Unit 19 Homework: Lets go Splunking! Brenda Schecher

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

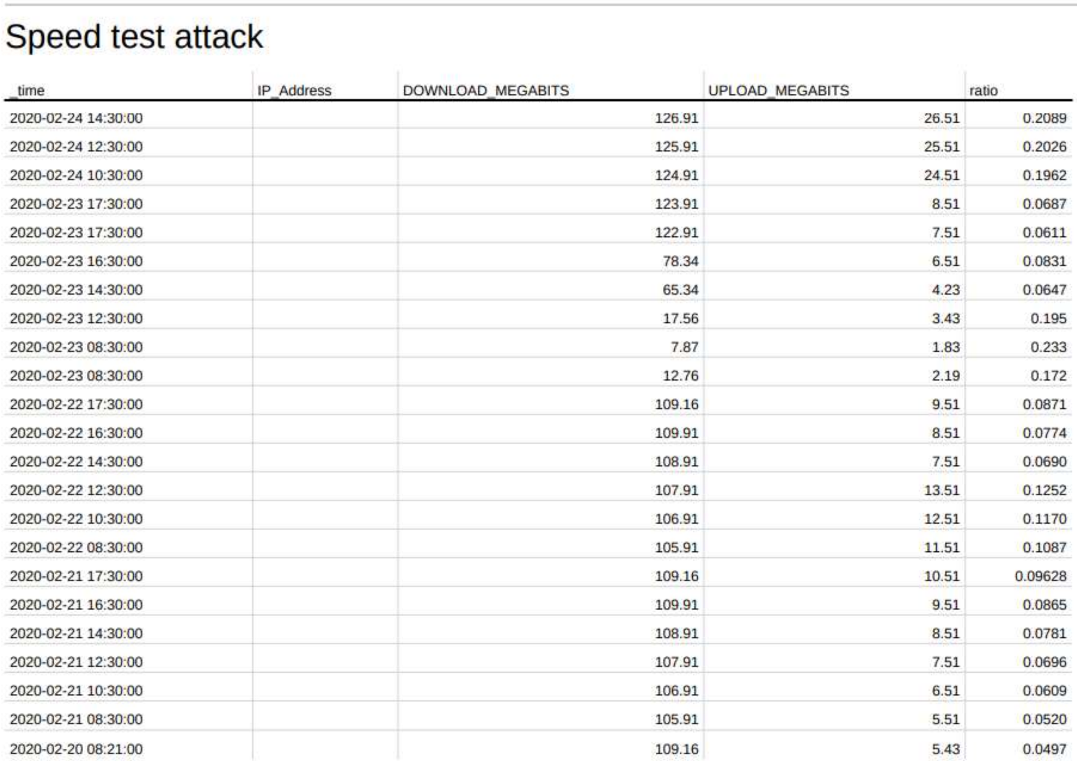
Step 1: The Need for Speed

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.

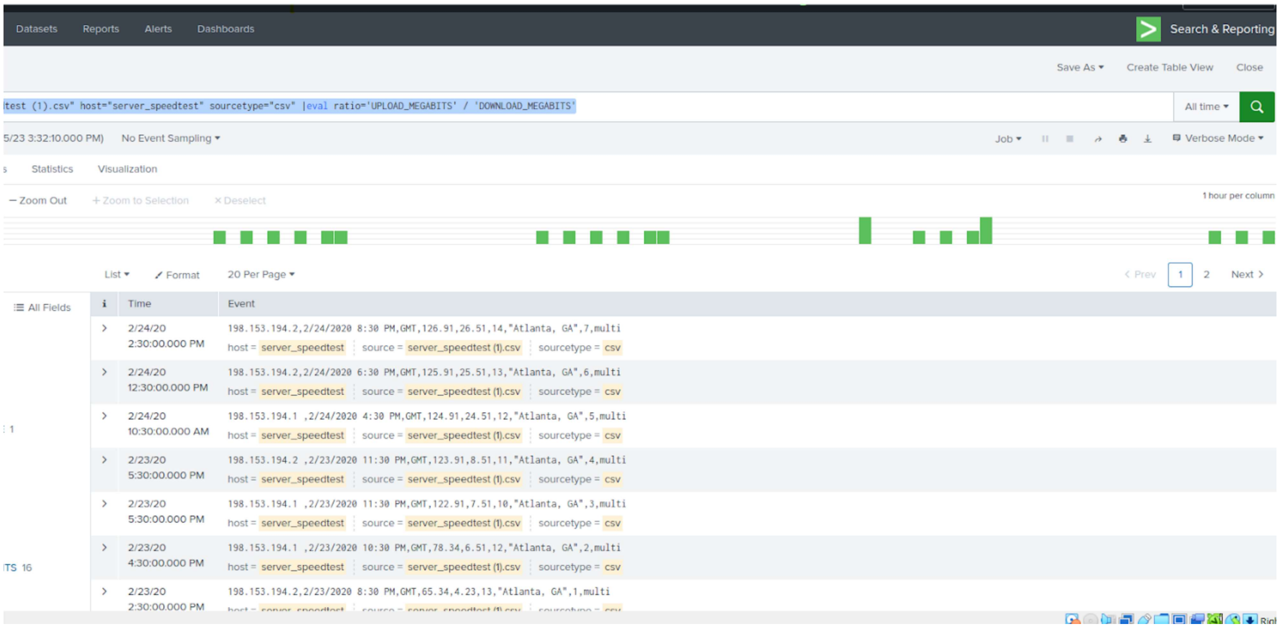
1. Upload the following file of the system speeds around the time of the attack.
    - Speed Test File
2. Using the `eval` command, create a field called `ratio` that shows the ratio between the upload and download speeds.
    - Hint: The format for creating a ratio is: `| eval new_field_name = 'fieldA'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



