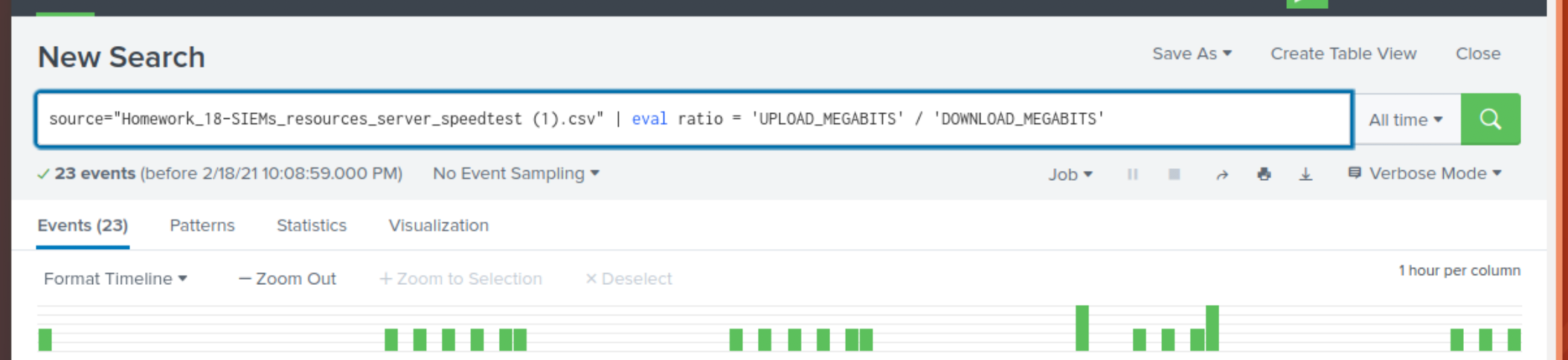
### **Step 1: The Need for Speed**

**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.

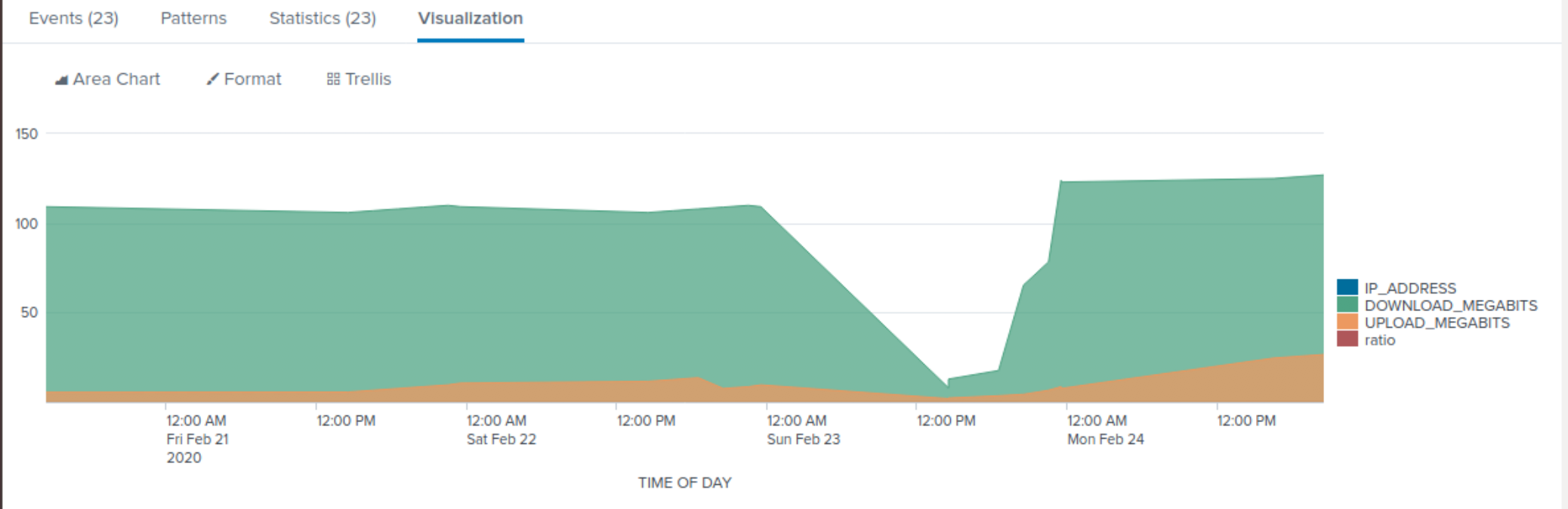


*Within the search bar above, I added a pipe to the current CSV file to evaluate or show the ratio between upload speeds and download speeds. That was created with the following:*

*< | eval ratio = “UPLOAD\_MEGABITS” / “DOWNLOAD\_MEGABITS” >*

1. Create a report using Splunk's table command to display the required fields in a statistics report:
2. Answer the following questions:
   * Based on the report created, what is the approximate date and time of the attack?
   * How long did it take your systems to recover?

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



*Based on the above visualization, it appears as if the attack started around 12:00AM on Sunday, February 23rd, and continued through 12:00 PM the next day. It appears as if the attack took almost a full 24 hours to stabilize. You can see from the graphic above that there is a steep valley where the downloads decreased dramatically. The uploads dipped, but not to a significant measure.*

*The graphic above had the X axis set to Time of Day for easy interpretation.*

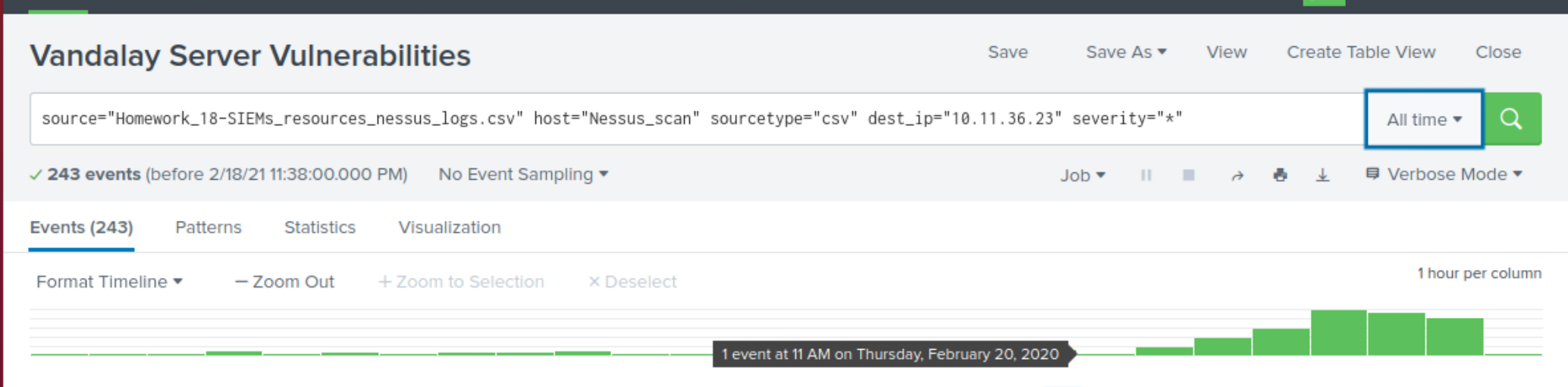
### **Step 2: Are We Vulnerable?**

**Background:** Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers are 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.

