

## Step 1: The Need for Speed

1. Upload the following file of the system speeds around the time of the attack.

- Speed Test File

Add Data - Select Source X

localhost:8000/en-US/manager/search/adddatamethods/selectsource?input\_mode=

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Next >

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **server\_speedtest.csv**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

Done

Add Data - Success | Splunk X

localhost:8000/en-US/manager/search/adddatamethods/success

splunk>enterprise Apps Administrator Messages Settings Activity

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Next >

File has been uploaded successfully.

Configure your inputs by going to [Settings > Data Inputs](#)

Start Searching Search your data now or see [examples and tutorials](#).

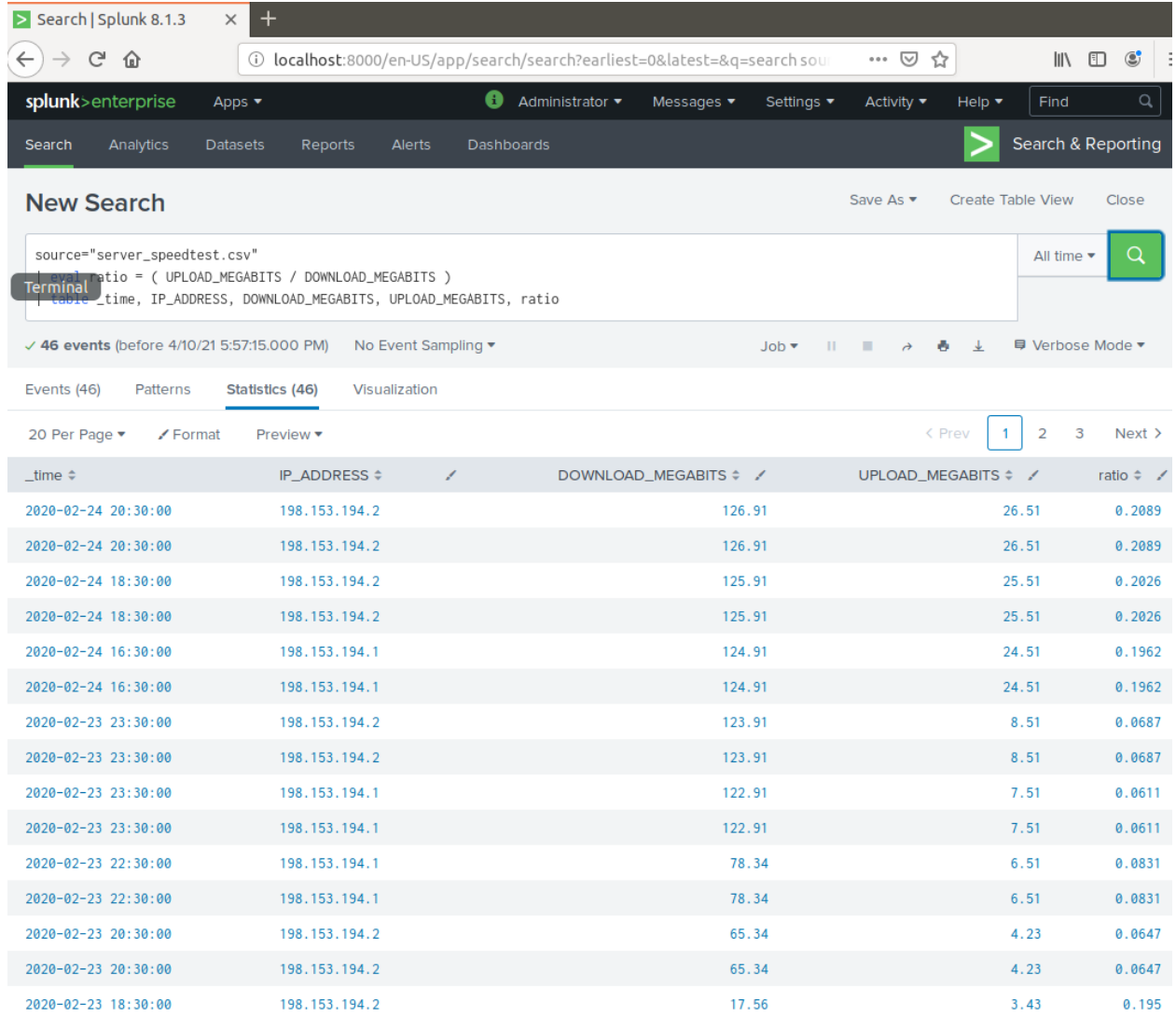
Extract Fields Create search-time field extractions. [Learn more about fields](#).

Add More Data Add more data inputs now or see [examples and tutorials](#).

Download Apps Apps help you do more with your data. [Learn more](#).

Build Dashboards Visualize your searches. [Learn more](#).

2. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.
  - Hint: The format for creating a ratio is: | eval new\_field\_name = 'fieldA' / 'fieldB'
  - | eval ratio = (UPLOAD\_MEGABITS / DOWNLOAD\_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



The screenshot shows the Splunk 8.1.3 interface. The search bar contains the query: `source="server_speedtest.csv" | eval ratio = ( UPLOAD_MEGABITS / DOWNLOAD_MEGABITS ) | table _time, IP_ADDRESS, DOWNLOAD_MEGABITS, UPLOAD_MEGABITS, ratio`. The search results show 46 events. The table view is selected, displaying the following data:

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	0.2089
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	0.2089
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	0.2026
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	0.2026
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	0.1962
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	0.1962
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195

4. Hint: Use the following format when for the table command: | table fieldA fieldB fieldC  
See above
5. Answer the following questions:
  - Based on the report created, what is the approximate date and time of the attack? **Feb 23 2020 1430-2330**
  - How long did it take your systems to recover? **9 hours**

Search | Splunk 8.1.3

localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search sou

| eval ratio = 'UPLOAD\_MEGABITS' / 'DOWNLOAD\_MEGABITS'  
| table \_time, IP\_ADDRESS, DOWNLOAD\_MEGABITS, UPLOAD\_MEGABITS, ratio

✓ 46 events (before 4/10/21 5:58:54.000 PM) No Event Sampling

Events (46) Patterns Statistics (46) Visualization

20 Per Page Format Preview

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611

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

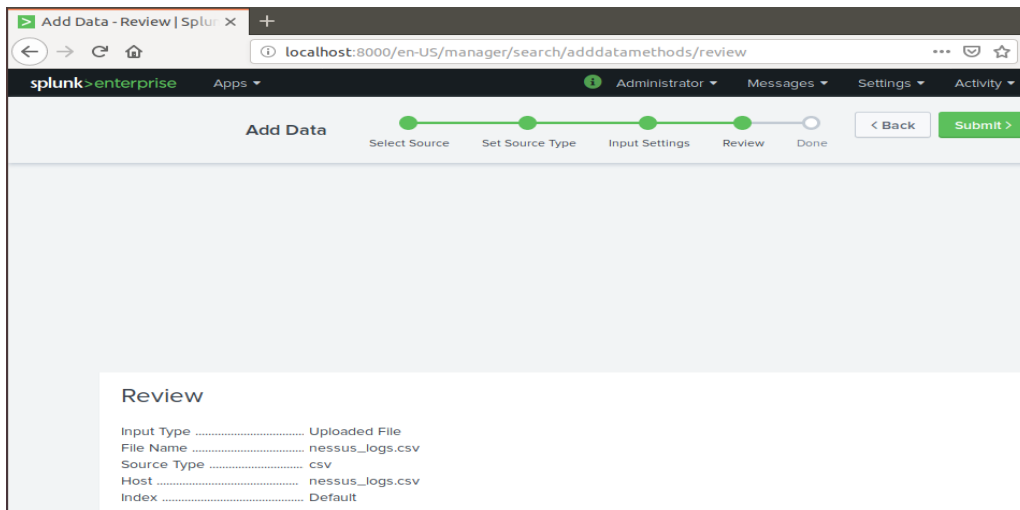
## Step 2: Are We Vulnerable?

