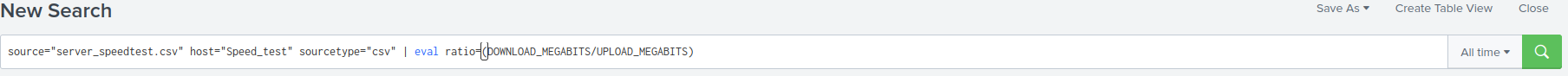
Week 18 Homework

Step 1: The Need for Speed

1. Eval command: eval ratio=(DOWNLOAD\_MEGABITS/UPLOAD\_MEGABITS)  
     
   Table

   Description automatically generated
2. Create a report: table \_time, IP\_ADDRESS, DOWNLOAD\_MEGABITS, UPLOAD\_MEGABITS, ratio  
   Graphical user interface, table

   Description automatically generated
3. Answer the following questions.
   1. Based on the report created, what is the approximate date and time of the attack? **02/23/2020 14:30:00 (2:30 PM)**
   2. How long did it take your systems to recover?  
      **6 Hours. It begins to pick up speed at 02/23/2020 20:30:00 (8:30 PM)**Graphical user interface, table

      Description automatically generated

Step 2: Are We Vulnerable

1. Create a report that shows the count of critical vulnerabilities from the customer database using the severity field and the destination IP address of the database (10.11.36.23).

**source="nessus\_logs.csv" host="Nessus\_Scan" sourcetype="csv" dest\_ip="10.11.36.23" severity="\*"|stats count by severity**  


1. Build an alert that emails [soc@vandalay.com](mailto:soc@vandalay.com)

Graphical user interface, application

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

A picture containing graphical user interface

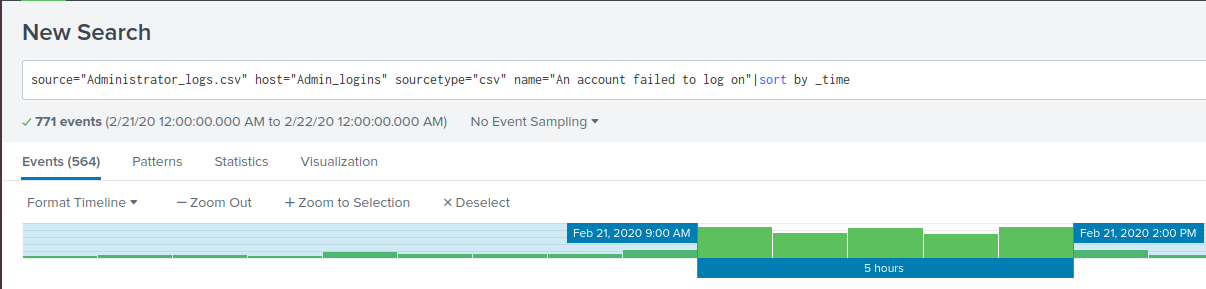
Description automatically generated

Step 3: Drawing the (base)line

1. When did the brute force attack occur?

**The brute force attack occurred February 21, 2020 9 AM – 2 PM.**

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

**Baseline: > 25 (Set to this because it does seem to go beyond that unless it’s before and after a brute force attack)**

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

Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence