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

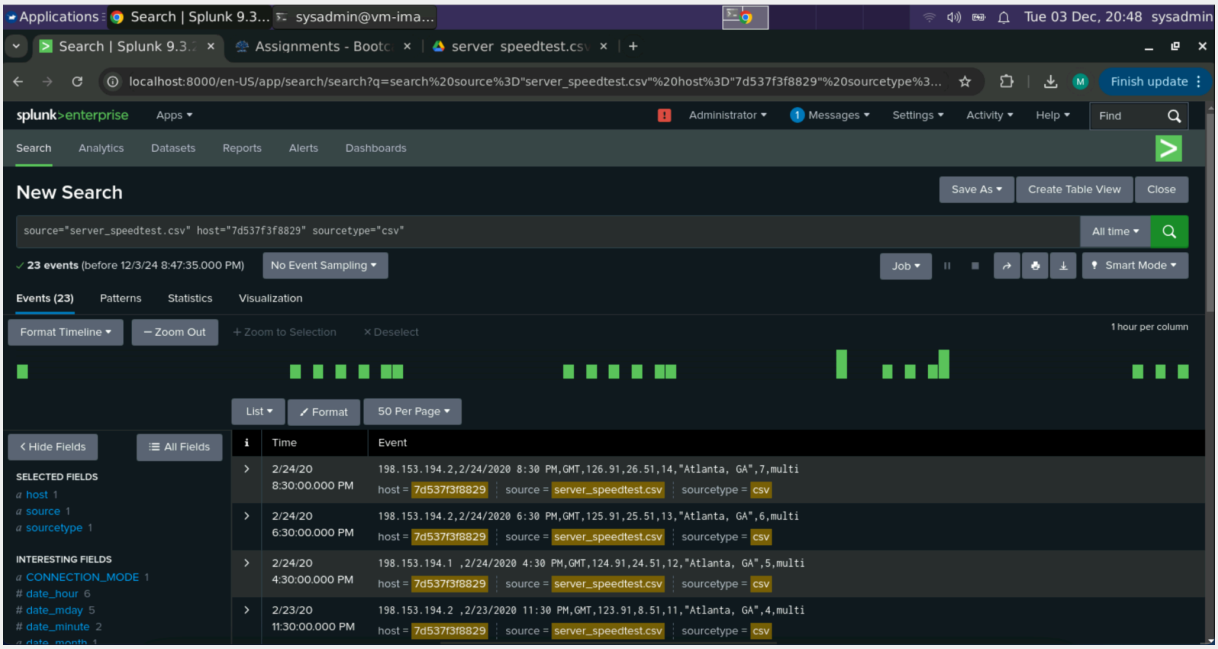
1. Based on the report you created, what is the approximate date and time of the attack?

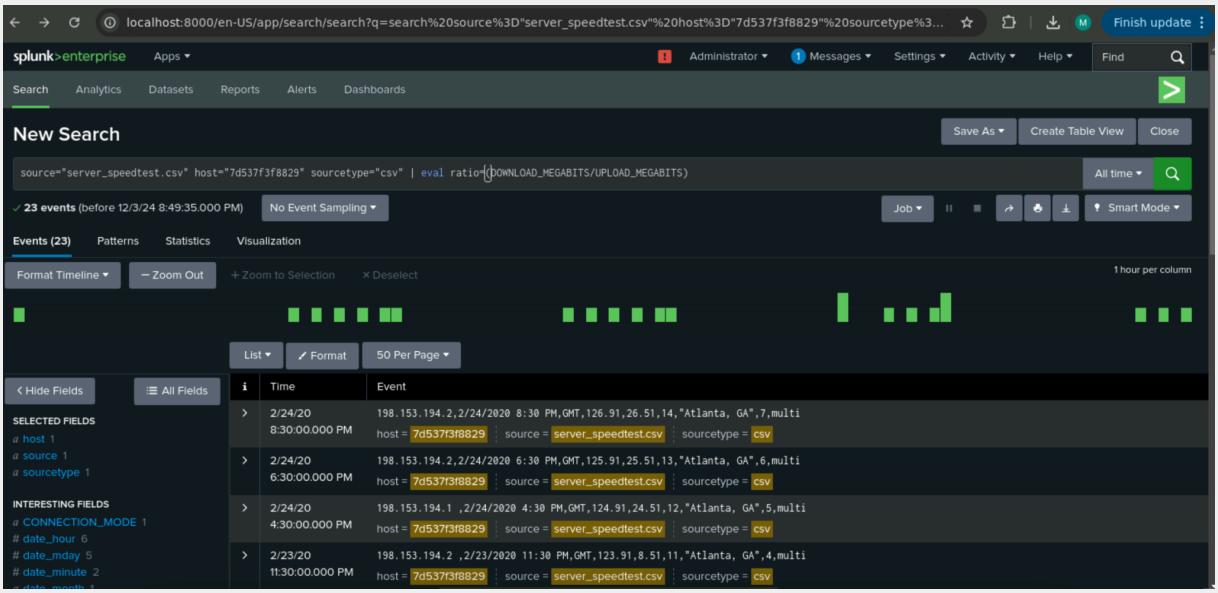
```
We can see download and upload speed was drastically dropped at
approximately 2:30PM on the 23rd of February (dropped to 7.87 at 2:30PM).
This is most likely when the attack started. We can see the downloaded
megabits jumped to 123.91 around 11:30PM on the 23rd of Feb, which is when
the system got back to normal.However, the attack likely ended at 8:30 on
Feb 23rd.
```

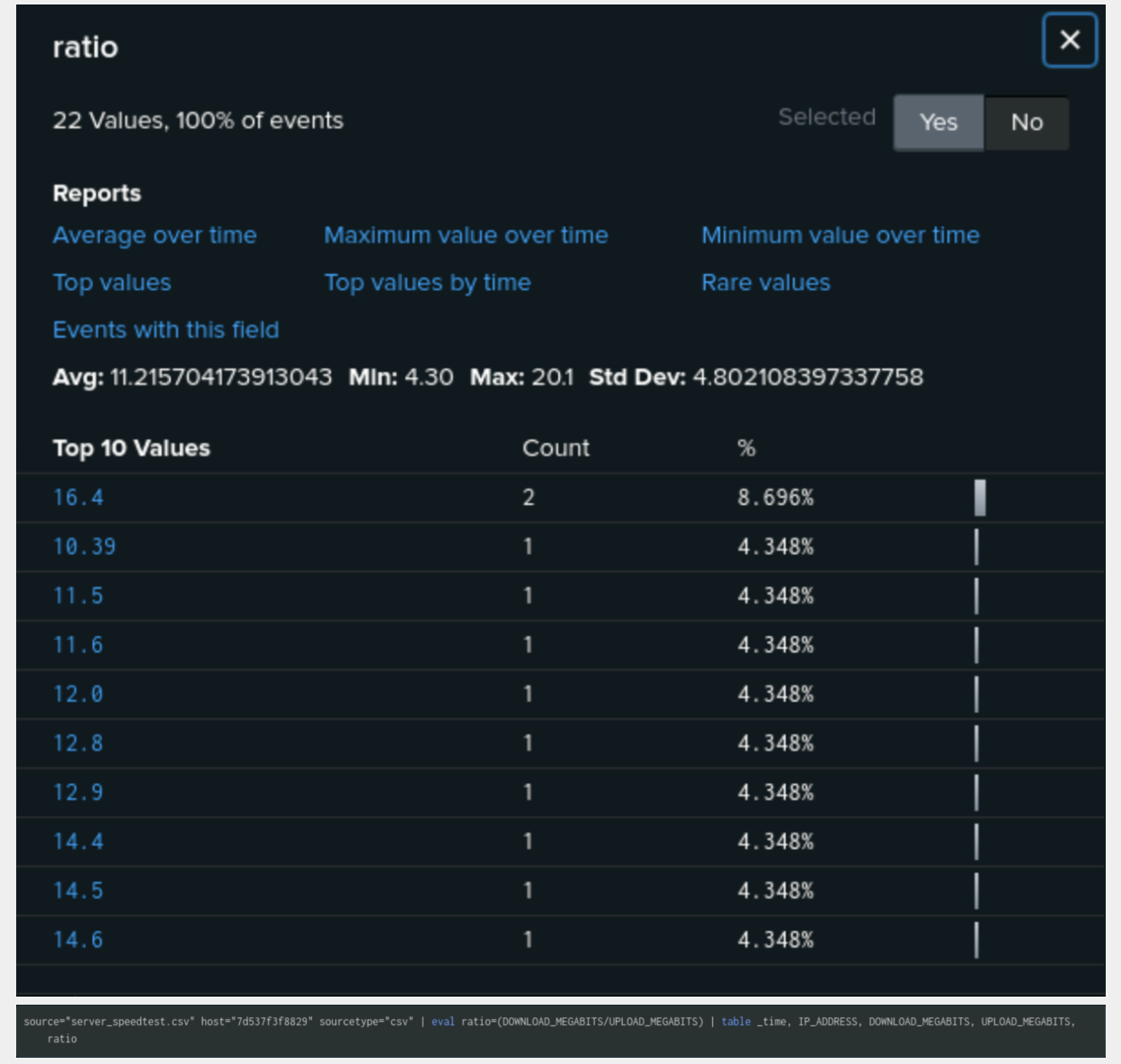
2. How long did it take your systems to recover?

