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

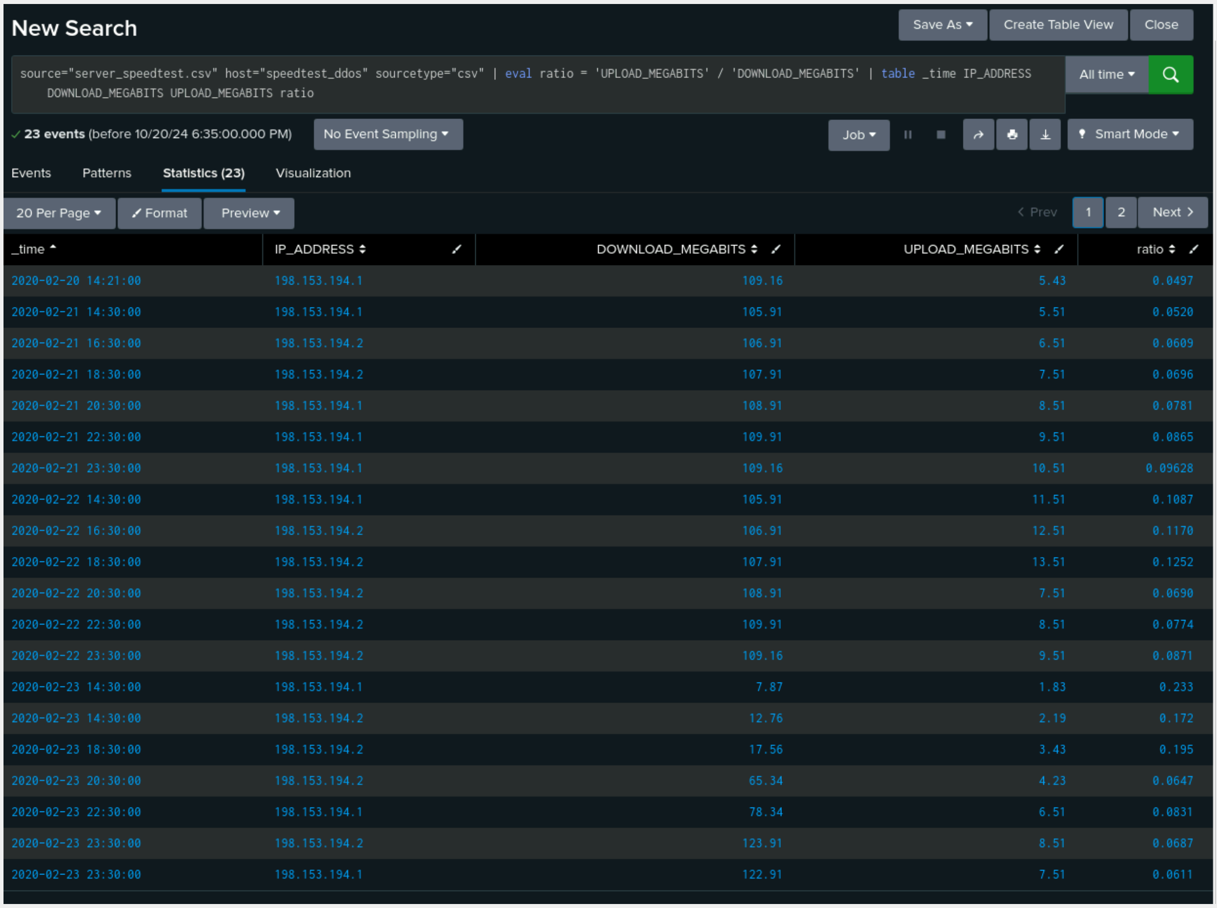
1. Based on the report you created, what is the approximate date and time of the attack?

```
Approximate date and time are 2020-02-23 14:30:00
```

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

```
About 6hrs to recover based on the speed diagnostics
```

Provide a screenshot of your report:



