# Cybersecurity

## Project 3 Review Questions

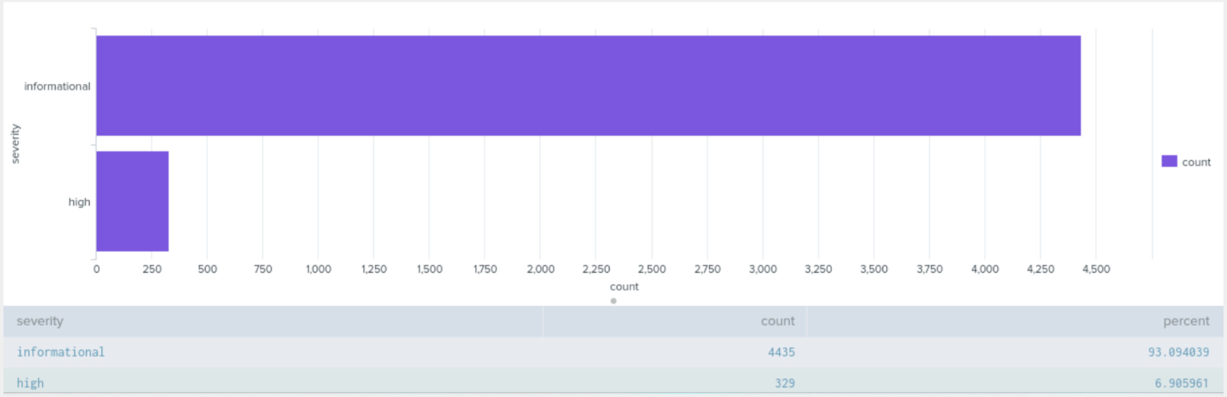
Make a copy of this document before you begin. Place your answers below each question.

## Windows Server Log Questions

### Report Analysis for Severity

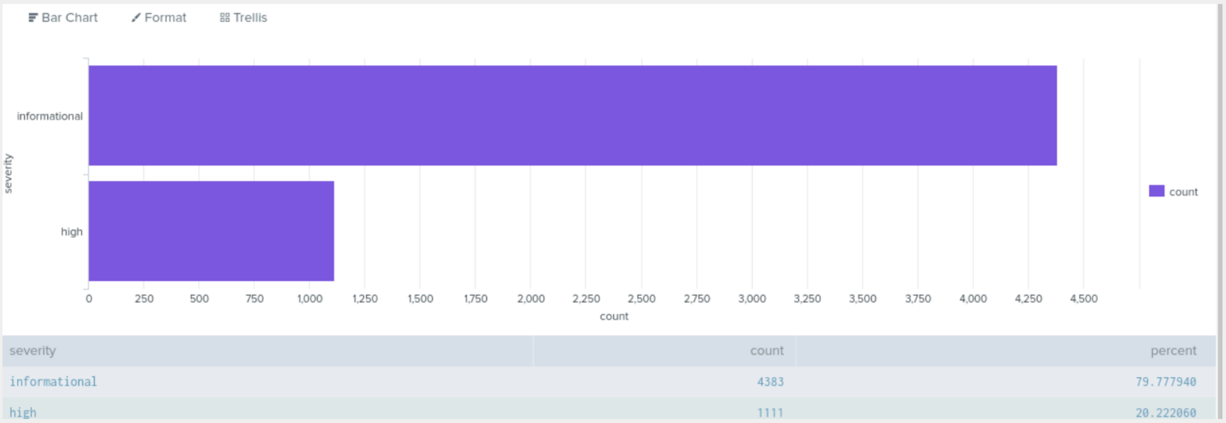
- Did you detect any suspicious changes in severity?
  Yes, we noticed a change. On day 1 and day 2 data of severity, the information data barely changed, But the high-value count had a significant increase from 329 on day 1 to 1111 on day 2.

**Before:**



| severity | count | percent |
|---|---|---|
| informational | 4435 | 93.094039 |
| high | 329 | 6.905961 |

After:



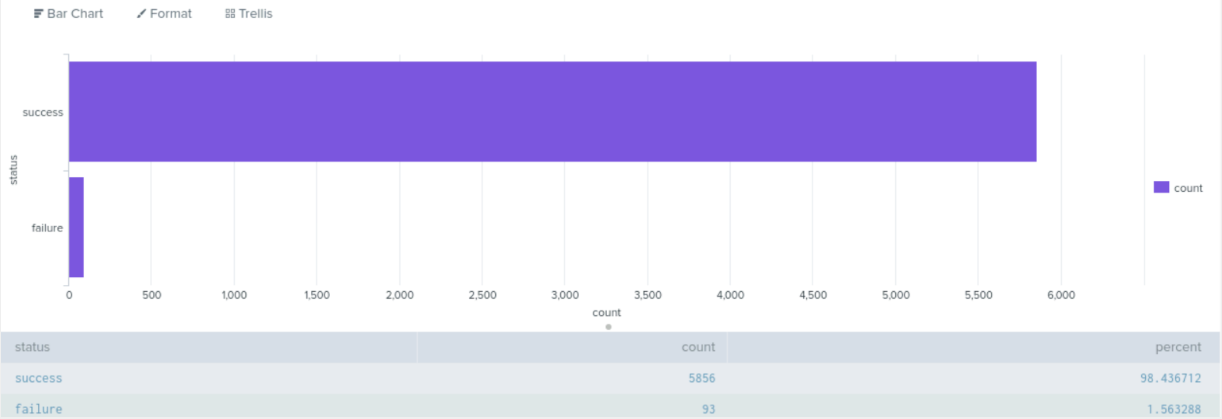
| severity | count | percent |
|---|---|---|
| informational | 4383 | 79.777940 |
| high | 1111 | 20.222060 |

## Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?
  The success rate remained practically the same with little increase on day 2, But the failure rate dropped from 142 to 53.

**Before:**

After:



| status | count | percent |
|---|---|---|
| success | 5856 | 98.436712 |
| failure | 93 | 1.563288 |

## Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes

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

```
35
```

- When did it occur?

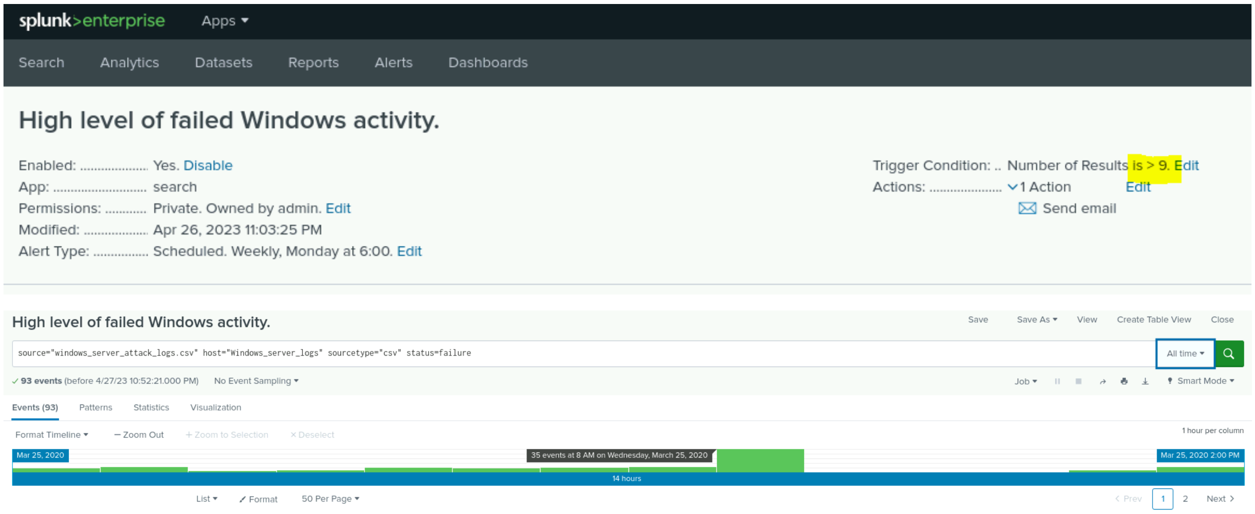
```
Wednesday March 25th, 2020 8:00 AM
```

- Would your alert be triggered for this activity?

```
Yes
```

- After reviewing, would you change your threshold from what you previously selected?

```
No. The baseline was set to 9 and was sufficient enough to detect the
attack.
```



High level of failed Windows activity.

Enabled: .................. Yes. Disable
App: .......................... search
Permissions: ........... Private. Owned by admin. Edit
Modified: ................. Apr 26, 2023 11:03:25 PM
Alert Type: ............... Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: .. Number of Results is > 9. Edit
Actions: .................... 1 Action Edit
Send email

High level of failed Windows activity.

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" status=failure
```

✓ 93 events (before 4/27/23 10:52:21.000 PM) No Event Sampling ▾

### Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
No
```

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

```
At 8:00 AM there were 16 successes, which was the most during the attack.
```

- Who is the primary user logging in?

```
User_a with 20 successes, at 14.3%
```

- When did it occur?

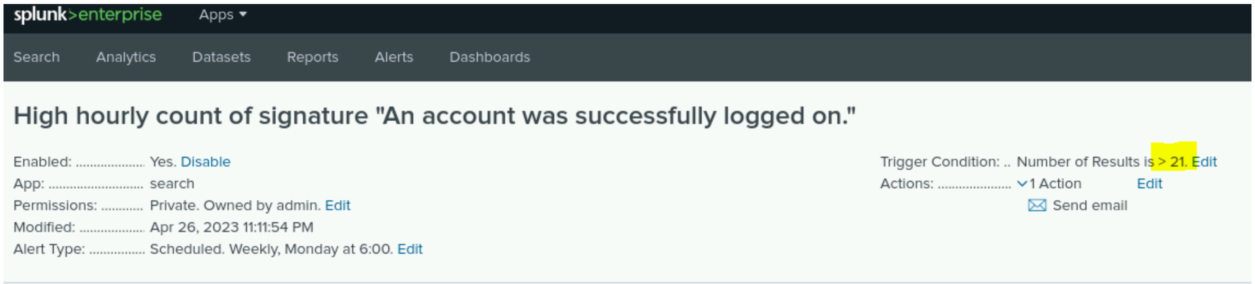
```
8:00 AM
```

- Would your alert be triggered for this activity?

No

- After reviewing, would you change your threshold from what you previously selected?

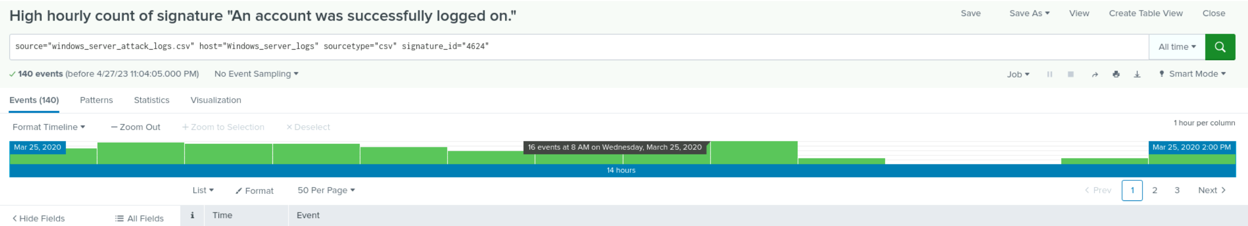
```
Yes, our baseline was set to 21 which would not have detected this activity
as it was too high.
```



High hourly count of signature "An account was successfully logged on."

Enabled: .................. Yes. Disable
App: .......................... search
Permissions: ........... Private. Owned by admin. Edit
Modified: .................. Apr 26, 2023 11:11:54 PM
Alert Type: ............... Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: .. Number of Results is > 21. Edit
Actions: ..................... ∨ 1 Action Edit
Send email


High hourly count of signature "An account was successfully logged on."

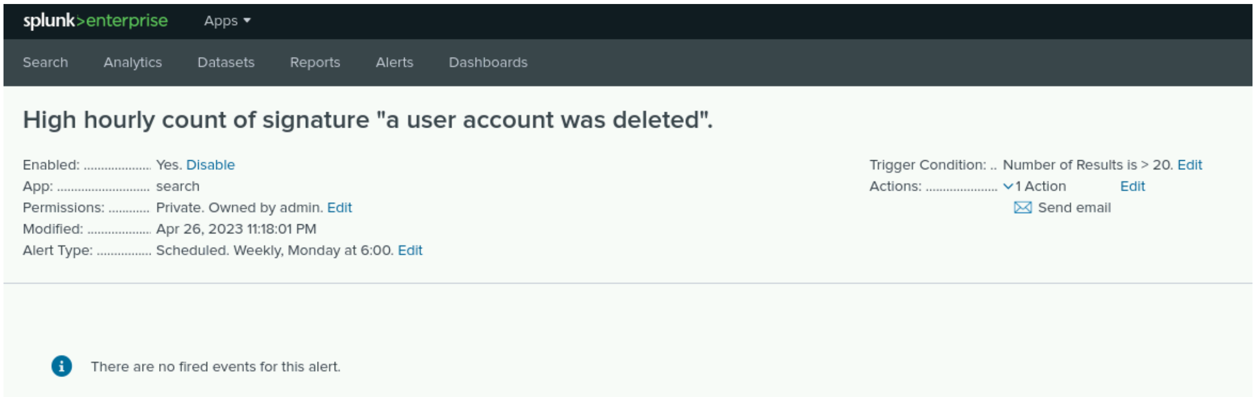
```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" signature_id="4624"
```

✓ 140 events (before 4/27/23 11:04:05.000 PM) No Event Sampling ▾

## Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No, the baseline is set to 20 with the highest hourly count being 19.
```

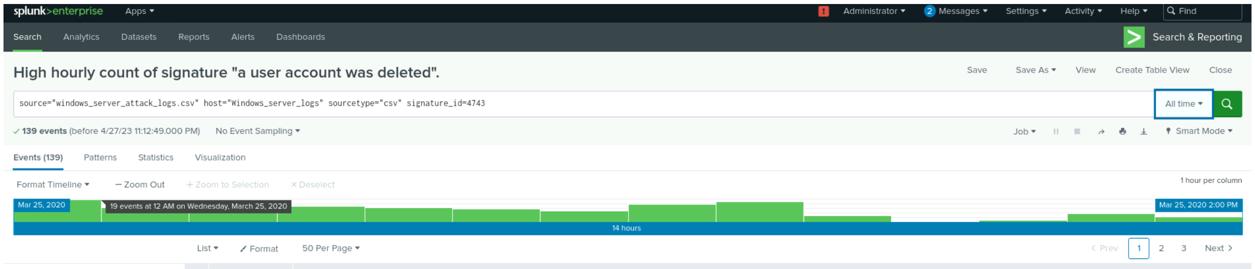


High hourly count of signature "a user account was deleted".

Enabled: .................. Yes. Disable
App: .......................... search
Permissions: ........... Private. Owned by admin. Edit
Modified: .................. Apr 26, 2023 11:18:01 PM
Alert Type: ............... Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: .. Number of Results is > 20. Edit
Actions: .................... ∨1 Action Edit
✉ Send email

There are no fired events for this alert.



High hourly count of signature "a user account was deleted".

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" signature_id=4743
```

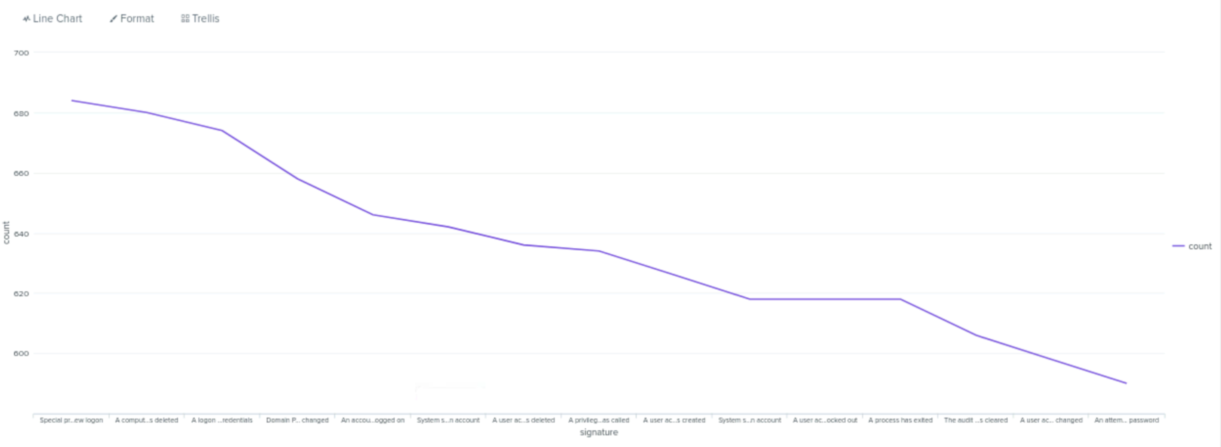
✓ 139 events (before 4/27/23 11:12:49.000 PM) No Event Sampling ▾

## Dashboard Analysis for Time Chart of Signatures

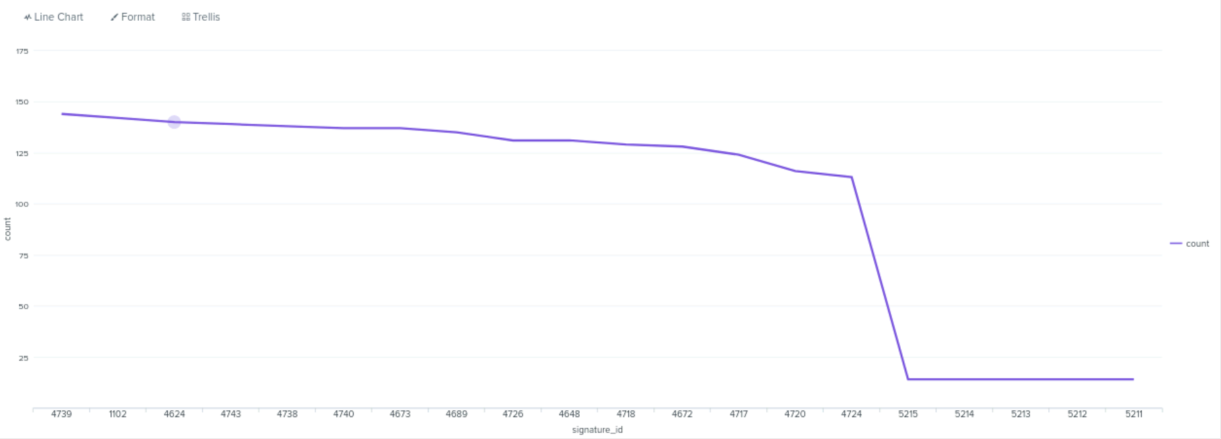
- Does anything stand out as suspicious?

