

## Scenario

You have just been hired as a SOC Analyst by Vandalay Industries, an importing and exporting company.

- Vandalay Industries uses Splunk for their security monitoring and has been experiencing a variety of security issues against their online systems over the past few months.
- You are tasked with developing searches, custom reports, and alerts to monitor Vandalay's security environment in order to protect them from future attacks.

## System Requirements

You will be using the Splunk app located in the Ubuntu VM.

## Your Objective

Utilize your Splunk skills to design a powerful monitoring solution to protect Vandalay from security attacks.

After you complete the assignment you are asked to provide the following:

- Screenshots where indicated.
- Custom report results where indicated.

## Topics Covered in This Assignment

- Researching and adding new apps
- Installing new apps
- Uploading files
- Splunk searching
- Using fields
- Custom reports
- Custom alerts

Let's get started!

## Vandalay Industries Monitoring Activity Instructions

## Step 1: The Need for Speed

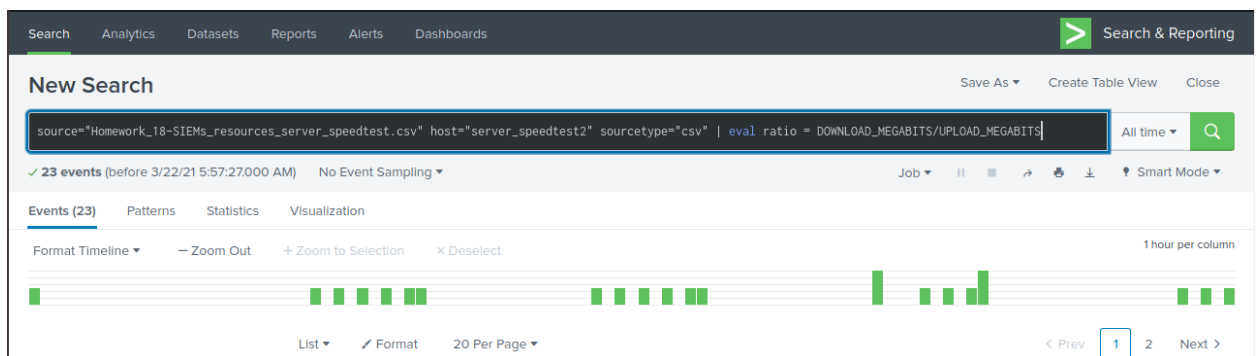
**Background:** As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandalay has been experiencing DDOS attacks against their web servers.

Not only were web servers taken offline by a DDOS attack, but upload and download speed were also significantly impacted after the outage. Your networking team provided results of a network speed run around the time of the latest DDOS attack.

**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 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.

```
source="Homework_18-SIEMs_resources_server_speedtest.csv"
host="server_speedtest2" sourcetype="csv" | eval ratio =
DOWNLOAD_MEGABITS/UPLOAD_MEGABITS
```



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`

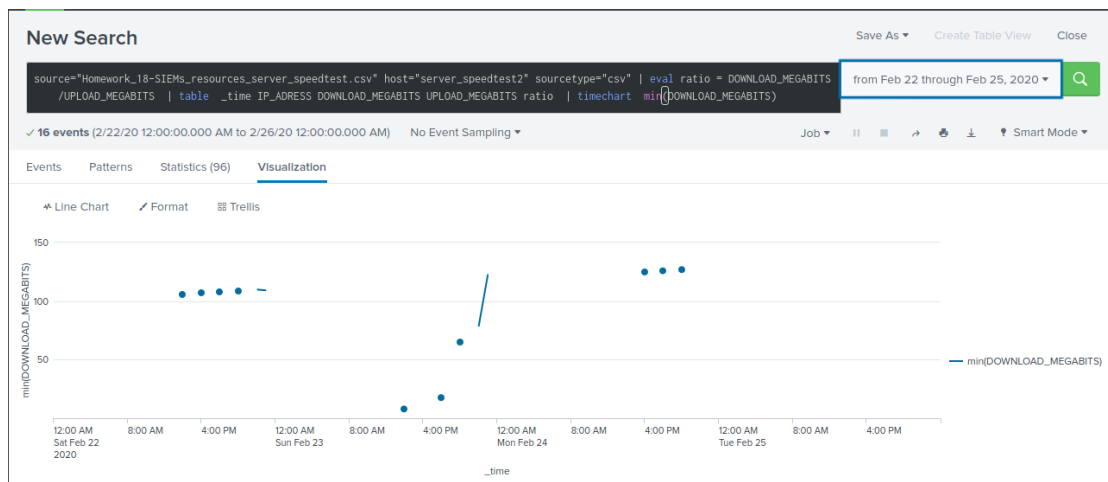
```
source="Homework_18-SIEMs_resources_server_speedtest.csv"
host="server_speedtest2" sourcetype="csv" | eval ratio =
DOWNLOAD_MEGABITS/UPLOAD_MEGABITS | table _time IP_ADRESS
DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio
```

