Step 1: The Need for Speed

Background: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandaly has been experiencing DDOS attacks against their web servers.

Not only were web servers taken offline by a DDOS attack, but upload and download speed were also significantly impacted after the outage. Your networking team provided results of a network speed run around the time of the latest DDOS attack.

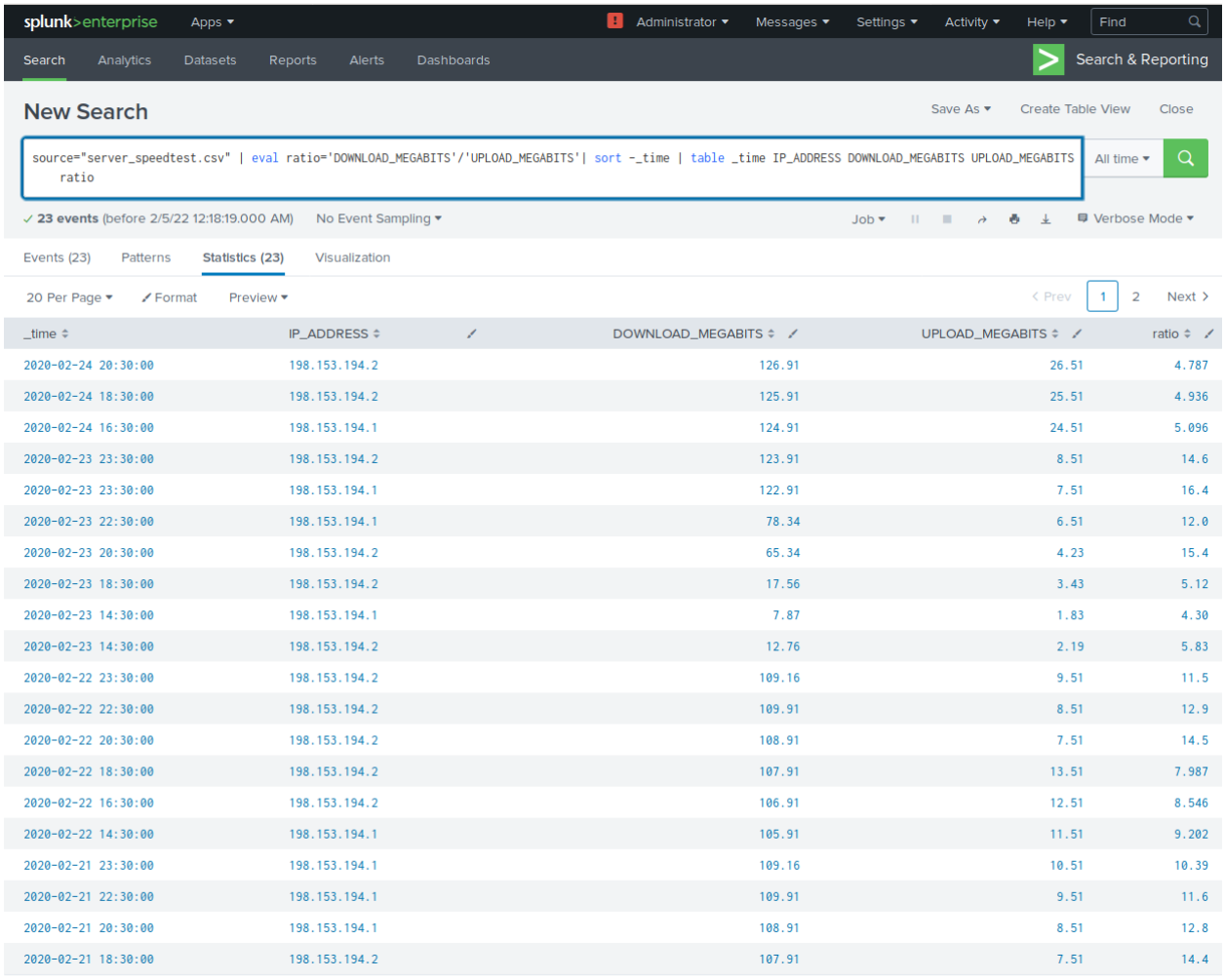
Task: Create a report to determine the impact that the DDOS attack had on download and upload speed. Additionally, create an additional field to calculate the ratio of the upload speed to the download speed.

