Vandalay Industries Monitoring Activity Instructions

Step 1: The Need for Speed

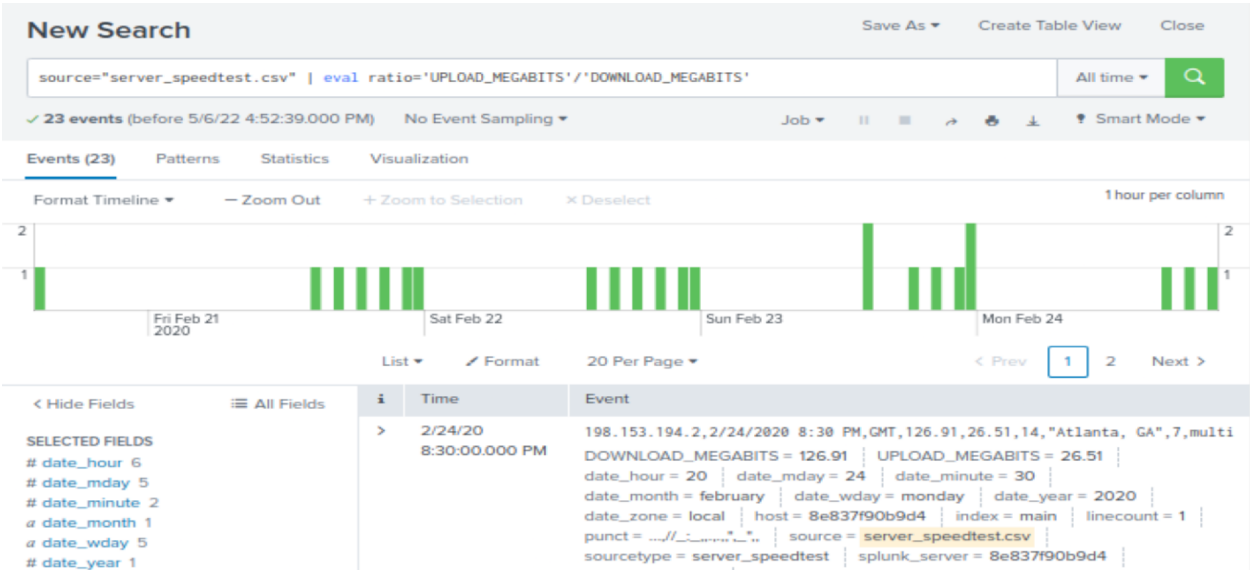
Background: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandaly has been experiencing DDOS attacks against their web servers.

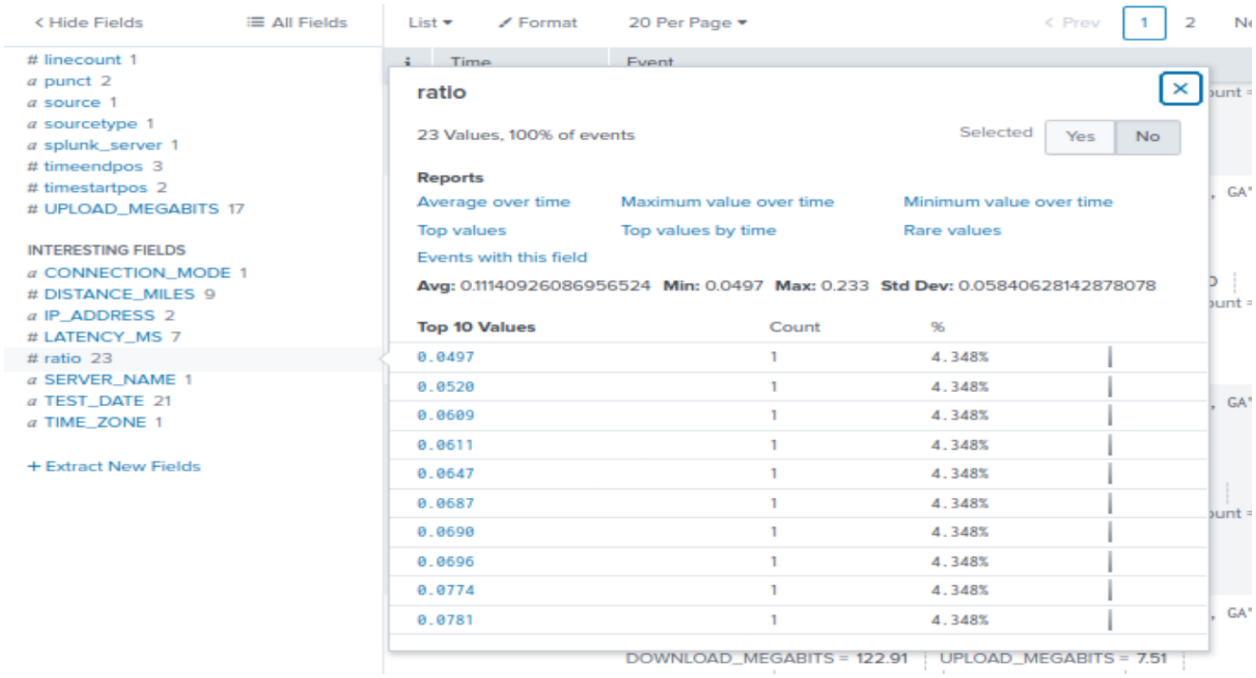
Not only were web servers taken offline by a DDOS attack, but upload and download speed were also significantly impacted after the outage. Your networking team provided results of a network speed run around the time of the latest DDOS attack.

