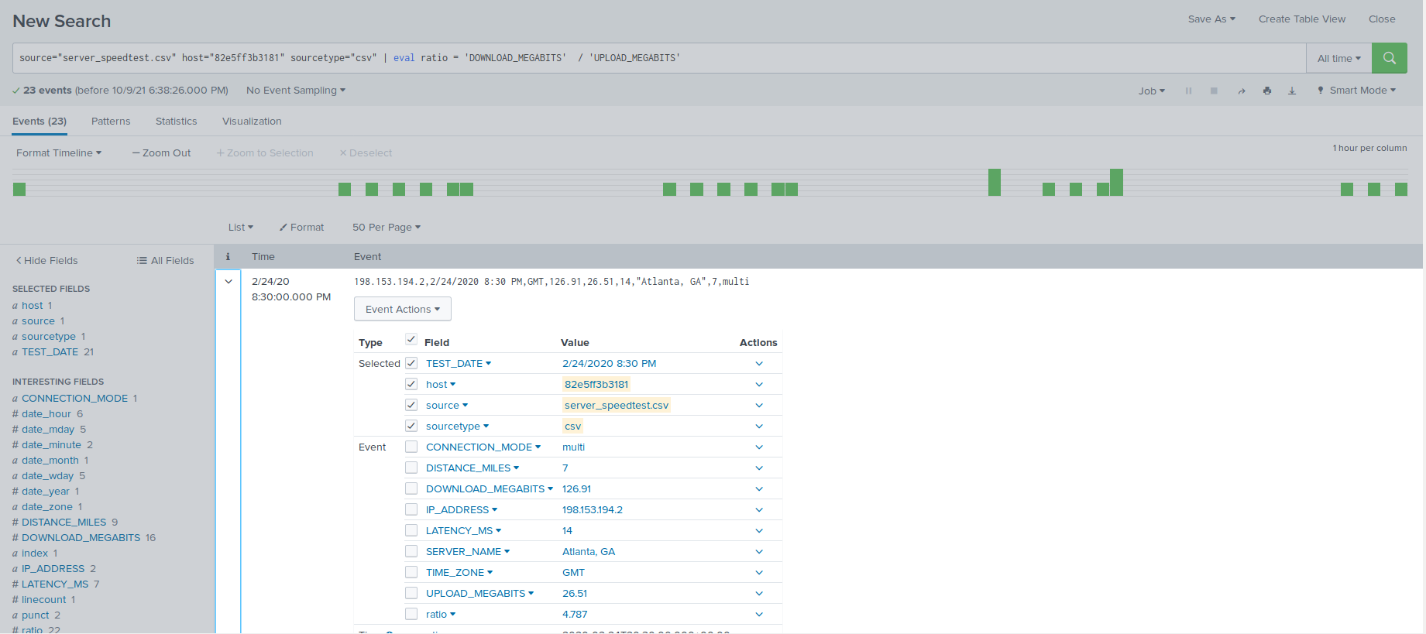
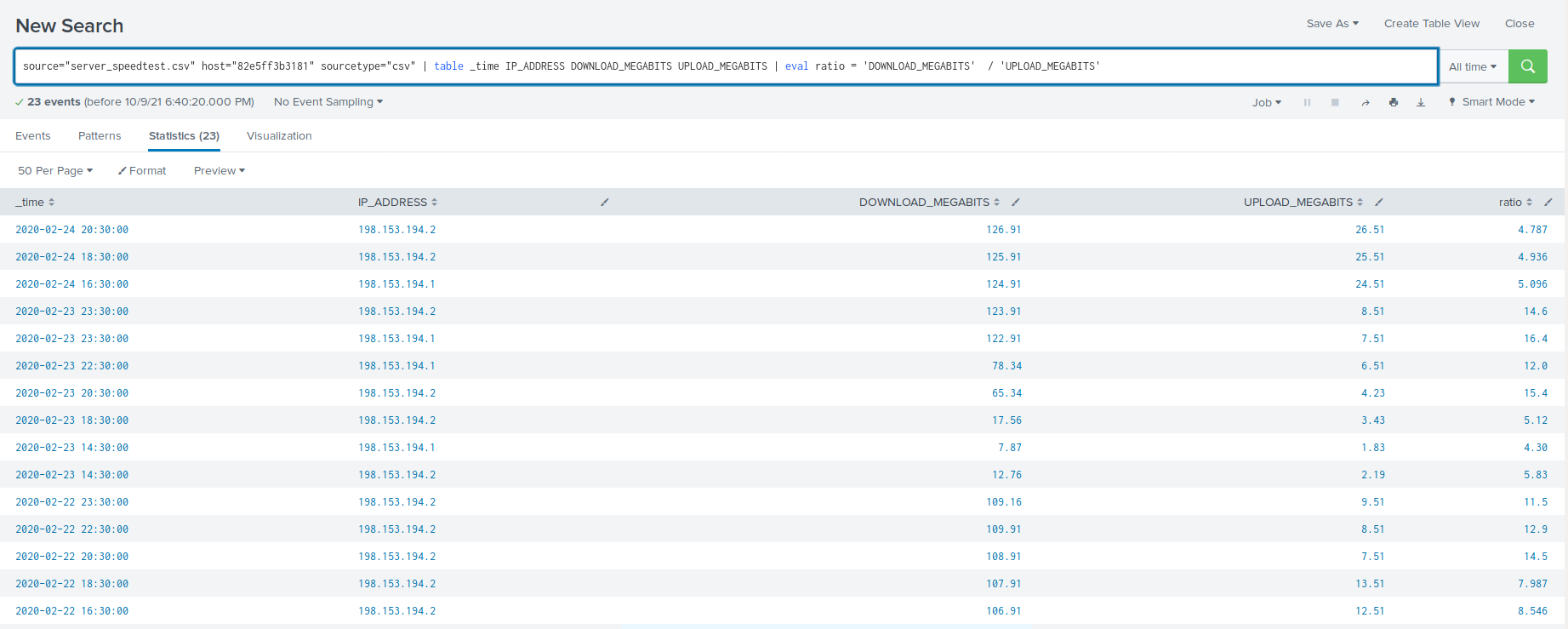
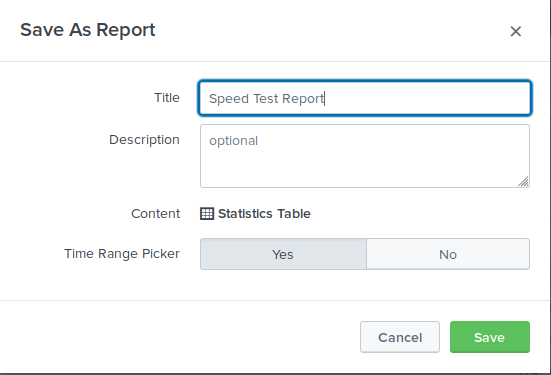
**Step 1: The Need for Speed**

Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.

****

Create a report using the Splunk's table command to display the following fields in a statistics report:

****



Answer the following questions:

Based on the report created, what is the approximate date and time of the attack?  
**2020-02-23 14:30:00pm**

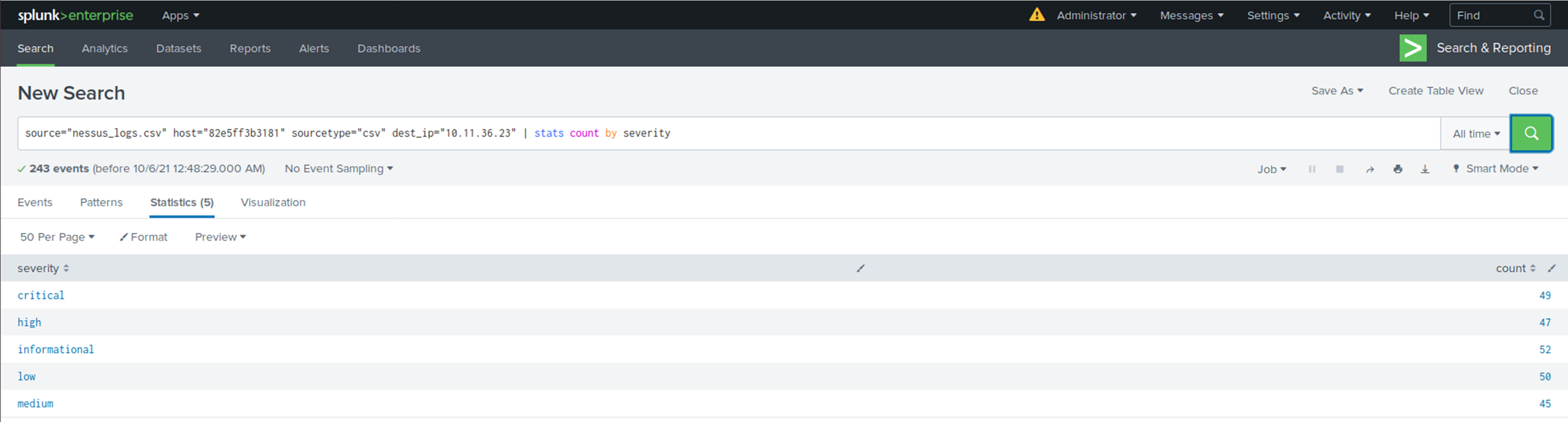
How long did it take your systems to recover?  
**Systems recovered at 2020-02-23 22:30:00pm. 8 hours total**

