***Unit 18 Homework: Let’s go Splunking***

**Step 1 –**

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

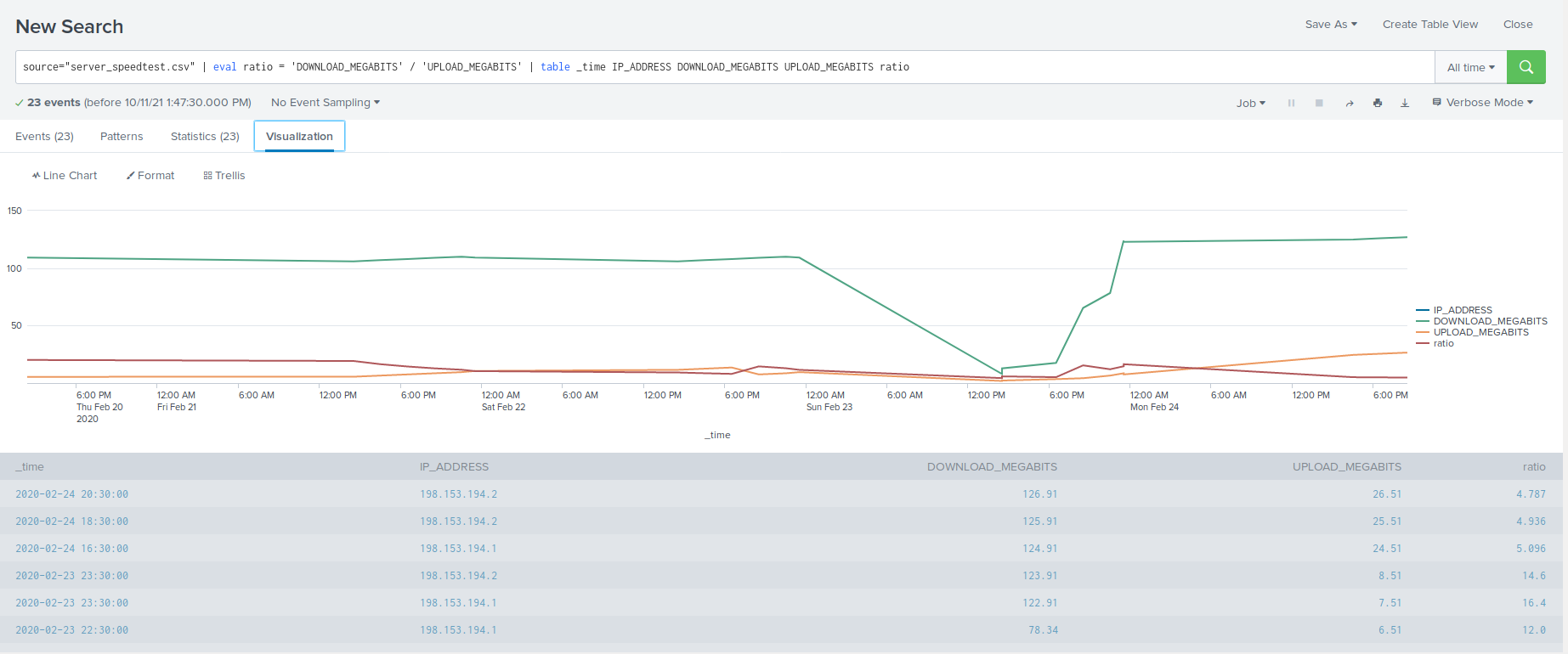
Feb 22nd, 2020 11:30pm is when the attack started.

**How long did it take your systems to recover?**

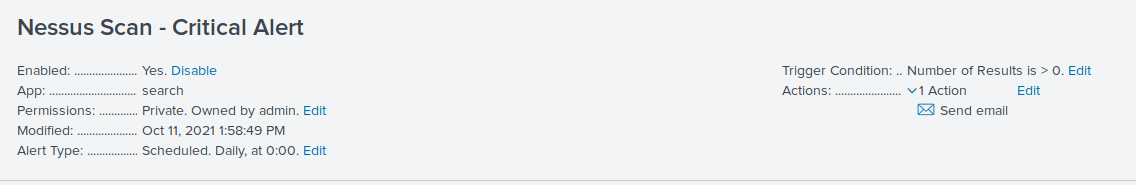
Systems took a FULL 24 hours to recover – Feb 23rd, 2020 11:30pm

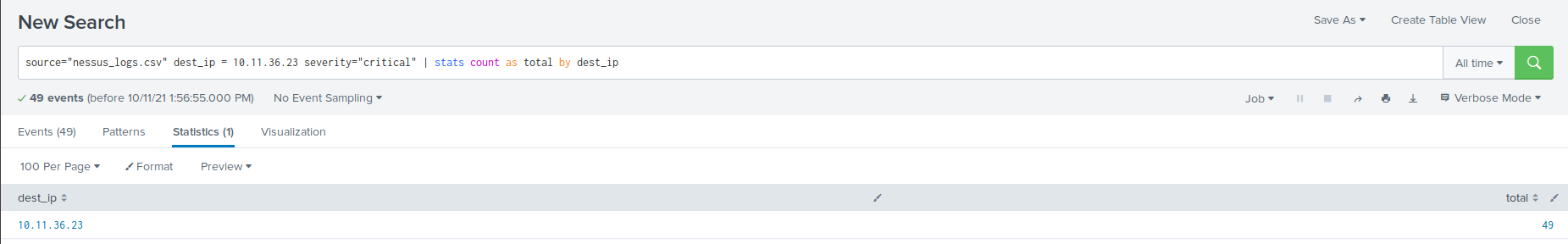
Graphical user interface, table

Description automatically generated



**Step 2 –**





**Step 3 –**

**When did the Brute Force attack Occur?**

This attack started at 9am, Friday, Feb 21st, 2020 though it should be noted it is possible that at 7am the failed attempts stay at 15 and at 8am jumps to 34 so it is likely that this is the beginning to the attack.

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

Using:

source=”Administrator\_logs.csv” name=”An account failed to log on” | timechart span=1h count(\_raw) as hourly, | outlier | eventstats avg(hourly) as avghourly | eventstats stdev(hourly) as stdhourly

we can determine the following:

* Baseline = 18 – this is set as an average (avghourly).
* Threshold = 52 – the standard deviation is 11.3, so adding 3 standard deviations on top of the average gives me 51.9 – rounded up to 52 (stdhourly).