YES

Day 1



Day 2



- What signatures stand out?

```
Day 1 signature_id 4672
Day 2 signature_id 4739
Both the top signatures
```

- What time did it begin and stop for each signature?

```
Day 1 Began at 12:00 AM and Stopped at 10:00 PM
Day 2 Began at 12:00 AM and Stopped at 01:00 PM
```

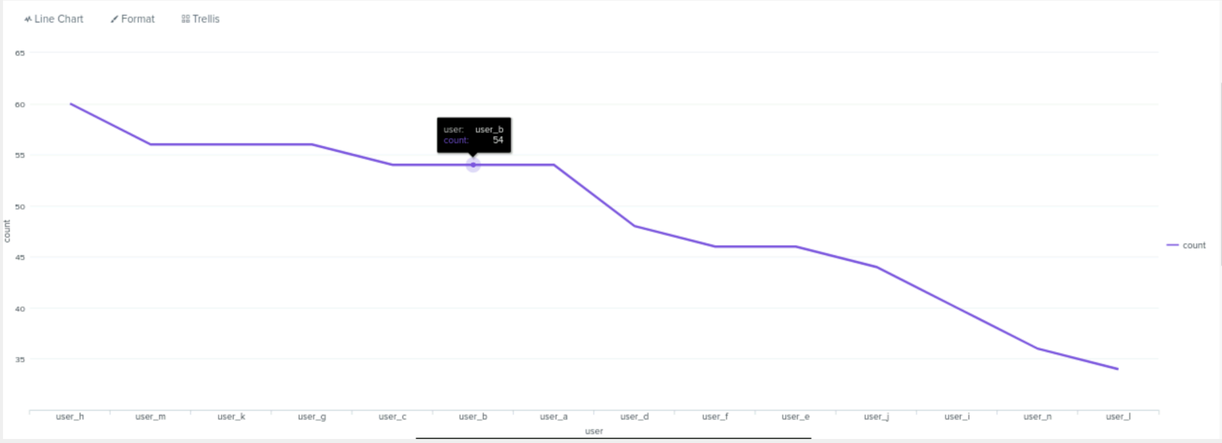
- What is the peak count of the different signatures?

```
Day 1 684
Day 2 144
```

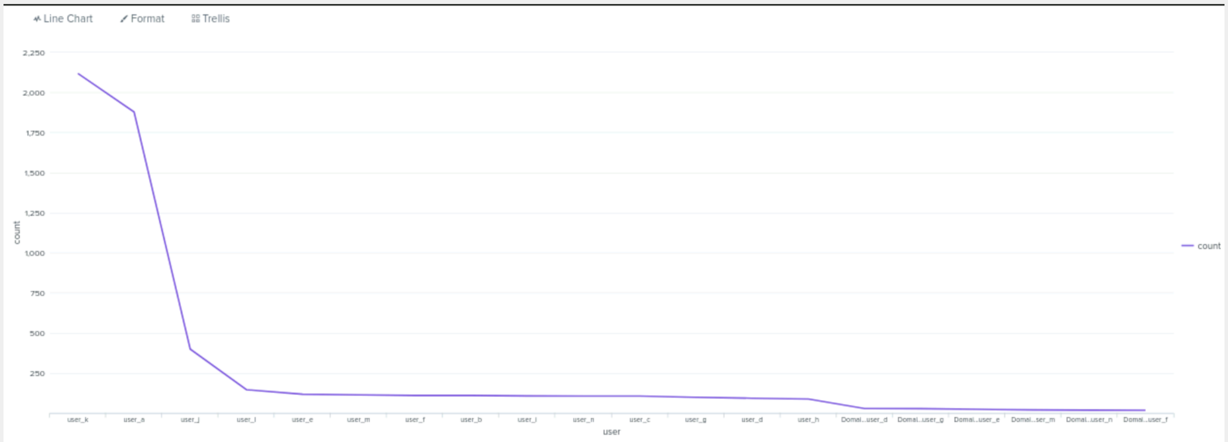
### Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
YES
Day 1
```



```
Day 2
```



- Which users stand out?

```
Day 1 User_h
Day 2 User_k
```

- What time did it begin and stop for each user?

```
Day 1 Began at 12:00 AM and Stopped at 10:00 PM
Day 2 Began at 12:00 AM and Stopped at 01:00 PM
```

- What is the peak count of the different users?

```
Day 1 User_h 60
Day 2 User_k 2118
```

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

- Does anything stand out as suspicious?

```
NO
```

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

```
YES
```

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

- Does anything stand out as suspicious?

```
NO
```

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

```
YES
```

### Dashboard Analysis for Users with Statistical Charts

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

