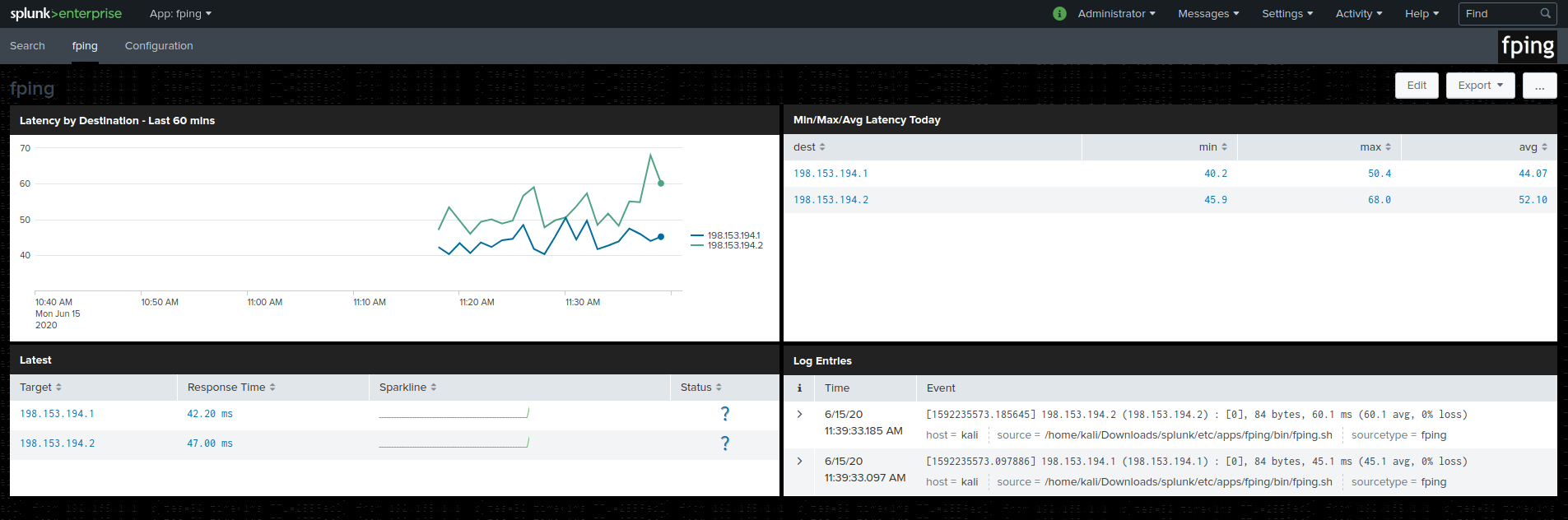
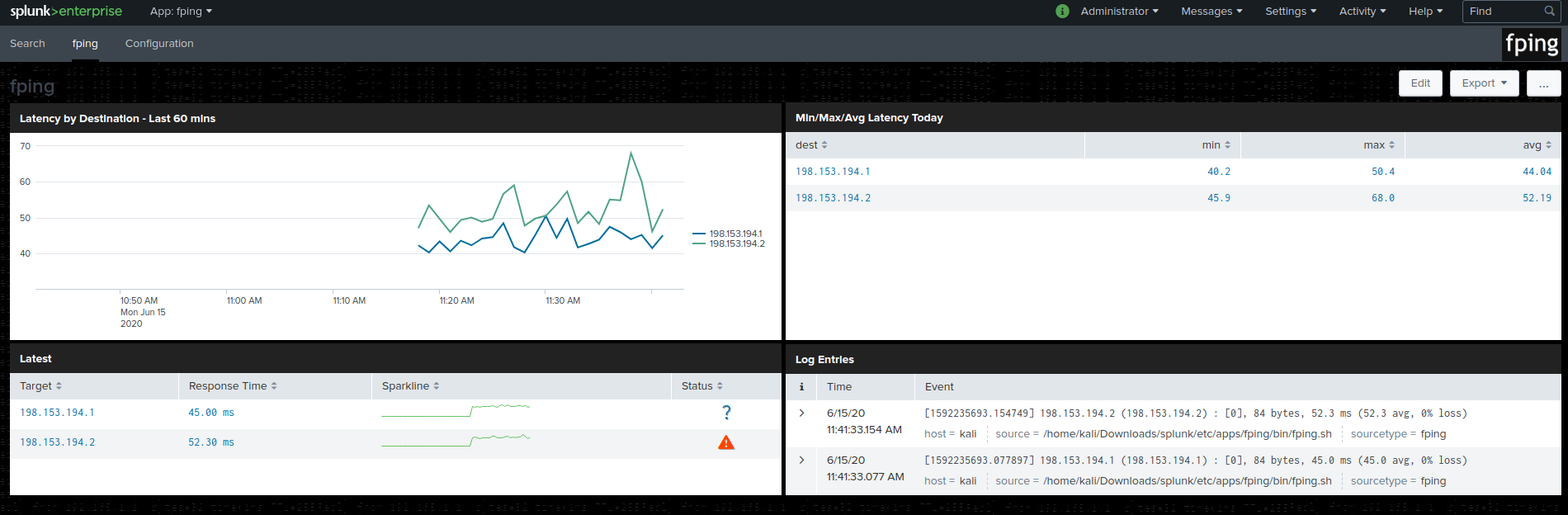
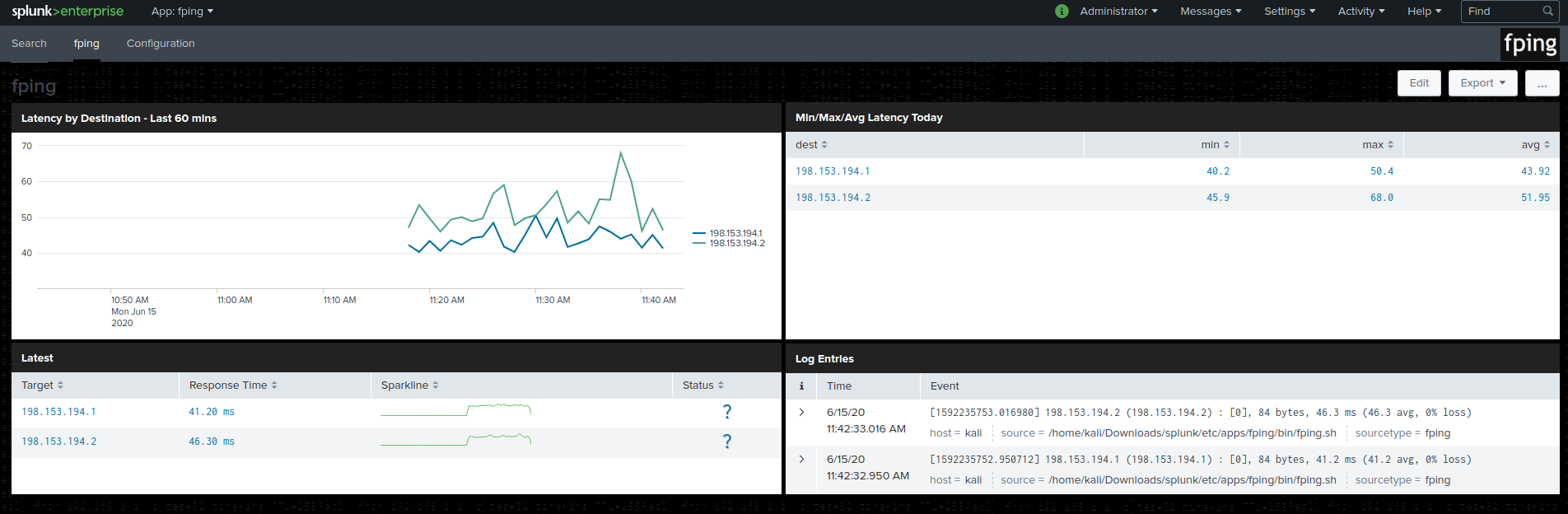
**SIEM HW 18**

JD Haynes

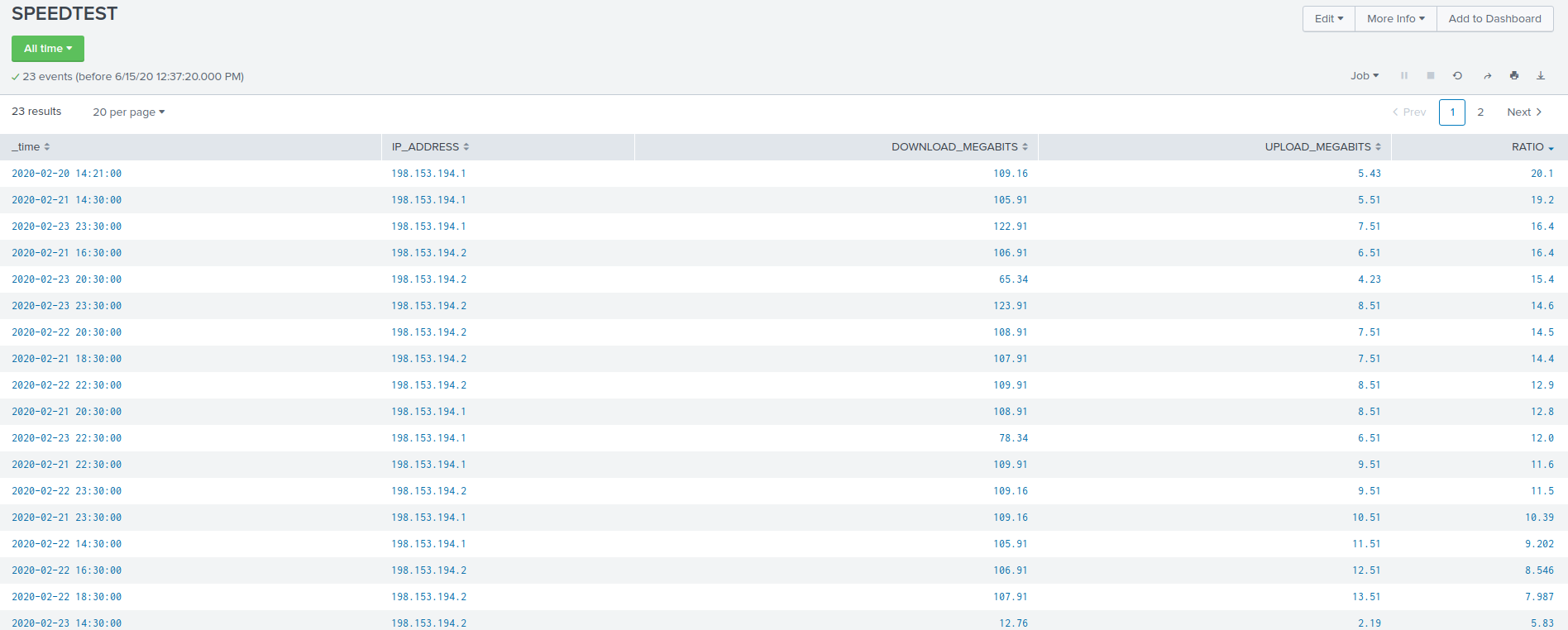
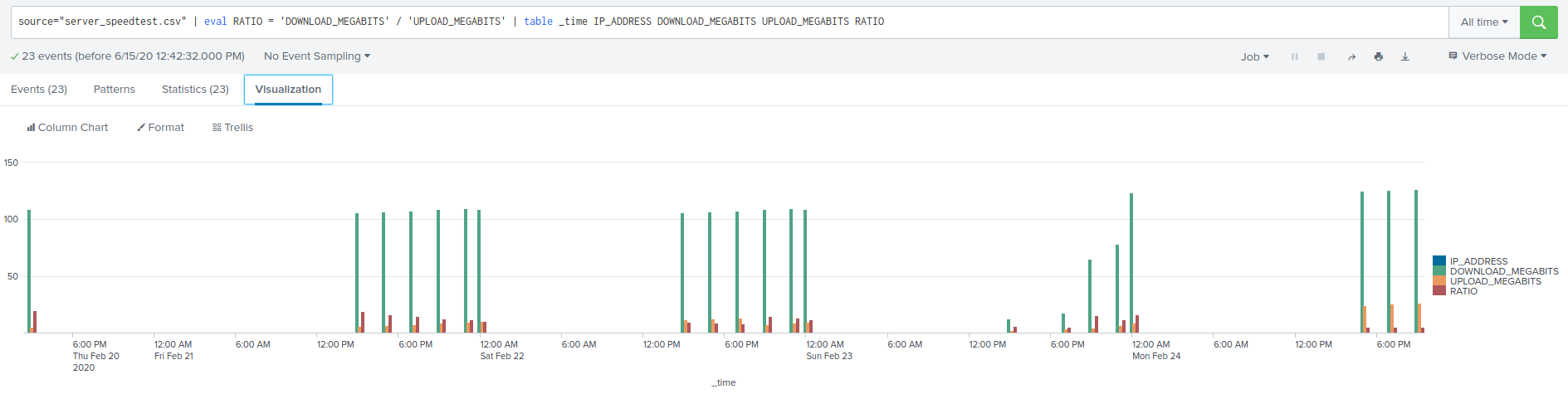
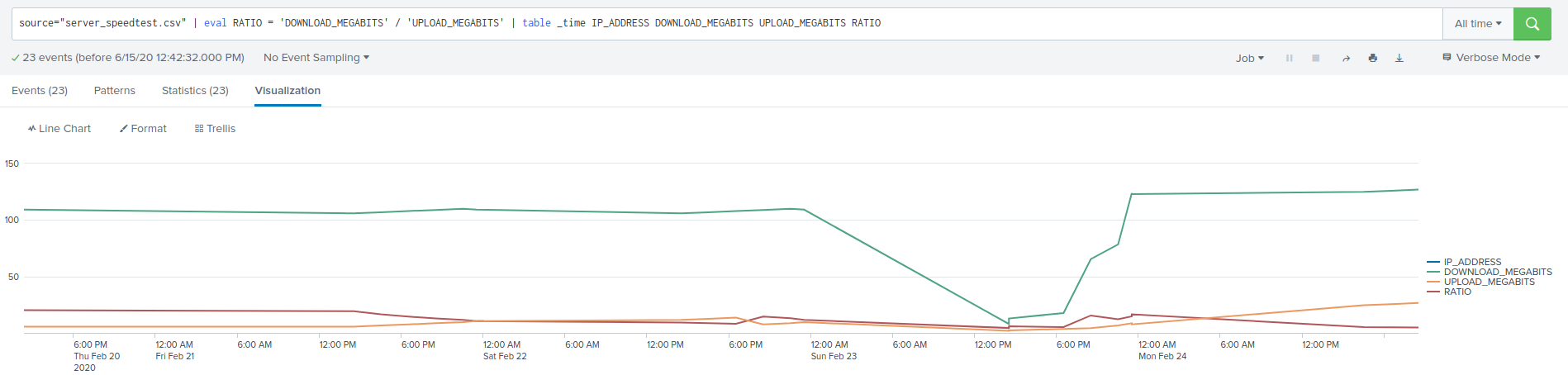
Step 1: Monitoring Vandalay’s Web Servers

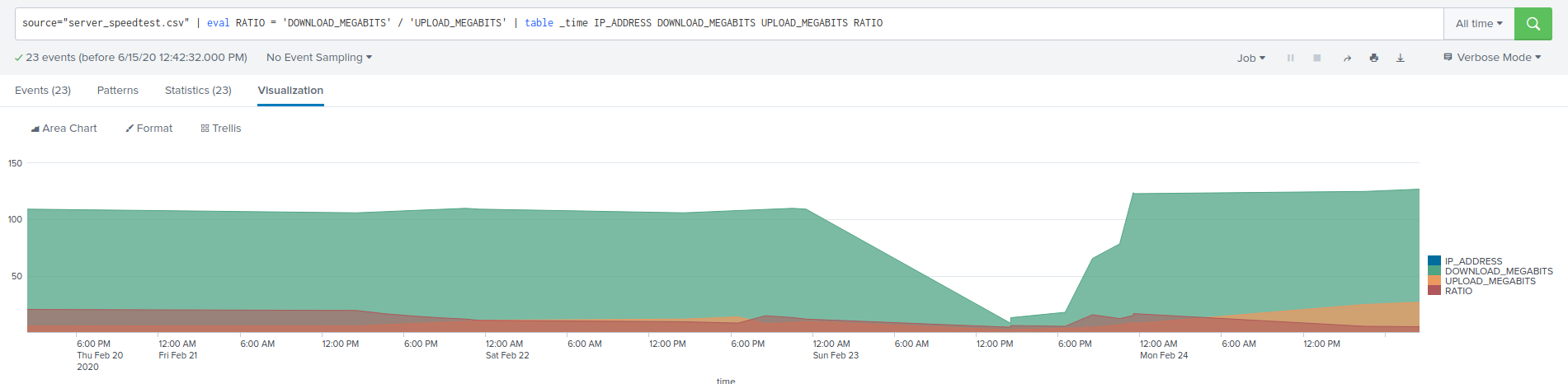
Fping results for 198.153.194.1 and 198.153.194.2



**Step 2: The Need for Speed**

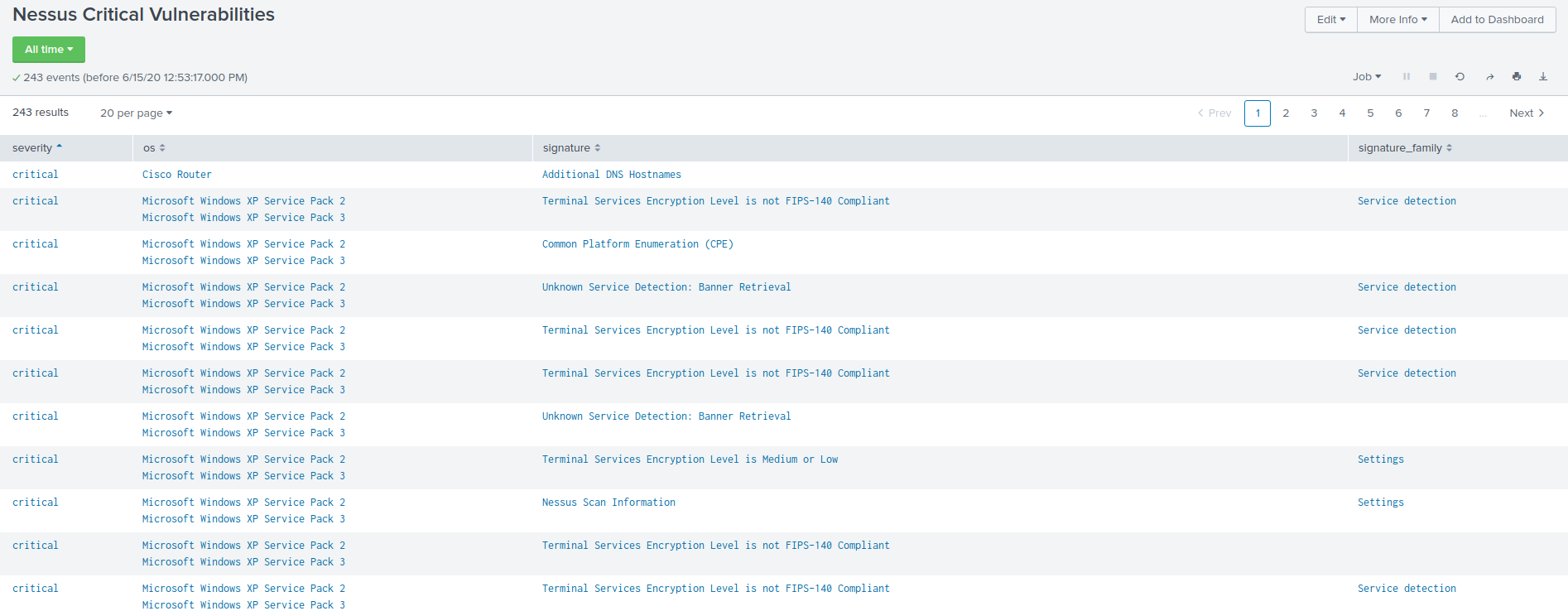
Create filter for ratio field and table: (note that answers to questions are below the charts for this section)

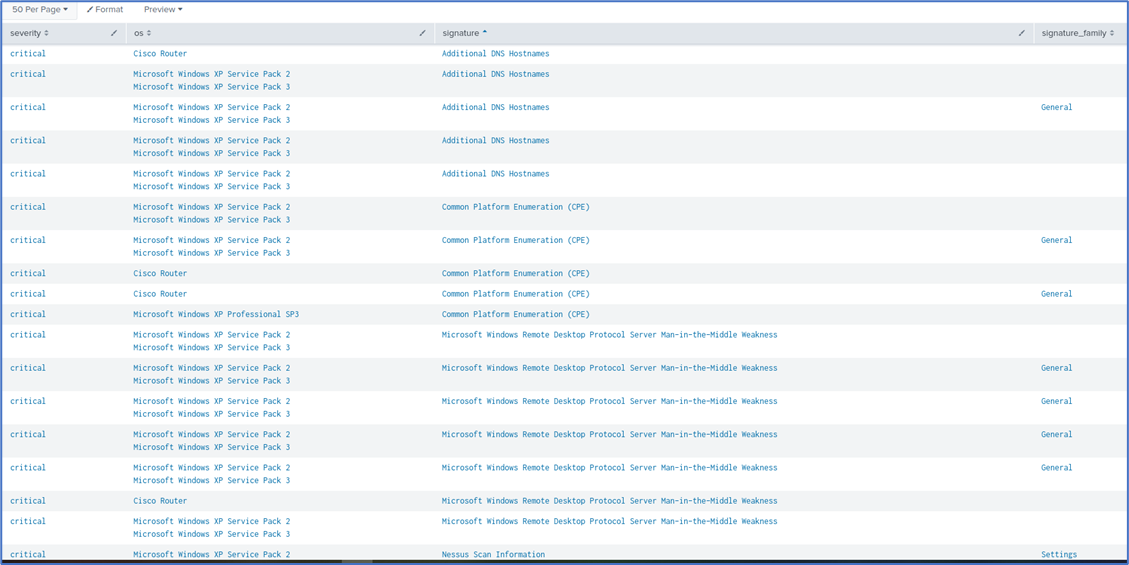
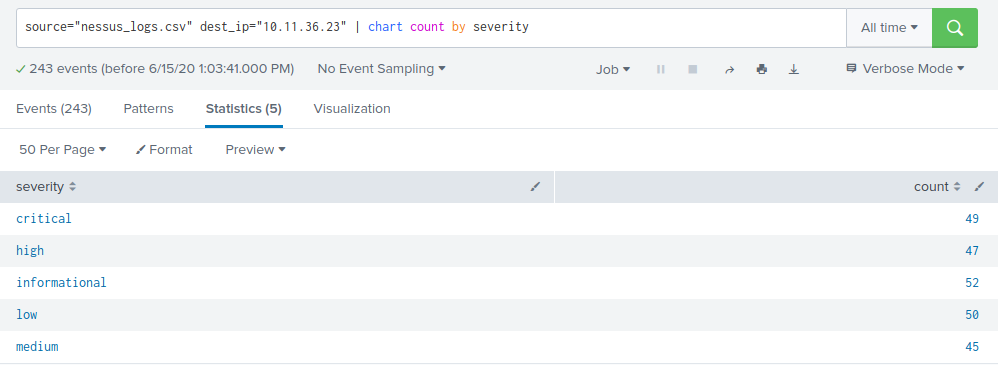
source="server\_speedtest.csv" | eval RATIO = 'DOWNLOAD\_MEGABITS' / 'UPLOAD\_MEGABITS' | table \_time IP\_ADDRESS DOWNLOAD\_MEGABITS UPLOAD\_MEGABITS RATIO

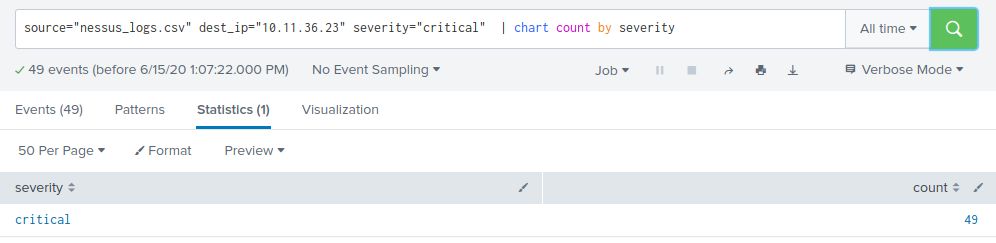


* Based on report, approximate date and time of attack is Feb 23, 2020 starting at 2:30 pm
* Based on the bar chart (2nd chart above, on 1st page), length of time for systems to recover was at least 4 hours before the ratio started returning to normal around 8:30 pm, although it was not fully back to normal until nearly midnight.

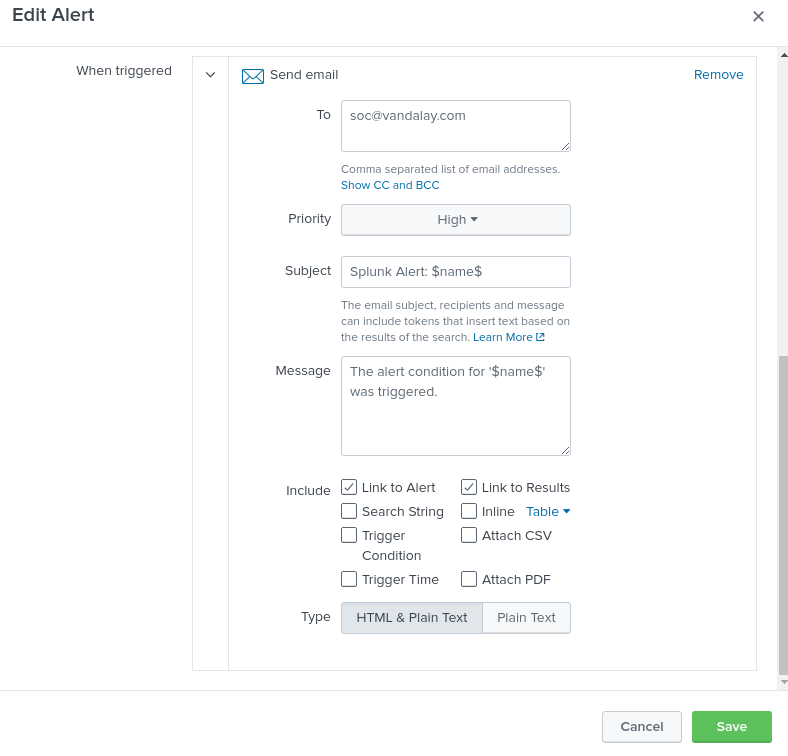
**Step 3: Are We Vulnerable? NESSUS**

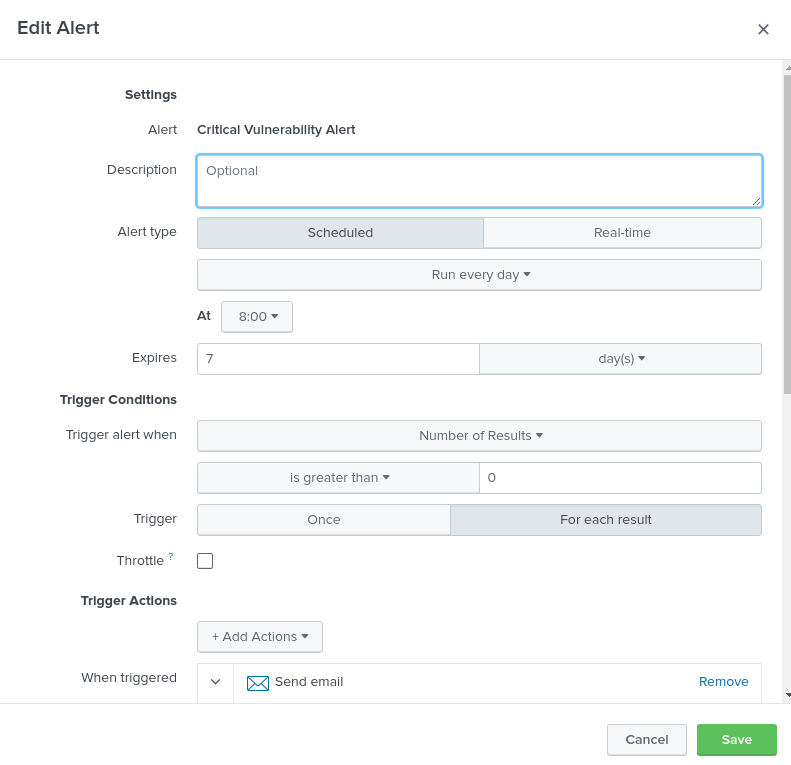


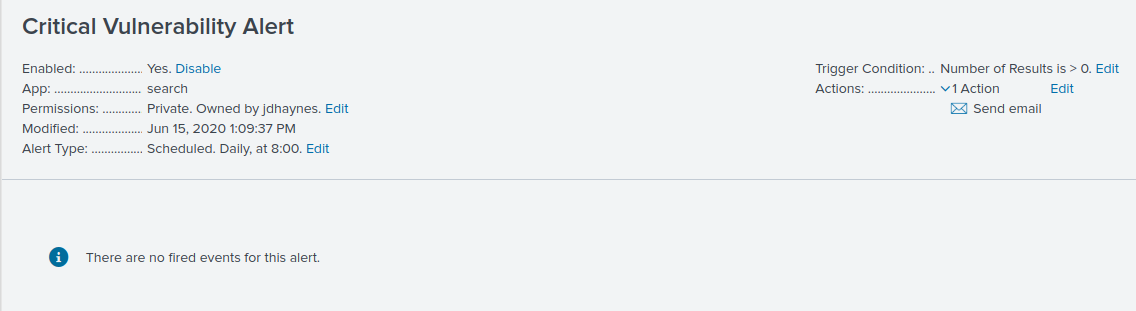




Alert for critical vulnerability captures list of events with severity measured as “critical”, then sends a daily alert report to [soc@vandalay.com](mailto:soc@vandalay.com) at 8 a.m.