Speed test attack

_time	IP_Address	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 14:30:00		126.91	26.51	0.2089
2020-02-24 12:30:00		125.91	25.51	0.2026
2020-02-24 10:30:00		124.91	24.51	0.1962
2020-02-23 17:30:00		123.91	8.51	0.0687
2020-02-23 17:30:00		122.91	7.51	0.0611
2020-02-23 16:30:00		78.34	6.51	0.0831
2020-02-23 14:30:00		65.34	4.23	0.0647
2020-02-23 12:30:00		17.56	3.43	0.195
2020-02-23 08:30:00		7.87	1.83	0.233
2020-02-23 08:30:00		12.76	2.19	0.172
2020-02-22 17:30:00		109.16	9.51	0.0871
2020-02-22 16:30:00		109.91	8.51	0.0774
2020-02-22 14:30:00		108.91	7.51	0.0690
2020-02-22 12:30:00		107.91	13.51	0.1252
2020-02-22 10:30:00		106.91	12.51	0.1170
2020-02-22 08:30:00		105.91	11.51	0.1087
2020-02-21 17:30:00		109.16	10.51	0.09628
2020-02-21 16:30:00		109.91	9.51	0.0865
2020-02-21 14:30:00		108.91	8.51	0.0781
2020-02-21 12:30:00		107.91	7.51	0.0696
2020-02-21 10:30:00		106.91	6.51	0.0609
2020-02-21 08:30:00		105.91	5.51	0.0520
2020-02-20 08:21:00		109.16	5.43	0.0497

3.



```
test (1).csv" host="server_speedtest" sourcetype="csv" |eval ratio='UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS'
```

5/23 3:32:10.000 PM)   No Event Sampling ▾

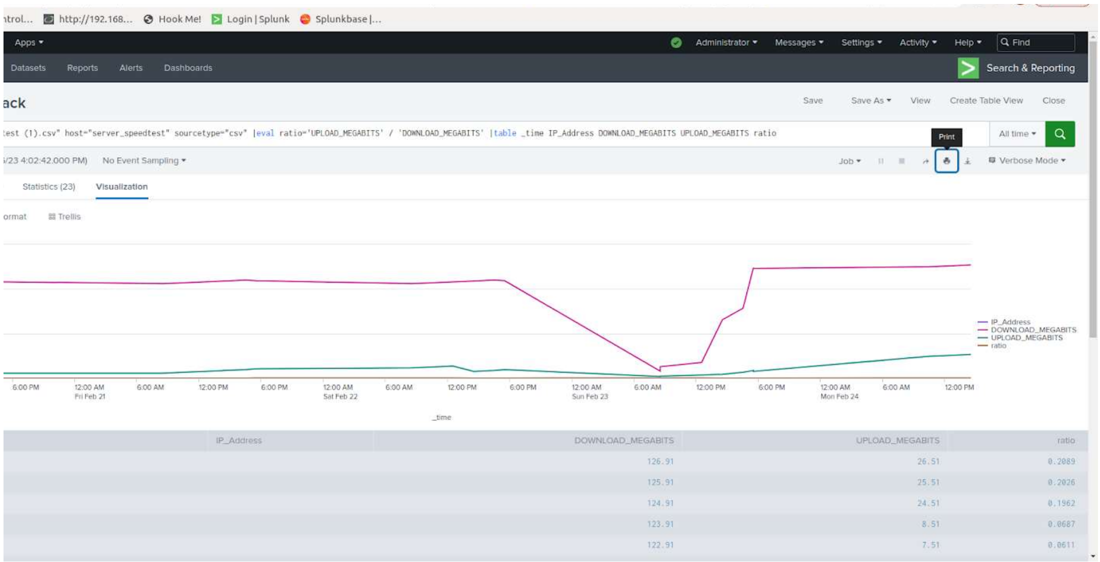
i	Time	Event
›	2/24/20 2:30:00.000 PM	198.153.194.2,2/24/2020 8:30 PM,GMT,126.91,26.51,14,"Atlanta, GA",7,multi host = server_speedtest source = server_speedtest (1).csv sourcetype = csv
›	2/24/20 12:30:00.000 PM	198.153.194.2,2/24/2020 6:30 PM,GMT,125.91,25.51,13,"Atlanta, GA",6,multi host = server_speedtest source = server_speedtest (1).csv sourcetype = csv
›	2/24/20 10:30:00.000 AM	198.153.194.1 ,2/24/2020 4:30 PM,GMT,124.91,24.51,12,"Atlanta, GA",5,multi host = server_speedtest source = server_speedtest (1).csv sourcetype = csv
›	2/23/20 5:30:00.000 PM	198.153.194.2 ,2/23/2020 11:30 PM,GMT,123.91,8.51,11,"Atlanta, GA",4,multi host = server_speedtest source = server_speedtest (1).csv sourcetype = csv
›	2/23/20 5:30:00.000 PM	198.153.194.1 ,2/23/2020 11:30 PM,GMT,122.91,7.51,10,"Atlanta, GA",3,multi host = server_speedtest source = server_speedtest (1).csv sourcetype = csv
›	2/23/20 4:30:00.000 PM	198.153.194.1 ,2/23/2020 10:30 PM,GMT,78.34,6.51,12,"Atlanta, GA",2,multi host = server_speedtest source = server_speedtest (1).csv sourcetype = csv
›	2/23/20 2:30:00.000 PM	198.153.194.2,2/23/2020 8:30 PM,GMT,65.34,4.23,13,"Atlanta, GA",1,multi