1. Upload the following file of the system speeds around the time of the attack.
    - Speed Test File
2. Using the **eval command**, create a field called ratio that shows the ratio between the upload and download speeds.
    - Hint: The format for creating a ratio is: | eval new_field_name = 'fieldA' / 'fieldB'

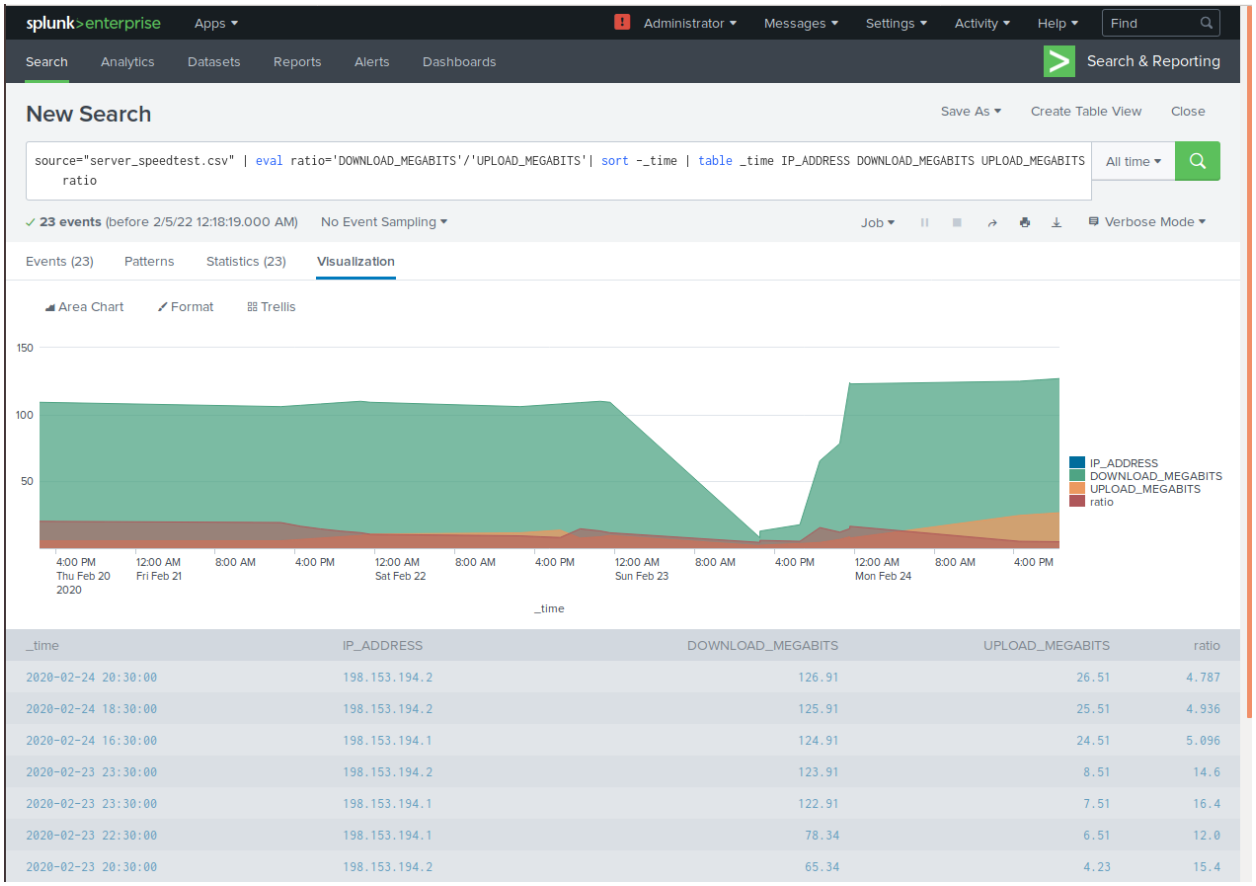
source="server_speedtest.csv" | eval ratio='DOWNLOAD_MEGABITS'/'UPLOAD_MEGABITS'

3. **Create a report using the Splunk's table command** to display the following fields in a statistics report:
    - _time
    - IP_ADDRESS
    - DOWNLOAD_MEGABITS
    - UPLOAD_MEGABITS
    - ratio
4. Hint: Use the following format when for the table command: | table fieldA fieldB fieldC

source="server_speedtest.csv" | eval ratio='DOWNLOAD_MEGABITS'/'UPLOAD_MEGABITS'| sort -_time | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio



_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	4.787
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	4.936
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	5.096
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	16.4
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	15.4
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	5.12
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	4.30
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	5.83
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	11.5
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	12.9
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	14.5
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	7.987
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	8.546
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	9.202
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	10.39
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	11.6
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	12.8
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	14.4



_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	4.787
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	4.936
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	5.096
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	16.4
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	15.4

Take note of this particular section of the results by sorting the results by time:

2020-02-22 18:30:00	198.153.194.2	107.91	13.51	7.987
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	14.5
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	12.9
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	11.5
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	4.30
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	5.83
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	5.12
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	15.4
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	16.4

5. Answer the following questions:

    - Based on the report created, what is the approximate date and time of the attack?

Based on the data provided above, the attack began on: **2020-02-23 at 1430 hours (2:30PM)** when the **download speed dropped from 108/109 average megabit download down to 7.87 megabits.**

- How long did it take your systems to recover?

It took a total of **nine** hours for the systems to recover.

Submit a screenshot of your report and the answer to the questions above.

Step 2: Are We Vulnerable?

Background: Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

- For more information on Nessus, read the following link: https://www.tenable.com/products/nessus

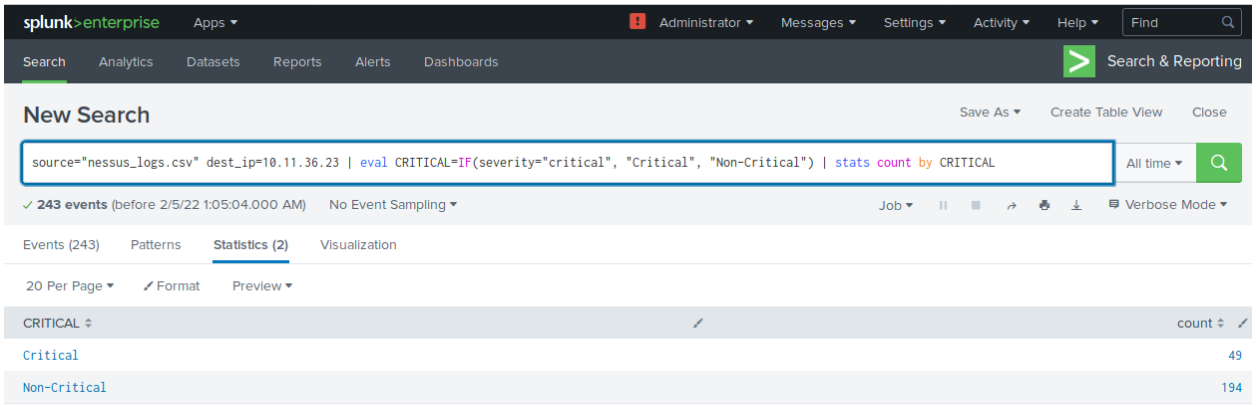
Task: Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

- Upload the following file from the Nessus vulnerability scan.
  Nessus Scan Results