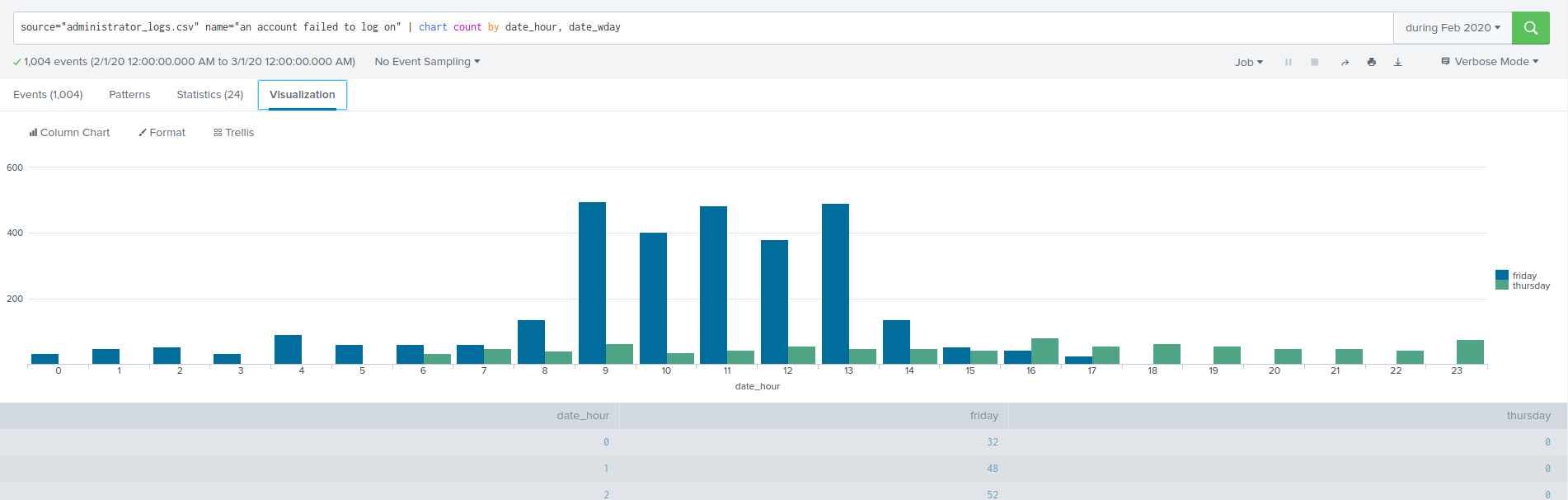


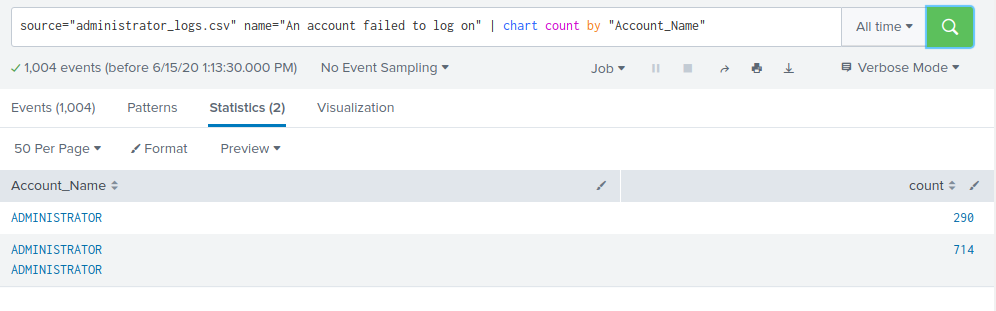


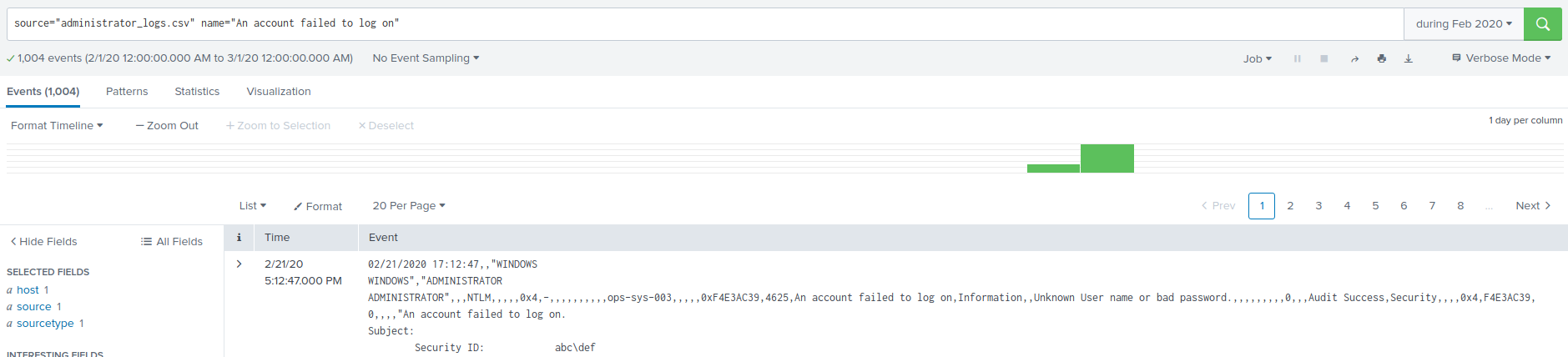
**Step 4: Drawing the (base)line**

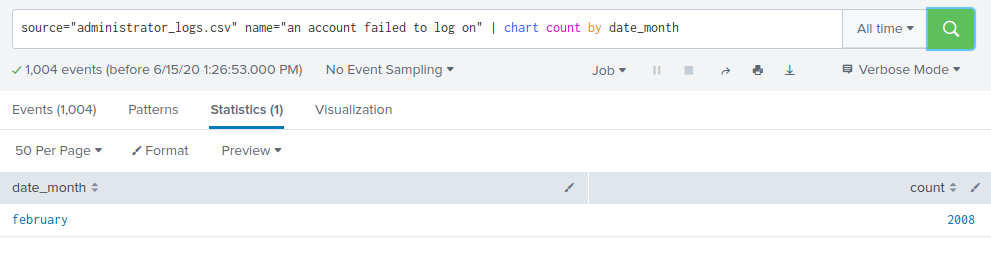
(Note that answers for the questions are below all the charts.)