4. 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`

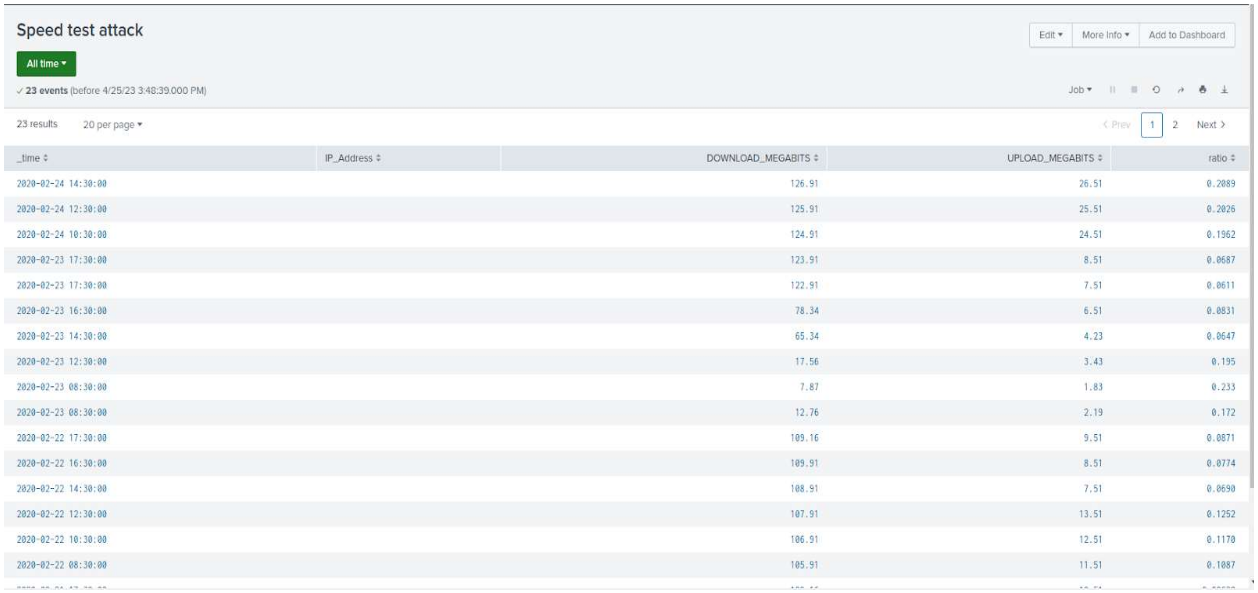
5. Hint: Use the following format when for the `table` command: `| table fieldA fieldB fieldC`
6. `Answer-`
7. `source="server_speedtest (1).csv" host="server_speedtest" sourcetype="csv" |eval ratio='UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' |table _time IP_Address DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio`

    `Create report (see screen shot)`



```
test (1).csv" host="server_speedtest" sourcetype="csv" |eval ratio='UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' |table _time IP_Address DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio
```

IP_Address	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
	126.91	26.51	0.2089
	125.91	25.51	0.2026
	124.91	24.51	0.1962
	123.91	8.51	0.0687
	122.91	7.51	0.0611



Speed test attack

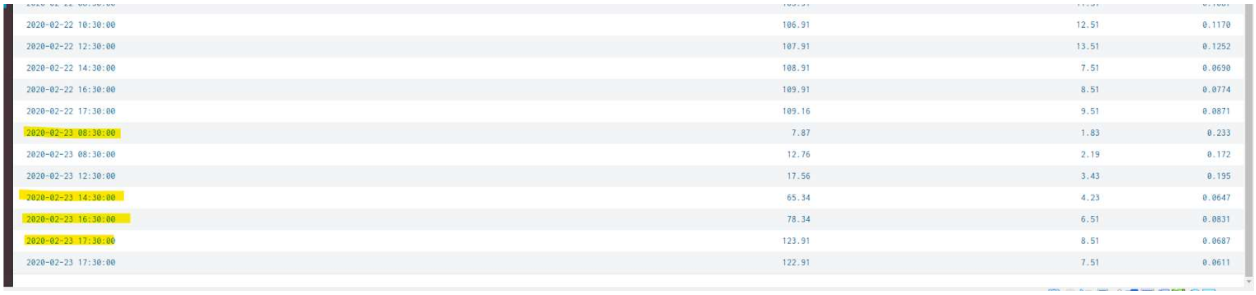
✓ 23 events (before 4/25/23 3:48:39.000 PM)

23 results

_time	IP_Address	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 14:30:00		126.91	26.51	0.2089
2020-02-24 12:30:00		125.91	25.51	0.2026
2020-02-24 10:30:00		124.91	24.51	0.1962
2020-02-23 17:30:00		123.91	8.51	0.0687
2020-02-23 17:30:00		122.91	7.51	0.0611
2020-02-23 16:30:00		78.34	6.51	0.0831
2020-02-23 14:30:00		65.34	4.23	0.0647
2020-02-23 12:30:00		17.56	3.43	0.195
2020-02-23 08:30:00		7.87	1.83	0.233
2020-02-23 08:30:00		12.76	2.19	0.172
2020-02-22 17:30:00		109.16	9.51	0.0871
2020-02-22 16:30:00		109.91	8.51	0.0774
2020-02-22 14:30:00		108.91	7.51	0.0690
2020-02-22 12:30:00		107.91	13.51	0.1252
2020-02-22 10:30:00		106.91	12.51	0.1170
2020-02-22 08:30:00		105.91	11.51	0.1087

8. Answer the following questions:

   - Based on the report created, what is the approximate date and time of the attack? started at 2/23/2020 8:30am-4:30pm. My documentation shows the recovery started at 5:30pm at 123.91.
   - How long did it take your systems to recover? roughly 8-9 hours



2020-02-22 10:30:00	106.91	12.51	0.1170
2020-02-22 12:30:00	107.91	13.51	0.1252
2020-02-22 14:30:00	108.91	7.51	0.0690
2020-02-22 16:30:00	109.91	8.51	0.0774
2020-02-22 17:30:00	109.16	9.51	0.0871
2020-02-23 08:30:00	7.87	1.83	0.233
2020-02-23 08:30:00	12.76	2.19	0.172
2020-02-23 12:30:00	17.56	3.43	0.195
2020-02-23 14:30:00	65.34	4.23	0.0647
2020-02-23 16:30:00	78.34	6.51	0.0831
2020-02-23 17:30:00	123.91	8.51	0.0687
2020-02-23 17:30:00	122.91	7.51	0.0611

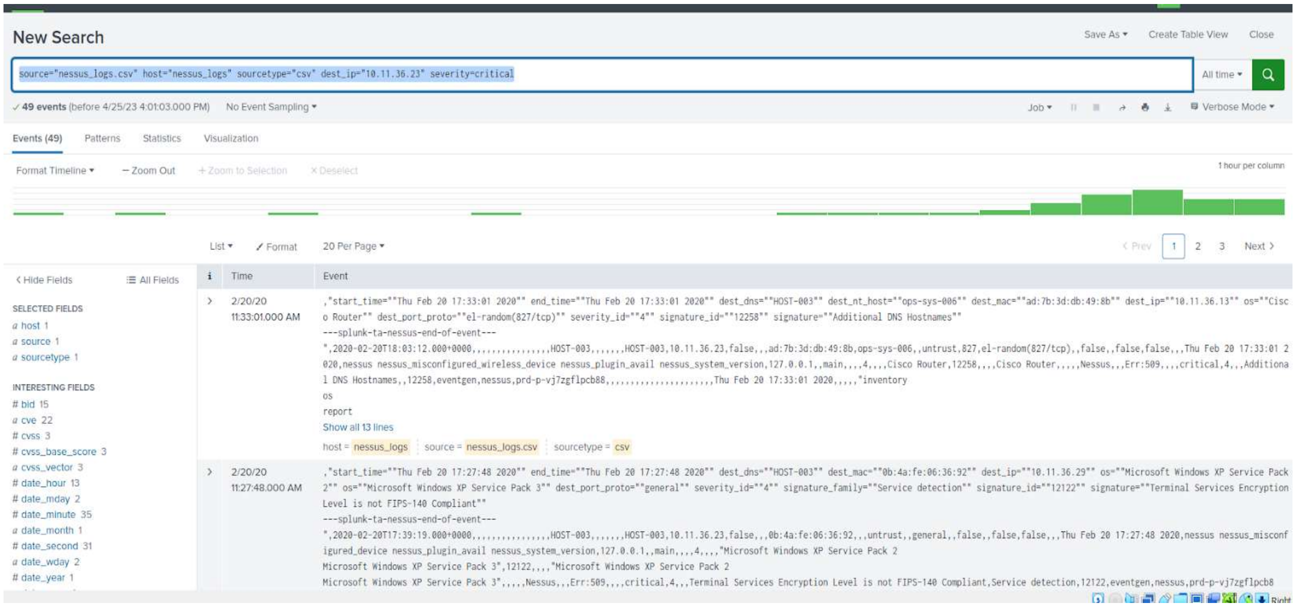
Step 2: Are We Vulnerable?

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. Answer-
4. `source="nessus_logs.csv" host="nessus_logs" sourcetype="csv" dest_ip="10.11.36.23" severity=critical`
5. 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" host="nessus_logs" sourcetype="csv" dest_ip="10.11.36.23" severity=critical
```

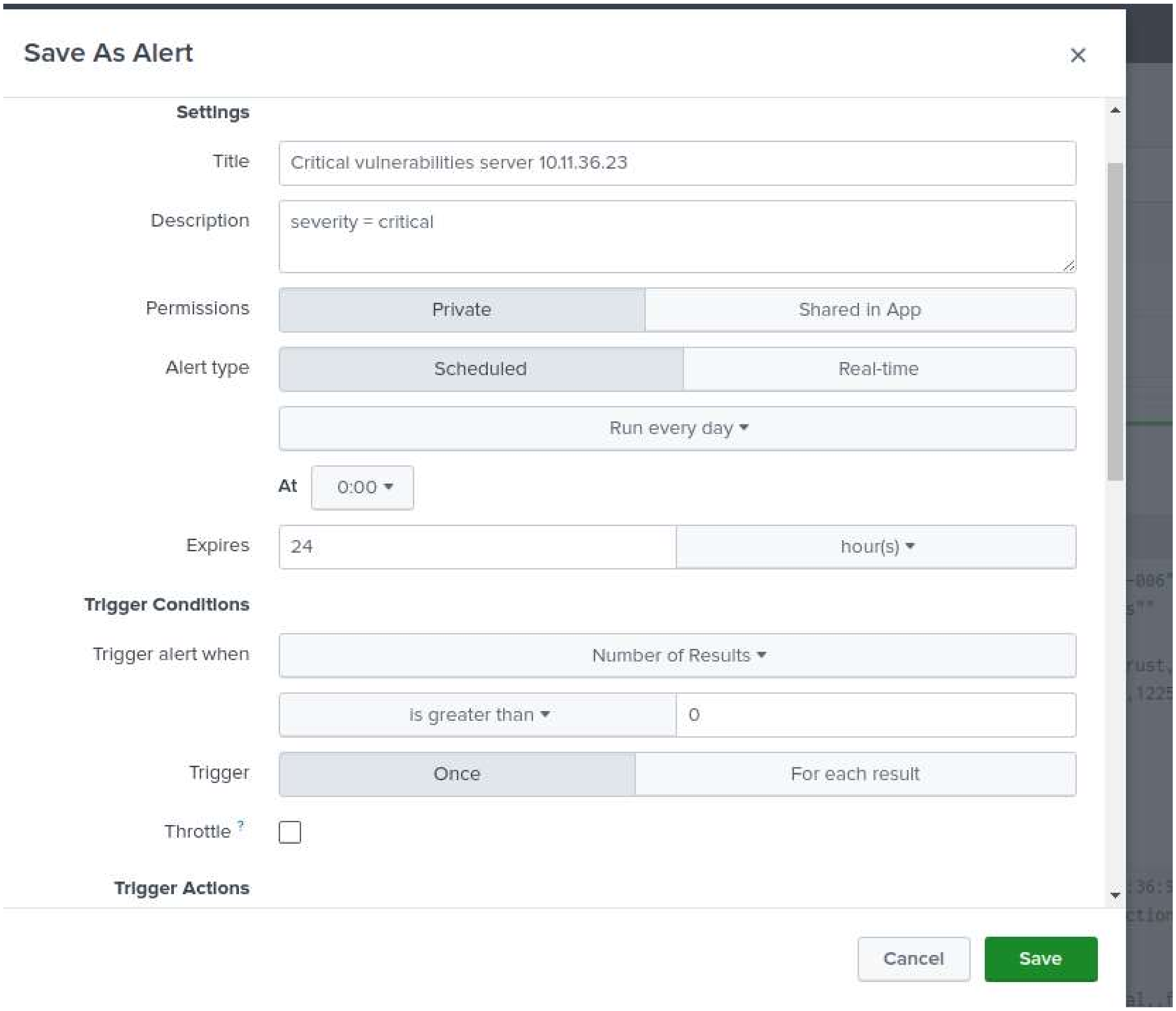
✓ 49 events (before 4/25/23 4:01:03.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bid 15
a cve 22
# cvss 3
# cvss_base_score 3
a cvss_vector 3
# date_hour 13
# date_mday 2
# date_minute 35
a date_month 1
# date_second 31
a date_wday 2
# date_year 1

```
2/20/20 11:33:01.000 AM
,"start_time=""Thu Feb 20 17:33:01 2020"" end_time=""Thu Feb 20 17:33:01 2020"" dest_dns=""HOST-003"" dest_nt_host=""ops-sys-006"" dest_mac=""ad:7b:3d:db:49:8b"" dest_ip=""10.11.36.13"" os=""Cisc
o Router"" dest_port_proto=""el-random(827/tcp)"" severity_id=""4"" signature_id=""12258"" signature=""Additional DNS Hostnames""
---splunk-ta-nessus-end-of-event---
",2020-02-20T18:03:12.000+0000,,,,,,,,,,,,,,,HOST-003,,,,,,HOST-003,10.11.36.23,false,,,ad:7b:3d:db:49:8b,ops-sys-006,,untrust,827,el-random(827/tcp),,false,,false,false,,,Thu Feb 20 17:33:01 2
020,nessus nessus_misconfigured_wireless_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,,Cisco Router,12258,,,,Cisco Router,,,,,Nessus,,,Err:509,,,,critical,4,,,Additiona
l DNS Hostnames,,12258,eventgen,nessus,prd-p-vj7zgflpcb88,,,,,,,,,,,,,,,,,,,,,Thu Feb 20 17:33:01 2020,,,,,"inventory
os
report
Show all 13 lines
host = nessus_logs | source = nessus_logs.csv | sourcetype = csv