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'

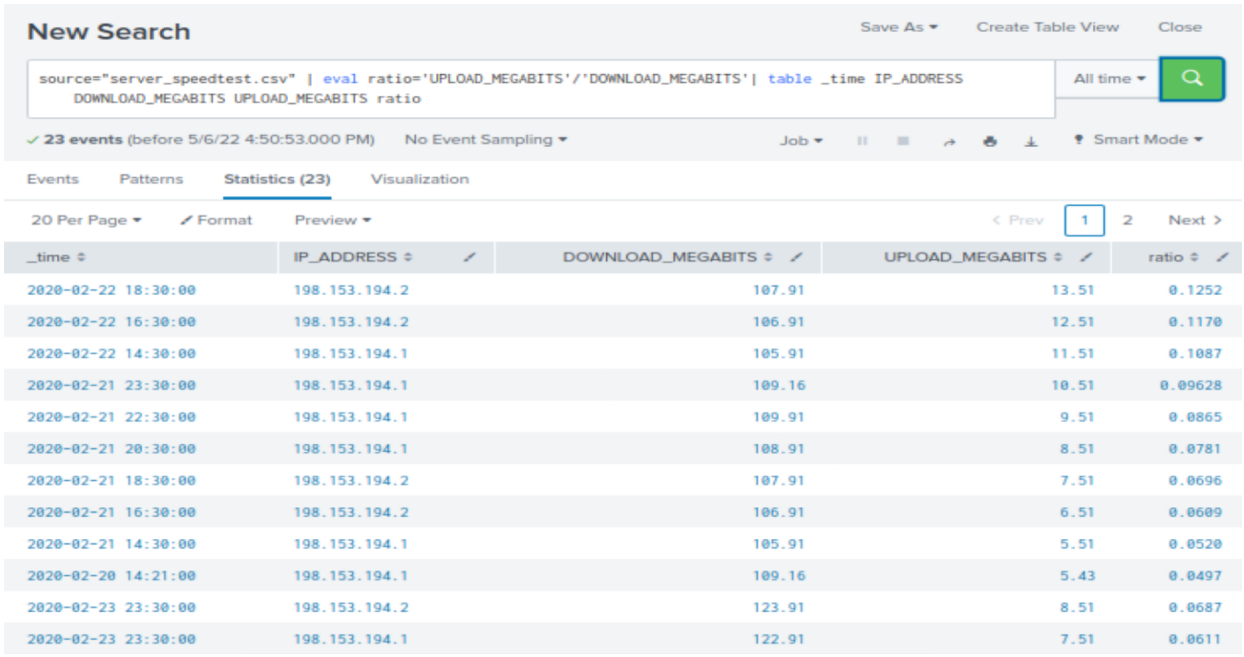
source="server_speedtest.csv" | eval ratio='UPLOAD_MEGABITS'/'DOWNLOAD_MEGABITS'





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='UPLOAD_MEGABITS'/'DOWNLOAD_MEGABITS'| table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio



_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611

5. Answer the following questions:

    - Based on the report created, what is the approximate date and time of the attack?
        1. The report's results show that the time of the attack was on Feb 22nd, 2020 at 11:30 PM.
    - How long did it take your systems to recover?
        2. The system started recovering at 2:30 PM on Feb 23nd, 2020

50 Per Page ▾ Format Preview ▾

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 14:30:00	198.153.194.1	2	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-22 23:30:00	198.153.194.2	1	109.16	9.51	0.0871

Step 2: Are We Vulnerable?

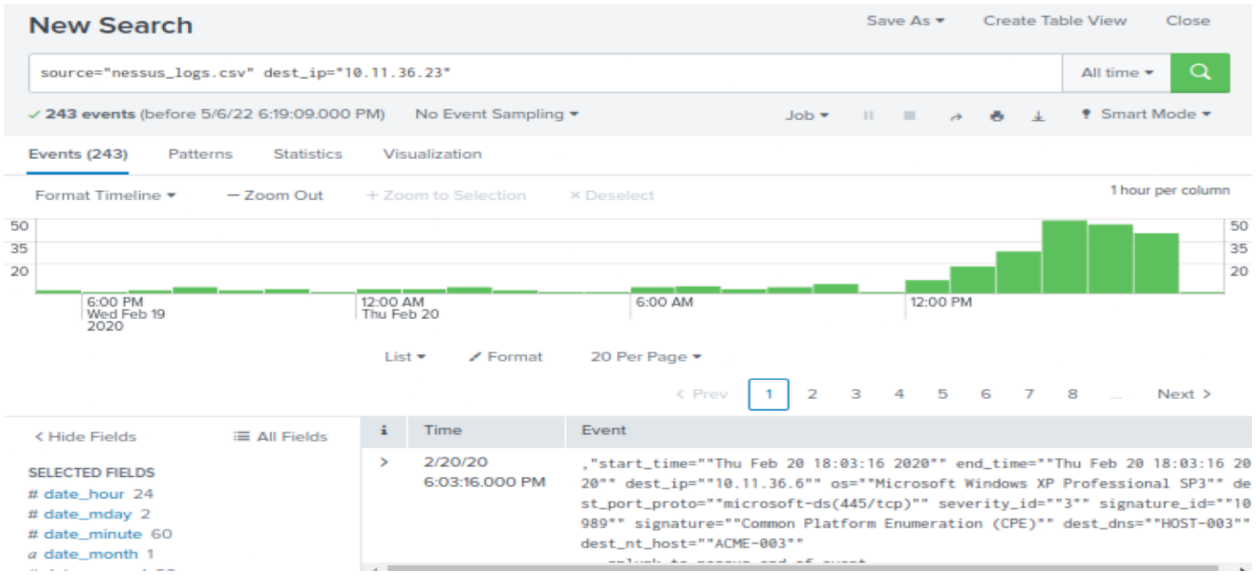
Background: Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