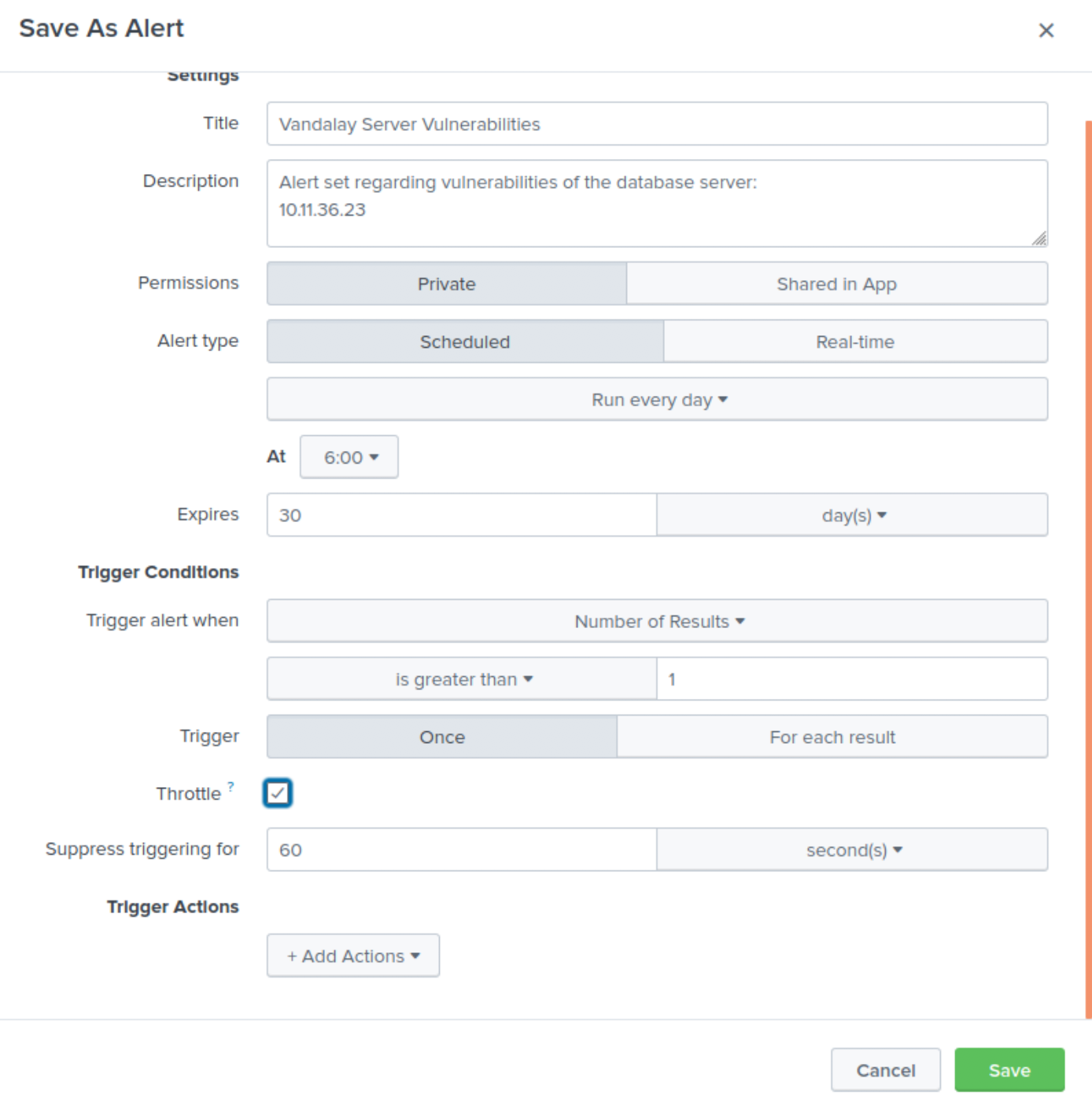
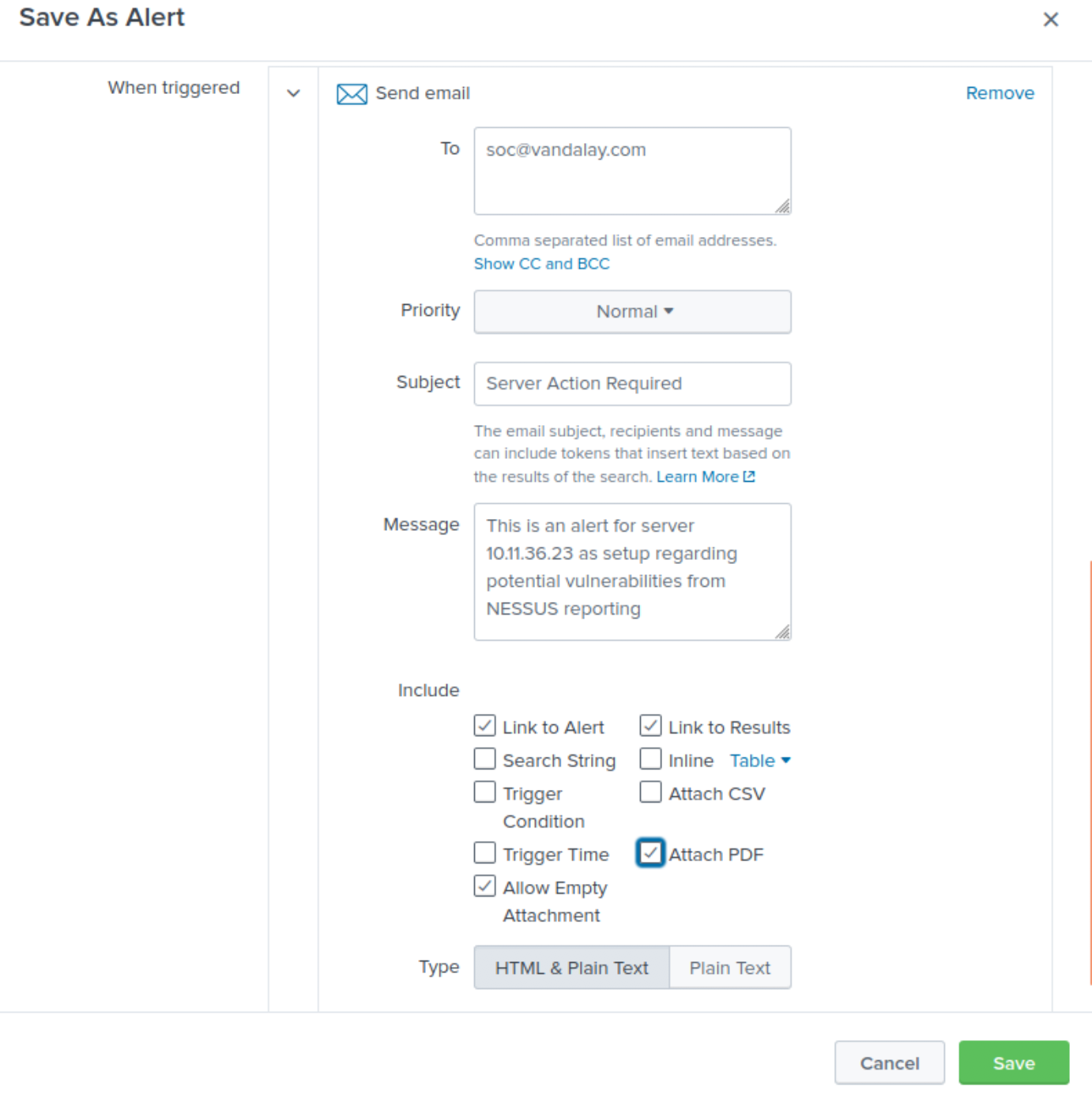
1. Upload the file from the Nessus vulnerability scan.
2. Create a report that shows the count of critical vulnerabilities from the customer database server.  
   * The database server IP is 10.11.36.23.
   * The field that identifies the level of vulnerabilities is severity.
3. Build an alert that monitors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