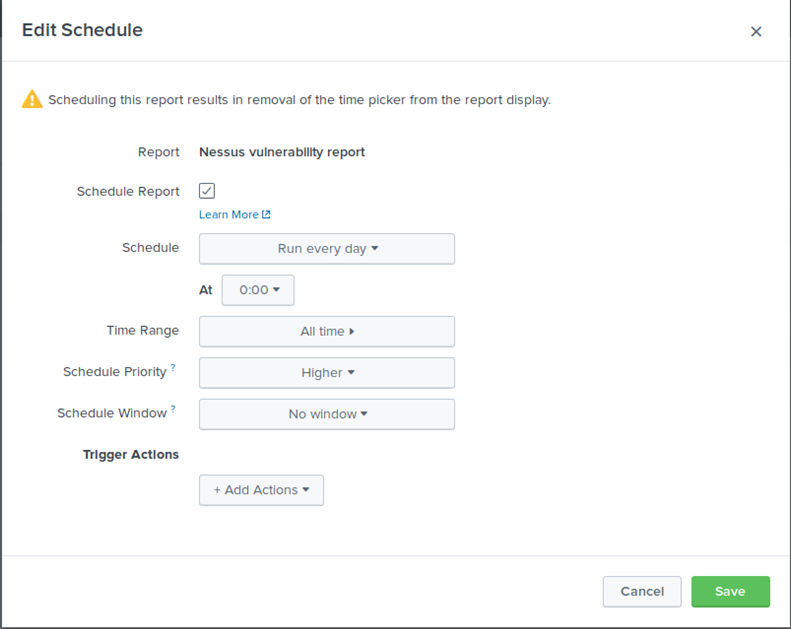
**Step 2: Are We Vulnerable?**

Create a report that shows the count of critical vulnerabilities from the customer database server.

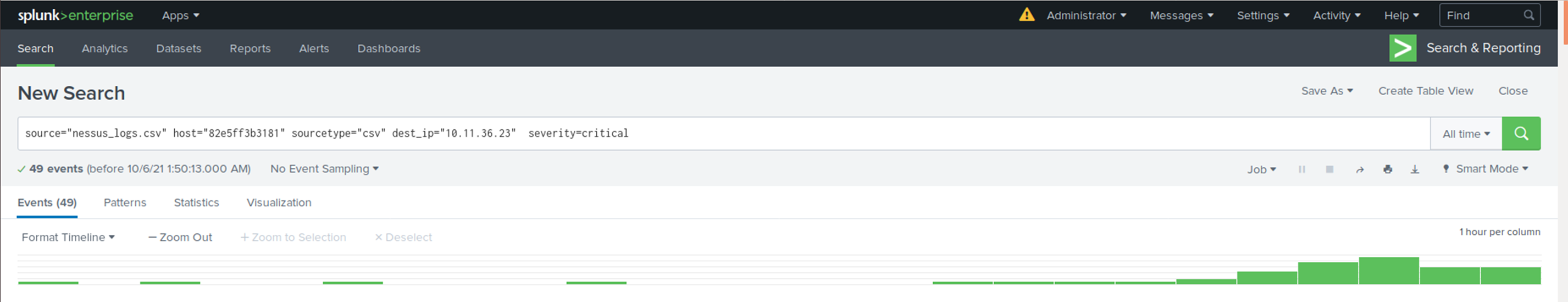
The database server IP is 10.11.36.23.