2/20/20 11:27:48.000 AM
,"start_time=""Thu Feb 20 17:27:48 2020"" end_time=""Thu Feb 20 17:27:48 2020"" dest_dns=""HOST-003"" dest_mac=""0b:4a:fe:06:36:92"" dest_ip=""10.11.36.29"" os=""Microsoft Windows XP Service Pack
2"" os=""Microsoft Windows XP Service Pack 3"" dest_port_proto=""general"" severity_id=""4"" signature_family=""Service detection"" signature_id=""12122"" signature=""Terminal Services Encryption
Level is not FIPS-140 Compliant""
---splunk-ta-nessus-end-of-event---
",2020-02-20T17:39:19.000+0000,,,,,,,,,,,,,,,HOST-003,,,,,,HOST-003,10.11.36.23,false,,,0b:4a:fe:06:36:92,,,untrust,,general,,false,,false,false,,,Thu Feb 20 17:27:48 2020,nessus nessus_misconf
igured_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,,"Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3",12122,,,,"Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3",,,,,Nessus,,,Err:509,,,,critical,4,,,Terminal Services Encryption Level is not FIPS-140 Compliant,Service detection,12122,eventgen,nessus,prd-p-vj7zgflpcb8
```



Save As Alert

Settings

Title: Critical vulnerabilities server 10.11.36.23

Description: severity = critical

Permissions: [✓ Private] Shared in App

Alert type: [✓ Scheduled] Real-time

Run every day ▾

At 0:00 ▾

Expires: 24 hour(s) ▾

Trigger Conditions

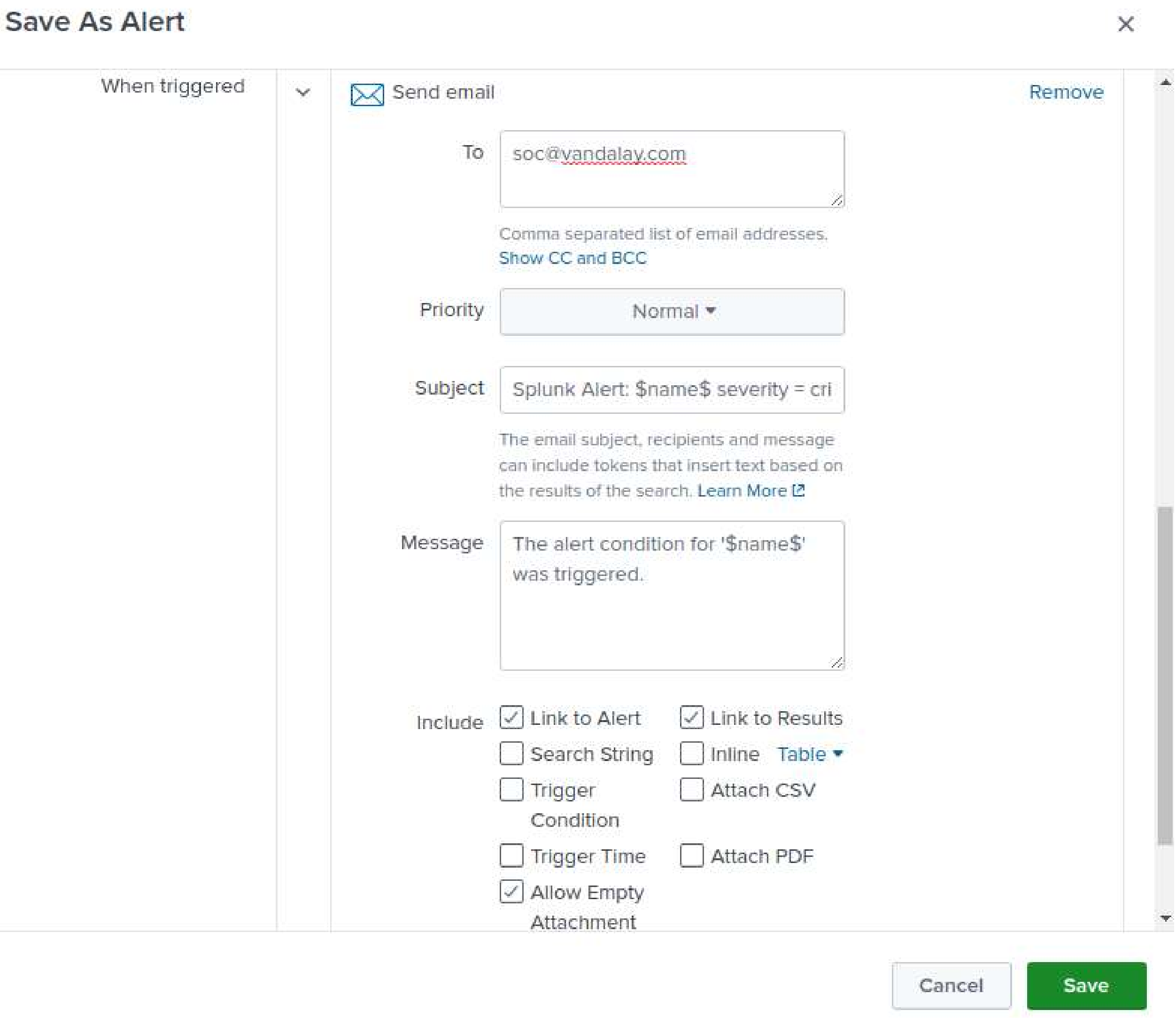
Trigger alert when: Number of Results ▾

is greater than ▾ 0

Trigger: [✓ Once] For each result

