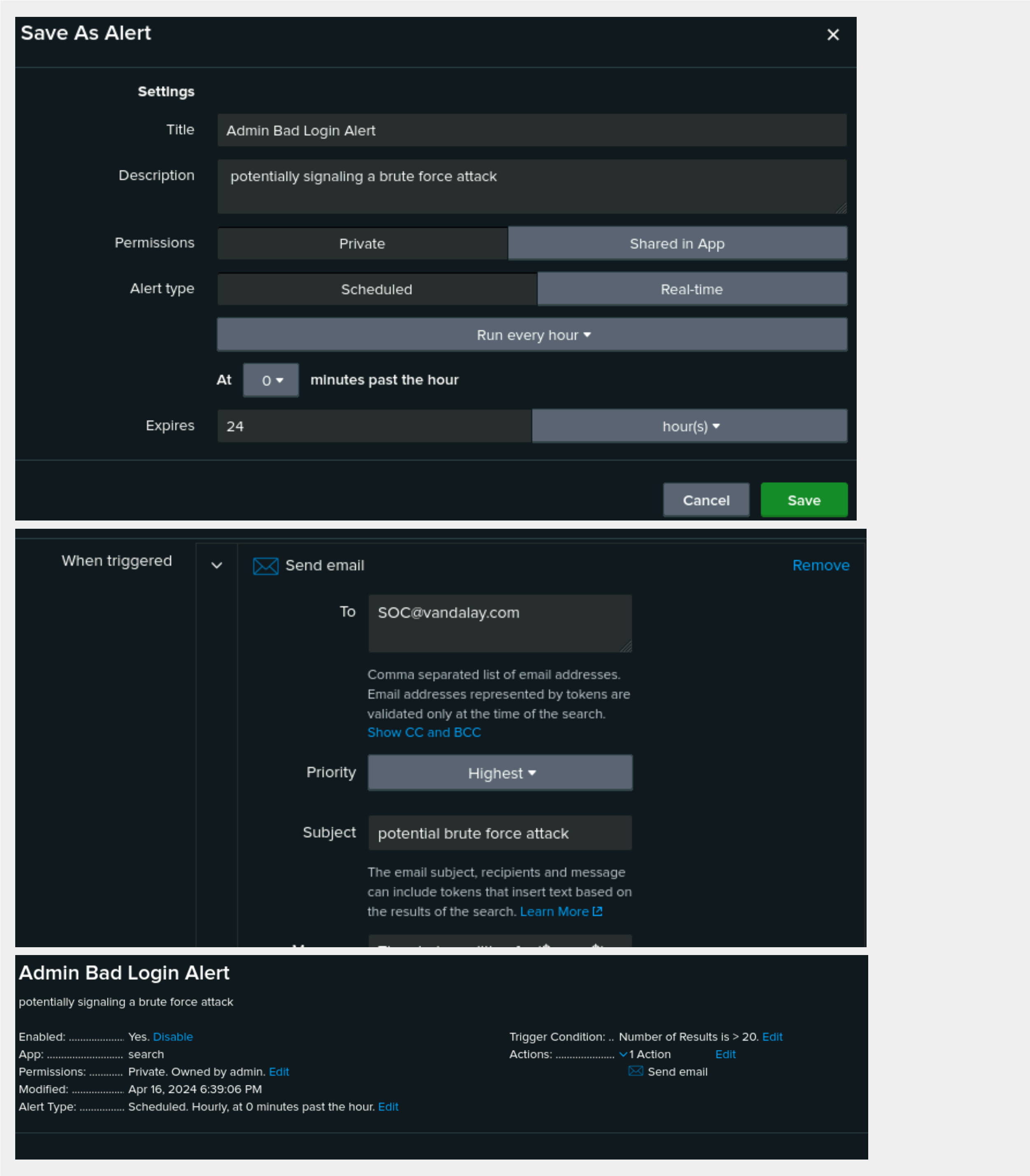
✓ **1,324 events** (2/21/20 8:00:00.000 AM to 2/21/20 11:00:00.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2
a Account_Name 2

i	_time	host	source
>	2/21/20 1:59:49.000 PM	fd105fbef91f	Administrator_logs.csv
>	2/21/20 1:59:49.000 PM	fd105fbef91f	Administrator_logs.csv
>	2/21/20	fd105fbef91f	Administrator_logs.csv

3. Provide a screenshot showing that the alert has been created:



Save As Alert

Settings

Title: Admin Bad Login Alert

Description: potentially signaling a brute force attack

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

At 0 minutes past the hour

Expires: 24 hour(s)

When triggered

Send email

To: SOC@vandalay.com

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search. Show CC and BCC

Priority: Highest

Subject: potential brute force attack

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

Admin Bad Login Alert

potentially signaling a brute force attack

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Apr 16, 2024 6:39:06 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 20. Edit
Actions: .... 1 Action Edit
Send email