Cybersecurity

Project 3 Review Questions

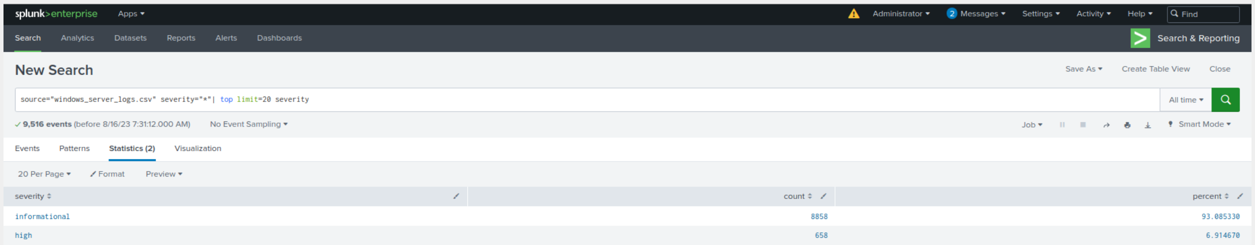
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, it's been discovered that there have been suspicious changes in severity. A suspicious change has been observed in the high-severity event which could indicate that a serious threat occurred to Windows Server during this attack. The Windows server logs had severity events around a maximum of 436 events per hour and The Windows server attack logs severity events drastically increased 1293 events per hour.

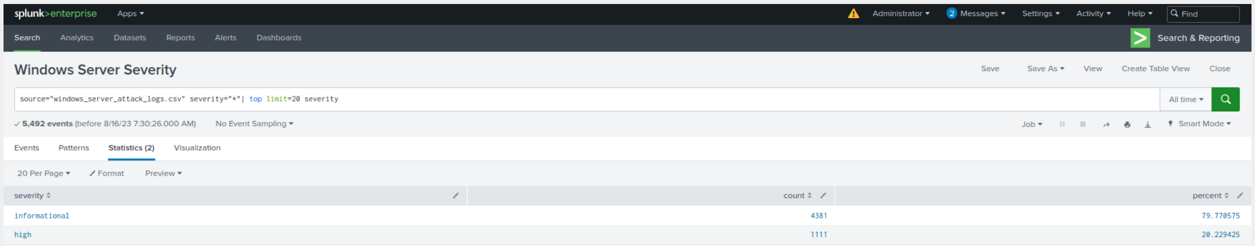


New Search

```
source="windows_server_logs.csv" severity="*"| top limit=20 severity
```

✓ 9,516 events (before 8/16/23 7:31:12.000 AM) No Event Sampling

severity	count	percent
informational	8858	93.085330
high	658	6.914670

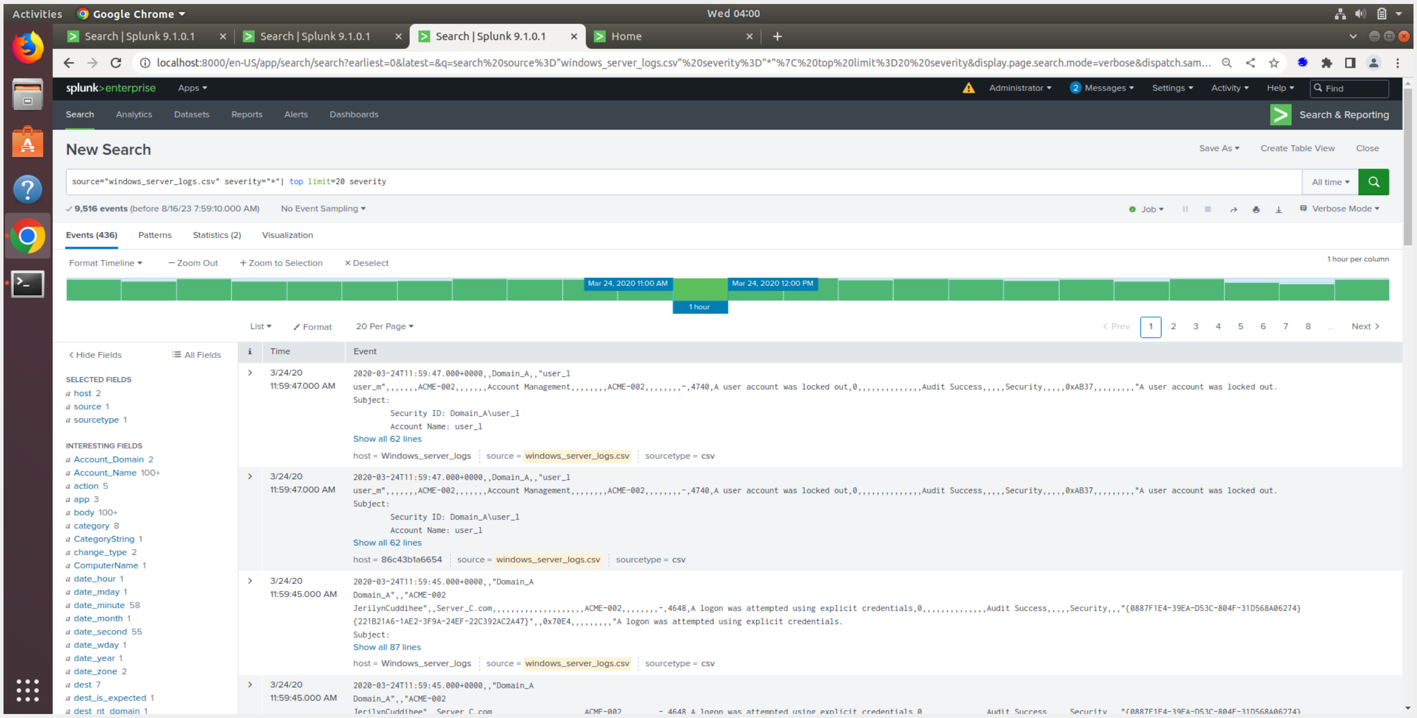


Windows Server Severity

```
source="windows_server_attack_logs.csv" severity="*"| top limit=20 severity
```

✓ 5,492 events (before 8/16/23 7:30:26.000 AM) No Event Sampling

severity	count	percent
informational	4381	79.770575
high	1111	20.229425



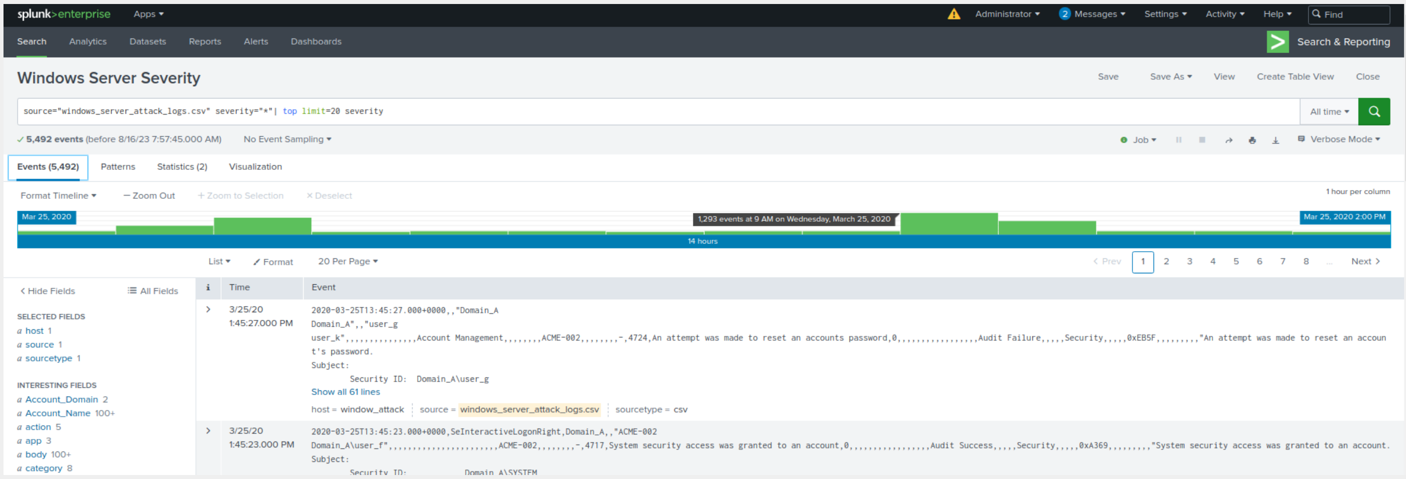
New Search

```
source="windows_server_logs.csv" severity="*"| top limit=20 severity
```

✓ 9,516 events (before 8/16/23 7:59:10.000 AM)   No Event Sampling

Events (436)   Patterns   Statistics (2)   Visualization

```
3/24/20 11:59:47.000 AM
2020-03-24T11:59:47.000+0000,,Domain_A,,"user_l
user_m",,,,,,,ACME-002,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4740,A user account was locked out,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xAB37,,,,,,,,,"A user account was locked out.
Subject:
        Security ID: Domain_A\user_l
        Account Name: user_l
Show all 62 lines
host = Windows_server_logs | source = windows_server_logs.csv | sourcetype = csv

3/24/20 11:59:47.000 AM
2020-03-24T11:59:47.000+0000,,Domain_A,,"user_l
user_m",,,,,,,ACME-002,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4740,A user account was locked out,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xAB37,,,,,,,,,"A user account was locked out.
Subject:
        Security ID: Domain_A\user_l
        Account Name: user_l
Show all 62 lines
host = 86c43b1a6654 | source = windows_server_logs.csv | sourcetype = csv

3/24/20 11:59:45.000 AM
2020-03-24T11:59:45.000+0000,,"Domain_A
Domain_A",,"ACME-002
JerilynCuddihee",,Server_C.com,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4648,A logon was attempted using explicit credentials,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,"{0887F1E4-39EA-D53C-804F-31D568A06274}
{221B21A6-1AE2-3F9A-24EF-22C392AC2A47}",,0x70E4,,,,,,,,,"A logon was attempted using explicit credentials.
Subject:
Show all 87 lines
host = Windows_server_logs | source = windows_server_logs.csv | sourcetype = csv

3/24/20 11:59:45.000 AM
2020-03-24T11:59:45.000+0000,,"Domain_A
Domain_A",,"ACME-002
```



Windows Server Severity

```
source="windows_server_attack_logs.csv" severity="*"| top limit=20 severity
```

✓ 5,492 events (before 8/16/23 7:57:45.000 AM)   No Event Sampling

Events (5,492)   Patterns   Statistics (2)   Visualization

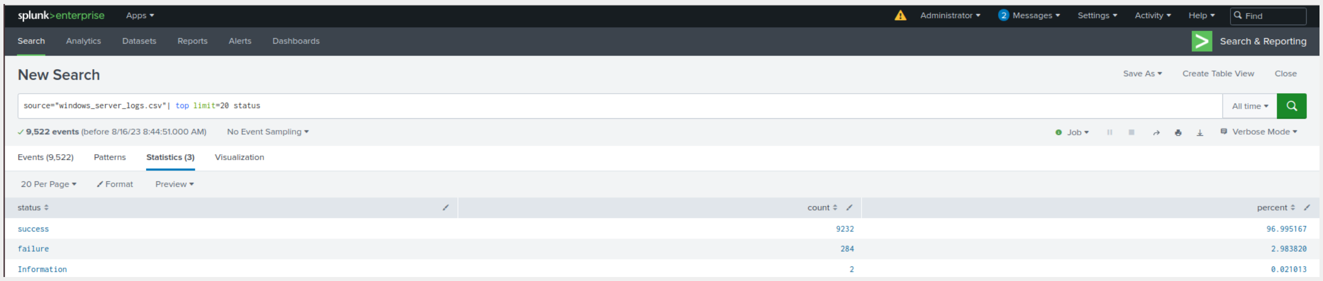
```
3/25/20 1:45:27.000 PM
2020-03-25T13:45:27.000+0000,,"Domain_A
Domain_A",,"user_g
user_k",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0xEB5F,,,,,,,,,"An attempt was made to reset an accoun
t's password.
Subject:
        Security ID:  Domain_A\user_g
Show all 61 lines
host = window_attack | source = windows_server_attack_logs.csv | sourcetype = csv

3/25/20 1:45:23.000 PM
2020-03-25T13:45:23.000+0000,SeInteractiveLogonRight,Domain_A,,"ACME-002
Domain_A\user_f",,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4717,System security access was granted to an account,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"System security access was granted to an account.
Subject:
        Security ID:            Domain_A\SYSTEM
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
We have spotted changes to the failed activities. Compared to the earlier log, the
counts of unsuccessful operations have decreased.
In the Windows Server log the percentage of failed activities was 2.98% and the
Windows server attack log has a 1.56%.
```

As per the findings, We did not find anything suspicious for events pertaining to failed activities



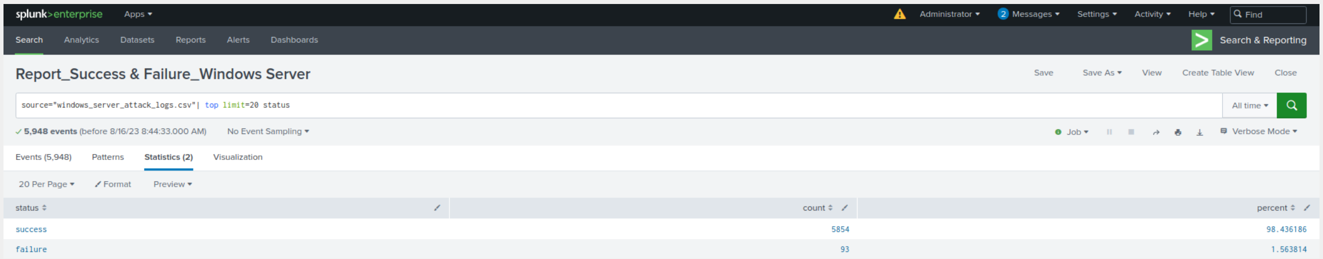
New Search

```
source="windows_server_logs.csv"| top limit=20 status
```

✓ 9,522 events (before 8/16/23 8:44:51.000 AM) No Event Sampling

Events (9,522) Patterns Statistics (3) Visualization

status	count	percent
success	9232	96.995167
failure	284	2.983820
Information	2	0.021013



Report_Success & Failure_Windows Server

```
source="windows_server_attack_logs.csv"| top limit=20 status
```

✓ 5,948 events (before 8/16/23 8:44:33.000 AM) No Event Sampling

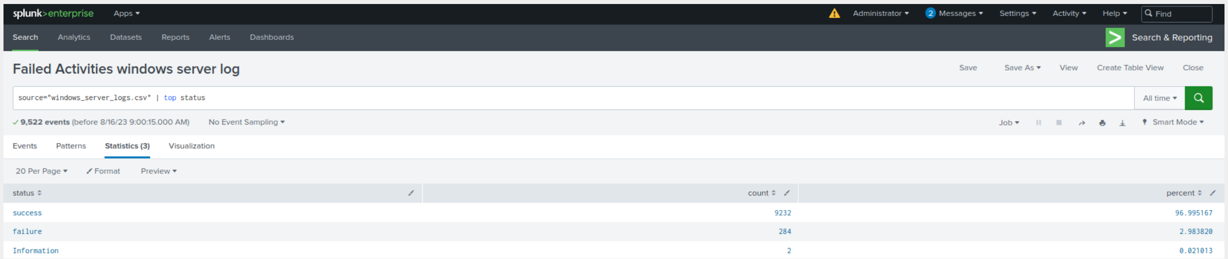
Events (5,948) Patterns Statistics (2) Visualization

status	count	percent
success	5854	98.436186
failure	93	1.563814

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

We have seen a change in the failed activities. Compared to the earlier log, the counts of unsuccessful operations have decreased. In the Windows Server log the percentage of failed activities was 2.98% and the Windows server attack log has a 1.56%. Based on the findings, we have found no evidence of any irregularity with regard to events concerning unsuccessful activities.



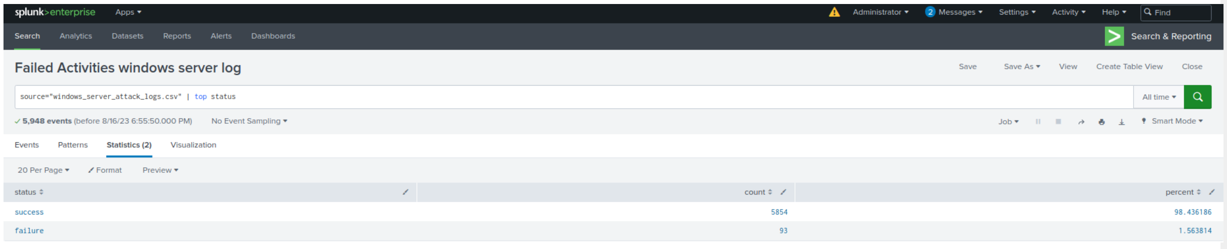
Failed Activities windows server log

```
source="windows_server_logs.csv" | top status
```

✓ 9,522 events (before 8/16/23 9:00:15.000 AM) No Event Sampling

Events Patterns Statistics (3) Visualization

status	count	percent
success	9232	96.995167
failure	284	2.983820
Information	2	0.021013

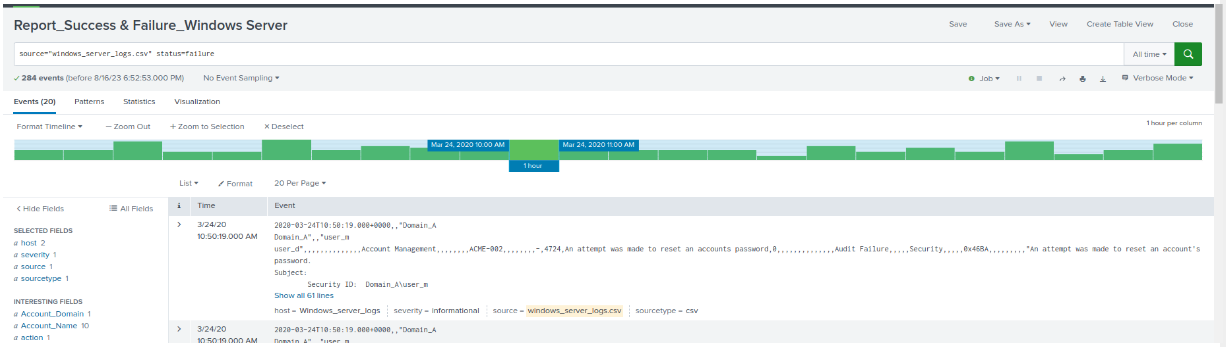


Failed Activities windows server log

```
source="windows_server_attack_logs.csv" | top status
```

✓ 5,948 events (before 8/16/23 6:55:50.000 PM) No Event Sampling

status	count	percent
success	5854	98.436186
failure	93	1.563814



Report_Success & Failure_Windows Server

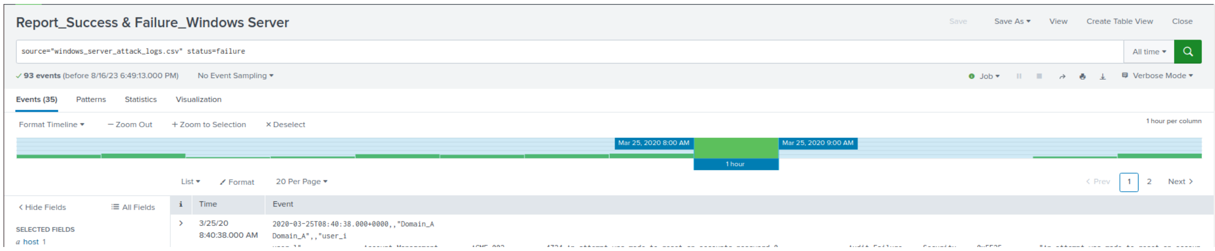
```
source="windows_server_logs.csv" status=failure
```

✓ 284 events (before 8/16/23 6:52:53.000 PM) No Event Sampling

SELECTED FIELDS
a host 2
a severity 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 1
a Account_Name 10
a action 1

```
i  Time                 Event
>  3/24/20              2020-03-24T10:50:19.000+0000,,"Domain_A
   10:50:19.000 AM      Domain_A",,"user_m
                        user_d",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x46BA,,,,,,,,,"An attempt was made to reset an account's
                        password.
                        Subject:
                                Security ID:  Domain_A\user_m
                        Show all 61 lines
                        host = Windows_server_logs | severity = informational | source = windows_server_logs.csv | sourcetype = csv
>  3/24/20              2020-03-24T10:50:19.000+0000,,"Domain_A
   10:50:19.000 AM      Domain_A",,"user_m
```



Report_Success & Failure_Windows Server

```
source="windows_server_attack_logs.csv" status=failure
```

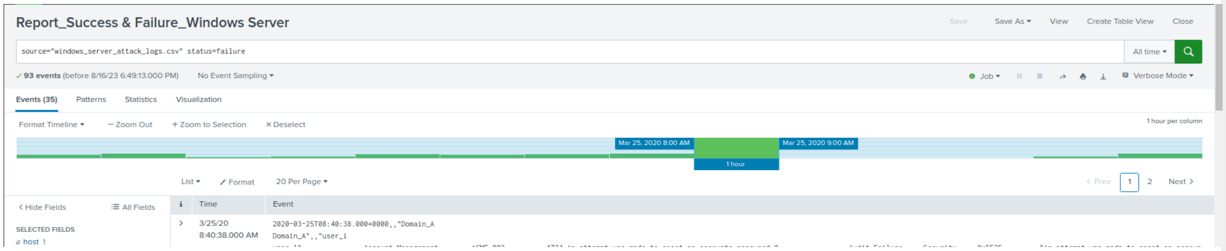
✓ 93 events (before 8/16/23 6:49:13.000 PM) No Event Sampling

SELECTED FIELDS
a host 1

```
i  Time                 Event
>  3/25/20              2020-03-25T08:40:38.000+0000,,"Domain_A
   8:40:38.000 AM       Domain_A",,"user_i
```

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

```
The elevated count of events is 35 per hour in the Windosw attack log file,
which is slightly higher than the Windows server log file.
```


Report_Success & Failure_Windows Server

source="windows_server_attack_logs.csv" status=failure

✓ 93 events (before 8/16/23 6:49:13.000 PM) No Event Sampling

Events (35) Patterns Statistics Visualization

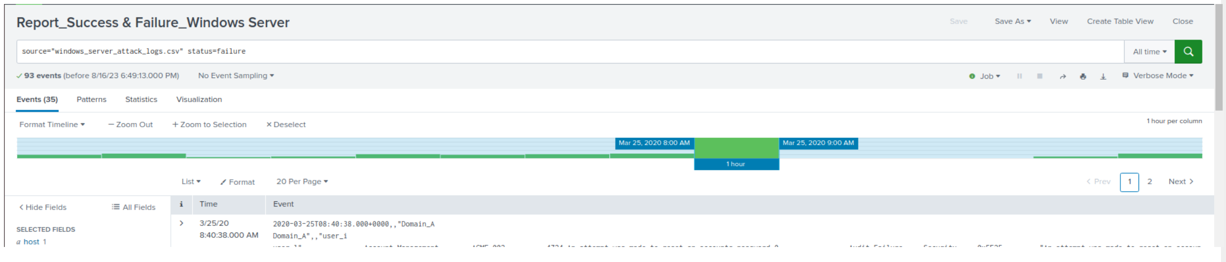
Mar 25, 2020 8:00 AM Mar 25, 2020 9:00 AM 1 hour

SELECTED FIELDS
a host 1

3/25/20 8:40:38.000 AM 2020-03-25T08:40:38.000+0000,,"Domain_A
Domain_A",,"user_i

- When did it occur?

The little elevated failed activity occurred at 8:00am on 2020-03-25



Report_Success & Failure_Windows Server

```
source="windows_server_attack_logs.csv" status=failure
```

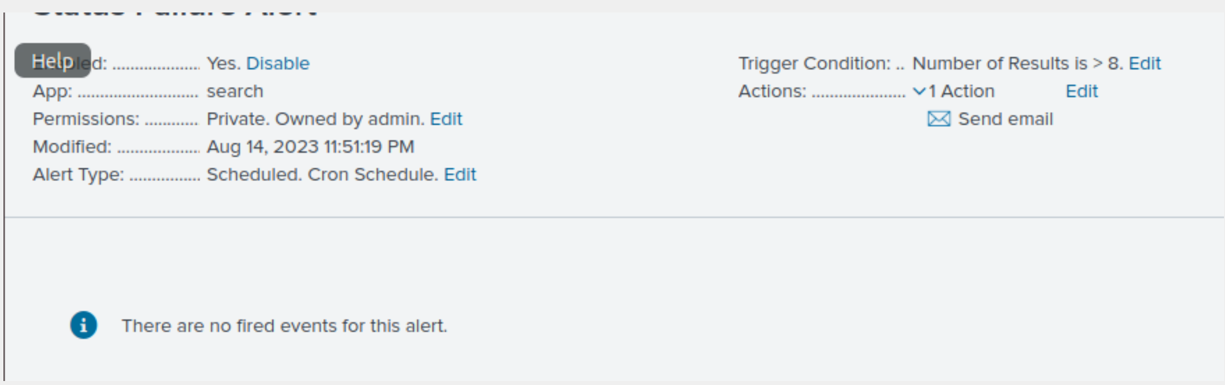
✓ 93 events (before 8/16/23 6:49:13.000 PM) No Event Sampling

Events (35) Patterns Statistics Visualization

i	Time	Event
›	3/25/20 8:40:38.000 AM	2020-03-25T08:40:38.000+0000,,"Domain_A Domain_A",,"user_i

- Would your alert be triggered for this activity?

Yes, My alert would be triggered by this activity because of the alert threshold set anything greater than 8 will trigger the alert.



Help d: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 14, 2023 11:51:19 PM
Alert Type: .... Scheduled. Cron Schedule. Edit

Trigger Condition: .. Number of Results is > 8. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

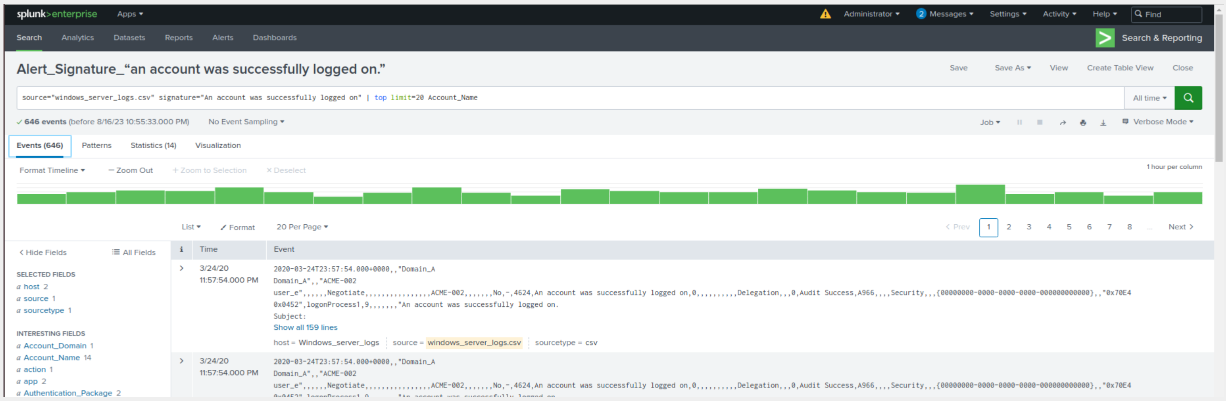
- After reviewing, would you change your threshold from what you previously selected?

No, I'm not going to make a difference in the trigger. A high number of unsuccessful activities, which were incongruous and warranted attention, had been detected by the existing trigger. This indicates that for the purpose of detecting irregular activity, a threshold should be set at an adequate level.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes, we're detecting a suspicious volume of successfully opened logins. Normal events range in size from 20 to 40 The attack logs indicate there have been 196 occurrences over an hour that are suspect.



Alert_Signature_"an account was successfully logged on."

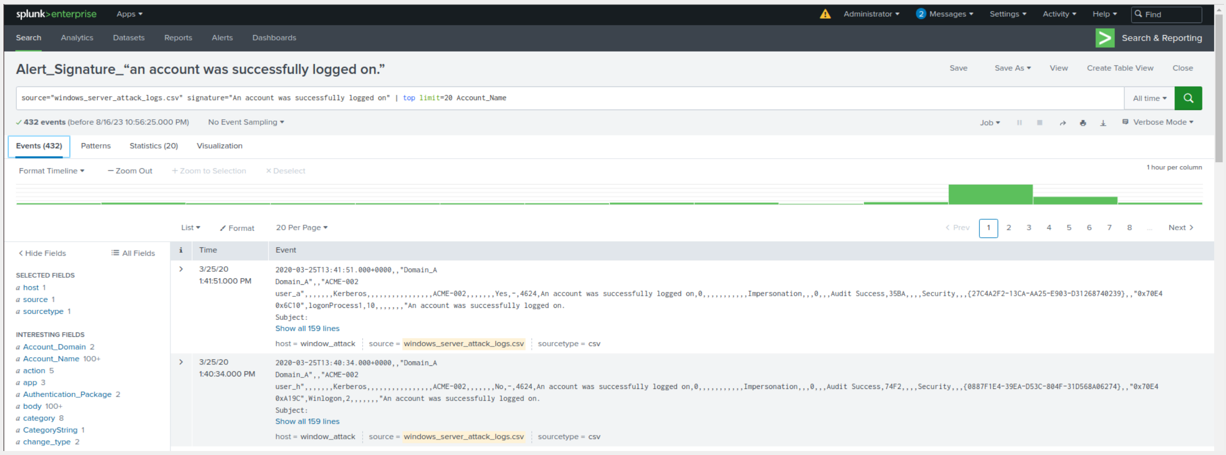
```
source="windows_server_logs.csv" signature="An account was successfully logged on" | top limit=20 Account_Name
```

✓ 646 events (before 8/16/23 10:55:33.000 PM) No Event Sampling

SELECTED FIELDS
- host 2
- source 1
- sourcetype 1

INTERESTING FIELDS
- Account_Domain 1
- Account_Name 14
- action 1
- app 2
- Authentication_Package 2

Time	Event
3/24/20 11:57:54.000 PM	2020-03-24T23:57:54.000+0000,,"Domain_A Domain_A",,"ACME-002 user_e",,,,,,Negotiate,,,,,,,,,,,,,,,ACME-002,,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,,Delegation,,,0,Audit Success,A966,,,,Security,,,{00000000-0000-0000-0000-000000000000},,"0x70E4 0x0452",logonProcess1,9,,,,,,,"An account was successfully logged on. Subject: Show all 159 lines host = Windows_server_logs source = windows_server_logs.csv sourcetype = csv
3/24/20 11:57:54.000 PM	2020-03-24T23:57:54.000+0000,,"Domain_A Domain_A",,"ACME-002 user_e",,,,,,Negotiate,,,,,,,,,,,,,,,ACME-002,,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,,Delegation,,,0,Audit Success,A966,,,,Security,,,{00000000-0000-0000-0000-000000000000},,"0x70E4



Alert_Signature_"an account was successfully logged on."

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on" | top limit=20 Account_Name
```

✓ 432 events (before 8/16/23 10:56:25.000 PM) No Event Sampling

SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- Account_Domain 2
- Account_Name 100+
- action 5
- app 3
- Authentication_Package 2
- body 100+
- category 8
- CategoryString 1
- change_type 2

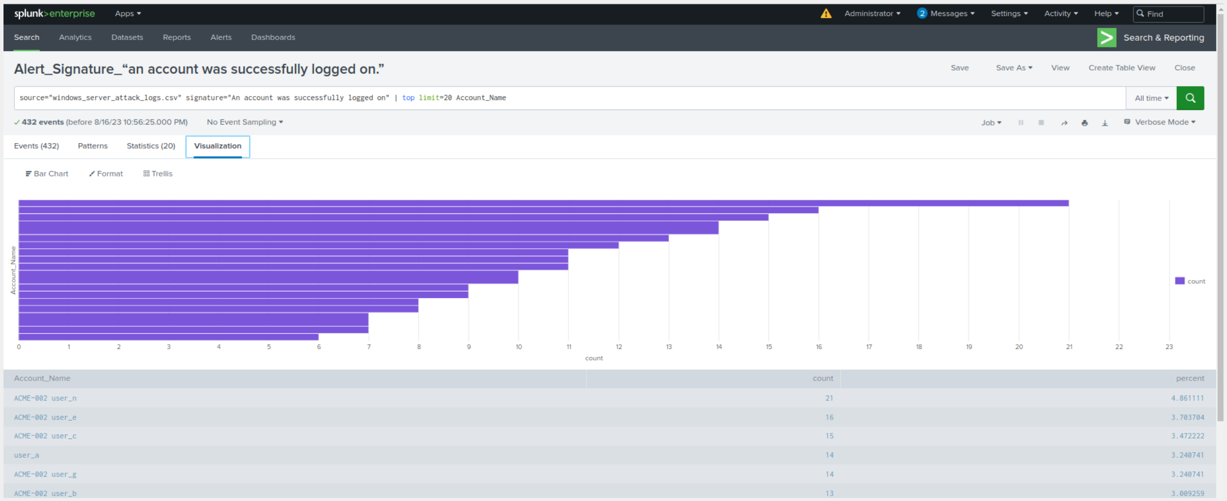
Time	Event
3/25/20 1:41:51.000 PM	2020-03-25T13:41:51.000+0000,,"Domain_A Domain_A",,"ACME-002 user_a",,,,,,,Kerberos,,,,,,,,,,,,,,,ACME-002,,,,,,,Yes,-,4624,An account was successfully logged on,0,,,,,,,,,,,Impersonation,,,0,,,Audit Success,35BA,,,,Security,,,{27C4A2F2-13CA-AA25-E903-D31268740239},,"0x70E4 0x6C10",logonProcess1,10,,,,,,,"An account was successfully logged on. Subject: Show all 159 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
3/25/20 1:40:34.000 PM	2020-03-25T13:40:34.000+0000,,"Domain_A Domain_A",,"ACME-002 user_h",,,,,,,Kerberos,,,,,,,,,,,,,,,ACME-002,,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,,,Impersonation,,,0,,,Audit Success,74F2,,,,Security,,,{0887F1E4-39EA-D53C-804F-31D568A06274},,"0x70E4 0xA19C",Winlogon,2,,,,,,,"An account was successfully logged on. Subject: Show all 159 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv

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

The count of the events is 196 events per hour.

- Who is the primary user logging in?

The primary user ACME=002 user_n is logging in.



Alert_Signature_“an account was successfully logged on.”

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on" | top limit=20 Account_Name
```