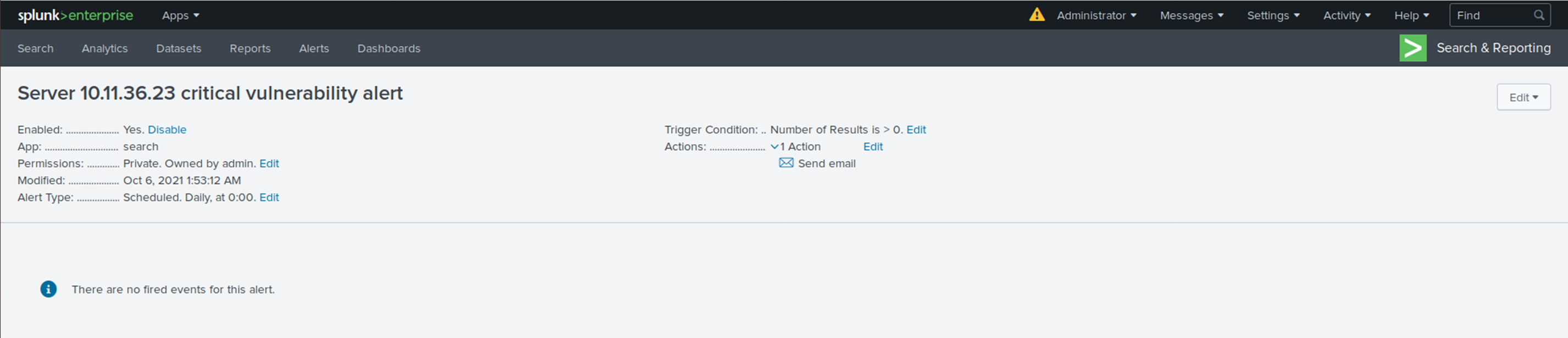
The field that identifies the level of vulnerabilities is severity.





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.

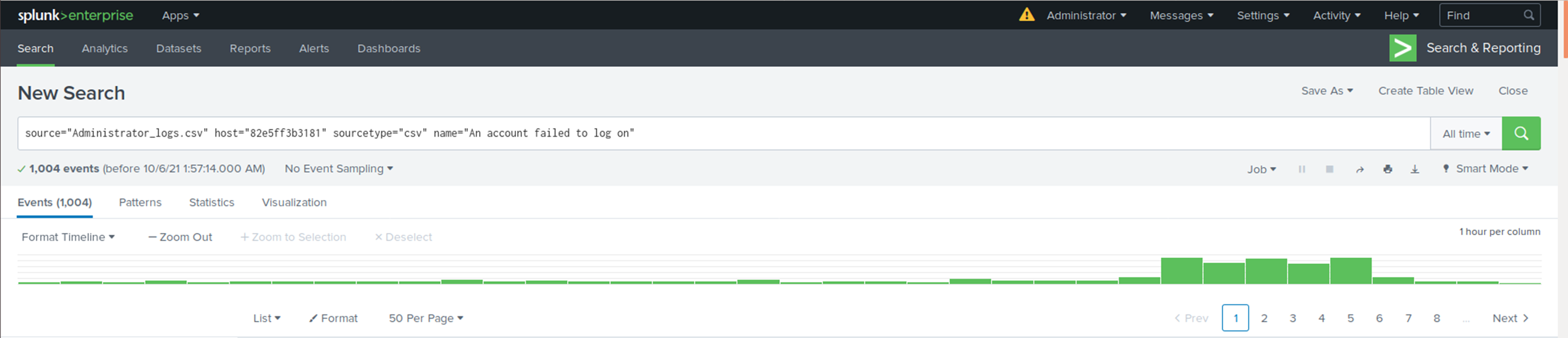




Submit a screenshot of your report and a screenshot of proof that the alert has been created.

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

When did the brute force attack occur?

  
  
**The attack started at 8AM on Feb 21 2020**

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

**Since the average failed logins attempts is around 6 to 23. I put the alert trigger at 30 or higher within an hour span.**

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