CRITICAL

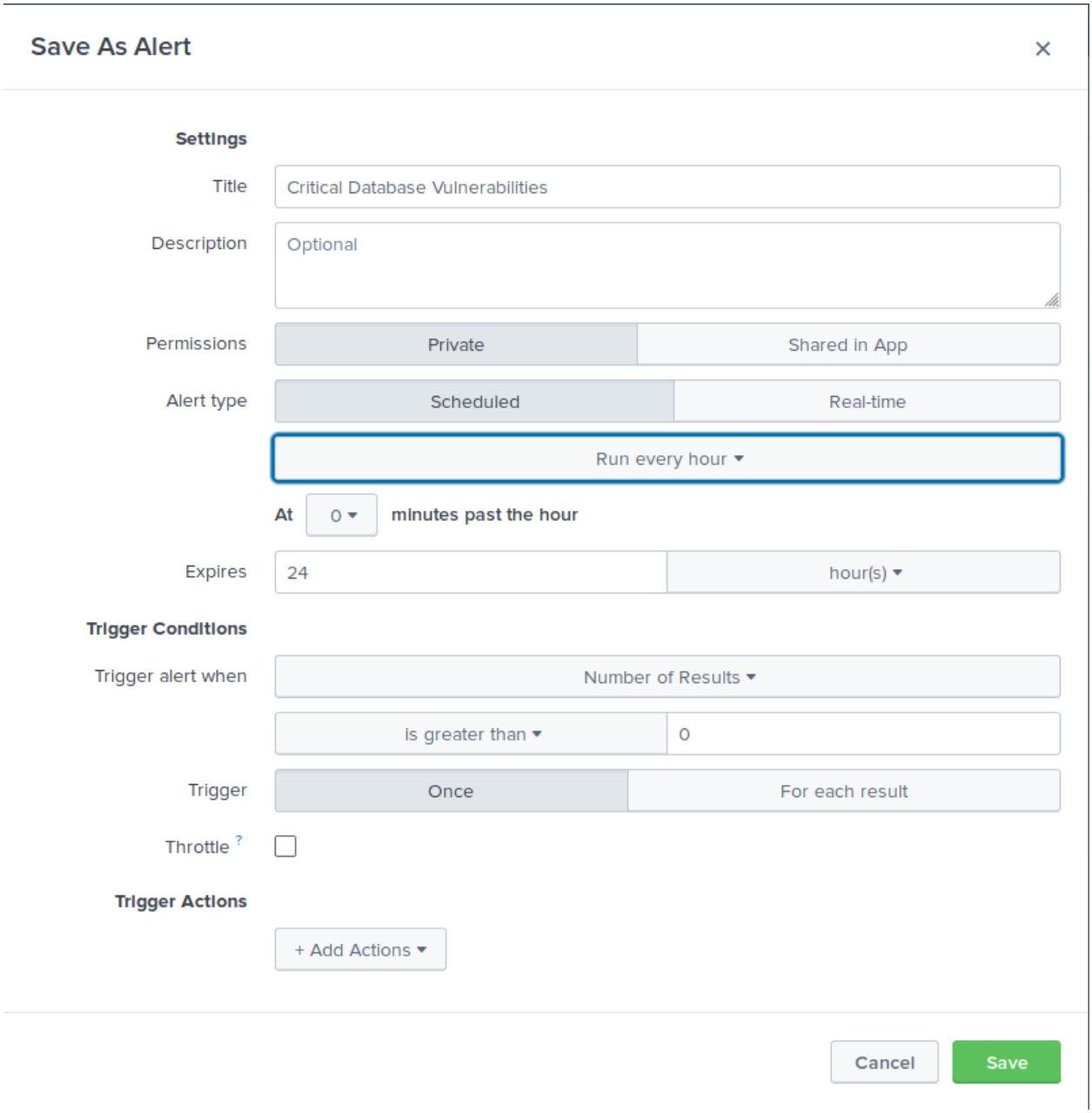
- Create a report that shows the count of critical vulnerabilities from the customer database server.
  - The database server IP is 10.11.36.23.
  - The field that identifies the level of vulnerabilities is severity.

source="nessus_logs.csv" dest_ip=10.11.36.23 | eval CRITICAL=IF(severity="critical", "Critical", "Non-Critical") | stats count by CRITICAL

