Unit 18 Homework: Lets go Splunking!

Scenario

You have just been hired as an SOC Analyst by Vandalay Industries, an importing and exporting company.

- Vandalay Industries uses Splunk for their security monitoring and have been experiencing a variety of security issues against their online systems over the past few months.
- You are tasked with developing searches, custom reports and alerts to monitor Vandalay's security environment in order to protect them from future attacks.

System Requirements

You will be using the Splunk app located in the Ubuntu VM.

Your Objective

Utilize your Splunk skills to design a powerful monitoring solution to protect Vandaly from security attacks.

After you complete the assignment, you are asked to provide the following:

- Screen shots where indicated.
- Custom report results where indicated.

Topics Covered in This Assignment

- Researching and adding new apps
- Installing new apps
- Uploading files
- Splunk searching
- Using fields
- Custom reports
- Custom alerts

Let's get started!

Vandalay Industries Monitoring Activity Instructions

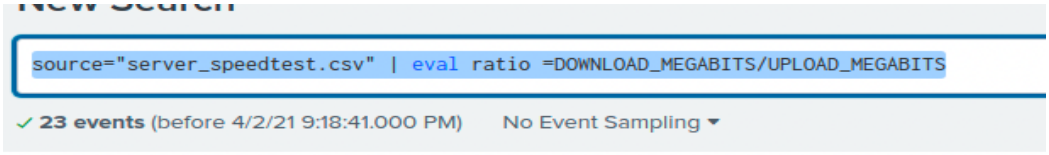
Step 1: The Need for Speed

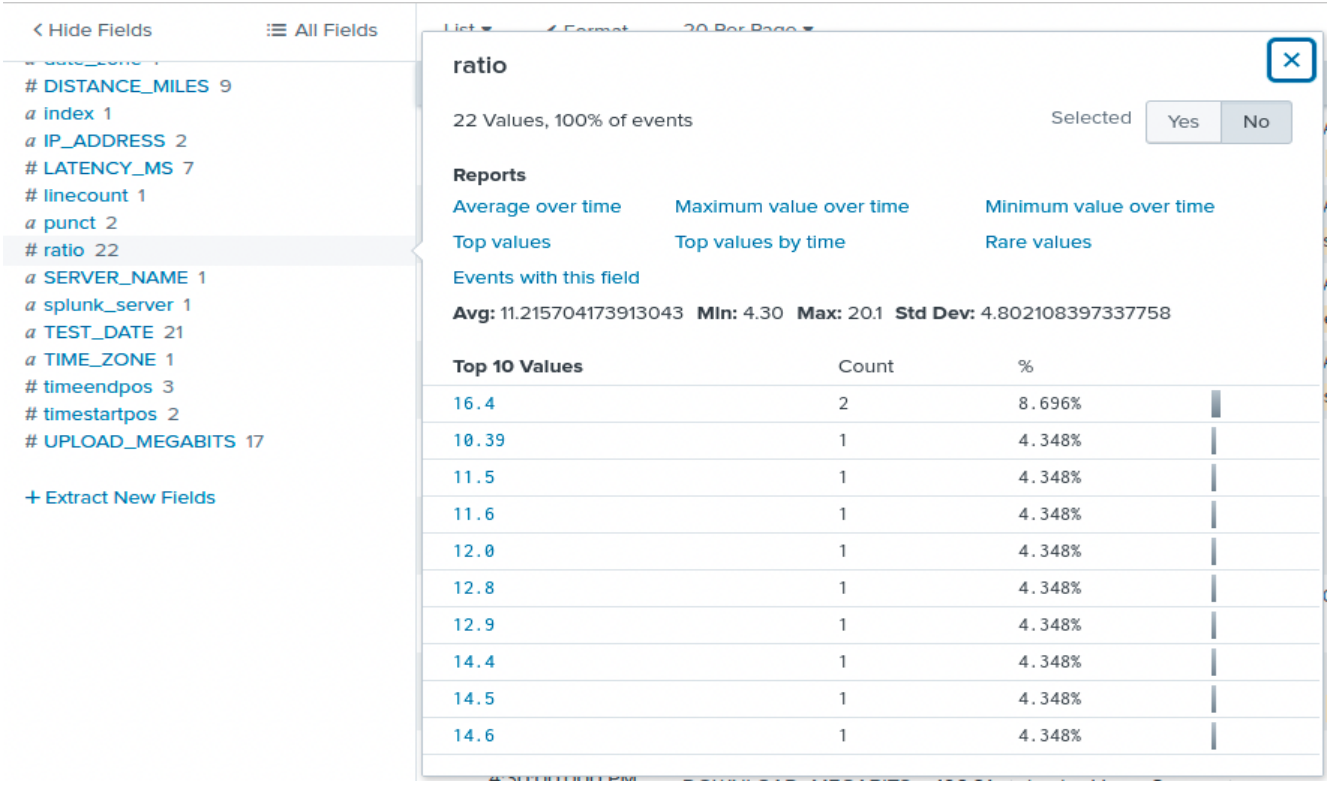
Background: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandaly has been experiencing DDOS attacks against their web servers.

