**Splunk**

## **Vandalay Industries Monitoring Activity Instructions**

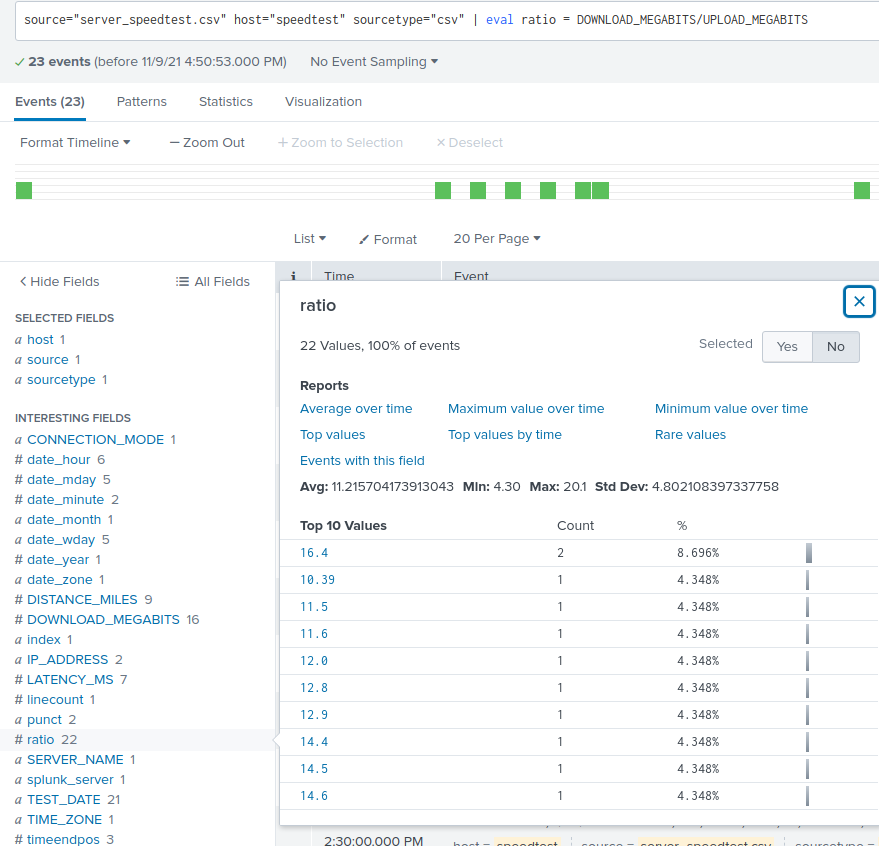
### **Step 1: The Need for Speed**

**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.

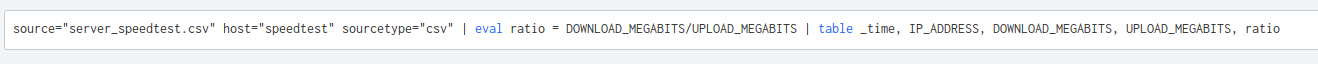
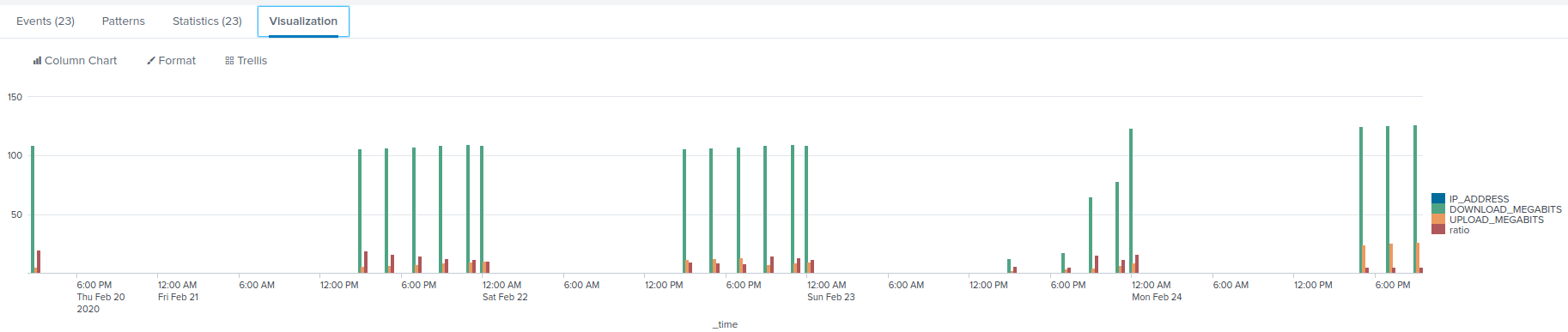
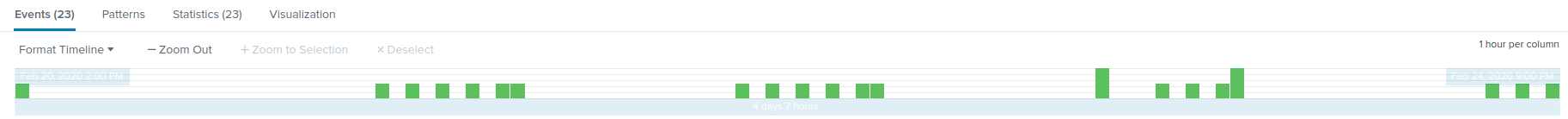
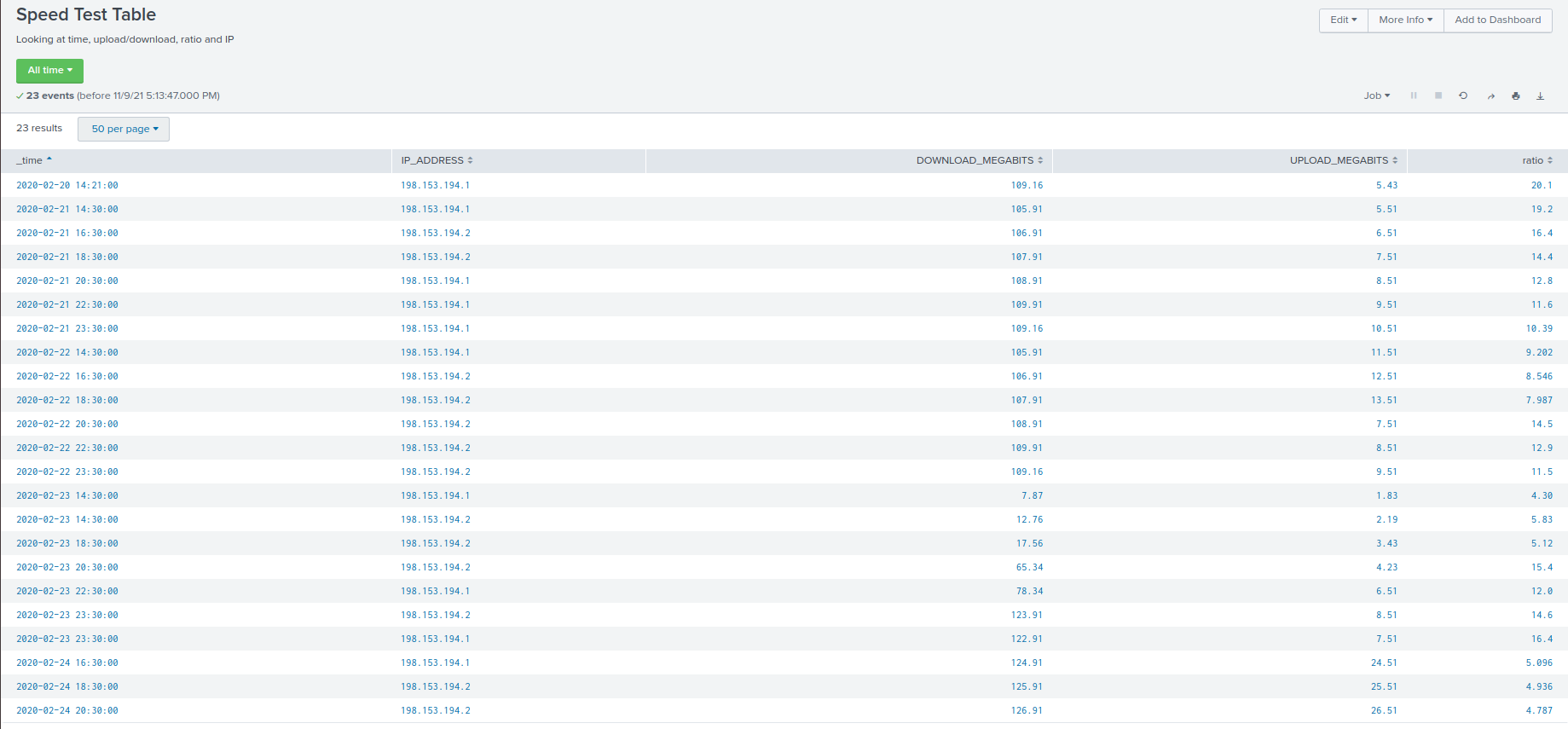
**Task:** Create a report to determine the impact that the DDOS attack had on download and upload speed. Additionally, create an additional field to calculate the ratio of the upload speed to the download speed.