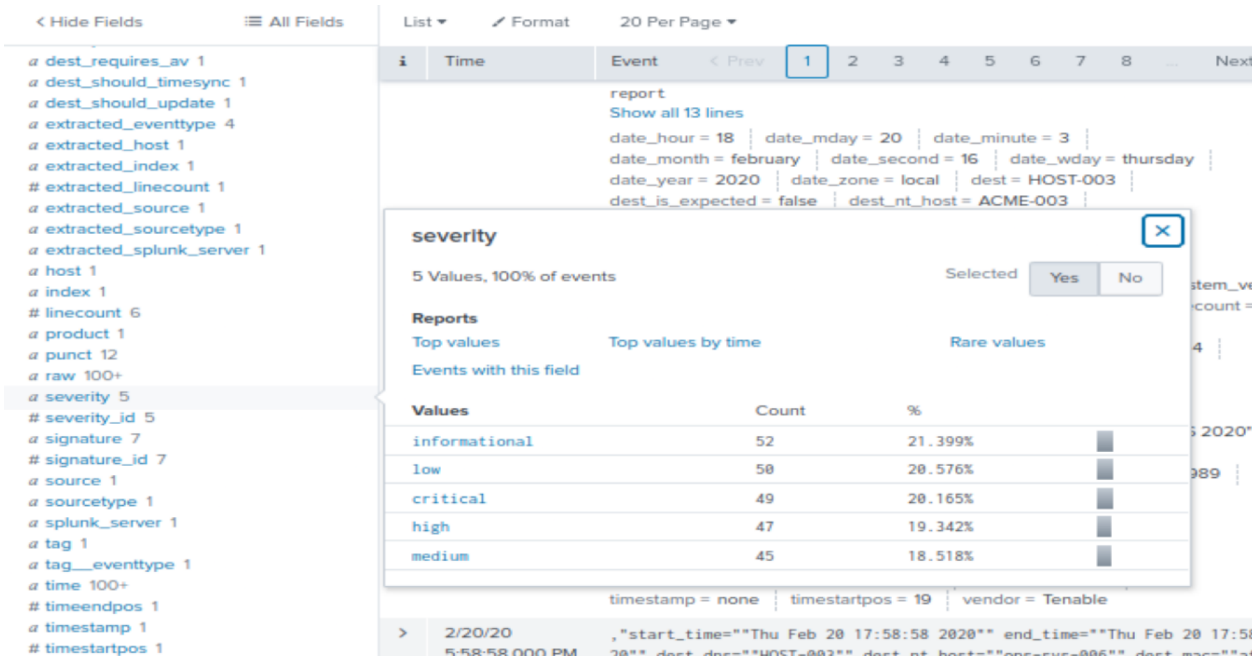
- For more information on Nessus, read the following link: https://www.tenable.com/products/nessus

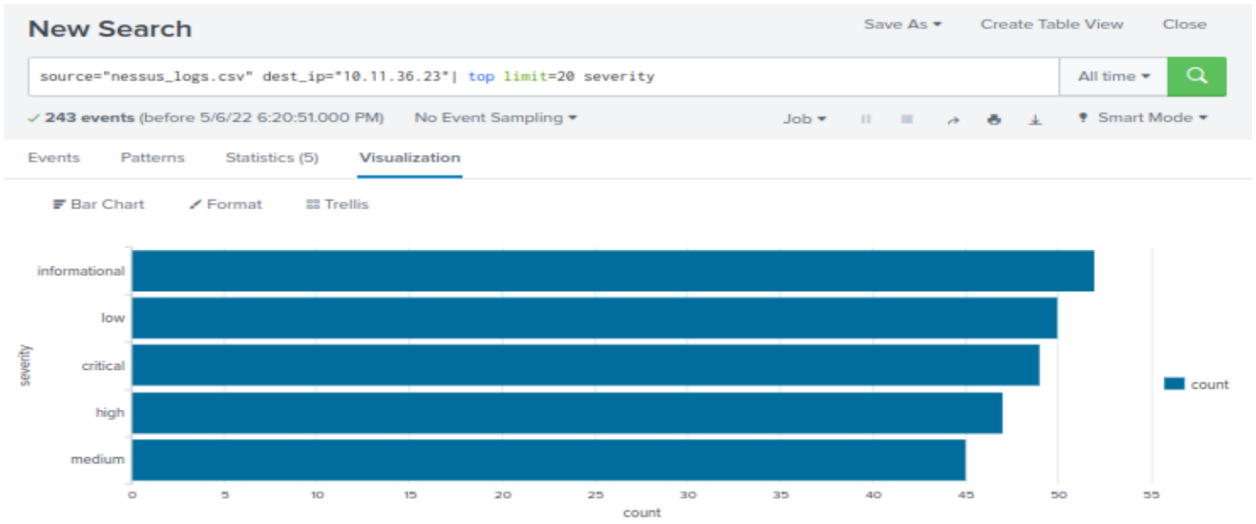
Task: Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

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.

source="nessus_logs.csv" dest_ip="10.11.36.23"