New Search					Save As ▾	Create Table View	Close
source="Homework_18-SIEMs_resources_server_speedtest.csv" host="server_speedtest2" sourcetype="csv"   eval ratio = DOWNLOAD_MEGABITS/UPLOAD_MEGABITS   table _time IP_ADRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio					All time ▾		
✓ 23 events (before 3/22/21 5:58:48.000 AM) No Event Sampling ▾					Job ▾		Smart Mode ▾
Events Patterns <b>Statistics (23)</b> Visualization							
100 Per Page ▾ Format Preview ▾							
_time ▴	IP_ADRESS ▴	DOWNLOAD_MEGABITS ▴	UPLOAD_MEGABITS ▴	ratio ▴			
2020-02-22 18:30:00		107.91	13.51	7.987			
2020-02-22 16:30:00		106.91	12.51	8.546			
2020-02-22 14:30:00		105.91	11.51	9.202			
2020-02-21 23:30:00		109.16	10.51	10.39			
2020-02-21 22:30:00		109.91	9.51	11.6			
2020-02-21 20:30:00		108.91	8.51	12.8			
2020-02-21 18:30:00		107.91	7.51	14.4			
2020-02-21 16:30:00		106.91	6.51	16.4			
2020-02-21 14:30:00		105.91	5.51	19.2			
2020-02-20 14:21:00		109.16	5.43	20.1			
2020-02-23 23:30:00		123.91	8.51	14.6			
2020-02-23 23:30:00		122.91	7.51	16.4			
2020-02-23 22:30:00		78.34	6.51	12.0			
2020-02-23 20:30:00		65.34	4.23	15.4			
2020-02-23 18:30:00		17.56	3.43	5.12			
2020-02-23 14:30:00		7.07	1.03	6.87			

4. Answer the following questions:

Based on the report created, what is the approximate date and time of the attack? **Between 22 February 2:00pm to 23 February 11:00pm**

How long did it take your systems to recover? **9 hours**



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

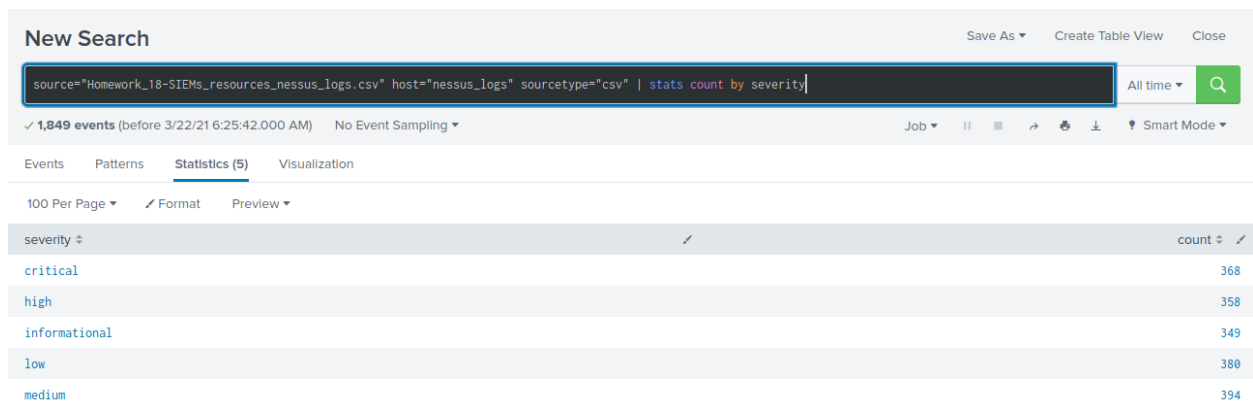
## Step 2: Are We Vulnerable?

