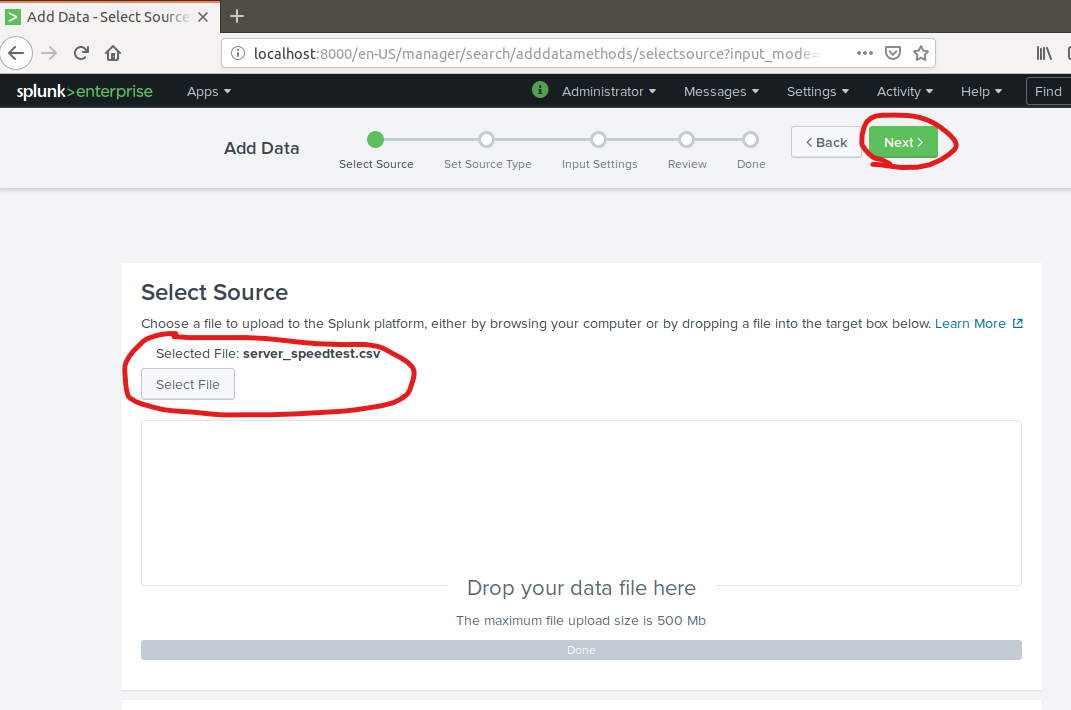
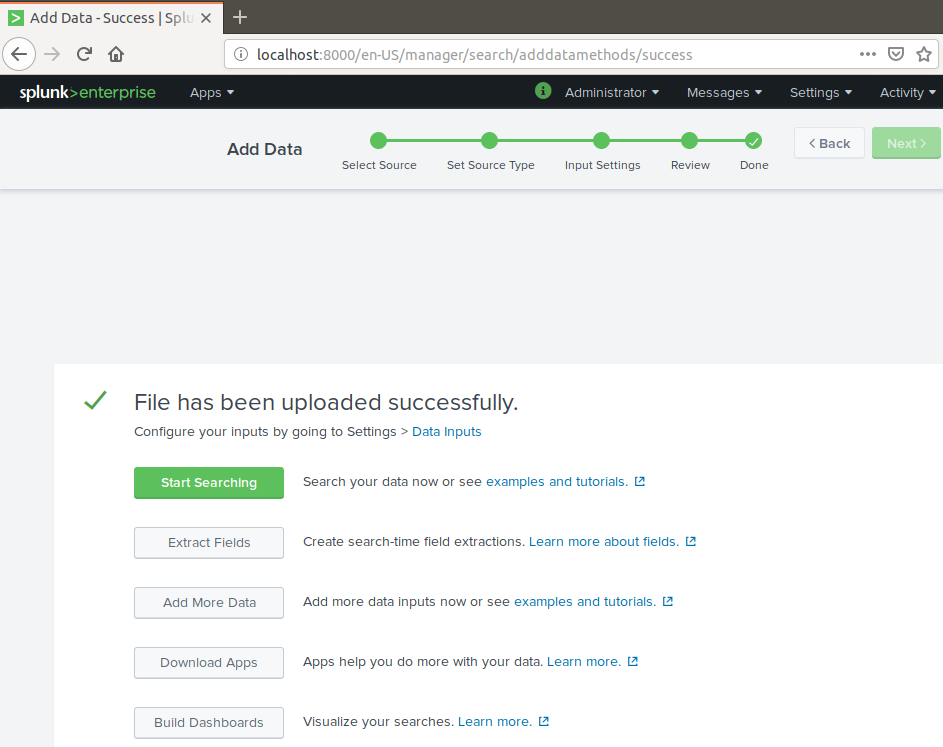
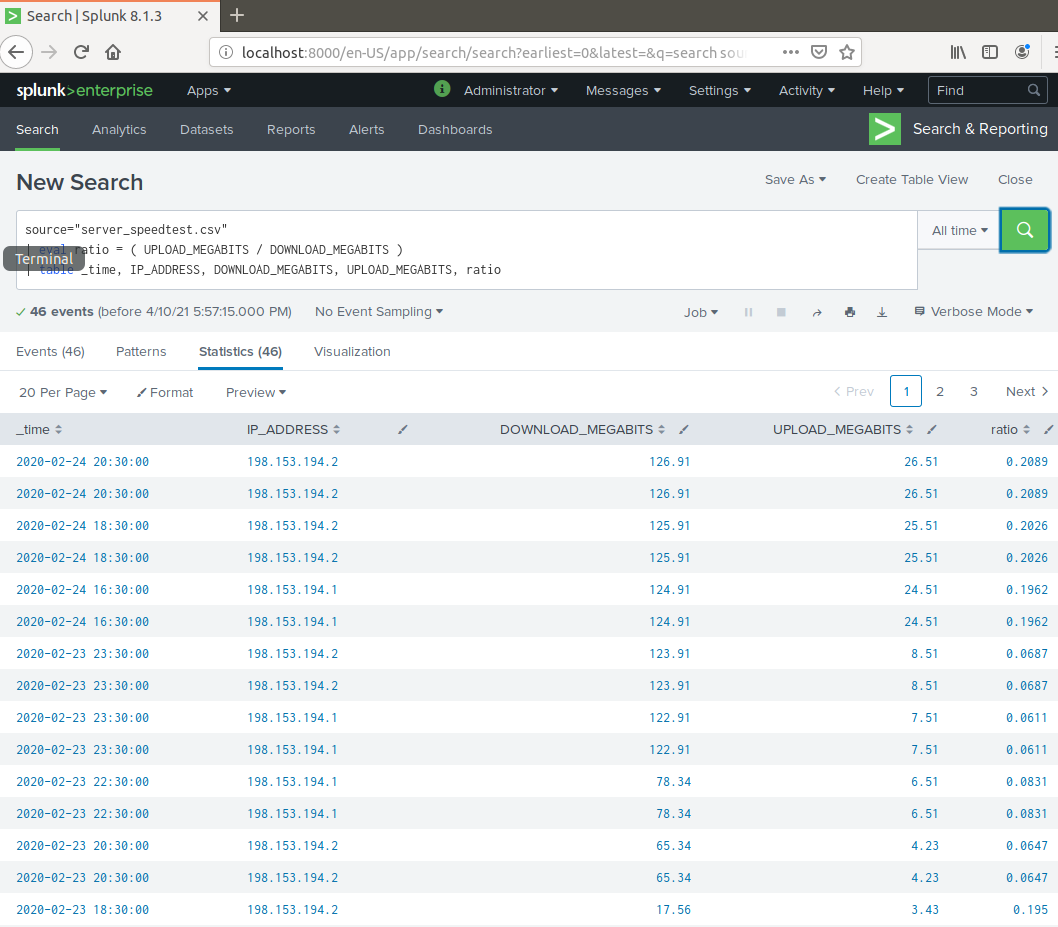
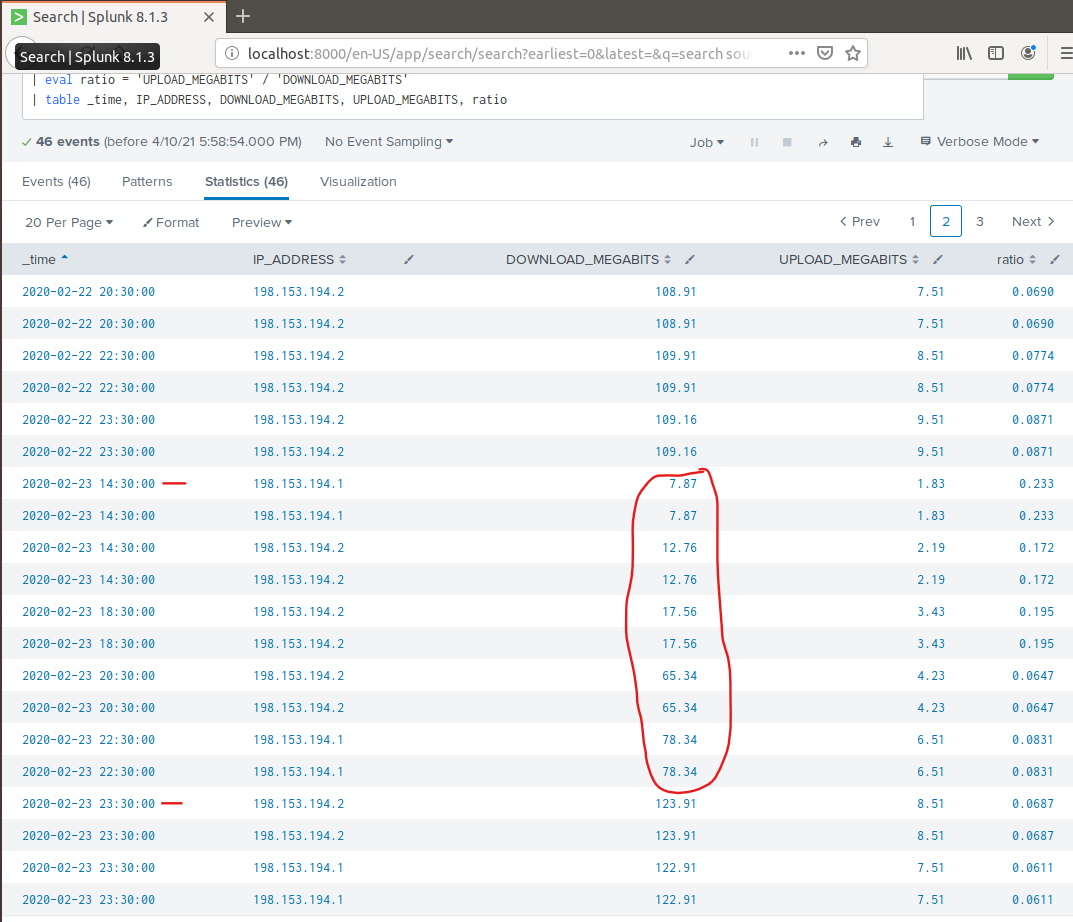
### **Step 1: The Need for Speed**

