## **Jacob Schoellkopf**

## **Unit 18 Homework: Let's go Splunking!**

### **Scenario**

You have just been hired as an SOC Analyst by Vandalay Industries, an importing and exporting company.

* Vandalay Industries uses Splunk for their security monitoring and have been experiencing a variety of security issues against their online systems over the past few months.
* You are tasked with developing searches, custom reports and alerts to monitor Vandalay's security environment in order to protect them from future attacks.

### **System Requirements**

You will be using the Splunk app located in the Ubuntu VM.

### **Your Objective**

Utilize your Splunk skills to design a powerful monitoring solution to protect Vandaly from security attacks.

After you complete the assignment you are asked to provide the following:

* Screen shots where indicated.
* Custom report results where indicated.

### **Topics Covered in This Assignment**

* Researching and adding new apps
* Installing new apps
* Uploading files
* Splunk searching
* Using fields
* Custom reports
* Custom alerts

Let's get started!

## **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 following file of the system speeds around the time of the attack.  
   * Speed Test File
2. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.  
   * Command used: **| eval ratio=(DOWNLOAD\_MEGABITS/UPLOAD\_MEGABITS)**
   * Image: **Scenario**

You have just been hired as an SOC Analyst by Vandalay Industries, an importing and exporting company.

* Vandalay Industries uses Splunk for their security monitoring and have been experiencing a variety of security issues against their online systems over the past few months.
* You are tasked with developing searches, custom reports and alerts to monitor Vandalay's security environment in order to protect them from future attacks.

### **System Requirements**

You will be using the Splunk app located in the Ubuntu VM.

### **Your Objective**

Utilize your Splunk skills to design a powerful monitoring solution to protect Vandaly from security attacks.

After you complete the assignment you are asked to provide the following:

* Screen shots where indicated.
* Custom report results where indicated.

### **Topics Covered in This Assignment**

* Researching and adding new apps
* Installing new apps
* Uploading files
* Splunk searching
* Using fields
* Custom reports
* Custom alerts

Let's get started!

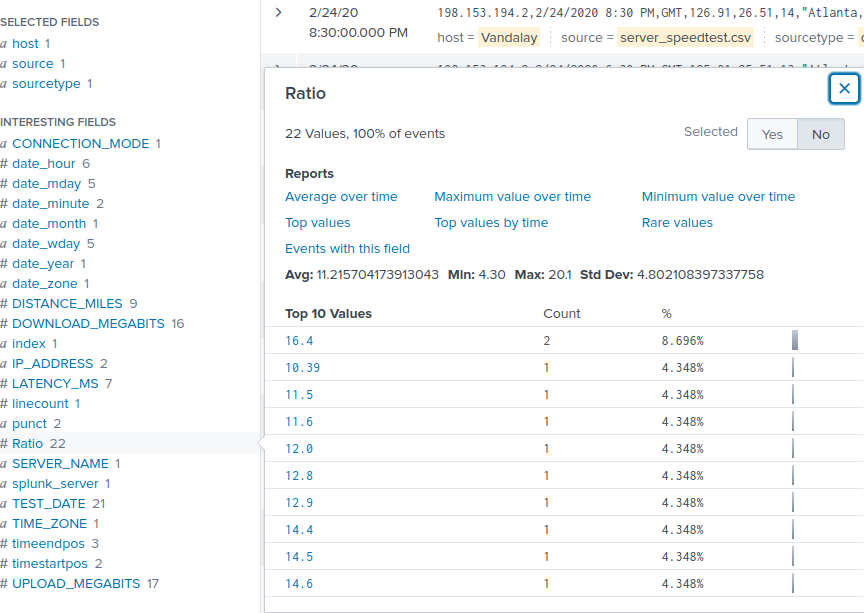
## **Vandalay Industries Monitoring Activity Instructions**

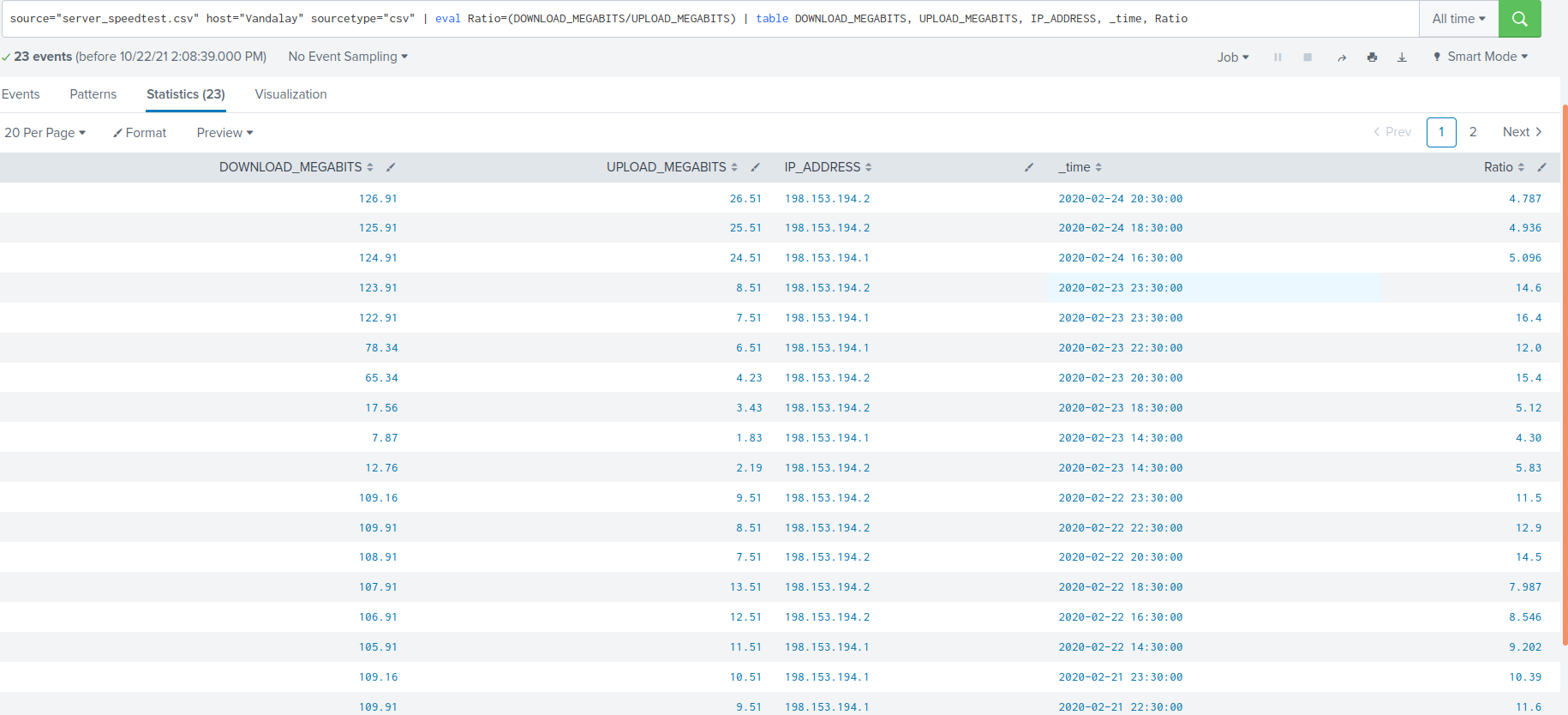
### **Step 1: The Need for Speed**

**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.

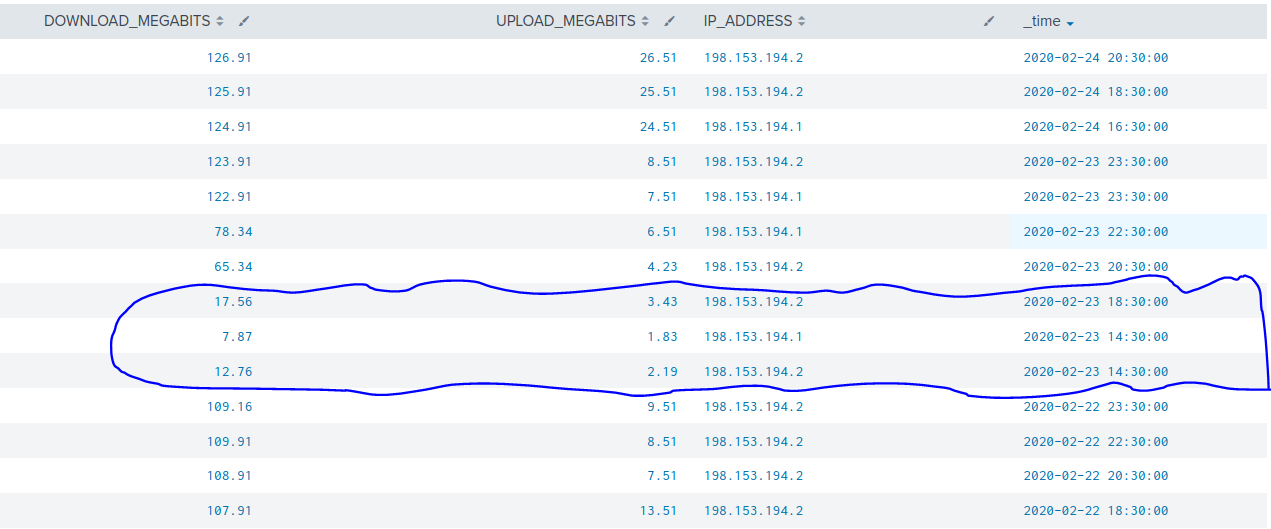
**Task:** Create a report to determine the impact that the DDOS attack had on download and upload speed. Additionally, create an additional field to calculate the ratio of the upload speed to the download speed.

1. Upload the following file of the system speeds around the time of the attack.  
   * Speed Test File
2. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.  
   * Command used: **| eval ratio=(DOWNLOAD\_MEGABITS/UPLOAD\_MEGABITS)**
3. Image: 
4. 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



Command and Results: The command used is **| table DOWNLOAD\_MEAGABITS, UPLOAD\_MEGABITS, IP\_ADDRESS, \_time, ratio**

1. Answer the following questions:

**Based on the report created, what is the approximate date and time of the attack?** After I arranged the time column to show me the events in reverse chronological order, I identified the following:

As illustrated above, the downloaded megabits from 2:30 pm on February 23rd to 6:30 pm on February 23rd had significantly less downloaded megabits, and this is most likely the timeframe that the attack occurred.

* + **How long did it take your systems to recover?** As seen above, the downloaded megabits started picking back up at 8:30 pm on February 23rd, but did not fully recover until 11:30 pm on February 23rd. The last time the systems were functioning properly was on February 22nd at 11:30 pm. This means it took 24 hours for the system to fully recover. That is unacceptable and while this may be an unpopular opinion, the SOC team needs to start operating at a 24 hour schedule in order to detect and prevent similar attacks such as the one being illustrated from occurring.

Submit a screenshot of your report and the answer to the questions above.

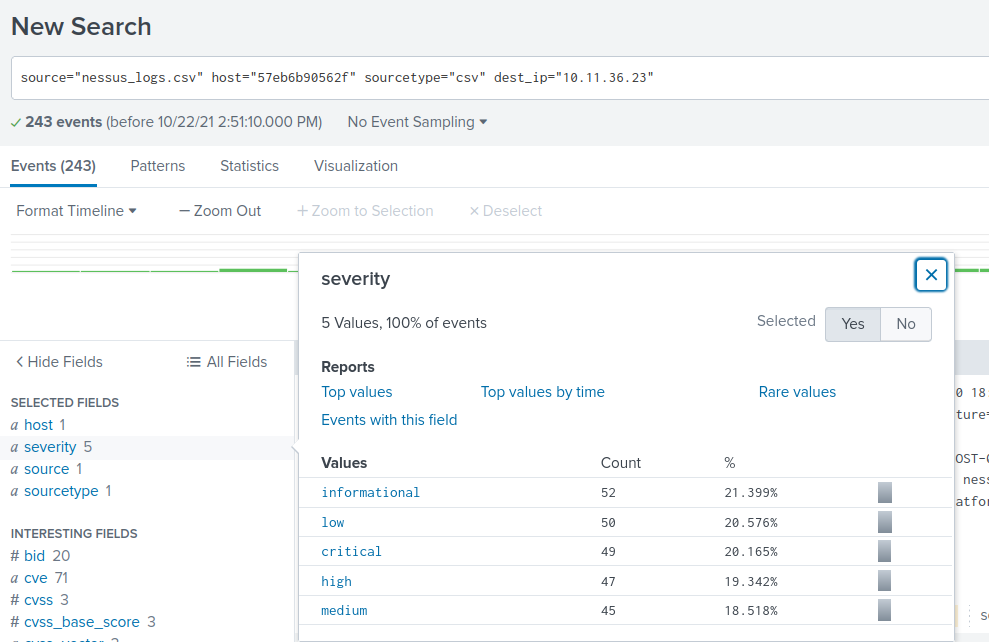
### **Step 2: Are We Vulnerable?**

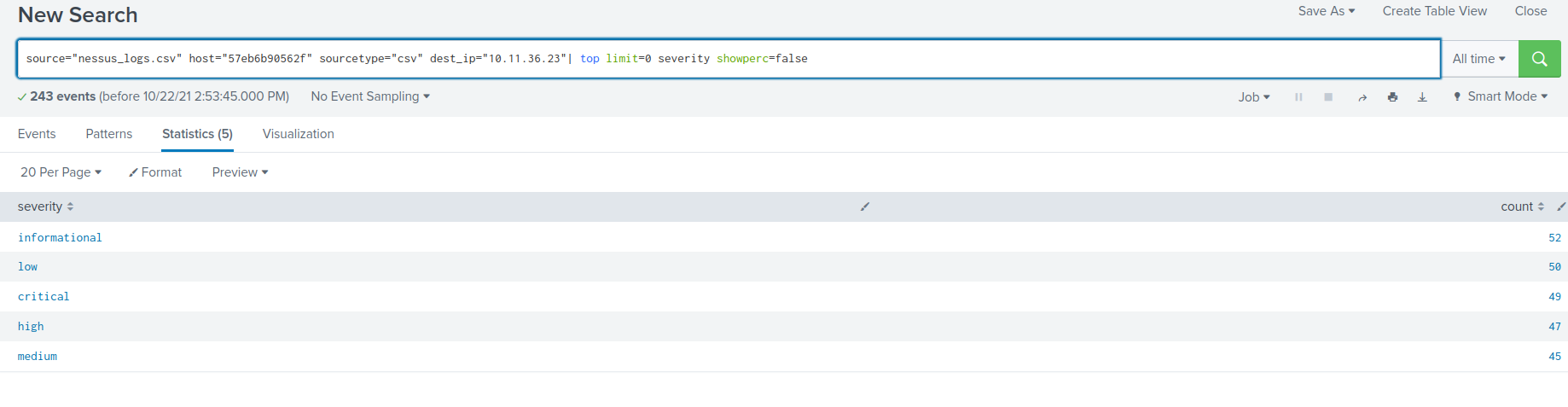
**Background:** Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

* For more information on Nessus, read the following link:<https://www.tenable.com/products/nessus>

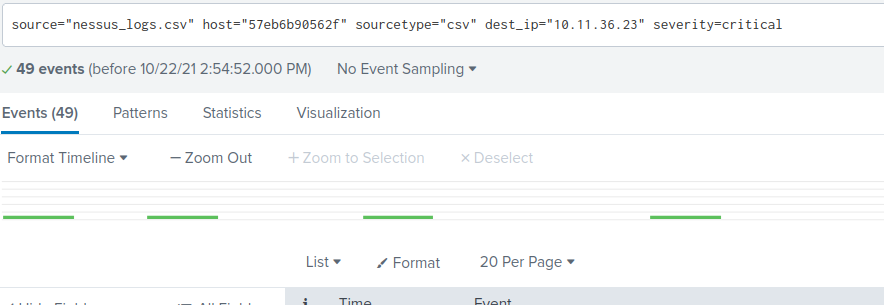
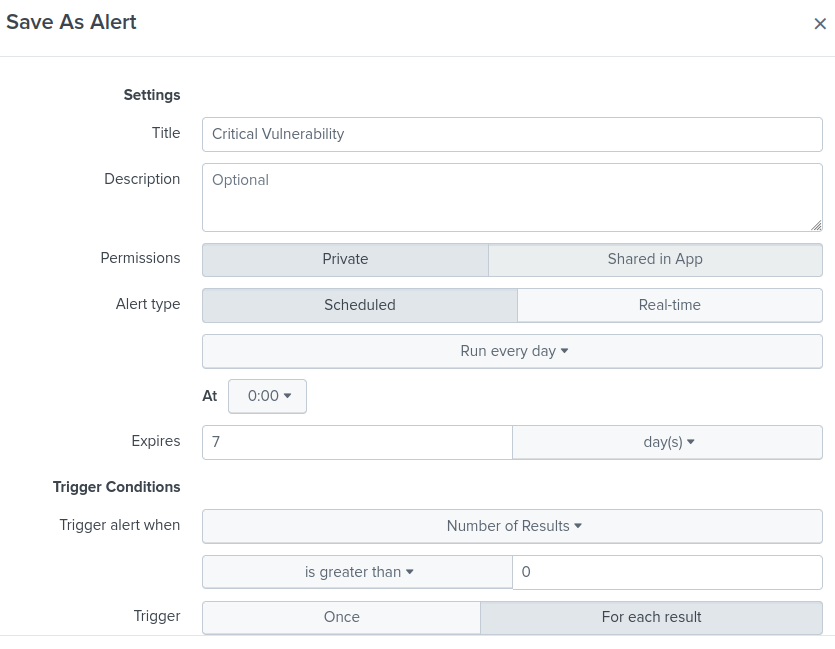
**Task:** Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

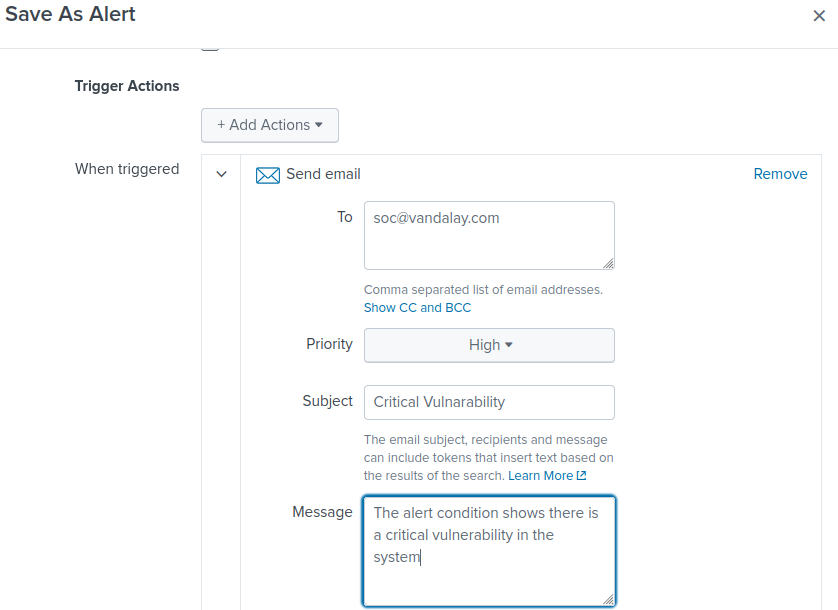
1. Upload the following file from the Nessus vulnerability scan.  
   * Nessus Scan Results
2. Create a report that shows the count of critical vulnerabilities from the customer database server.
   * The database server IP is 10.11.36.23.
   * The field that identifies the level of vulnerabilities is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