**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>

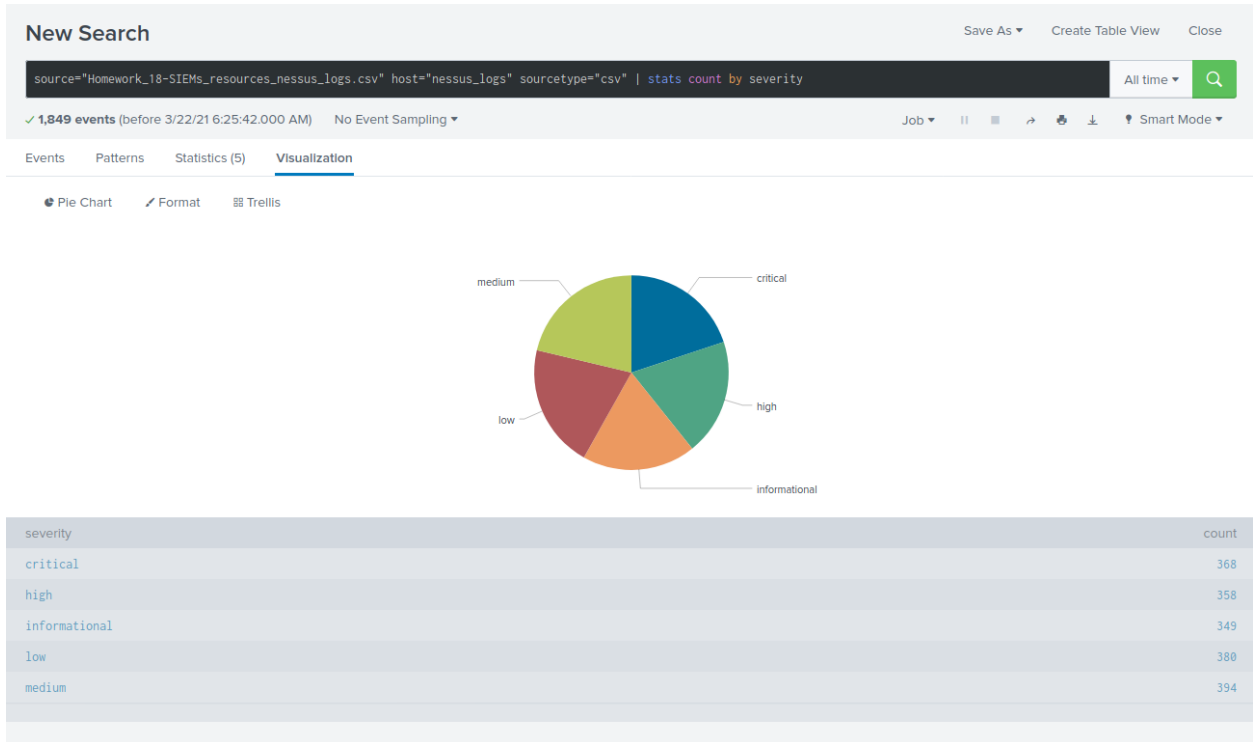
**Task:** Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

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.



The screenshot shows the Nessus search interface with a search query: `source="Homework_18-SIEMs_resources_nessus_logs.csv" host="nessus_logs" sourcetype="csv" | stats count by severity`. The results show 1,849 events. The search is filtered by 'All time' and 'Smart Mode' is enabled. The 'Statistics (5)' tab is selected, showing a table with severity levels and their counts.

severity	count
critical	368
high	358
informational	349
low	380
medium	394



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](mailto:soc@vandalay.com).

**Critical Vulnerabilities** Edit

Enabled: ..... Yes. [Disable](#) Trigger Condition: .. Number of Results is > 1. [Edit](#)

App: ..... search Actions: ..... 1 Action [Edit](#)

Permissions: ..... Private. Owned by admin. [Edit](#) [Send email](#)

Modified: ..... Mar 22, 2021 6:50:04 AM

Alert Type: ..... Scheduled. Weekly, Monday at 6:00. [Edit](#)

i There are no fired events for this alert.

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 Vandelay 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? **It happened on February 21st between 8:00 am and 2:00 pm. My determined baseline is 20 logins in an hour and my threshold is a count greater than or equal to 30.**
  - Hints:
    - Look for the name field to find failed logins.
    - Note the attack lasted several hours.

```
source="Homework_18-SIEMs_resources_Administrator_logs.csv"
host="Admin_Logs" sourcetype="csv" | stats count by name | eval BruteForce =
if(name= "An account failed to log on" AND count > 20, "Potential Brute Force",
"Not Brute Force") | search BruteForce = "Potential Brute Force"
```

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query: `source="Homework_18-SIEMs_resources_Administrator_logs.csv" host="Admin_Logs" sourcetype="csv" | stats count by name | eval BruteForce = if(name= "An account failed to log on" AND count > 20, "Potential Brute Force", "Not Brute Force") | search BruteForce = "Potential Brute Force"`. Below the search bar, it indicates 3,742 events. The interface is set to 'Statistics (t)' view. A table displays the results:

name	count	BruteForce
An account failed to log on	1004	Potential Brute Force

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@vandelay.com if triggered.

splunk>enterprise

Apps

Administrator

4 Messages

Settings

Activity

Help

Find

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

### Brute Force Alert

Edit

Enabled: ..... Yes. [Disable](#)

App: ..... search

Permissions: ..... Private. Owned by admin. [Edit](#)

Modified: ..... Mar 22, 2021 6:48:55 AM

Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 25. [Edit](#)

Actions: ..... 1 Action [Edit](#)

☒ Send email

There are no fired events for this alert.

Save As Alert

When triggered

Send email

Remove

To

soc@vandalay.com

Comma separated list of email addresses.  
[Show CC and BCC](#)

Priority

Normal

Subject

Splunk Alert: \$name\$

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message

The alert condition for '\$name\$' was triggered.

Include

☒ Link to Alert

☒ Link to Results

☐ Search String

☐ Inline [Table](#)

☐ Trigger Condition

☐ Attach CSV

☐ Trigger Time

☐ Attach PDF

☒ Allow Empty Attachment

Cancel

Save