Uploading ‘Speed Test’ file then using the eval command to create a field called ratio that shows the ratio between the upload and download speeds. Formatting the ratio is: *| eval new\_field\_name = 'fieldA' / 'fieldB'*



Next I will create a report using the Splunk's table command to display the following fields in a statistics report. I’ll use the following format for the table command: *| table fieldA, fieldB, fieldC*

* + \_time
  + IP\_ADDRESS
  + DOWNLOAD\_MEGABITS
  + UPLOAD\_MEGABITS
  + ratio

Based on the report created and other tools in Splunk, we find the approximate date and time of the attack occurred on 02/23/2020 at 2:30pm and lasted until 02/23/2020 at 11:30pm. The systems took about 9 hours to recover.

### **Step 2: Are We Vulnerable?**

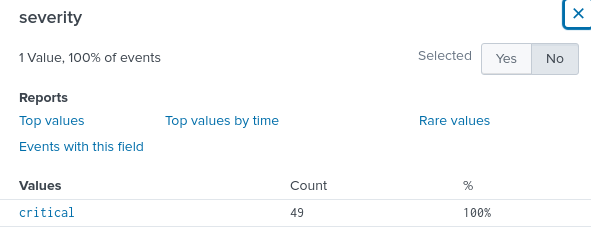
**Background:** Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

**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.

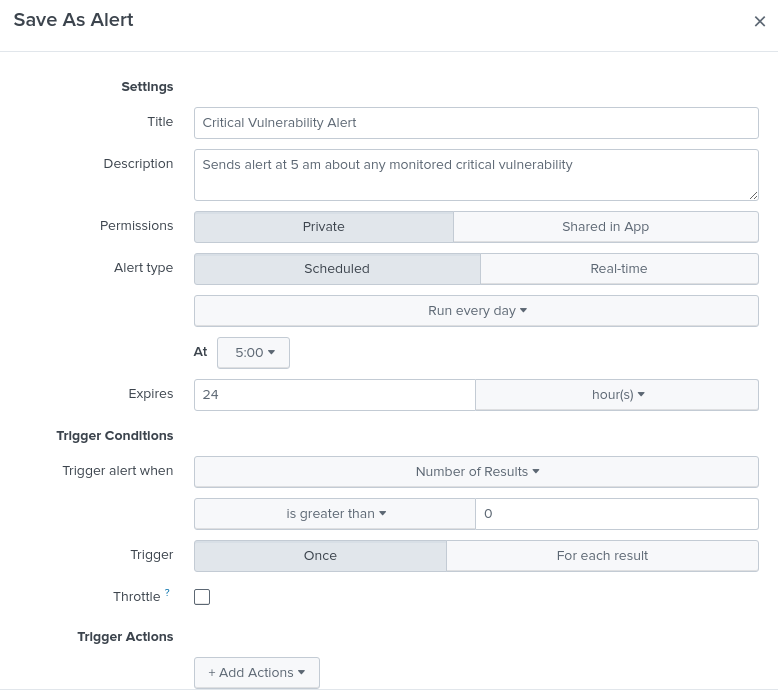
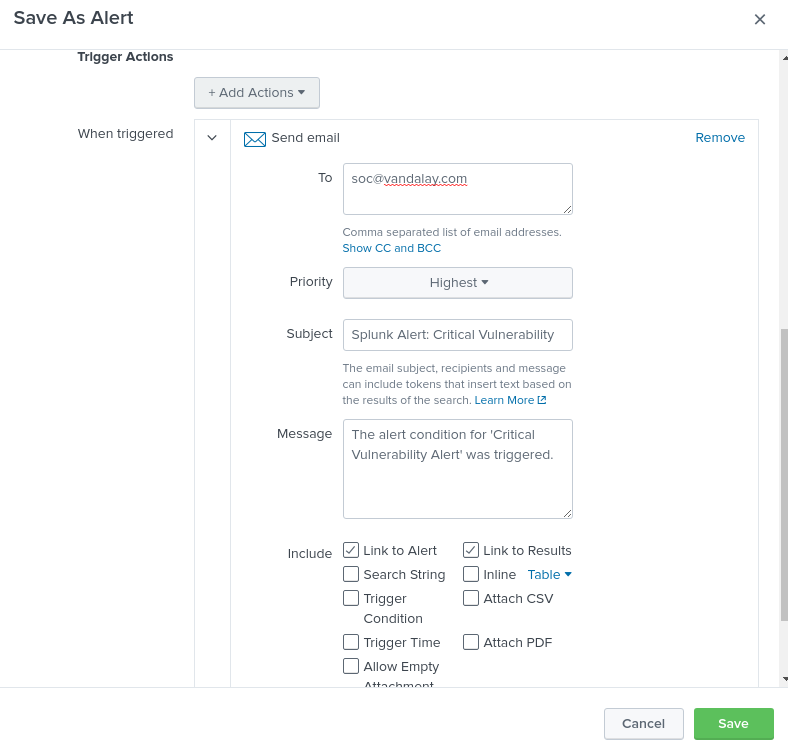
I have uploaded our Nessus file and determined how many critical vulnerabilities exist on the customer data server using the below information:

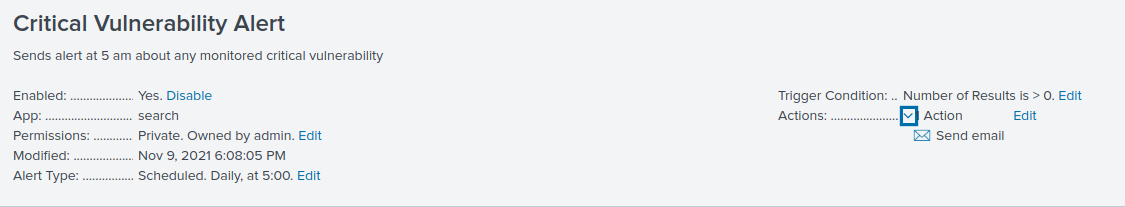
* + The database server IP is 10.11.36.23.
  + The field that identifies the level of vulnerabilities is severity.