Throttle ? □

Trigger Actions



Save As Alert

When triggered

Send email

Remove

To: soc@vandalay.com

Comma separated list of email addresses.
Show CC and BCC

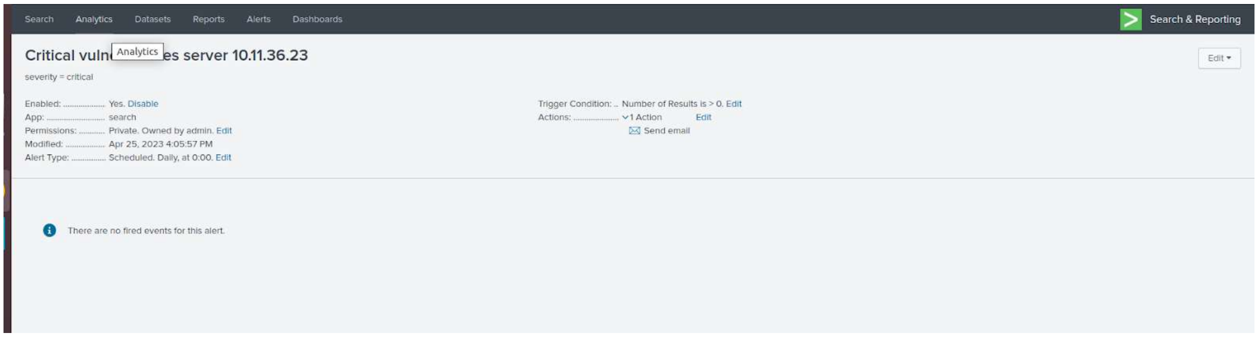
Priority: Normal ▾

Subject: Splunk Alert: $name$ severity = cri

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.

Include:
☑ Link to Alert
☑ Link to Results
☐ Search String
☐ Inline Table ▾
☐ Trigger Condition
☐ Attach CSV
☐ Trigger Time
☐ Attach PDF
☑ Allow Empty Attachment



Critical vuln es server 10.11.36.23

severity = critical

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Apr 25, 2023 4:05:57 PM
Alert Type: Scheduled. Daily, at 0:00. Edit

Trigger Condition: Number of Results is > 0. Edit
Actions: 1 Action Edit
Send email

There are no fired events for this alert.

.

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.

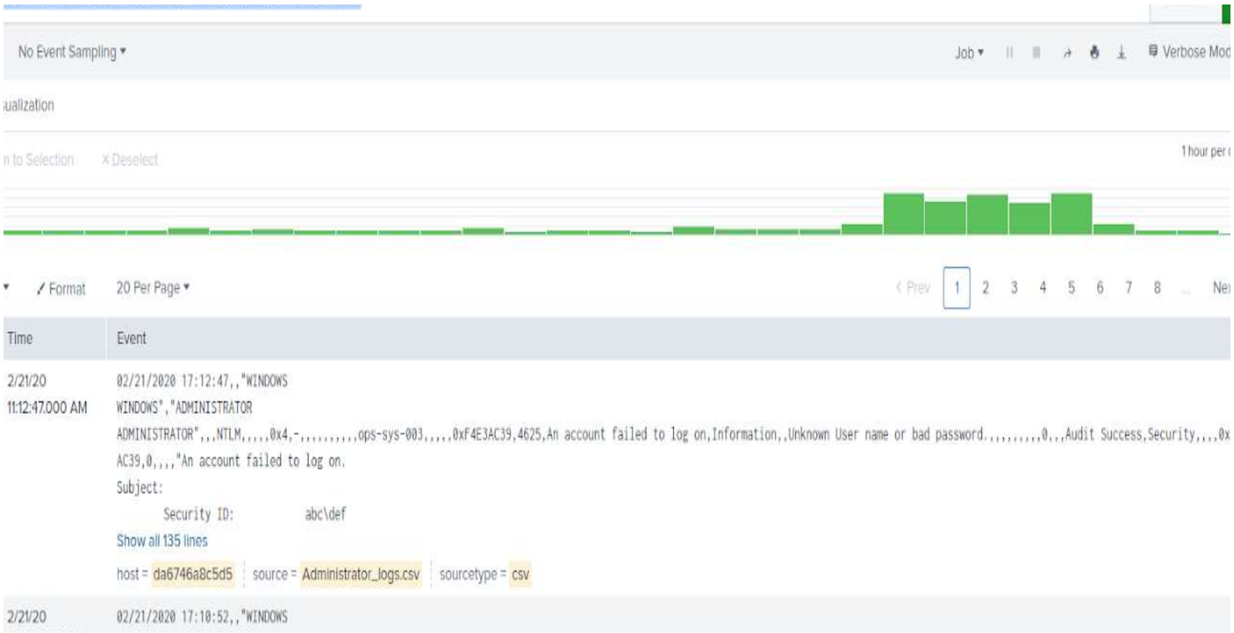
Answer-

- source="Administrator_logs.csv" host="da6746a8c5d5" sourcetype="csv" name="An account failed to log on"
- brute force attack started at 3am Friday FEb 21, 2020 and ended 7am Friday Feb 21,2020. (approx 4 hours)

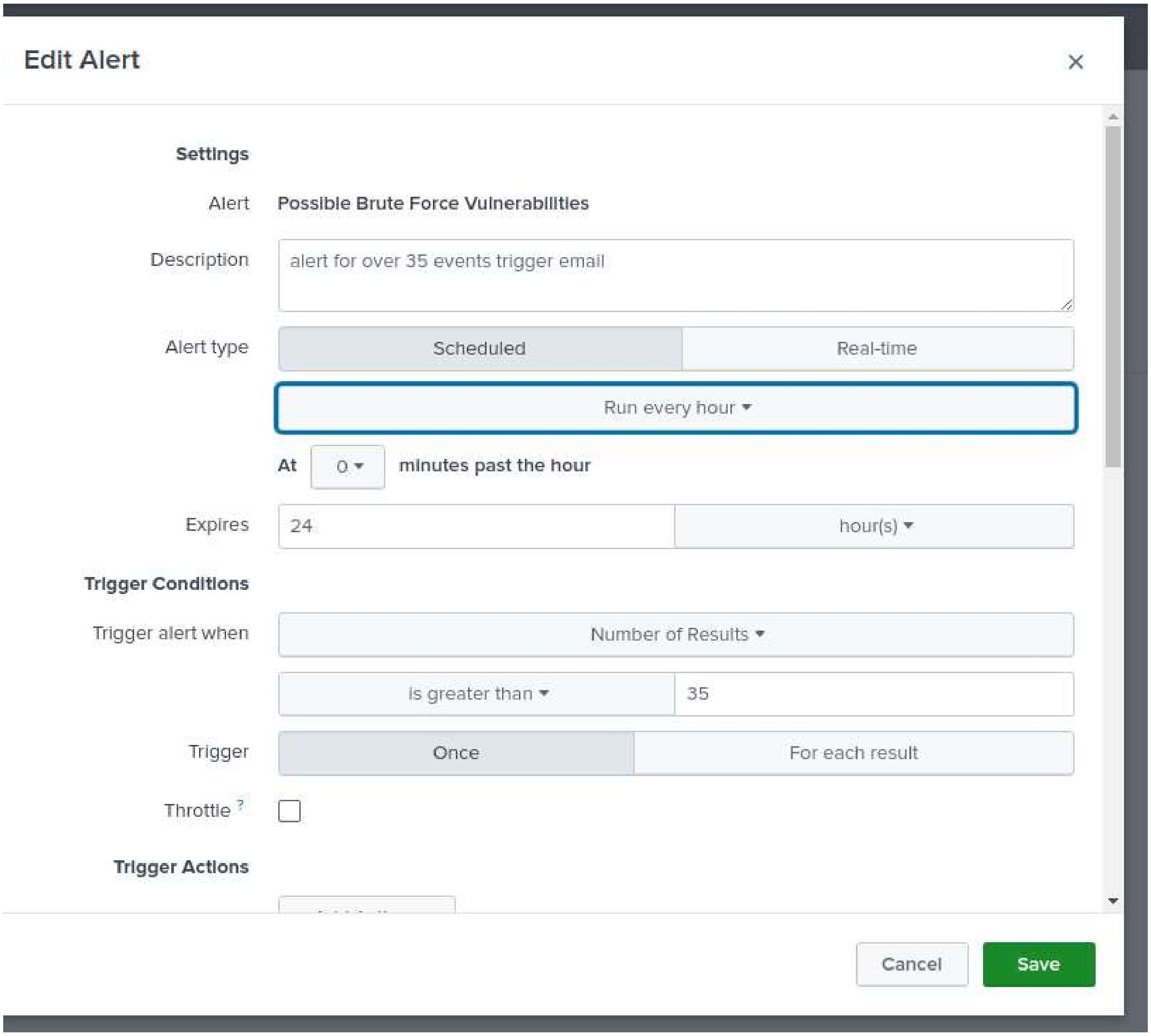
3. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.

   Normal events are approx 10-35 events. My threshold is a count greater than 35.

4.



Time	Event