**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.

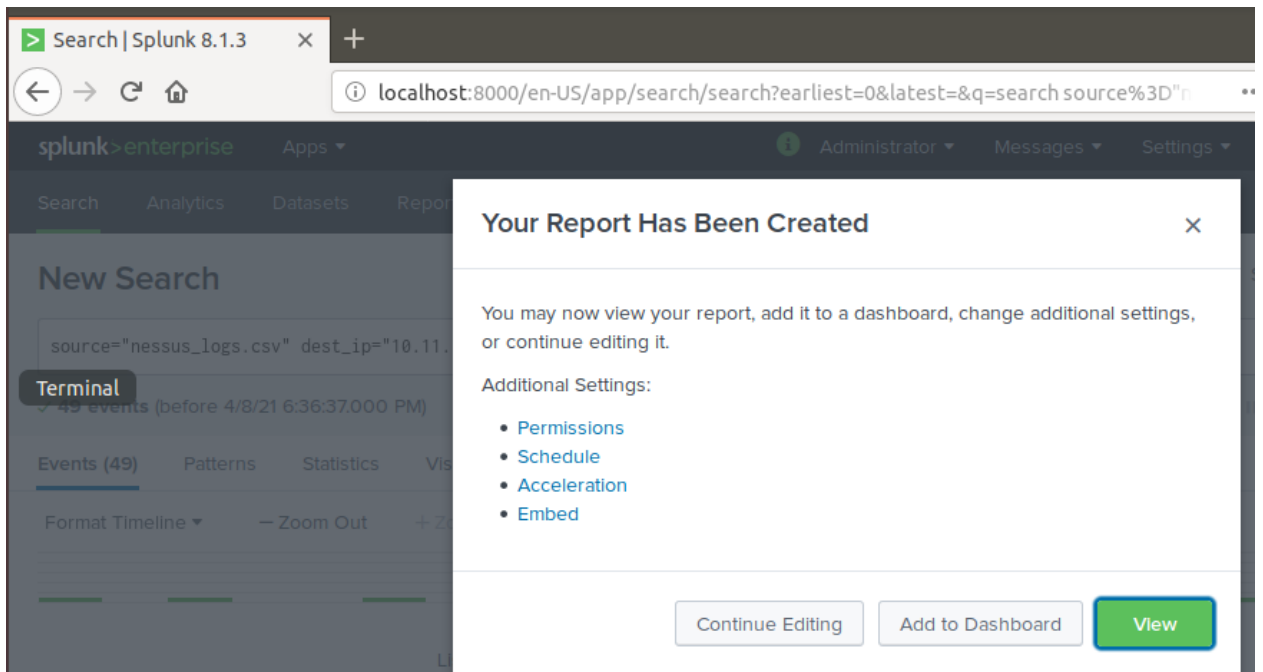
- For more information on Nessus, read the following link:  
<https://www.tenable.com/products/nessus>

**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.

- 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.



nessus\_logs | Splunk 8.1. X

localhost:8000/en-US/app/search/report?s=%2FservicesNS%2Fadmin%2Fsearch%2F...

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### nessus\_logs

nessus logs, severity critical, dest\_ip 10.11.36.23

All time

✓ 49 events (before 4/8/21 6:36:37.000 PM)

