Ame-on Budhaka (Amy)

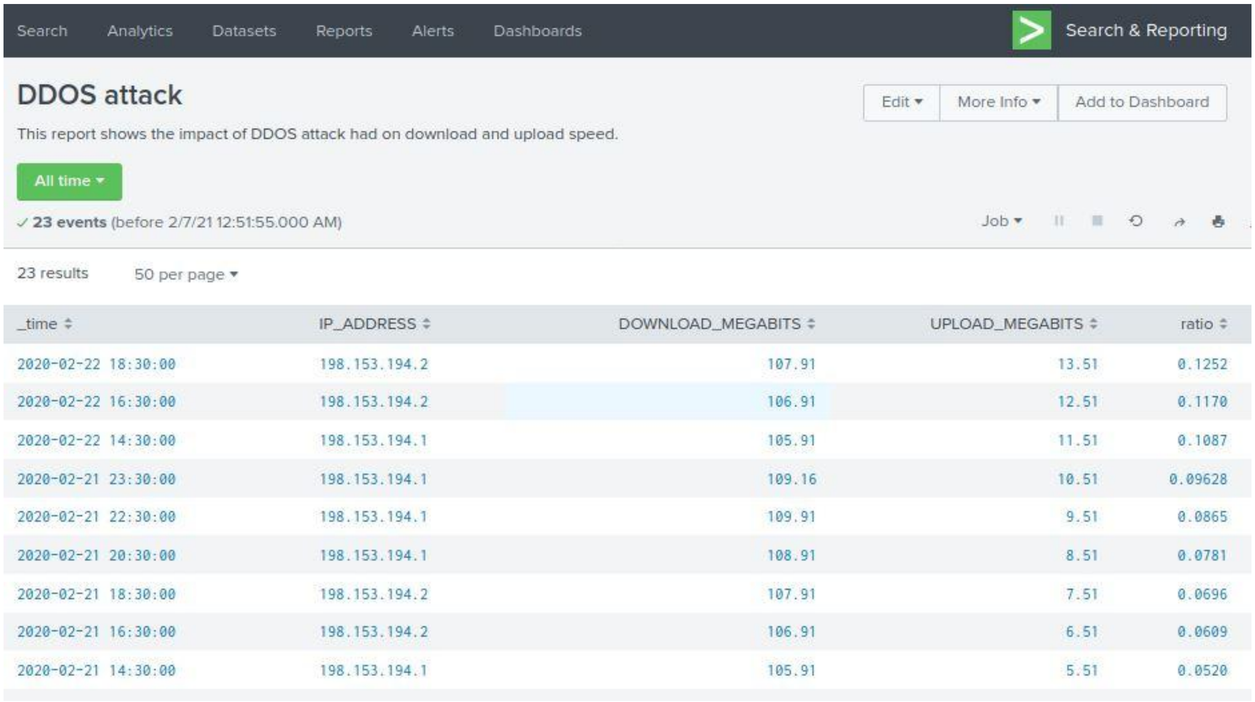
Lets go Splunking!

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.



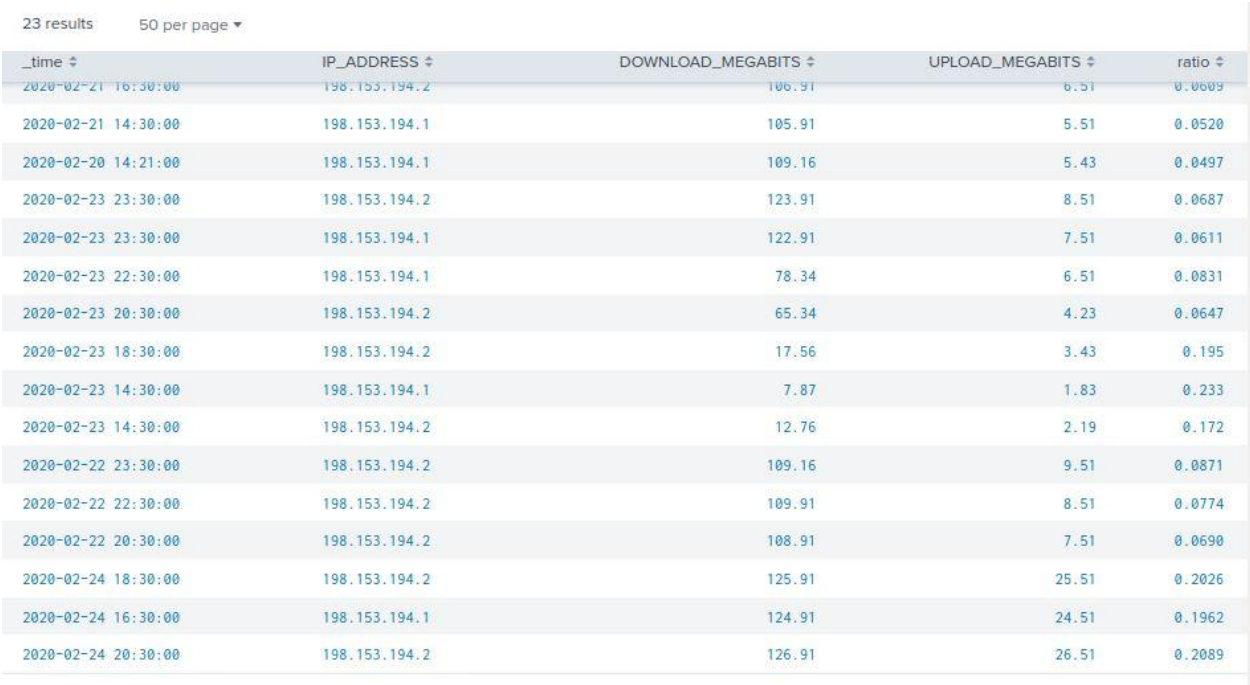
DDOS attack

This report shows the impact of DDOS attack had on download and upload speed.

✓ **23 events** (before 2/7/21 12:51:55.000 AM)

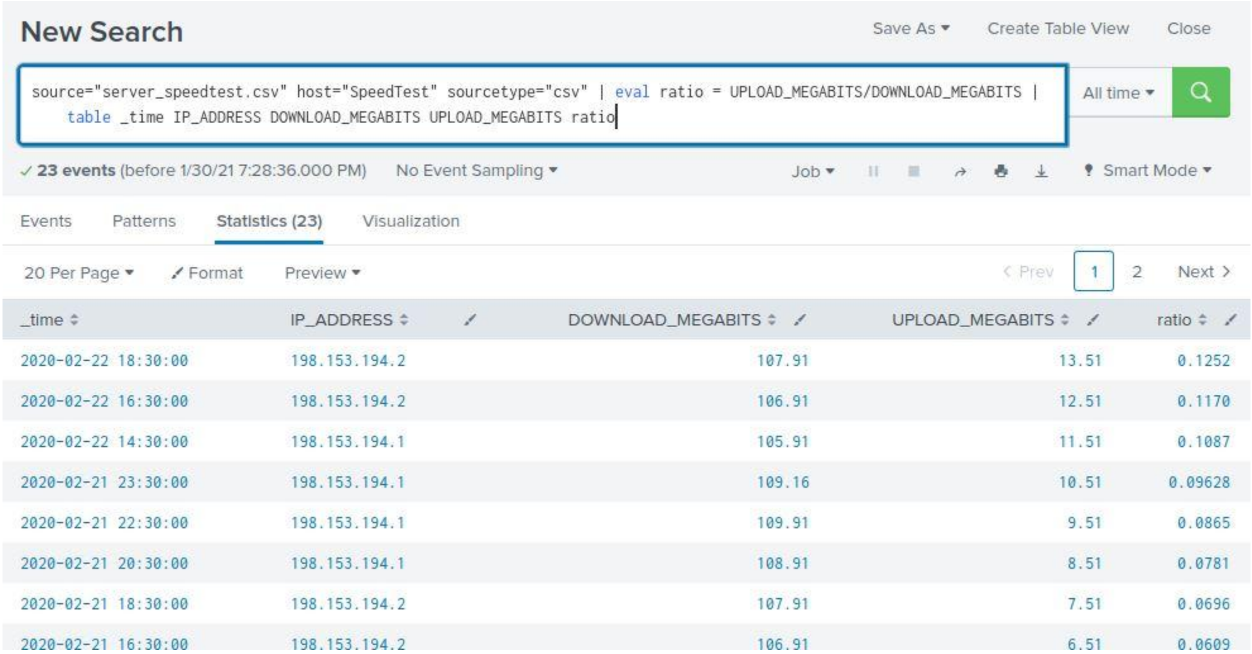
23 results   50 per page ▾

_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



_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
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	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	109.16	9.51	0.0871
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	0.2026
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	0.1962
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	0.2089