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.

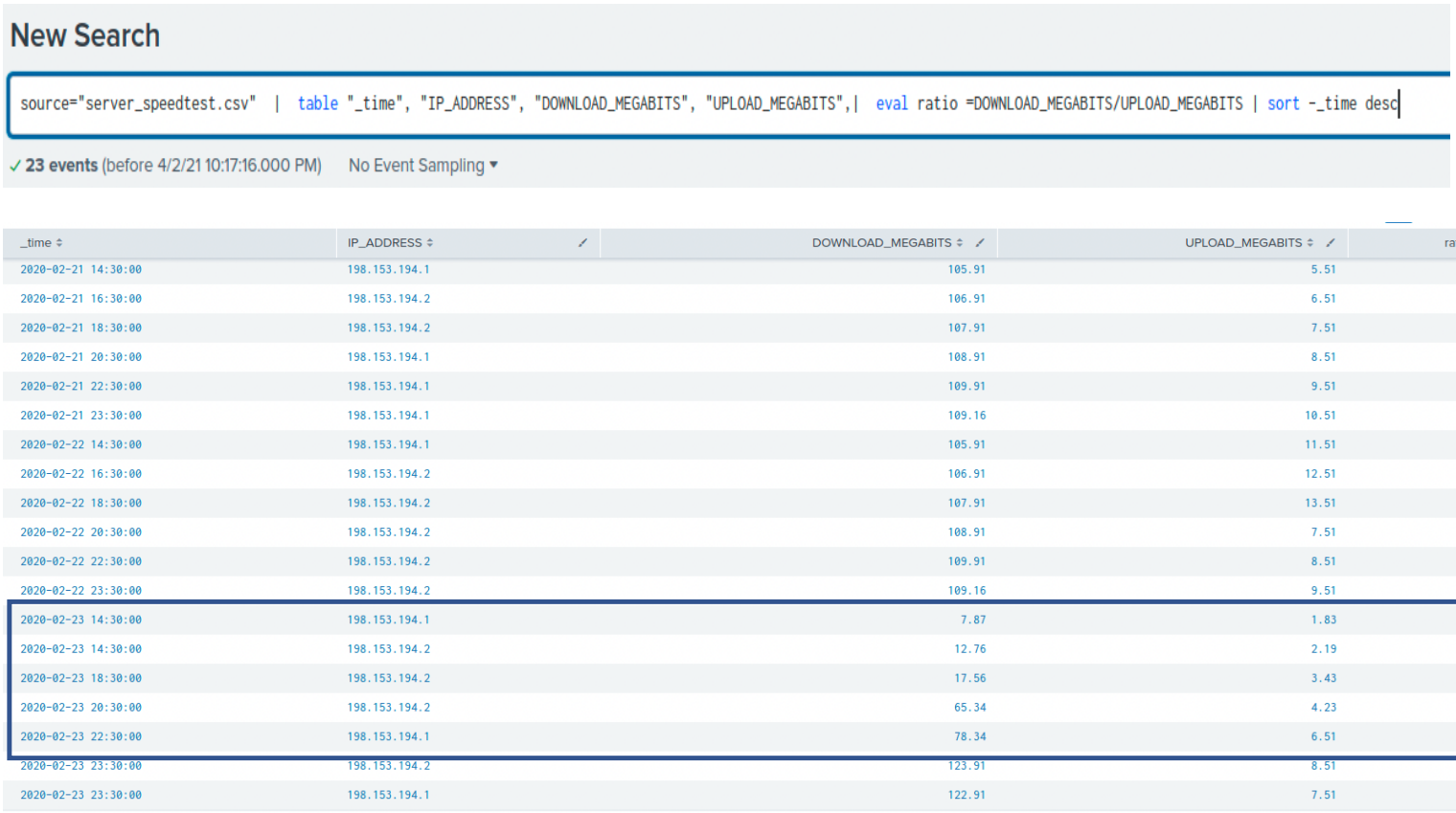
1. Upload the following file of the system speeds around the time of the attack.
    - Speed Test File
2. Using the `eval` command, create a field called `ratio` that shows the ratio between the upload and download speeds.
    - Hint: The format for creating a ratio is: `| eval new_field_name = 'fieldA'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



