

SIEM

Scenario

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

- Vandalay Industries uses Splunk for their security monitoring and have 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:

- Screen shots 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

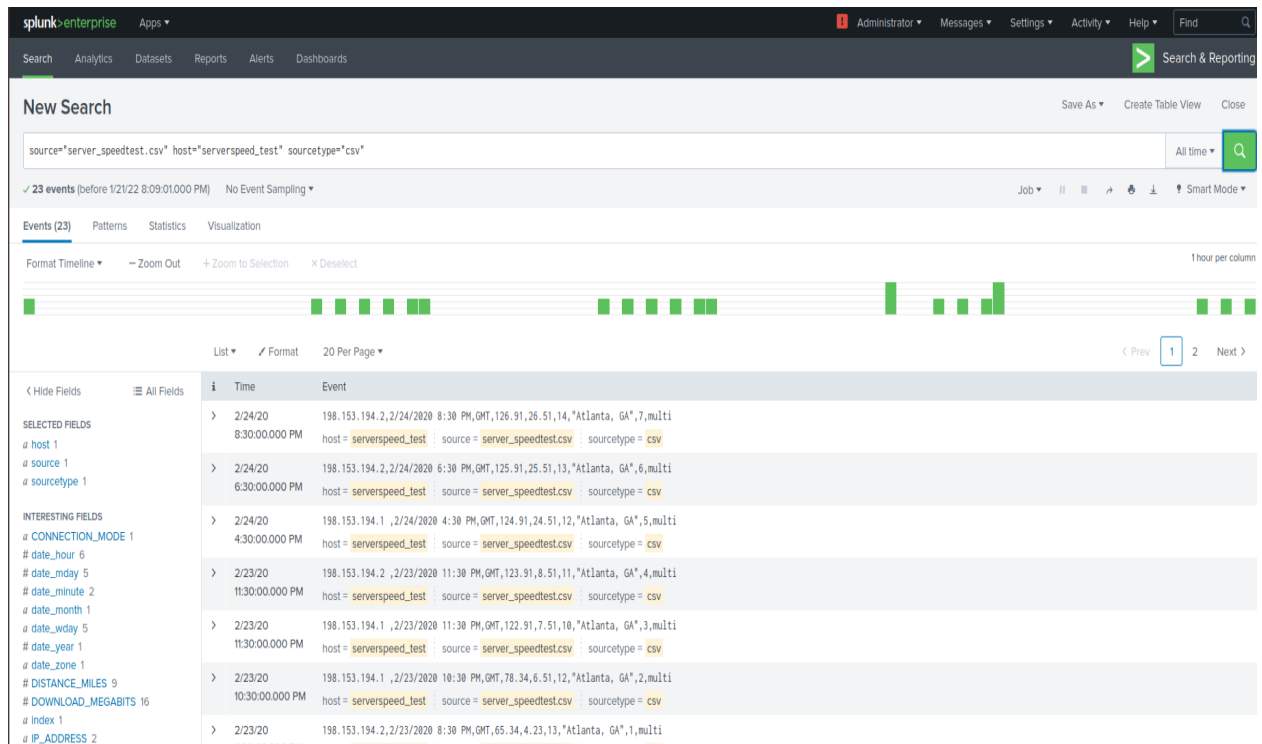
Background: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandalay has been experiencing DDOS attacks against their web servers.

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.

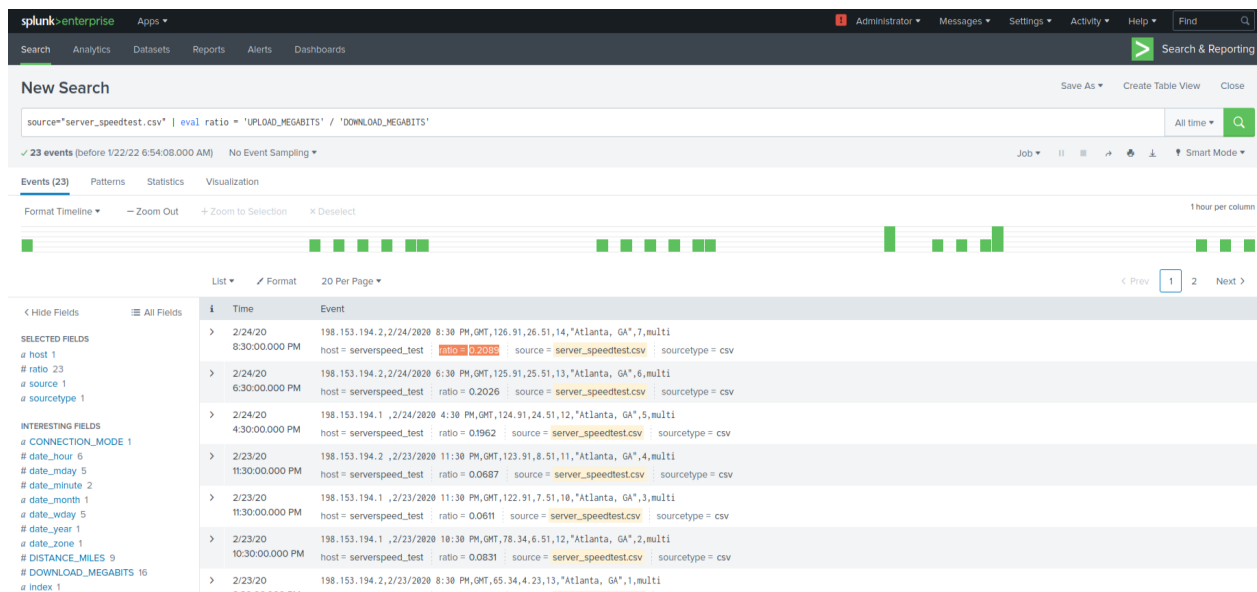
- Speed Test File



- 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'

```
source="server_speedtest.csv" | eval ratio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS'
```



The screenshot shows the Splunk Enterprise interface with a search results table. The search query is `source="server_speedtest.csv" | eval ratio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS'`. The results table has two columns: **Time** and **Event**. The **Event** column contains details about server speed tests, including host, ratio, source, and sourcetype.

Time	Event
2/24/20 8:30:00.000 PM	198.153.194.2,2/24/2020 8:30 PM,GHT,126.91,26.51,14,"Atlanta, GA",7,multi host = serverspeed_test ratio = 0.2026 source = server_speedtest.csv sourcetype = csv
2/24/20 6:30:00.000 PM	198.153.194.2,2/24/2020 6:30 PM,GHT,125.91,25.51,13,"Atlanta, GA",6,multi host = serverspeed_test ratio = 0.2026 source = server_speedtest.csv sourcetype = csv
2/24/20 4:30:00.000 PM	198.153.194.1,2/24/2020 4:30 PM,GHT,124.91,24.51,12,"Atlanta, GA",5,multi host = serverspeed_test ratio = 0.1962 source = server_speedtest.csv sourcetype = csv
2/23/20 11:30:00.000 PM	198.153.194.2,2/23/2020 11:30 PM,GHT,123.91,8.51,11,"Atlanta, GA",4,multi host = serverspeed_test ratio = 0.0687 source = server_speedtest.csv sourcetype = csv
2/23/20 11:30:00.000 PM	198.153.194.1,2/23/2020 11:30 PM,GHT,122.91,7.51,10,"Atlanta, GA",3,multi host = serverspeed_test ratio = 0.0611 source = server_speedtest.csv sourcetype = csv
2/23/20 10:30:00.000 PM	198.153.194.1,2/23/2020 10:30 PM,GHT,78.34,6.51,12,"Atlanta, GA",2,multi host = serverspeed_test ratio = 0.0831 source = server_speedtest.csv sourcetype = csv
2/23/20 8:30:00.000 PM	198.153.194.2,2/23/2020 8:30 PM,GHT,65.34,4.23,13,"Atlanta, GA",1,multi

- 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`

Hint: Use the following format when for the table command: | table fieldA fieldB fieldC

```
source="server_speedtest.csv" | eval ratio = 'UPLOAD_MEGABITS' /
'DOWNLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS
UPLOAD_MEGABITS ratio
```

The screenshot shows the Splunk Enterprise interface with a search results table. The search query is: `source="server_speedtest.csv" | eval ratio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio`. The results show 23 events. The table has columns: `_time`, `IP_ADDRESS`, `DOWNLOAD_MEGABITS`, `UPLOAD_MEGABITS`, and `ratio`. The data shows a significant drop in download speed on 2020-02-23 at 23:30:00, followed by a recovery period.

_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 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
2020-02-23 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 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 18:30:00	198.153.194.2	17.56	3.43	0.195
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
2020-02-22 23:30:00	198.153.194.2	189.16	9.51	0.0571
2020-02-22 22:30:00	198.153.194.2	189.91	8.51	0.0774
2020-02-22 20:30:00	198.153.194.2	188.91	7.51	0.0598
2020-02-22 18:30:00	198.153.194.2	187.91	13.51	0.1252
2020-02-22 16:30:00	198.153.194.2	186.91	12.51	0.1178

4. Answer the following questions:

- Based on the report created, what is the approximate date and time of the attack?

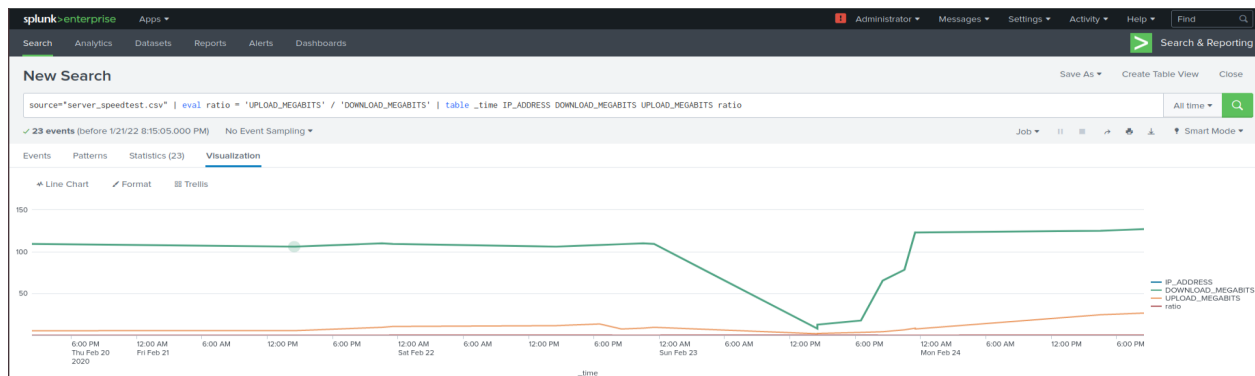
Date of attack: 2020-2-22 @ 23:30:00 through 2020-2-23 @ 23:30:00

The screenshot shows a table of network speed test data. The table has columns: `_time`, `IP_ADDRESS`, `DOWNLOAD_MEGABITS`, `UPLOAD_MEGABITS`, and `ratio`. The data shows a significant drop in download speed on 2020-02-23 at 23:30:00, followed by a recovery period.

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
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 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
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

- How long did it take your systems to recover?

Duration of system recovery: On 2020-2-23, From 14:30:00-23:30:00 (9 hours to full recovery).



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.

- Upload the following file from the Nessus vulnerability scan.

- Nessus Scan Results

The screenshot shows the Splunk Enterprise interface with a search query: `source="nessus_logs.csv" host="Nessus_scan" sourcetype="csv"`. The search results show 1,849 events. The timeline view shows a series of green bars representing events over time. The table view shows two events. The first event is a Microsoft Windows XP Service Pack 2 vulnerability detection. The second event is a Common Platform Enumeration (CPE) vulnerability detection.

Time	Event
2/20/20 6:09:23.000 PM	<pre>"start_time":"Thu Feb 20 18:09:23 2020" end_time":"Thu Feb 20 18:09:23 2020" dest_dns="HOST-003" dest_mac="52:70:fa:52:7c:e4" dest_ip="10.11.36.11" os="Microsoft Windows XP Service Pack 2" os="Microsoft Windows XP Service Pack 3" cvss_base_score="4.3" cvss_vector="CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N" dest_port_protocol="microsoft-ds(139/tcp)" severity_id="0" signature_family="Service detection" signature_id="12122" signature="Terminal Services Encryption Level is not FTPS-140 Compliant" bid="1499" cve="CVE-2017-1000385" cve="CVE-2017-17428" cve="CVE-2017-6168" cwe="280" osvdb="5230" osvdb="299" xref="OSVDB:8230" xref="OSVDB:299" xref="CVE:200" ---splunk-ta-nessus-end-of-event---</pre>
2/20/20 6:03:16.000 PM	<pre>"start_time":"Thu Feb 20 18:03:16 2020" end_time":"Thu Feb 20 18:03:16 2020" dest_ip="10.11.36.6" os="Microsoft Windows XP Professional SP3" dest_port_protocol="microsoft-ds(445/tcp)" severity_id="3" signature_id="10989" signature="Common Platform Enumeration (CPE)" dest_dns="HOST-003" dest_nt_host="ACME-003" ---splunk-ta-nessus-end-of-event---</pre>

- 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.

source="nessus_logs.csv" host="Nessus_scan" sourcetype="csv" dest_ip="10.11.36.23" severity=critical

splunk-enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

source="nessus_logs.csv" host="Nessus_scan" sourcetype="csv" dest_ip="10.11.36.23" severity=critical All time

49 events (before 1/21/22 8:44:55.000 PM) No Event Sampling Job

Events (49) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- bid 15
- cve 22
- cvss 3
- cvss_base_score 3
- cvs_vector 3
- date_hour 13
- date_mday 2
- date_minute 35
- date_month 1
- date_second 31
- date_wday 2

localhost:8000/en-US/app/search/dashboards

i	Time	Event
>	2/20/20 5:33:01.000 PM	<p>"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"</p> <p>---splunk-ta-nessus-end-of-event---</p> <p>"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-vj7zgf1pcb88,,,,,,,,,,,,,Thu Feb 20 17:33:01 2020,,,,,"inventory</p> <p>os</p> <p>report</p> <p>Show all 13 lines</p> <p>host = Nessus_scan source = nessus_logs.csv sourcetype = csv</p>
>	2/20/20 5:27:48.000 PM	<p>"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"</p> <p>---splunk-ta-nessus-end-of-event---</p> <p>"2020-02-20T17:35:19.000+0000,,,,,,,,,HOST-003,,,,,HOST-003,10.11.36.23,false,,0b:4a:fe:06:36:92,,untrust,,general,,false,,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</p> <p>Microsoft Windows XP Service Pack 3",12122,,,,,"Microsoft Windows XP Service Pack 2</p> <p>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-vj7zgf1pcb88,,,,,,,,,,,,,Thu Feb 20 17:27:48 2020,,,,,"inventory</p> <p>os</p> <p>report</p> <p>Show all 15 lines</p> <p>host = Nessus_scan source = nessus_logs.csv sourcetype = csv</p>
>	2/20/20 5:19:58.000 PM	<p>"start_time""Thu Feb 20 17:19:58 2020" end_time""Thu Feb 20 17:19:58 2020" dest_dns""HOST-003" dest_nt_host""HOST-003" dest_mac""fb:69:33:d1:44:a4" dest_ip""10.11.36.29" os""Microsoft Windows XP Service Pack 2" os""Microsoft Windows XP Service Pack 3" dest_port_proto""el-random(2426/tcp)" severity_id""4" signature_id""10989" signature""Common Platform Enumeration (CPE)"</p> <p>---splunk-ta-nessus-end-of-event---</p> <p>"2020-02-20T18:07:40.000+0000,,,,,,,,,HOST-003,,,,,HOST-003,10.11.36.23,false,,fb:69:33:d1:44:a4,HOST-003,,untrust,2426,el-random(2426/tcp),.false,.false,false,,Thu Feb 20 17:19:58 2020,nessus_nessus_misconfigured_device_nes</p>

Nessus report

splunk-enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Nessus Scan Results

Edit More Info Add to Dashboard

All time

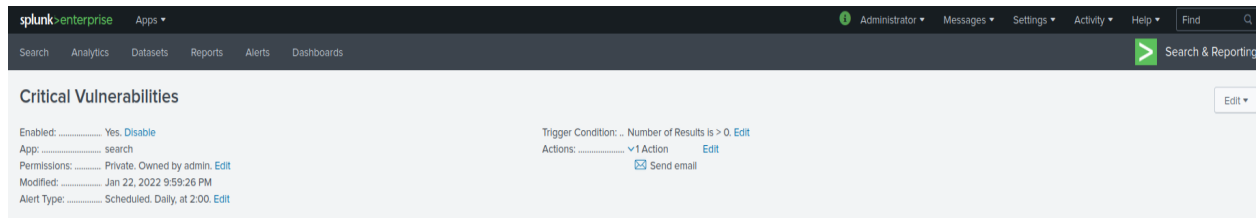
49 events (before 1/21/22 6:40:18.000 AM) Job

20 per page

< Prev 1 2 3 Next >

i	Time	Event
>	2/20/20 5:33:01.000 PM	<p>"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"</p> <p>---splunk-ta-nessus-end-of-event---</p> <p>"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-vj7zgf1pcb88,,,,,,,,,,,,,Thu Feb 20 17:33:01 2020,,,,,"inventory</p> <p>os</p> <p>report</p> <p>Show all 13 lines</p> <p>host = Nessus_scan source = nessus_logs.csv sourcetype = csv</p>
>	2/20/20 5:27:48.000 PM	<p>"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"</p> <p>---splunk-ta-nessus-end-of-event---</p> <p>"2020-02-20T17:35:19.000+0000,,,,,,,,,HOST-003,,,,,HOST-003,10.11.36.23,false,,0b:4a:fe:06:36:92,,untrust,,general,,false,,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</p> <p>Microsoft Windows XP Service Pack 3",12122,,,,,"Microsoft Windows XP Service Pack 2</p> <p>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-vj7zgf1pcb88,,,,,,,,,,,,,Thu Feb 20 17:27:48 2020,,,,,"inventory</p> <p>os</p> <p>report</p> <p>Show all 15 lines</p> <p>host = Nessus_scan source = nessus_logs.csv sourcetype = csv</p>
>	2/20/20 5:19:58.000 PM	<p>"start_time""Thu Feb 20 17:19:58 2020" end_time""Thu Feb 20 17:19:58 2020" dest_dns""HOST-003" dest_nt_host""HOST-003" dest_mac""fb:69:33:d1:44:a4" dest_ip""10.11.36.29" os""Microsoft Windows XP Service Pack 2" os""Microsoft Windows XP Service Pack 3" dest_port_proto""el-random(2426/tcp)" severity_id""4" signature_id""10989" signature""Common Platform Enumeration (CPE)"</p> <p>---splunk-ta-nessus-end-of-event---</p> <p>"2020-02-20T18:07:40.000+0000,,,,,,,,,HOST-003,,,,,HOST-003,10.11.36.23,false,,fb:69:33:d1:44:a4,HOST-003,,untrust,2426,el-random(2426/tcp),.false,.false,false,,Thu Feb 20 17:19:58 2020,nessus_nessus_misconfigured_device_nes</p>

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.