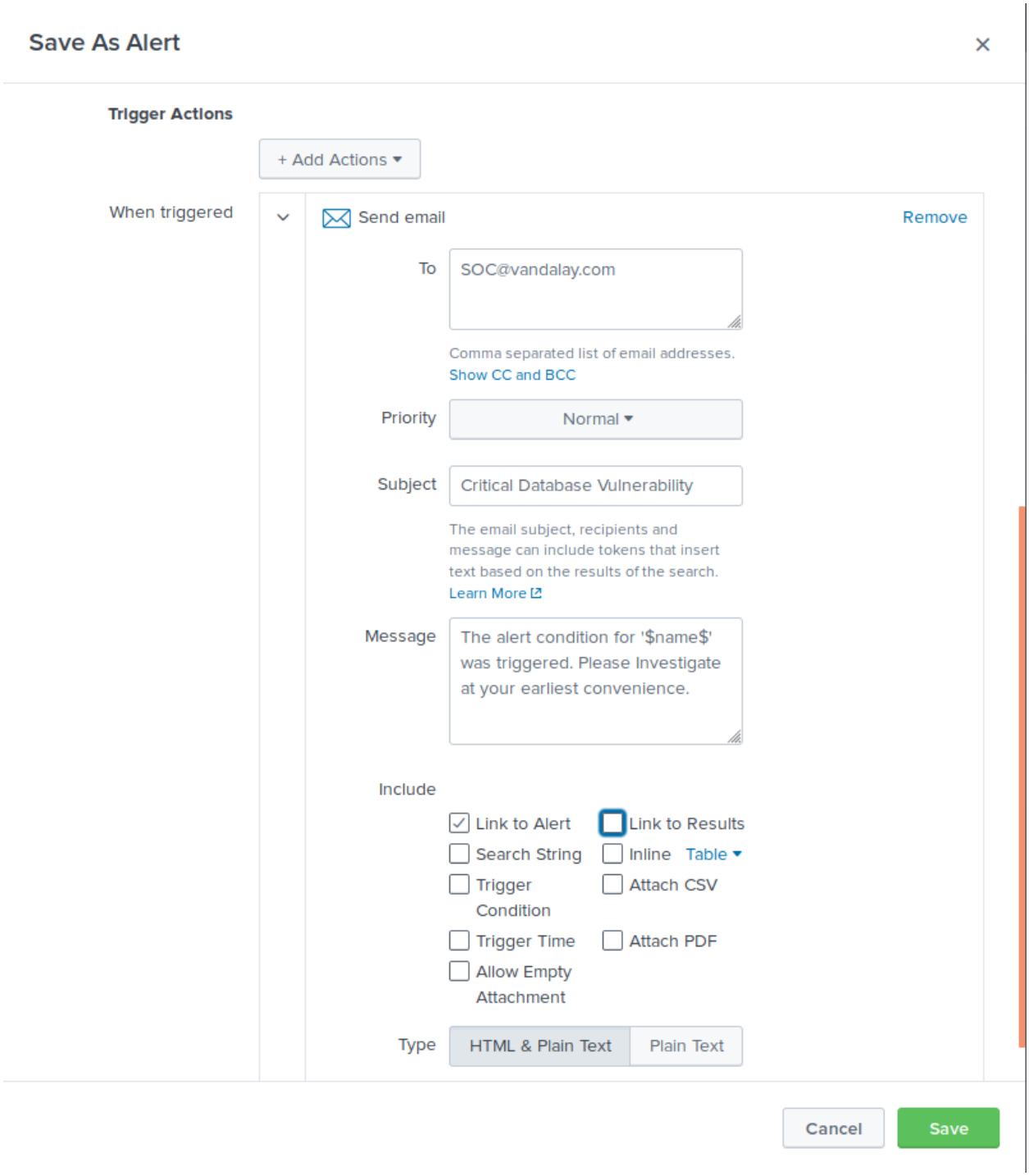


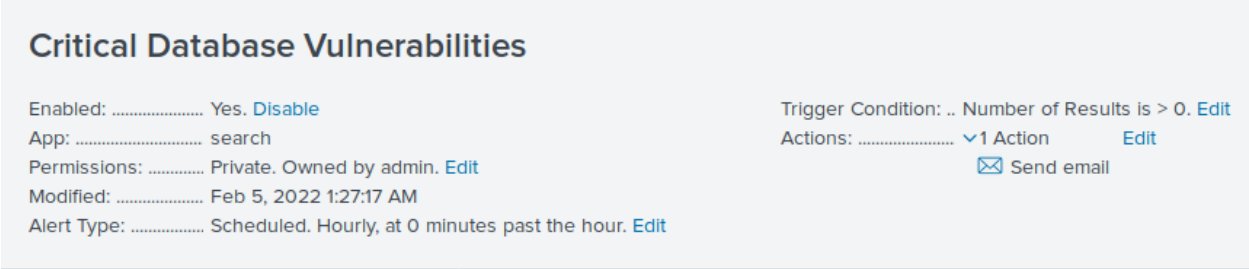
Our results list **Forty-Nine (49) “Critical” and One hundred ninety-four (194) “Non-Critical” results**

- Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to soc@vandalay.com.



