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

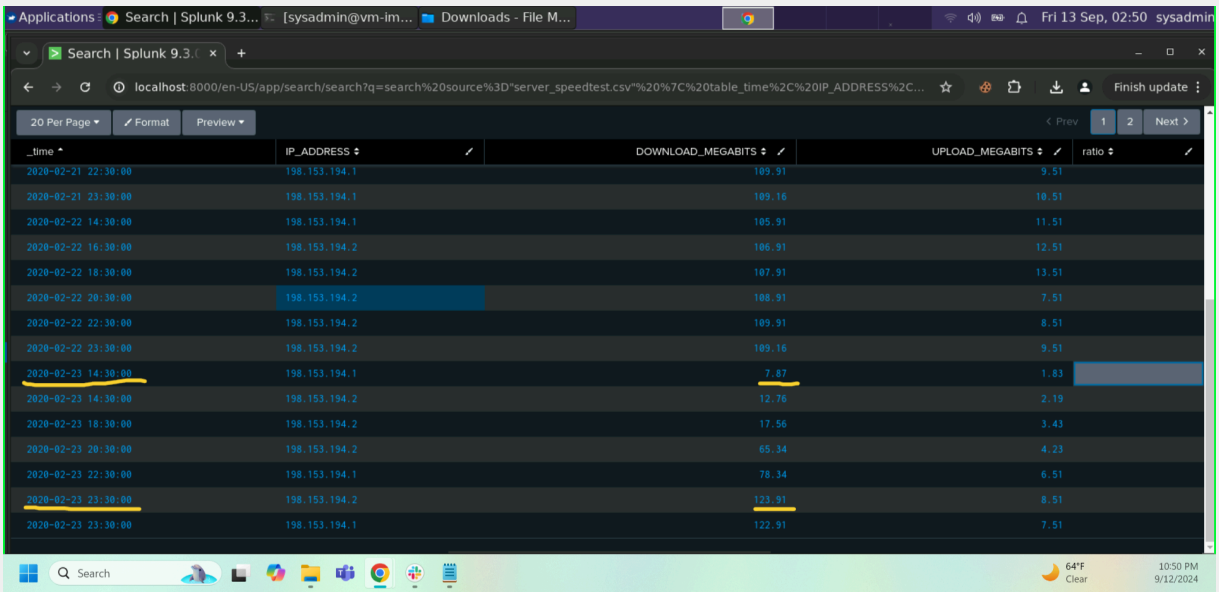
1. Based on the report you created, what is the approximate date and time of the attack?

```
The approximate date and time of the attack was February 23, 2020 at
14:30:00. This was when an obvious and significant drop in megabits
occurred.
```

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

```
The download megabits returned to more normal levels at 23:30:00 on Feburary
23, 2020 translating to about 9 total hours of download speed slowness.
```

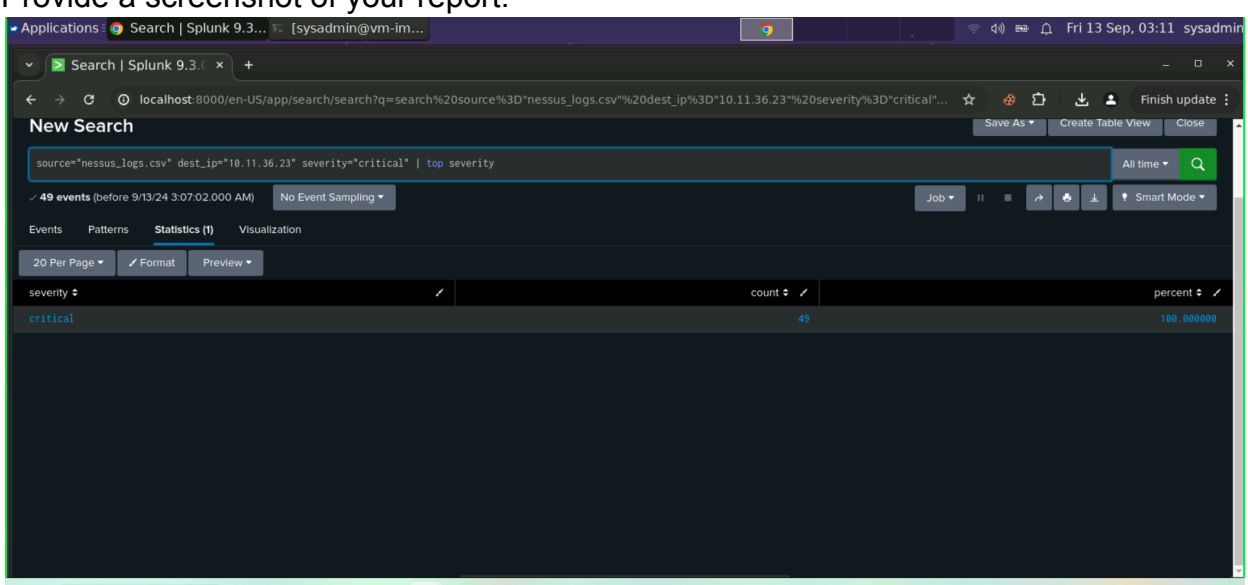
Provide a screenshot of your report:



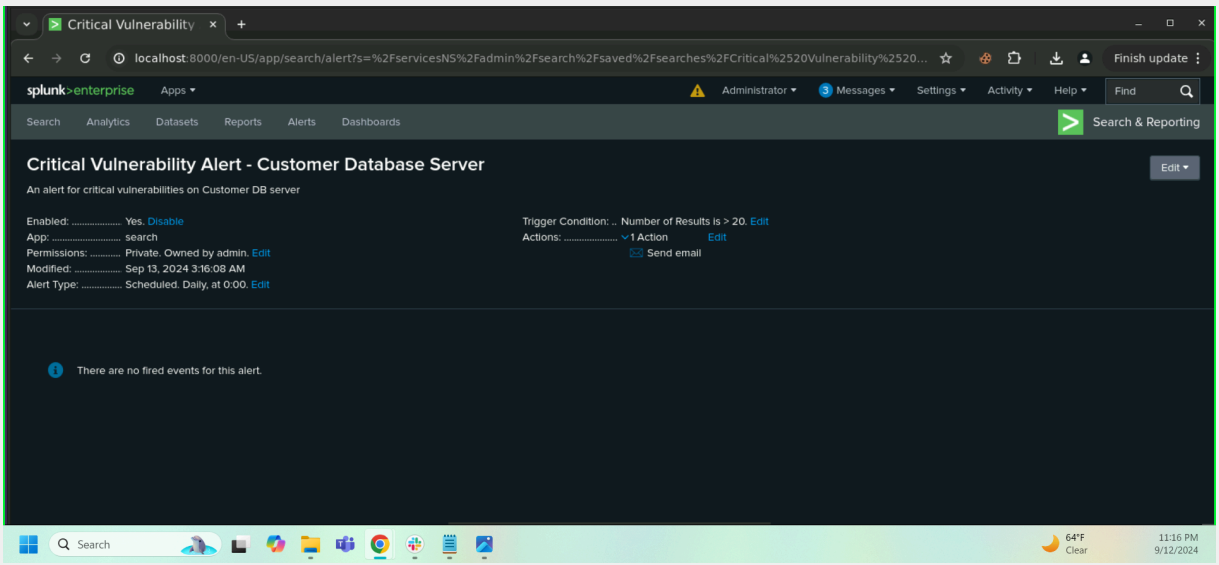
Screenshot of the first instance of a significant drop in megabits and the window of time it took to recover back to normal levels.

Step 2: Are We Vulnerable?

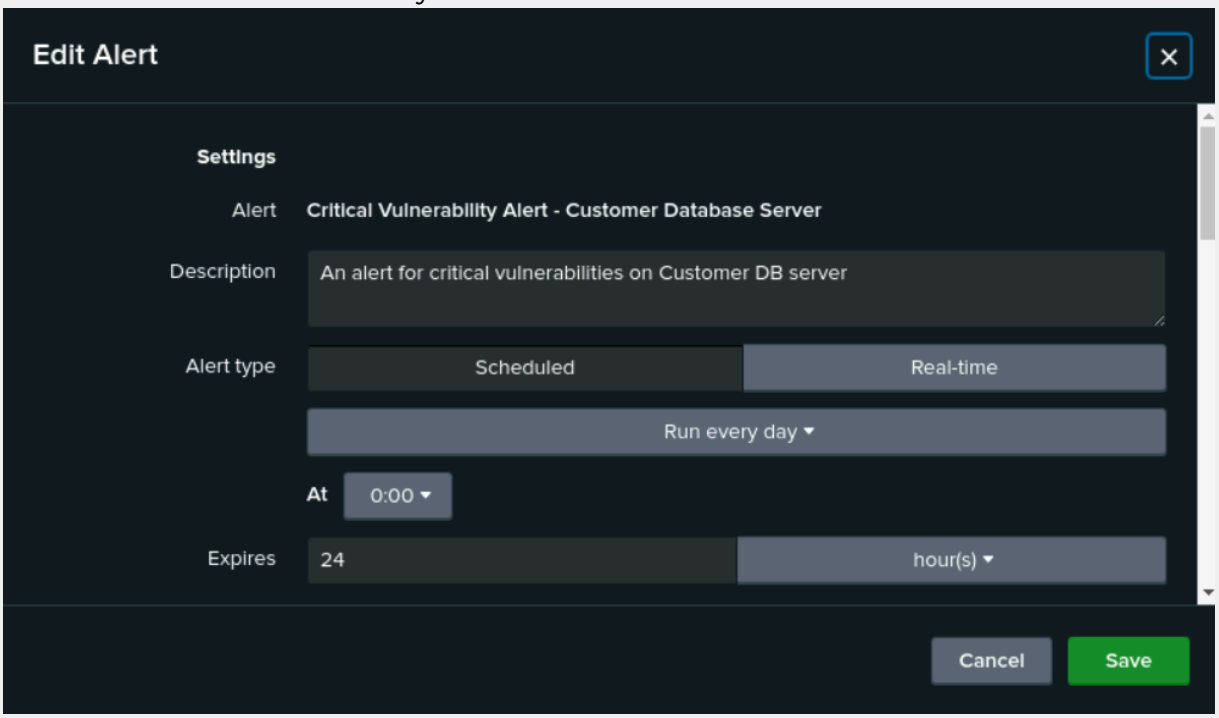
Provide a screenshot of your report:

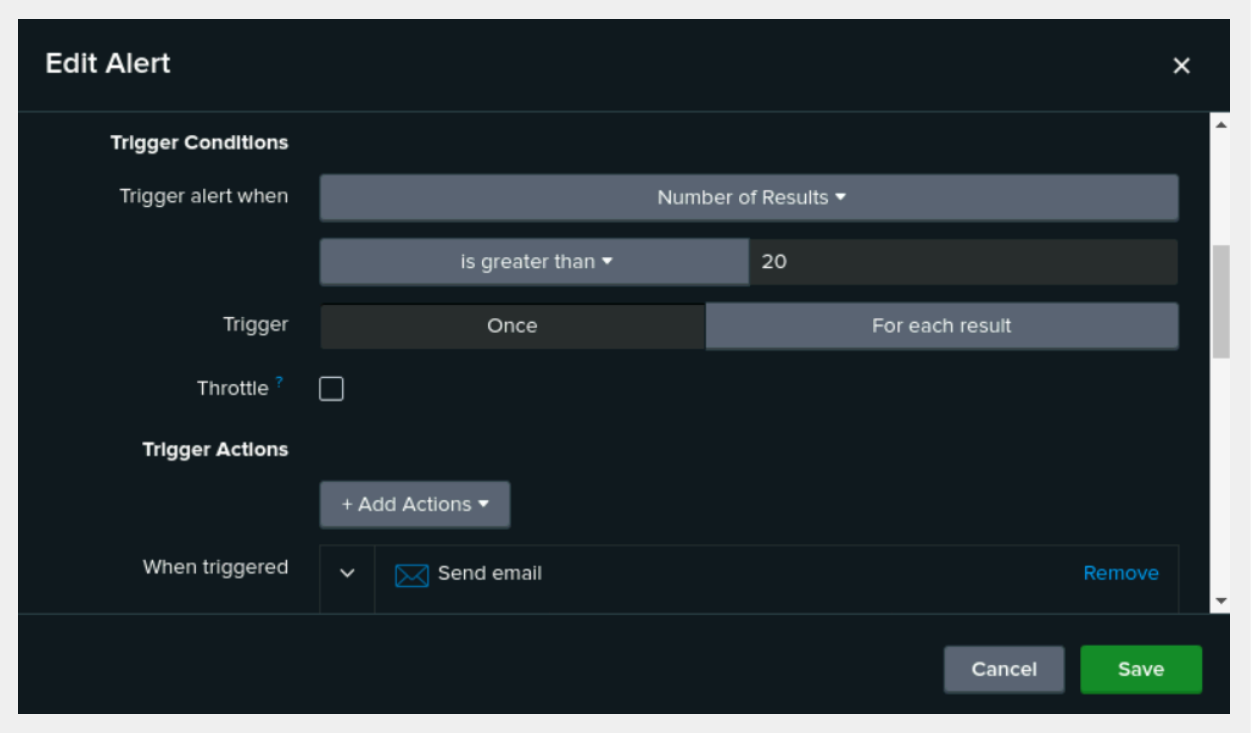


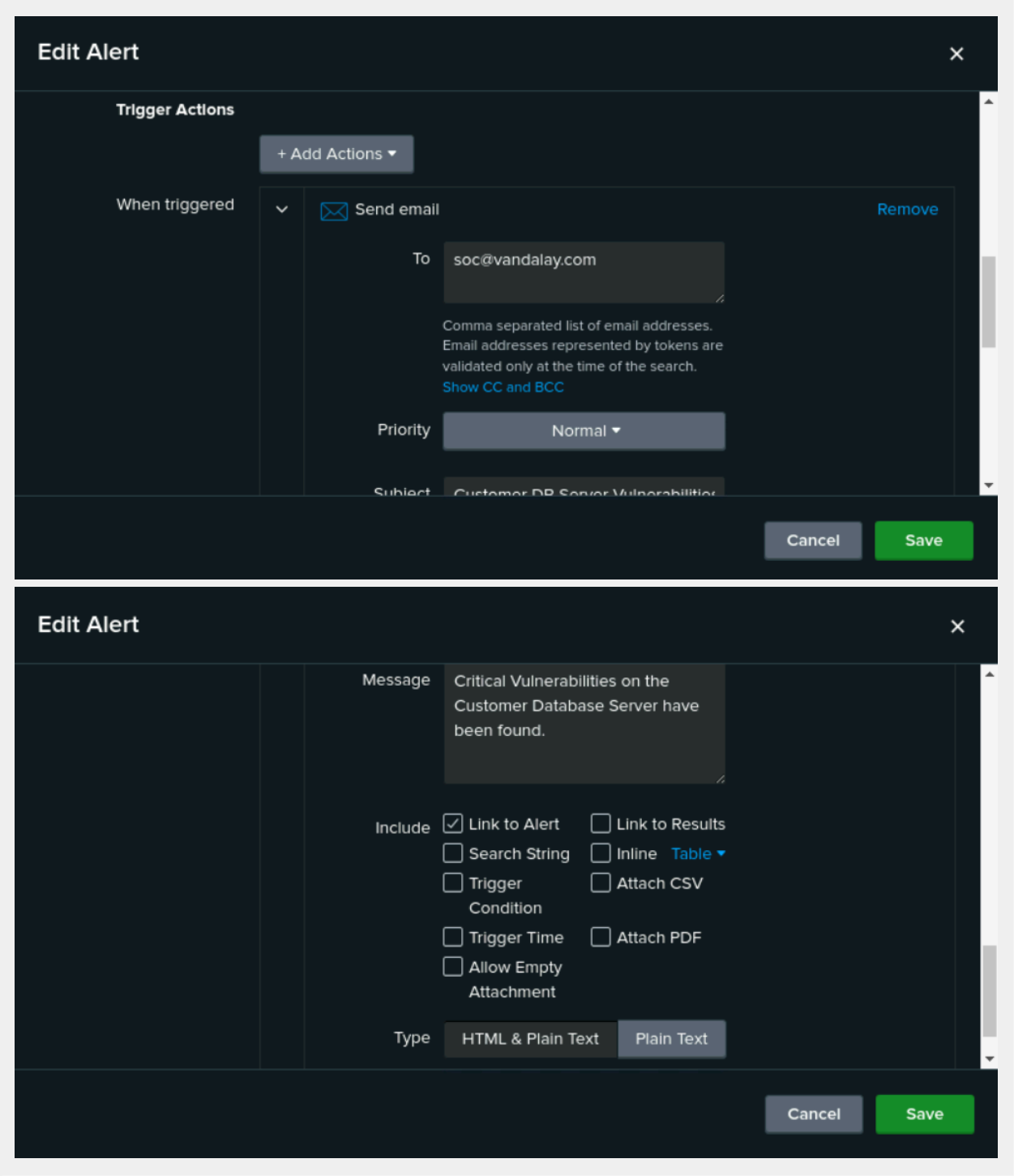
Provide a screenshot showing that the alert has been created:



My trigger condition was set at 20 to account for “false positives.” Lower conditions may result in an alert being triggered more frequently for vulnerabilities incorrectly classified as critical.

