Cybersecurity

Module 19 Challenge Submission File

Let's Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: The Need for Speed

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

```
Between 2020-02-23 T18:30:00.000Z and 2020-02-23 T14:30:00.000Z
```

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

```
Systems recovered at 2020-02-22 T23:30:00.000Z or the next day
```

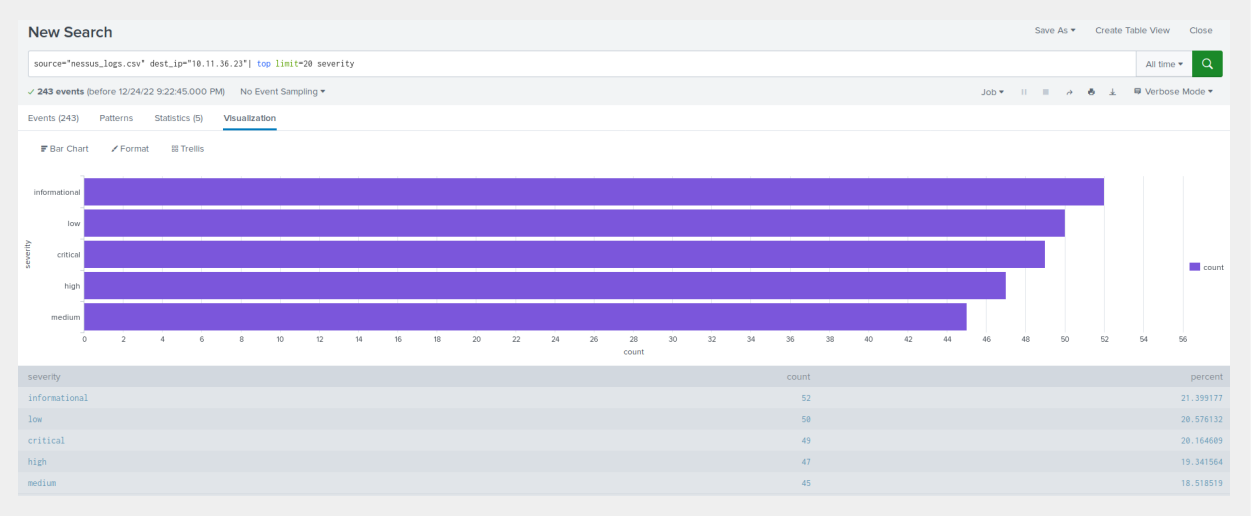
Provide a screenshot of your report:

✓ **Previewing 23 events** (2/20/20 2:21:00.000 PM to 12/20/22 10:39:24.000 PM) Event Limiting: ~100,000

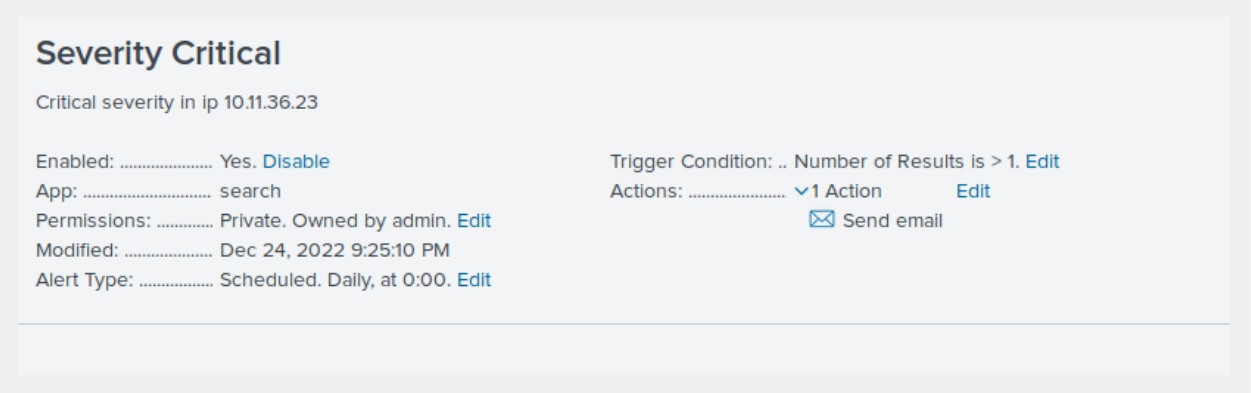
*	_time	# DOWNLOAD_MEGA...	IP IP_ADDRESS	# ratio	# UPLOAD_MEGABITS
1	2020-02-22T18:30:00.000Z	107.91	198.153.194.2	0.1252	13.51
2	2020-02-22T16:30:00.000Z	106.91	198.153.194.2	0.1170	12.51
3	2020-02-22T14:30:00.000Z	105.91	198.153.194.1	0.1087	11.51
4	2020-02-21T23:30:00.000Z	109.16	198.153.194.1	0.09628	10.51
5	2020-02-21T22:30:00.000Z	109.91	198.153.194.1	0.0865	9.51
6	2020-02-21T20:30:00.000Z	108.91	198.153.194.1	0.0781	8.51
7	2020-02-21T18:30:00.000Z	107.91	198.153.194.2	0.0696	7.51
8	2020-02-21T16:30:00.000Z	106.91	198.153.194.2	0.0609	6.51
9	2020-02-21T14:30:00.000Z	105.91	198.153.194.1	0.0520	5.51
10	2020-02-20T14:21:00.000Z	109.16	198.153.194.1	0.0497	5.43
11	2020-02-23T23:30:00.000Z	123.91	198.153.194.2	0.0687	8.51
12	2020-02-23T23:30:00.000Z	122.91	198.153.194.1	0.0611	7.51
13	2020-02-23T22:30:00.000Z	78.34	198.153.194.1	0.0831	6.51
14	2020-02-23T20:30:00.000Z	65.34	198.153.194.2	0.0647	4.23
15	2020-02-23T18:30:00.000Z	17.56	198.153.194.2	0.195	3.43
16	2020-02-23T14:30:00.000Z	7.87	198.153.194.1	0.233	1.83
17	2020-02-23T14:30:00.000Z	12.76	198.153.194.2	0.172	2.19

Step 2: Are We Vulnerable?

Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

```
The attack occurred between 9:00 AM and 2:00 PM
```

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

```
Our baseline would be 13 and the threshold for an alert would be 25 failed logins.
```

3. Provide a screenshot showing that the alert has been created: