## Activity File: Part 2 - Defend Your SOC

- VSI recently experienced several cyberattacks, likely from their adversary JobeCorp.

- Fortunately, your SOC team had set up several monitoring solutions to help VSI quickly identify what was attacked.

- These monitoring solutions will also help VSI create mitigation strategies to protect the organization.

You have been provided two logs files of suspicious activity:

- One for a Windows server

- One for an Apache web server

### Windows Server Logs

Load the logs in your Splunk environment.

- Select all default options provided.

- \*\*Important:\*\* For the time range, always select \*\*All Time\*\*.

- \*\*Important:\*\* For the time range, always select \*\*All Time\*\*.

- \*\*Important:\*\* For the time range, always select \*\*All Time\*\*.

Now you will review the reports you created in Part 1 and analyze the results.

#### Report Analysis for Severity

1. Access the \*\*Reports\*\* tab and select \*\*Yours\*\* to view the reports created from Part 1.

2. Select the report you created to analyze the different severities.

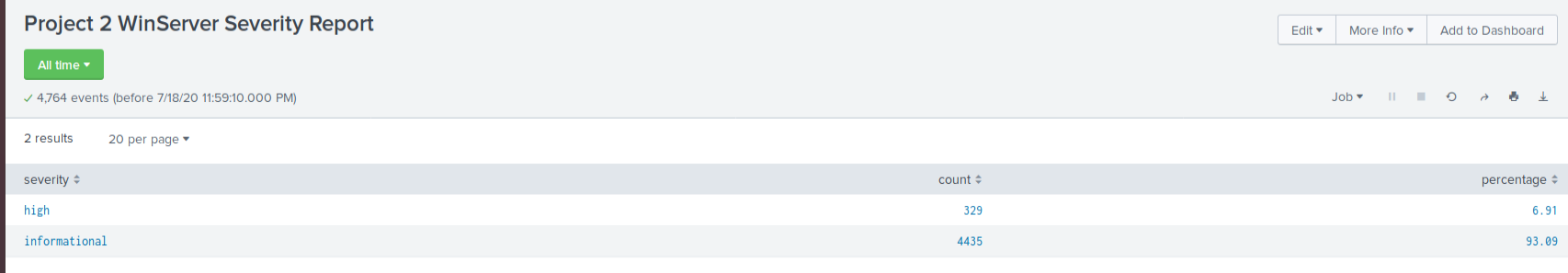
3. Select \*\*Edit\*\* > \*\*Open in Search\*\*.

4. Take note of the percentages of different severities.

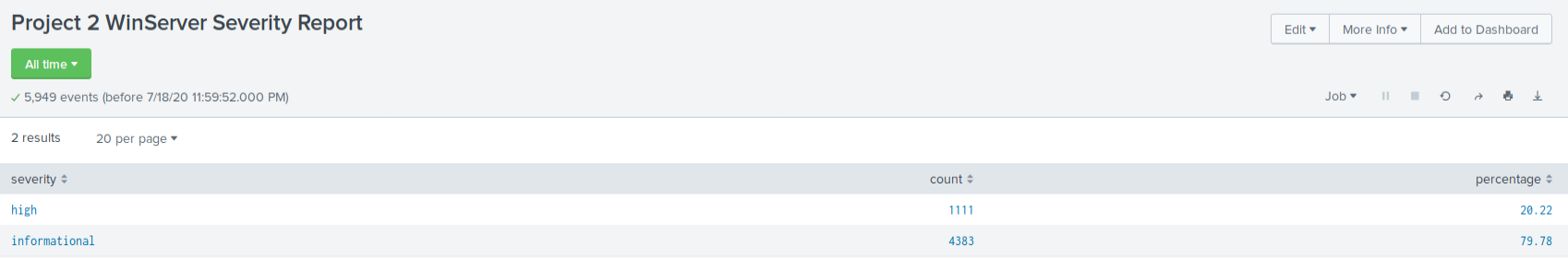
5. Change the source from `windows\_server\_logs.csv` to "`source="windows\_server\_attack\_logs.csv`

6. Select \*\*Save\*\*.

**BEFORE:**

****

**AFTER:**



Review the updated results and answer the following question:

**- Did you detect any suspicious changes in severity? Yes, the percentage of HIGH priority incidents increased for 7% to 20%.**

#### Report Analysis for Failed Activities

1. Access the \*\*Reports\*\* tab and select \*\*Yours\*\* to view the reports created from Part 1.

2. Select the report you created to analyze the different activities.

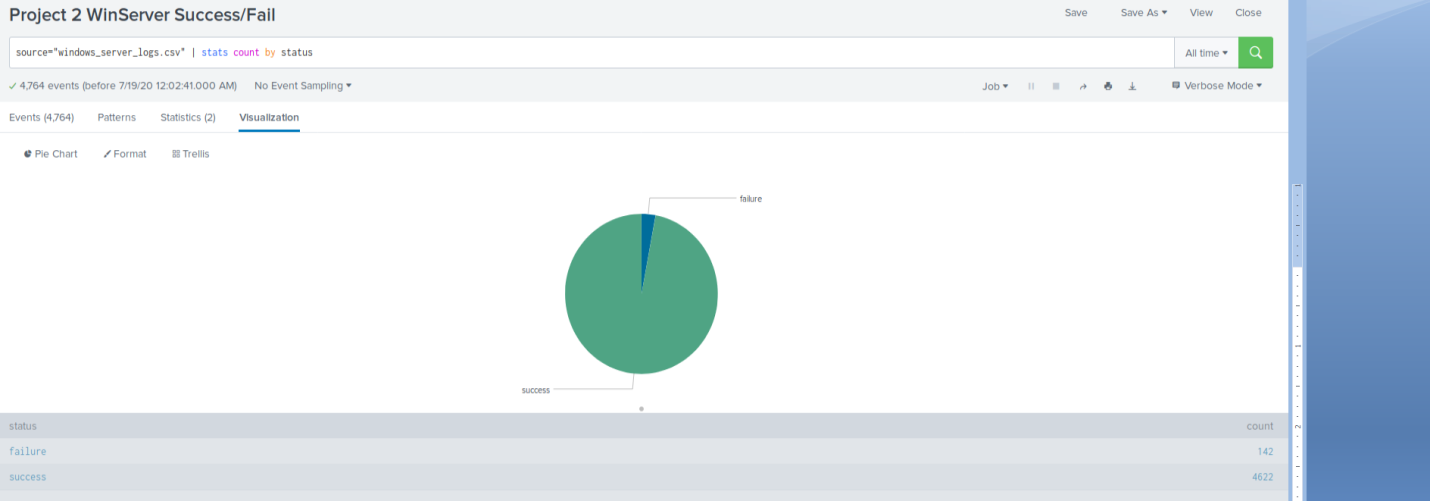
3. Select \*\*Edit\*\* > \*\*Open in Search\*\*.

4. Take note of the failed activities percentage.

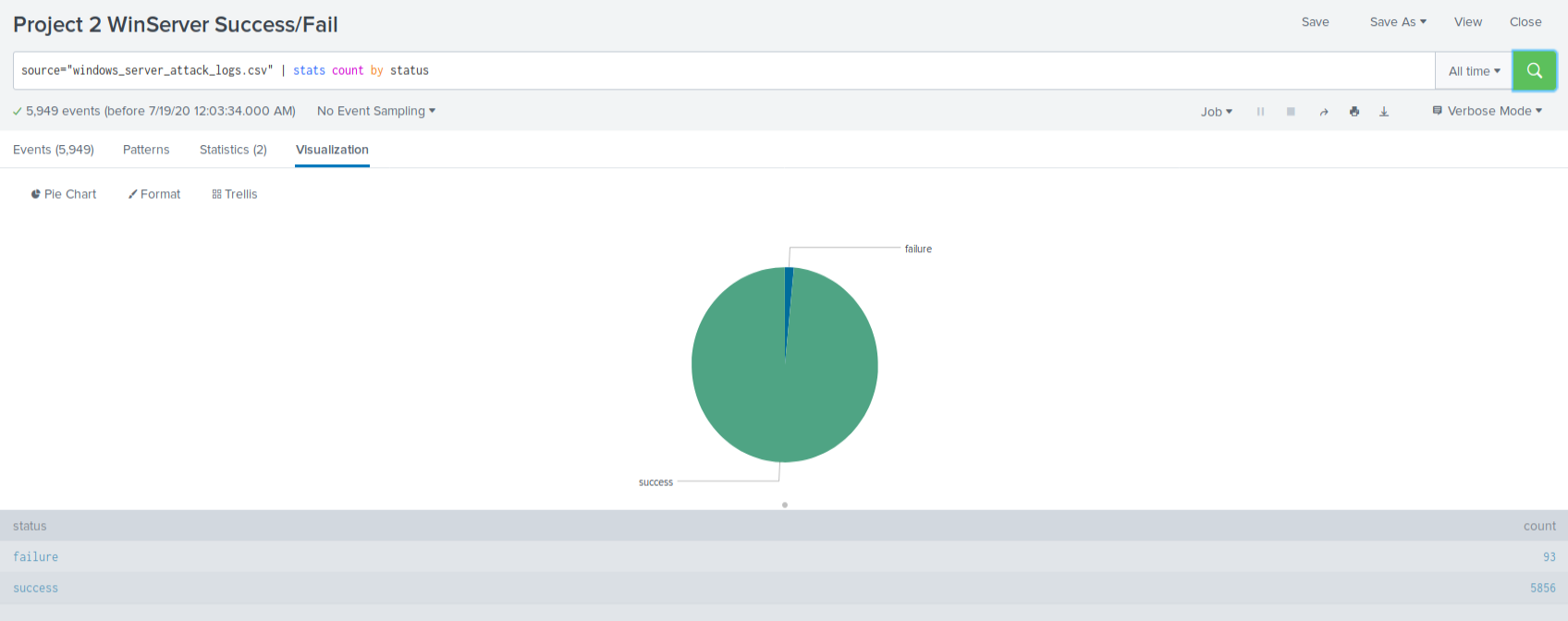
5. Change the source from `windows\_server\_logs.csv` to "`source="windows\_server\_attack\_logs.csv`.

6. Select \*\*Save\*\*.

**BEFORE:**

****

**AFTER:**

****

Review the updated results and answer the following question:

**- Did you detect any suspicious changes in failed activities? Not sure if it is suspicious but the failure count dropped from 142 to 93**

---

Now you will review the alerts you created in Part 1 and analyze the results.

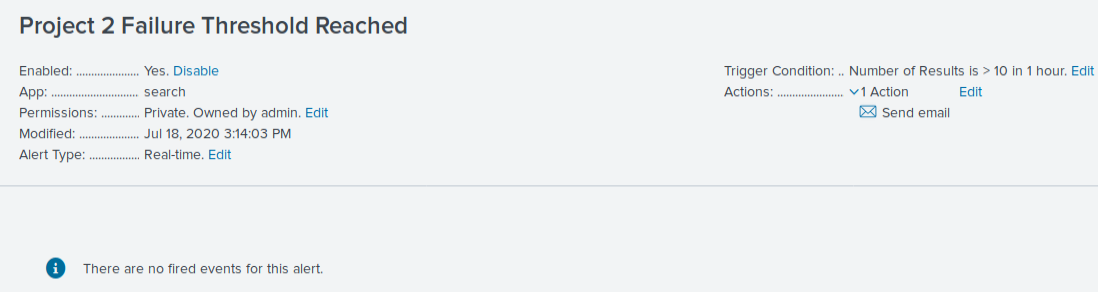
#### Alert Analysis for Failed Windows Activity

1. Access the \*\*Alerts\*\* tab and select \*\*Yours\*\* to view the alerts created in Part 1.

2. Select the alert for suspicious volume of failed activities.

3. Select \*\*Open in Search\*\*.

BEFORE:



5. Change the source from `windows\_server\_logs.csv` to "`source="windows\_server\_attack\_logs.csv`.

Review the updated results and answer the following questions:

**- Did you detect a suspicious volume of failed activity? Yes, we set the threshold for failure attempts at 10. The failure count during the attacks rose to 35 in a single hour.**

**- If so, what was the count of events in the hour(s) it occurred? 35**

**- When did it occur? 8AM to 9AM March 25, 2020.**

**- Would your alert be triggered for this activity? Ideally yes. However, the alert was created for real-time events and since this was a historical feed of events from the past, the alert did not trigger.**

**- After reviewing, would you change your threshold from what you previously selected? No, I am happy with my threshold of 10.**

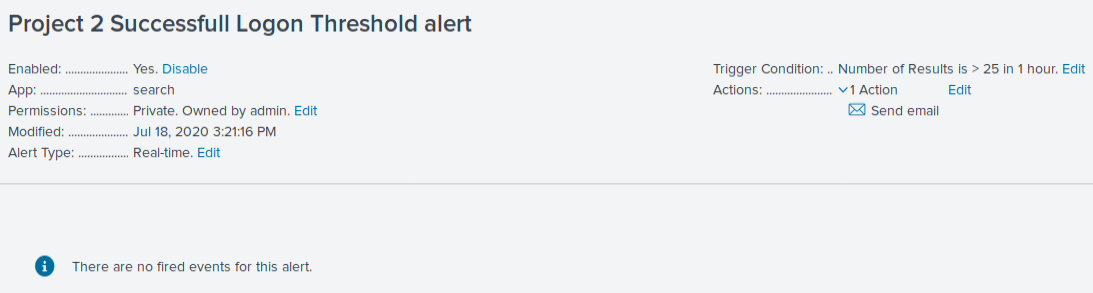
#### Alert Analysis for Successful Logons

1. Access the \*\*Alerts\*\* tab and select \*\*Yours\*\* to view the alerts created in Part 1.

2. Select the alert of suspicious volume of successful logons.

3. Select \*\*Open in Search\*\*.

**BEFORE:**



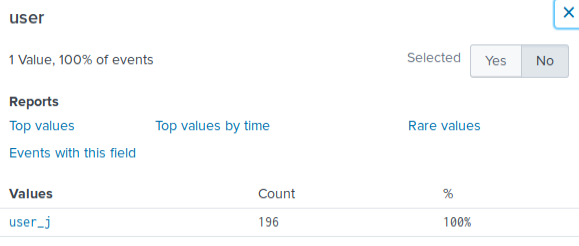
5. Change the source from `windows\_server\_logs.csv` to "`source="windows\_server\_attack\_logs.csv`.

Review the updated results, and answer the following questions:

**- Did you detect a suspicious volume of successful logons? Yes**

**- If so, what was the count of events in the hour(s) it occurred? 196 events between 11Am and 12PM March 25,2020.**

**- Who is the primary user logging in? user\_j**



**- When did it occur? between 11AM and 12PM March 25,2020.**

**- Would your alert be triggered for this activity? Yes, my alert was set for 25**

**- After reviewing, would you change your threshold from what you previously selected? No.**

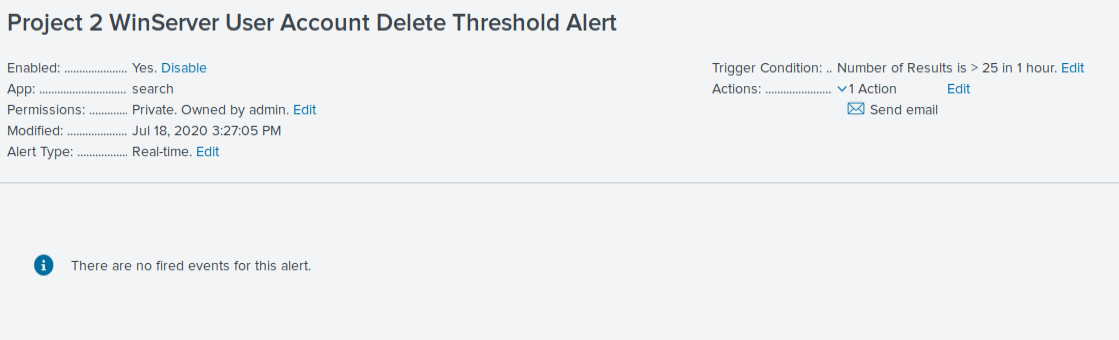
#### Alert Analysis for Deleted Accounts

1. Access the \*\*Alerts\*\* tab and select \*\*Yours\*\* to view the alerts created in Part 1.

2. Select the alert of suspicious volume of deleted accounts.

3. Select \*\*Open in Search\*\*.

**BEFORE:**

****

4. Change the source from `windows\_server\_logs.csv` to "`source="windows\_server\_attack\_logs.csv`.

Review the updated results and answer the following question:

**1. Did you detect a suspicious volume of deleted accounts? No. There was no activity for this alert that looked suspicious.**

---

Now you will set up a dashboard and analyze the results.

#### Dashboard Setup

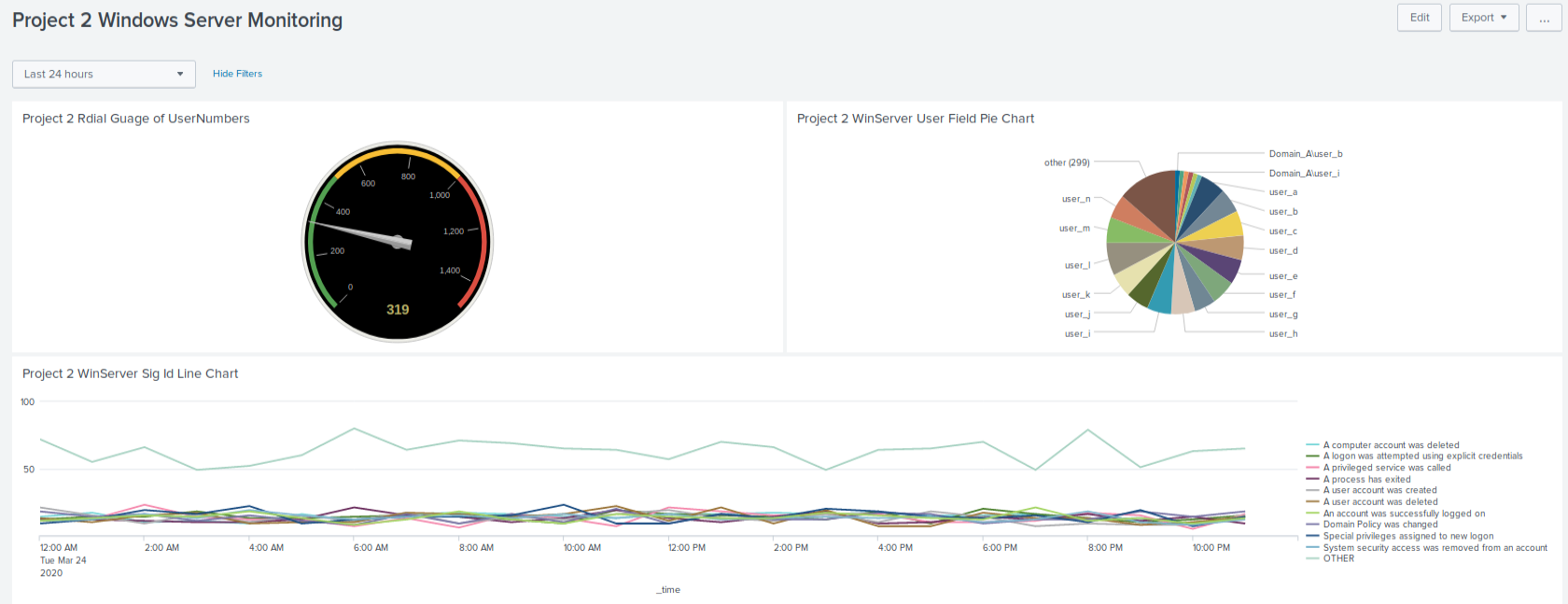
1. Access the \*\*Windows Server Monitoring\*\* dashboard.

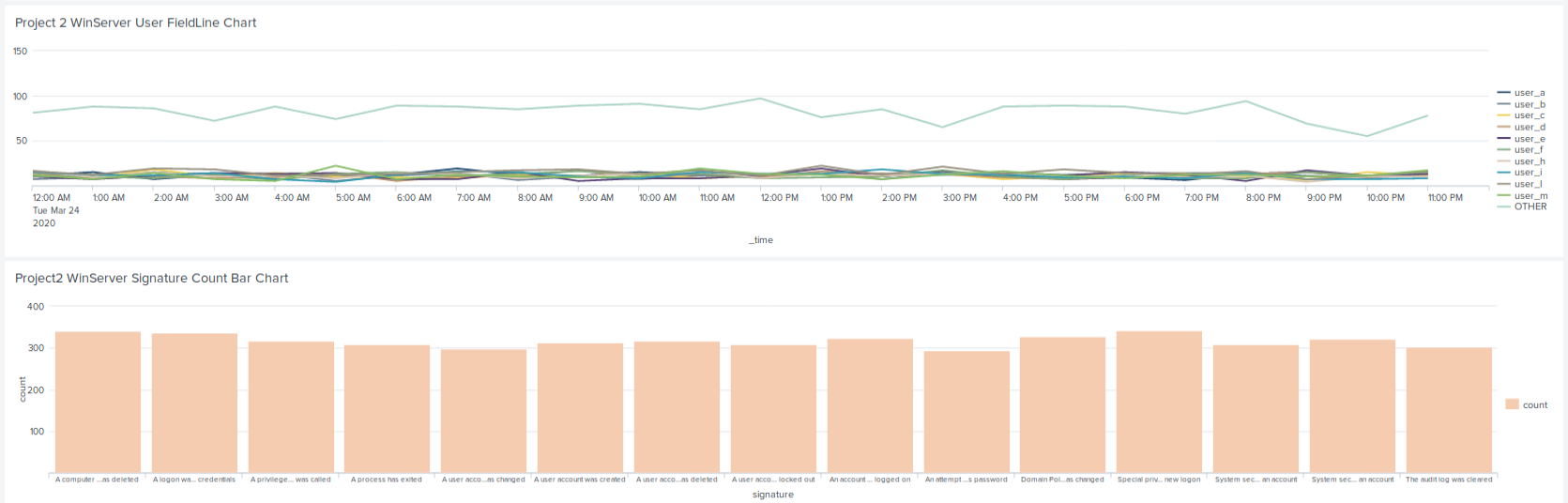
- Select \*\*Edit\*\*.

2. Access each panel you created and complete the following:

- Select \*\*Edit Search\*\*.

**BEFORE:**





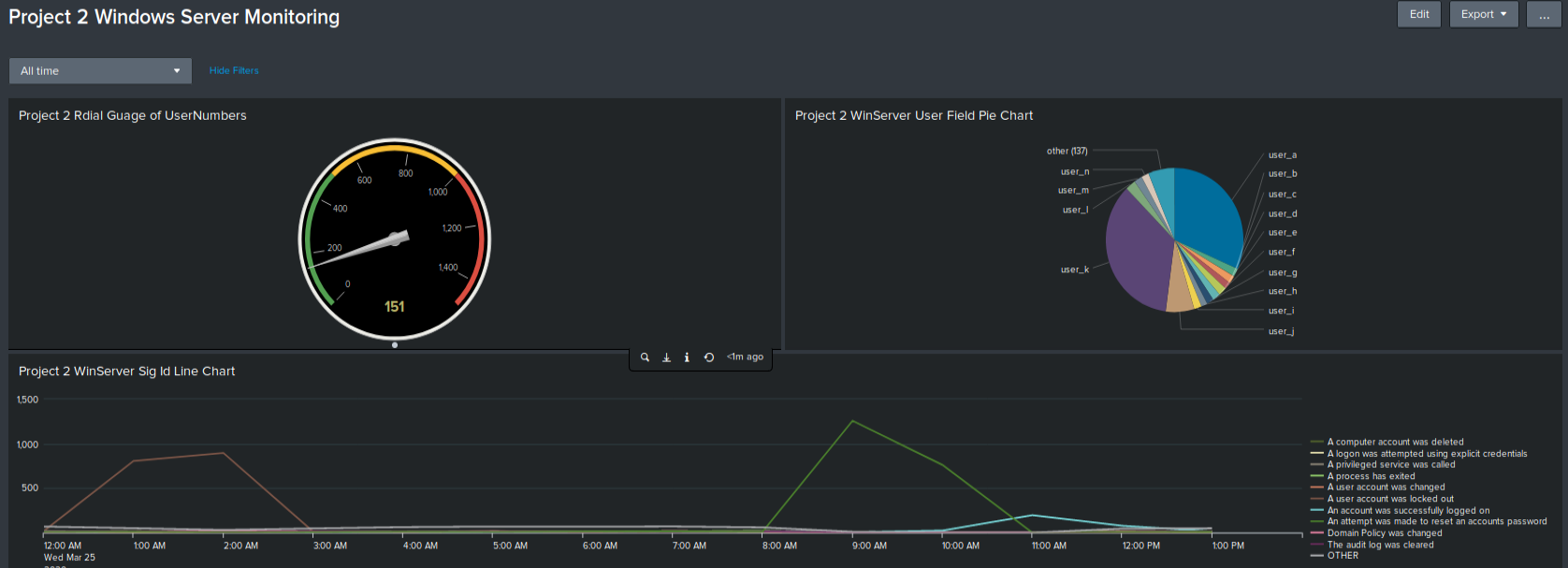
- Change the source from: `windows\_server\_logs.csv` to `source="windows\_server\_attack\_logs.csv`.

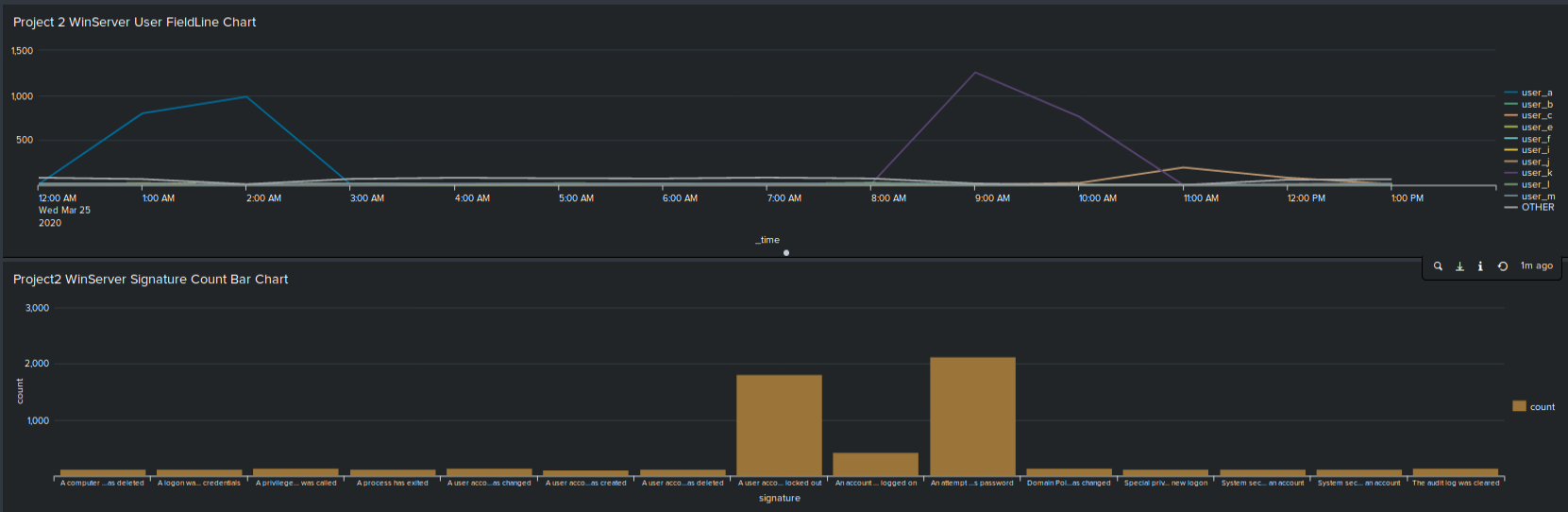
- Select \*\*Apply\*\*.

- Save the dashboard.

- Edit the time on the dashboard to be \*\*All Time\*\*.

**AFTER:**





#### Dashboard Analysis for Time Chart of Signatures

Analyze your new dashboard results and answer the following questions:

**- Does anything stand out as suspicious? Yes**

- What signatures stand out? **Activities involving locked out user accounts and attempts to change passwords rose sharply.**

**- What time did it begin/stop for each signature?**

**For Locked out user accounts: Time was between midnight and 3AM**

**For resetting account passwords: Time was between 8AM and 11AM**

- What is the peak count of the different signatures?

**For Locked out user accounts: 984**

**For resetting account passwords: 1256**

#### Dashboard Analysis for Users

Analyze your new dashboard results and answer the following questions:

**- Does anything stand out as suspicious?Yes**

**- Which users stand out? Users A and K**

**- What time did it begin and stop for each user? Same answer as above**

**- What is the peak count of the different users? Same answer as above**

#### Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

Analyze your new dashboard results and answer the following questions:

**- Does anything stand out as suspicious? Yes.**

**- Do the results match your findings in your time chart for signatures? Yes**

#### Dashboard Analysis for Users with Bar, Graph, and Pie Charts

Analyze your new dashboard results, and answer the following questions:

**- Does anything stand out as suspicious? Yes**

**- Do the results match your findings in your time chart for users? Yes**

#### Dashboard Analysis for Users with Statistical Charts

Analyze your new dashboard results, and answer the following question:

- What are the advantages and disadvantages of using this report, compared to the other user panels you created?

---

### Apache Web Server Logs

Load the logs in your Splunk environment.

- Select all default options provided.

- \*\*Important:\*\* For the time range, always select \*\*All Time\*\*.

Now you will review the reports you created in Part 1 and analyze the results.

#### Report Analysis for Methods

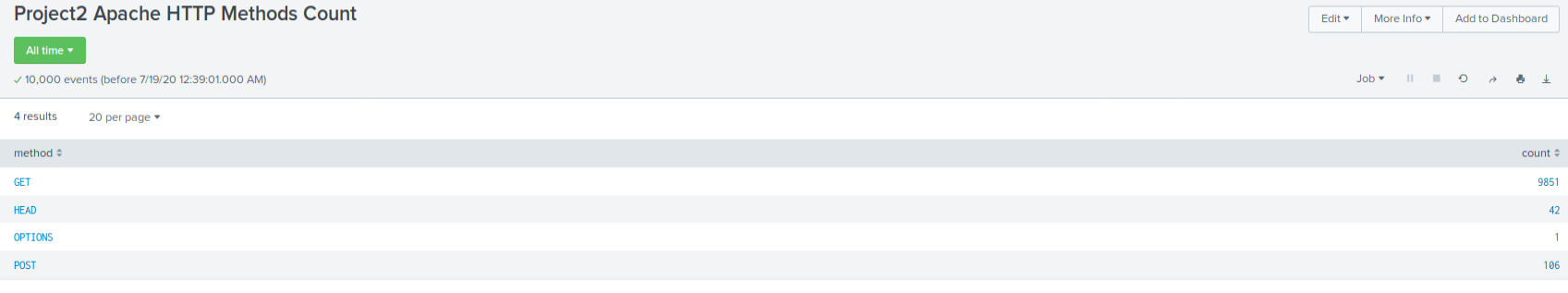
1. Access the \*\*Reports\*\* tab and select \*\*Yours\*\* to view the reports created from Part 1.

2. Select the report that analyzes the different HTTP methods.

3. Select \*\*Edit\*\* > \*\*Open in Search\*\*.

4. Take note of the percent/count of the various methods.

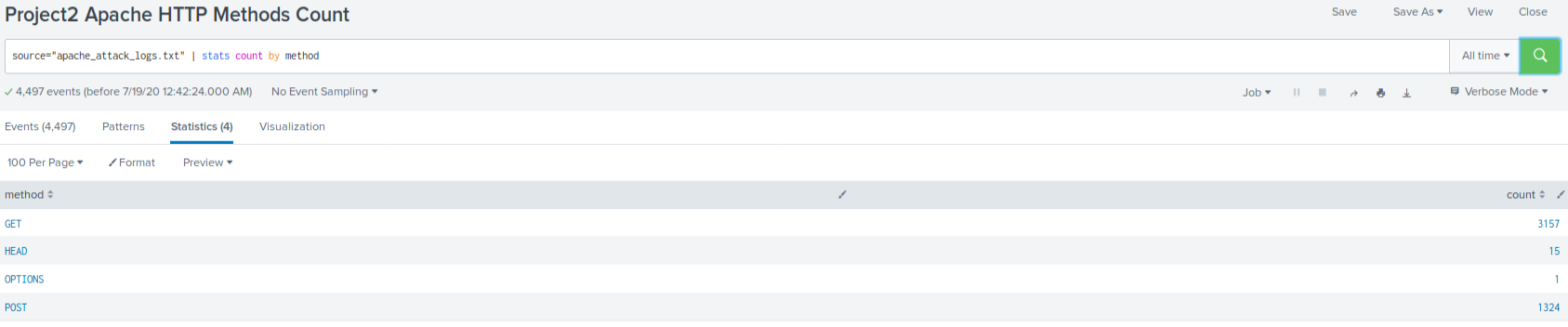
**BEFORE:**



5. Change the source from: `source=apache\_logs.txt` to `source="apache\_attack\_logs.txt`.

6. Select \*\*Save\*\*.

**AFTER:**



Review the updated results and answer the following questions:

**1. Did you detect any suspicious changes in HTTP methods? If so which one? Yes, POST.**

**2. What is that method used for? Inputting data to the website**

#### Report Analysis for Referrer Domains

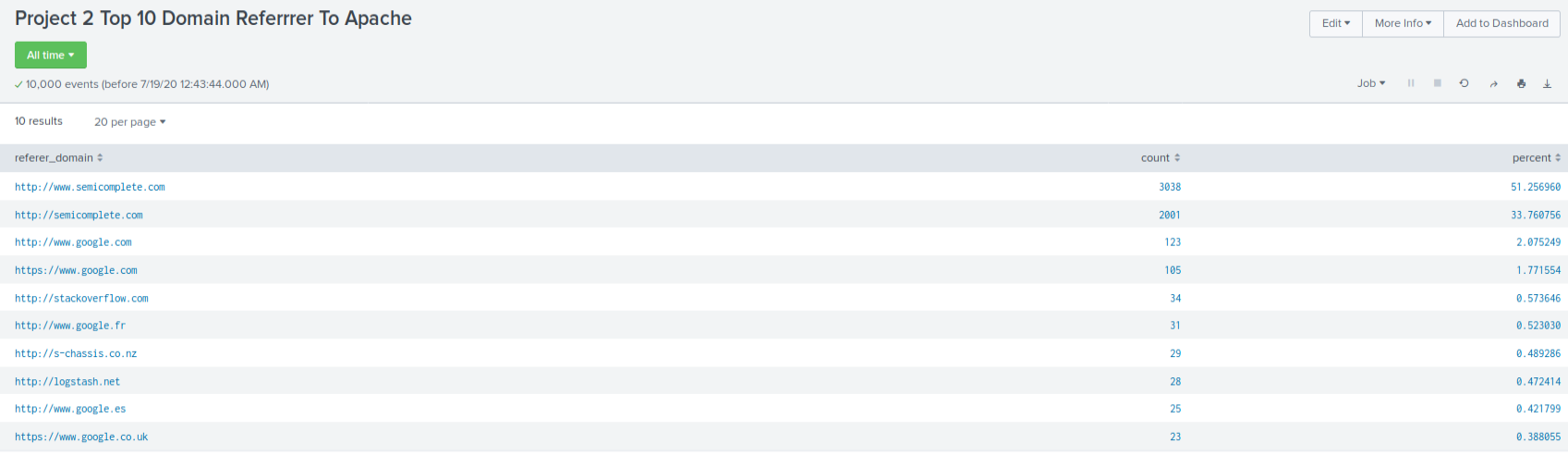
1. Access the \*\*Reports\*\* tab and select \*\*Yours\*\* to view the reports created from Part 1.

2. Select the report that analyzes the different referrer domains.

3. Select \*\*Edit\*\* > \*\*Open in Search\*\*.

4. Take note of the different referrer domains.

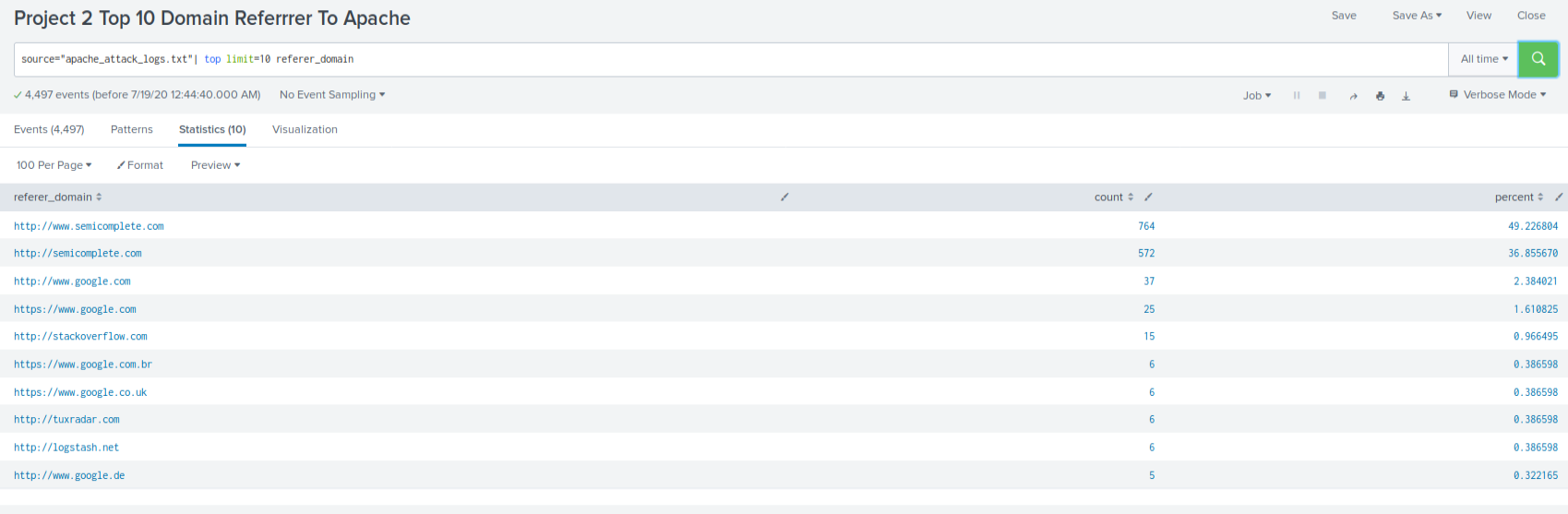
**BEFORE:**



5. Change the source from: `source=apache\_logs.txt` to `source="apache\_attack\_logs.txt`.

6. Select \*\*Save\*\*.

**AFTER:**



Review the updated results, and answer the following question:

**1. Did you detect any suspicious changes in referrer domains? No**

#### Report Analysis for HTTP Response Codes

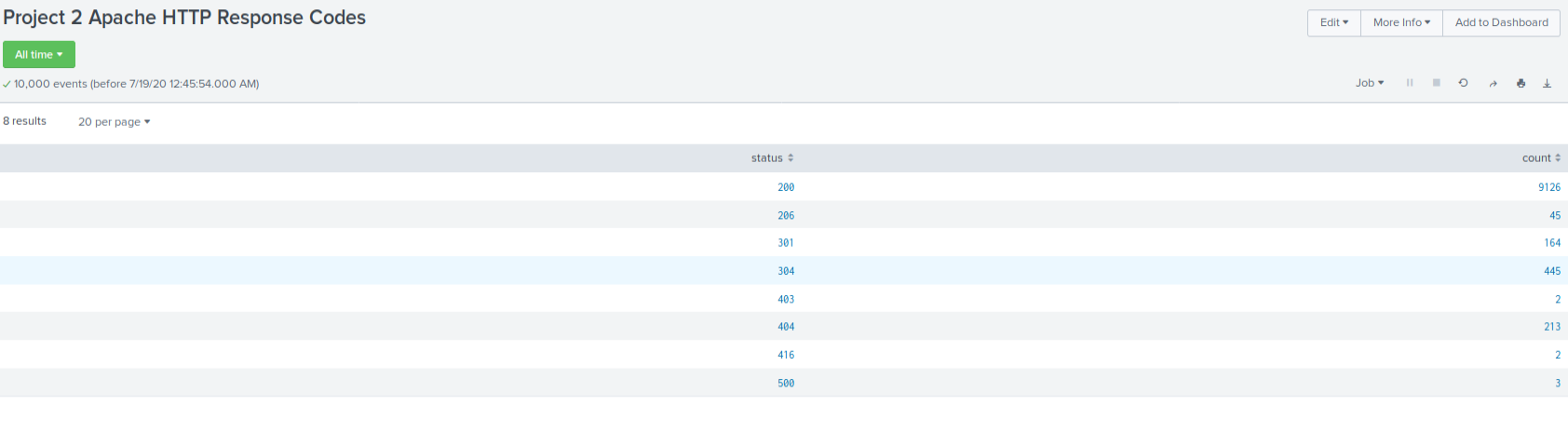
1. Access the \*\*Reports\*\* tab and select \*\*Yours\*\* to view the reports created from Part 1.

2. Select the report that analyzes the different HTTP response codes.

3. Select \*\*Edit\*\* > \*\*Open in Search\*\*.

4. Take a note of the different HTTP response codes.

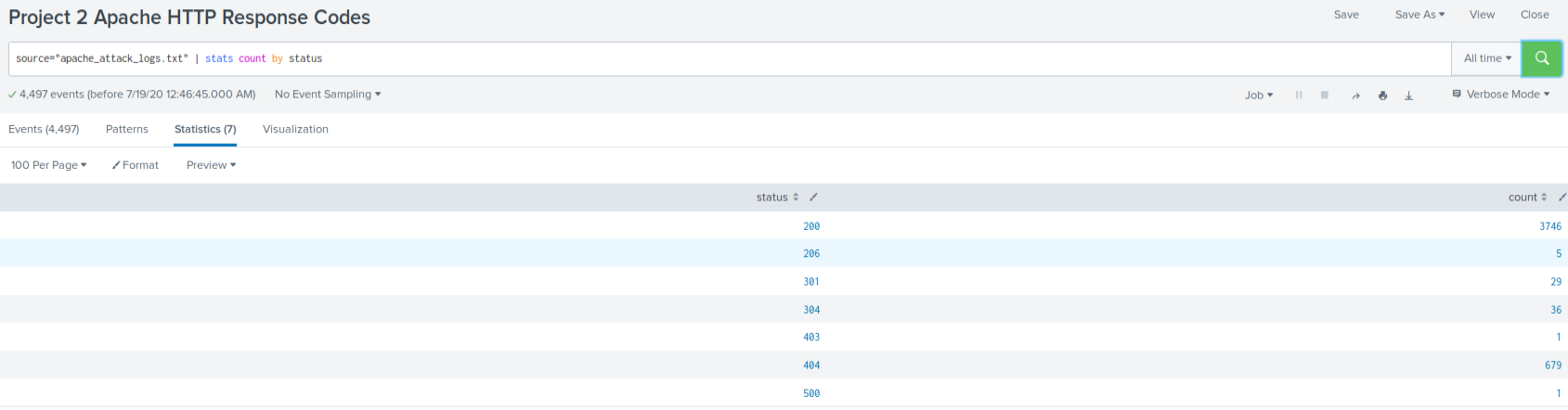
**BEFORE:**



5. Change the source from: `source=apache\_logs.txt` to `source="apache\_attack\_logs.txt`.

6. Select \*\*Save\*\*.

**AFTER:**

****

Review the updated results and answer the following question:

**1. Did you detect any suspicious changes in HTTP response codes? Yes, the numbers of 301, 304 and 404 error codes spiked. This indicates some kind of re-direct (spoofing) activity.**

---

Now you will review the alerts you created in Part 1 and analyze the results.

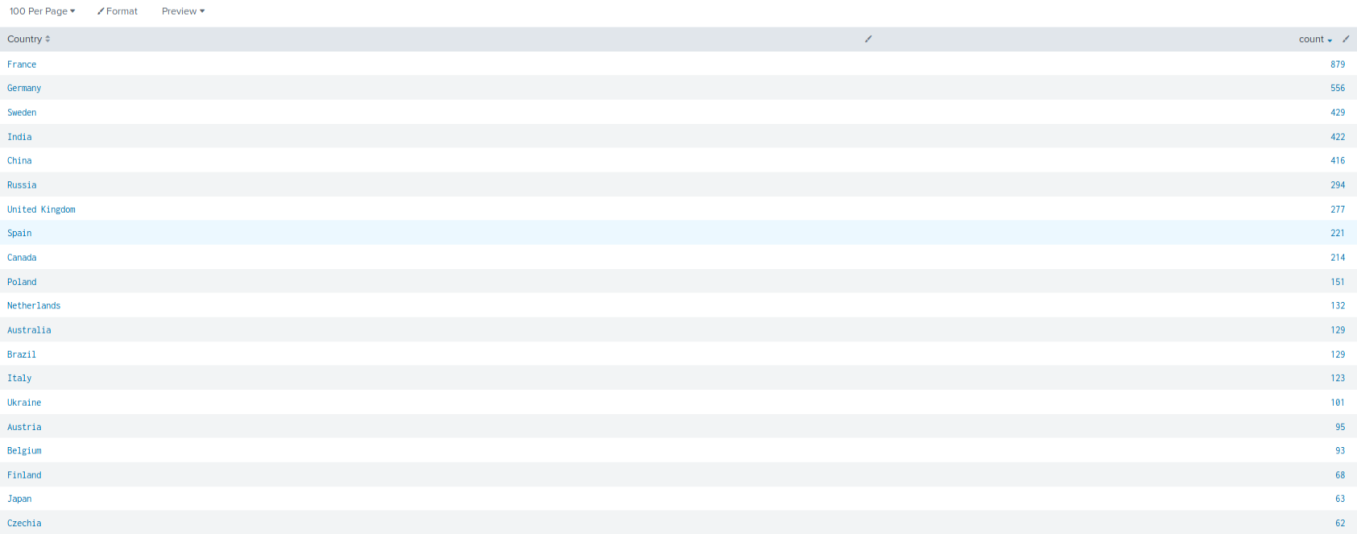
#### Alert Analysis for International Activity

1. Access the \*\*Alerts\*\* tab and select \*\*Yours\*\* to view the alerts created in Part 1.

2. Select the alert of suspicious volume of international activity.

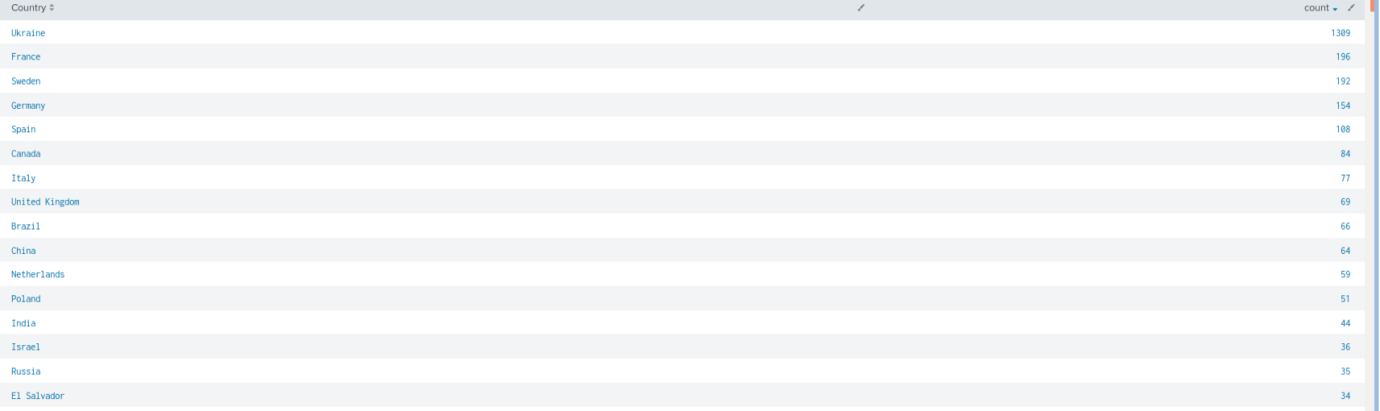
3. Select \*\*Open in Search\*\*.

**BEFORE:**



4. Change the source from: `source=apache\_logs.txt` to `source="apache\_attack\_logs.txt`.

**AFTER:**

****

Review the updated results and answer the following questions:

**- Did you detect a suspicious volume of international activity? Yes**

**- If so, what was the count of the hour it occurred in? From Ukraine between 8PM and 9PM**

**- Would your alert be triggered for this activity? Yes. My threshold was set to 1000.**

**- After reviewing, would you change the threshold you previously selected? No**

#### Alert Analysis for HTTP POST Activity

1. Access the \*\*Alerts\*\* tab and select \*\*Yours\*\* to view the alerts created in Part 1.

2. Select the alert of suspicious volume of HTTP POST activity.

3. Select \*\*Open in Search\*\*.

4. Change the source from: `source=apache\_logs.txt` to `source="apache\_attack\_logs.txt`.

Review the updated results, and answer the following questions:

**- Did you detect any suspicious volume of HTTP POST activity? Yes**

**- If so, what was the count of the hour it occurred in? 1296 Events**

**- When did it occur? 8PM to 9PM**

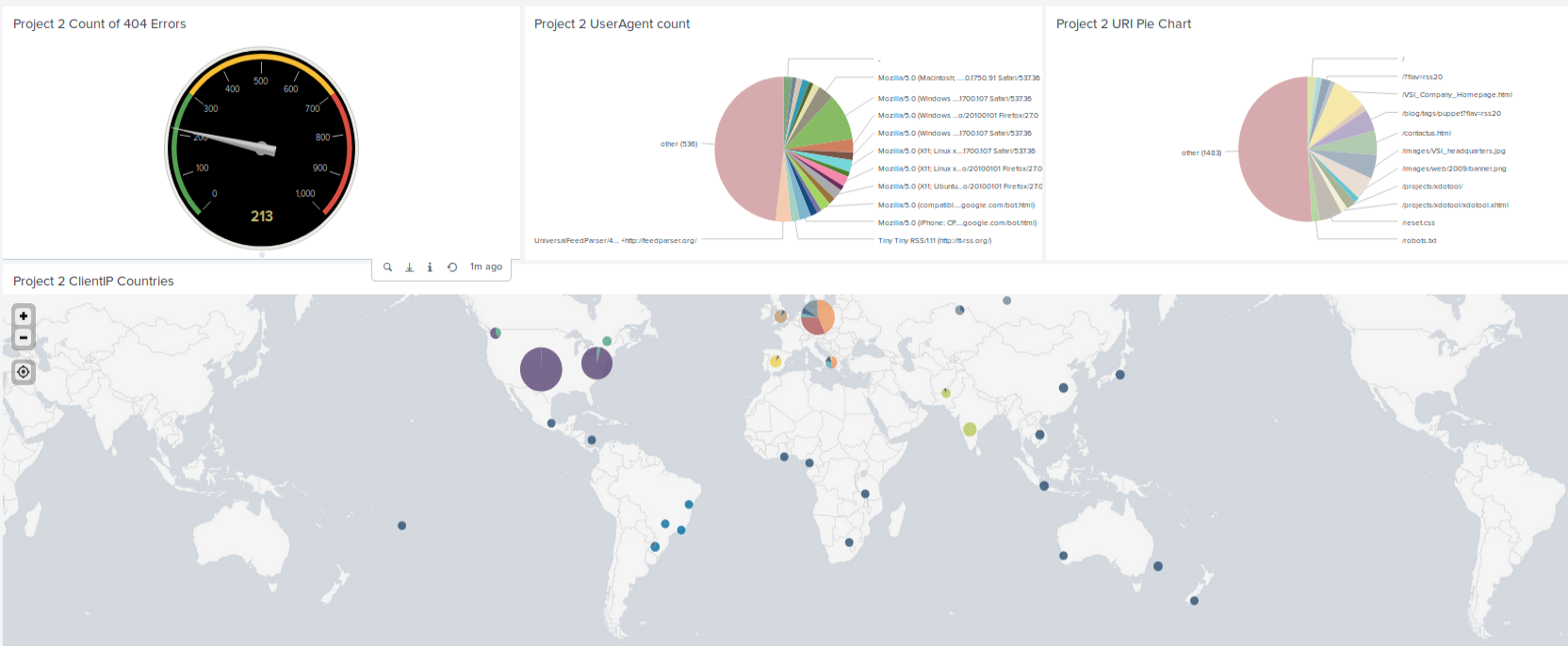
**- After reviewing, would you change the threshold that you previously selected? No.**

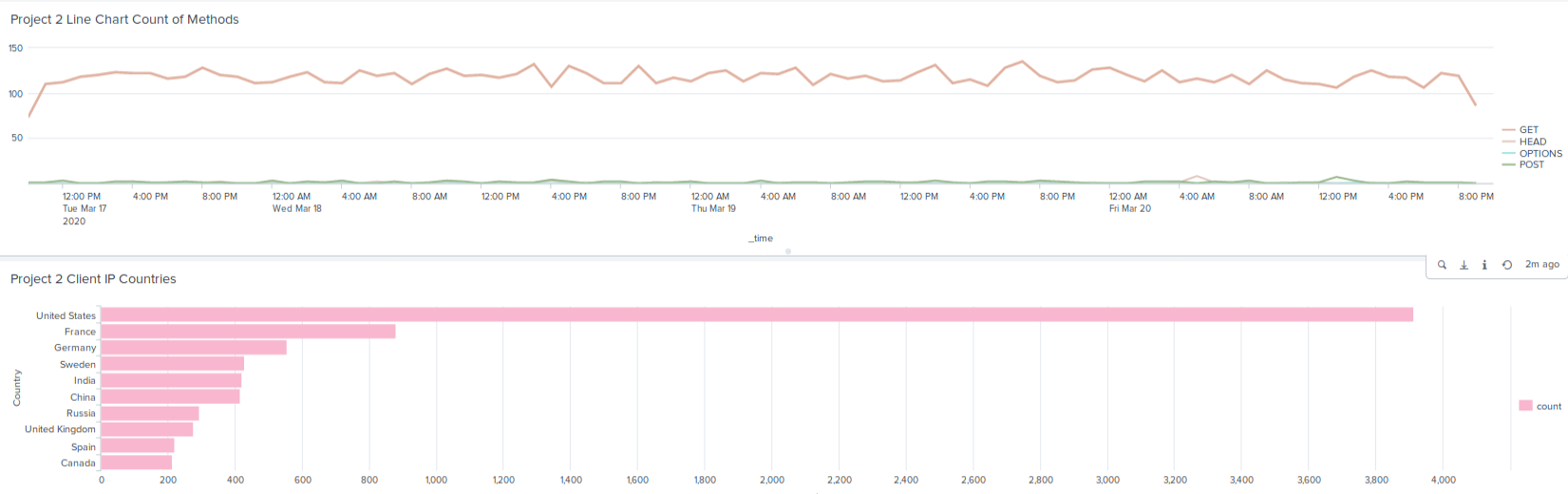
---

Now you will set up a dashboard and analyze the results.