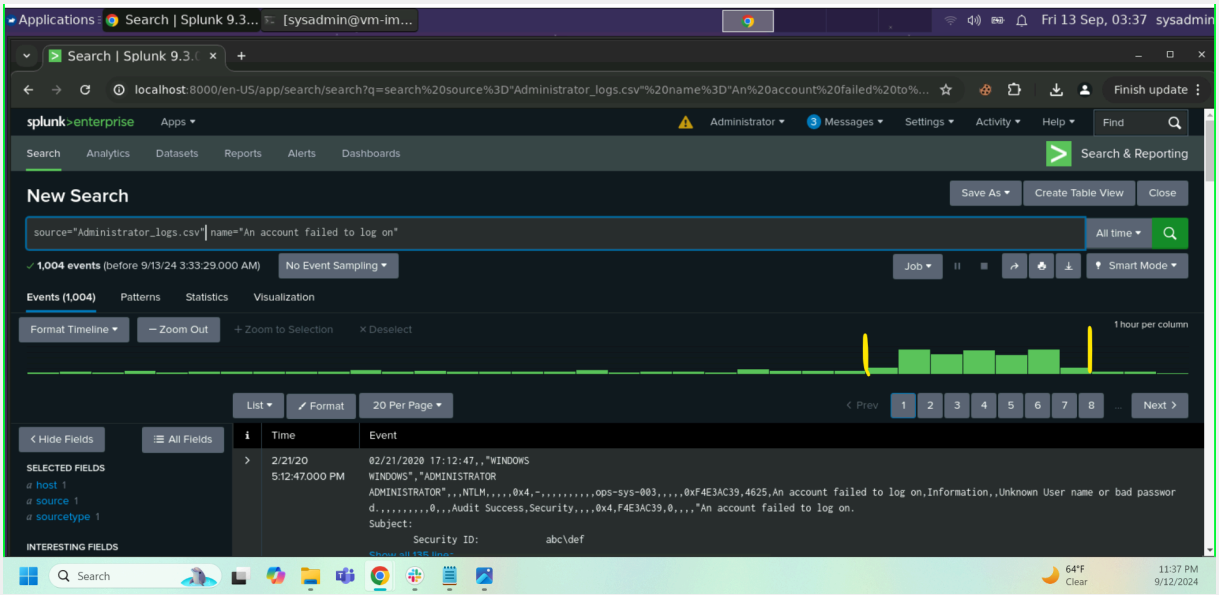



Edit Alert
Trigger Conditions
Trigger alert when
Number of Results
is greater than
20
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
When triggered
Send email
Remove
Cancel
Save



