Cybersecurity

Project 3 Review Questions

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

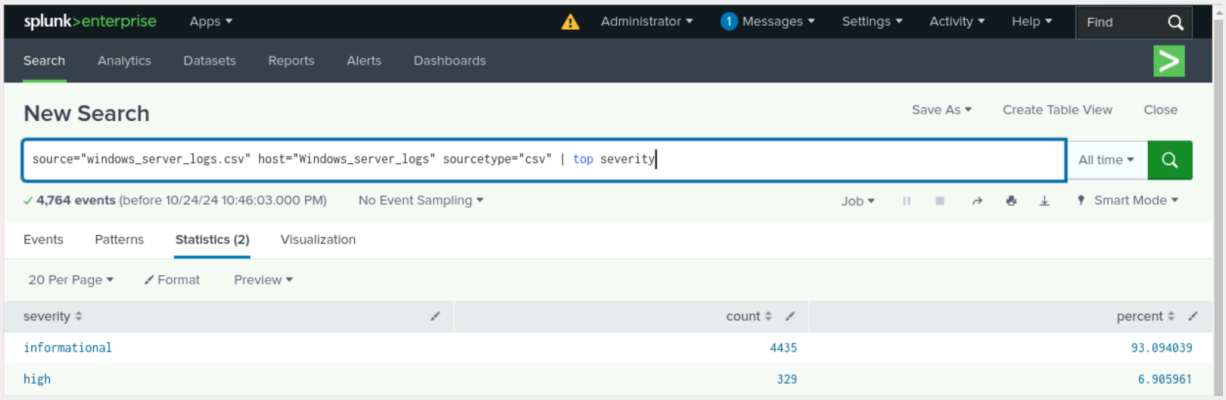
Windows Server Log Questions

Report Analysis for Severity

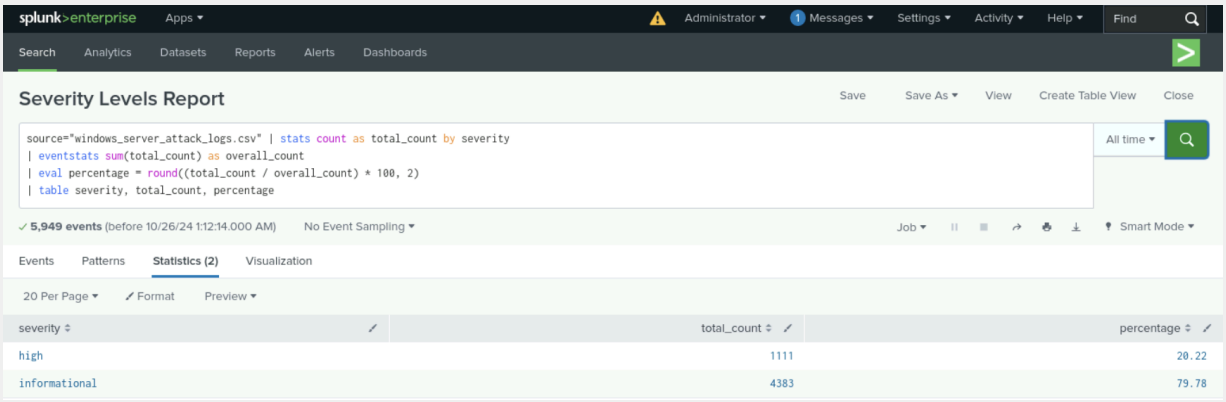
- Did you detect any suspicious changes in severity?

Yes, our report identified notable changes in severity, with high-severity events increasing from approximately 7% to 20% during the attack.

Normal Activity Logs:



Attack Logs:

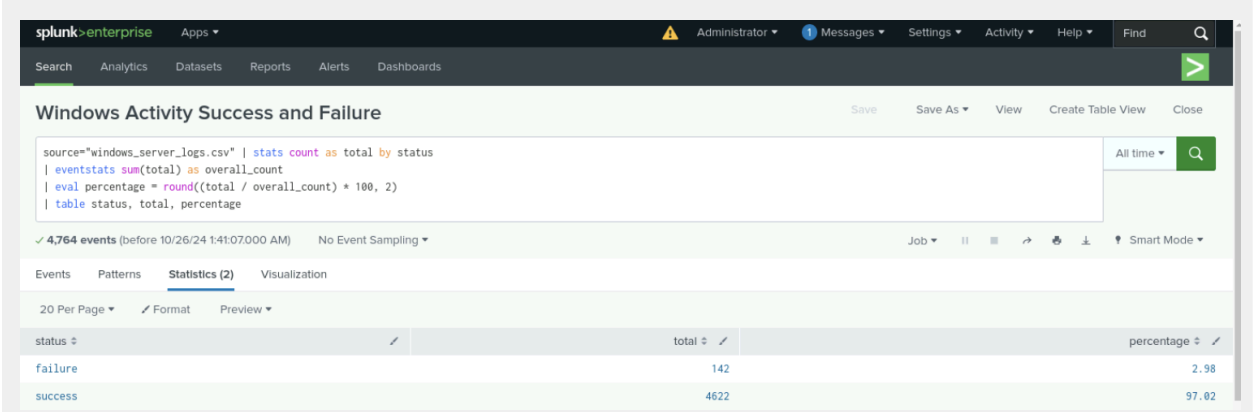


Report Analysis for Failed Activities

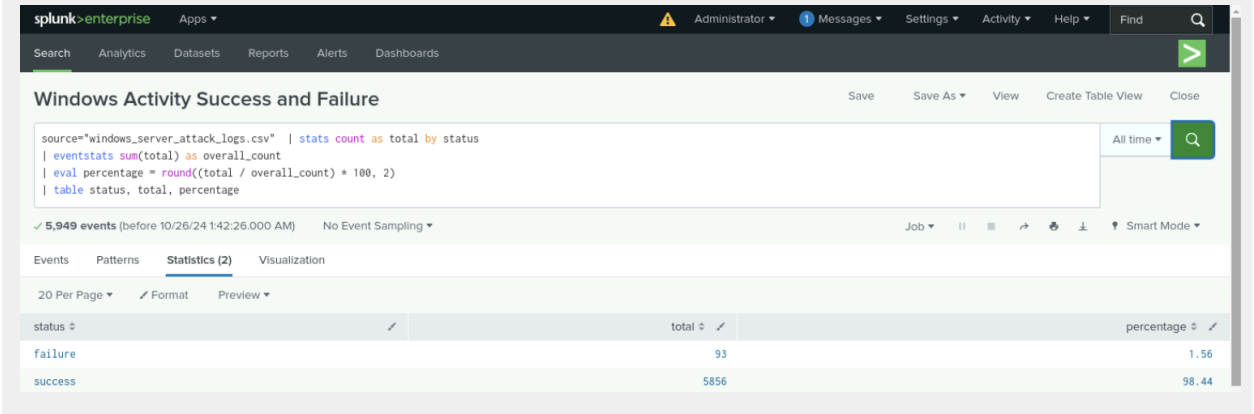
- Did you detect any suspicious changes in failed activities?

Yes, our report revealed significant changes in the status of activities between normal and attack logs, showing an increase in successful activities and a decrease in failed activities during the attack.

Normal Activity Logs:



Attack Logs:



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

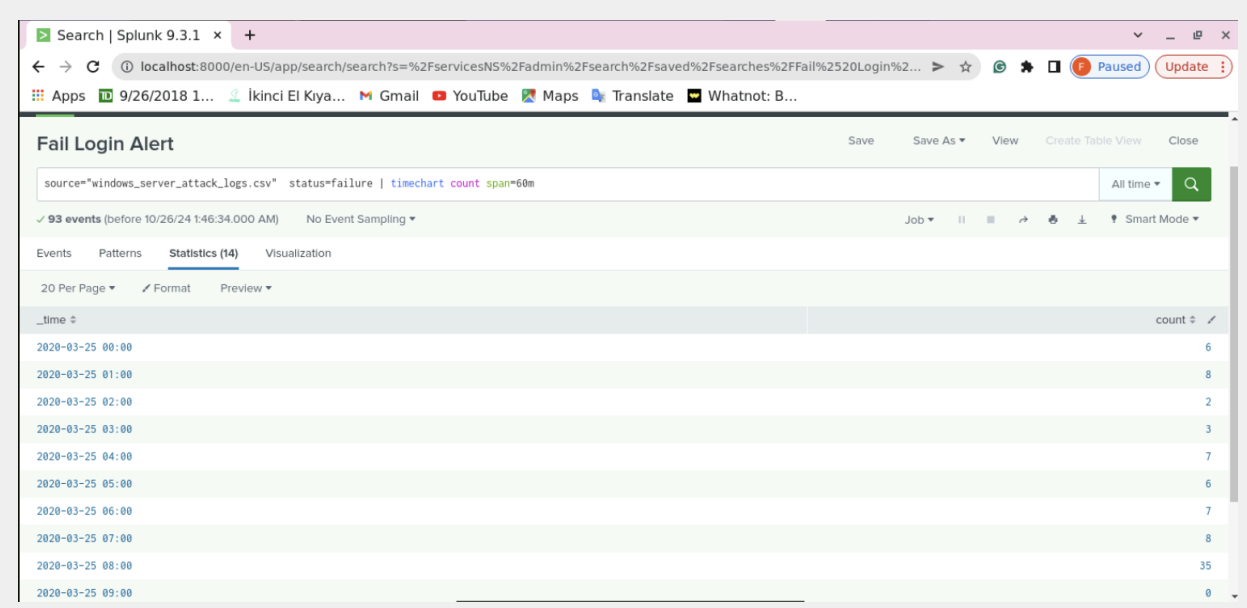
```
Yes, our alert detected a suspicious volume of failed Windows activity.
```

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

```
The count was 35 failed Windows activities.
```

- When did it occur?

```
It occurred at 08:00 AM on 2020-03-25.
```



- Would your alert be triggered for this activity?

```
Yes, our alert would have been triggered as we set our threshold to alert us
if there were more than 15 failed Windows activities in an hour.
```