```
Advantages
```

- Easy to use and understand, with the ability for easy comparisons of different types of statistical charts. Creating two different charts was simple and allowed data to be viewed easily if you knew what exactly to look for; allowing an easy comparison between top values and top values over time
-

Disadvantages

- Difficult to customize, being that there are very few data input options, which can also lead to oversimplification of data, and giving the wrong information. Multiple chats of the same data were necessary to find all the answers from time, top 10 users/signatures, and the addition of all other users combined into the other categories.

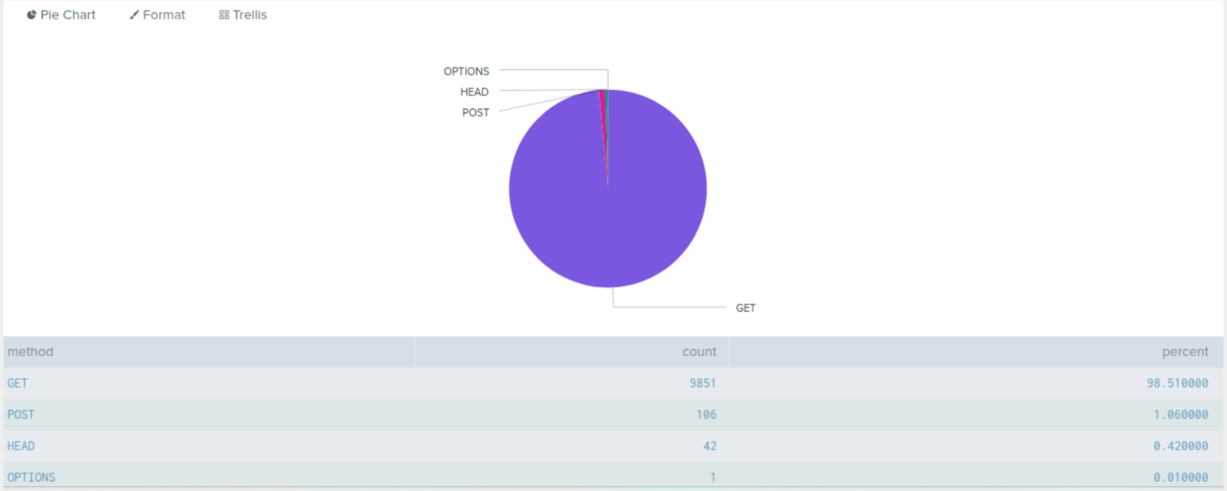
## Apache Web Server Log Questions

### Report Analysis for Methods

- Did you detect any suspicious changes in HTTP methods? If so, which one?

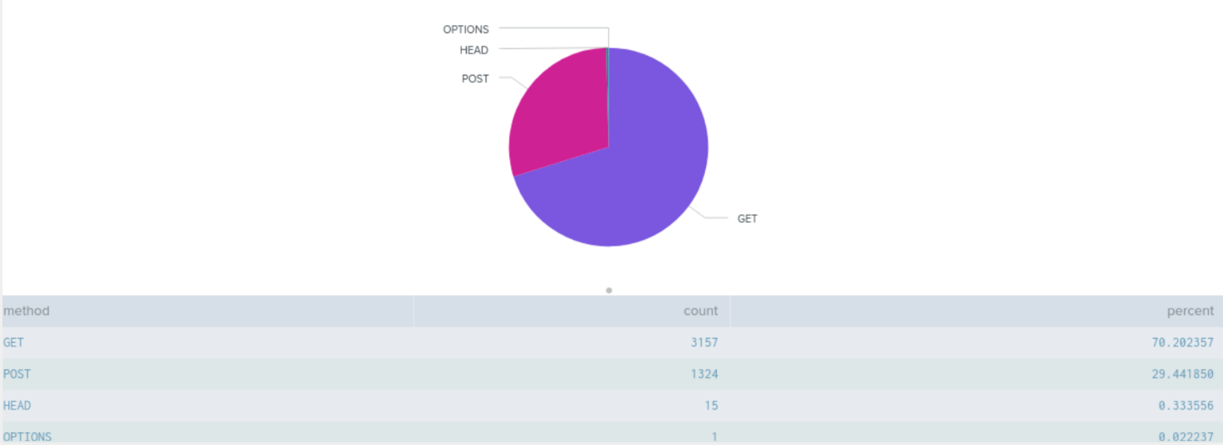
There was a huge change of activity for the GET and POST requests on day 2. On day1 the GET request count started at 9851 and ended with 3157. The POST request started with 105 and ended with 1324.

**Day1**



| method | count | percent |
|---|---|---|
| GET | 9851 | 98.510000 |
| POST | 106 | 1.060000 |
| HEAD | 42 | 0.420000 |
| OPTIONS | 1 | 0.010000 |

```
Day2
```



| method | count | percent |
|---|---|---|
| GET | 3157 | 70.202357 |
| POST | 1324 | 29.441850 |
| HEAD | 15 | 0.333556 |
| OPTIONS | 1 | 0.022237 |

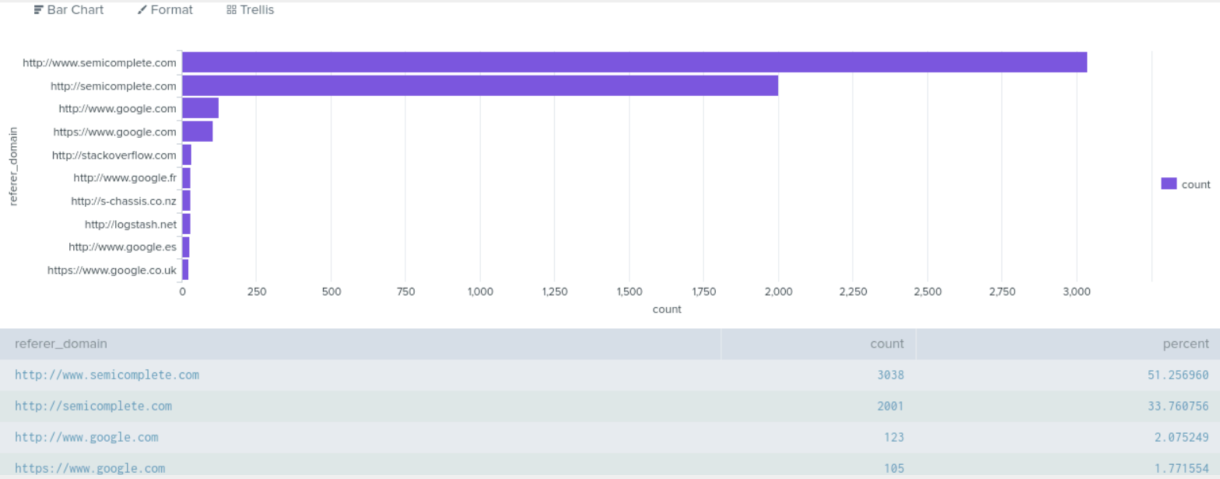
- What is that method used for?