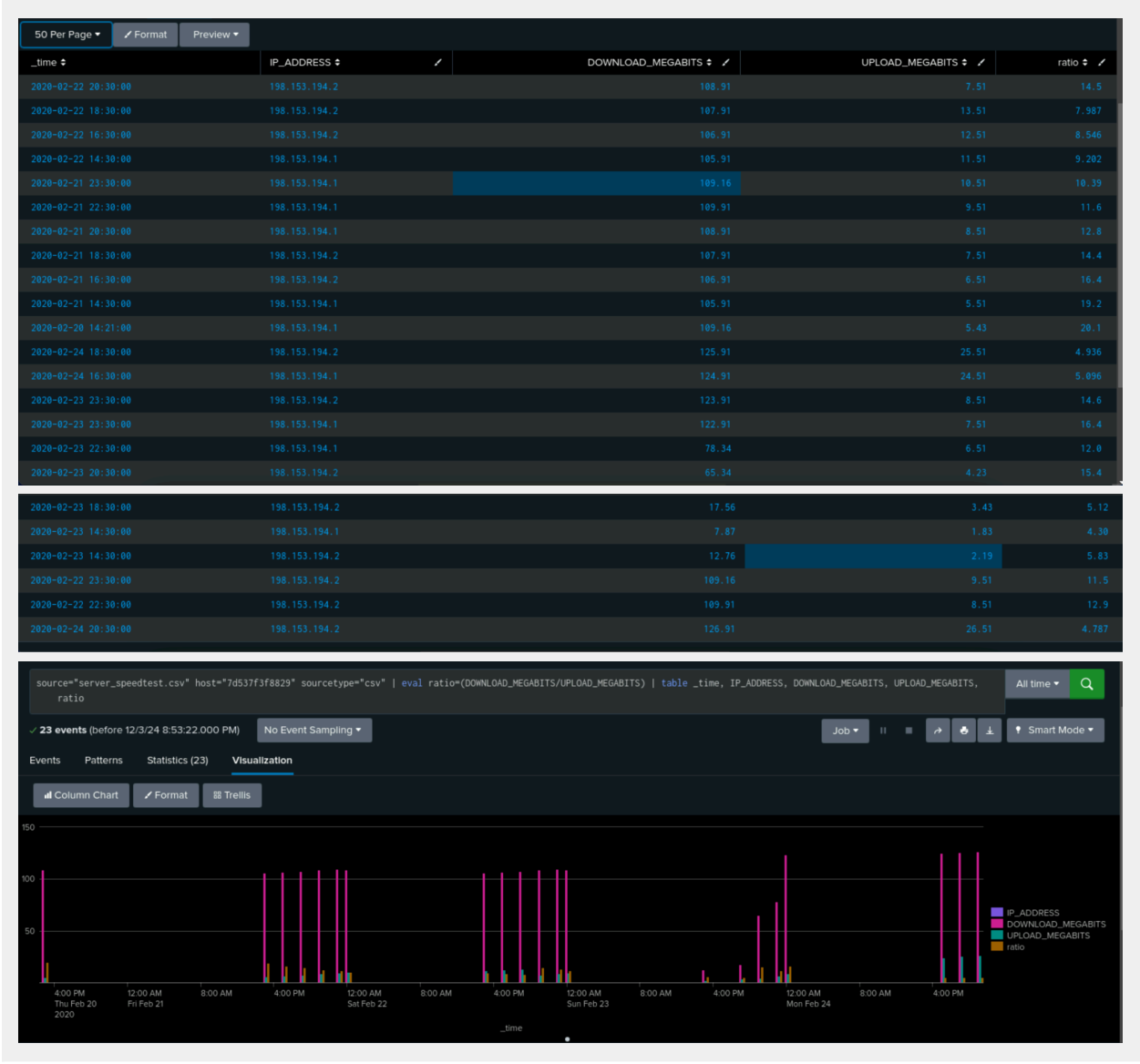
```
6 hours
```

Provide a screenshot of your report:


Applications
Search | Splunk 9.3...
sysadmin@vm-ima...
Tue 03 Dec, 20:48 sysadmin
Search | Splunk 9.3...
Assignments - Bootc
server speedtest.csv
localhost:8000/en-US/app/search/search?q=search%20source%3D"server_speedtest.csv"%20host%3D"7d537f3f8829"%20sourcetype%3...
Finish update
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
Create Table View
Close
source="server_speedtest.csv" host="7d537f3f8829" sourcetype="csv"
All time
23 events (before 12/3/24 8:47:35.000 PM)
No Event Sampling
Job
Smart Mode
Events (23)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
CONNECTION_MODE 1
date_hour 6
date_mday 5
date_minute 2
Time
Event
2/24/20 8:30:00.000 PM
198.153.194.2,2/24/2020 8:30 PM,GMT,126.91,26.51,14,"Atlanta, GA",7,multi
host = 7d537f3f8829 source = server_speedtest.csv sourcetype = csv
2/24/20 6:30:00.000 PM
198.153.194.2,2/24/2020 6:30 PM,GMT,125.91,25.51,13,"Atlanta, GA",6,multi
host = 7d537f3f8829 source = server_speedtest.csv sourcetype = csv
2/24/20 4:30:00.000 PM
198.153.194.1 ,2/24/2020 4:30 PM,GMT,124.91,24.51,12,"Atlanta, GA",5,multi
host = 7d537f3f8829 source = server_speedtest.csv sourcetype = csv
2/23/20 11:30:00.000 PM
198.153.194.2 ,2/23/2020 11:30 PM,GMT,123.91,8.51,11,"Atlanta, GA",4,multi
host = 7d537f3f8829 source = server_speedtest.csv sourcetype = csv

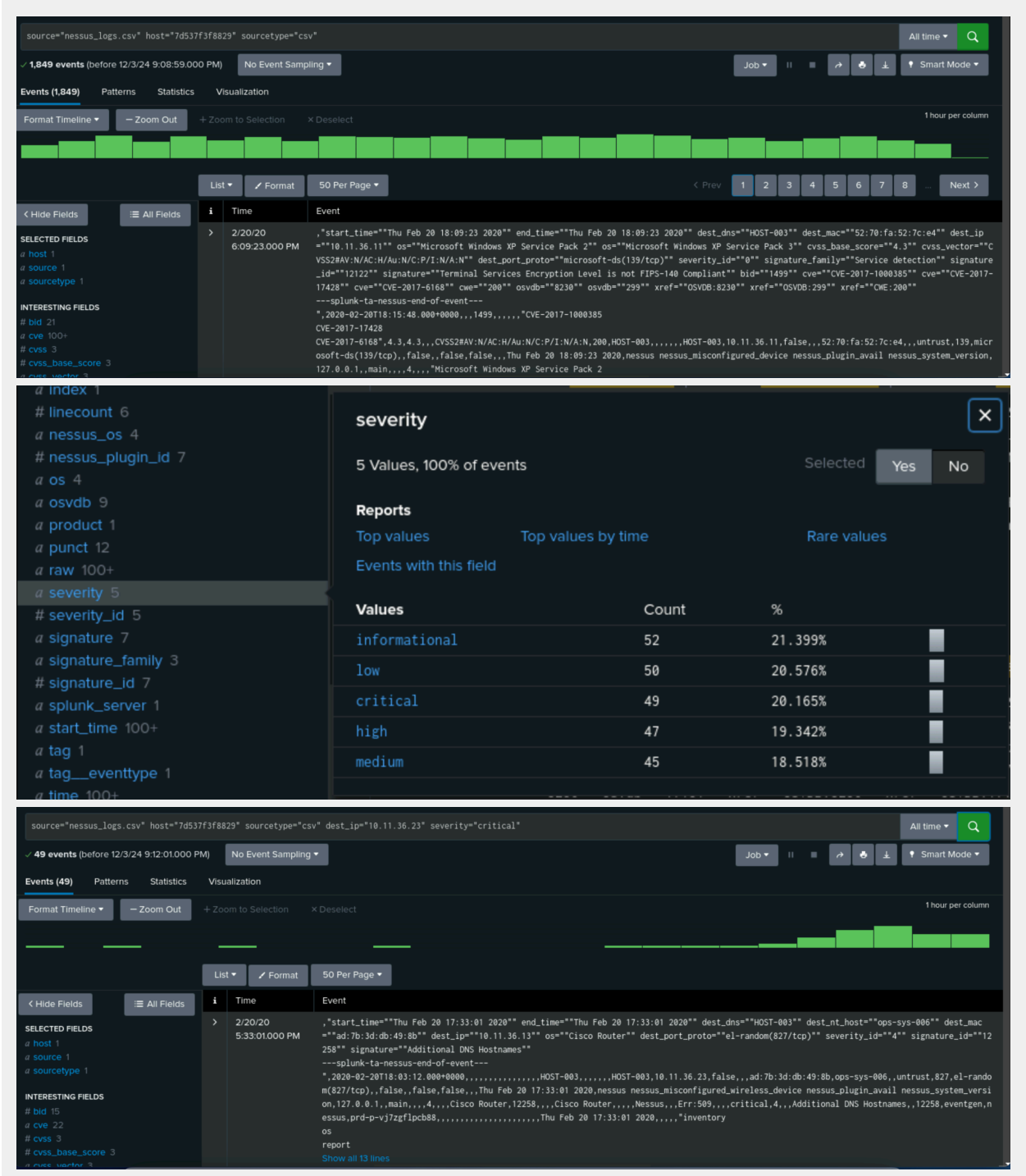

localhost:8000/en-US/app/search/search?q=search%20source%3D"server_speedtest.csv"%20host%3D"7d537f3f8829"%20sourcetype%3...
Finish update
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
Create Table View
Close
source="server_speedtest.csv" host="7d537f3f8829" sourcetype="csv" | eval ratio=(DOWNLOAD_MEGABITS/UPLOAD_MEGABITS)
All time
23 events (before 12/3/24 8:49:35.000 PM)
No Event Sampling
Job
Smart Mode
Events (23)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
CONNECTION_MODE 1
date_hour 6
date_mday 5
date_minute 2
Time
Event
2/24/20 8:30:00.000 PM
198.153.194.2,2/24/2020 8:30 PM,GMT,126.91,26.51,14,"Atlanta, GA",7,multi
host = 7d537f3f8829 source = server_speedtest.csv sourcetype = csv
2/24/20 6:30:00.000 PM
198.153.194.2,2/24/2020 6:30 PM,GMT,125.91,25.51,13,"Atlanta, GA",6,multi
host = 7d537f3f8829 source = server_speedtest.csv sourcetype = csv
2/24/20 4:30:00.000 PM
198.153.194.1 ,2/24/2020 4:30 PM,GMT,124.91,24.51,12,"Atlanta, GA",5,multi
host = 7d537f3f8829 source = server_speedtest.csv sourcetype = csv
2/23/20 11:30:00.000 PM
198.153.194.2 ,2/23/2020 11:30 PM,GMT,123.91,8.51,11,"Atlanta, GA",4,multi
host = 7d537f3f8829 source = server_speedtest.csv sourcetype = csv


ratio
22 Values, 100% of events
Selected
Yes
No
Reports
Average over time
Maximum value over time
Minimum value over time
Top values
Top values by time
Rare values
Events with this field
Avg: 11.215704173913043 Min: 4.30 Max: 20.1 Std Dev: 4.802108397337758
Top 10 Values
Count
%
16.4 2 8.696%
10.39 1 4.348%
11.5 1 4.348%
11.6 1 4.348%
12.0 1 4.348%
12.8 1 4.348%
12.9 1 4.348%
14.4 1 4.348%
14.5 1 4.348%
14.6 1 4.348%
source="server_speedtest.csv" host="7d537f3f8829" sourcetype="csv" | eval ratio=(DOWNLOAD_MEGABITS/UPLOAD_MEGABITS) | table _time, IP_ADDRESS, DOWNLOAD_MEGABITS, UPLOAD_MEGABITS, ratio