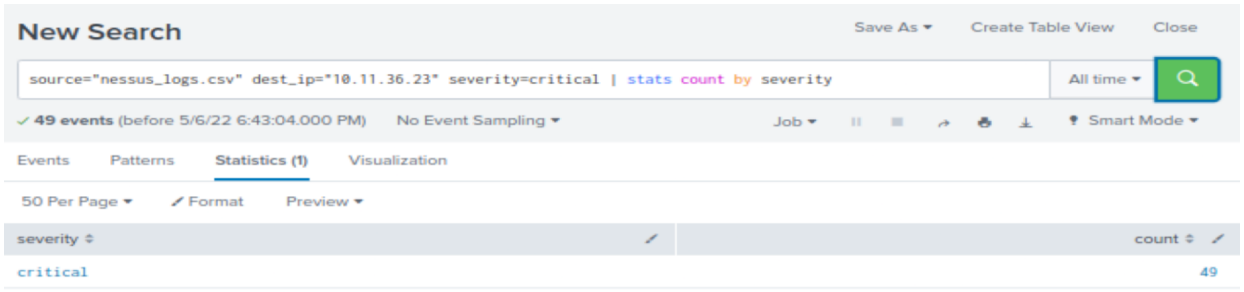


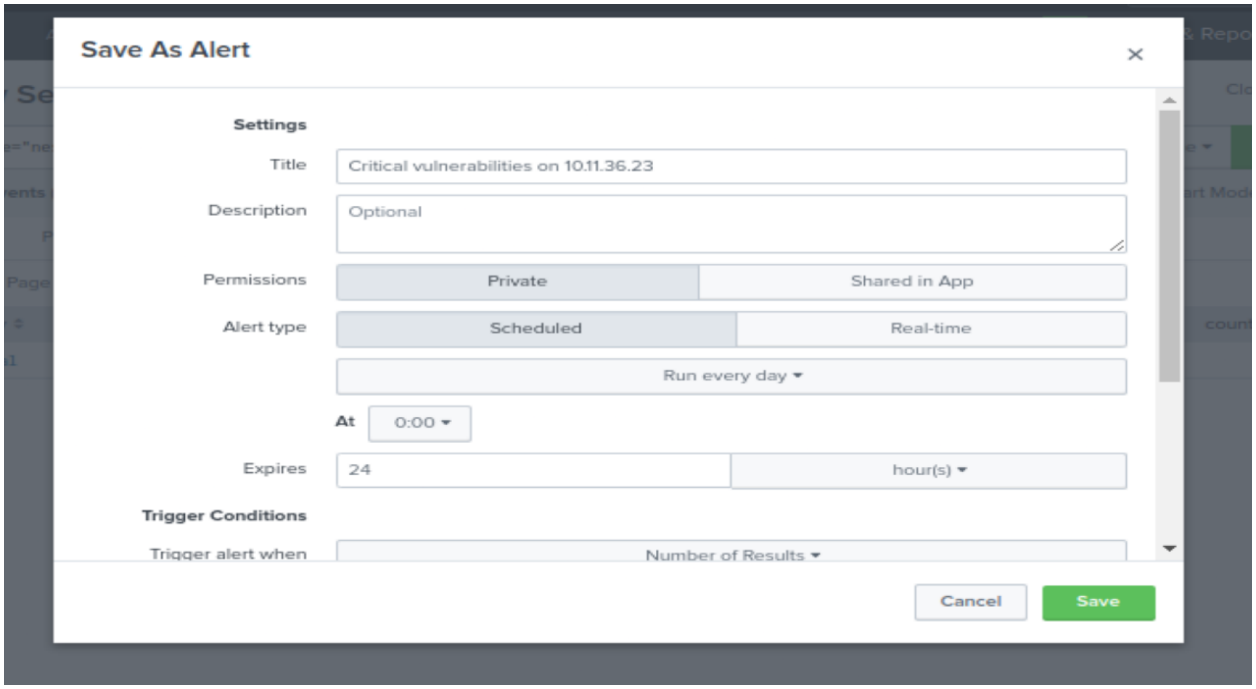


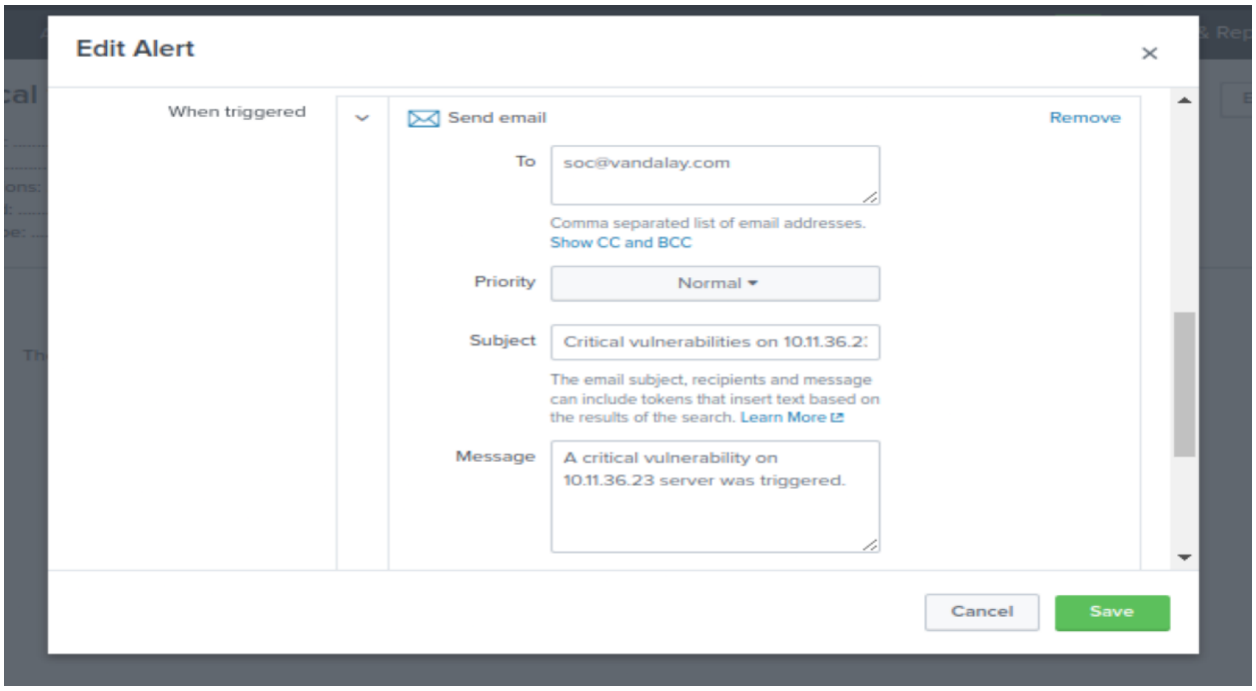


3. Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to soc@vandalay.com.

source="nessus_logs.csv" dest_ip="10.11.36.23" severity=critical | stats count by severity


New Search
Save As
Create Table View
Close
source="nessus_logs.csv" dest_ip="10.11.36.23" severity=critical | stats count by severity
All time
49 events (before 5/6/22 6:43:04.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (1)
Visualization
50 Per Page
Format
Preview
severity
count
critical
49


Save As Alert
Settings
Title
Critical vulnerabilities on 10.11.36.23
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every day
At
0:00
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
Cancel
Save