From here click on “Add Actions” at the bottom and select “Send email”


Save As Alert
Trigger Actions
+ Add Actions
When triggered
Send email
Remove
To
SOC@vandalay.com
Comma separated list of email addresses.
Show CC and BCC
Priority
Normal
Subject
Critical Database Vulnerability
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 '$name$' was triggered. Please Investigate at your earliest convenience.
Include
Link to Alert
Link to Results
Search String
Inline
Table
Trigger Condition
Attach CSV
Trigger Time
Attach PDF
Allow Empty Attachment
Type
HTML & Plain Text
Plain Text
Cancel
Save



Submit a screenshot of your report and a screenshot of proof that the alert has been created.

Step 3: Drawing the (base)line

Background: A Vandaly server is also experiencing brute force attacks on their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.

Task: Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.

1. Upload the administrator login logs.
    - Admin Logins
2. When did the brute force attack occur?
    - Hints:
        - Look for the name field to find failed logins.
        - Note the attack lasted several hours.
3. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.

source="Administrator_logs.csv" | stats count by name | sort -count | eval Bruteforce=if(name="An account failed to log" AND count>5, "Potential Brute Force", "Not Brute Force")

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
source="Administrator_logs.csv" | stats count by name | sort -count | eval Bruteforce=if(name="An account failed to log on" AND count>5, "Potential
    Brute Force", "Not Brute Force")
```

All time

✓ **3,742 events** (before 2/5/22 1:40:30.000 AM) No Event Sampling Job Verbose Mode

Events (3,742) Patterns **Statistics (7)** Visualization

20 Per Page Format Preview

name	count	Bruteforce
An account failed to log on	1004	Potential Brute Force
An account was logged off	417	Not Brute Force
Special privileges assigned to new logon	414	Not Brute Force
A logon was attempted using explicit credentials	399	Not Brute Force
Key file operation	382	Not Brute Force
Cryptographic operation	369	Not Brute Force
An account was successfully logged on	365	Not Brute Force

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

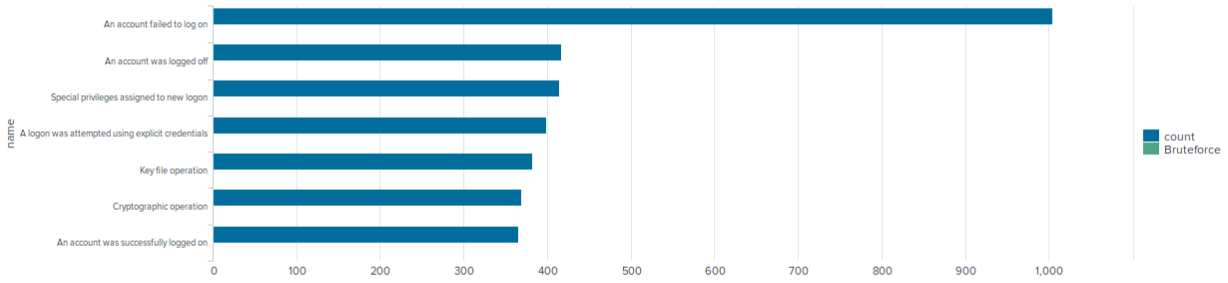
source="Administrator_logs.csv" | stats count by name | sort -count | eval Bruteforce=if(name="An account failed to log on" AND count>5, "Potential
Brute Force", "Not Brute Force")

All time

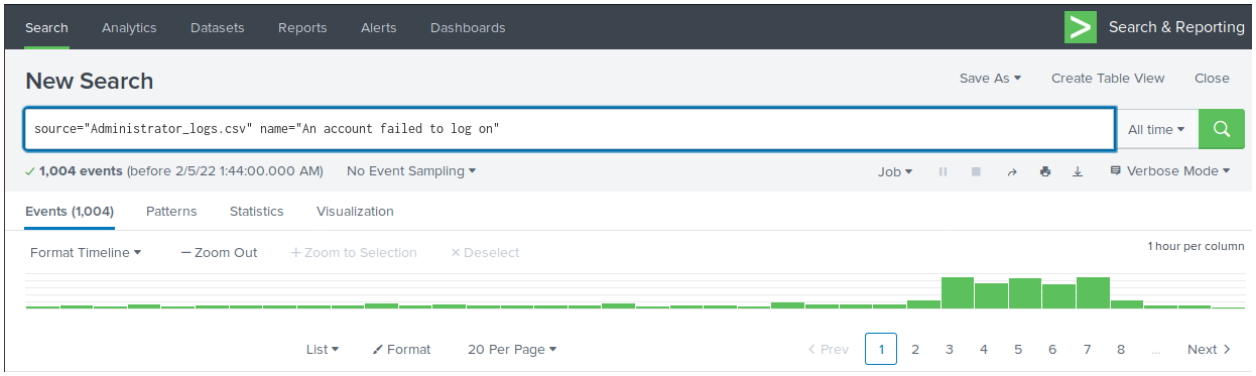
✓ 3,742 events (before 2/5/22 1:40:30.000 AM) No Event Sampling Job Verbose Mode

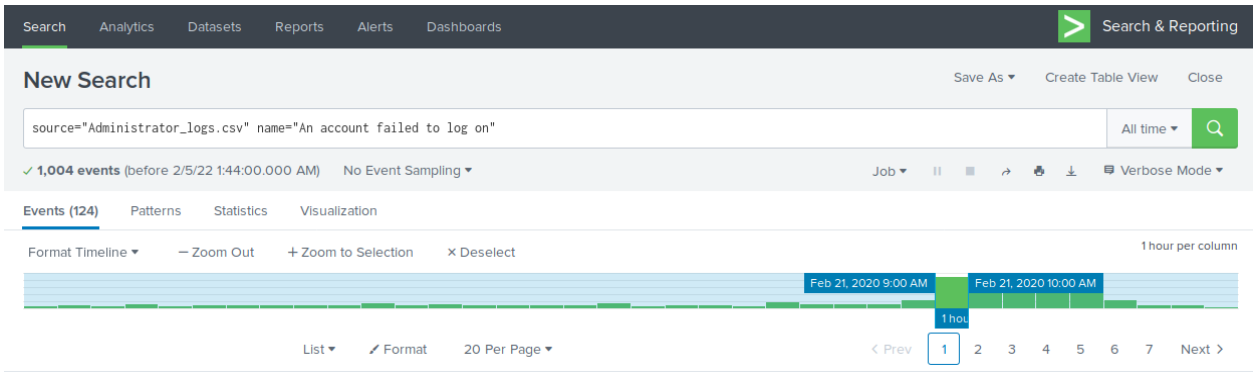
Events (3,742) Patterns Statistics (7) Visualization

Bar Chart Format Trellis



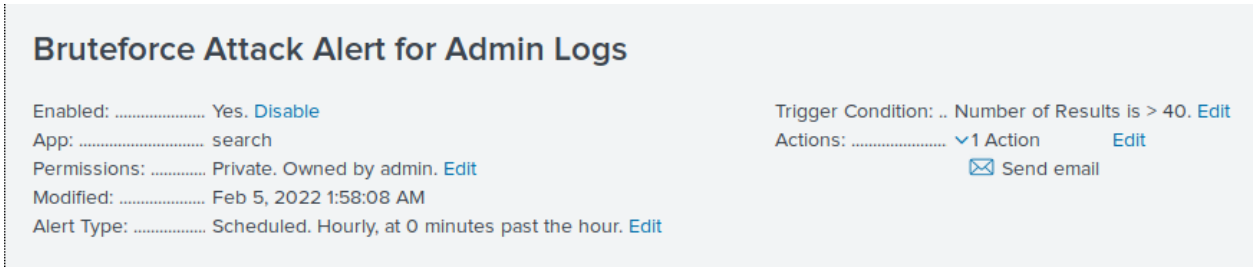
name	count	Bruteforce
An account failed to log on	1004	Potential Brute Force
An account was logged off	417	Not Brute Force
Special privileges assigned to new logon	414	Not Brute Force
A logon was attempted using explicit credentials	399	Not Brute Force
Key file operation	382	Not Brute Force
Cryptographic operation	369	Not Brute Force
An account was successfully logged on	365	Not Brute Force





If we examine the logs of when the attempts began to happen, we can identify that it began at **9:00AM on Feb 21st, 2020 and continued until 2:00PM of the same day** for a total of **5 hours**.

4. Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.



Data showed a range of 5-35 logins per hour; a threshold has been set to notify when logins occur at 40 or above per hour at SOC@vandalay.com as the email recipient.

Submit the answers to the questions about the brute force timing, baseline and threshold. Additionally, provide a screenshot as proof that the alert has been created.

Your Submission

In a word document, provide the following:

- Answers to all questions where indicated.
- Screenshots where indicated.