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

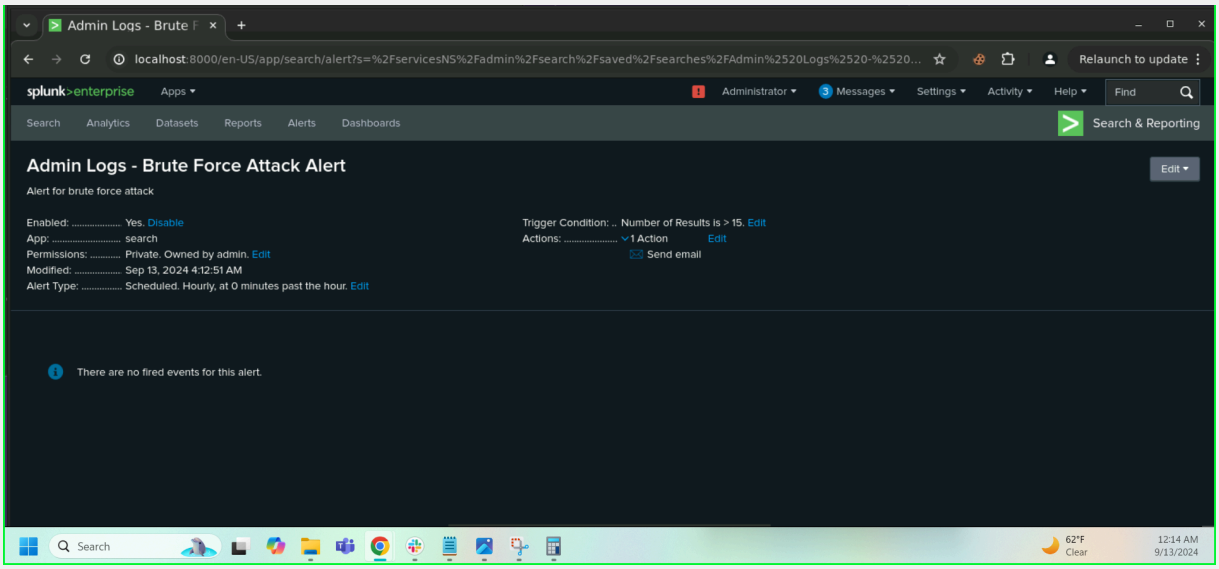


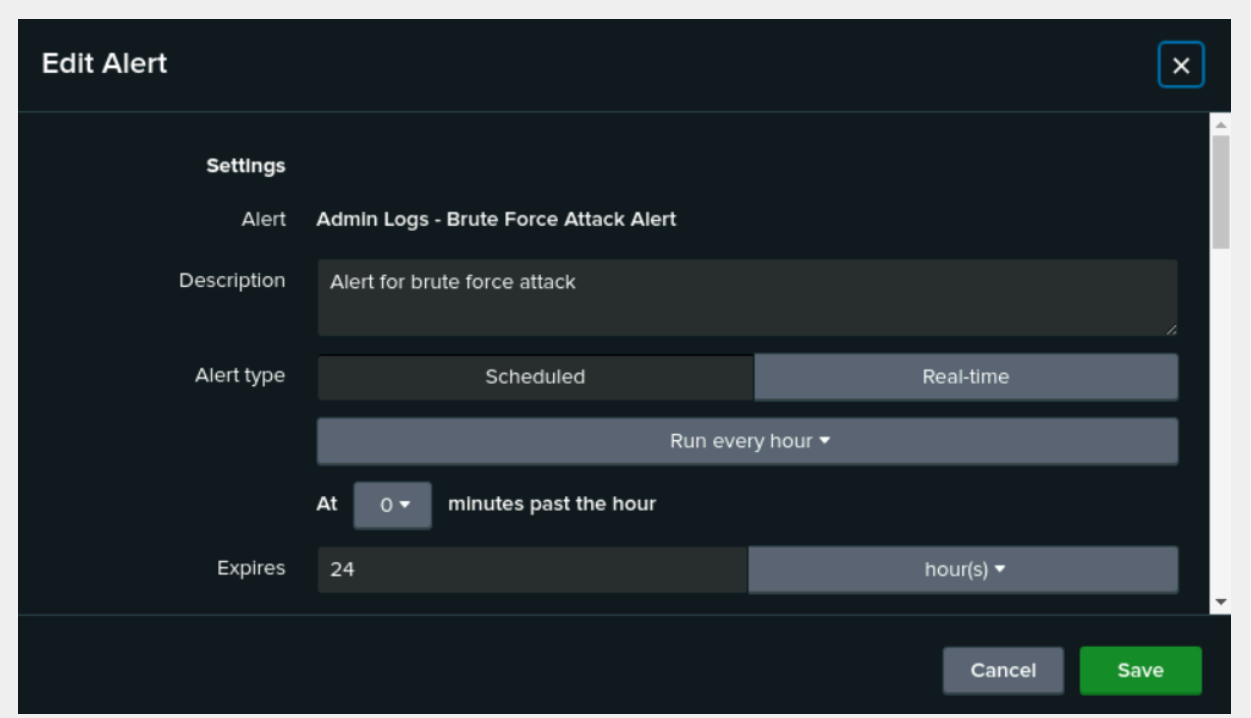
It appears a typical amount of failed login attempts range from as little as 8 in an hour to as many as 23 in an hour. At **8am on Friday, February 21, 2020**, we see failed login attempts deviate from this range to 34 failed attempts. That number increases to 124 failed attempts at 9am. Between the hours of 9am and 1pm there were over 95 failed login attempts each hour. At 2pm the number reduced to 34 failed login attempts that hour before returning to our baseline.