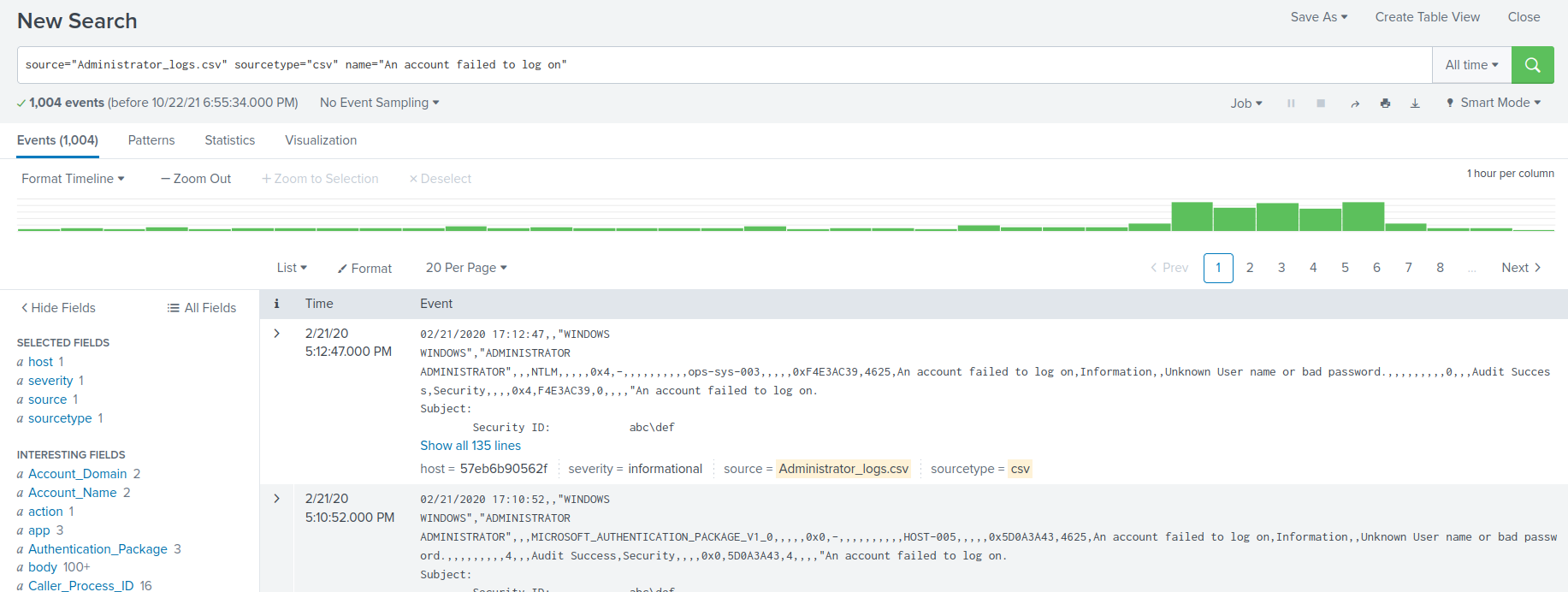


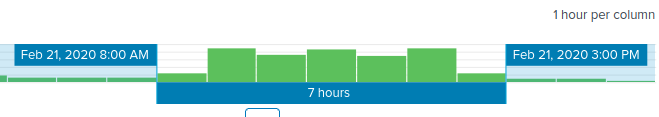
Submit a screenshot of your report and a screenshot of proof that the alert has been created.

### **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.

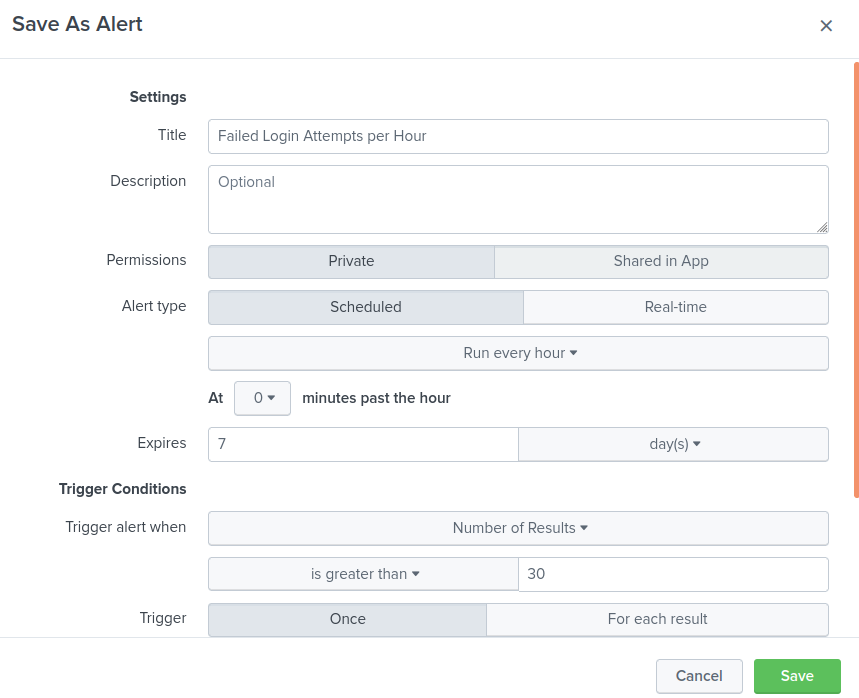
**Task:** Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.