This is a query for the above report.



```
source="server_speedtest.csv" host="SpeedTest" sourcetype="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

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

   The approximate dates and times of the attacks, causing slowdown of upload and download speed, are the followings

   Answer: Feb 23, 2020 at 14:30 pm

   Feb 23, 2020 at 18:30 pm

   Feb 23, 2020 at 20:30 pm

   Feb 23, 2020 at 22:30 pm

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

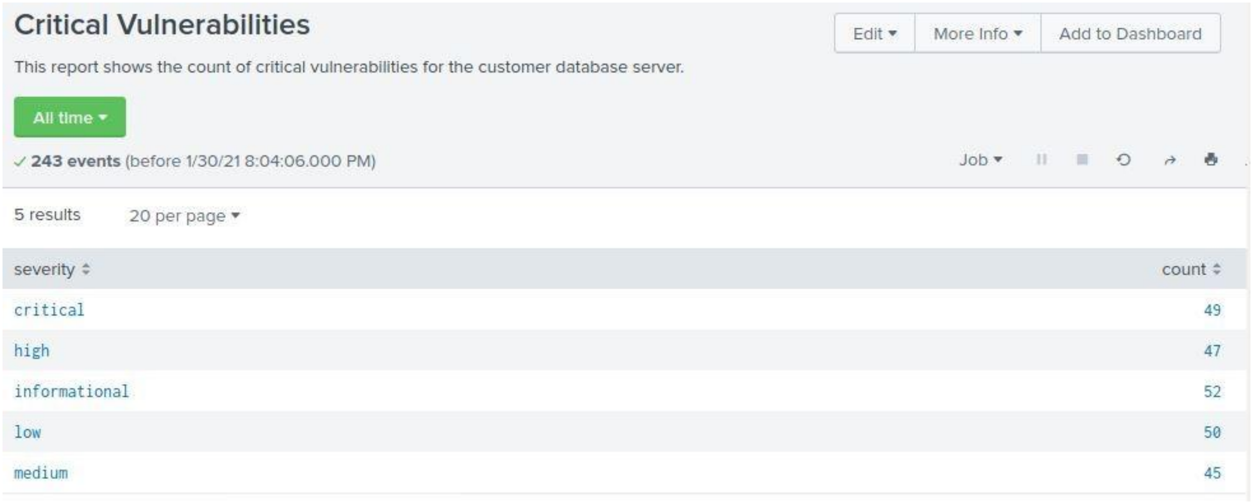
   Answer: The system was recovered at 23:30 pm. It took approximately 8 hours to recover the system.

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.

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. Create a report that shows the count of critical vulnerabilities from the customer database server. The database server IP is 10.11.36.23.



Critical Vulnerabilities

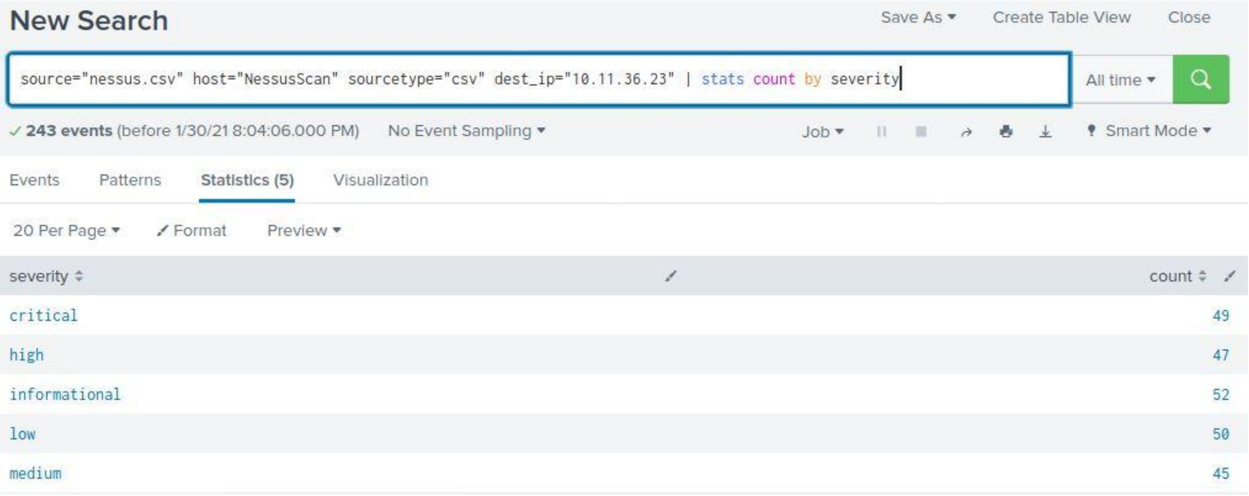
This report shows the count of critical vulnerabilities for the customer database server.

✓ 243 events (before 1/30/21 8:04:06.000 PM)

5 results 20 per page ▾

severity	count
critical	49
high	47
informational	52
low	50
medium	45

This is a query for the above report.



New Search

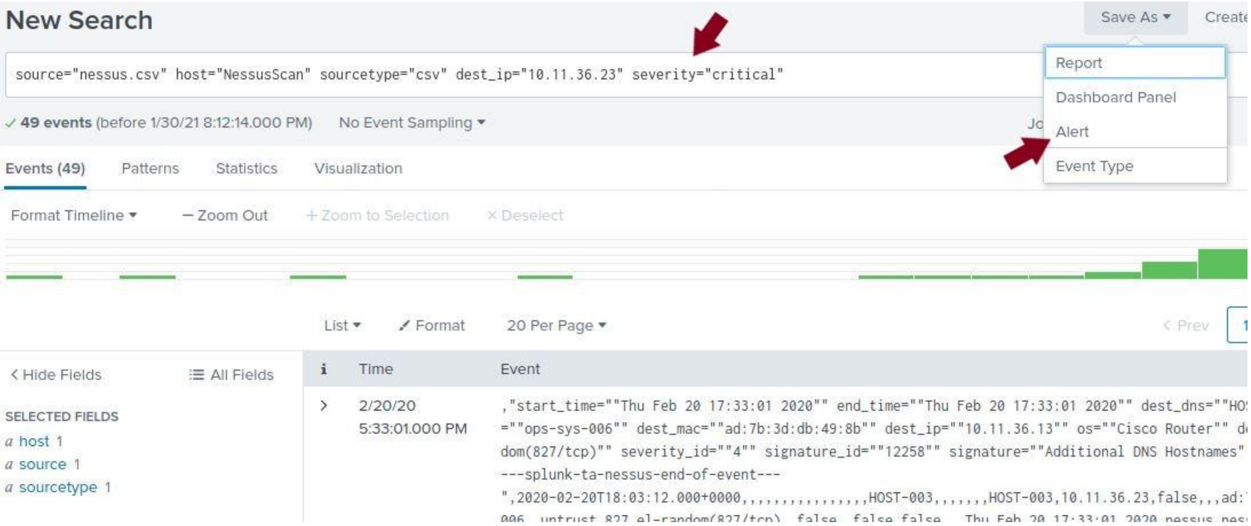
```
source="nessus.csv" host="NessusScan" sourcetype="csv" dest_ip="10.11.36.23" | stats count by severity
```

✓ 243 events (before 1/30/21 8:04:06.000 PM) No Event Sampling

Statistics (5)

severity	count
critical	49
high	47
informational	52
low	50
medium	45

2. 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.



New Search

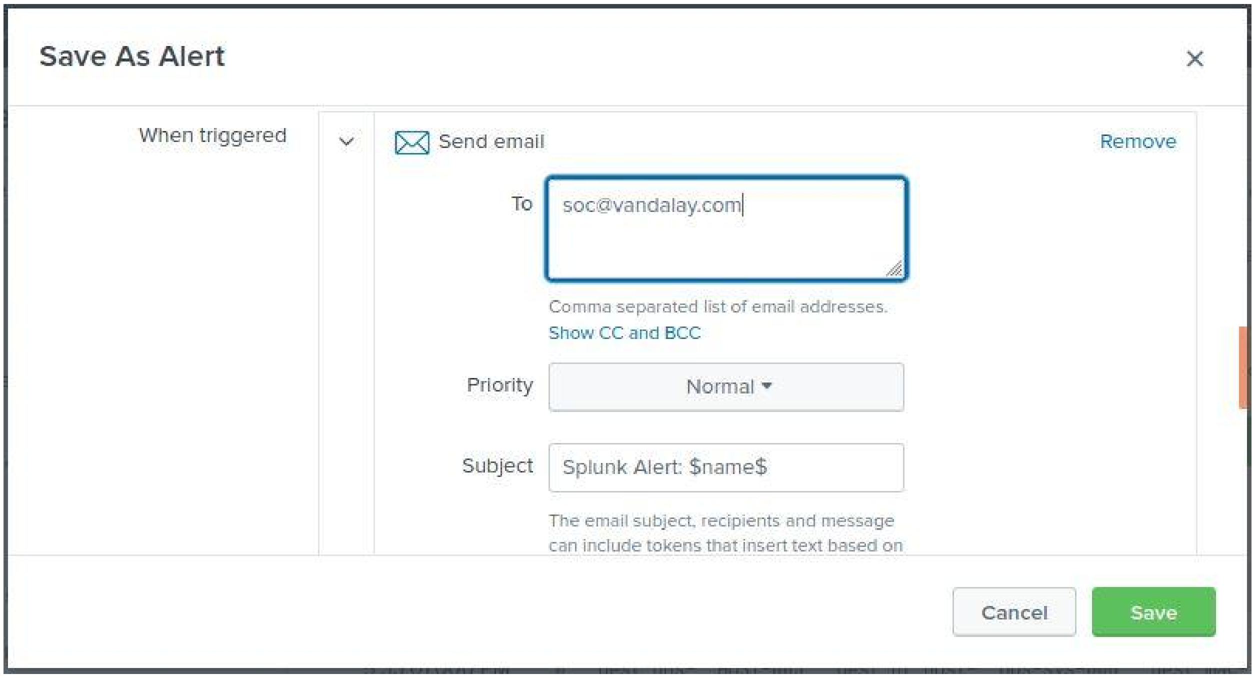
```
source="nessus.csv" host="NessusScan" sourcetype="csv" dest_ip="10.11.36.23" severity="critical"
```

✓ 49 events (before 1/30/21 8:12:14.000 PM) No Event Sampling

Save As ▾: Report, Dashboard Panel, Alert, Event Type

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

i	Time	Event