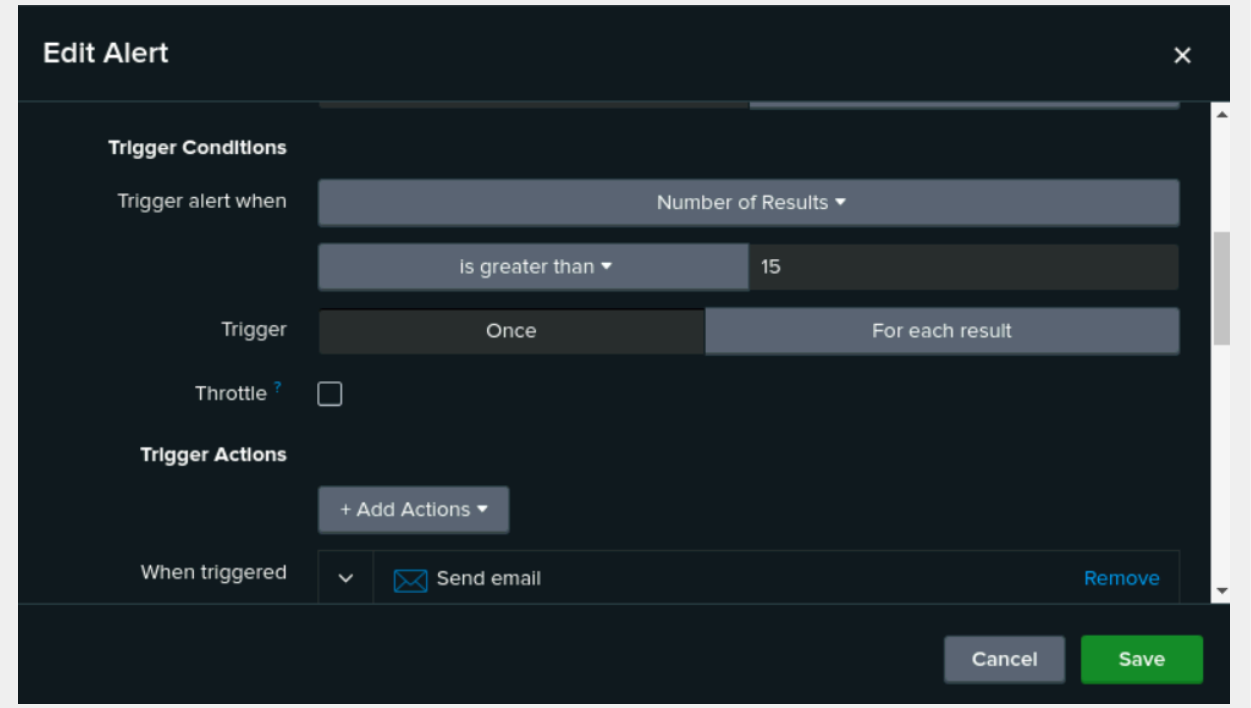
2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

The total number of failed logins in the 26 hours before the brute force attack began was about 366. I took 366 and divided it into 26 to get an average of 14.07 failed logins per hour. My suggested baseline of normal activity would not exceed about 15 failed logins in an hour.

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


Admin Logs - Brute F
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FAdmin%2520Logs%2520-%2520...
Relaunch to update
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Admin Logs - Brute Force Attack Alert
Edit
Alert for brute force attack
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Sep 13, 2024 4:12:51 AM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit
Trigger Condition: Number of Results is > 15. Edit
Actions: 1 Action Edit
Send email
There are no fired events for this alert.
Search
62°F
Clear
12:14 AM
9/13/2024


Edit Alert
Settings
Alert
Admin Logs - Brute Force Attack Alert
Description
Alert for brute force attack
Alert type
Scheduled
Real-time
Run every hour
At
0
minutes past the hour
Expires
24
hour(s)
Cancel
Save


Edit Alert
Trigger Conditions
Trigger alert when
Number of Results
is greater than
15
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
When triggered
Send email
Remove
Cancel
Save