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

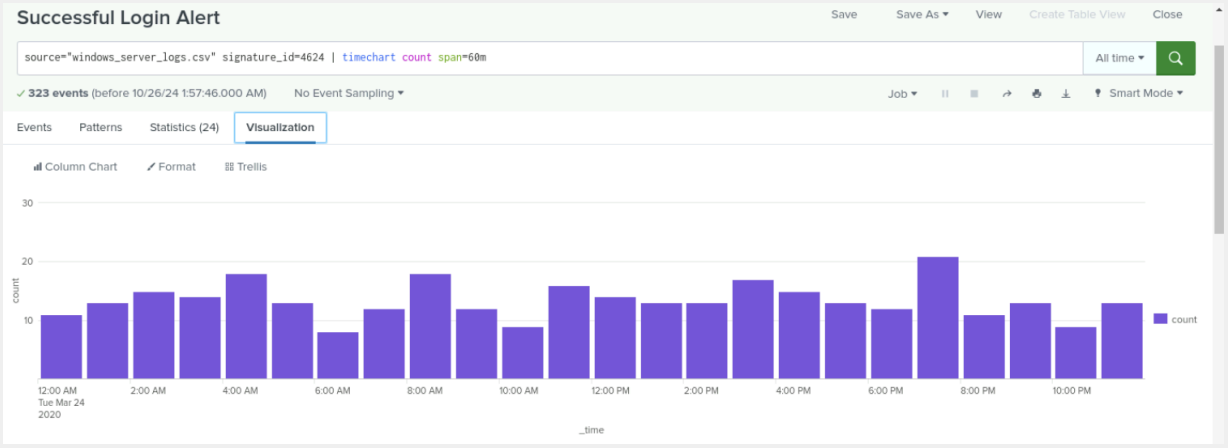
```
I would recommend maintaining our threshold, as it was appropriately set low
enough to capture this attack while remaining high enough to avoid false
positives during other hours, thus preventing alert fatigue.
```

Alert Analysis for Successful Logins

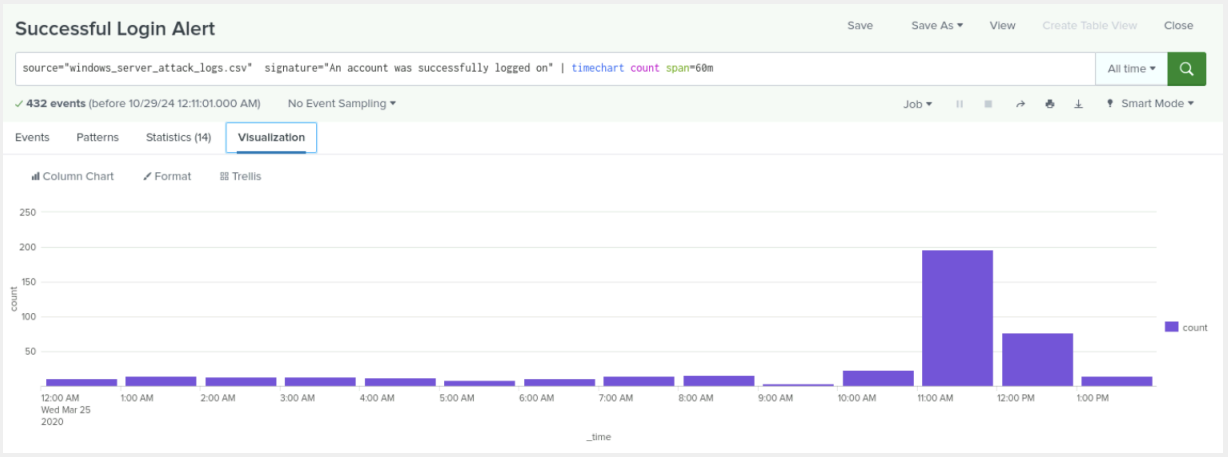
- Did you detect a suspicious volume of successful logins?

```
Yes, we detected a suspicious volume of successful logins between 11:00 AM
and 12:00 PM.
```

Normal Log Activity:



Attack Logs:



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

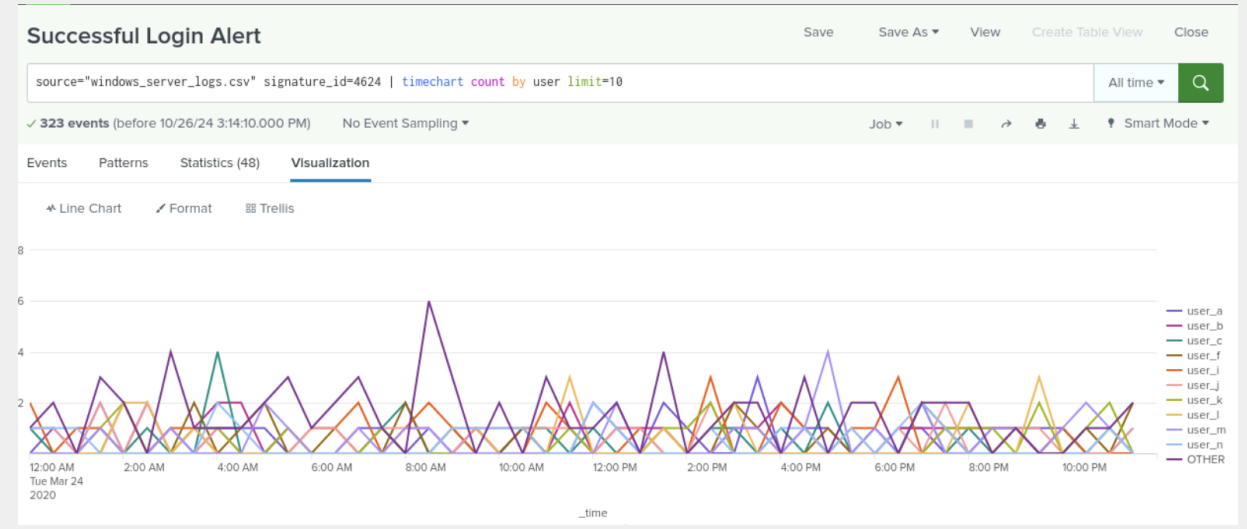
At 10:00 AM there were a total of 23 successful logins that occurred and then the number significantly increased to 196 at 11:00 AM and continued by decreasing to 77 at 12:00 PM. (2 hours).

_time	count
2020-03-25 00:00	11
2020-03-25 01:00	15
2020-03-25 02:00	14
2020-03-25 03:00	14
2020-03-25 04:00	12
2020-03-25 05:00	9
2020-03-25 06:00	11
2020-03-25 07:00	15
2020-03-25 08:00	16
2020-03-25 09:00	4
2020-03-25 10:00	23
2020-03-25 11:00	196
2020-03-25 12:00	77
2020-03-25 13:00	15

- Who is the primary user logging in?

Upon further analysis it appears that at 11:00 AM user_j had a spike in logins.

Normal Logs:



Attack Logs:

- When did it occur?

```
At 11:00 AM to 12:00 PM on 2020-03-25.
```

- Would your alert be triggered for this activity?

```
Our alert system is configured to trigger only when there are 30 or more
successful logins within an hour, so this activity would not have activated
any alerts for the SOC.
```

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

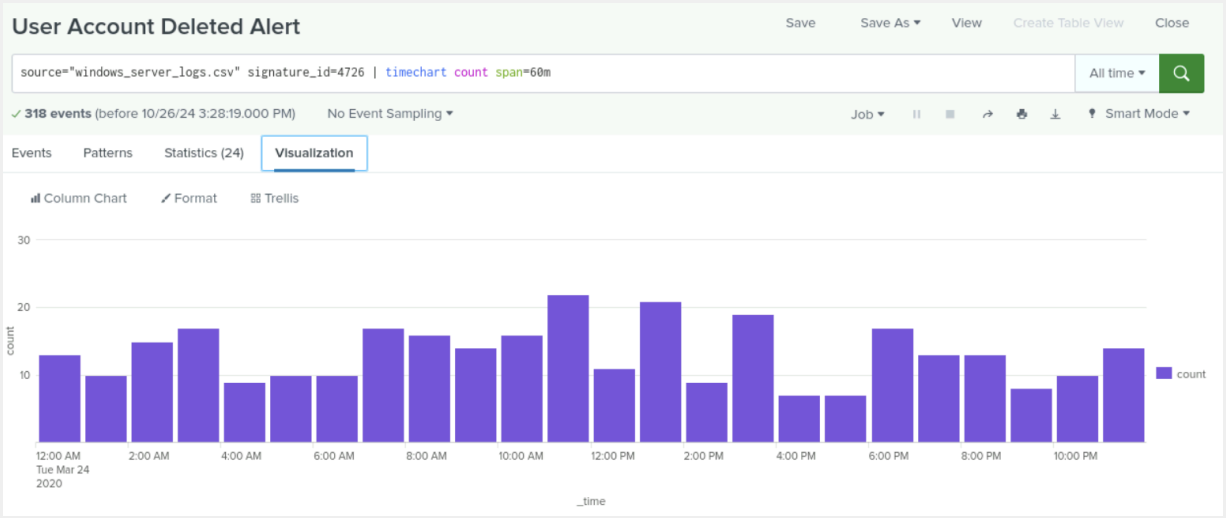
```
I would suggest adjusting the threshold number slightly; however, I believe
we need to analyze more log data to make an informed decision, as we want to
avoid alert fatigue. Additionally, we should consider creating an alert if
logins dip below a certain threshold per hour, since this could impact login
capabilities. Moreover, as activity for other signature events that we're
currently not monitoring increases, we should implement additional alerts to
capture those occurrences.
```