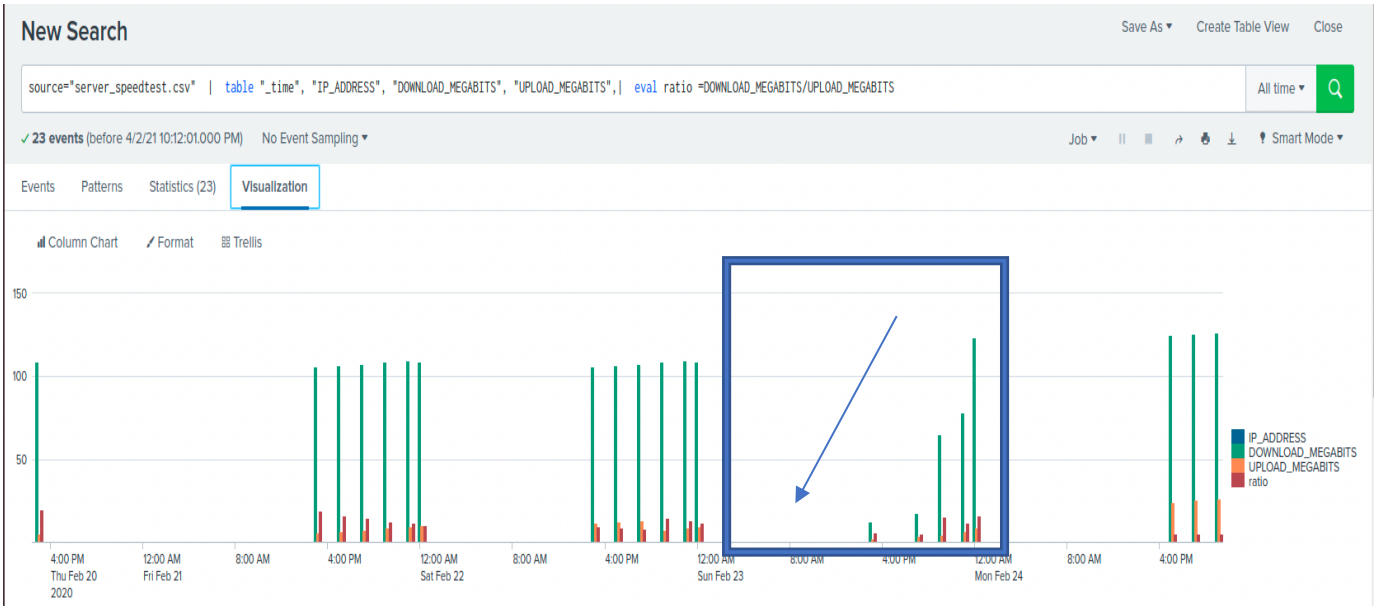


3. Create a report using the Splunk's `table` command to display the following fields in a statistics report:
    - `_time`
    - `IP_ADDRESS`
    - `DOWNLOAD_MEGABITS`
    - `UPLOAD_MEGABITS`
    - `ratio`

    Hint: Use the following format when for the `table` command: `| table fieldA fieldB fieldC`

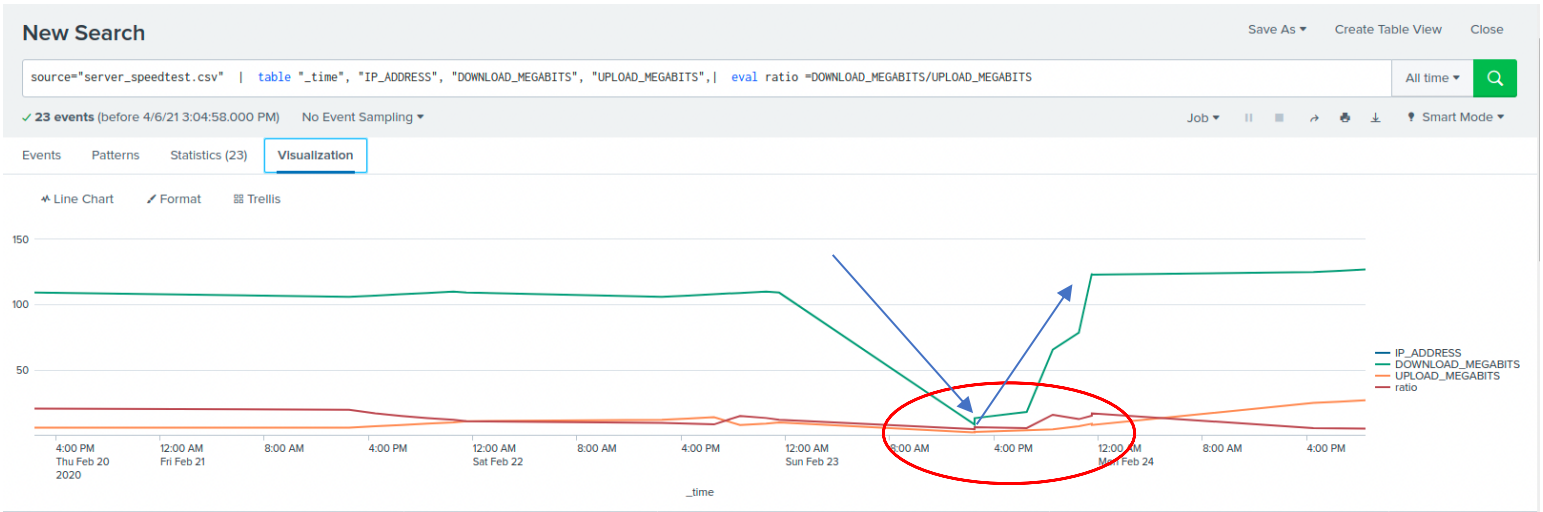


_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	19.2
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	16.4
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	14.4
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	12.8
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	11.6
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	10.39
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	9.202
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	8.546
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