✓ 432 events (before 8/16/23 10:56:25.000 PM) No Event Sampling ▾

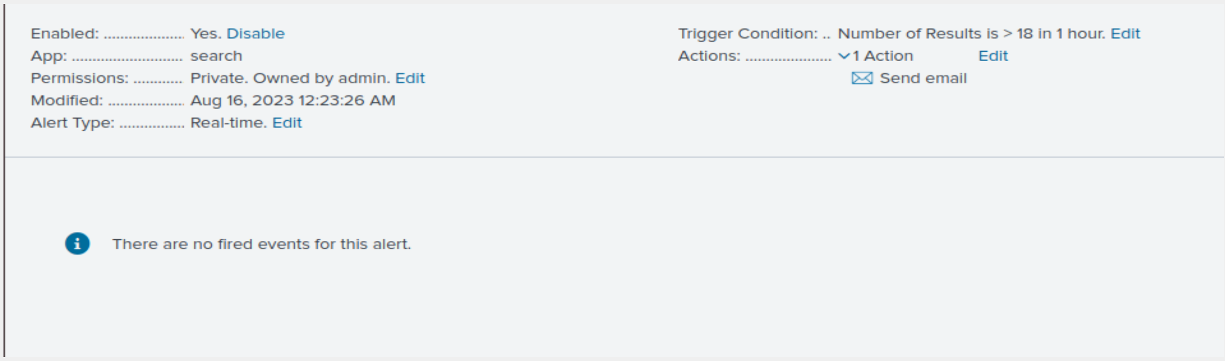
Account_Name	count	percent
ACME-002 user_n	21	4.861111
ACME-002 user_e	16	3.703704
ACME-002 user_c	15	3.472222
user_a	14	3.240741
ACME-002 user_g	14	3.240741
ACME-002 user_b	13	3.009259

- When did it occur?

```
March 25, 2020, 11:00 AM to 12:00 PM
```

- Would your alert be triggered for this activity?

```
Yes, My alert triggers as my threshold is set to 18
```



Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 16, 2023 12:23:26 AM
Alert Type: .... Real-time. Edit

Trigger Condition: .. Number of Results is > 18 in 1 hour. Edit
Actions: .... ⌄1 Action Edit
Send email

There are no fired events for this alert.

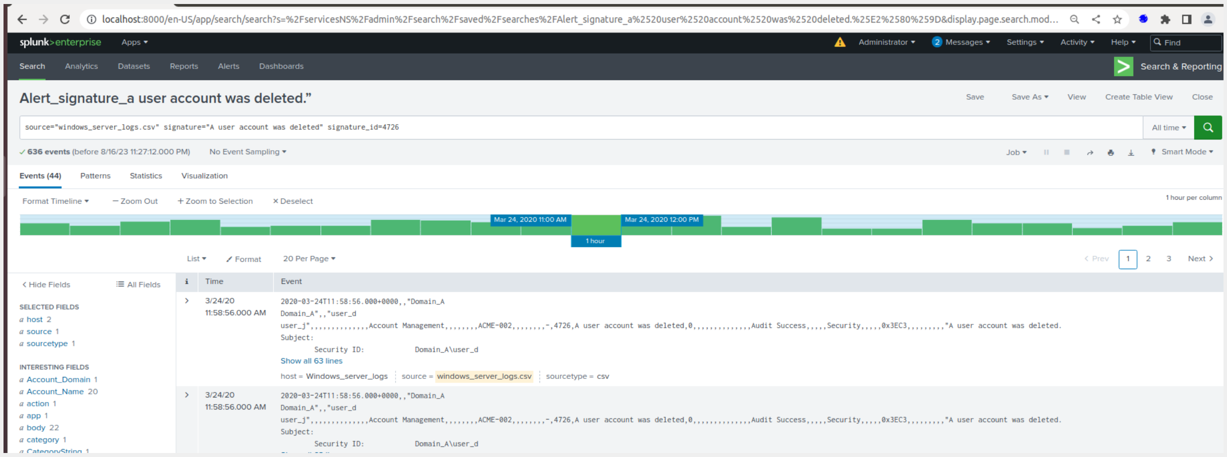
- After reviewing, would you change your threshold from what you previously selected?

```
No, We are not going to make a difference in the trigger. My threshold is set to anything greater than 18 will trigger the alert. This threshold was successfully alerted when the an increase in suspicious counts for the successfully logged-in account.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

No, it doesn't look like there's a suspicious amount of deleted accounts. The total number of accounts lost within the attack logs is equal to that found in an ordinary log. Indeed, the attack logs in question seem to show a lower number of accounts that have been shut down during some hours than when they are normally recorded.



Alert_signature_a user account was deleted.”

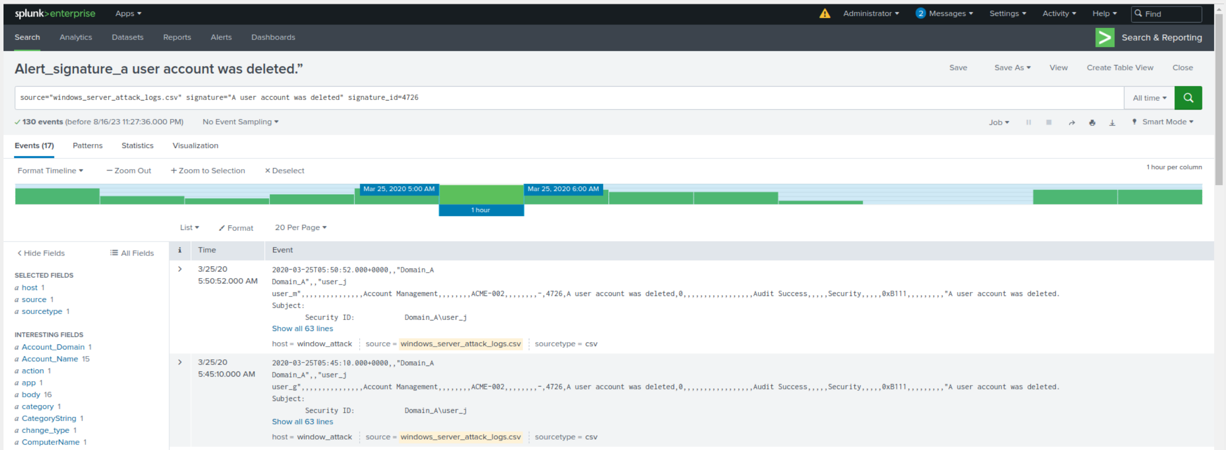
```
source="windows_server_logs.csv" signature="A user account was deleted" signature_id=4726
```

✓ 636 events (before 8/16/23 11:27:12.000 PM)

SELECTED FIELDS
- a host 2
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a Account_Domain 1
- a Account_Name 20
- a action 1
- a app 1
- a body 22
- a category 1
- a CategoryString 1

```
3/24/20 11:58:56.000 AM
2020-03-24T11:58:56.000+0000,,"Domain_A
Domain_A",,"user_d
user_j",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x3EC3,,,,,,,,,"A user account was deleted.
Subject:
        Security ID:            Domain_A\user_d
Show all 63 lines
host = Windows_server_logs | source = windows_server_logs.csv | sourcetype = csv

3/24/20 11:58:56.000 AM
2020-03-24T11:58:56.000+0000,,"Domain_A
Domain_A",,"user_d
user_j",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x3EC3,,,,,,,,,"A user account was deleted.
Subject:
        Security ID:            Domain_A\user_d
```



Alert_signature_a user account was deleted.”

```
source="windows_server_attack_logs.csv" signature="A user account was deleted" signature_id=4726
```

✓ 130 events (before 8/16/23 11:27:36.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

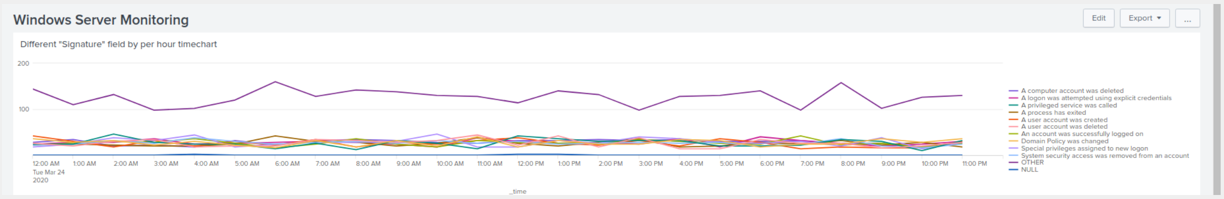
INTERESTING FIELDS
- a Account_Domain 1
- a Account_Name 15
- a action 1
- a app 1
- a body 16
- a category 1
- a CategoryString 1
- a change_type 1
- a ComputerName 1

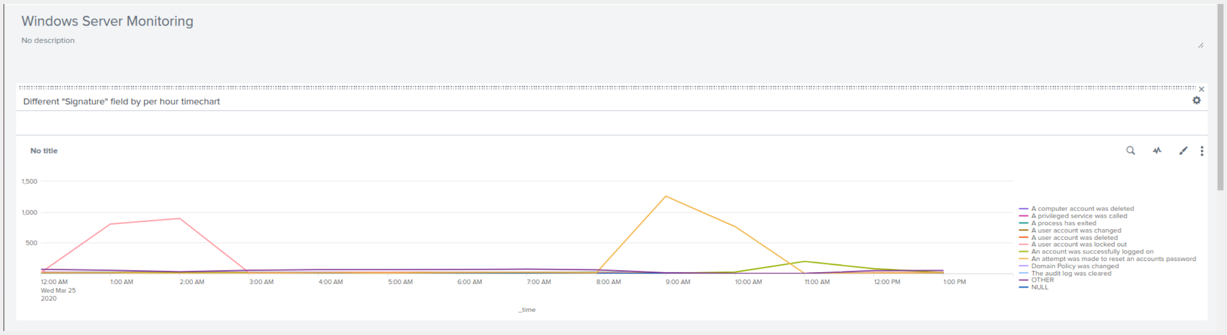
```
3/25/20 5:50:52.000 AM
2020-03-25T05:50:52.000+0000,,"Domain_A
Domain_A",,"user_j
user_m",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xB111,,,,,,,,,"A user account was deleted.
Subject:
        Security ID:            Domain_A\user_j
Show all 63 lines
host = window_attack | source = windows_server_attack_logs.csv | sourcetype = csv

3/25/20 5:45:10.000 AM
2020-03-25T05:45:10.000+0000,,"Domain_A
Domain_A",,"user_j
user_g",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xB111,,,,,,,,,"A user account was deleted.
Subject:
        Security ID:            Domain_A\user_j
Show all 63 lines
host = window_attack | source = windows_server_attack_logs.csv | sourcetype = csv
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

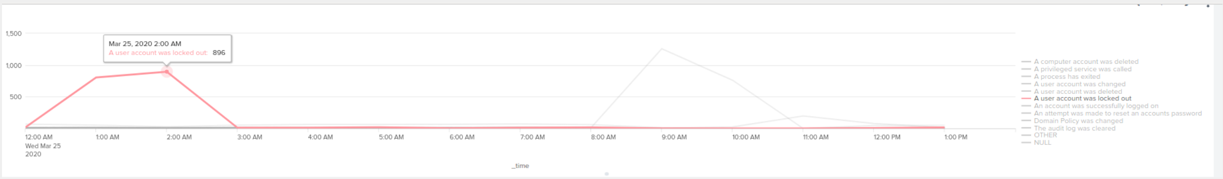
Yes, the Windows Server Time chart before the attack is higher for the “others” signature but after the attack time chart changes, and is suspicious activity detected. The user account has been locked and an attempt has been made to reset the password significantly higher than before.