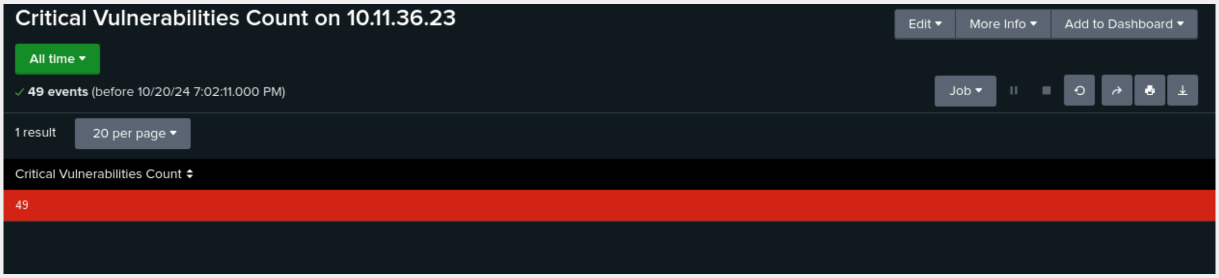
```
source="server_speedtest.csv" host="speedtest_ddos" sourcetype="csv" | eval ratio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' | table _time IP_ADDRESS
    DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio
```

✓ **23 events** (before 10/20/24 6:35:00.000 PM) No Event Sampling ▾

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
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
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
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

Step 2: Are We Vulnerable?

Provide a screenshot of your report:



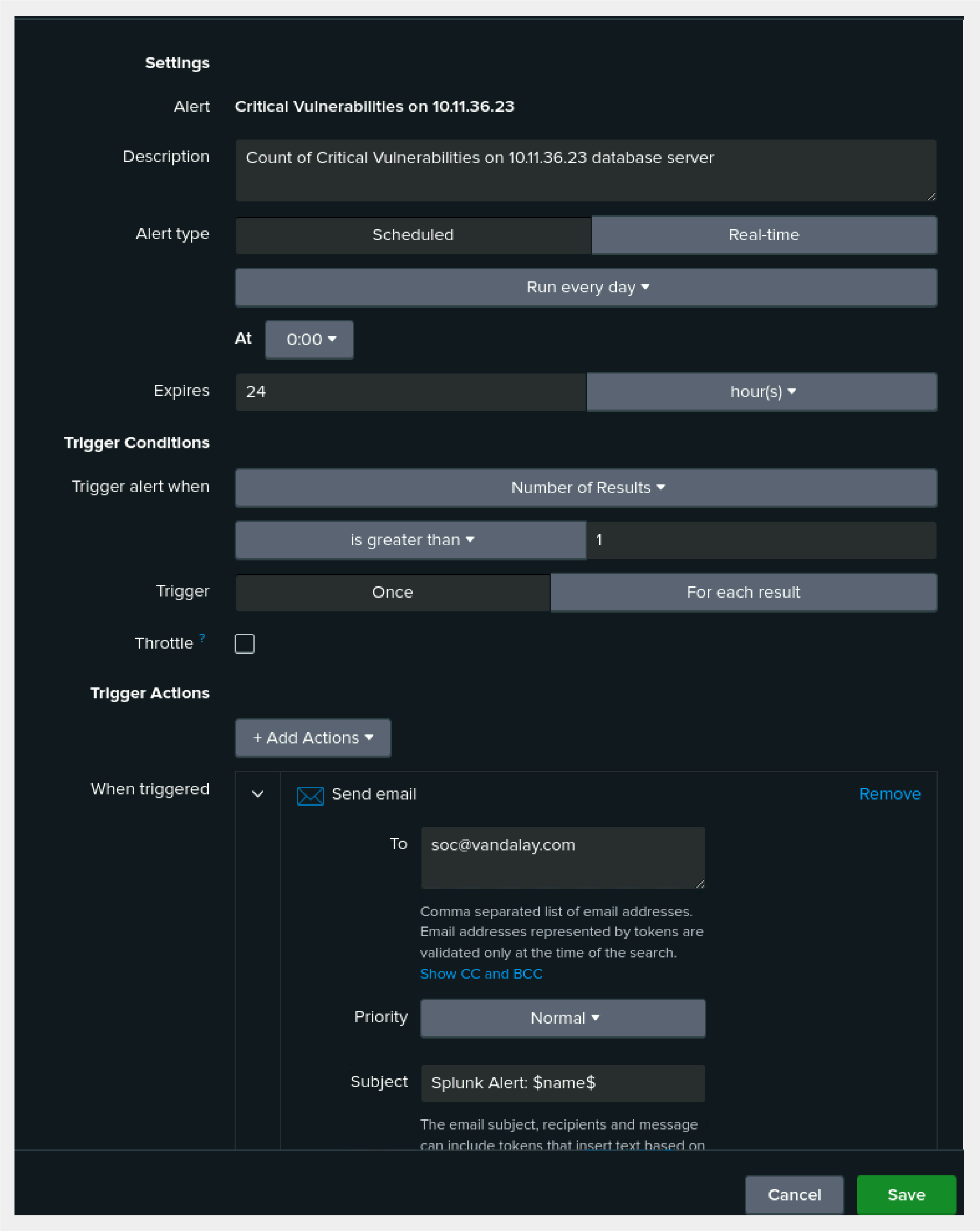
Critical Vulnerabilities Count on 10.11.36.23

