## **Vandalay Industries Monitoring Activity Instructions**

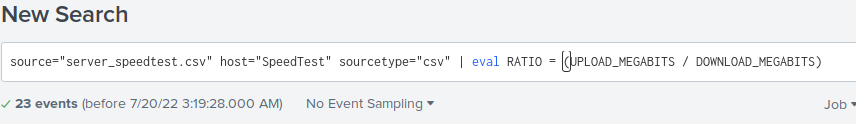
### **Step 1: The Need for Speed**

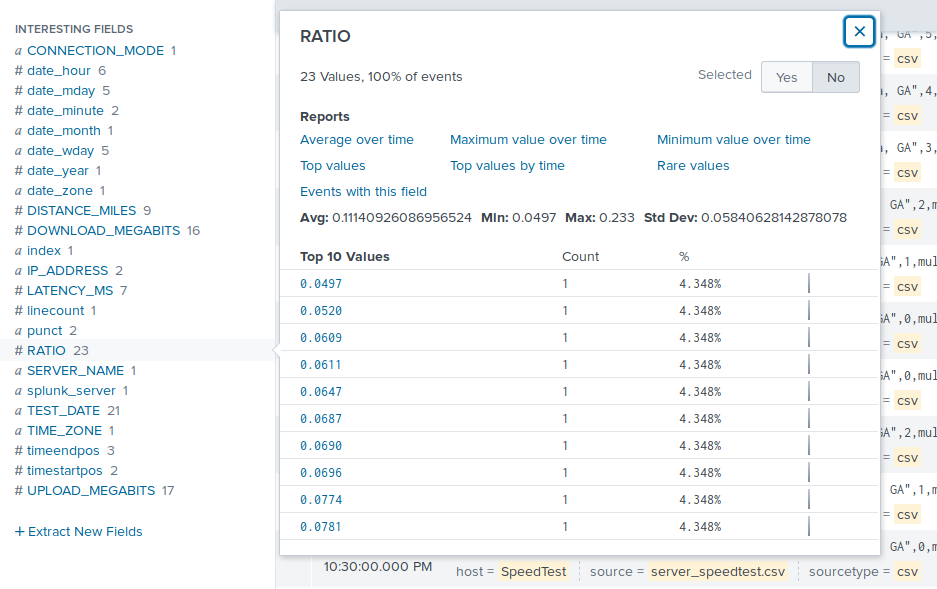
**Background**: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandaly has been experiencing DDOS attacks against their web servers.

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.

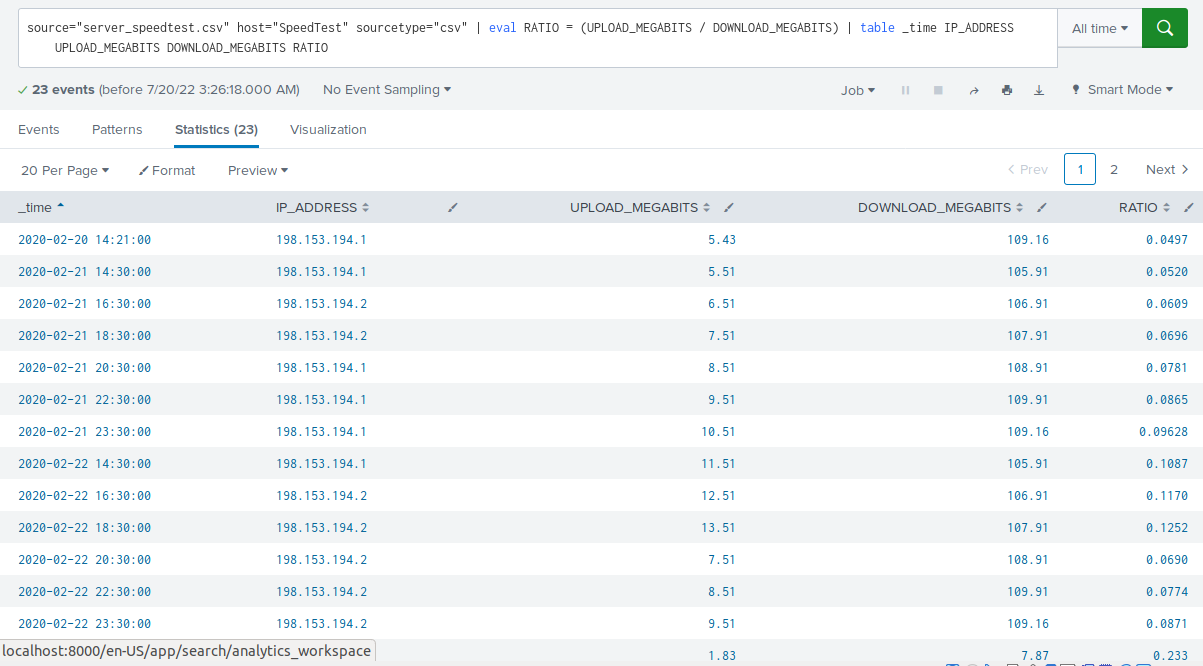
**Task:** Create a report to determine the impact that the DDOS attack had on download and upload speed. Additionally, create an additional field to calculate the ratio of the upload speed to the download speed.

1. Upload the file of the system speeds around the time of the attack.
2. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.

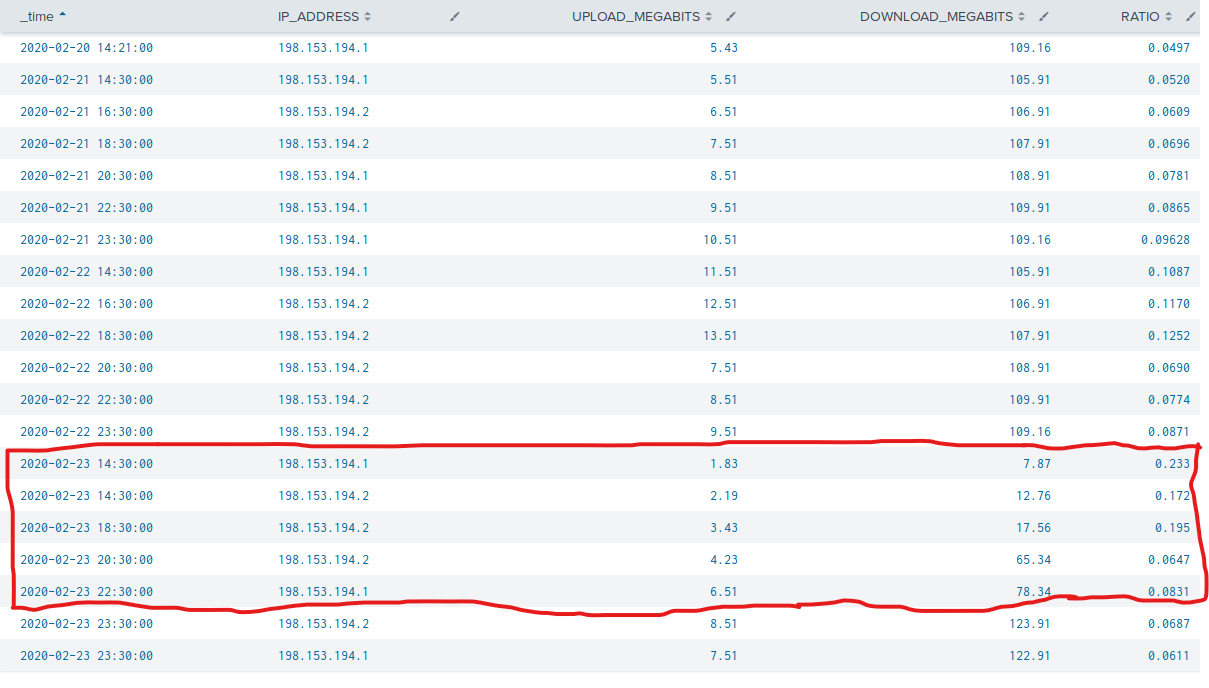




1. Create a report using the Splunk's table command to display the following fields in a statistics report:  
   * \_time
   * IP\_ADDRESS
   * DOWNLOAD\_MEGABITS
   * UPLOAD\_MEGABITS
   * ratio



1. Answer the following questions:



* + Based on the report created, what is the approximate date and time of the attack?
    1. Answer: **The approximate date and time of the attack is 2020-02-23 at 14:30:00 (2:30PM) to 22:30:00 (10:30PM). This is when download speeds appear to be drastically reduced.**
  + How long did it take your systems to recover?
    1. Answer: **It took approximately 8 to 9 hours to recover**

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

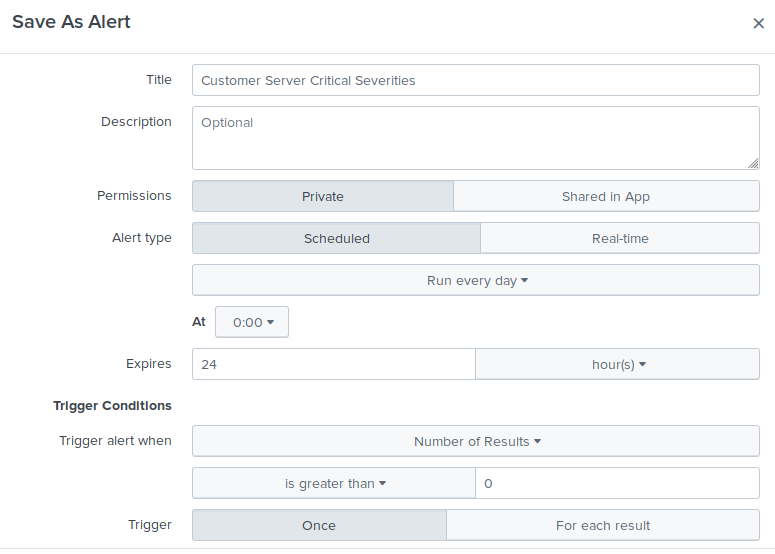
**Background:** Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