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

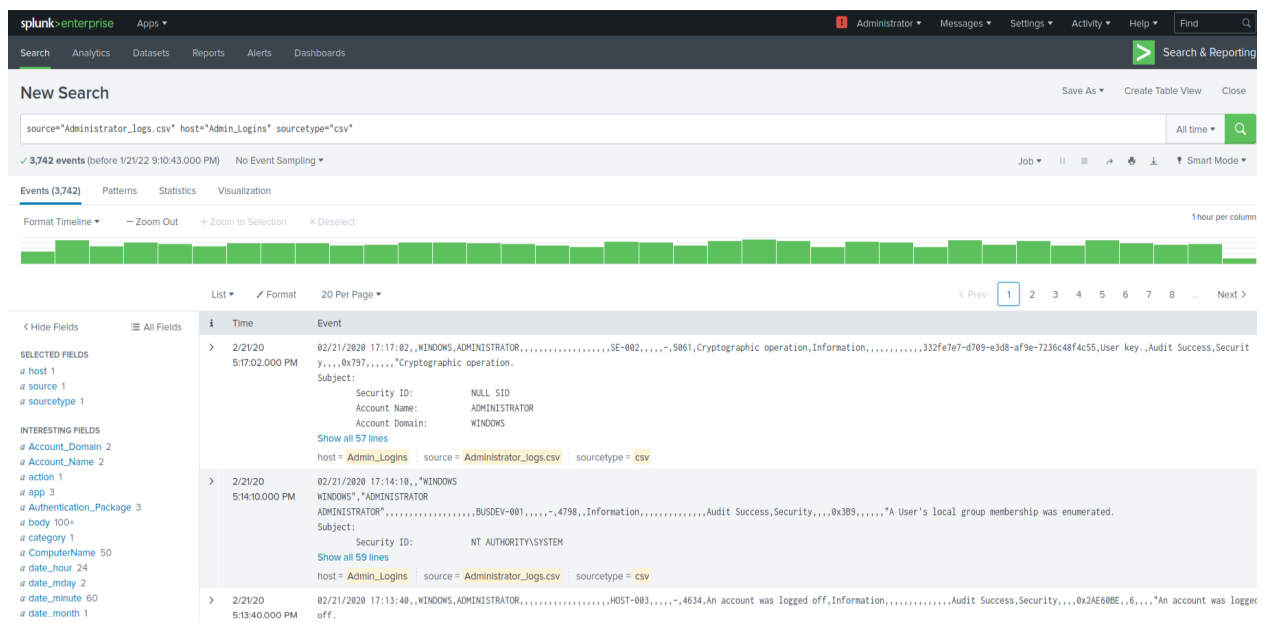
Step 3: Drawing the (base)line

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

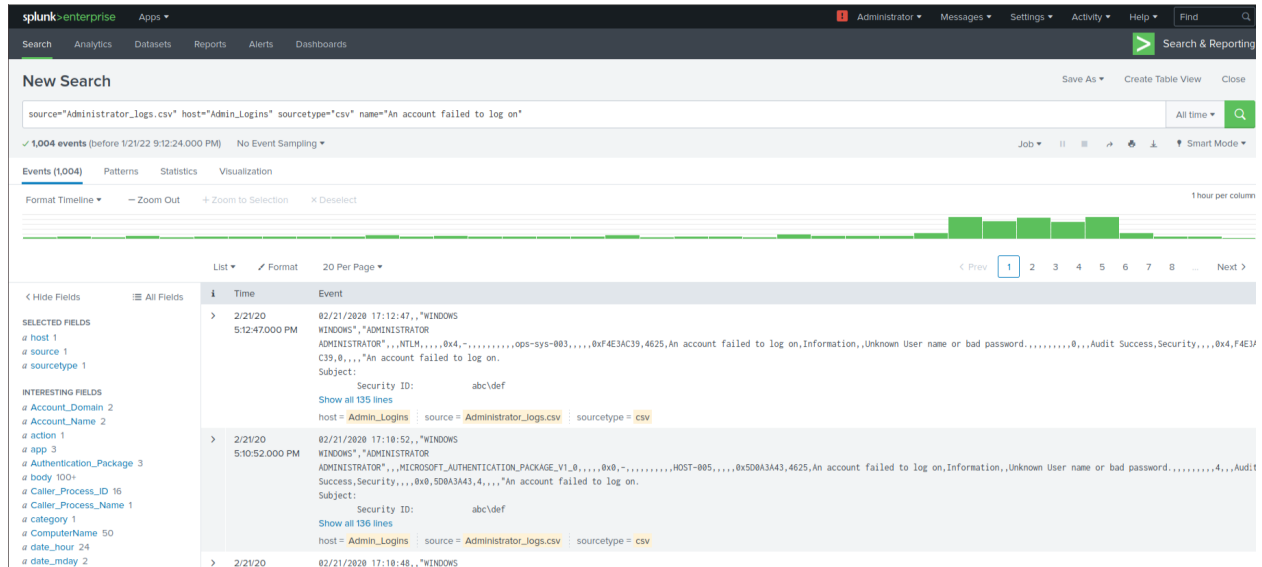


2. When did the brute force attack occur?

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

Time & date of Brute Force attack: **2020-2-21 from 9AM-1PM**

Duration of attack: **5 hours**



3. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring. **The normal range of logins fails is between 11-23 events.**

The chosen baseline for normal activity is: **28**

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

The screenshot shows the Splunk Alert configuration page for an alert named "Brute Force Attack". The alert is enabled and scheduled hourly. The trigger condition is set to "Number of Results is > 28". The actions are configured to send an email to `SOC@vandalay.com` every 1 action.

Alert Name: Brute Force Attack

Enabled: ☒ Yes [Disable](#)

App: [search](#)

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

Modified: Jan 22, 2022 10:10:08 PM

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

Trigger Condition: [Number of Results is > 28](#) [Edit](#)

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

[Send email](#)

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.