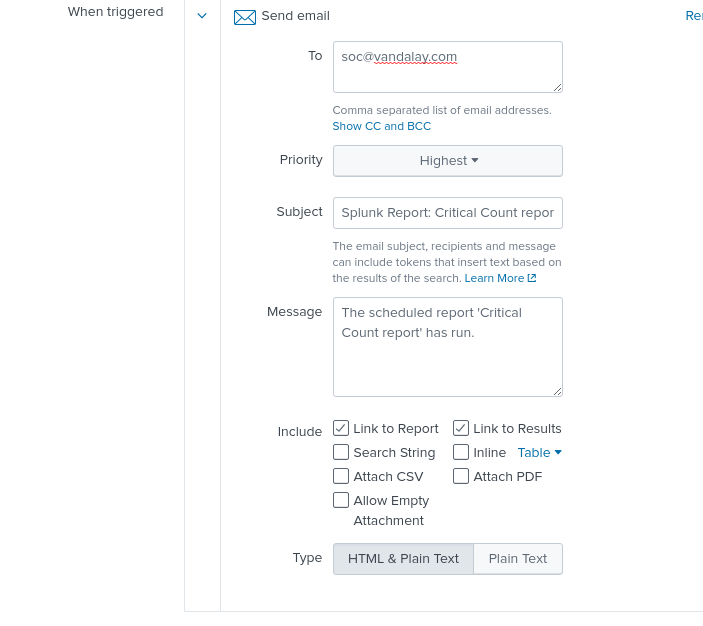
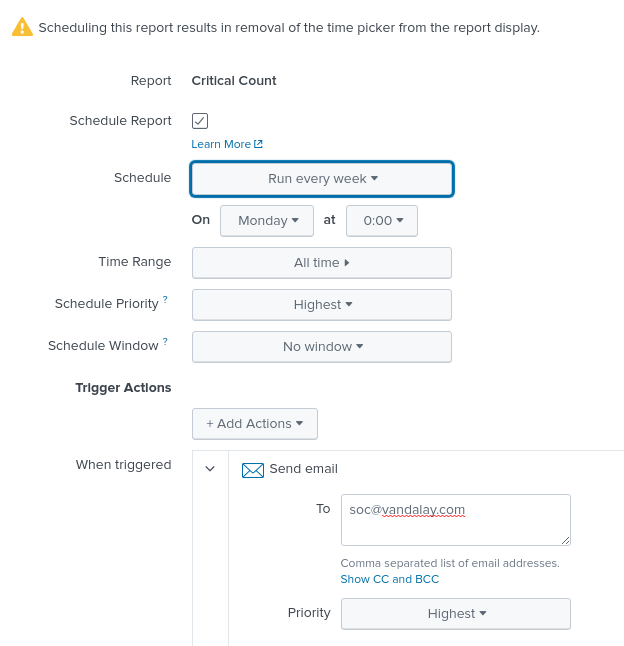


I then built an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, the alert is emailed to [soc@vandalay.com](mailto:soc@vandalay.com)

.



I’ve also created a scheduled email sending the critical vulnerability report every week for additional monitoring and information:



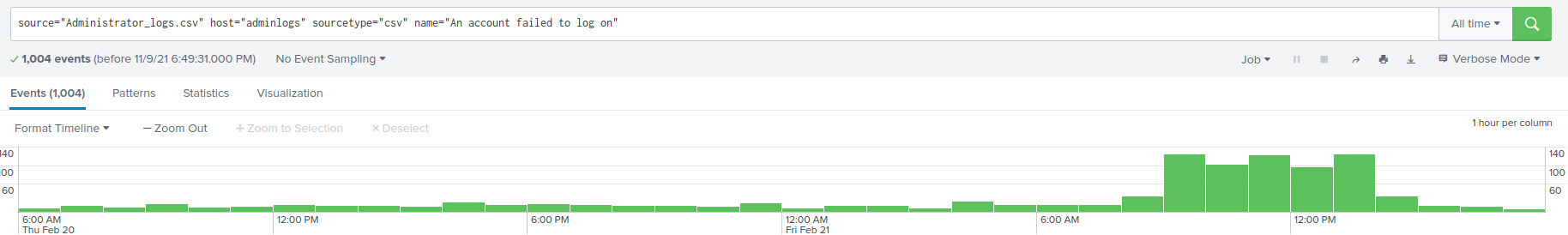
### **Step 3: Drawing the (base)line**

**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.

I have uploaded the admin logs and found out when the brute force attack occurred using the below information to make the event easier to identify.

* + - Look for the name field to find failed logins.



The attack started to spike at 9 am on 02/21/2020. The attack started to slow down after 1 pm the same day. The attack lasted about 4 hours.

I have determined a baseline of normal activity and a threshold that would alert if a brute force attack is occurring to be about 15.

I then designed an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.