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.  
   * Hint: The format for creating a ratio is: | eval new\_field\_name = 'fieldA' / 'fieldB'
   * **| eval ratio = (UPLOAD\_MEGABITS / DOWNLOAD\_MEGAEBITS)**
3. 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
   * 
4. Hint: Use the following format when for the table command: | table fieldA fieldB fieldC  
   See above
5. Answer the following questions:  
   * Based on the report created, what is the approximate date and time of the attack? **Feb 23 2020 1430-2330**
   * How long did it take your systems to recover? **9 hours**
   * ****

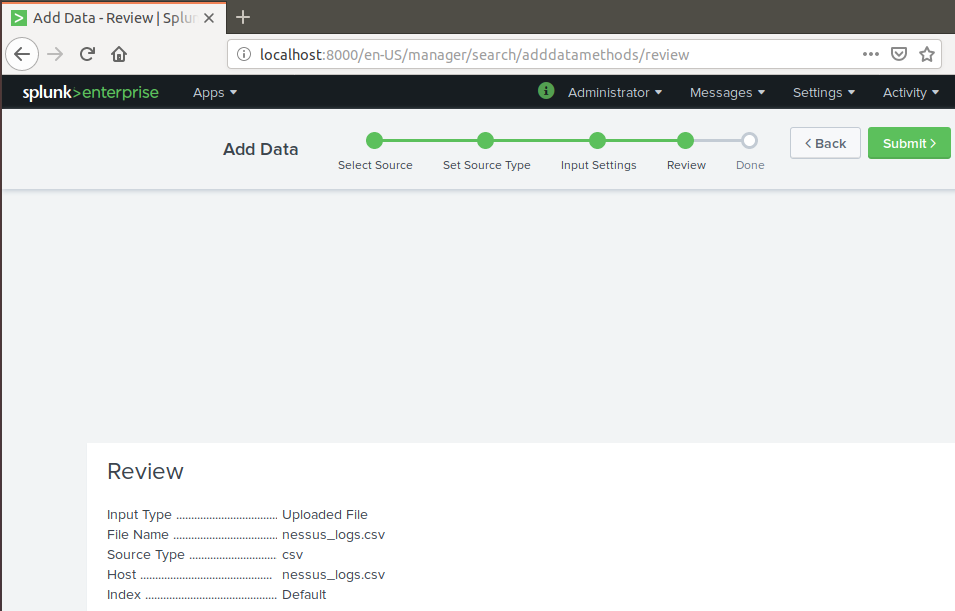
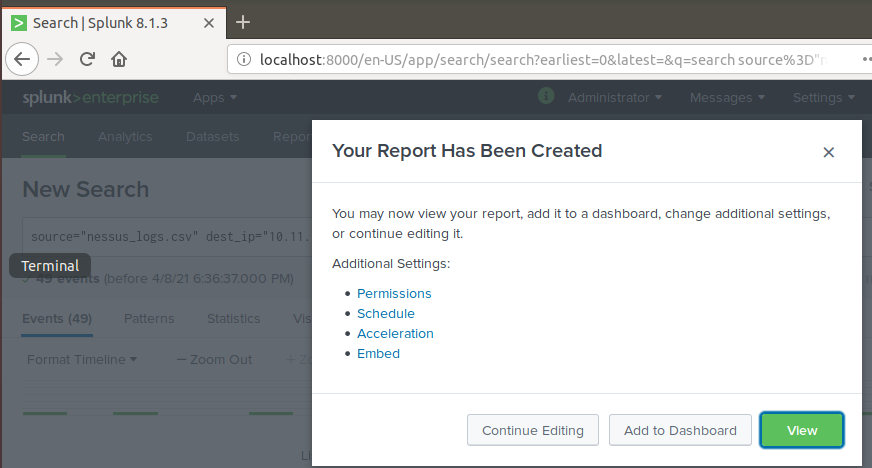
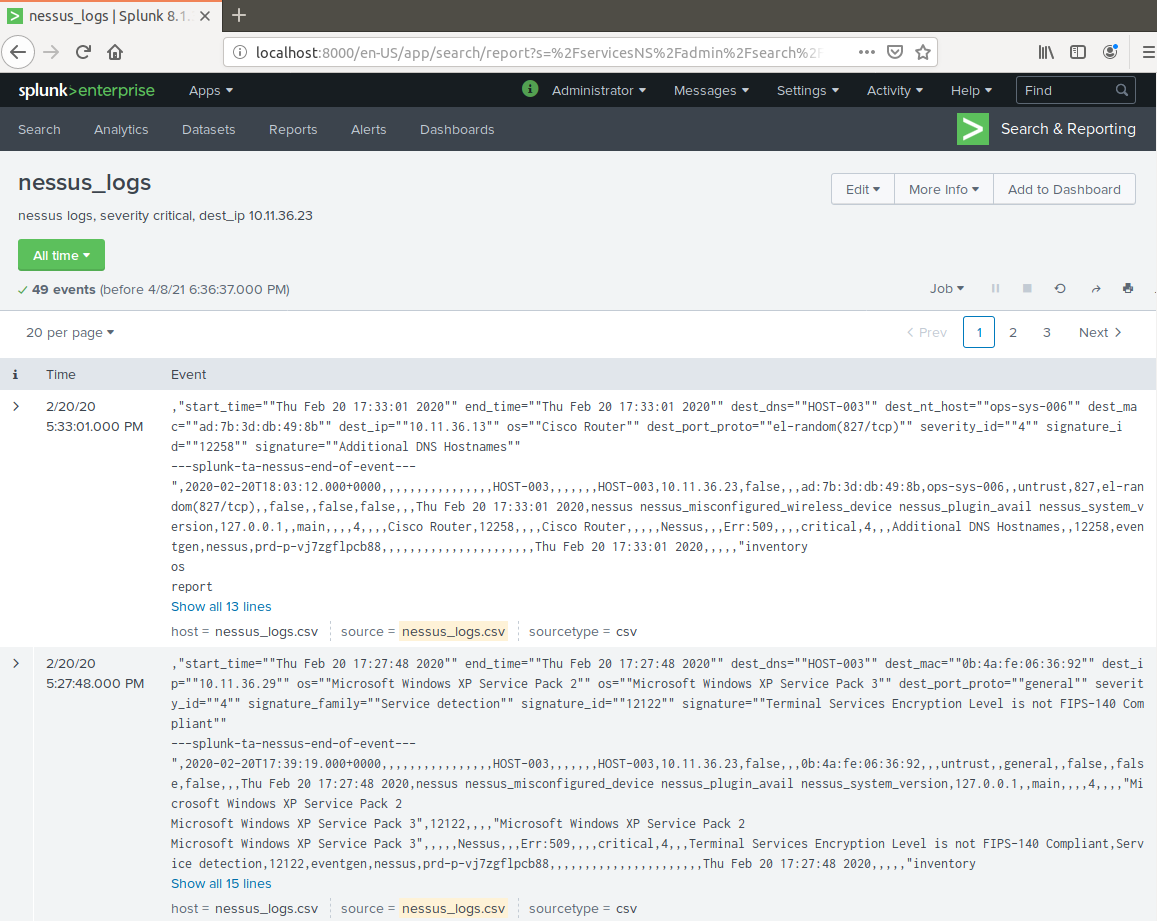
Submit a screen shot of your report and the answer to the questions above.