#### Dashboard Setup

- Access the dashboard for Apache Webserver Monitoring.





- Select \*\*Edit\*\*.

- Access each panel and complete the following:

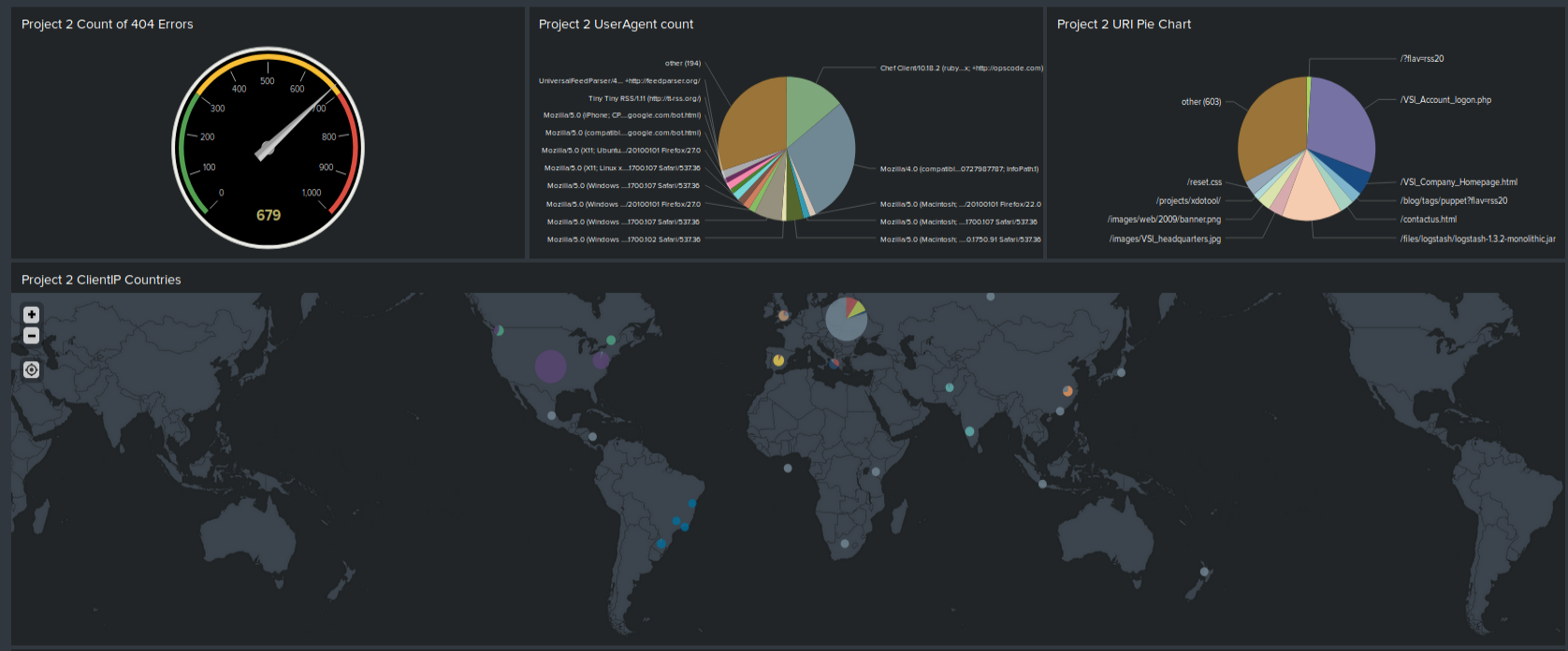
- Select \*\*Edit Search\*\*.

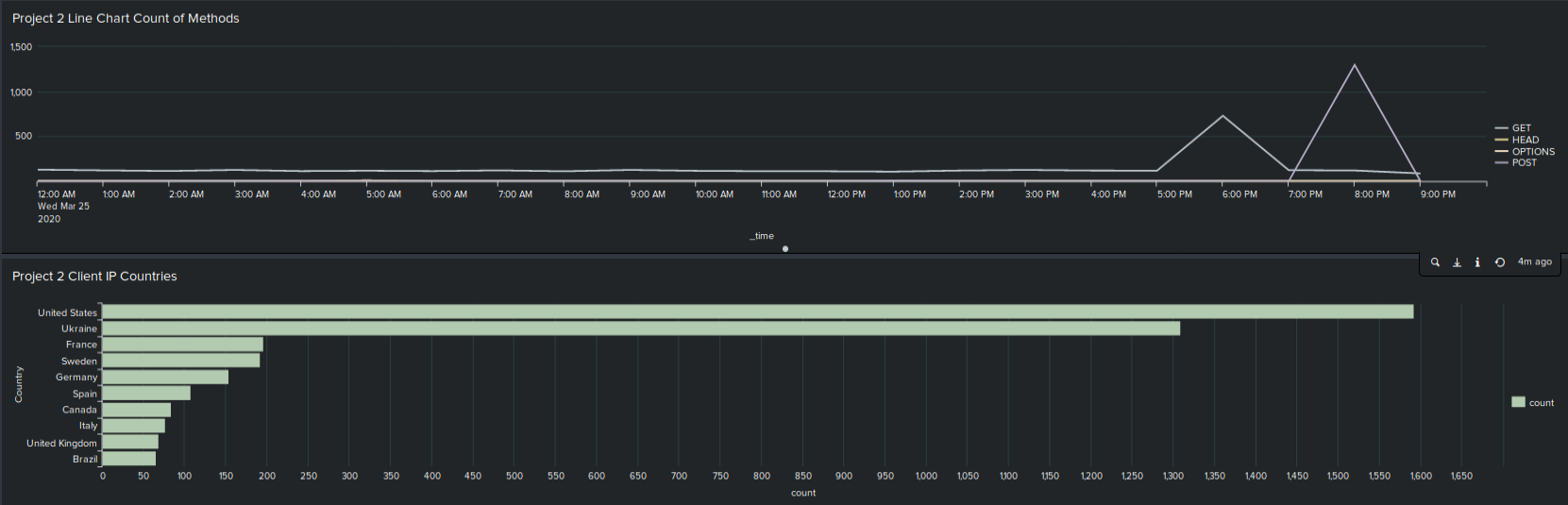
- Change the source from: `source=apache\_logs.txt` to `source="apache\_attack\_logs.txt`

- Select \*\*Apply\*\*.

- Save the whole dashboard.

- Edit the time on the whole dashboard to be \*\*All Time\*\*.





#### Dashboard Analysis for Time Chart of HTTP Methods

Analyze your new dashboard results and answer the following questions:

**- Does anything stand out as suspicious? yes**

**- Which method seems to be used in the attack? POST**

**- At what times did the attack start and stop? 7PM to 9PM**

**- What is the peak count of the top method during the attack? 1296**

#### Dashboard Analysis for Cluster Map

Analyze your new cluster map results and answer the following questions:

**- Does anything stand out as suspicious? Yes**

**- Which new city, country on the map has a high volume of activity? Kiev, Ukraine**

**- \*\*Hint:\*\* Zoom in on the map.**

**- What is the count of that city? 872**

#### Dashboard Analysis for URI Data

Analyze your dashboard panel of the URI data and answer the following questions:

**- Does anything stand out as suspicious? Yes**

**- What URI is hit the most? /VSI\_Account\_logon.php**

**- Based on the URI being accessed, what could the attacker potentially be doing? Brute Force Attack**