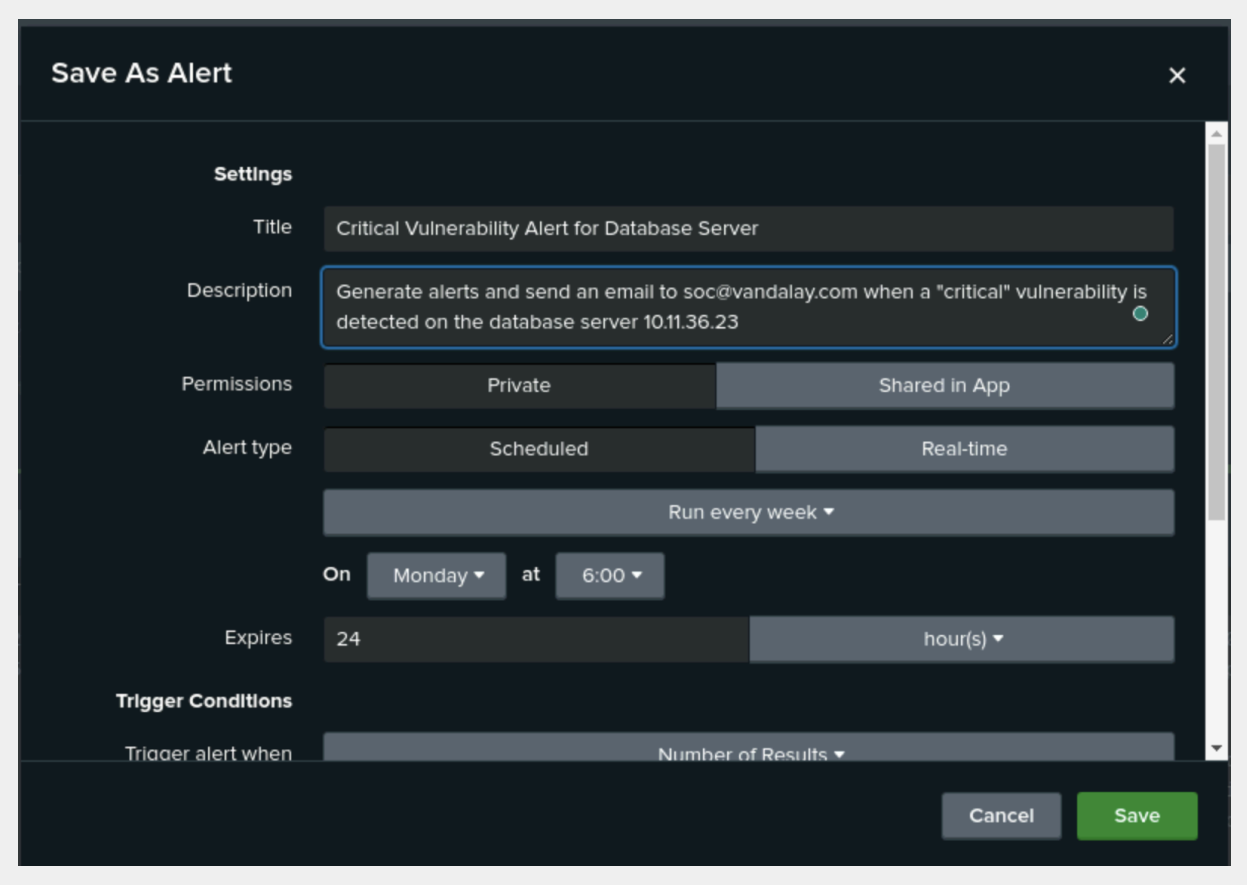


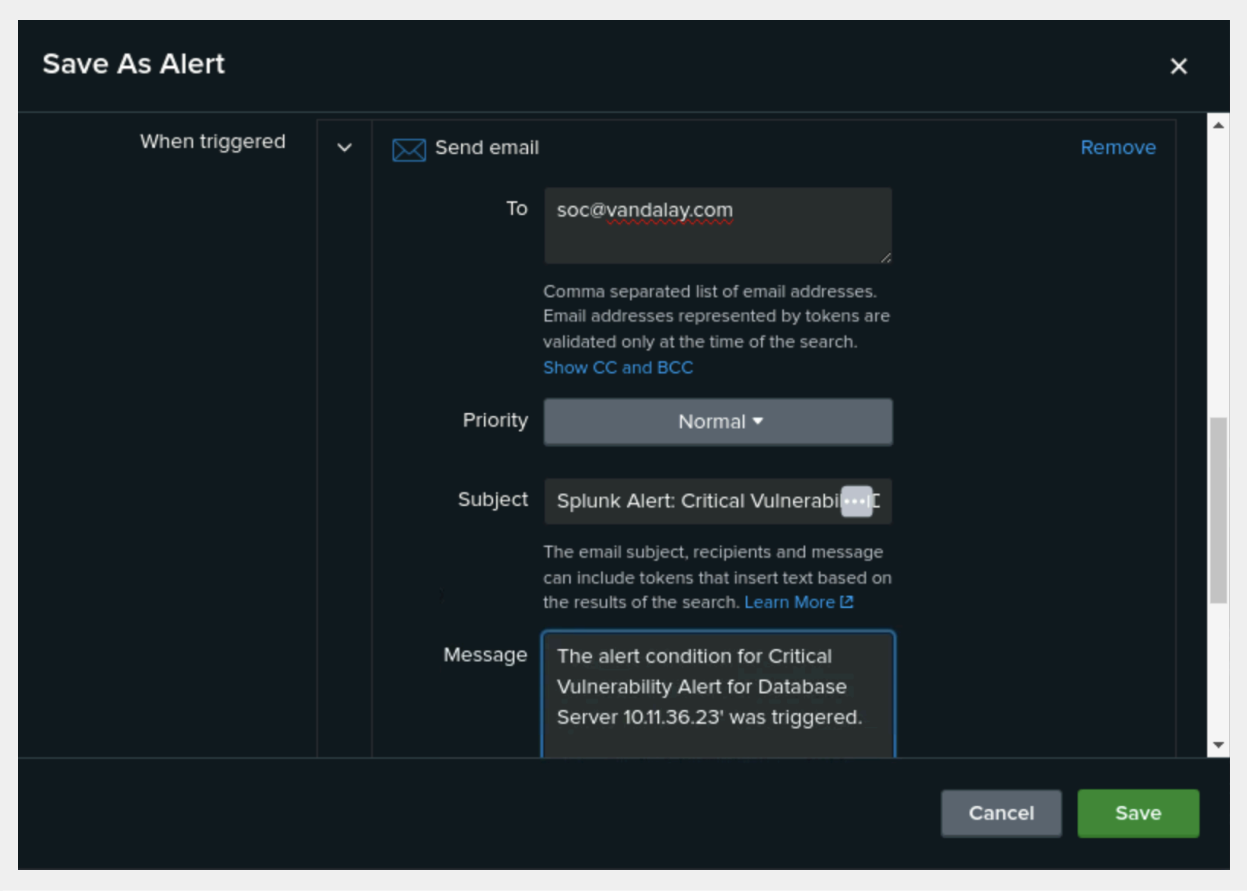
Step 2: Are We Vulnerable?

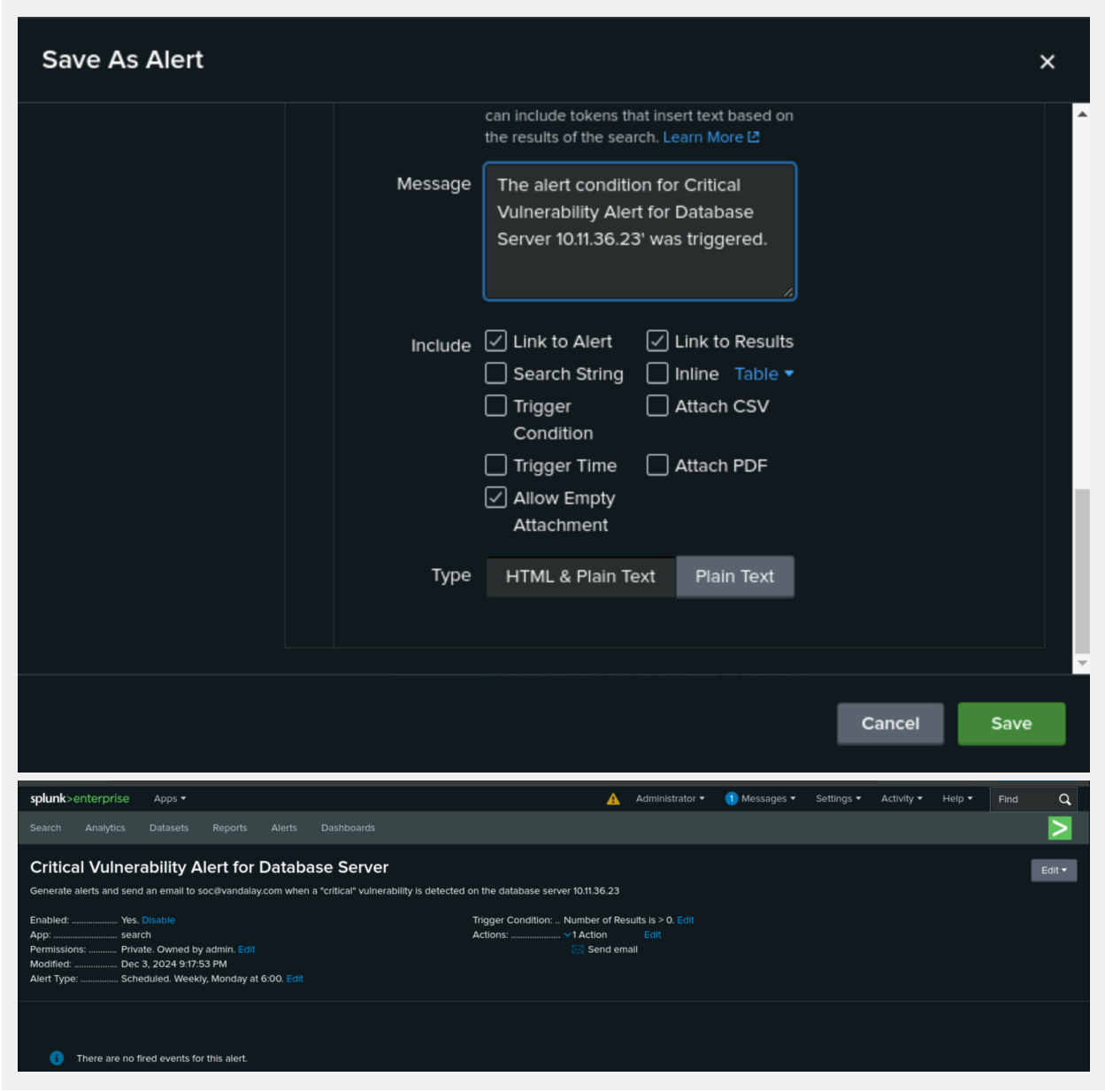
Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:


Save As Alert
Settings
Title
Critical Vulnerability Alert for Database Server
Description
Generate alerts and send an email to soc@vandalay.com when a "critical" vulnerability is detected on the database server 10.11.36.23
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every week
On
Monday
at
6:00
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
Cancel
Save


Save As Alert
When triggered
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
Normal
Subject
Splunk Alert: Critical Vulnerabi
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More
Message
The alert condition for Critical Vulnerability Alert for Database Server 10.11.36.23' was triggered.
Cancel
Save



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

```
Indicators of a brute force attacks will include multiple accounts failed to log on. We can add this value from the field 'name' where we can see the values in the logs. There is a count of 1004 for "An account failed to log on", which is a good indicator that a brute force attack has occurred. From the screenshot we can see a large spike in the events whereby "An account
```

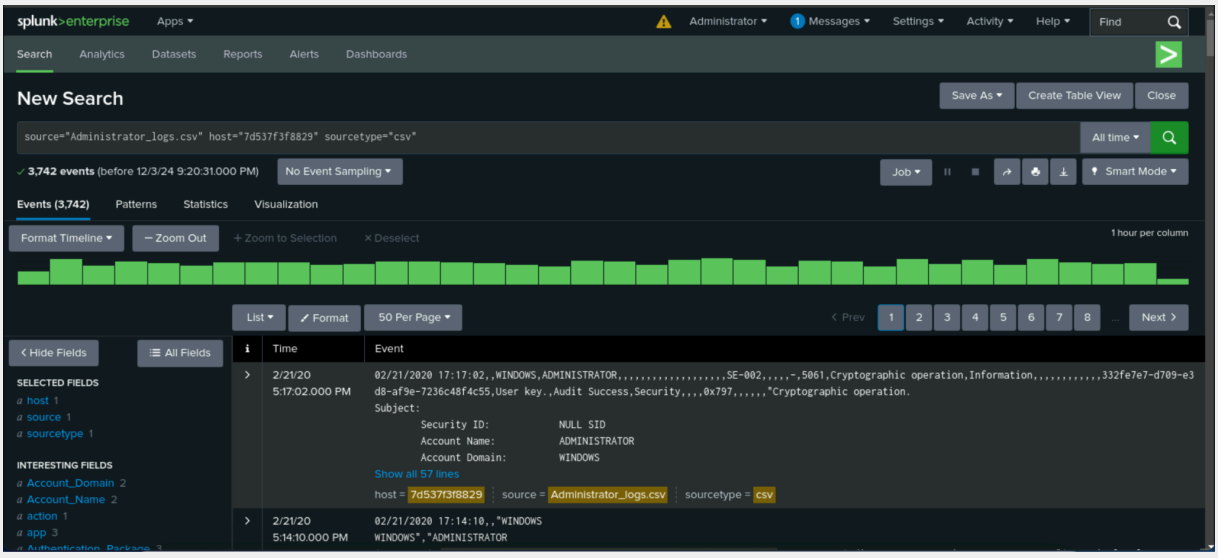
failed to log on" at around 9am on the 21st of February. Of the total 1004 events that occurred, at 9am there was 124 instances with similar numbers appearing in the hours after. This would lead me to believe the attack started around this time - 9:00AM on the 21st of February 2020.

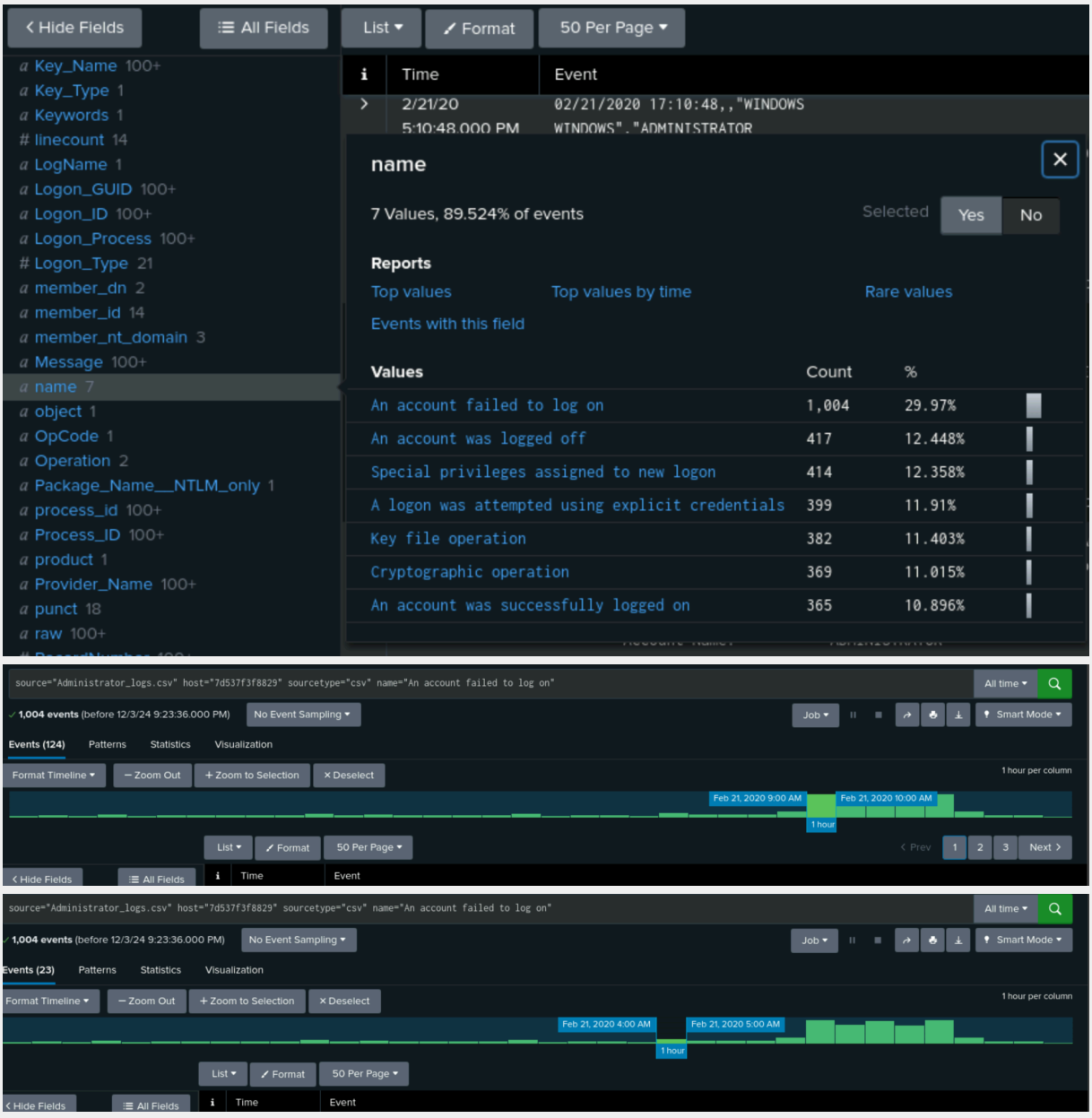
2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

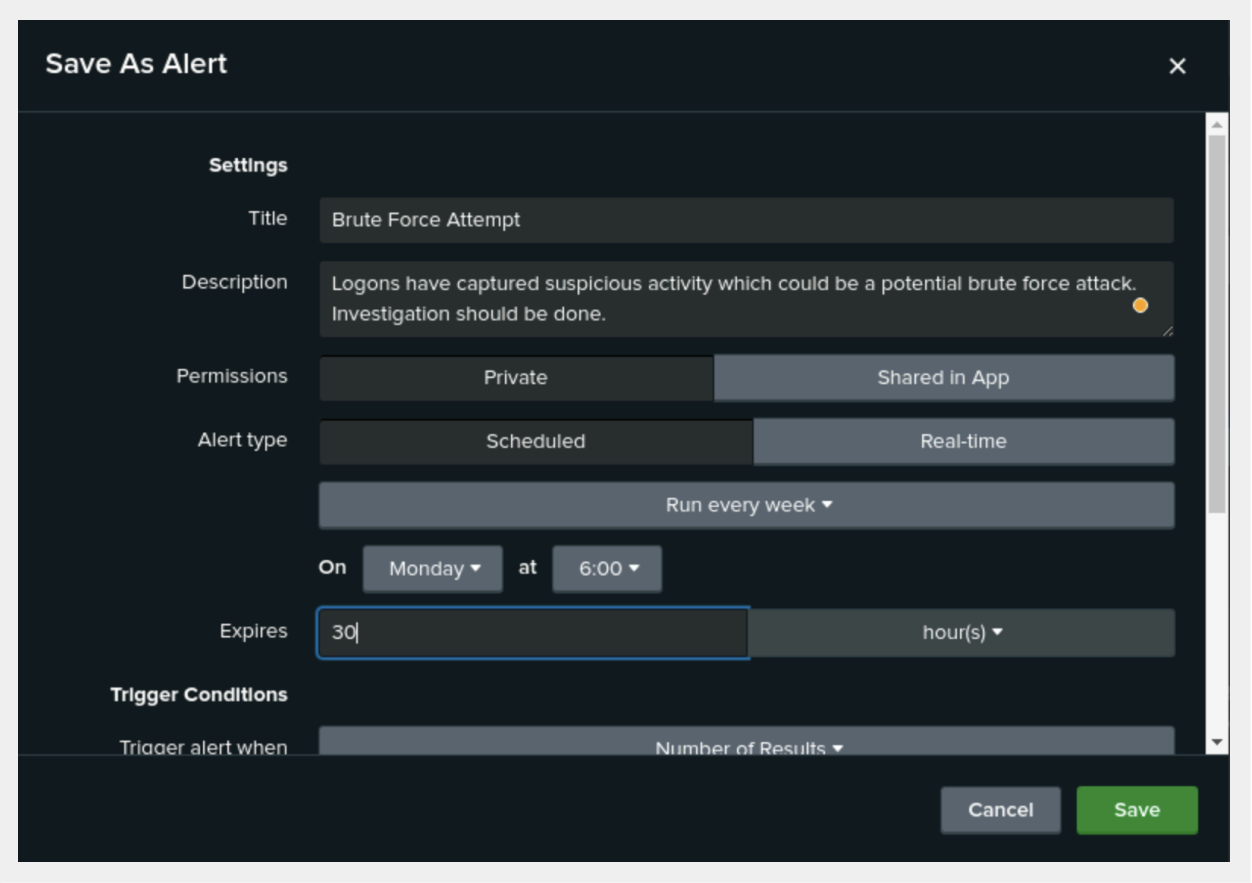
We can see from the events timeline that 124 is an unsual spike. In the proceeding hours to this event, the most amount of bad logins were around 23, this can be considered normal behaviour. With the bad logon attempts being around 124-135 when the brute force attack occurred, I would consider a baseline of about 40 bad log ons per hour. The ranges I would make for bad logons are:

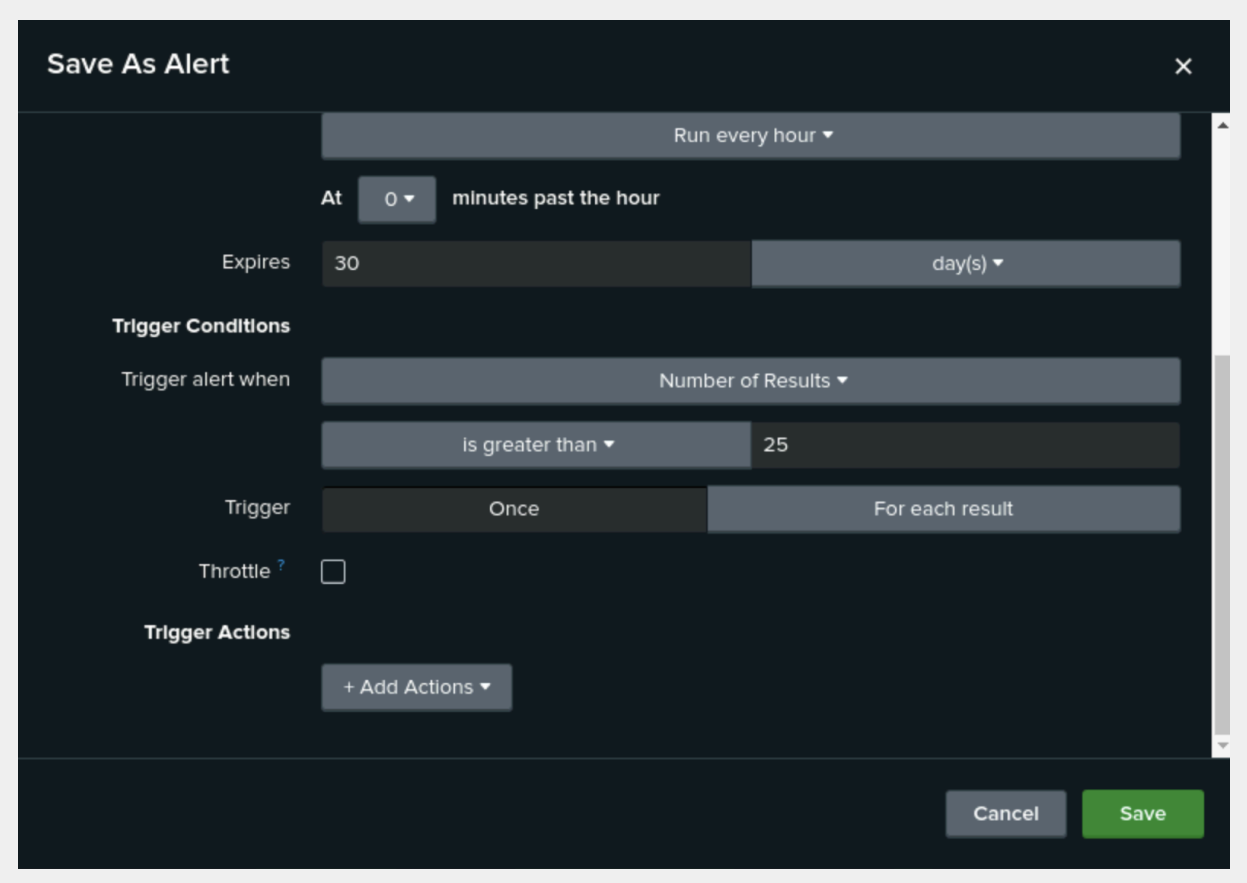
0-25 - normal behaviour
25-50 - worth investigating
50+ - considered critical, investigate immediately

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




Hide Fields
All Fields
List
Format
50 Per Page
Key_Name 100+
Key_Type 1
Keywords 1
linecount 14
LogName 1
Logon_GUID 100+
Logon_ID 100+
Logon_Process 100+
Logon_Type 21
member_dn 2
member_id 14
member_nt_domain 3
Message 100+
name 7
object 1
OpCode 1
Operation 2
Package_Name__NTLM_only 1
process_id 100+
Process_ID 100+
product 1
Provider_Name 100+
punct 18
raw 100+
Time
Event
2/21/20
5:10:48.000 PM
02/21/2020 17:10:48,,"WINDOWS
WINDOWS","ADMINISTRATOR
name
7 Values, 89.524% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
An account failed to log on
1,004
29.97%
An account was logged off
417
12.448%
Special privileges assigned to new logon
414
12.358%
A logon was attempted using explicit credentials
399
11.91%
Key file operation
382
11.403%
Cryptographic operation
369
11.015%
An account was successfully logged on
365
10.896%
source="Administrator_logs.csv" host="7d537f3f8829" sourcetype="csv" name="An account failed to log on"
All time
1,004 events (before 12/3/24 9:23:36.000 PM)
No Event Sampling
Job
Smart Mode
Events (124)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Feb 21, 2020 9:00 AM
Feb 21, 2020 10:00 AM
1 hour
List
Format
50 Per Page
Prev
1
2
3
Next
Hide Fields
All Fields
Time
Event
source="Administrator_logs.csv" host="7d537f3f8829" sourcetype="csv" name="An account failed to log on"
All time
1,004 events (before 12/3/24 9:23:36.000 PM)
No Event Sampling
Job
Smart Mode
Events (23)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Feb 21, 2020 4:00 AM
Feb 21, 2020 5:00 AM
1 hour
List
Format
50 Per Page
Hide Fields
All Fields
Time
Event


Save As Alert
Settings
Title
Brute Force Attempt
Description
Logons have captured suspicious activity which could be a potential brute force attack. Investigation should be done.
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every week
On
Monday
at
6:00
Expires
30
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
Cancel
Save


Save As Alert
Run every hour
At 0 minutes past the hour
Expires 30 day(s)
Trigger Conditions
Trigger alert when Number of Results
is greater than 25
Trigger Once For each result
Throttle
Trigger Actions
+ Add Actions
Cancel
Save