Step 3: Drawing the (base)line

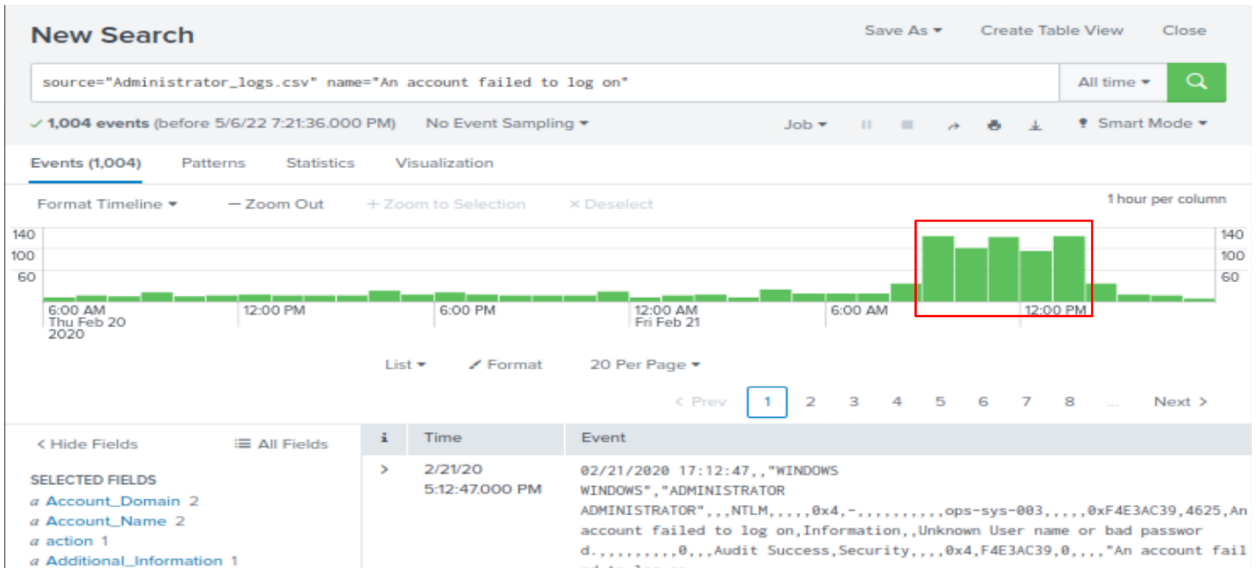
Background: A Vandaly server is also experiencing brute force attacks into their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.

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.

source="Administrator_logs.csv" name="An account failed to log on"

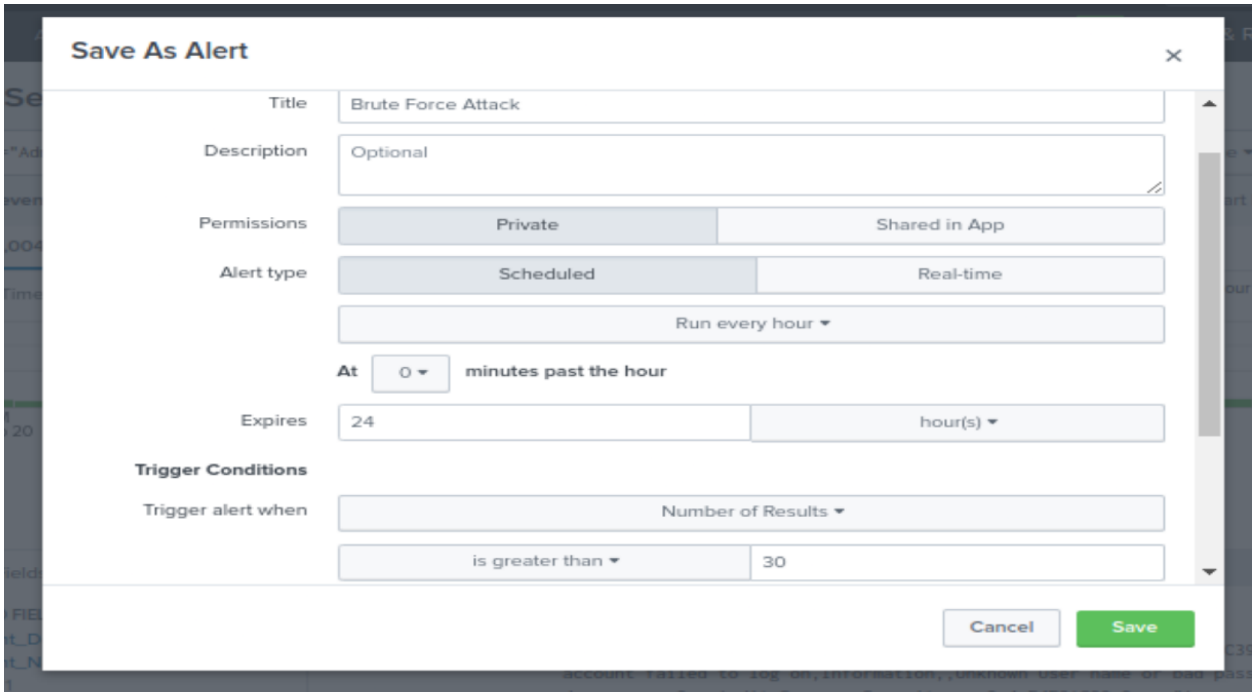
The attack occurred on Feb 21st, 2020 from 9 AM to 1 PM, when the failed login attempts ranged from 95 to 124 logins per hour.

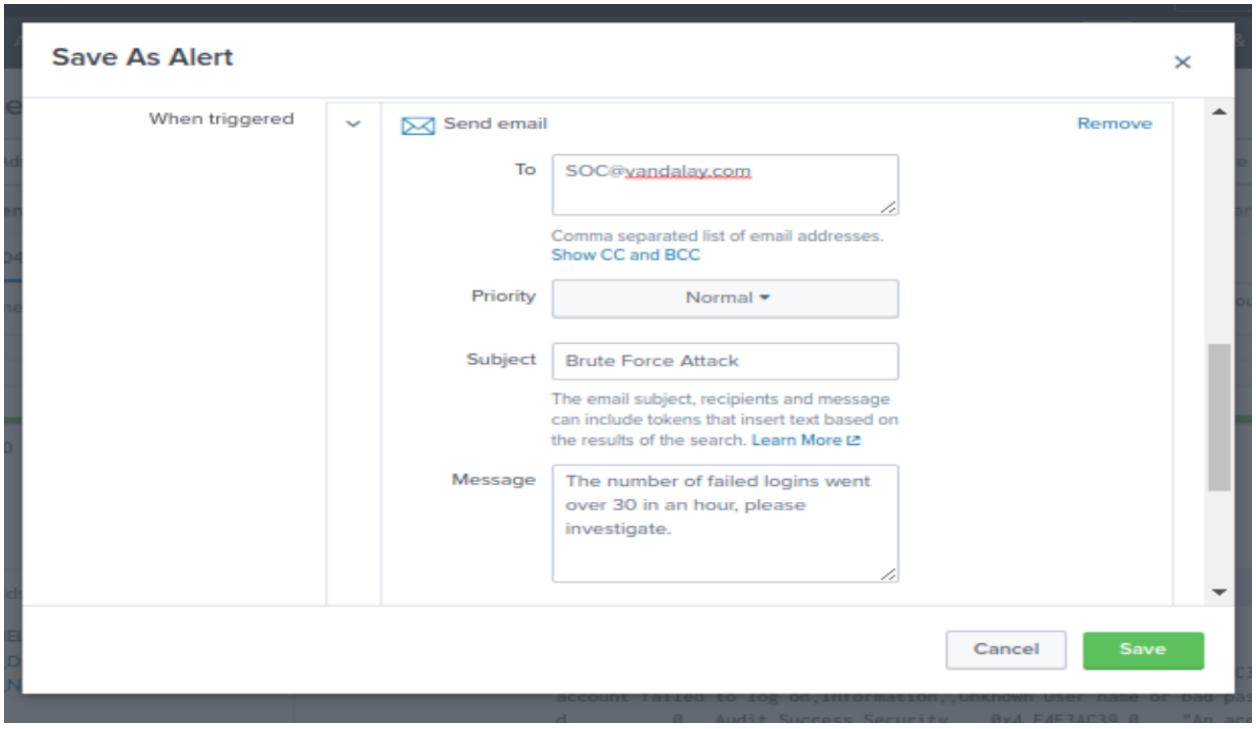


3. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.

Based on past login data the baseline for normal activity ranged from 6 to 20 logins per hour with a threshold for more than 30 failed login attempts.

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


Save As Alert
Title
Brute Force Attack
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every hour
At
0
minutes past the hour
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
30
Cancel
Save


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
Brute Force Attack
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More
Message
The number of failed logins went over 30 in an hour, please investigate.
Cancel
Save

Brute Force Attack

Edit

Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by admin. Edit
Modified: ..... May 6, 2022 7:51:58 PM
Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 30. Edit
Actions: ..... 1 Action Edit
Send email