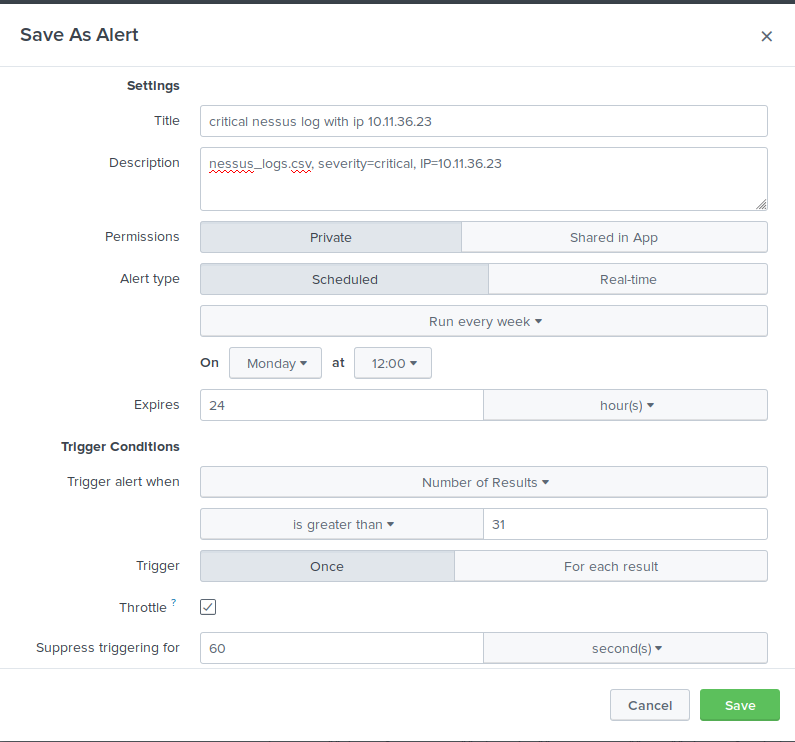
### **Step 2: Are We Vulnerable?**

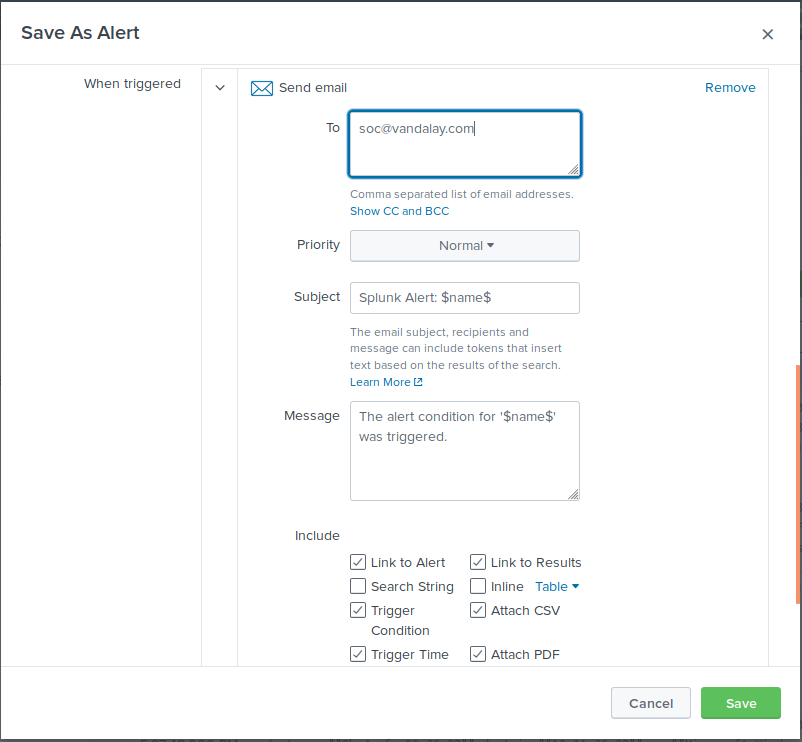
**Background:** Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

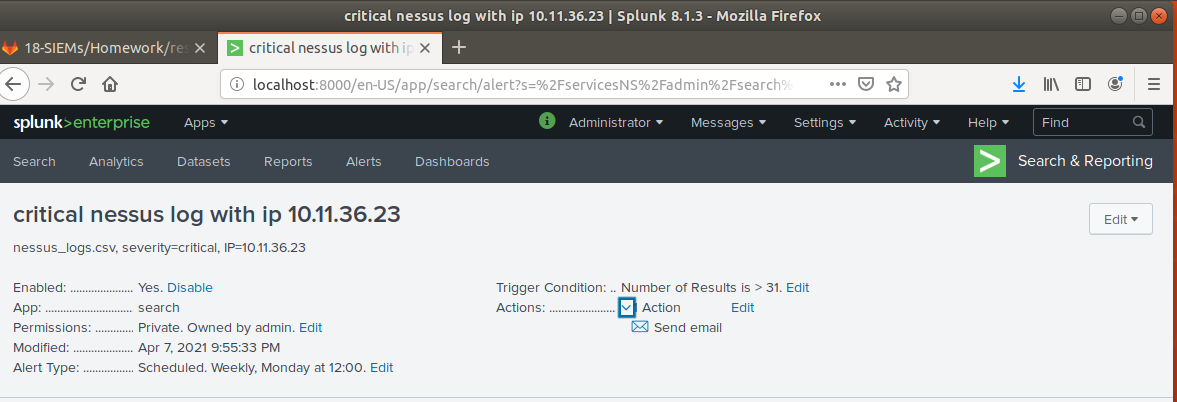
* For more information on Nessus, read the following link:<https://www.tenable.com/products/nessus>

**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.
   * 
   * 
3. 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.