4. Answer the following questions:
   - Based on the report created, what is the approximate date and time of the attack? **2/23/21 14:30 – 22:30**
   - How long did it take your systems to recover? **6 - 8 hours**. The **ratio** value for 20:30 and 22:30 hours are back to normal averaging the approximate timeframes on 2/21/21. However, Download_Megabits is still 25 – 30 mbs lower than its normal usual range for the same hours of 20:30 and 22:30 hours on 2/21/21. We can communicate that the system is recovering and performance is improving after 6 hours, and returned to normal completely after 8 hours.

Submit a screen shot of your report and the answer to the questions above. **See the two screenshots above, and below includes are more detailed and clear decline during the attack.**



The first diagram shows a step ladder down and up while the behavior was occurring. The second diagram clearly confirms there was a significant drop in performance during the event. The diagram displays the potential attack and possible recovery.

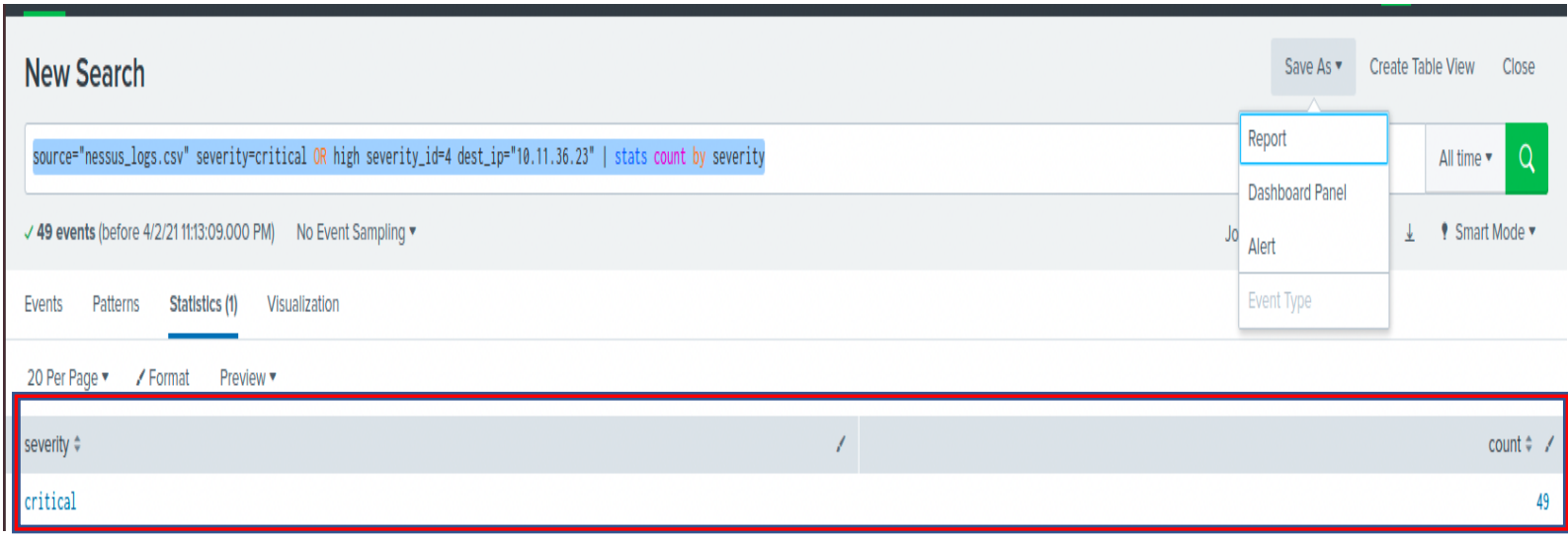
Step 2: Are We Vulnerable?