*Within the search bar above, I added on to the CSV file to gather the information requested. I filtered by the destination IP address to narrow the results to specify ones we are concerned with that correlate to the specific server, additionally, I filtered to see results of any of the vulnerabilities categorized through their severity factor. I used the following:*

*< dest\_ip “10.11.36.23”> <severity=”\*”>*

*Once the search and filtering mechanisms were verified, I saved this as an alert. I used a description that should be easy to interpret for all users with access and backed off on repeated alerts by activating the throttle.*

*I then have this trigger activity of sending out an email with an attached PDF to the Security Operations Center as requested. The message explains that the email is in relation to the specified data server and the possible vulnerabilities that are now exposed. This will be sent to all on the following email list:*

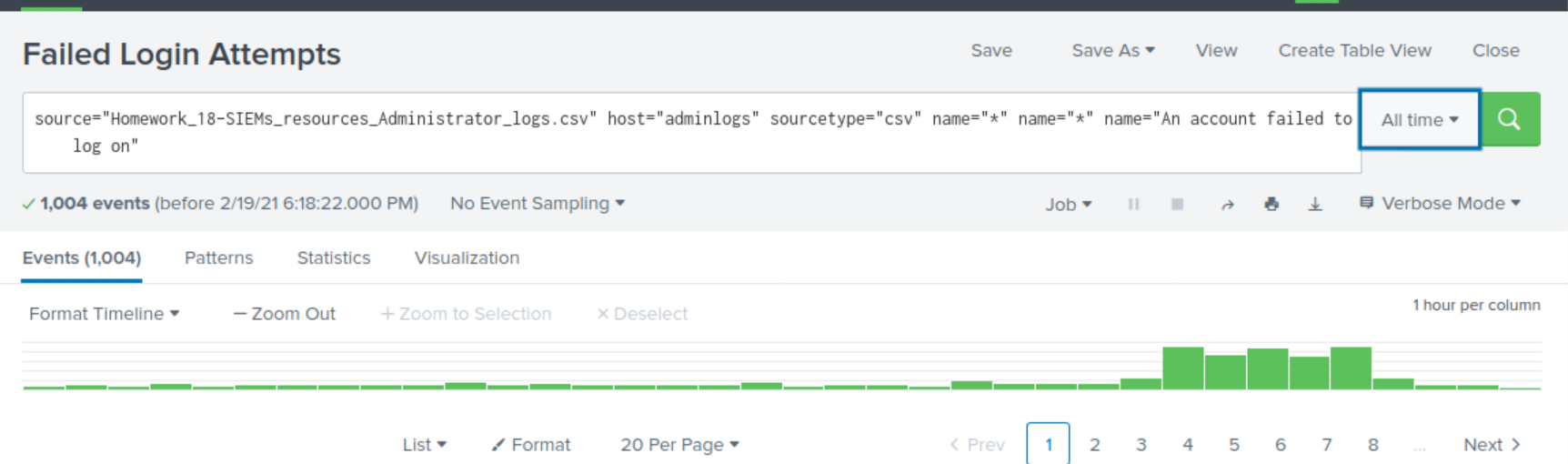
*< soc@vandalay.com >*

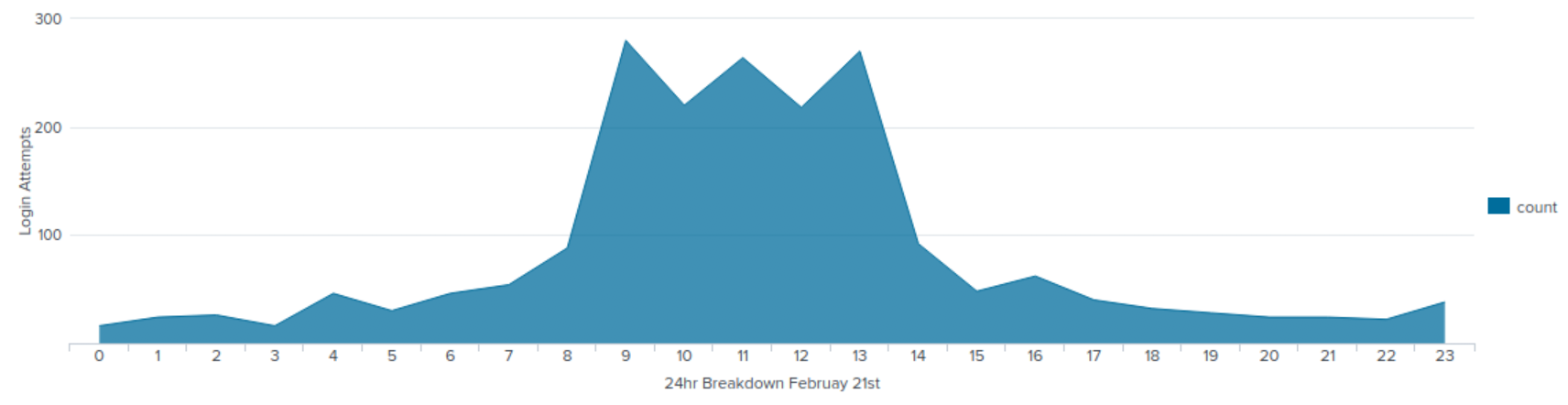
### **Step 3: Drawing the (base)line**

**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?
3. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.
4. Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.