>	2/20/20 5:33:01.000 PM	,"start_time=""Thu Feb 20 17:33:01 2020"" end_time=""Thu Feb 20 17:33:01 2020"" dest_dns=""HO =""ops-sys-006"" dest_mac=""ad:7b:3d:db:49:8b"" dest_ip=""10.11.36.13"" os=""Cisco Router"" d dom(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: 006 untrust 827 el-random(827/tcp) false false false Thu Feb 20 17:33:01 2020 nessus nes



Save As Alert

When triggered

Send email

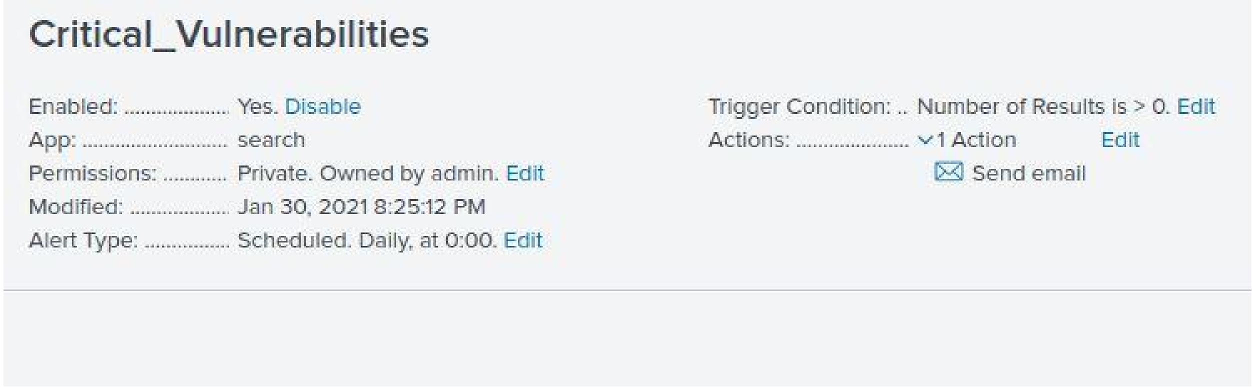
To: soc@vandalay.com

Comma separated list of email addresses.

Priority: Normal

Subject: Splunk Alert: $name$

The email subject, recipients and message can include tokens that insert text based on



Critical_Vulnerabilities

Enabled: .... Yes. Disable

App: .... search

Permissions: .... Private. Owned by admin. Edit

Modified: .... Jan 30, 2021 8:25:12 PM

Alert Type: .... Scheduled. Daily, at 0:00. Edit

Trigger Condition: .. Number of Results is > 0. Edit

Actions: .... 1 Action Edit

Send email

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.

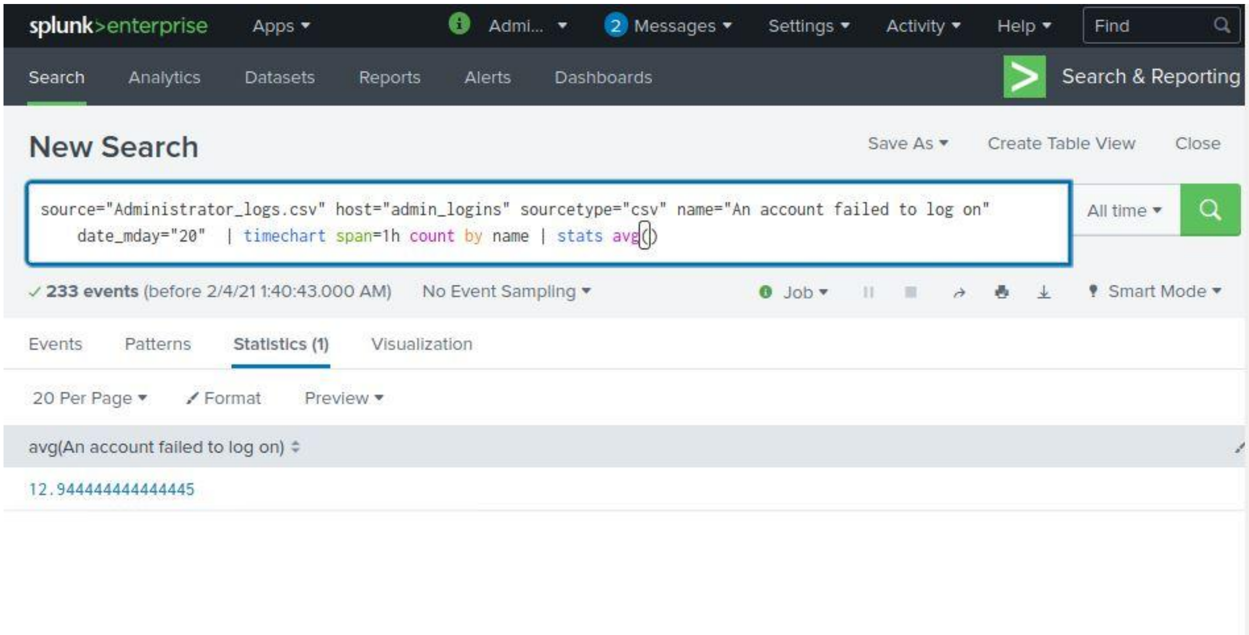
1. When did the brute force attack occur?

   Answer: Brute Force attack started at 9 am on Friday, February 21, 2020 and ended at 2 pm on the same day. It lasted for 6 hours.

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

   Answer: A baseline of normal activity is calculated based on data of the normal day where a brute force attack occurred, which was on Thursday, February 20, 2020. The baseline of normal activity is determined by averaging the number of failed logins on that day. The averaged failed login is 12.94 per hour. Therefore, the baseline of normal activity is 13 failed logins per hour.

   Threshold is calculated based on data of the day of the brute force attack, which was on Friday, February 21, 2020. The threshold is determined by averaging the number of failed logins on that day. The averaged failed login is 42.83 per hour. Therefore, the threshold is 43 failed logins per hour.

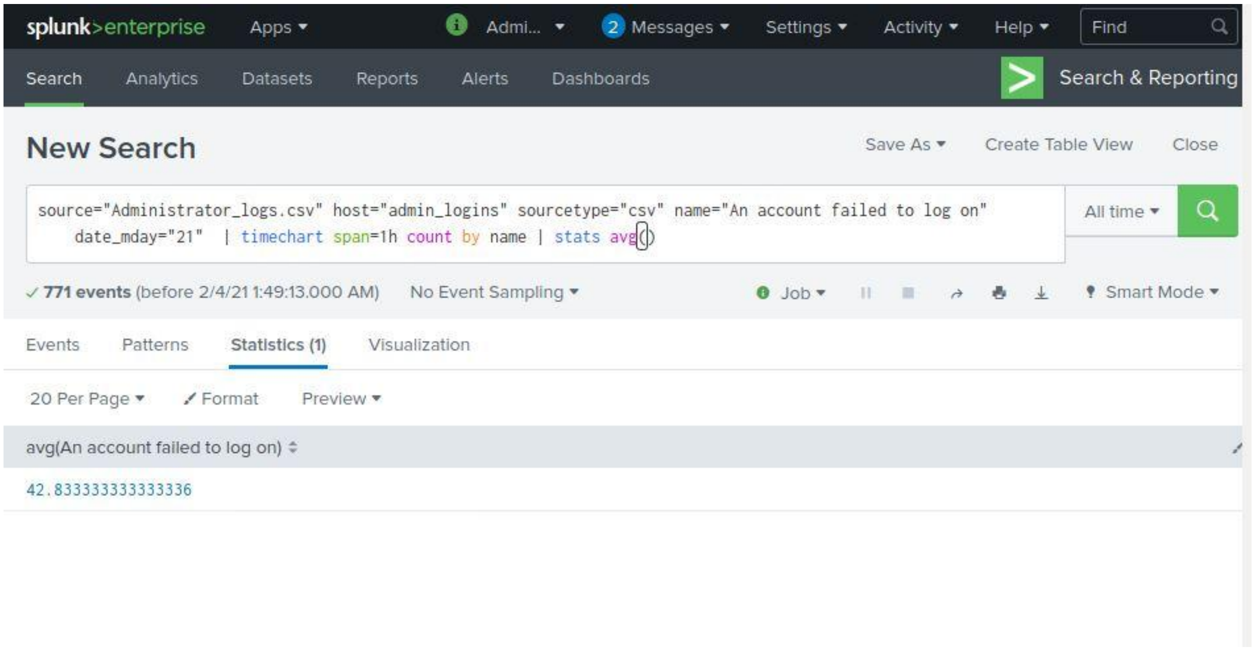


New Search

```
source="Administrator_logs.csv" host="admin_logins" sourcetype="csv" name="An account failed to log on"
    date_mday="20"  | timechart span=1h count by name | stats avg()
```

✓ 233 events (before 2/4/21 1:40:43.000 AM)

avg(An account failed to log on)
12.944444444444445



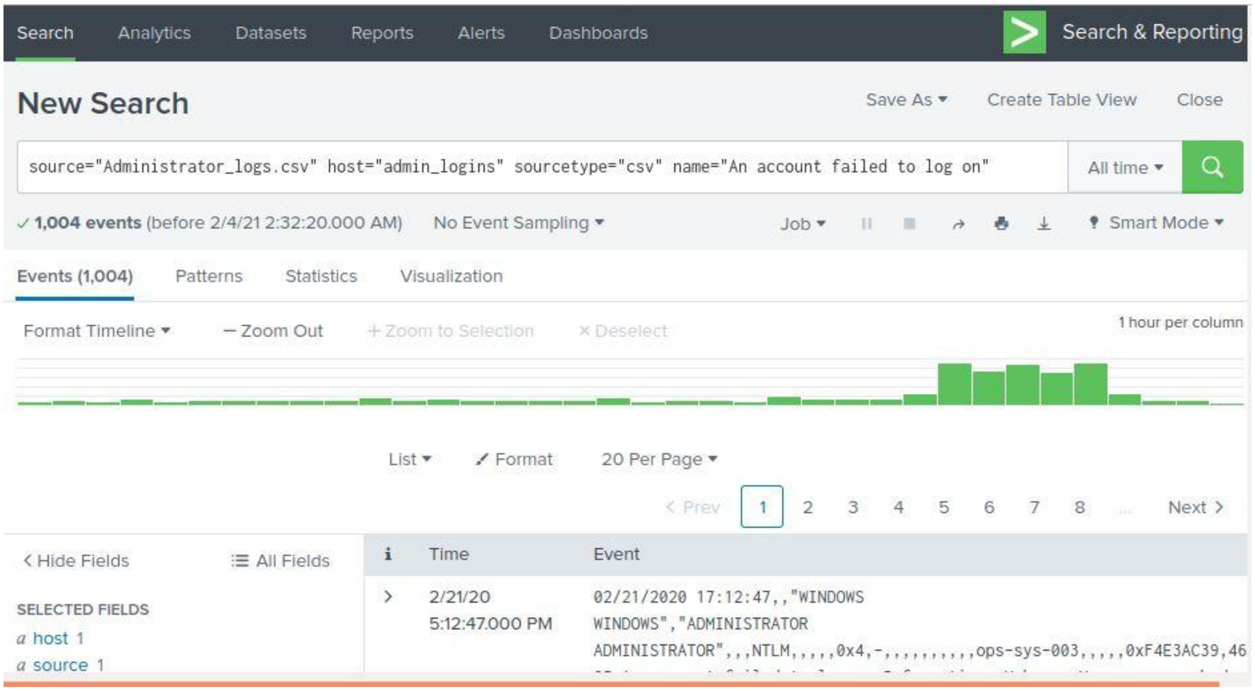
New Search

```
source="Administrator_logs.csv" host="admin_logins" sourcetype="csv" name="An account failed to log on"
    date_mday="21"  | timechart span=1h count by name | stats avg()
```

✓ 771 events (before 2/4/21 1:49:13.000 AM)

avg(An account failed to log on)
42.833333333333336

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

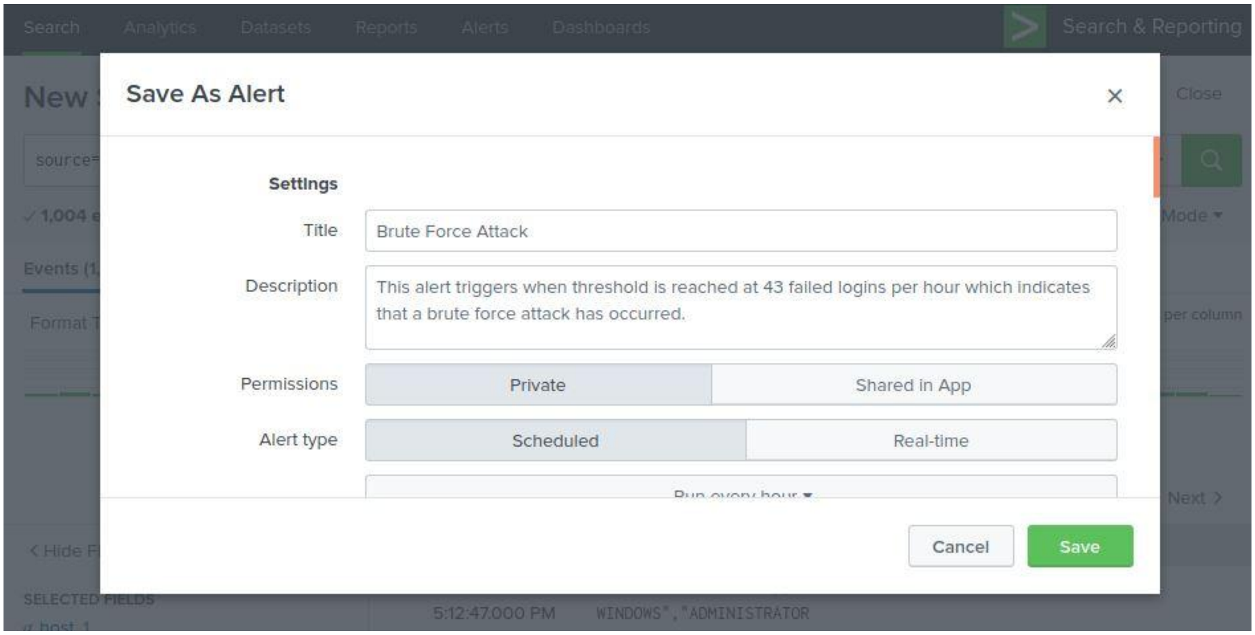