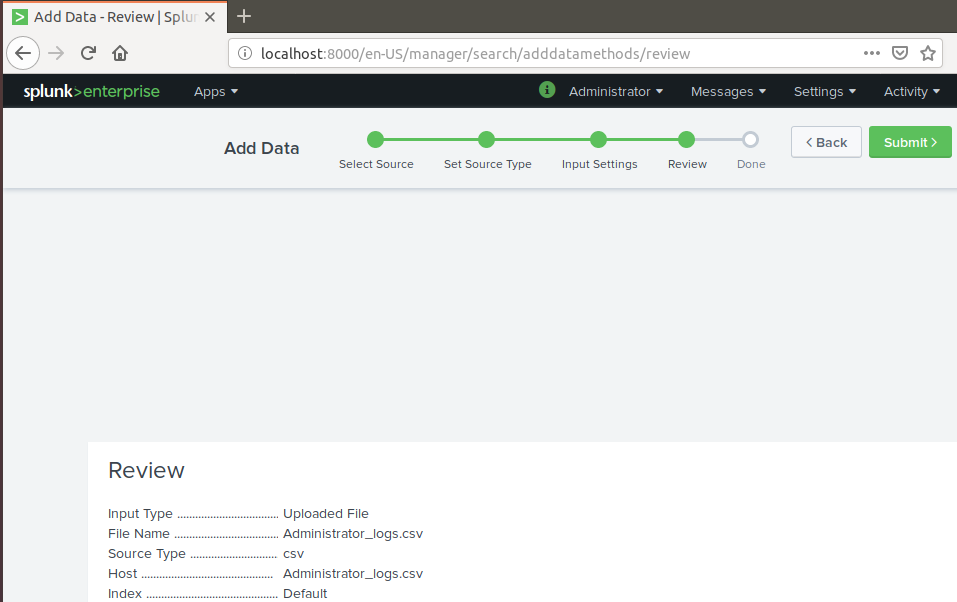


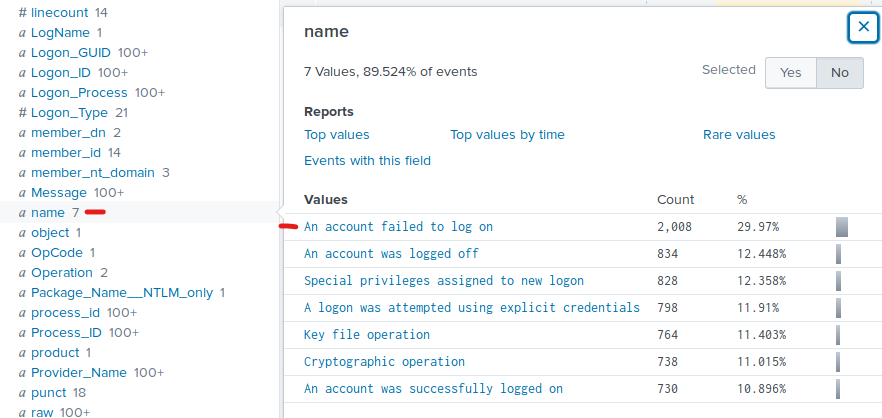
Submit a screenshot of your report and a screenshot of proof that the alert has been created.

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

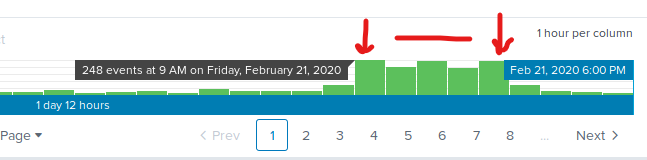
**Background:** A Vandaly server is also experiencing brute force attacks into their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.

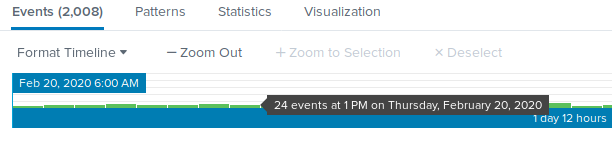
**Task:** Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.

1. Upload the administrator login logs.  
   * Admin Logins
   * 
2. When did the brute force attack occur?  
   See pic below of timeframe
   * Hints:
     + Look for the name field to find failed logins.
     + Note the attack lasted several hours.

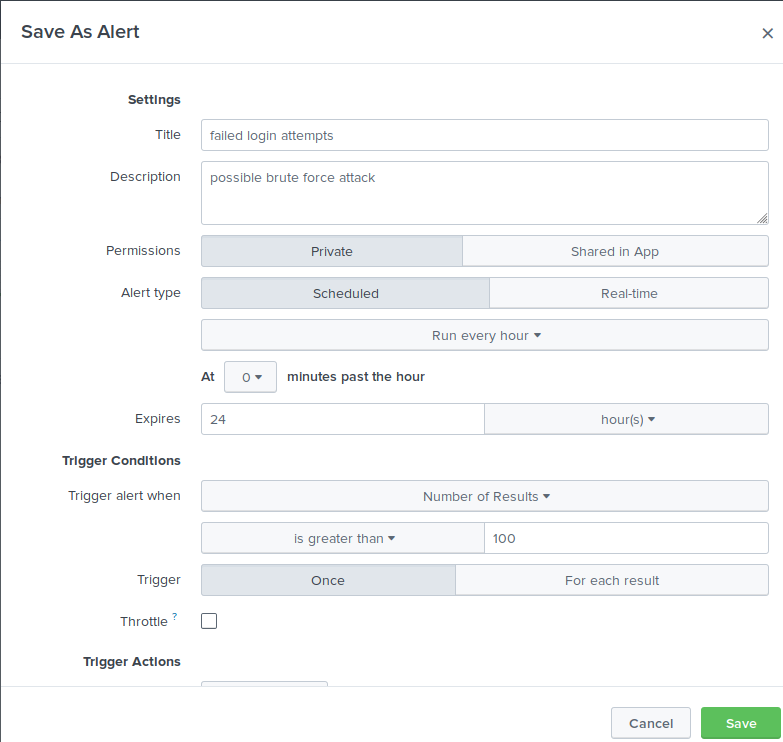


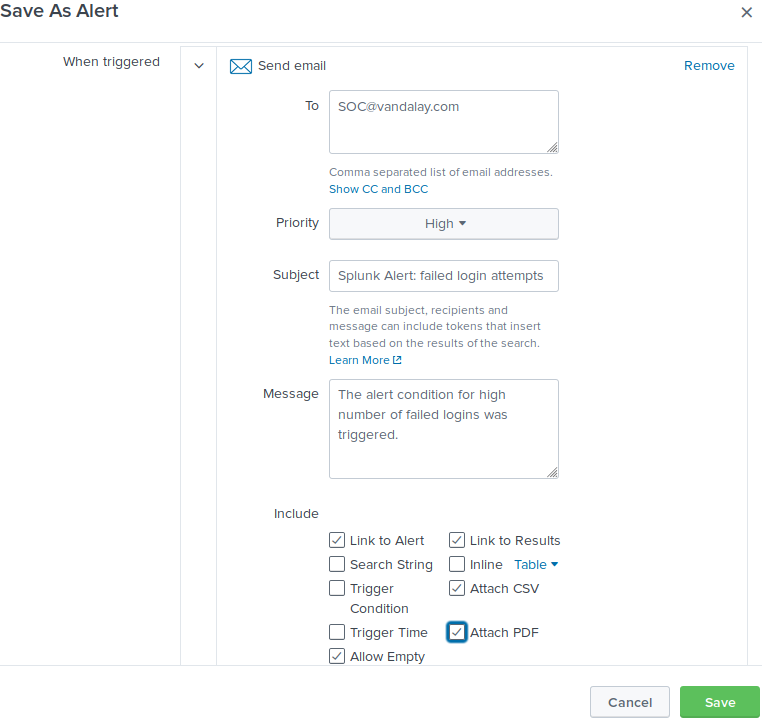
1. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.

  
**Unusual failed login activity from 9am to 1pm on Friday, February 21, 2020.**

** Significantly less failed logins during the same time of day but different day of the week.**

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.

### **Your Submission**

In a word document, provide the following:

* Answers to all questions where indicated.
* Screenshots where indicated.