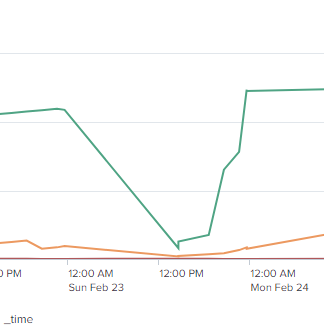
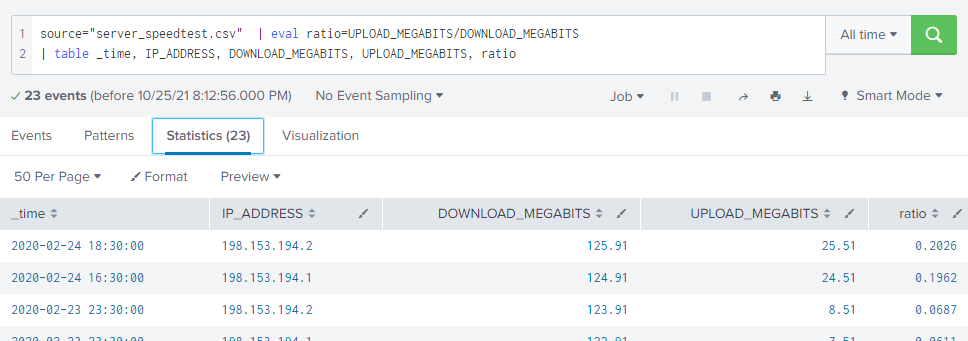
18 Homework: Lets go Splunking!

### Step 1: The Need for Speed

Q: Based on the report created, what is the approximate date and time of the attack?  
A: Feb 22, 11:30 PM to Feb 23, 2:30 PM

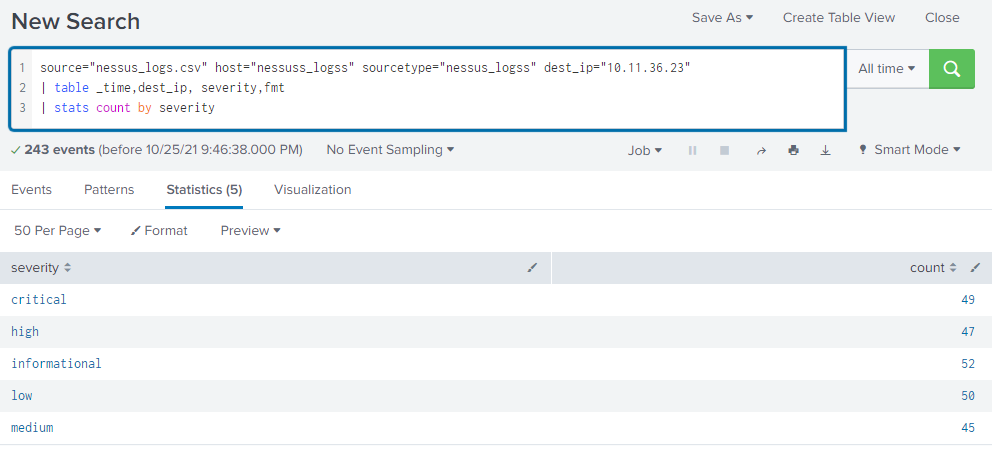
Q: How long did it take your systems to recover?  
A: it took 9 hours to recover

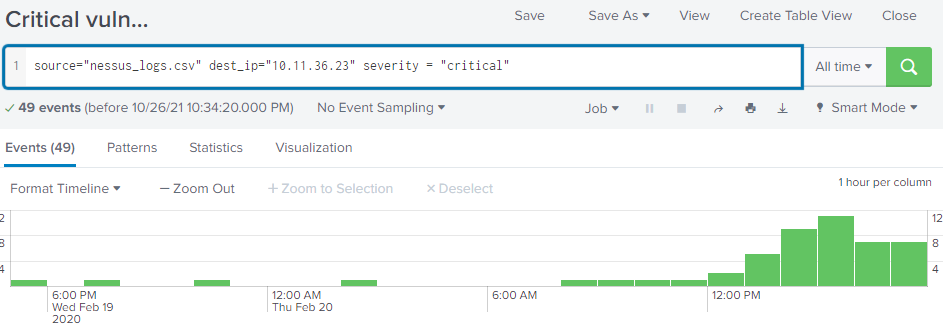
The Report

Time of attack

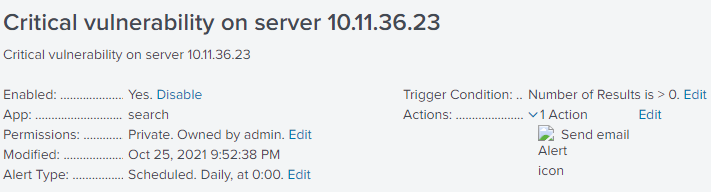
Step 2: Are We Vulnerable?

Count of critical vulnerabilities report

  
Query for alert



Alert Configuration

  
  
Step 3: Drawing the (base)line

Q: When did the brute force attack occur?  
A: 8AM Friday Feb 21st till 2PM Friday Feb 21st

Q: Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.  
  
A: normal activity is less than 25 fails per hour.

Alert Configuration