```
source="Administrator_logs.csv" host="admin_logins" sourcetype="csv" name="An account failed to log on"
```

✓ 1,004 events (before 2/4/21 2:32:20.000 AM)

2/21/20 5:12:47.000 PM

```
02/21/2020 17:12:47,,"WINDOWS
WINDOWS","ADMINISTRATOR
ADMINISTRATOR",,,NTLM,,,,,0x4,-,,,,,,,,,,ops-sys-003,,,,,0xF4E3AC39,46
```



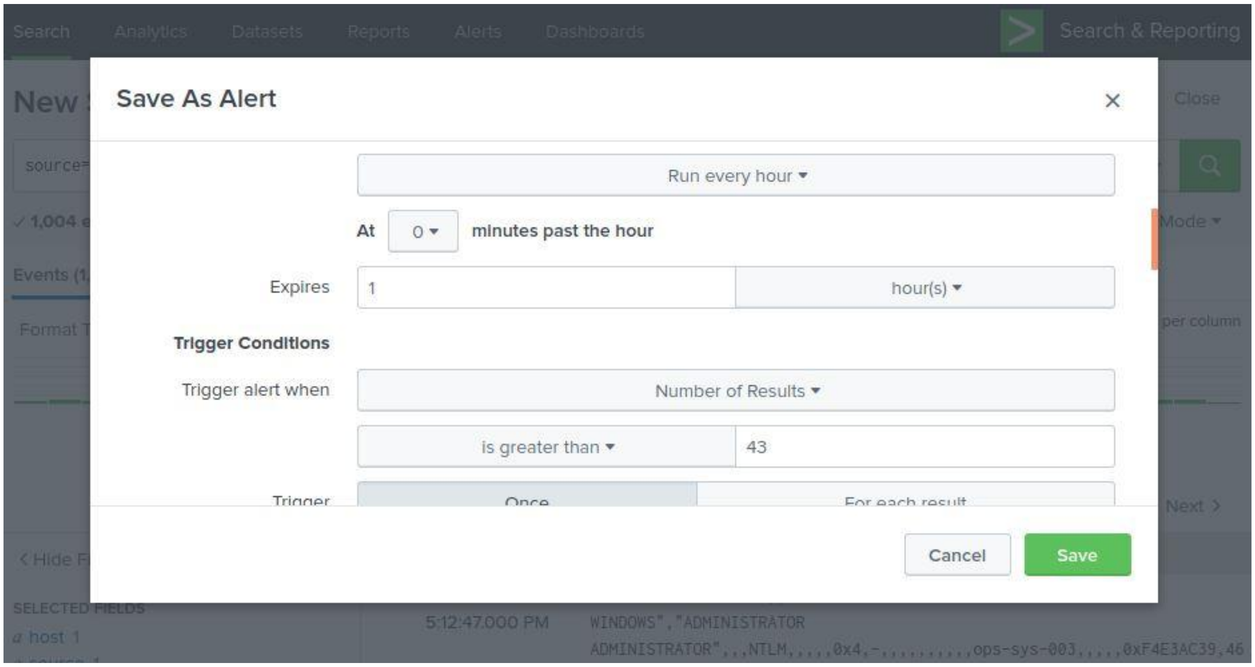
Title: Brute Force Attack

Description: This alert triggers when threshold is reached at 43 failed logins per hour which indicates that a brute force attack has occurred.

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour ▾



Save As Alert

Run every hour

At 0 minutes past the hour

Expires: 1 hour(s)

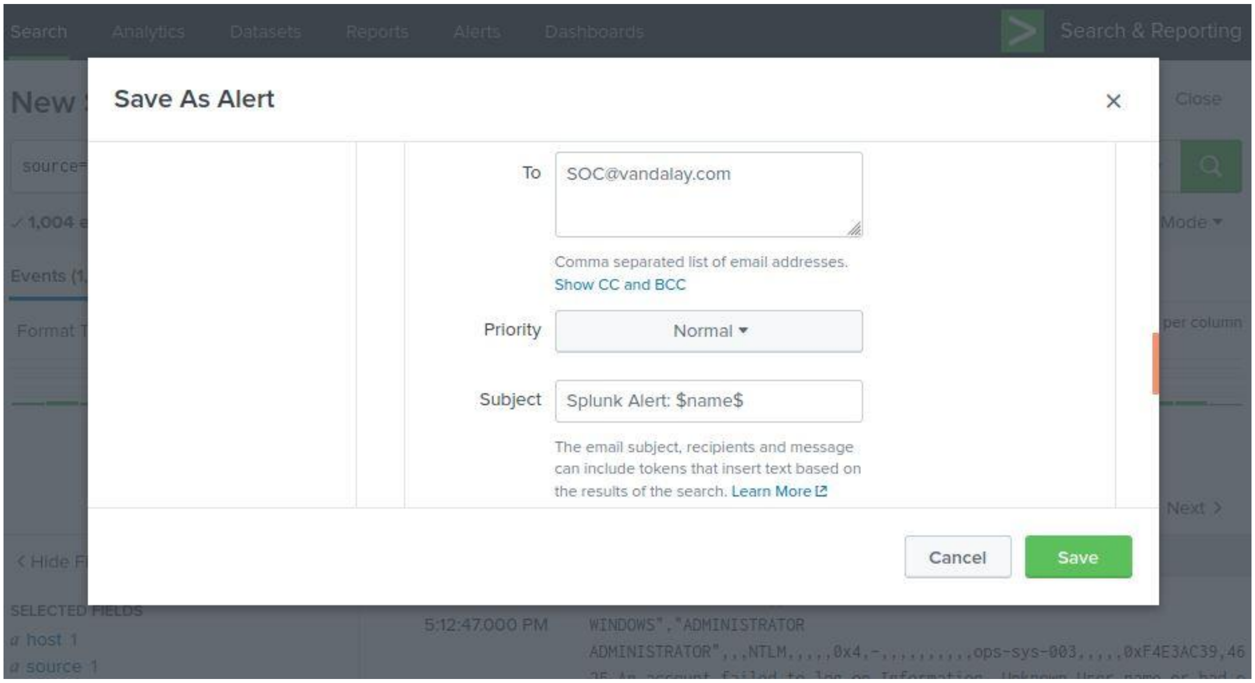
Trigger Conditions

Trigger alert when: Number of Results

is greater than: 43

Trigger: Once | For each result

```
5:12:47.000 PM   WINDOWS","ADMINISTRATOR
                 ADMINISTRATOR",,,NTLM,,,,,0x4,-,,,,,,,,,,,ops-sys-003,,,,,0xF4E3AC39,46
```



Save As Alert

To: SOC@vandalay.com

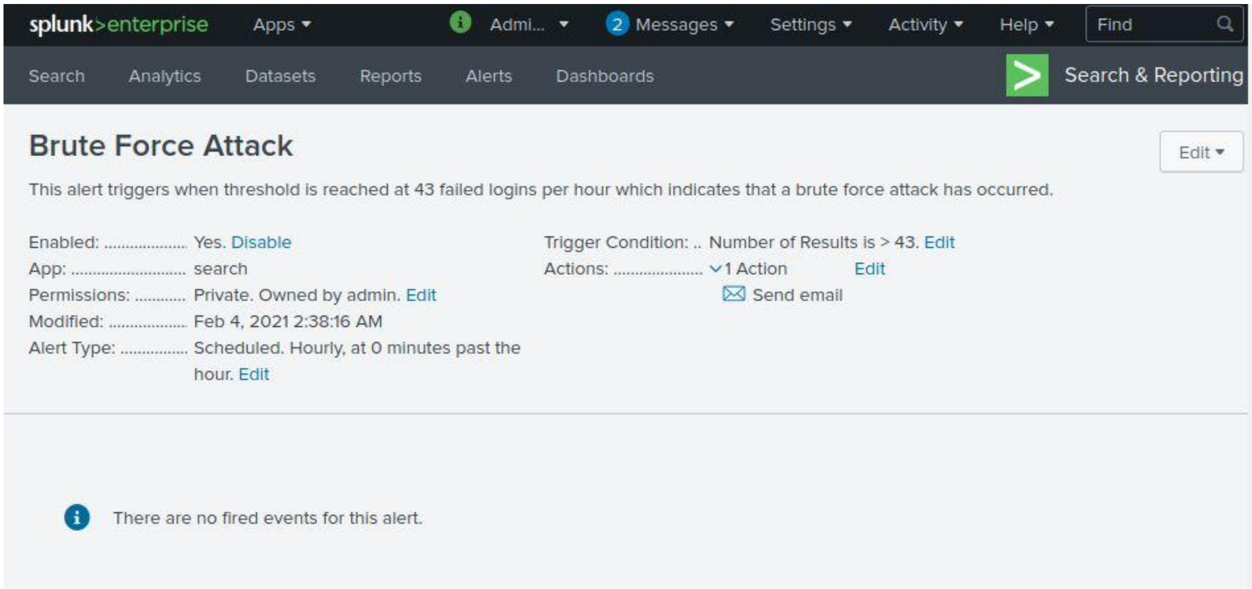
Comma separated list of email addresses.
Show CC and BCC

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

```
5:12:47.000 PM   WINDOWS","ADMINISTRATOR
                 ADMINISTRATOR",,,NTLM,,,,,0x4,-,,,,,,,,,,,ops-sys-003,,,,,0xF4E3AC39,46
```



Brute Force Attack

This alert triggers when threshold is reached at 43 failed logins per hour which indicates that a brute force attack has occurred.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 4, 2021 2:38:16 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 43. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.