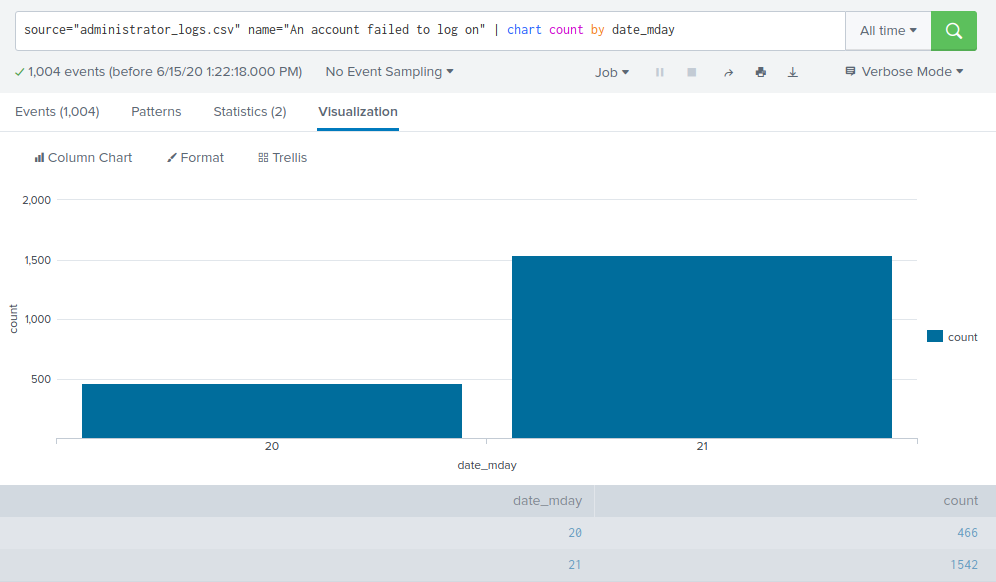


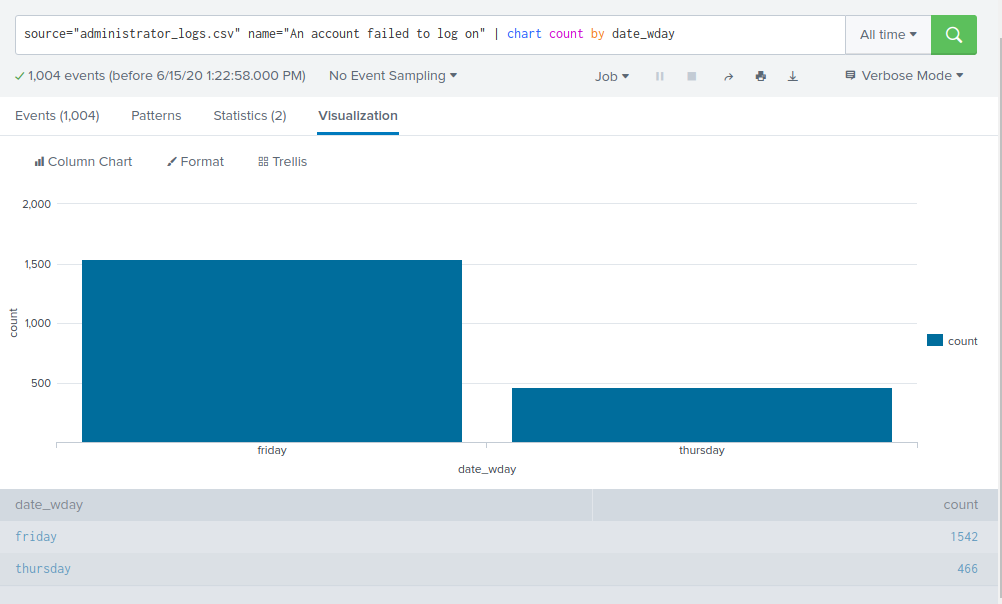


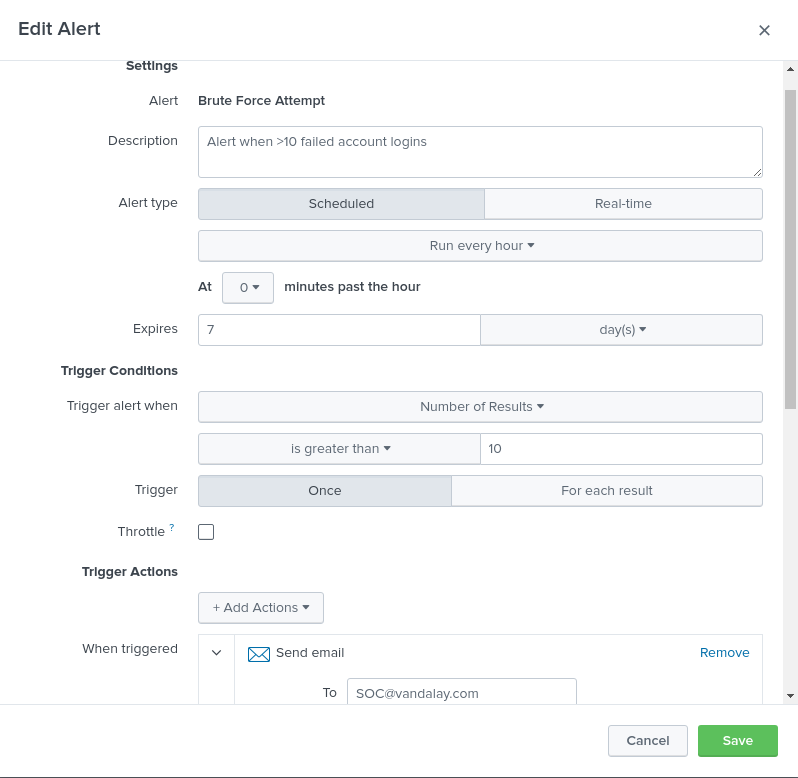


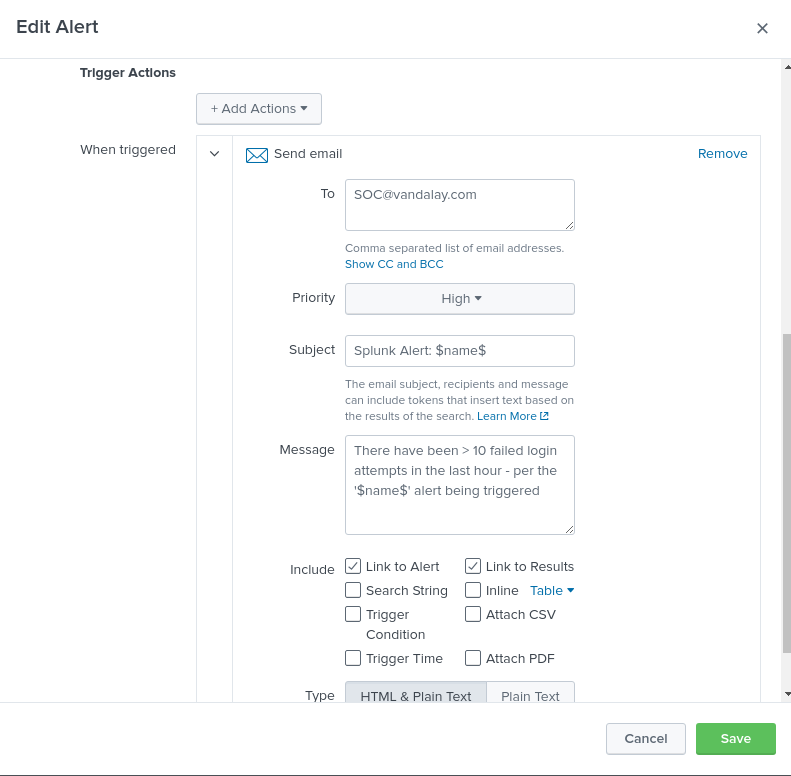


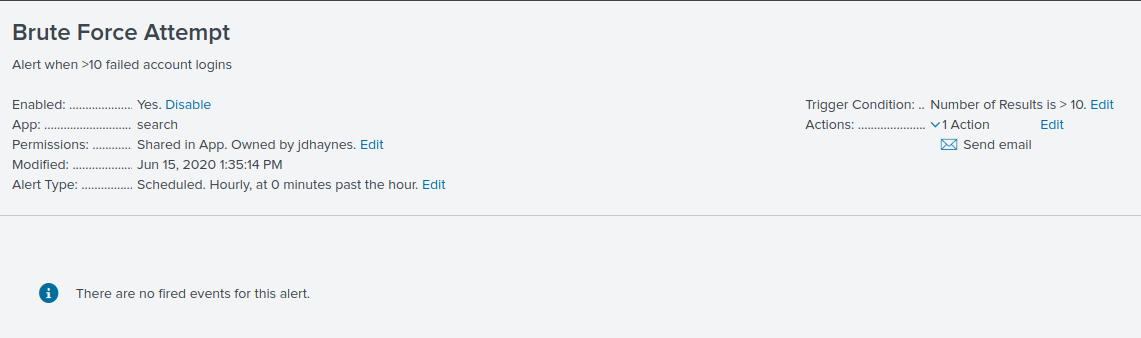












* Brute force attack on Thursday, Feb 20 around 6 a.m. and continued through 2 separate days:
  + Feb 20 – Thursday, there were 223 events. The events occurred at a rate of 8 to 20 failed logins per hour, perhaps kept low to avoid detection.
  + Feb 21 – Friday, there were 771 total events. The hourly failure rate continued to be ~ 10 to 20. The failure rate ramped up considerably starting with 34 events at 6 a.m., followed by > 100 events per hour between 9 am – 2 pm
* Set alert to send email to [SOC@vandalay.com](mailto:SOC@vandalay.com) when > 10 failed logins occurred within one hour. I considered lowering the threshold to > 5 but was concerned about creating alert fatigue.
* I based these conclusions on the data above and these additional searches I performed below:
  + source="administrator\_logs.csv" name="an account failed to log on" date\_wday=thursday
  + source="administrator\_logs.csv" name="an account failed to log on" date\_wday=Friday
  + source="administrator\_logs.csv" name="an account failed to log on" date\_wday=saturday

THE END