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

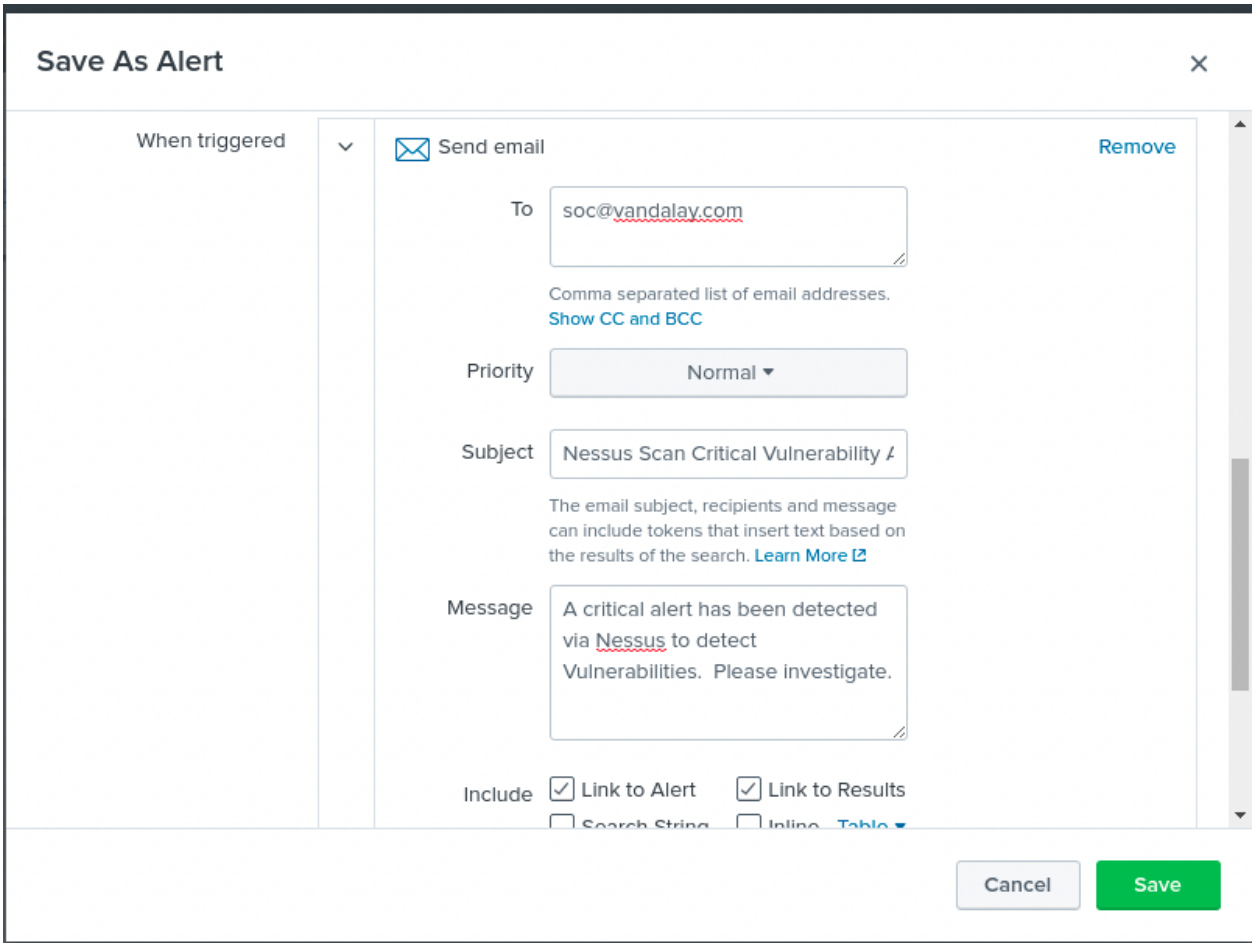
Task: Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

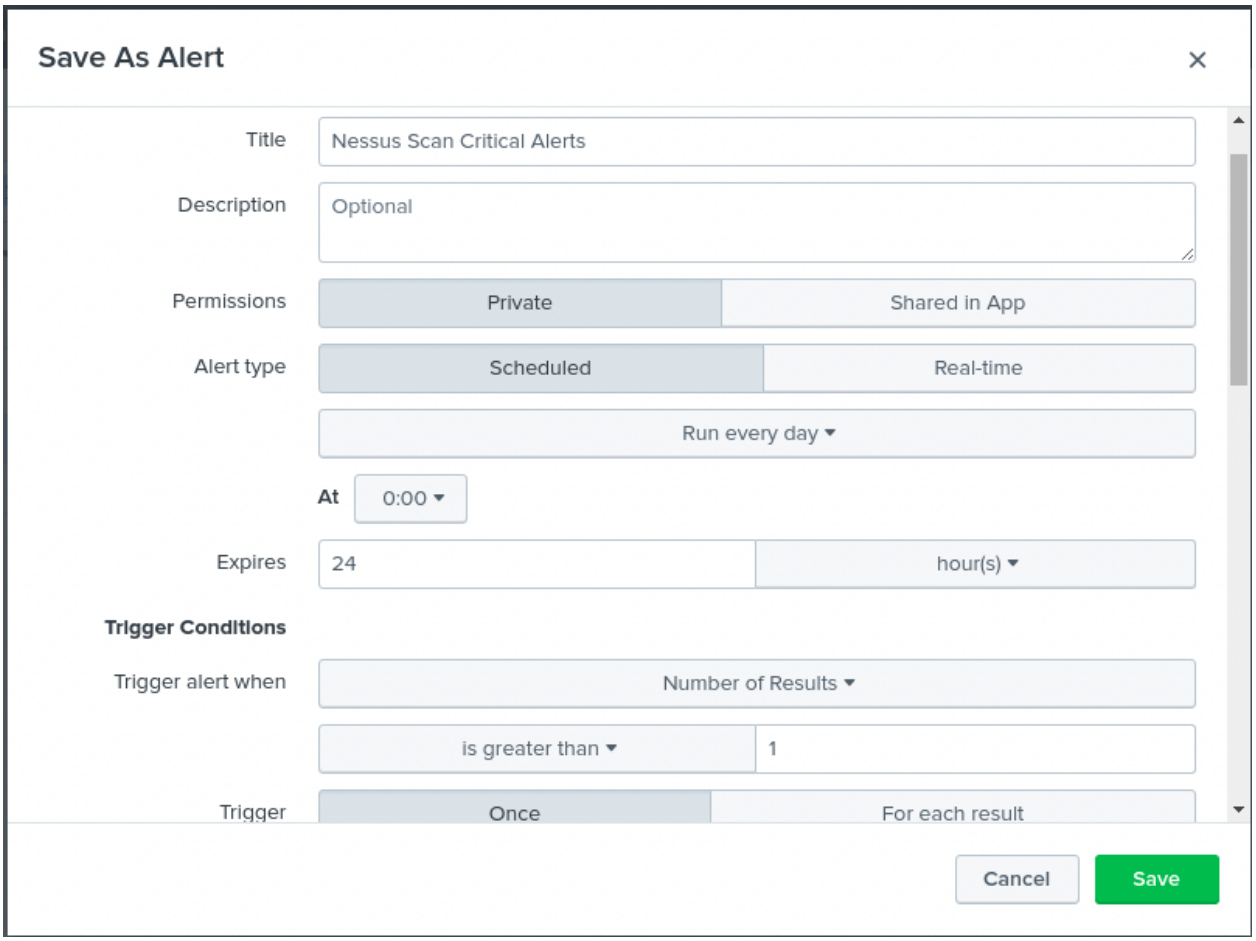
1. Upload the following file from the Nessus vulnerability scan.
    - Nessus Scan Results
2. Create a report that shows the `count` of critical vulnerabilities from the customer database server.
    - The database server IP is `10.11.36.23`.
    - The field that identifies the level of vulnerabilities is `severity`.