Alert Analysis for Deleted Accounts

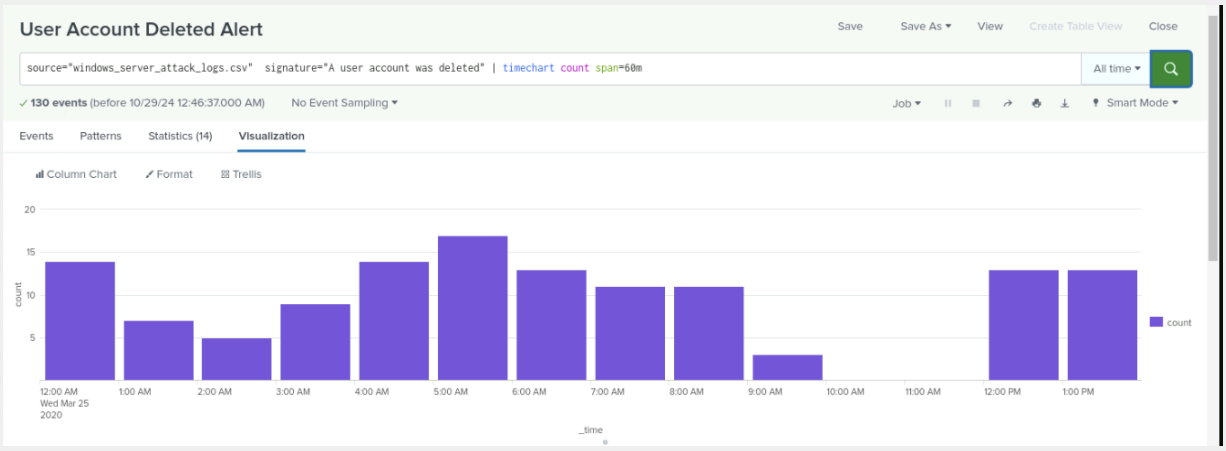
- Did you detect a suspicious volume of deleted accounts?

We detected a suspicious amount of deleted accounts, between the hours of 09:00 AM and 11:00 AM there was a significant drop in the number of deletions. There were 11 events on 08:00 AM and it decreased to 3 at 09:00 AM, 0 at 10:00 AM, 0 at 11:00 am and went back to normal at 12:00 PM with 13.

Normal Logs:



Attack Logs:

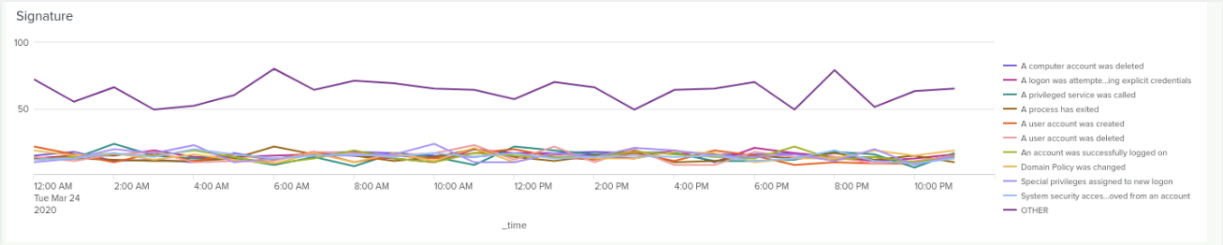


Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

In the time chart signatures for the “attack logs” there are events that stand out from the regular Windows activity logs.

Normal Logs:




```
source="windows_server_logs.csv" | timechart span=1h count by signature
```

All time

✓ **4,764 events** (before 10/26/24 3:34:08.000 PM) No Event Sampling

Job Smart Mode

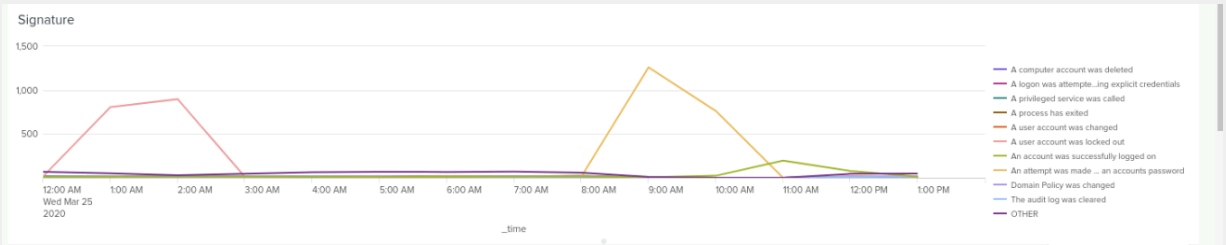
Events Patterns **Statistics (24)** Visualization

20 Per Page Format Preview

< Prev 1 2 Next >

_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was created	A user account was deleted	An account was successfully logged on	Domain Policy was changed	Special privileges assigned to new logon	System security access was removed from an account	OTHER
2020-03-24 00:00	14	12	12	12	21	13	11	18	9	11	72
2020-03-24 01:00	17	14	12	12	15	10	13	14	12	12	55
2020-03-24 02:00	10	14	23	11	9	15	15	16	19	16	66
2020-03-24 03:00	11	18	14	10	16	17	14	11	16	13	49
2020-03-24 04:00	9	13	12	10	10	9	18	15	22	19	52
2020-03-24 05:00	16	13	12	12	15	10	13	11	9	15	60
2020-03-24 06:00	11	14	7	21	11	10	8	8	12	12	80
2020-03-24 07:00	16	15	13	15	17	17	12	16	14	14	64

Attack Logs:




```
source="windows_server_attack_logs.csv" | timechart span=1h count by signature
```

All time

✓ **5,949 events** (before 10/26/24 3:39:16.000 PM) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (14)** Visualization

20 Per Page Format Preview

_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was changed	A user account was locked out	An account was successfully logged on	An attempt was made to reset an accounts password	Domain Policy was changed	The audit log was cleared	OTHER
2020-03-25 00:00	19	14	14	8	10	16	11	10	10	12	68
2020-03-25 01:00	12	8	20	13	7	805	15	11	16	16	50
2020-03-25 02:00	9	2	3	16	9	896	14	3	17	8	30
2020-03-25 03:00	13	13	13	12	16	10	14	6	16	14	47
2020-03-25 04:00	12	15	18	8	11	12	12	11	10	16	62

2020-03-25 05:00	11	11	14	12	16	19	9	8	14	10	68
2020-03-25 06:00	9	11	14	12	17	3	11	14	8	13	66
2020-03-25 07:00	15	14	8	15	17	11	15	16	20	7	69
2020-03-25 08:00	17	11	13	23	11	16	16	12	11	16	59
2020-03-25 09:00	5	5	2	1	3	1	4	1258	0	4	10
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	7	14	9	7	11	6	77	6	6	9	45
2020-03-25 13:00	4	12	8	7	9	16	15	12	15	17	49

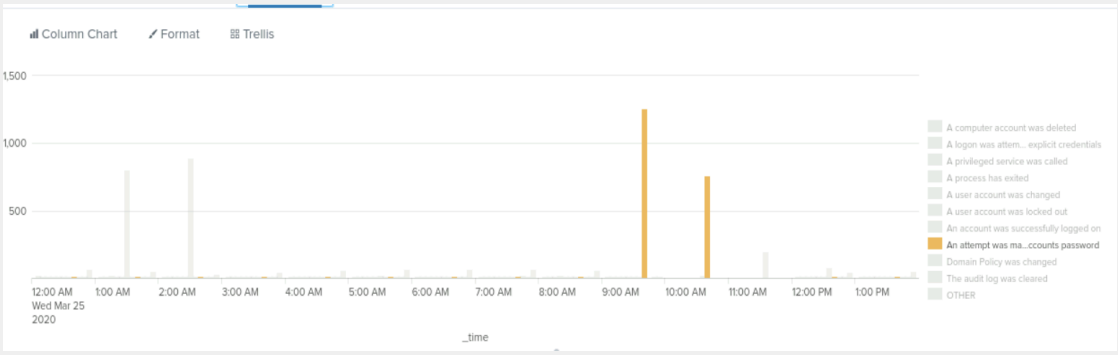
- What signatures stand out?

There are two events that have significant increases in activity:

1. An attempt was made to reset an account password.
2. A user account was locked out.

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

1. “An attempt was made to reset an account password” occurred between 09:00 AM and 11:00 AM.



2. “A user account was locked out” occurred between 01:00 AM and 02:30 AM

- What is the peak count of the different signatures?