2/21/20 11:12:47.000 AM	02/21/2020 17:12:47,,"WINDOWS WINDOWS","ADMINISTRATOR ADMINISTRATOR",,,NTLM,,,,,0x4,-,,,,,,,,,,ops-sys-003,,,,,0xF4E3AC39,4625,An account failed to log on,Information,,Unknown User name or bad password.,,,,,,,,,0,,,Audit Success,Security,,,,0x AC39,0,,,,"An account failed to log on. Subject: Security ID: abc\def host = da6746a8c5d5 source = Administrator_logs.csv sourcetype = csv
2/21/20	02/21/2020 17:10:52,,"WINDOWS



Edit Alert

Settings

Alert: **Possible Brute Force Vulnerabilities**

Description: alert for over 35 events trigger email

Alert type: Scheduled | Real-time

Run every hour ▾

At 0 ▾ **minutes past the hour**

Expires: 24 hour(s) ▾

Trigger Conditions

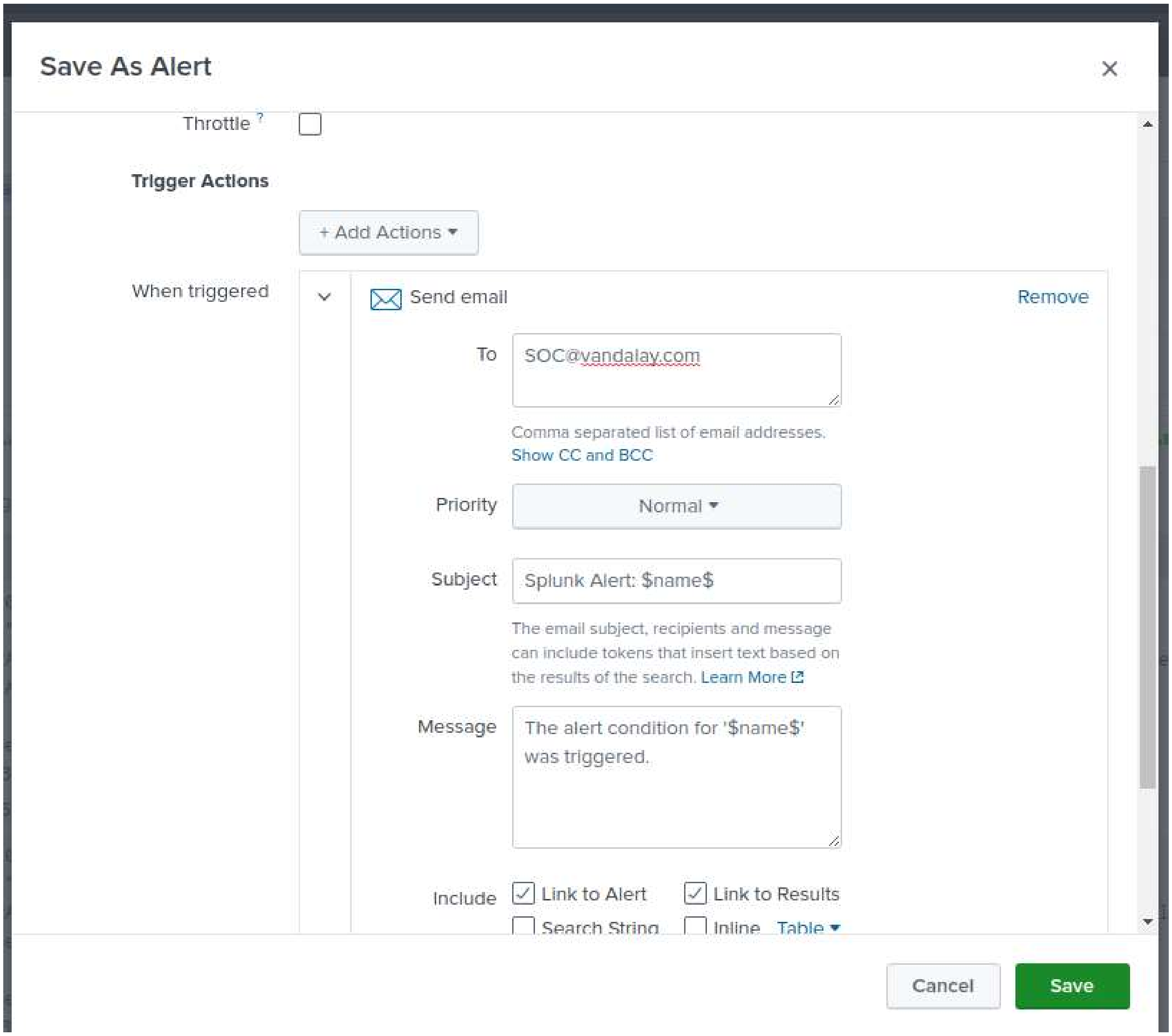
Trigger alert when: Number of Results ▾

is greater than ▾ 35

Trigger: Once | For each result

Throttle ? □

Trigger Actions



Save As Alert

Throttle ? □

Trigger Actions

When triggered

Send email

To: SOC@vandalay.com

Comma separated list of email addresses.
Show CC and BCC

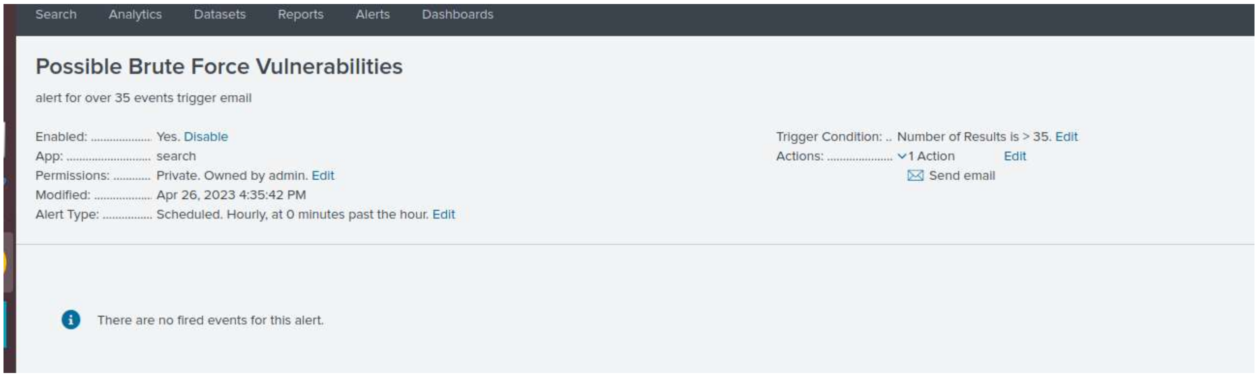
Priority: Normal ▾

Subject: Splunk Alert: $name$

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.

Include ☑ Link to Alert ☑ Link to Results
□ Search String □ Inline Table ▾



Possible Brute Force Vulnerabilities

alert for over 35 events trigger email

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Apr 26, 2023 4:35:42 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 35. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.