```
GET/POST/HEAD/OPTION is HTTP request to retrieve or send data to a server.
```

**Report Analysis for Referrer Domains**

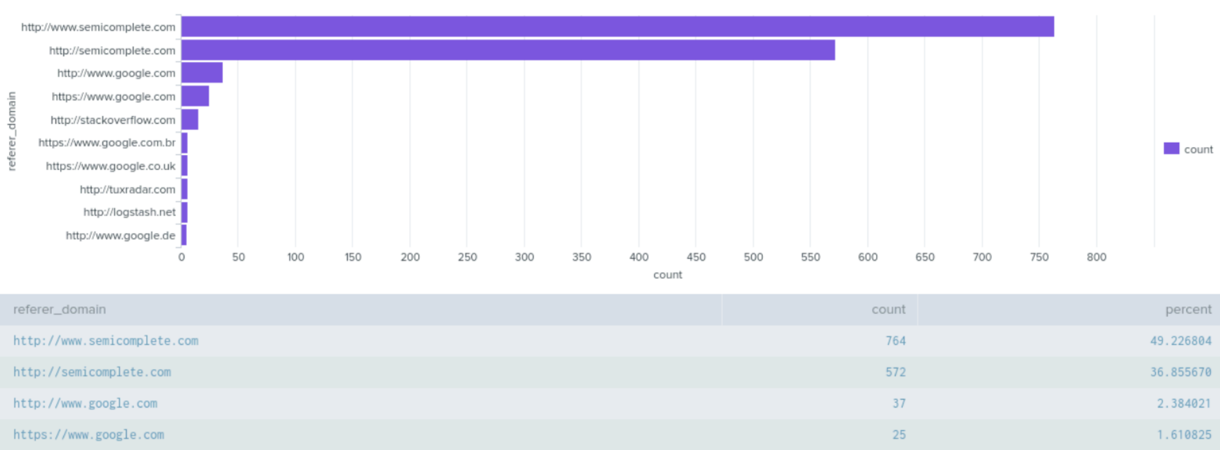
- Did you detect any suspicious changes in referrer domains?
  We noticed a huge decrease on day 2 in the count for all referrer domains. Specifically http://www.semicomplete & http://semicomplete.com

**Day1:**



| referer_domain | count | percent |
|---|---|---|
| http://www.semicomplete.com | 3038 | 51.256960 |
| http://semicomplete.com | 2001 | 33.760756 |
| http://www.google.com | 123 | 2.075249 |
| https://www.google.com | 105 | 1.771554 |

**Day2:**

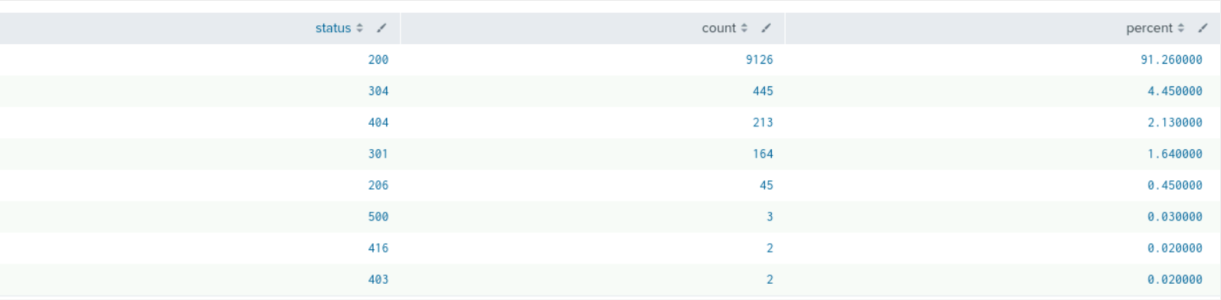


| referer_domain | count | percent |
|---|---|---|
| http://www.semicomplete.com | 764 | 49.226804 |
| http://semicomplete.com | 572 | 36.855670 |
| http://www.google.com | 37 | 2.384021 |
| https://www.google.com | 25 | 1.610825 |

## Report Analysis for HTTP Response Codes

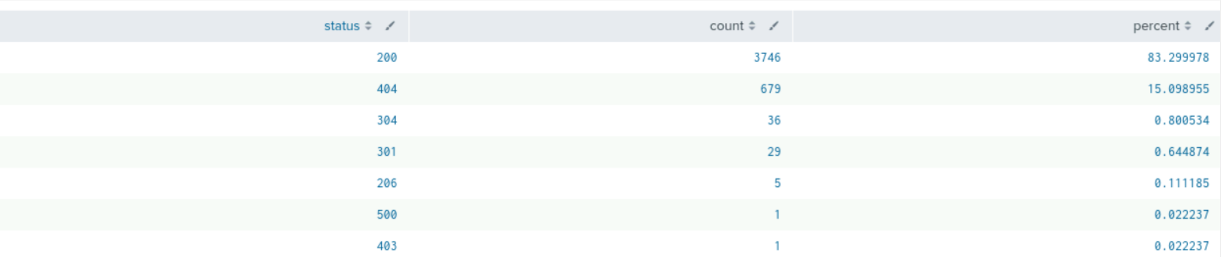
- Did you detect any suspicious changes in HTTP response codes?
  We noticed on Day1 the response code status of 200 was significantly higher with the count of 9126, than on Day2 with a count of only 3745. The other response codes are fluctuating at a normal rate.

**Day1:**



| status | count | percent |
|---|---|---|
| 200 | 9126 | 91.260000 |
| 304 | 445 | 4.450000 |
| 404 | 213 | 2.130000 |
| 301 | 164 | 1.640000 |
| 206 | 45 | 0.450000 |
| 500 | 3 | 0.030000 |
| 416 | 2 | 0.020000 |
| 403 | 2 | 0.020000 |

**Day2:**



| status | count | percent |
|---|---|---|
| 200 | 3746 | 83.299978 |
| 404 | 679 | 15.098955 |
| 304 | 36 | 0.800534 |
| 301 | 29 | 0.644874 |
| 206 | 5 | 0.111185 |
| 500 | 1 | 0.022237 |
| 403 | 1 | 0.022237 |

### Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes
```

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

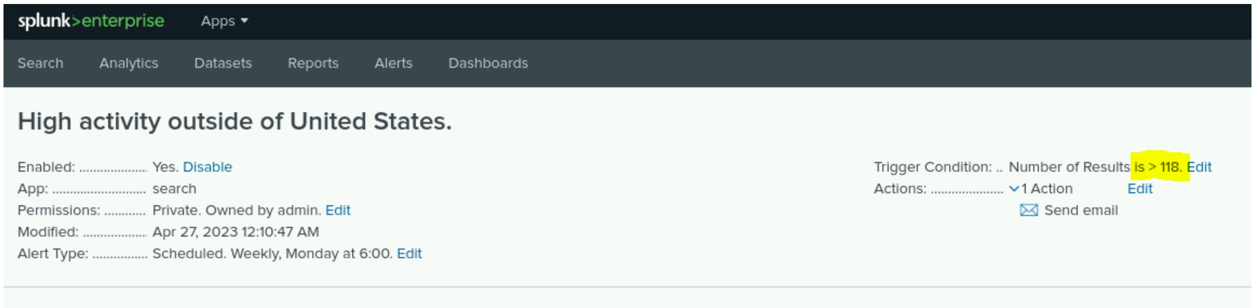
```
939
```

- Would your alert be triggered for this activity?

```
Yes
```

- After reviewing, would you change the threshold that you previously selected?