✓ **49 events** (before 10/20/24 7:02:11.000 PM)

1 result

Critical Vulnerabilities Count
49

Provide a screenshot showing that the alert has been created:



Settings

Alert: **Critical Vulnerabilities on 10.11.36.23**

Description: Count of Critical Vulnerabilities on 10.11.36.23 database server

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 ▾ | 1

Trigger: Once | For each result

Throttle ? ☐

Trigger Actions

+ Add Actions ▾

When triggered: Send email — Remove

To: soc@vandalay.com

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.
Show CC and BCC

Priority: Normal ▾

Subject: Splunk Alert: $name$

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

Step 3: Drawing the (Base)line

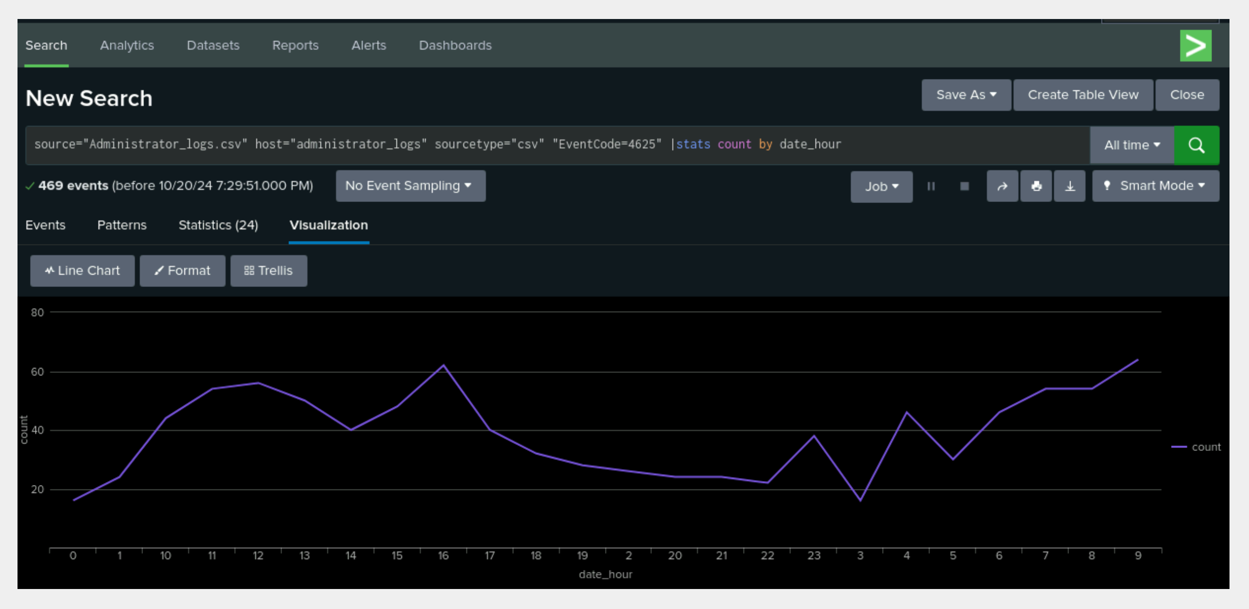
1. When did the brute force attack occur?

```
Friday Feb 21 2020 around 9am - 1pm
```