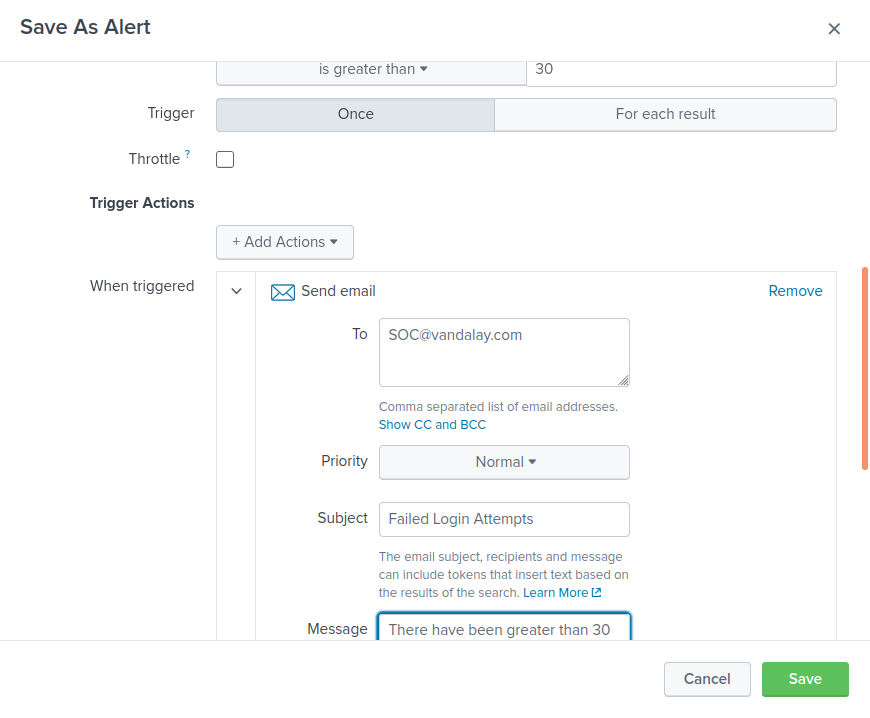
1. Upload the administrator login logs.  
   * Admin Logins
2. When did the brute force attack occur?  
   



This attack lasted for 7 hours. Make sure this department uses a maximum of password attempts, blocks IP addresses that attempt to log on more than these attempts, and that we are using multi-factor. Also, since brute force attacks are web based attacks, we need to make sure that we have strong input validation. This could prevent other attacks such as XSS or SQL injections.

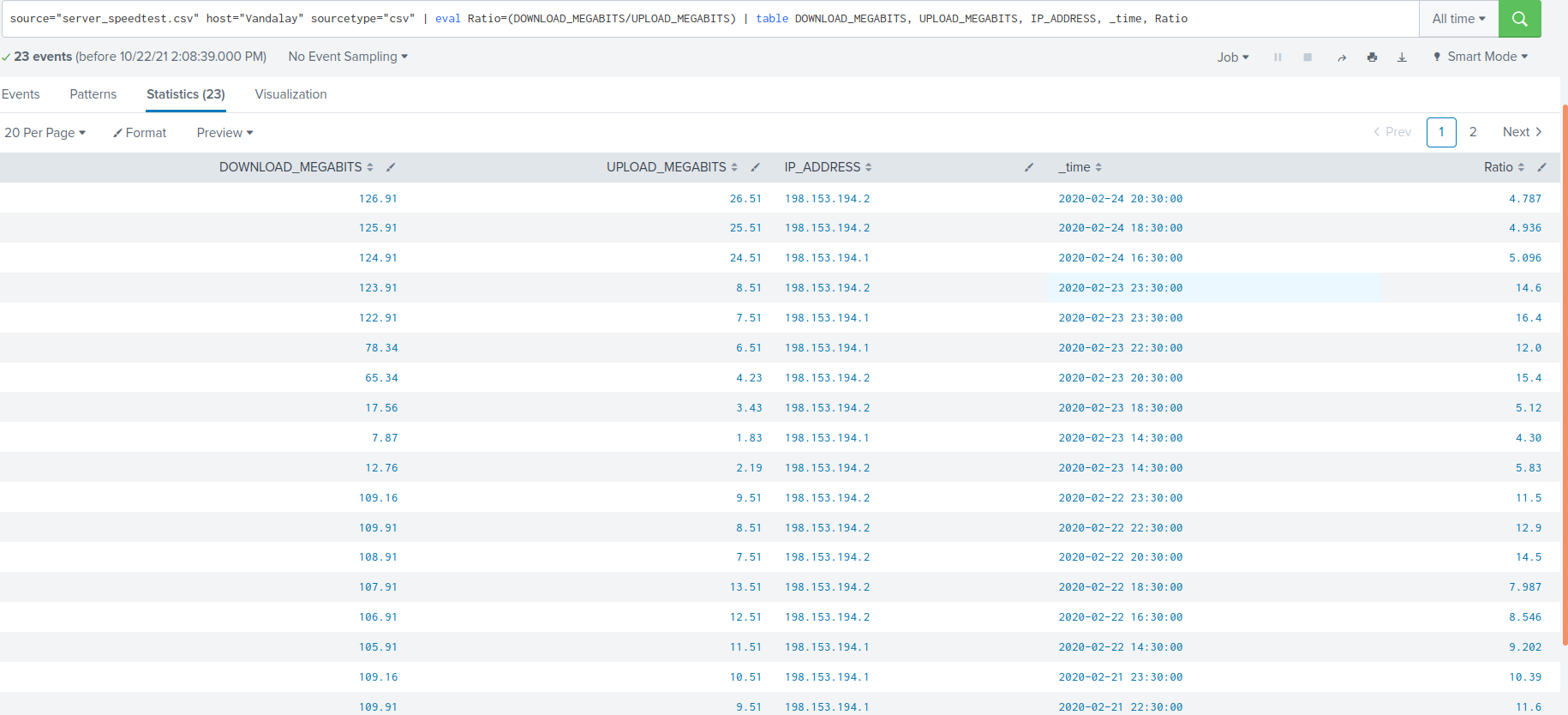
* + Hints:
    - Look for the name field to find failed logins.
    - Note the attack lasted several hours.

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

1. Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.  
   

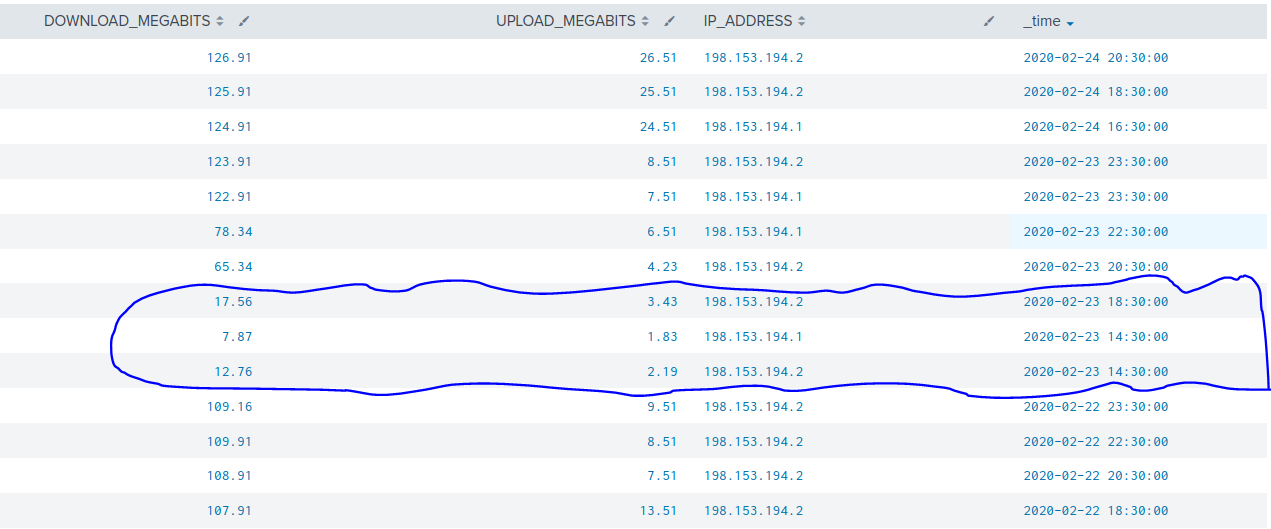
Submit the answers to the questions about the brute force timing, baseline and threshold. Additionally, provide a screenshot as proof that the alert has been created.

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



Command and Results: The command used is **| table DOWNLOAD\_MEAGABITS, UPLOAD\_MEGABITS, IP\_ADDRESS, \_time, ratio**

1. Answer the following questions:

**Based on the report created, what is the approximate date and time of the attack?** After I arranged the time column to show me the events in reverse chronological order, I identified the following:

As illustrated above, the downloaded megabits from 2:30 pm on February 23rd to 6:30 pm on February 23rd had significantly less downloaded megabits, and this is most likely the timeframe that the attack occurred.

* + **How long did it take your systems to recover?** As seen above, the downloaded megabits started picking back up at 8:30 pm on February 23rd, but did not fully recover until 11:30 pm on February 23rd. The last time the systems were functioning properly was on February 22nd at 11:30 pm. This means it took 24 hours for the system to fully recover. That is unacceptable and while this may be an unpopular opinion, the SOC team needs to start operating at a 24 hour schedule in order to detect and prevent similar attacks such as the one being illustrated from occurring.

Submit a screenshot of your report and the answer to the questions above.

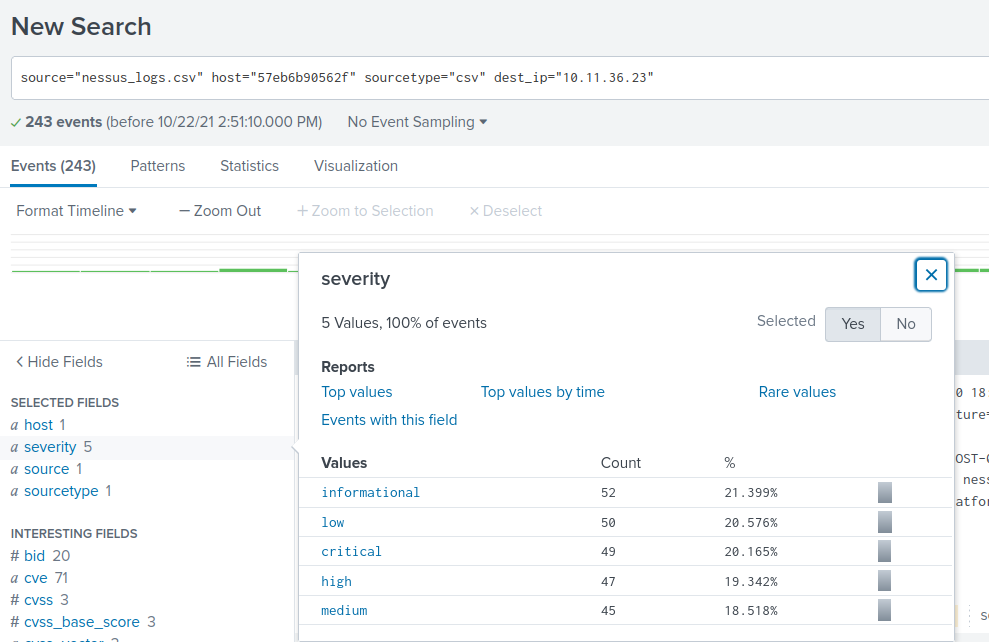
### **Step 2: Are We Vulnerable?**

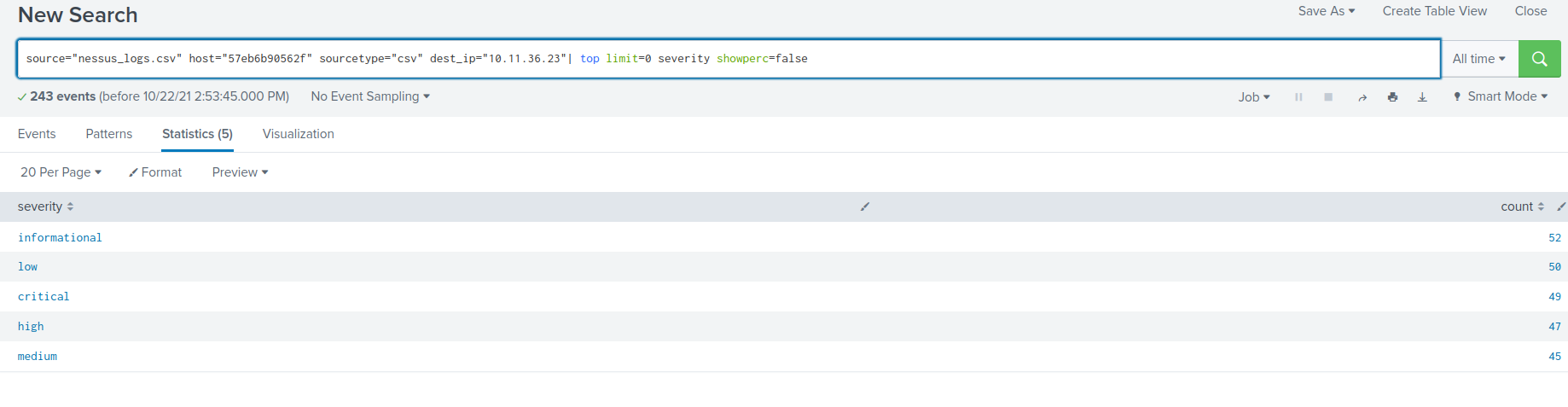
**Background:** Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