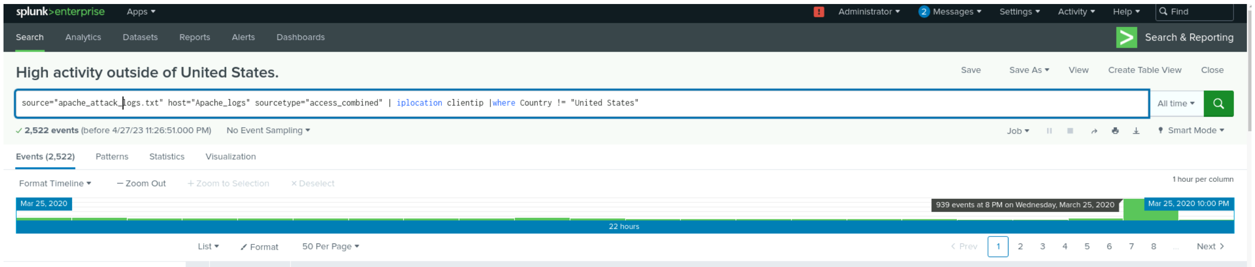
```
No. The baseline is set to 118 which would have been easily able to detect
this influx of new activity.
```



High activity outside of United States.

Enabled: .................. Yes. Disable
App: .......................... search
Permissions: ........... Private. Owned by admin. Edit
Modified: .................. Apr 27, 2023 12:10:47 AM
Alert Type: .............. Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: .. Number of Results is > 118. Edit
Actions: .................... ∨ 1 Action Edit
✉ Send email



High activity outside of United States.

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip |where Country != "United States"
```

✓ 2,522 events (before 4/27/23 11:26:51.000 PM) No Event Sampling ▾

## Alert Analysis for HTTP POST Activity

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

```
Yes
```

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

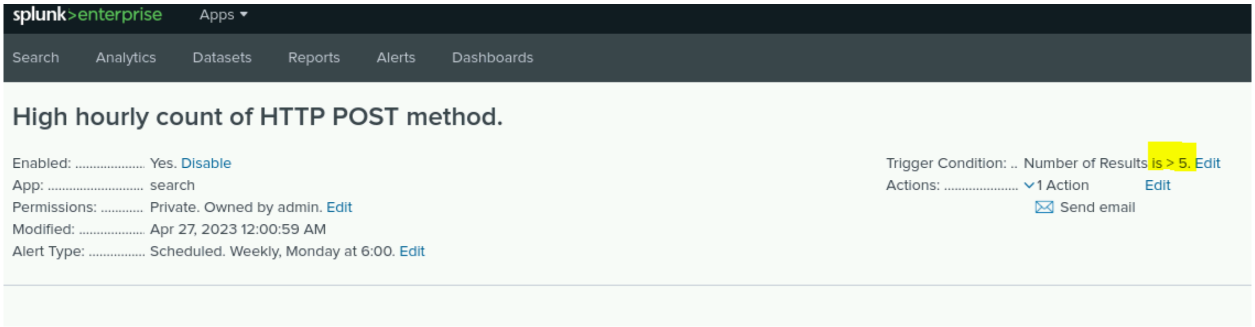
```
1,296
```

- When did it occur?

```
March 25th, 2020 9:00 PM
```

- After reviewing, would you change the threshold that you previously selected?

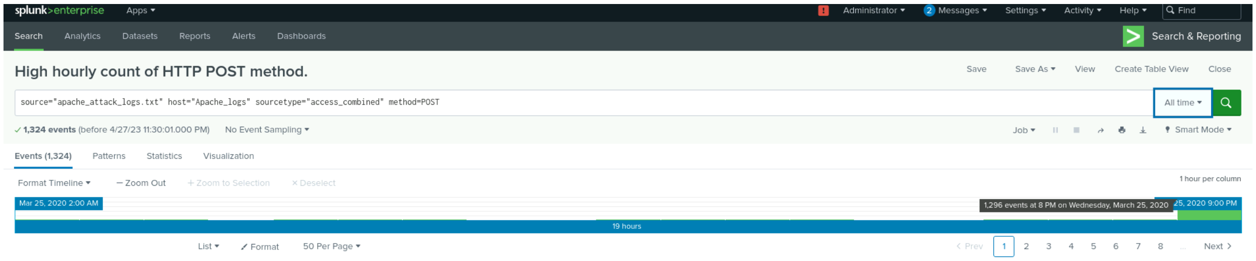
```
No. This is far beyond normal business activity and the baseline of 5 would
have been sufficient here.
```



High hourly count of HTTP POST method.

Enabled: .................. Yes. Disable
App: .......................... search
Permissions: ........... Private. Owned by admin. Edit
Modified: ................. Apr 27, 2023 12:00:59 AM
Alert Type: ............... Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: .. Number of Results is > 5. Edit
Actions: .................... ✓ 1 Action Edit
✉ Send email



High hourly count of HTTP POST method.

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" method=POST
```

✓ 1,324 events (before 4/27/23 11:30:01.000 PM) No Event Sampling ▾

## Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
A spike in GET requests between 5 and 6 PM and a strong spike in POST
requests between 7 and 8 PM.
```

- Which method seems to be used in the attack?

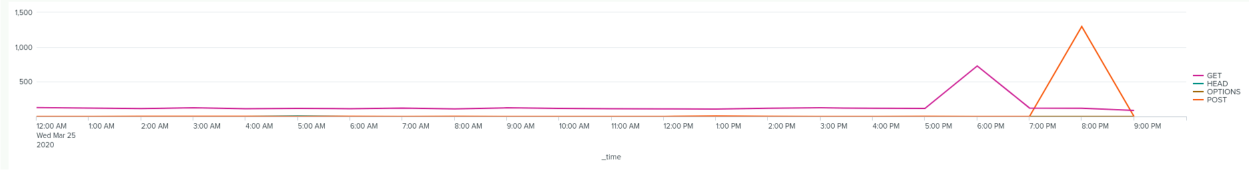
```
GET and POST
```

- At what times did the attack start and stop?