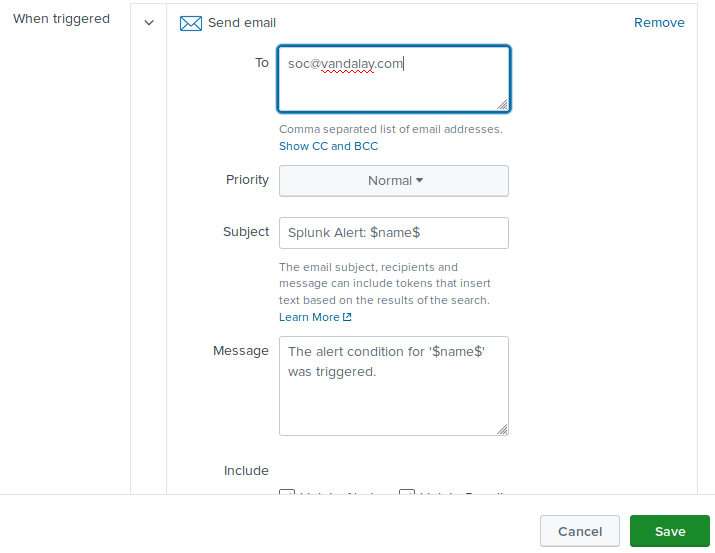
**Task:** Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

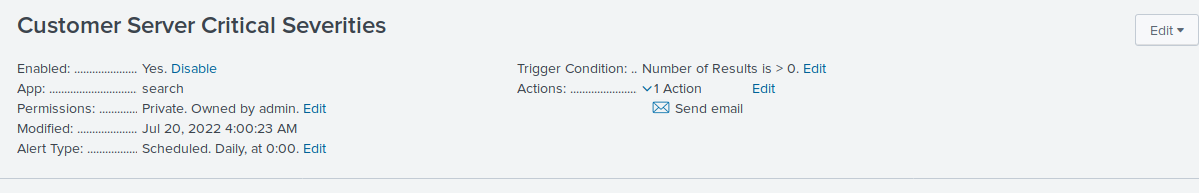
1. Upload the file from the Nessus vulnerability scan.
2. Create a report that shows the count of critical vulnerabilities from the customer database server.  
   * The database server IP is 10.11.36.23.
   * The field that identifies the level of vulnerabilities is severity.



1. Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to soc@vandalay.com.





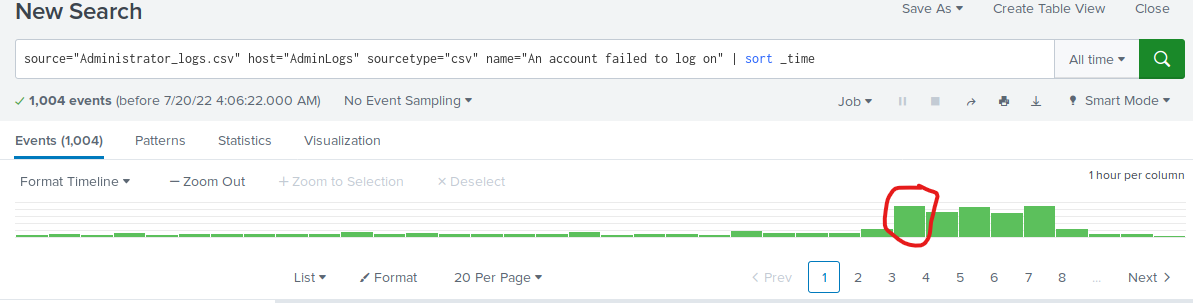


### **Step 3: Drawing the (base)line**

**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.

1. Upload the administrator login logs.
2. When did the brute force attack occur?
   * Answer: **The attack occurred at approximately 9AM to 1PM on Friday, February 21, 2020**



1. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.
   * Answer: **Based on the graph above, I determined a threshold to be 35. During the attack, failed logins numbered nearly tripled. Before and after the attack, failed logins numbered less than 35. Less than 35 failed logins would be the baseline, anything above that should trigger an alert for further review.**
2. Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.