20 per page

< Prev 1 2 3 Next >

i	Time	Event
>	2/20/20 5:33:01.000 PM	<pre> ,"start_time":"Thu Feb 20 17:33:01 2020" end_time="Thu Feb 20 17:33:01 2020" dest_dns="HOST-003" dest_nt_host="ops-sys-006" dest_mac="ad:7b:3d:db:49:8b" dest_ip="10.11.36.13" os="Cisco Router" dest_port_proto="el-random(827/tcp)" severity_id="4" signature_id="12258" signature="Additional DNS Hostnames" ---splunk-ta-nessus-end-of-event--- ",2020-02-20T18:03:12.000+0000,,,,,,,,,,,,,HOST-003,,,,,,,,,HOST-003,10.11.36.23,false,,,ad:7b:3d:db:49:8b,ops-sys-006,,untrust,827,el-random(827/tcp),,false,,false,false,,,Thu Feb 20 17:33:01 2020,nessus nessus_misconfigured_wireless_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,Cisco Router,12258,,,Cisco Router,,,,,Nessus,,,Err:509,,,critical,4,,,Additional DNS Hostnames,,12258,eventgen,nessus,prd-p-vj7zgflpcb88,,,,,,,,,,,,,Thu Feb 20 17:33:01 2020,,,,,"inventory os report Show all 13 lines host = nessus_logs.csv   source = nessus_logs.csv   sourcetype = csv </pre>
>	2/20/20 5:27:48.000 PM	<pre> ,"start_time":"Thu Feb 20 17:27:48 2020" end_time="Thu Feb 20 17:27:48 2020" dest_dns="HOST-003" dest_mac="0b:4a:fe:06:36:92" dest_ip="10.11.36.29" os="Microsoft Windows XP Service Pack 2" os="Microsoft Windows XP Service Pack 3" dest_port_proto="general" severity_id="4" signature_family="Service detection" signature_id="12122" signature="Terminal Services Encryption Level is not FIPS-140 Compliant" ---splunk-ta-nessus-end-of-event--- ",2020-02-20T17:39:19.000+0000,,,,,,,,,,,,,HOST-003,,,,,,,,,HOST-003,10.11.36.23,false,,,0b:4a:fe:06:36:92,,,untrust,,general,,false,,false,,,Thu Feb 20 17:27:48 2020,nessus nessus_misconfigured_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3",12122,,,,"Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3",,,,,,Nessus,,,Err:509,,,critical,4,,,Terminal Services Encryption Level is not FIPS-140 Compliant,Service detection,12122,eventgen,nessus,prd-p-vj7zgflpcb88,,,,,,,,,,,,,Thu Feb 20 17:27:48 2020,,,,,"inventory Show all 15 lines host = nessus_logs.csv   source = nessus_logs.csv   sourcetype = csv </pre>

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.

### Save As Alert

Settings

Title: critical nessus log with ip 10.11.36.23

Description: nessus\_logs.csv, severity=critical, IP=10.11.36.23

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run every week

On: Monday at 12:00

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results

is greater than 31

Trigger: Once For each result

Throttle: ☒

Suppress triggering for: 60 second(s)

Cancel Save

Save As Alert

When triggered

Send email

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

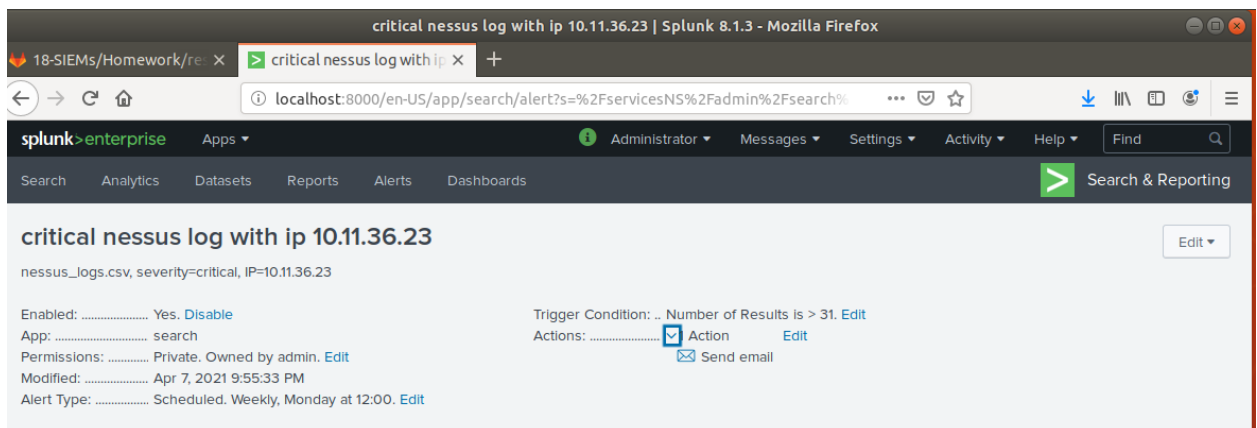
☒ Attach CSV

☒ Trigger Time

☒ Attach PDF

Cancel

Save



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

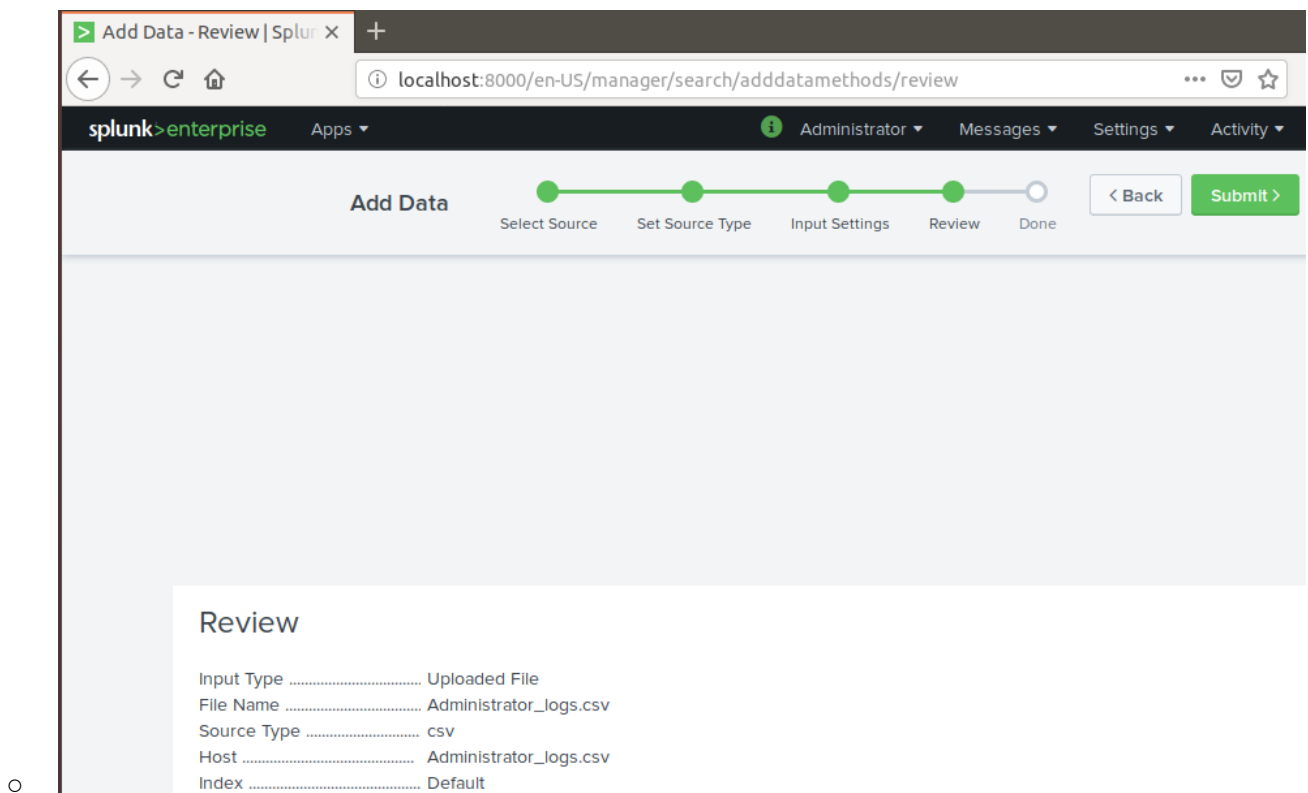
### Step 3: Drawing the (base)line

**Background:** A Vandalay 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?

See pic below of timeframe

- Hints:
  - Look for the name field to find failed logins.
  - Note the attack lasted several hours.

```
# linecount 14
a LogName 1
a Logon_GUID 100+
a Logon_ID 100+
a Logon_Process 100+
# Logon_Type 21
a member_dn 2
a member_id 14
a member_nt_domain 3
a Message 100+
a name 7
a object 1
a OpCode 1
a Operation 2
a Package_Name__NTLM_only 1
a process_id 100+
a Process_ID 100+
a product 1
a Provider_Name 100+
a punct 18
a raw 100+
```