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

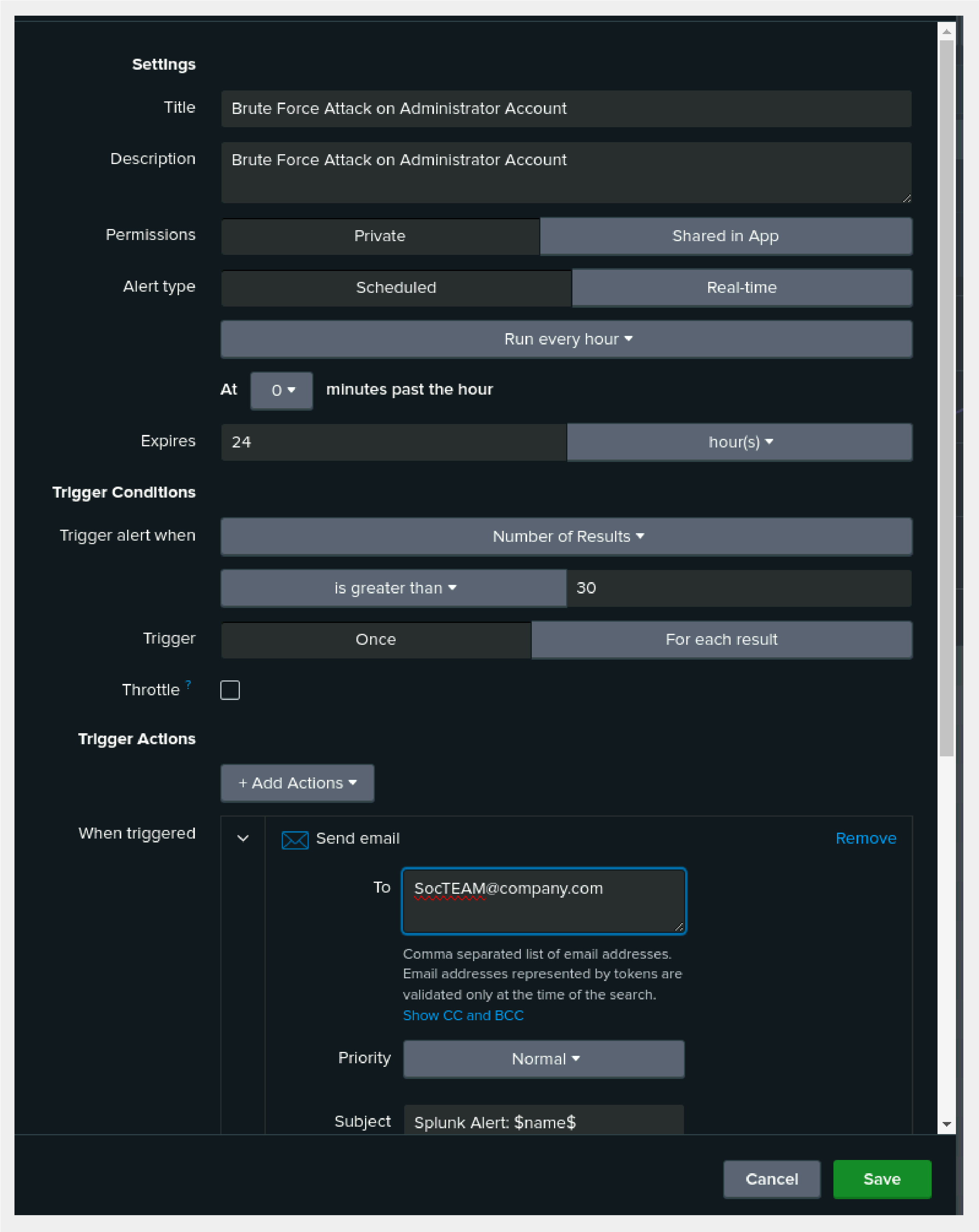
```
Baseline = about 35 /hr
```

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



```
source="Administrator_logs.csv" host="administrator_logs" sourcetype="csv" "EventCode=4625" |stats count by date_hour
```

✓ **469 events** (before 10/20/24 7:29:51.000 PM)



Settings

Title: Brute Force Attack on Administrator Account

Description: Brute Force Attack on Administrator Account

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

Trigger: Once | For each result

Throttle ? □

Trigger Actions

+ Add Actions ▾

When triggered: Send email

To: SocTEAM@company.com

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.

Show CC and BCC

Priority: Normal ▾

Subject: Splunk Alert: $name$