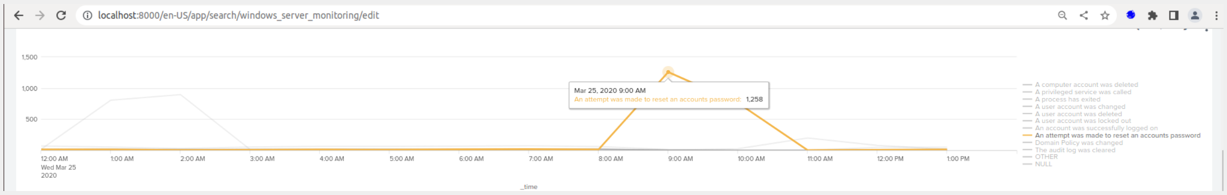




- What signatures stand out?

These two signatures stand out as follows:
1. A user account was locked out
2. An attempt was made to reset an account password





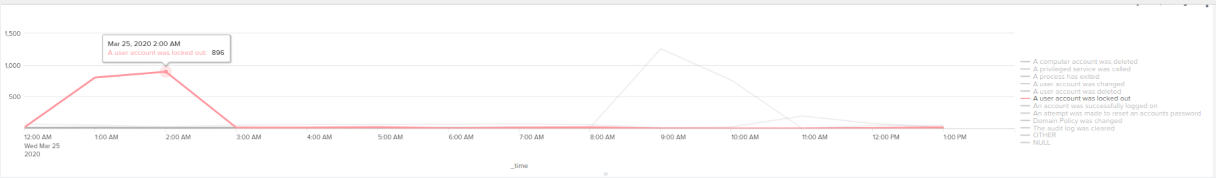
- What time did it begin and stop for each signature?

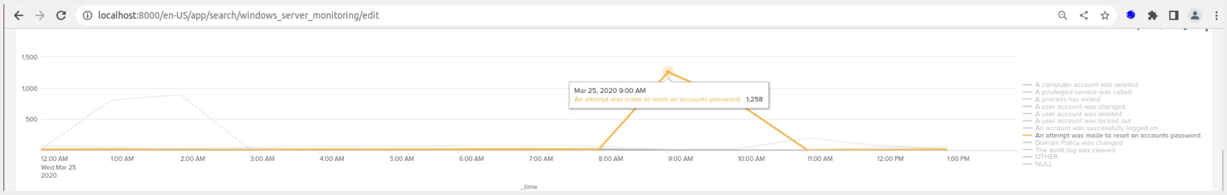
1. A user account was locked out
(It starts from 12:00 AM - 3:00 AM)

2. An attempt was made to reset an account password
(It starts from 8:00 AM - 11:00 AM)

- What is the peak count of the different signatures?

1. The signature “A user account was locked out” Peak count is 896
2. The signature “An attempt was made to reset an account password” peak count is 1258

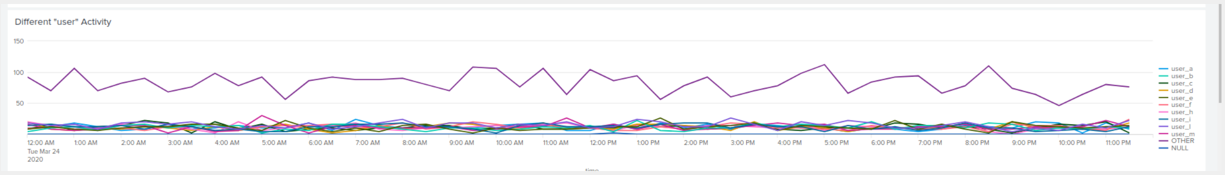


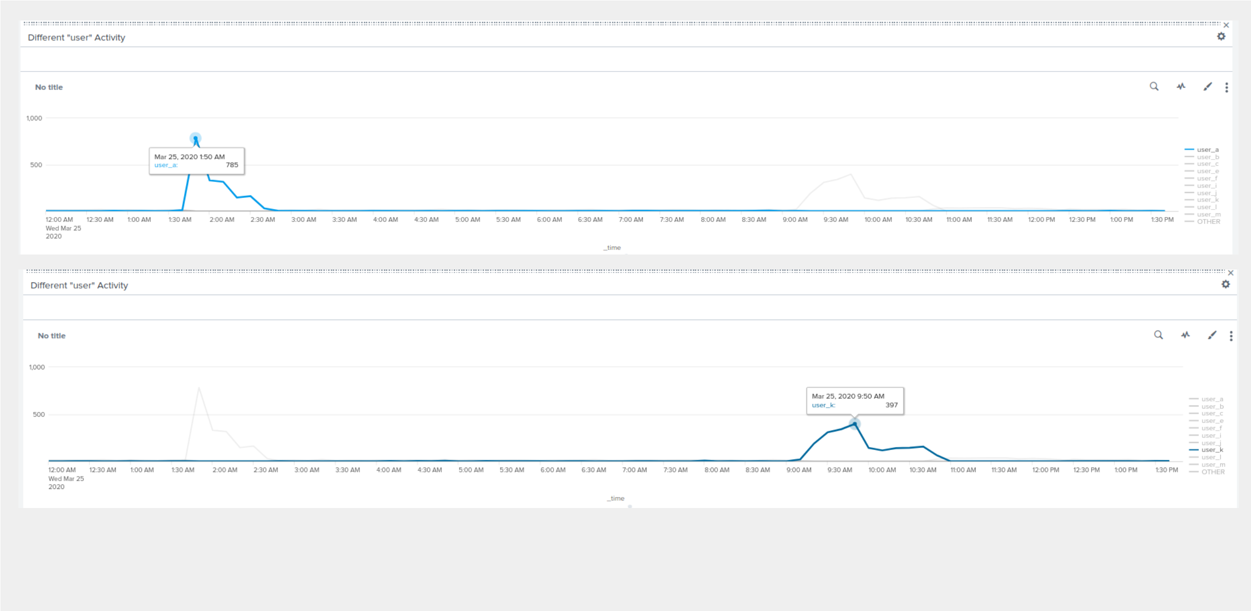

localhost:8000/en-US/app/search/windows_server_monitoring/edit
1,500
1,000
500
Mar 25, 2020 9:00 AM
An attempt was made to reset an accounts password: 1,258
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
_time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
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
NULL

Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes, two users “user_a” and “user_k” stand out, looks like their accounts are compromised.





- Which users stand out?

```
“User_a” and “User_k” stand out and looks like their account got
compromised.
```

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

```
  1. It starts for the “User_a” from 1:30 AM to 2:30 AM
  2. It starts for the “User_k” from 9:00 AM to 11:00 AM
```

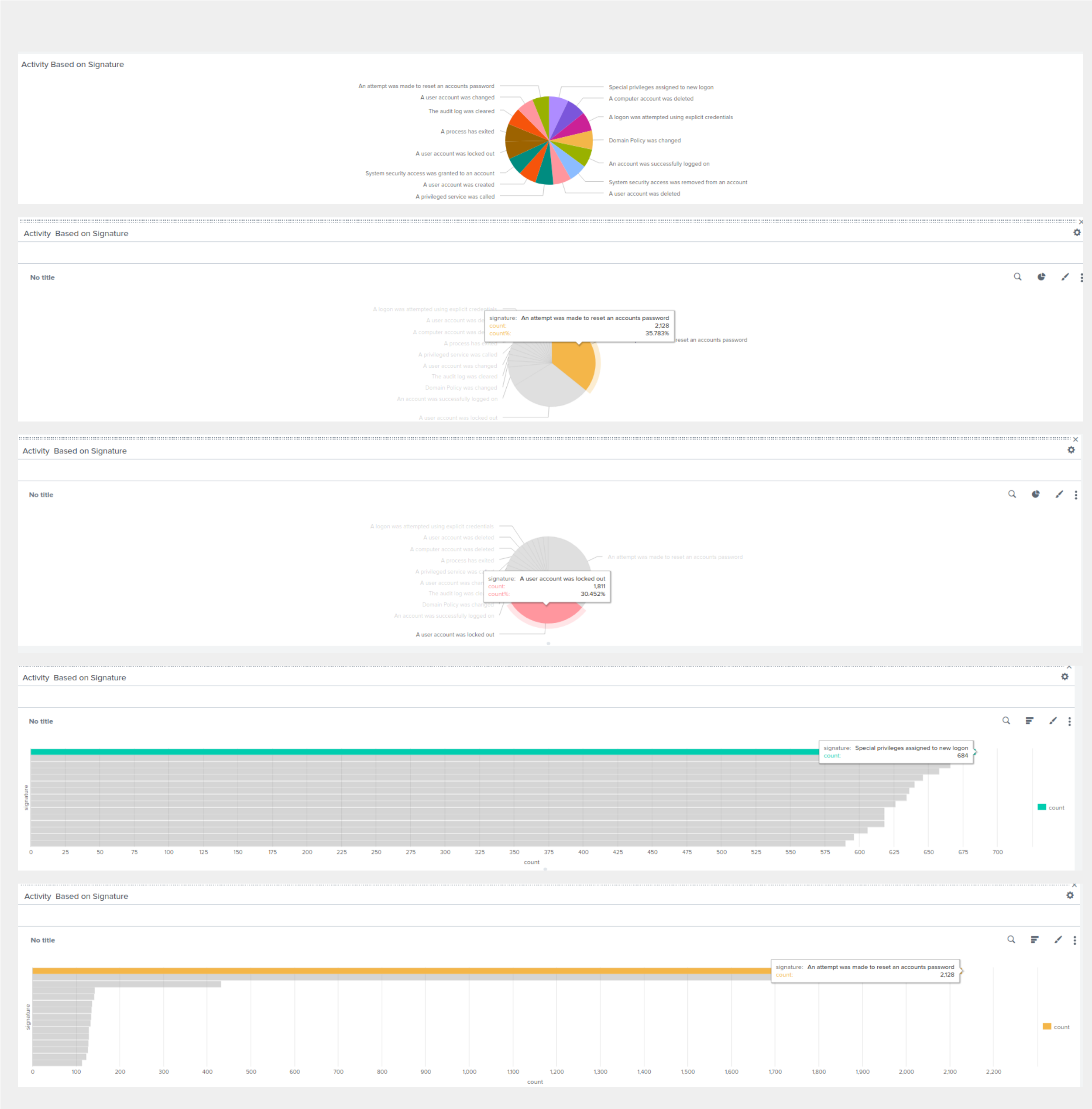
- What is the peak count of the different users?

```
  1. The “User_a” peak count is 785.
  2. The “User_k” peak count is 397.
```

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

- Does anything stand out as suspicious?

```
If you see the comparison between both the logs, two signatures are out as
suspicious due to their high counts.

“User was locked out”, “an attempt made to reset account password”.
```



Activity Based on Signature

An attempt was made to reset an accounts password
A user account was changed
The audit log was cleared
A process has exited
A user account was locked out
System security access was granted to an account
A user account was created
A privileged service was called
Special privileges assigned to new logon
A computer account was deleted
A logon was attempted using explicit credentials
Domain Policy was changed
An account was successfully logged on
System security access was removed from an account
A user account was deleted

Activity Based on Signature

No title

signature: An attempt was made to reset an accounts password
count: 2,128
count%: 35.783%

A logon was attempted using explicit credentials
A user account was de
A computer account was de
A process has exited
A privileged service was called
A user account was changed
The audit log was cleared
Domain Policy was changed
An account was successfully logged on
A user account was locked out
reset an accounts password

Activity Based on Signature

No title

signature: A user account was locked out
count: 1,811
count%: 30.452%

A logon was attempted using explicit credentials
A user account was deleted
A computer account was deleted
A process has exited
A privileged service was ca
A user account was chan
The audit log was cle
Domain Policy was changed
An account was successfully logged on
A user account was locked out
An attempt was made to reset an accounts password

Activity Based on Signature

No title

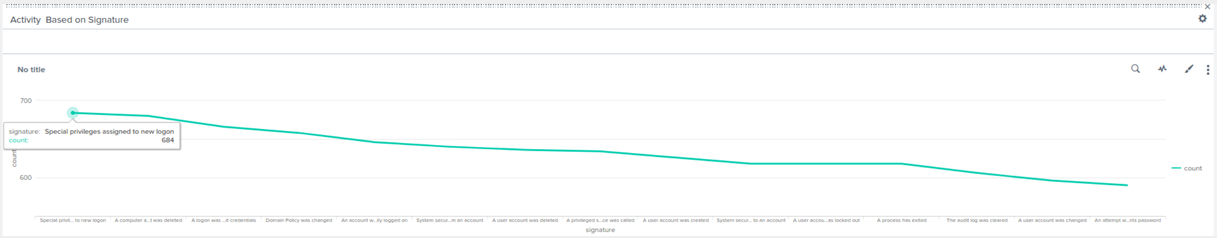
signature: Special privileges assigned to new logon
count: 684

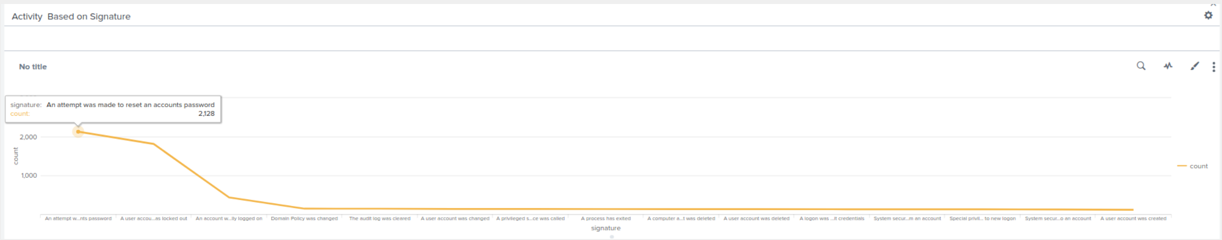
signature
0
25
50
75
100
125
150
175
200
225
250
275
300
325
350
375
400
425
450
475
500
525
550
575
600
625
650
675
700
count
count

Activity Based on Signature

No title

signature: An attempt was made to reset an accounts password
count: 2,128





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

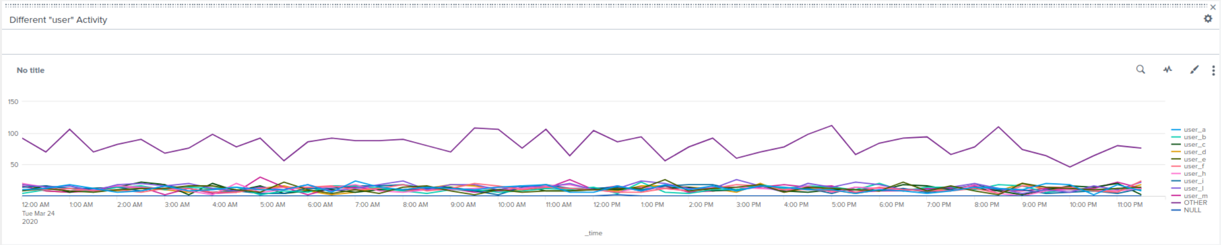
As a result of the count findings, it is apparent that this signature has also high counts in the timeline. Thus, the results of the bar chart appear to be in line with what has been observed on the time graph.

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

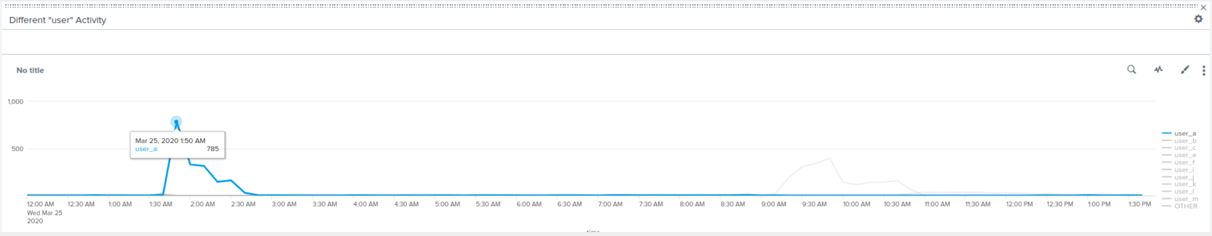
- Does anything stand out as suspicious?

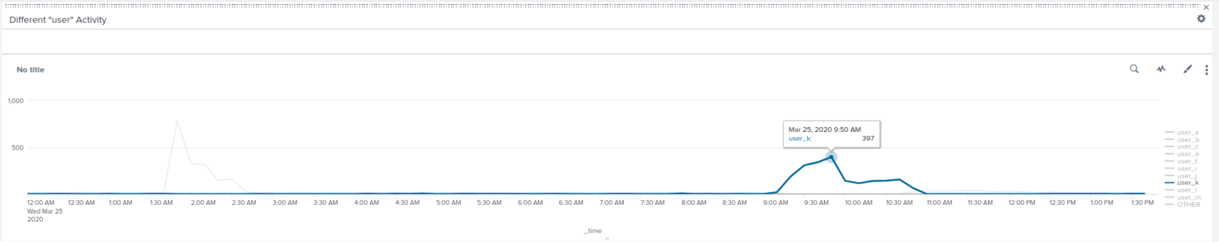
Yes, this chart change shows the activities that have been performed in response to the behavior of user_a and user_k user accounts that have been locked and attempted to change their password.

(Before the attack chart)

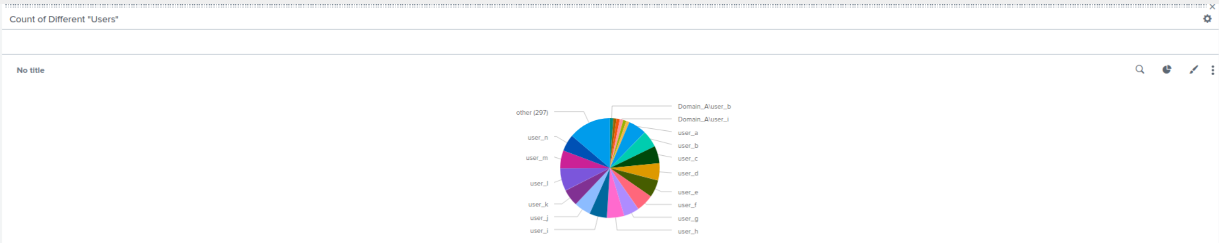


(After the attack chart)

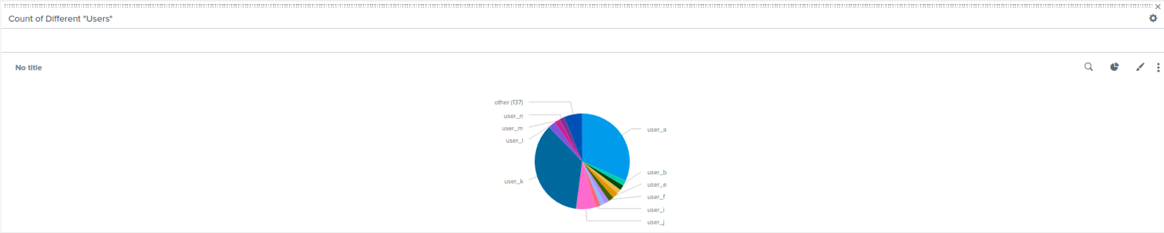




(Before the attack)



(After the attack)



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

The Comparison between the panel chart of the user's time chart and different user count does not match completely as we don’t have time chart in the different user chart panels but both the chart indicates the user “a” and user “k” has higher suspicious event count and possibly they are compromised.

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?

The advantages are as follows:

1. We can customize the reports to show specific information and create visualizations to make them easier to analyze.
2. We can save the report, allowing you to modify and improve it over time to gain different perspectives from your data.
3. These reports can be used to detect outliers, as they will be different from the standard statistical models.

The disadvantages are as follows:

1. Typically, reports are unstructured visualizations and lack the interactivity of some user panels. It is not possible to view the data in a real-time format or to drill down into detailed information.

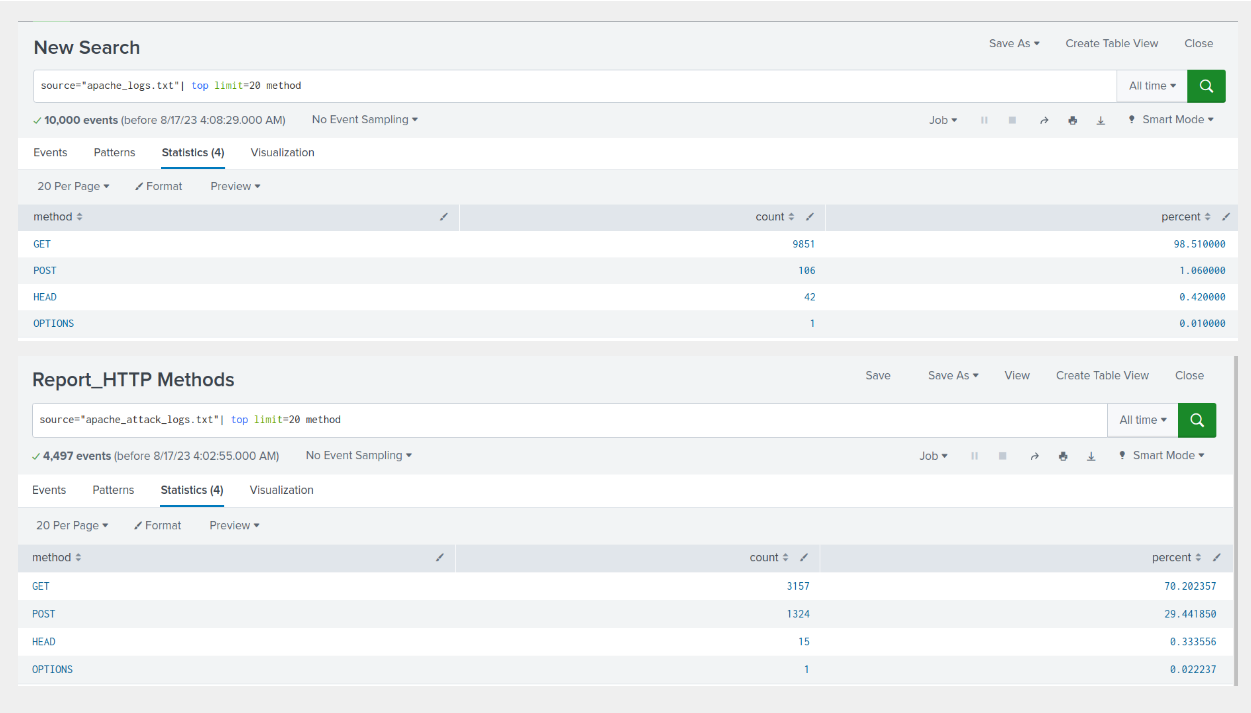
2. Most reports are based on data from the past. If you're looking for real-time info or close-to-real-time tracking, you might want to look at other user panels.
3. Having minimal technical knowledge, It is a hard time creating complicated reports. That's because you'll need to know a lot about Splunk and its search processing language and data model.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, the HTTP methods have been modified in a strange way. There have been substantial decreases in the number of GET requests, while the number of post requests increased dramatically after the attack.



```
source="apache_logs.txt"| top limit=20 method
```

✓ **10,000 events** (before 8/17/23 4:08:29.000 AM) No Event Sampling ▾

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

```
source="apache_attack_logs.txt"| top limit=20 method
```

✓ **4,497 events** (before 8/17/23 4:02:55.000 AM) No Event Sampling ▾

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 is a request method that is supported by HTTP. It is used to get data from a specific resource. It only retrieves the data from the server and does nothing else.

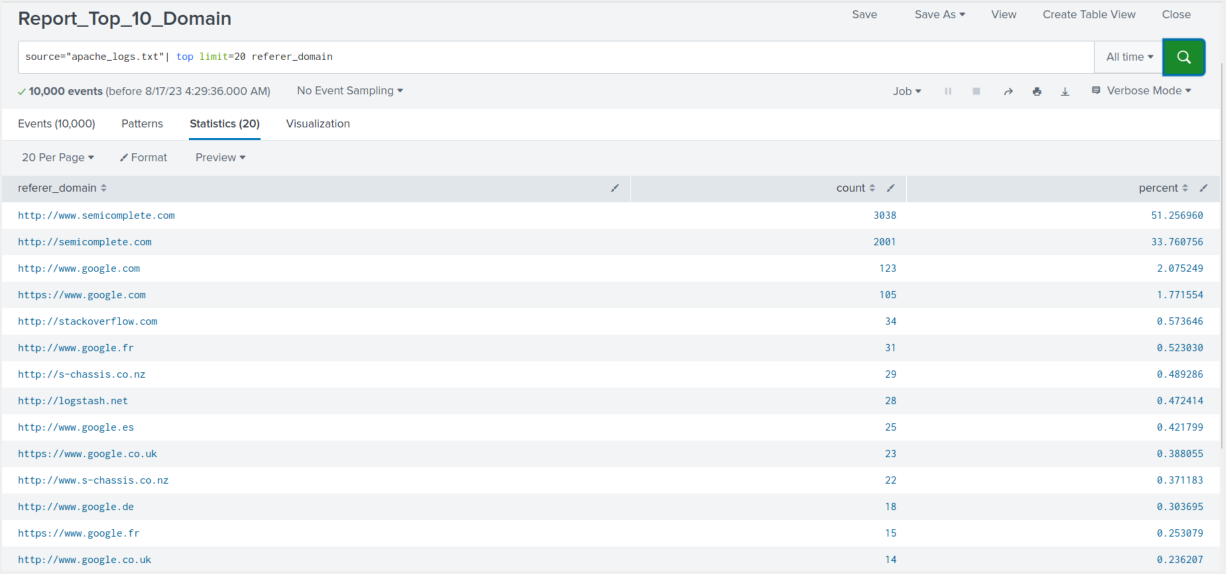
PUT is a request method supported by HTTP that sends data to the server for creating/updating resources. The data in the request body is included.

This can create a new resource or update an existing one, or both.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

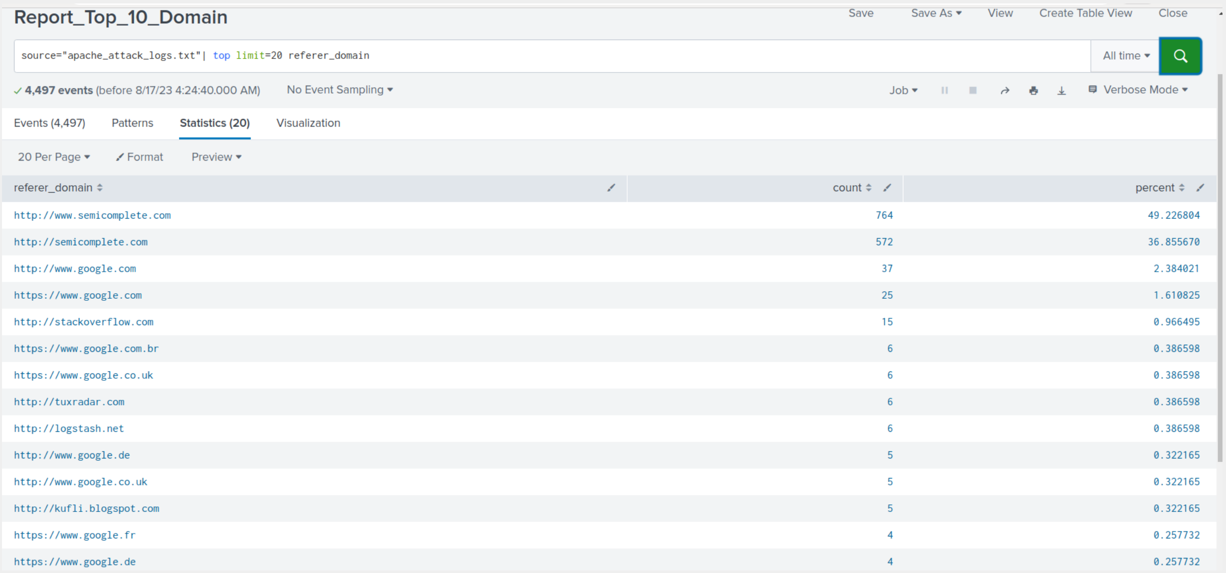
Yes, referrer domains are subject to suspicious changes. The share of the top referrers has changed. New referrer domains show up in attack logs. Counts for some referrers that were previously present have decreased significantly. These changes indicate a change in traffic origin or traffic type that may be associated with the attack.



```
source="apache_logs.txt"| top limit=20 referer_domain
```

✓ 10,000 events (before 8/17/23 4:29:36.000 AM) No Event Sampling ▾

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
http://www.s-chassis.co.nz	22	0.371183
http://www.google.de	18	0.303695
https://www.google.fr	15	0.253079
http://www.google.co.uk	14	0.236207



```
source="apache_attack_logs.txt"| top limit=20 referer_domain
```

✓ 4,497 events (before 8/17/23 4:24:40.000 AM) No Event Sampling ▾

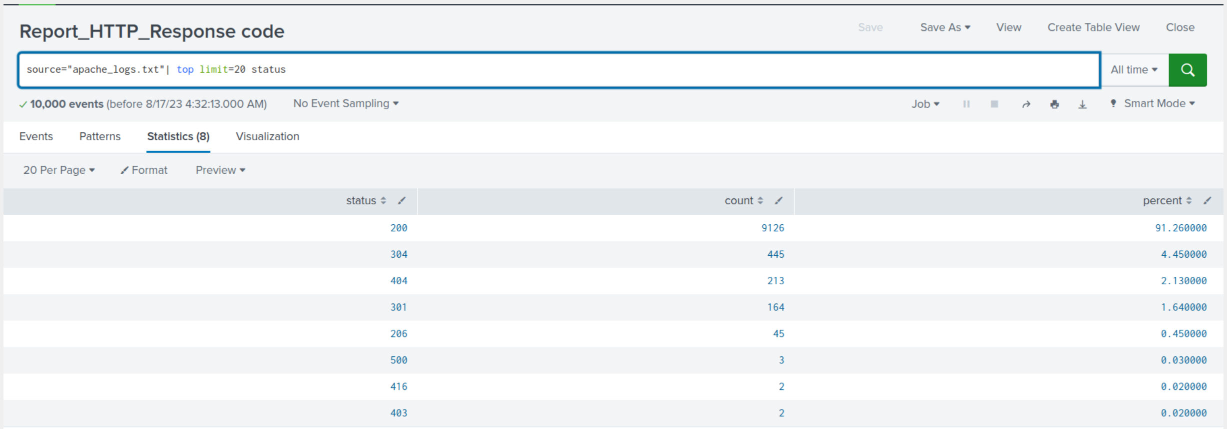
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165
http://www.google.co.uk	5	0.322165
http://kufli.blogspot.com	5	0.322165
https://www.google.fr	4	0.257732
https://www.google.de	4	0.257732

Report Analysis for HTTP Response Codes

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

```
Yes, there are some suspicious HTTP response codes. There is a significant
decrease in the number of 200 (normal) responses, while there is a dramatic
increase in 404 (not found) responses after the attack.
```

This could indicate that the attacker was requesting resources that don’t exist on the server. It’s possible that the attacker was trying to find vulnerabilities or misconfigurations.



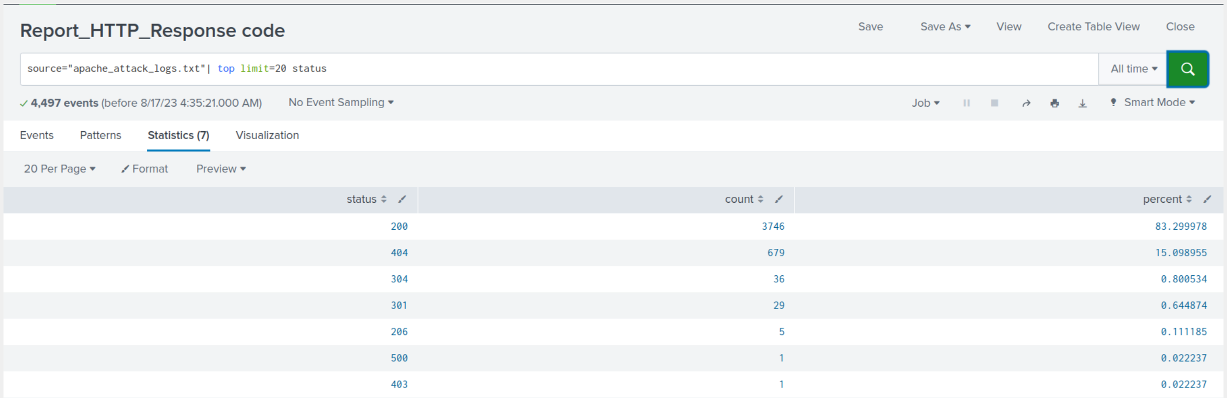
Report_HTTP_Response code

```
source="apache_logs.txt"| top limit=20 status
```

✓ 10,000 events (before 8/17/23 4:32:13.000 AM)   No Event Sampling

Statistics (8)

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



Report_HTTP_Response code

```
source="apache_attack_logs.txt"| top limit=20 status
```

✓ 4,497 events (before 8/17/23 4:35:21.000 AM)   No Event Sampling

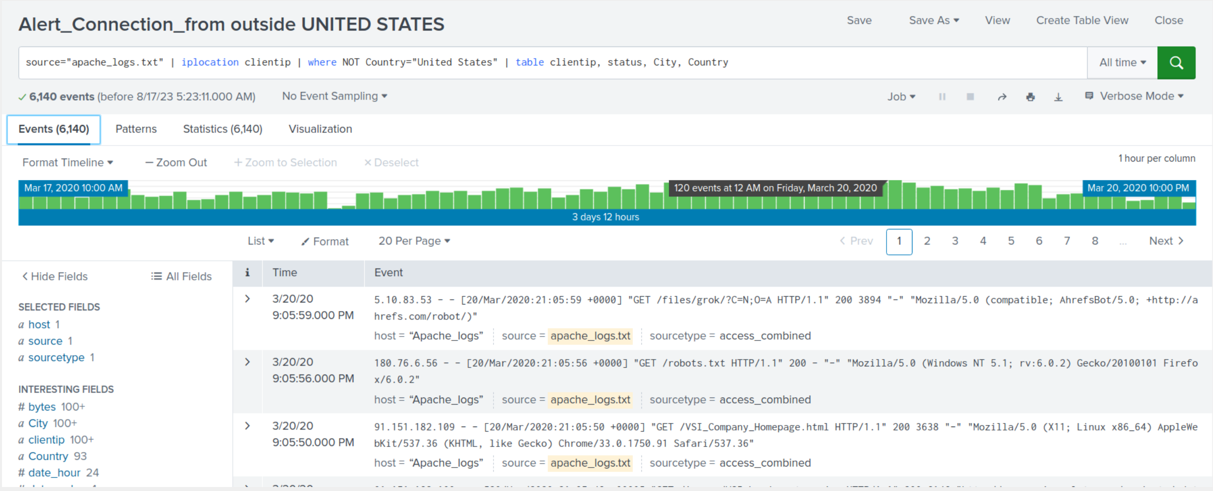
Statistics (7)

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, there is a high level of international activity. The number of occurrences is higher than at any other time in both normal and attack logs.