3. 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`.


Nessus Scan Critical Alerts
Edit
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Apr 2, 2021 11:23:17 PM
Alert Type: Scheduled. Daily, at 0:00. Edit
Trigger Condition: Number of Results is > 1. Edit
Actions: 1 Action Edit
Send email


Save As Alert
When triggered
Send email
Remove
To
soc@vandalay.com
Comma separated list of email addresses.
Show CC and BCC
Priority
Normal
Subject
Nessus Scan Critical Vulnerability A
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More
Message
A critical alert has been detected via Nessus to detect Vulnerabilities. Please investigate.
Include
Link to Alert
Link to Results
Cancel
Save



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

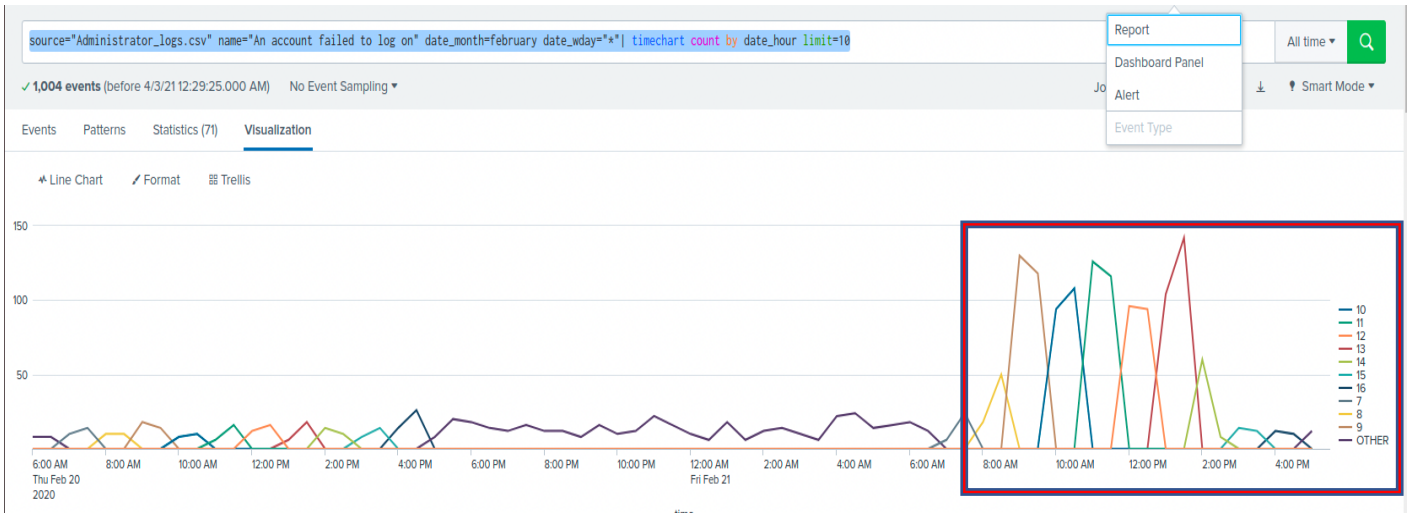
Step 3: Drawing the (base)line

Background: A Vandaly server is also experiencing brute force attacks into 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.