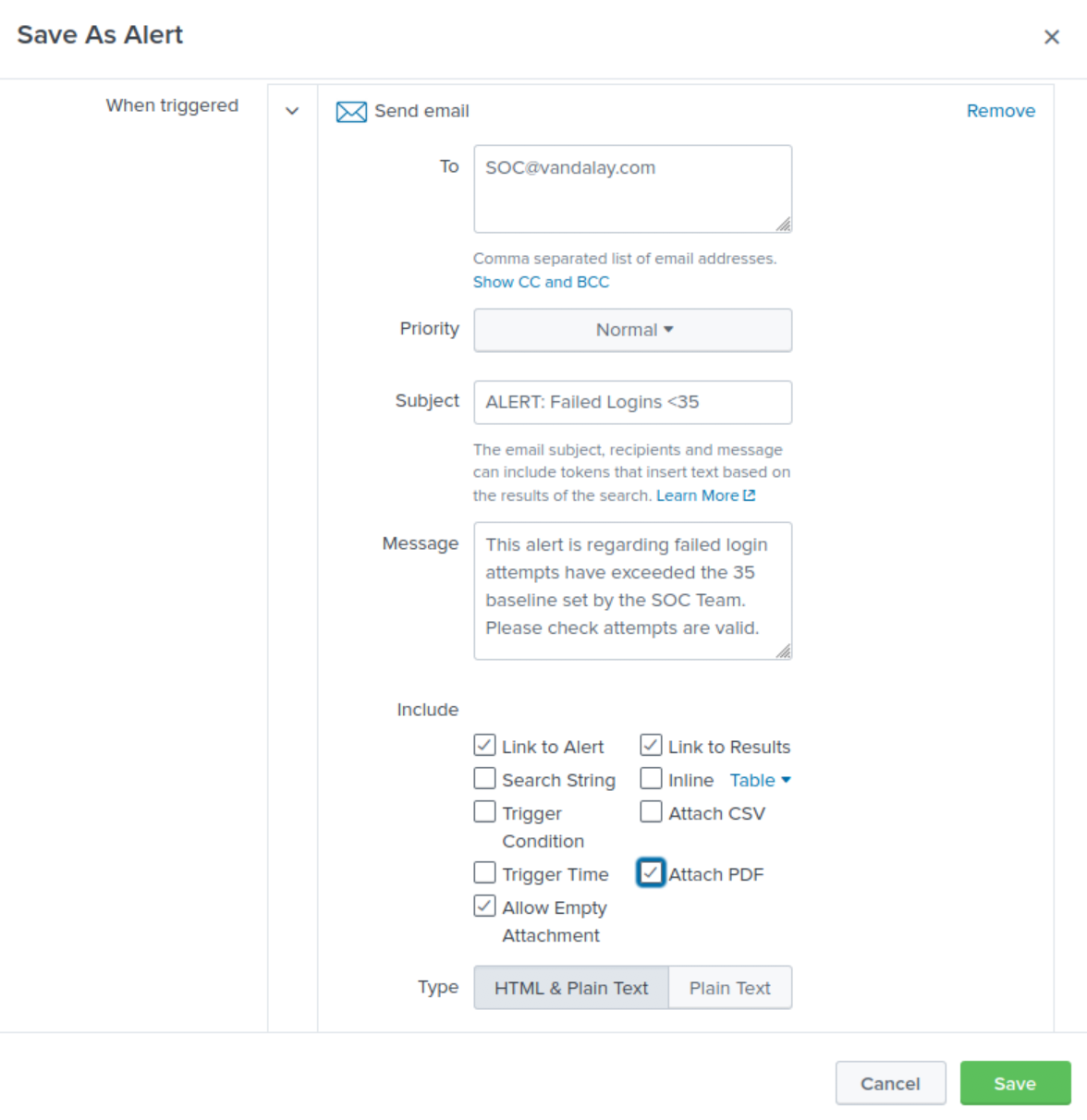
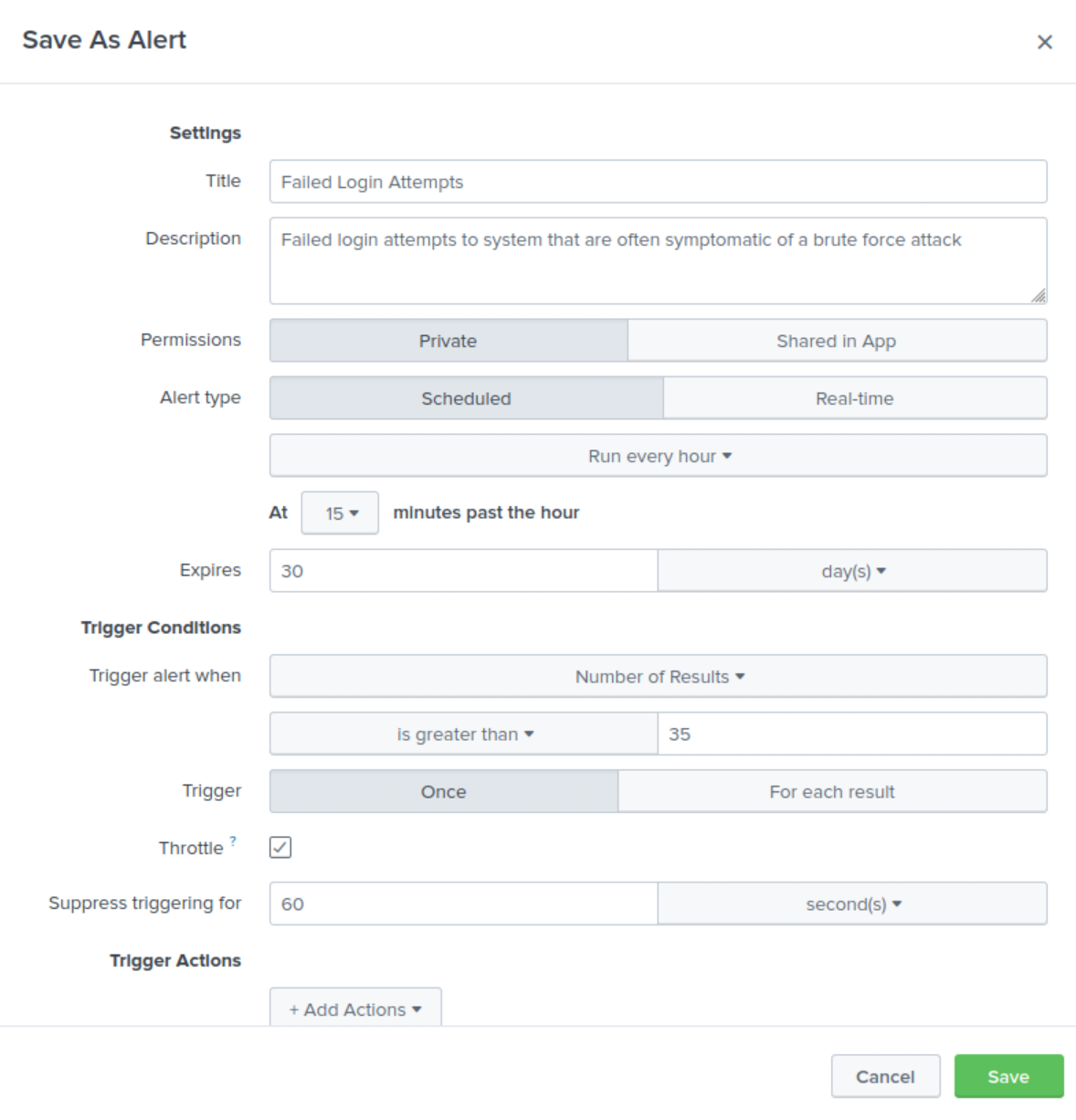




*Within the search bar above, I added the CSV file to review looking for the administrative login attempts. Within that, I further filtered for failed login attempts. That gave me 1,004 responses in total. Within the data, you can see that the majority of these attempts occurred on February 21st, between 9:00 AM and 1:00 PM. The failed login attempts averaged below 30 within each hour before that. The jump then quickly moved to 124 failed login attempts at 900AM. This is a strong statistical variance and does not seem to correlate with employees arriving at work or a reboot. This is over (4) times the previous attempts in previously recorded hours within the day.*

*A added a visualization chart above to show the breakdown over the 24 hour period on February 21st of failed login attempts. I believe this helps demonstrate the significant jump in these incidents. For this chart, I added the following to the CSV search already in place:*

*< | chart count by date\_hour >*

*Once the variance was established, I set an alert for any amount greater than 35 events (failed login attempts). This should give just enough wiggle room for the inevitable Monday morning failed login attempts without creating alert fatigue. The alert was set to send an email to the Security Operations Center as requested. Additionally, a PDF of the report will be attached to the email alert. This makes it easier for all to read over the material and not actually have to be in the ‘War Room’ or be plugged into a Splunk application.*