name

7 Values, 89.524% of events

Selected

Yes

No

Reports

Top values

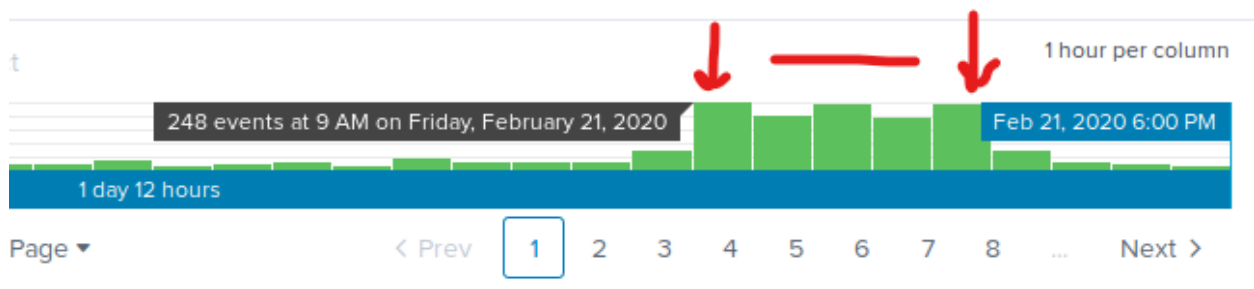
Top values by time

Rare values

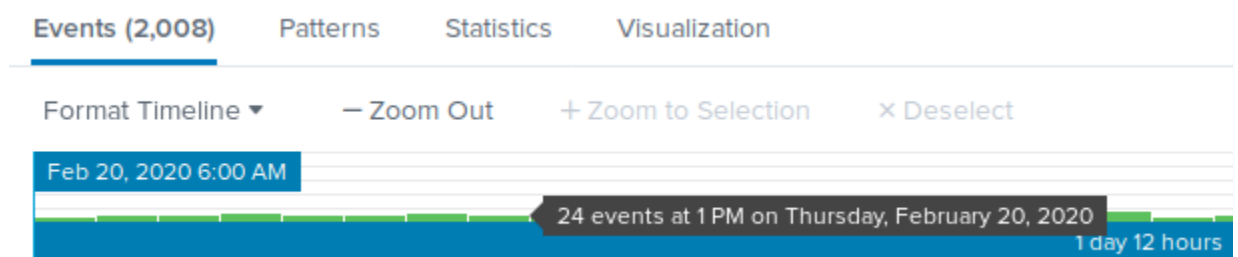
Events with this field

Values	Count	%	
An account failed to log on	2,008	29.97%	
An account was logged off	834	12.448%	
Special privileges assigned to new logon	828	12.358%	
A logon was attempted using explicit credentials	798	11.91%	
Key file operation	764	11.403%	
Cryptographic operation	738	11.015%	
An account was successfully logged on	730	10.896%	

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



**Unusual failed login activity from 9am to 1pm on Friday, February 21, 2020.**



**Significantly less failed logins during the same time of day but different day of the week.**

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

Save As Alert

Settings

Title

failed login attempts

Description

possible brute force attack

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every hour

At

0

minutes past the hour

Expires

24

hour(s)

Trigger Conditions

Trigger alert when

Number of Results

Is greater than

100

Trigger

Once

For each result

Throttle

Trigger Actions

Cancel

Save



Save As Alert

When triggered

▼

✉ Send email

Remove

To

SOC@vandalay.com

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

Priority

High ▼

Subject

Splunk Alert: failed login attempts

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 high number of failed logins was triggered.

Include

☒ Link to Alert

☐ Search String

☐ Trigger Condition

☐ Trigger Time

☒ Allow Empty

☒ Link to Results

☐ Inline [Table ▼](#)

☒ Attach CSV

☒ Attach PDF

Cancel

Save

Submit the answers to the questions about the brute force timing, baseline and threshold. Additionally, provide a screenshot as proof that the alert has been created.

## Your Submission

In a word document, provide the following:

- Answers to all questions where indicated.
- Screenshots where indicated.