- **If you look at the diagram below and the diagram provided for #3. The attacks occurred on Feb 20th and 21st (Thursday and Friday). The heaviest attack occurred on Friday during 9am – 1pm. Provided directly below as well.**

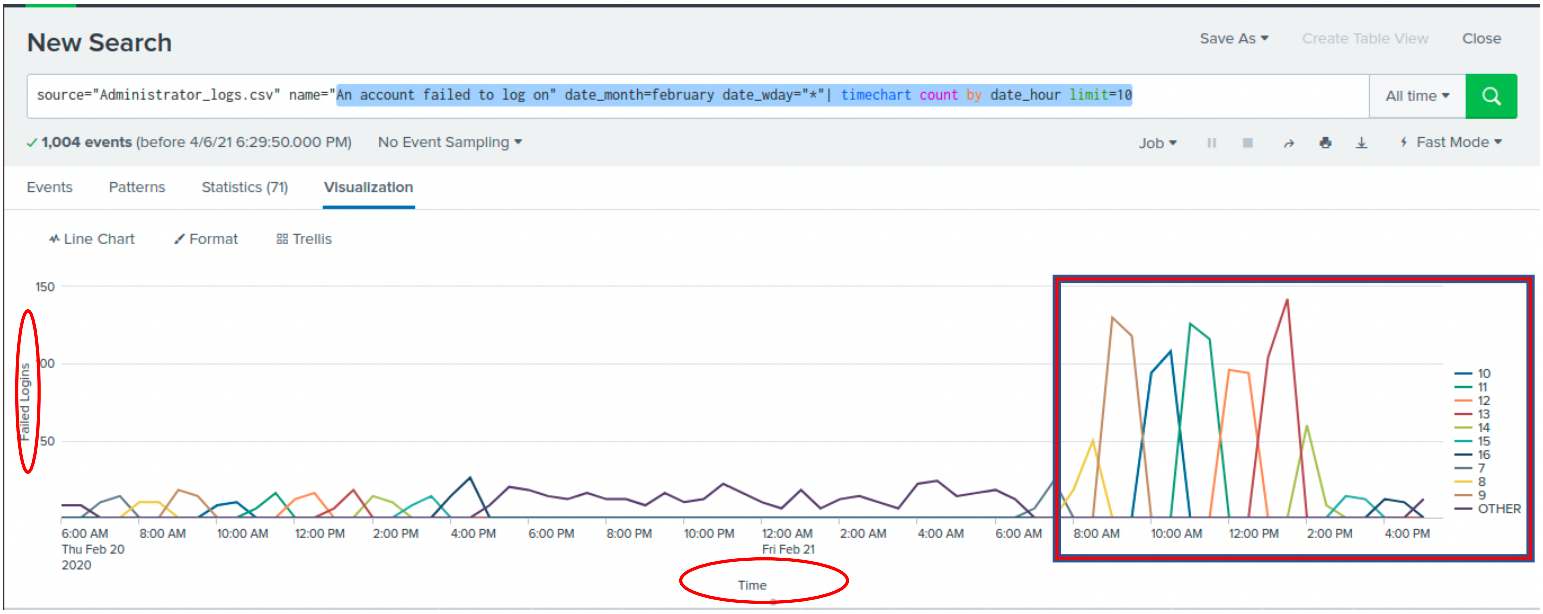


This diagram confirms the number of attempts per hour from 9am – 1pm.

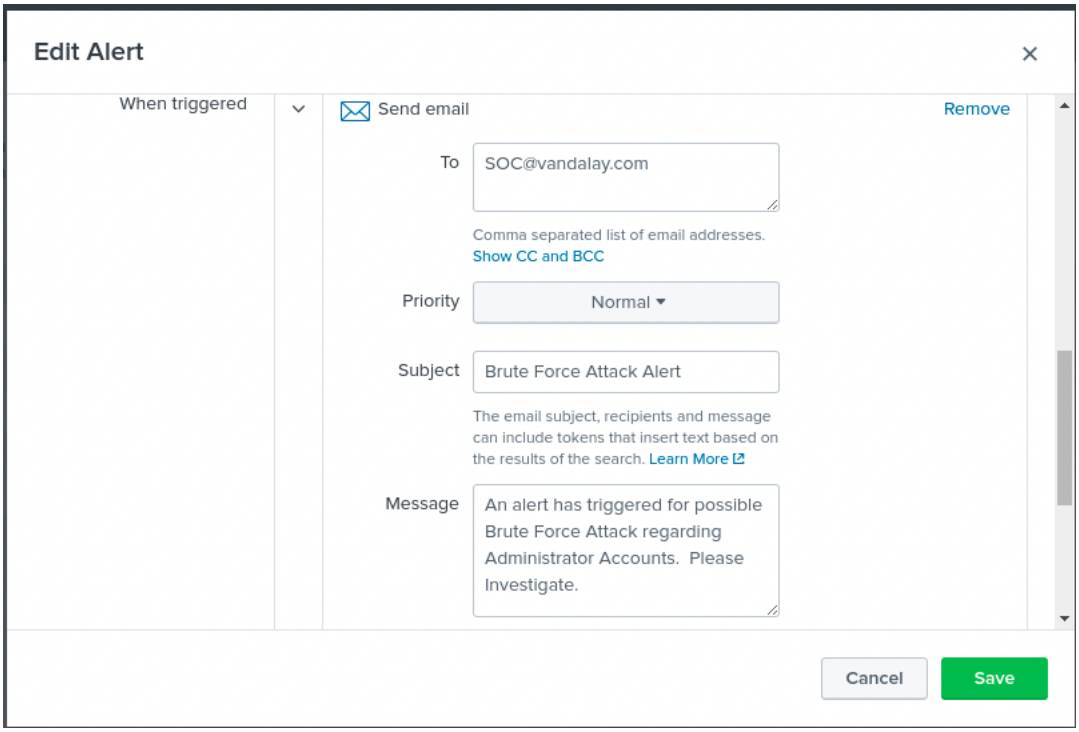
3. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.

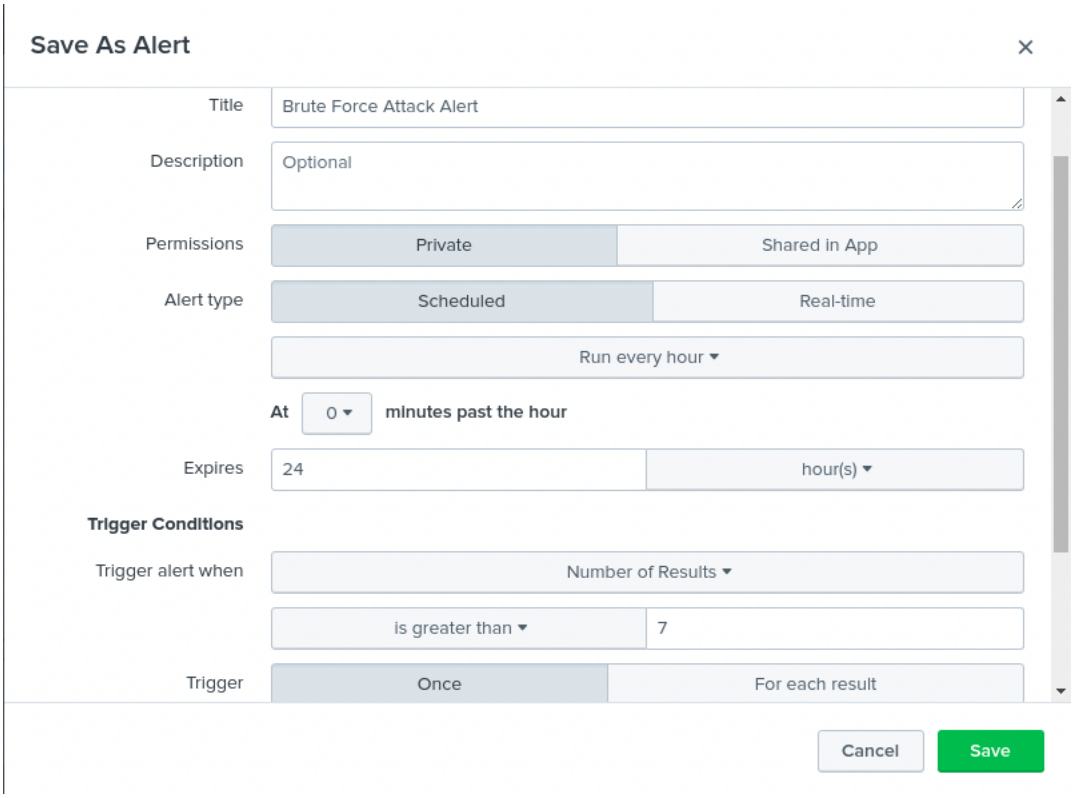
    - Administrator Accounts should never experience lockouts or failed logins; however, sometimes admins could possibly forget their passwords. I would create two alerts due to the situation:
        1. **A Warning Level of over 7 per the baseline diagram below**
        2. **Next Alert Level would be over 20**

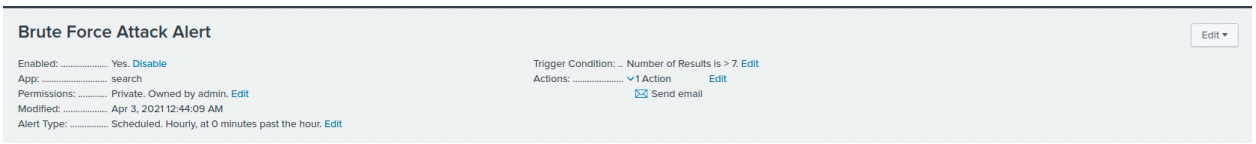
        we



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







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.