* For more information on Nessus, read the following link:<https://www.tenable.com/products/nessus>

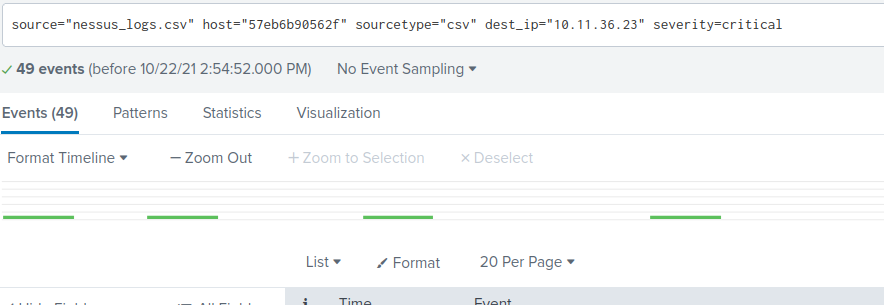
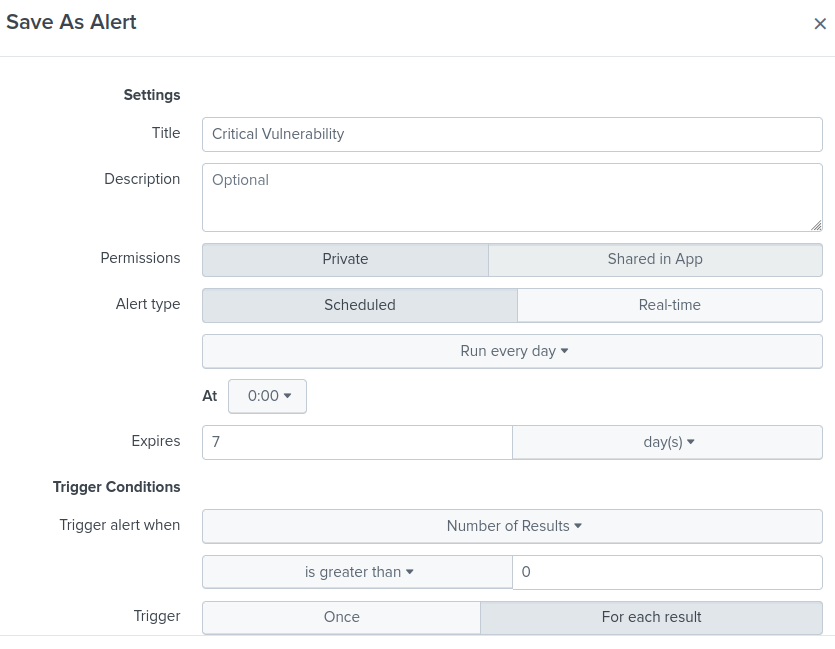
**Task:** Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

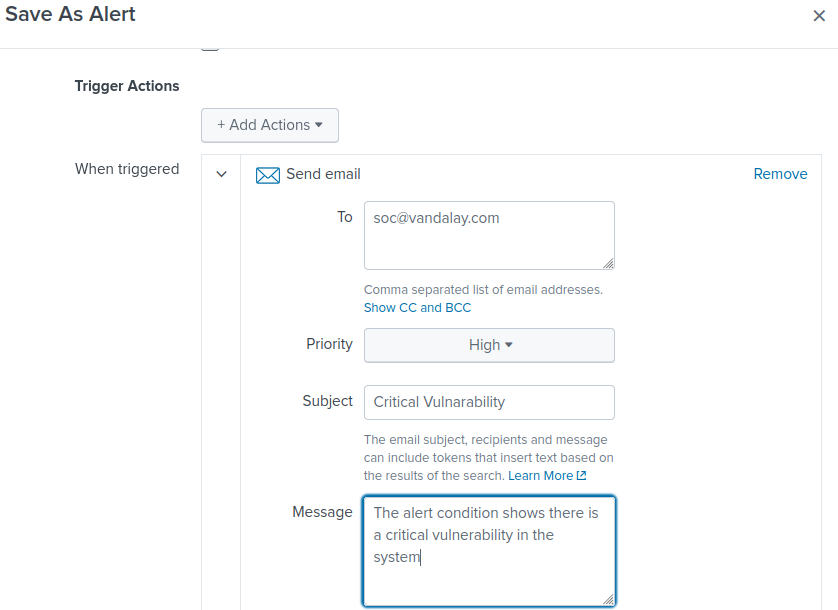
1. Upload the following file from the Nessus vulnerability scan.  
   * Nessus Scan Results
2. Create a report that shows the count of critical vulnerabilities from the customer database server.
   * The database server IP is 10.11.36.23.
   * The field that identifies the level of vulnerabilities is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

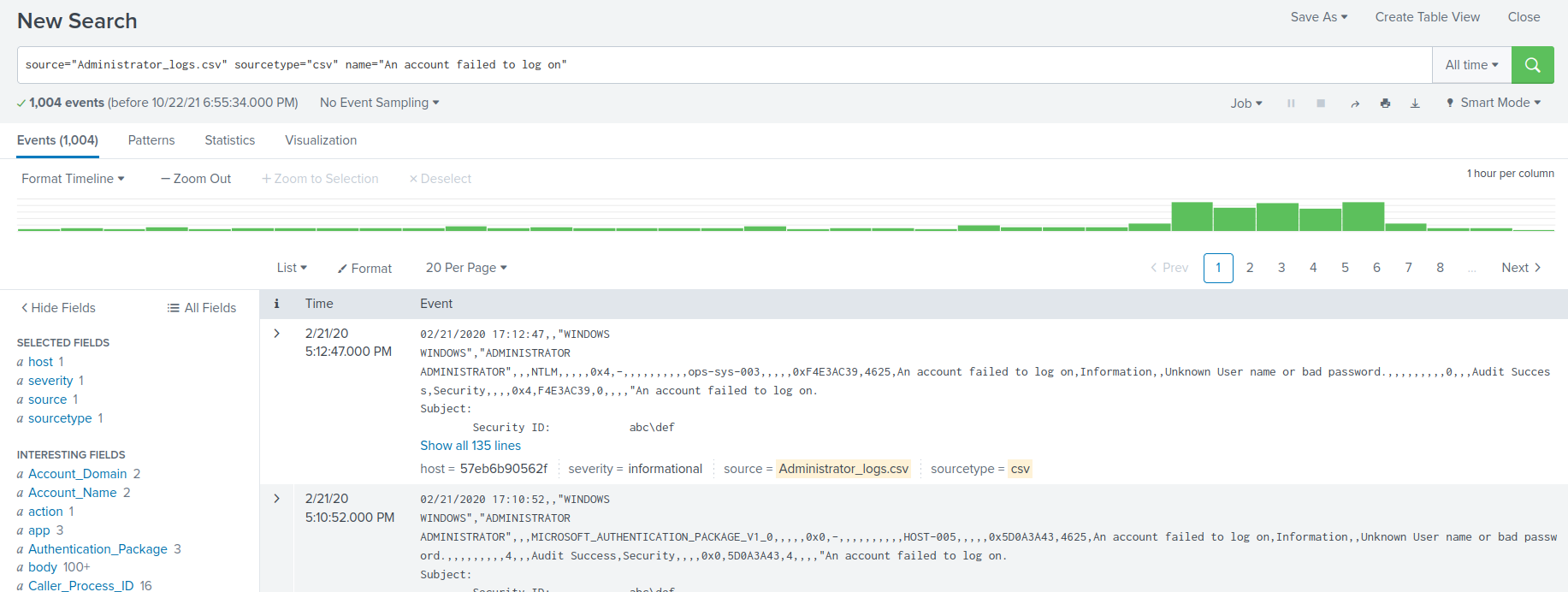


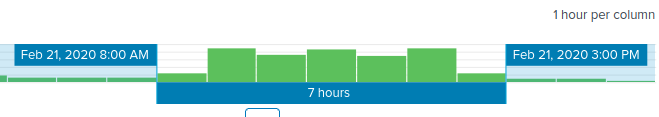
Submit a screenshot of your report and a screenshot of proof that the alert has been created.

### **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.

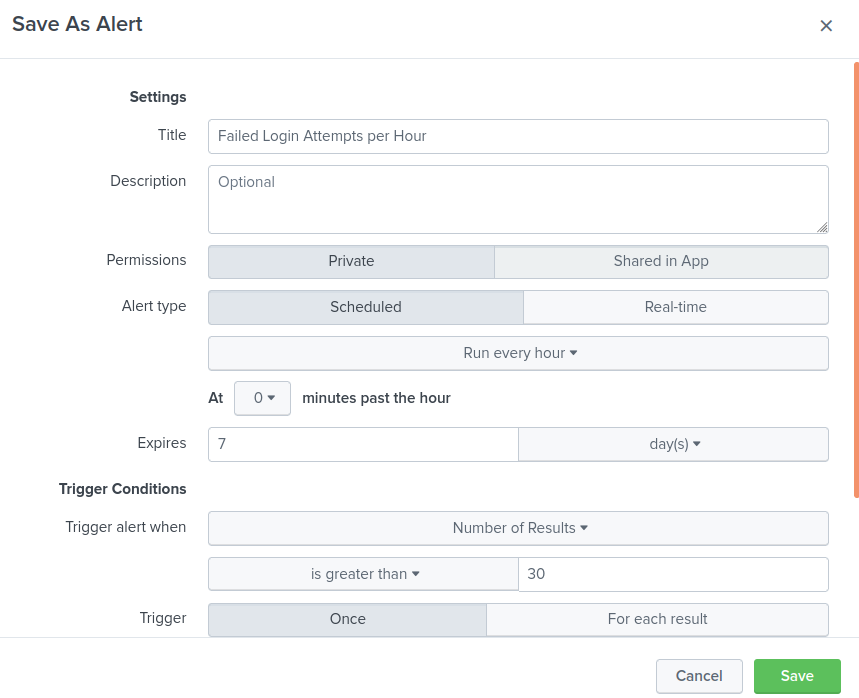
**Task:** Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.

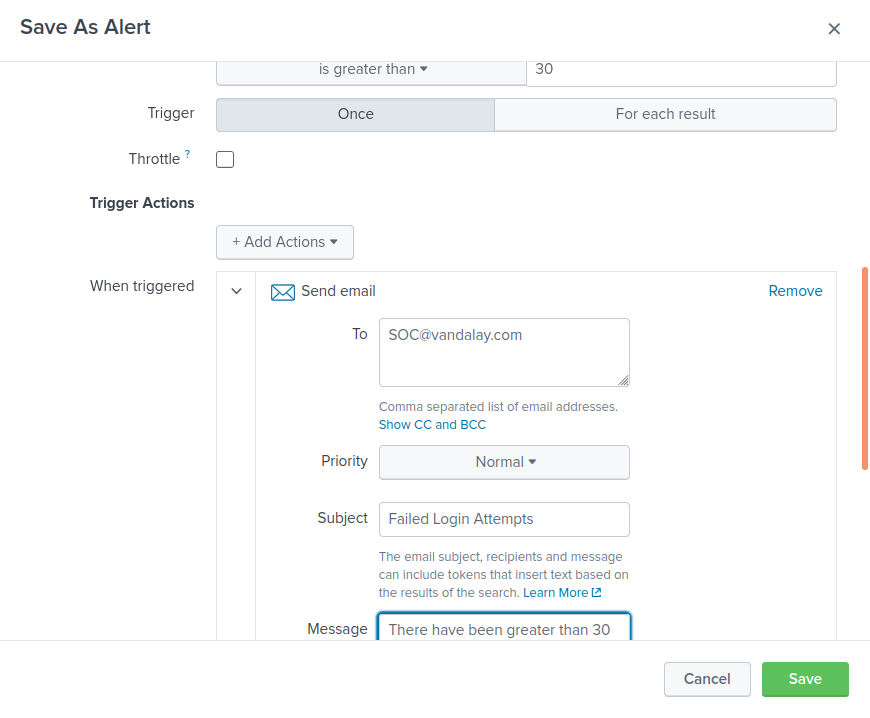
1. Upload the administrator login logs.  
   * Admin Logins
2. When did the brute force attack occur?  
   



This attack lasted for 7 hours. Make sure this department uses a maximum of password attempts, blocks IP addresses that attempt to log on more than these attempts, and that we are using multi-factor. Also, since brute force attacks are web based attacks, we need to make sure that we have strong input validation. This could prevent other attacks such as XSS or SQL injections.

* + Hints:
    - Look for the name field to find failed logins.
    - Note the attack lasted several hours.

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

1. Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.  
   

Submit the answers to the questions about the brute force timing, baseline and threshold. Additionally, provide a screenshot as proof that the alert has been created.