```
Between roughly 5 and 9 pm.
```

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

```
1,296 POST requests
```

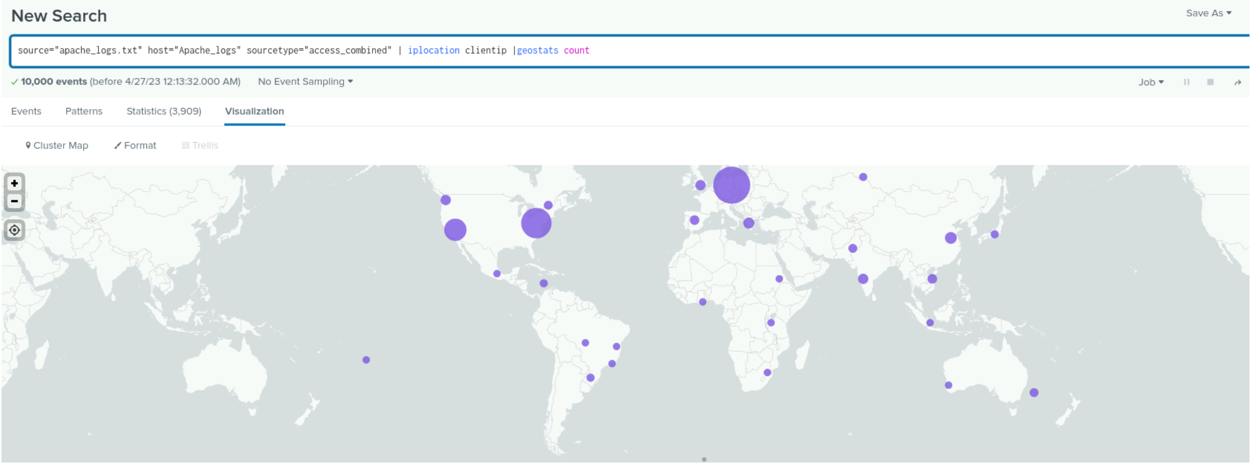


## Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
There is new activity out of New Zealand that was not present before the
attack.
```

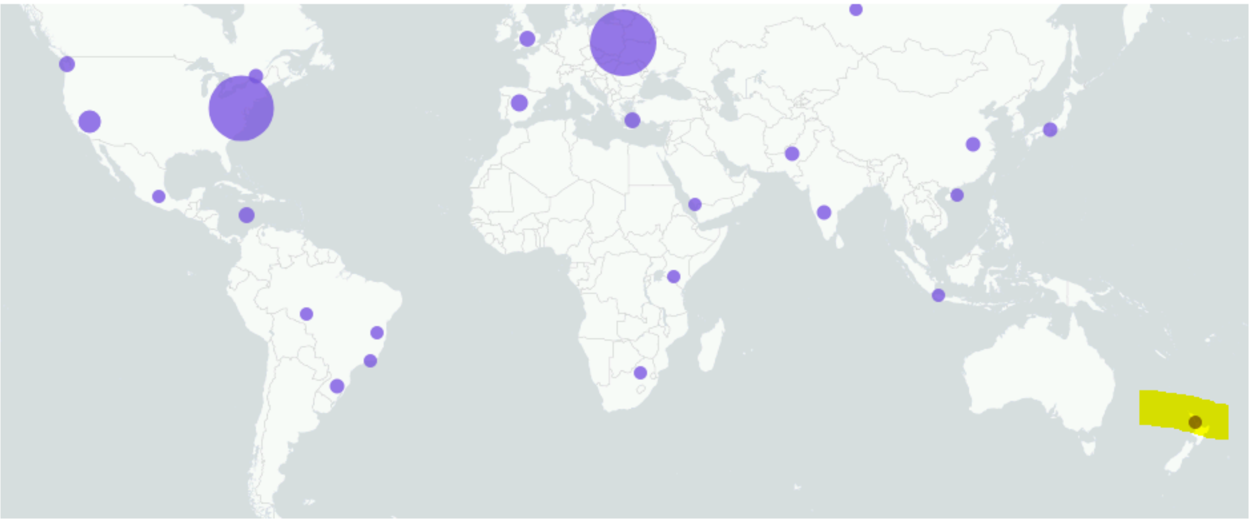
Before



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip |geostats count
```

✓ **10,000 events** (before 4/27/23 12:13:32.000 AM)

After



- Which new location (city, country) on the map has a high volume of activity? (**Hint**: Zoom in on the map.)

```
Auckland, New Zealand
```

- What is the count of that city?

```
3
```

### Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

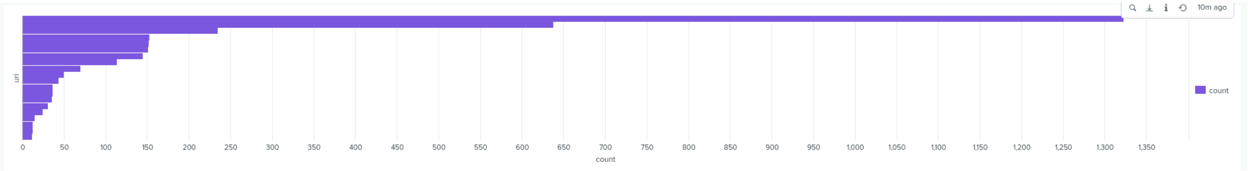
```
Very high count of /VSI_Account_logon.php URIs
```

- What URI is hit the most?

```
/VSI_Account_logon.php
```

- Based on the URI being accessed, what could the attacker potentially be doing?

```
Potentially Brute Force attacks on employee accounts.
```


10m ago
url
count
0
50
100
150
200
250
300
350
400
450
500
550
600
650
700
750
800
850
900
950
1,000
1,050
1,100
1,150
1,200
1,250
1,300
1,350
count