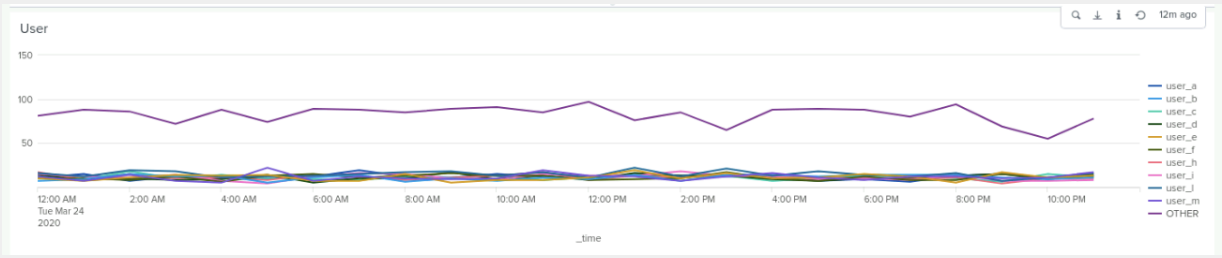
```
Account locked out peaked at 896
Attempt to reset password peaked at 1258.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes, there are significant increases in the amount of user activity for two users that are shown in the Users by Hour Time Chart.

Normal Logs:

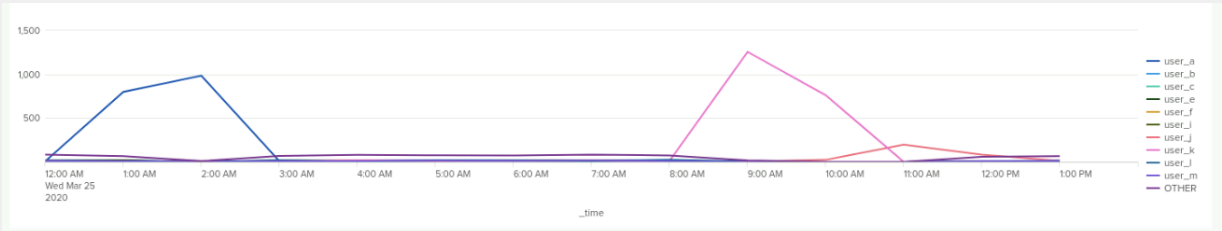


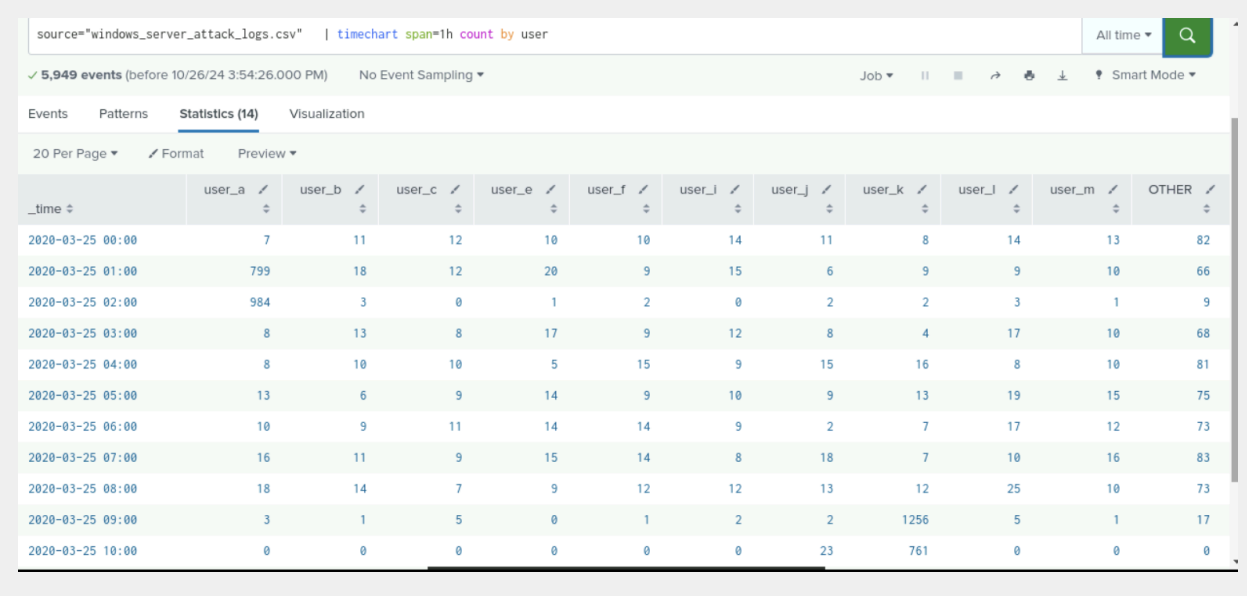
Events | Patterns | **Statistics (24)** | Visualization

20 Per Page ▾ | Format | Preview ▾ | < Prev | 1 | 2 | Next >

_time	user_a	user_b	user_c	user_d	user_e	user_f	user_h	user_i	user_l	user_m	OTHER
2020-03-24 00:00	11	7	12	14	10	10	17	15	16	12	81
2020-03-24 01:00	15	9	9	8	7	10	9	12	12	7	88
2020-03-24 02:00	7	15	18	10	11	8	15	11	19	14	86
2020-03-24 03:00	12	12	10	8	14	12	10	14	18	7	72
2020-03-24 04:00	12	13	14	9	13	6	11	7	11	5	88
2020-03-24 05:00	10	5	10	14	14	13	8	4	12	22	74
2020-03-24 06:00	12	11	9	5	7	15	14	12	13	7	89
2020-03-24 07:00	19	14	8	10	7	11	13	16	15	12	88
2020-03-24 08:00	12	6	12	10	15	13	8	15	17	10	85
2020-03-24 09:00	11	10	11	17	5	16	11	10	18	9	89
2020-03-24 10:00	15	7	13	9	8	13	13	8	13	10	91
2020-03-24 11:00	12	11	8	13	8	13	17	15	17	19	85
2020-03-24 12:00	11	9	11	9	11	8	8	13	11	13	97

Attack Logs:





_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9
2020-03-25 03:00	8	13	8	17	9	12	8	4	17	10	68
2020-03-25 04:00	8	10	10	5	15	9	15	16	8	10	81
2020-03-25 05:00	13	6	9	14	9	10	9	13	19	15	75
2020-03-25 06:00	10	9	11	14	14	9	2	7	17	12	73
2020-03-25 07:00	16	11	9	15	14	8	18	7	10	16	83
2020-03-25 08:00	18	14	7	9	12	12	13	12	25	10	73
2020-03-25 09:00	3	1	5	0	1	2	2	1256	5	1	17
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0

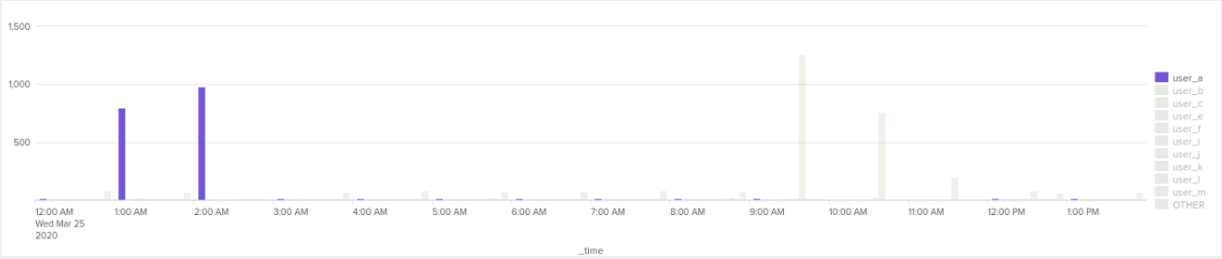
- Which users stand out?

There are two users who have significant increase in activity:

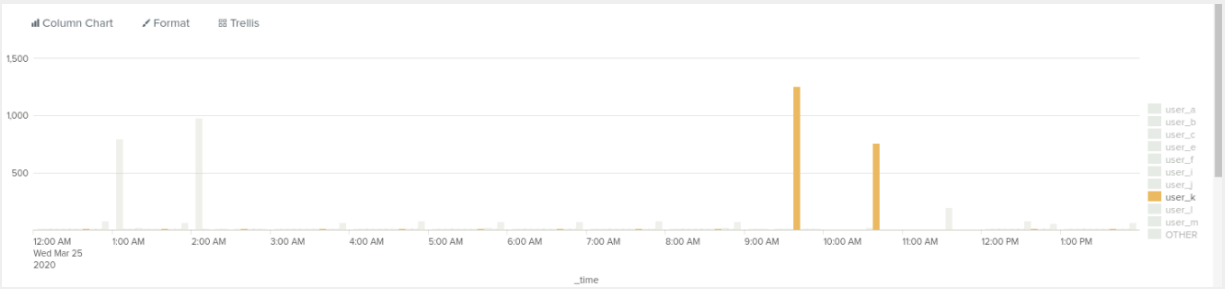
1. User_a
2. User_k

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

User_a had increased activity between 01:00 AM and 02:00 AM.



User_k had increased activity between 09:00 AM and 10:00 AM.



- What is the peak count of the different users?

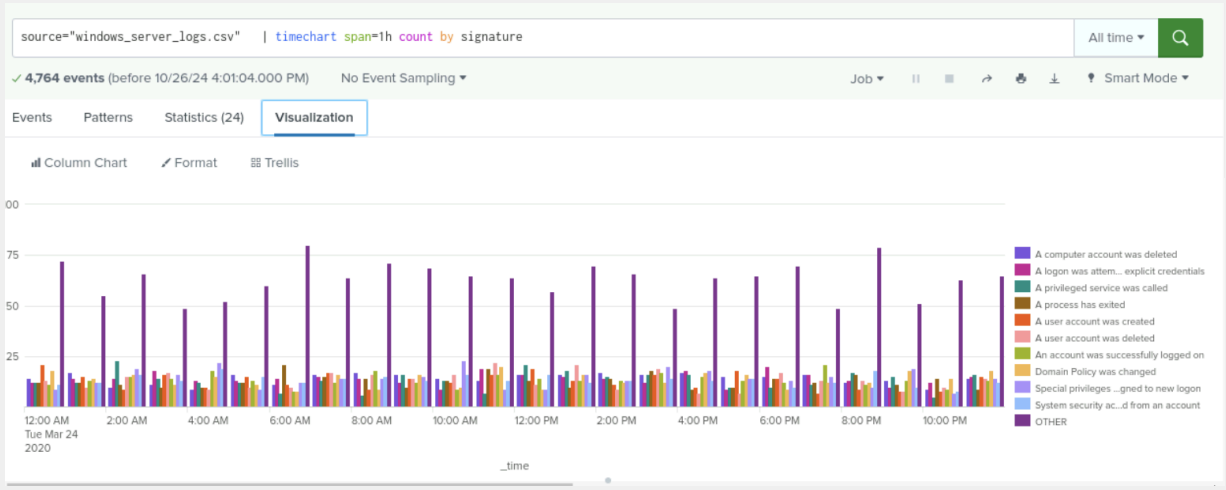
```
User_a peaked at 984.
User_k peaked at 1256.
```

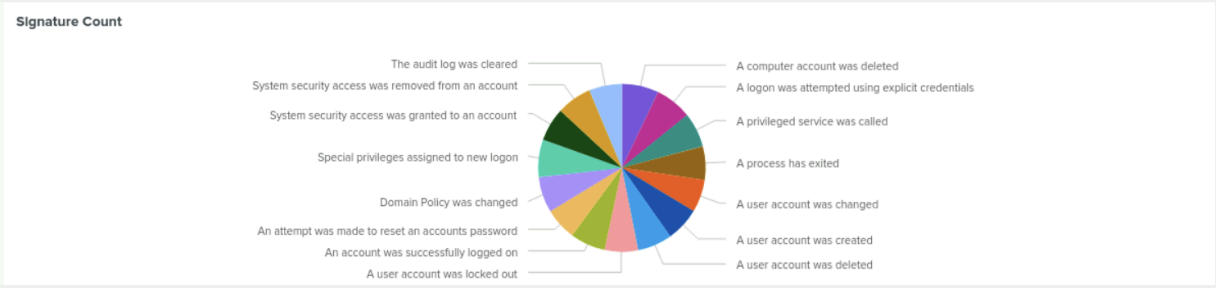
Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

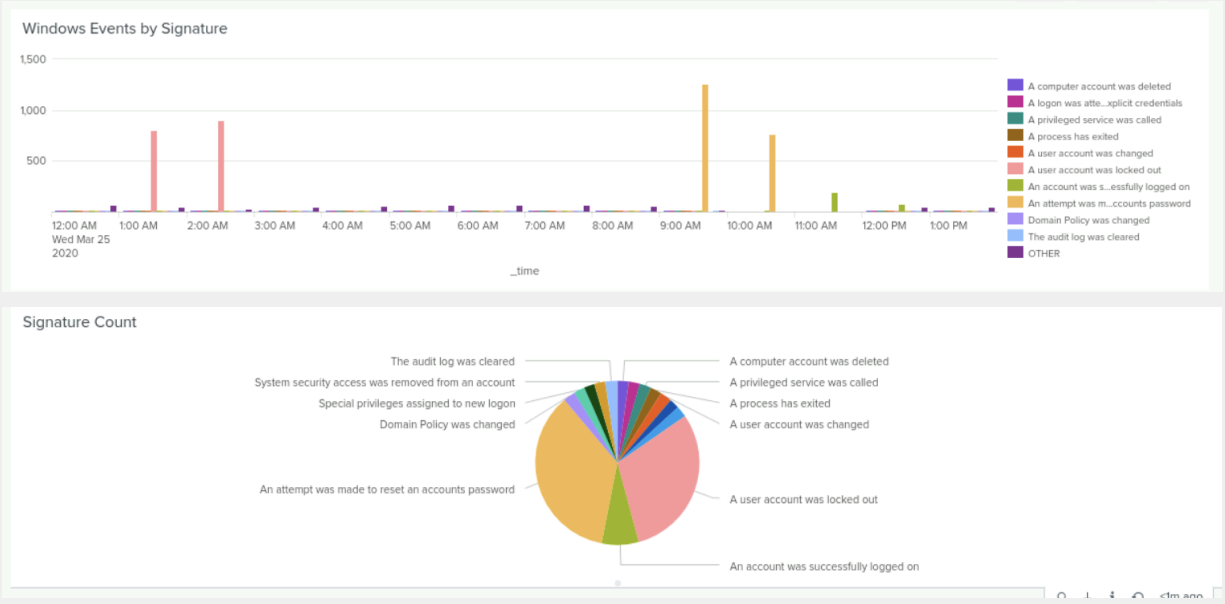
```
Yes, there is a significant increase in two signature types:
   1. An attempt was made to reset an account password.
   2. A user account was locked out.
```

Normal Logs:





Attack Logs:



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

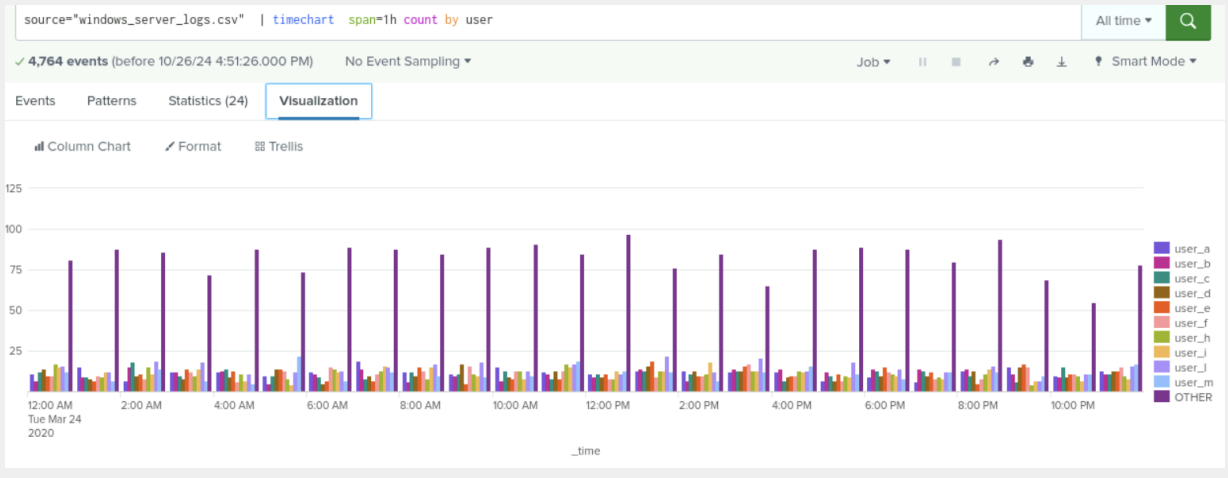
Yes, they do.

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

- Does anything stand out as suspicious?

Yes, there is increased activity for user_a and user_k.

Normal Logs:



Attack Logs:

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

```
Yes, they do.
```

Dashboard Analysis for Users with Statistical Charts

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

```
One advantage of using statistical time charts for signatures and users is
the ability to quickly determine the count for each event or user per hour.
However, a disadvantage compared to bar graphs and pie charts is that time
charts do not clearly indicate when there are changes in activity levels. In
contrast, visualizations like bar graphs and pie charts effectively
highlight spikes or declines in events, as well as the specific times these
```

changes occur. Pie charts, in particular, provide a quick overview of which events or users are experiencing an increase in activity.

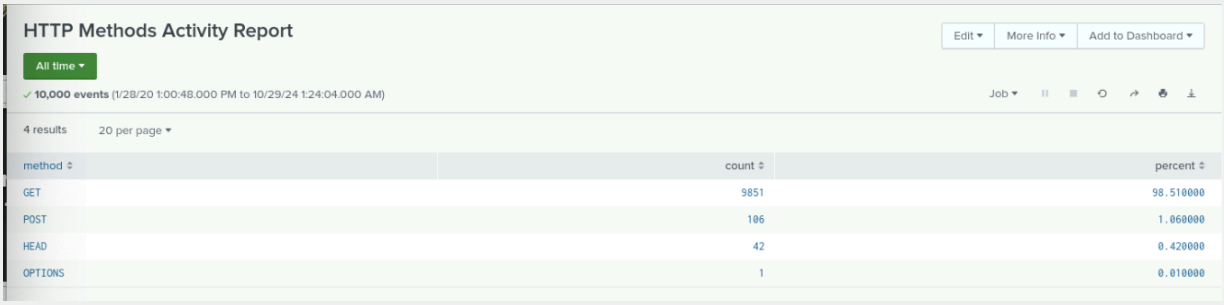
Apache Web Server Log Questions

Report Analysis for Methods

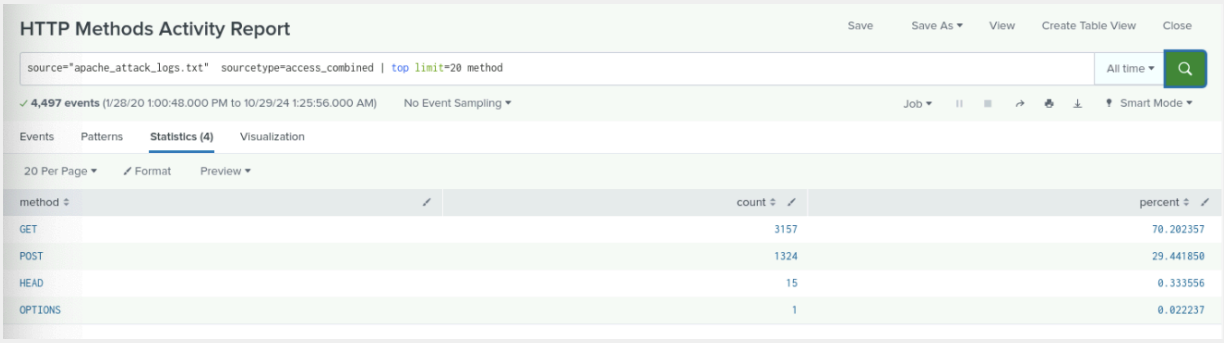
- Did you detect any suspicious changes in HTTP methods? If so, which one?

Yes, we detected suspicious changes in HTTP methods, specifically with "POST".

Normal Logs:



Attack Logs:



- What is that method used for?

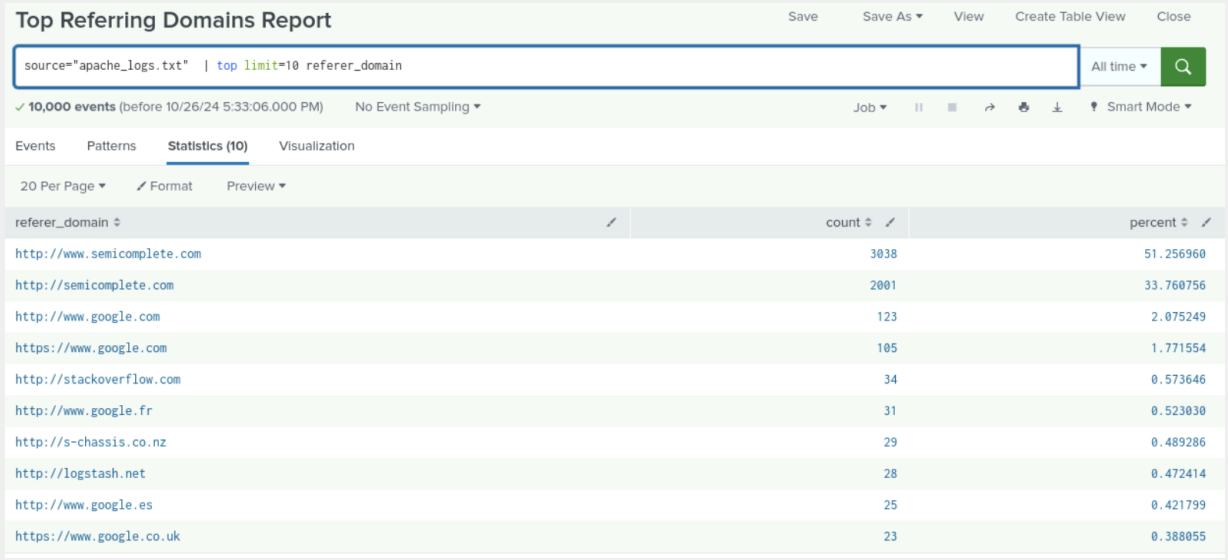
POST:is used to send data to the server from the HTTP client.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

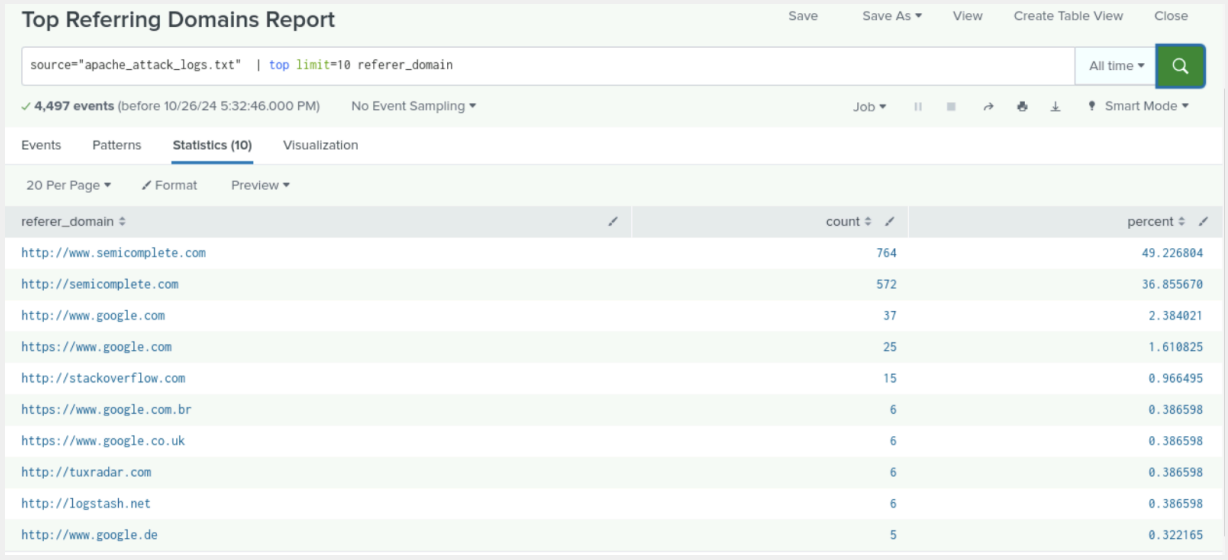
We noticed some changes in the results of the top 10 referrer domains' specifically with the last 5 of the list.

Normal Logs:



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
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

Attack Logs:



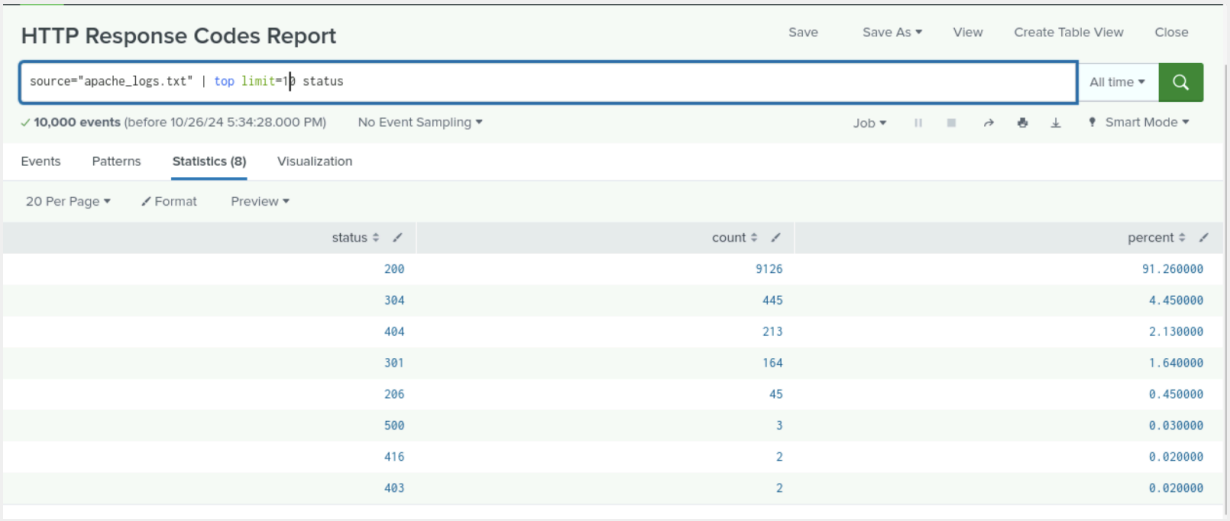
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

Report Analysis for HTTP Response Codes

- Did you detect any suspicious changes in HTTP response codes?

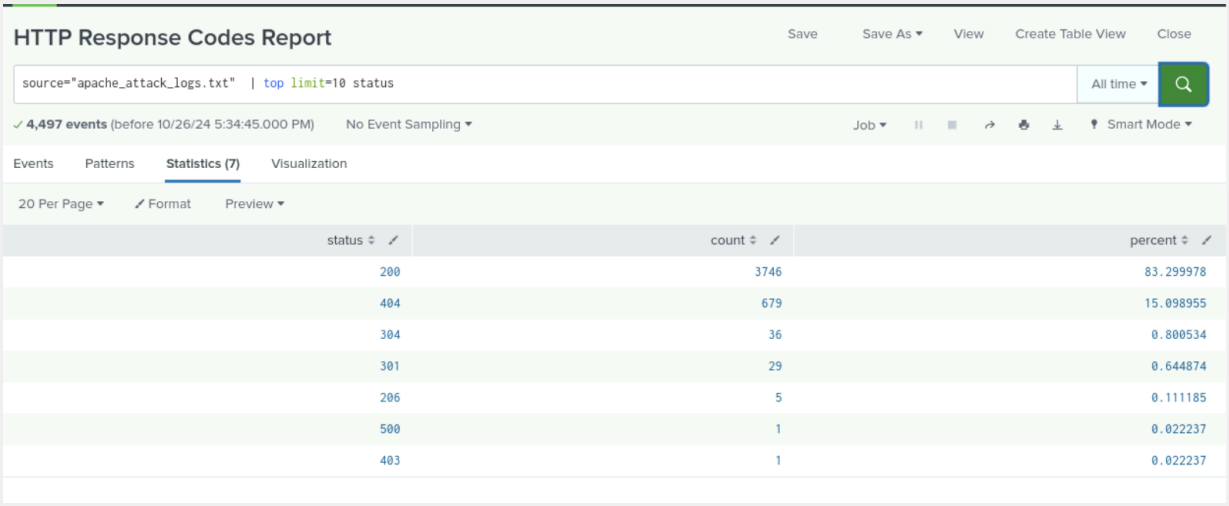
We detected a suspicious change in HTTP response codes, specifically with response code "200" and "404". Response code 200 saw a decrease in amount and 404 saw an increase.

Normal Logs:



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

Attack Logs:

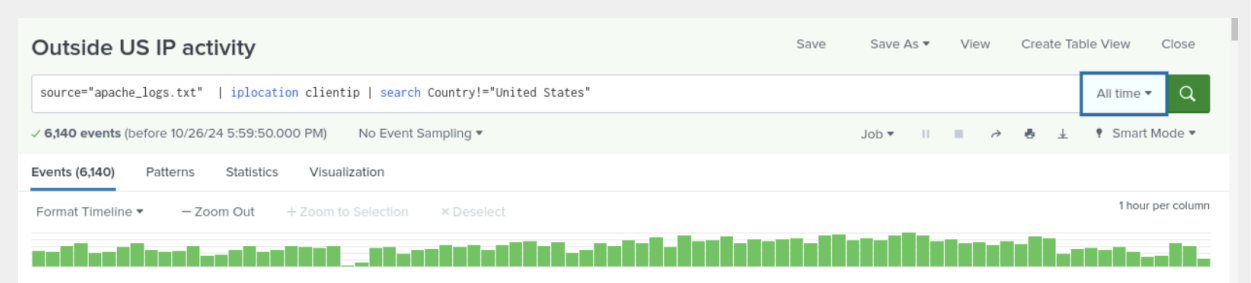


status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

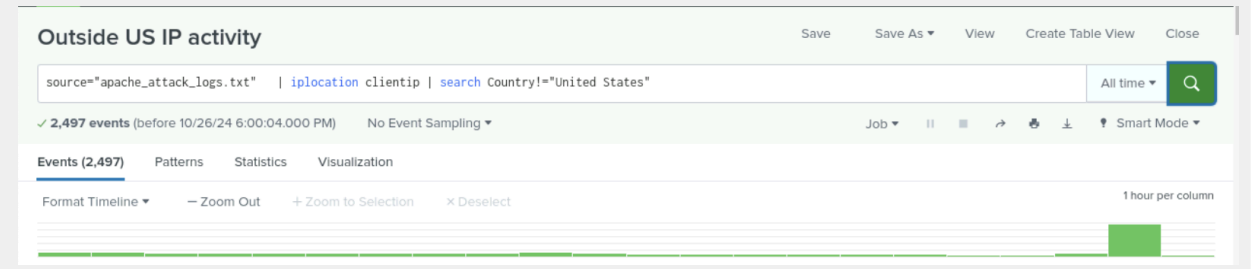
Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, we detected a suspicious volume of international activity.
Normal Logs:
```

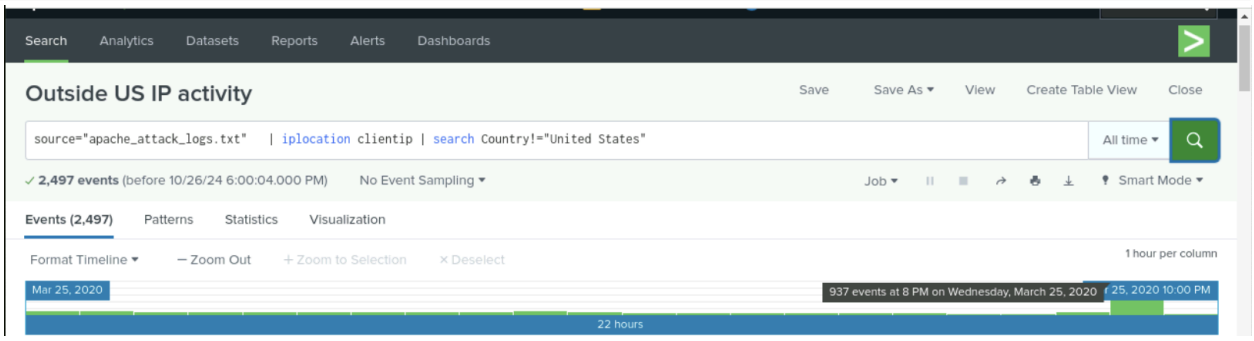


Attack Logs:



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

The count was 937 at 08:00 PM.



- Would your alert be triggered for this activity?

Yes, our alert would have been triggered, as we set the threshold to over 150 events per hour, and this activity significantly exceeded that limit.

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

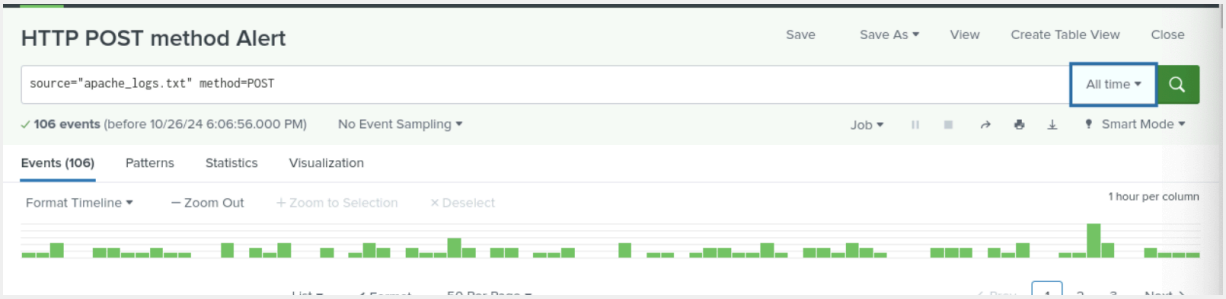
I would keep my threshold the same but continue monitoring the Apache logs to see if we could safely raise the threshold amount in the future.

Alert Analysis for HTTP POST Activity

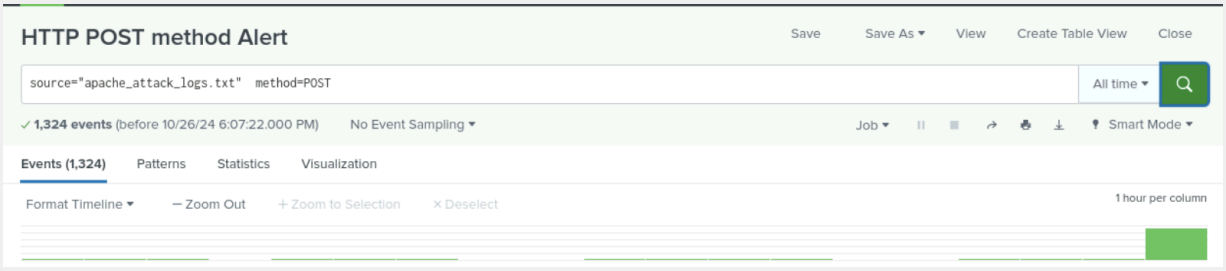
- Did you detect any suspicious volume of HTTP POST activity?

Yes, we detected a suspicious volume of HTTP POST activity.

Normal Logs:

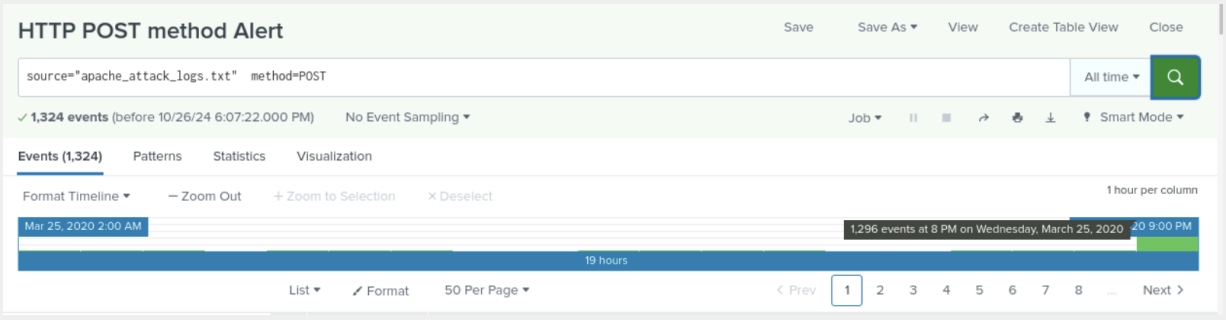


Attack Logs:



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

The count was 1296 at 08:00 PM



- When did it occur?

On 2020-03-25 at 08:00 PM.

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

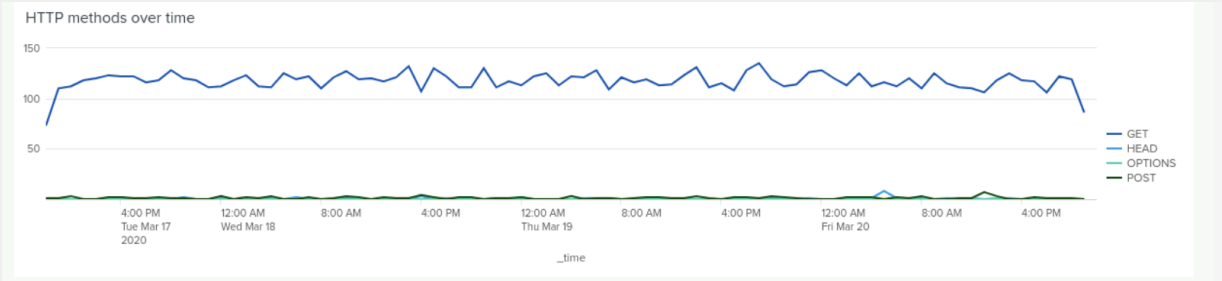
I would initially adjust my threshold number, which is currently set at 15, and conduct further analysis of the daily Apache logs to assess whether it could be safely increased.

Dashboard Analysis for Time Chart of HTTP Methods

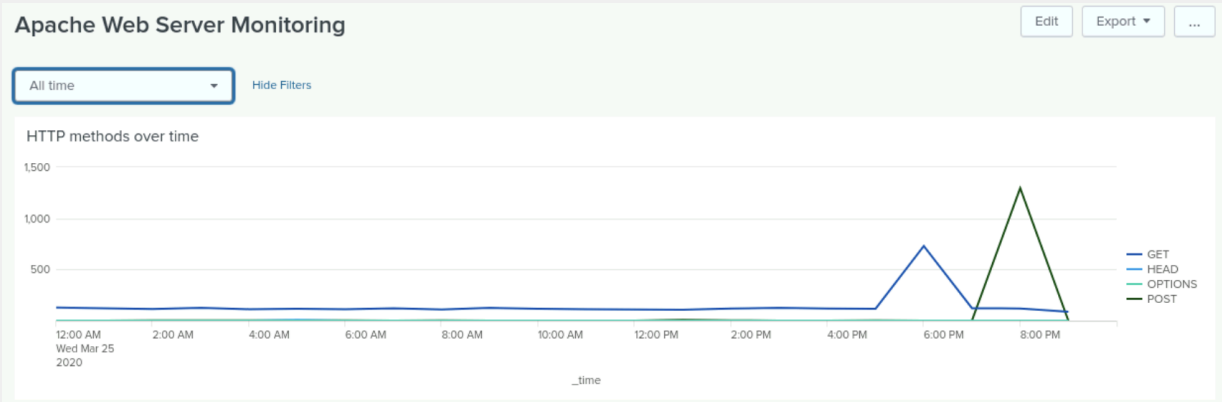
- Does anything stand out as suspicious?

Yes, there is a significant difference in the HTTP method time charts.

Normal Logs:



Attack Logs:



- Which method seems to be used in the attack?

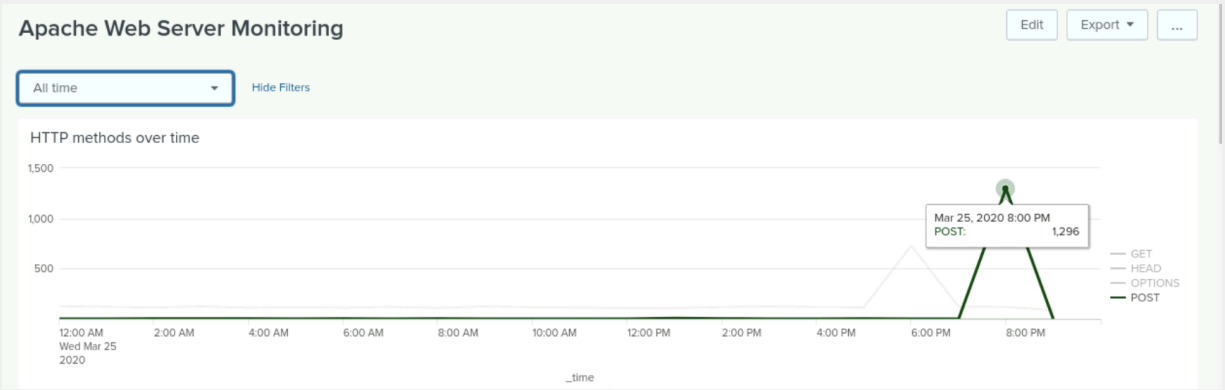
POST.

- At what times did the attack start and stop?

It appears to have occurred between 07:00 PM and 09:00 PM.

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

1296.

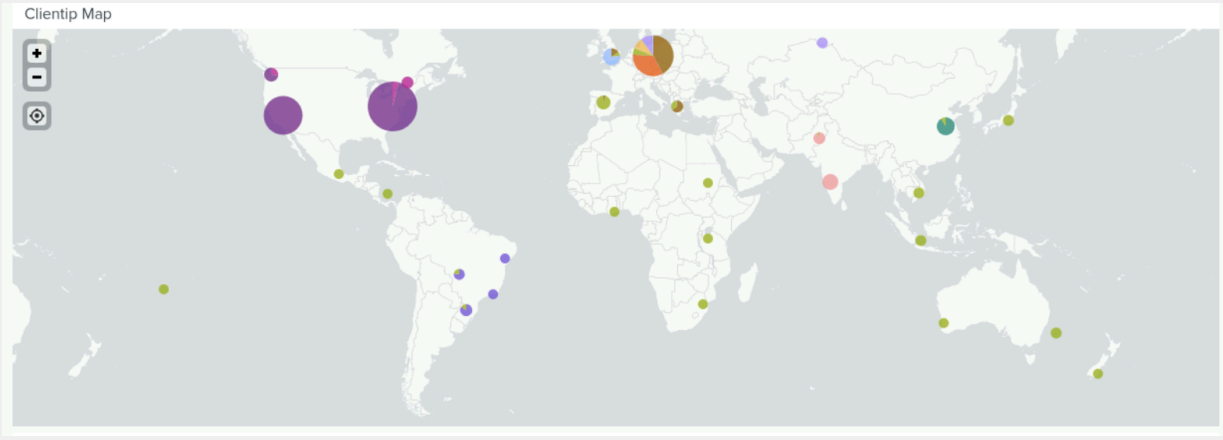


Dashboard Analysis for Cluster Map

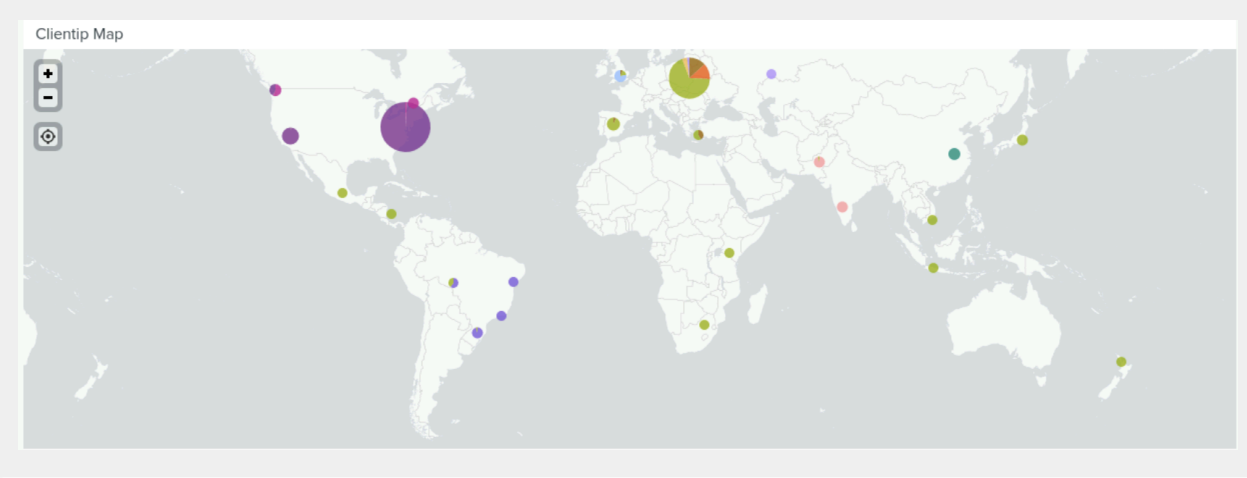
- Does anything stand out as suspicious?

Yes.

Normal Logs:



Attack Logs:

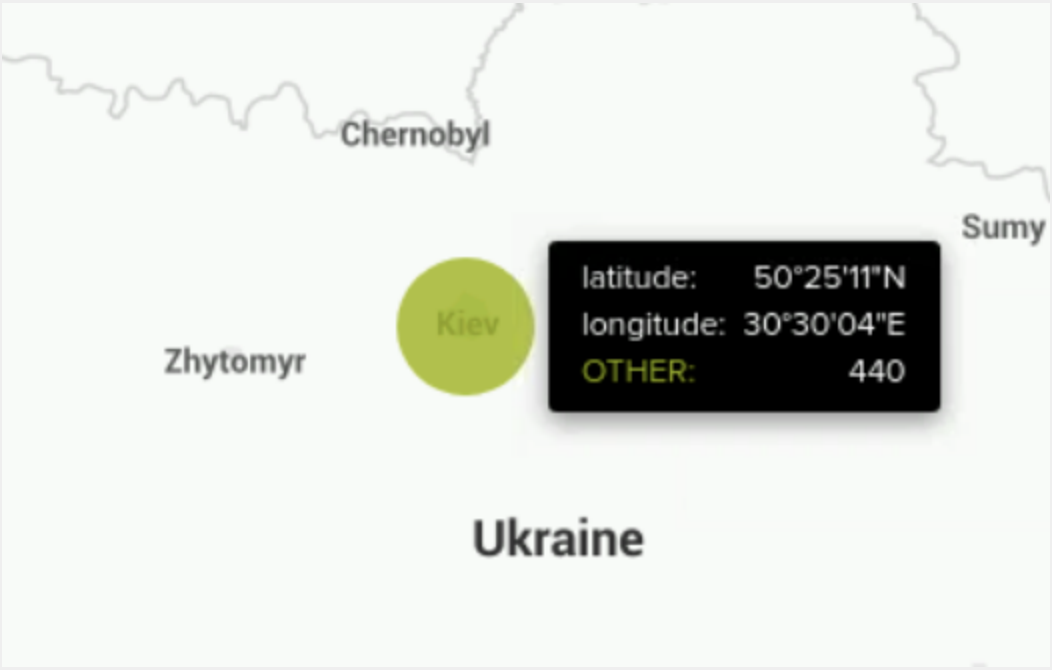


- Which new location (city, country) on the map has a high volume of activity? (**Hint**: Zoom in on the map.)

```
Kiev and Kharkiv in Ukraine both had an increase in activity.
```

- What is the count of that city?

```
Kiev:440
```

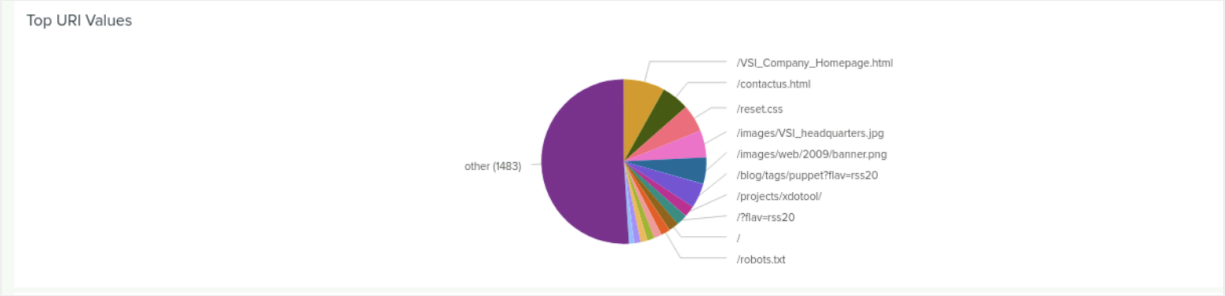


Kharkiv:432

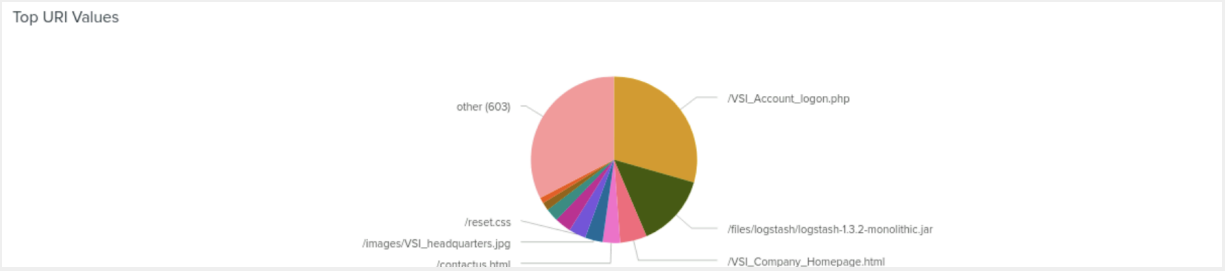
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, it does.
Normal Log:



Attack Logs:



- What URI is hit the most?

```
Taking out “other” as it is composed of many URIs too small to chart , the
URI hit the most is VSI_Account_logon.php.
```

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

```
Based on the URI being accessed, the attacker may be attempting a brute
force attack or an SQL injection. The significant number of 404 errors
further suggests that we could narrow our focus to an attacker conducting
reconnaissance by scanning the network through brute force attempts to
gather information.
```