Alert_Connection_from outside UNITED STATES

```
source="apache_logs.txt" | iplocation clientip | where NOT Country="United States" | table clientip, status, City, Country
```

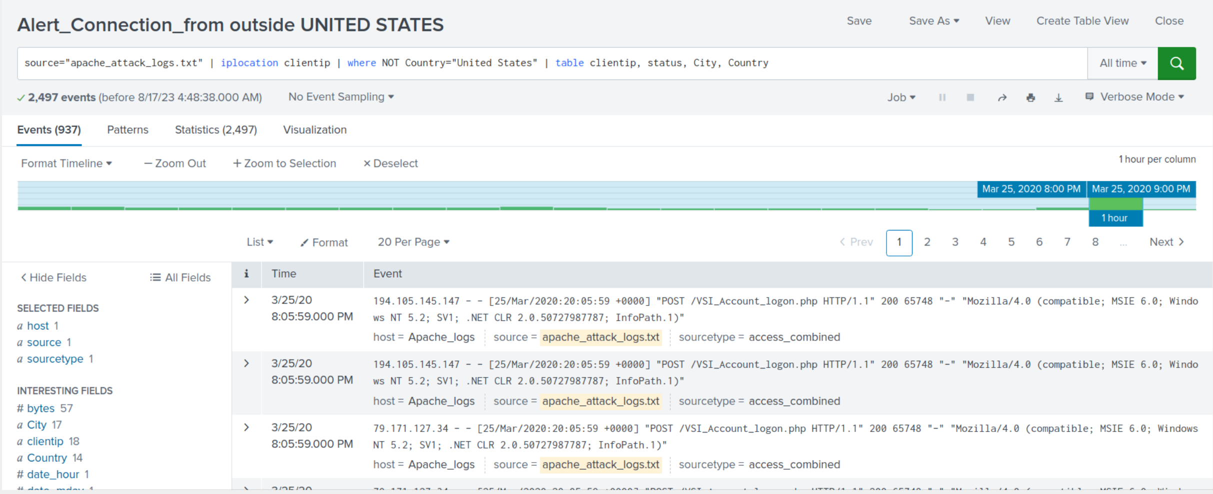
✓ 6,140 events (before 8/17/23 5:23:11.000 AM) No Event Sampling

Events (6,140) Statistics (6,140)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bytes 100+
a City 100+
a clientip 100+
a Country 93
# date_hour 24

Time	Event
3/20/20 9:05:59.000 PM	5.10.83.53 - - [20/Mar/2020:21:05:59 +0000] "GET /files/grok/?C=N;O=A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:56.000 PM	180.76.6.56 - - [20/Mar/2020:21:05:56 +0000] "GET /robots.txt HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:50.000 PM	91.151.182.109 - - [20/Mar/2020:21:05:50 +0000] "GET /VSI_Company_Homepage.html HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined



Alert_Connection_from outside UNITED STATES

```
source="apache_attack_logs.txt" | iplocation clientip | where NOT Country="United States" | table clientip, status, City, Country
```

✓ 2,497 events (before 8/17/23 4:48:38.000 AM) No Event Sampling

Events (937) Statistics (2,497)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bytes 57
a City 17
a clientip 18
a Country 14
# date_hour 1

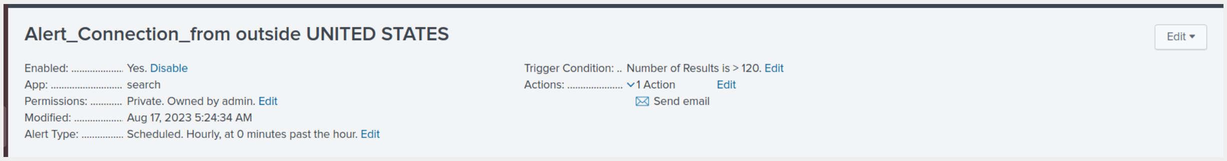
Time	Event
3/25/20 8:05:59.000 PM	194.105.145.147 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined
3/25/20 8:05:59.000 PM	194.105.145.147 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined
3/25/20 8:05:59.000 PM	79.171.127.34 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined

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

The count of the event was 937.

- Would your alert be triggered for this activity?

Yes, My alert would be triggered by this activity because the count of 937 is higher than my threshold of 120.



Alert_Connection_from outside UNITED STATES

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 17, 2023 5:24:34 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 120. Edit
Actions: .... 1 Action Edit
Send email

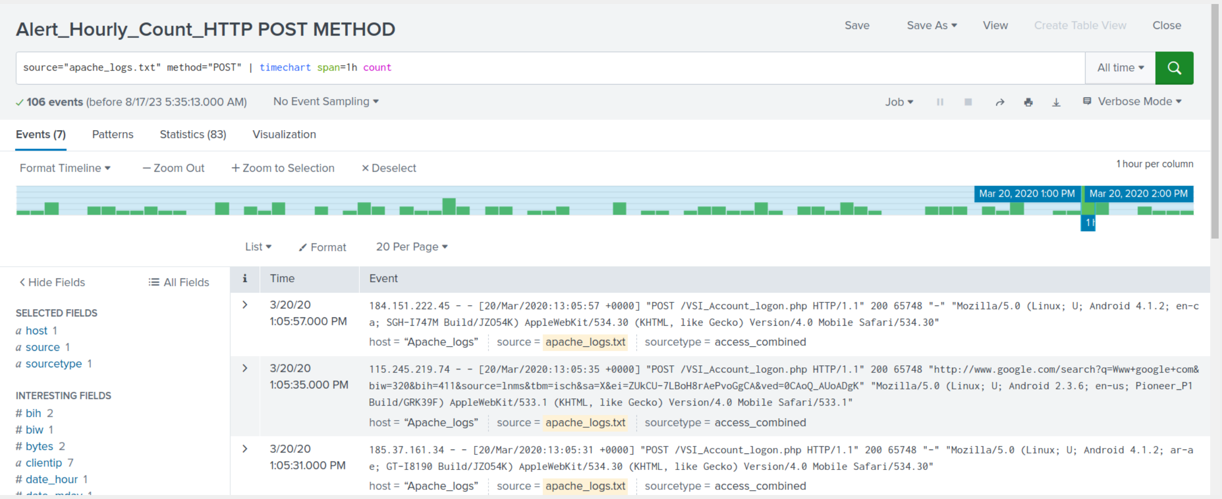
- After reviewing, would you change the threshold that you previously selected?

No, We would not change the threshold that we have selected because it successfully triggered the alert.

Alert Analysis for HTTP POST Activity

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

Yes, HTTP POST activity is suspicious. The number of HTTP POST requests at 8:00 p.m. on 25 March 2020 is higher than at any other time of day per hour.



Alert_Hourly_Count_HTTP POST METHOD

```
source="apache_logs.txt" method="POST" | timechart span=1h count
```

✓ 106 events (before 8/17/23 5:35:13.000 AM) No Event Sampling

Events (7) Patterns Statistics (83) Visualization

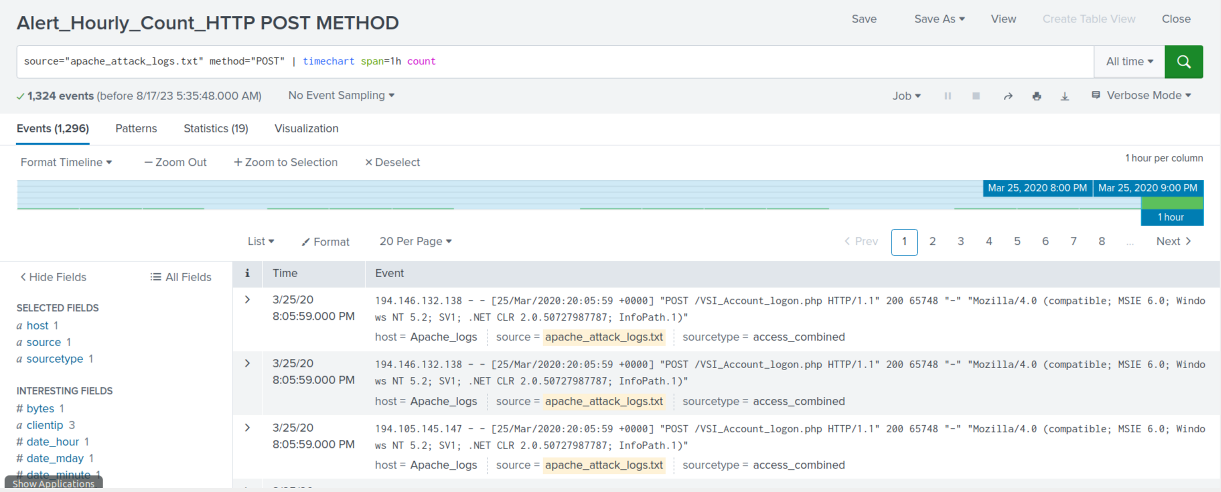
1 hour per column

Mar 20, 2020 1:00 PM | Mar 20, 2020 2:00 PM

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bih 2
# biw 1
# bytes 2
a clientip 7
# date_hour 1

Time	Event
3/20/20 1:05:57.000 PM	184.151.222.45 - - [20/Mar/2020:13:05:57 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-ca; SGH-I747M Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 1:05:35.000 PM	115.245.219.74 - - [20/Mar/2020:13:05:35 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "http://www.google.com/search?q=Www+google+com&biw=320&bih=411&source=lnms&tbm=isch&sa=X&ei=ZUkCU-7LBoH8rAePvoGgCA&ved=0CAoQ_AUoADgK" "Mozilla/5.0 (Linux; U; Android 2.3.6; en-us; Pioneer_P1 Build/GRK39F) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 1:05:31.000 PM	185.37.161.34 - - [20/Mar/2020:13:05:31 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/5.0 (Linux; U; Android 4.1.2; ar-ae; GT-I8190 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined



Alert_Hourly_Count_HTTP POST METHOD

```
source="apache_attack_logs.txt" method="POST" | timechart span=1h count
```

✓ 1,324 events (before 8/17/23 5:35:48.000 AM) No Event Sampling

Events (1,296) Patterns Statistics (19) Visualization

1 hour per column

Mar 25, 2020 8:00 PM | Mar 25, 2020 9:00 PM

1 hour

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bytes 1
a clientip 3
# date_hour 1
# date_mday 1
# date_minute 1

Time	Event
3/25/20 8:05:59.000 PM	194.146.132.138 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined
3/25/20 8:05:59.000 PM	194.146.132.138 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined
3/25/20 8:05:59.000 PM	194.105.145.147 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined

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

```
The count of events is 1296 per hour.
```

- When did it occur?

```
The suspicious volume of HTTP POST activity occurred at 8:00 PM
```

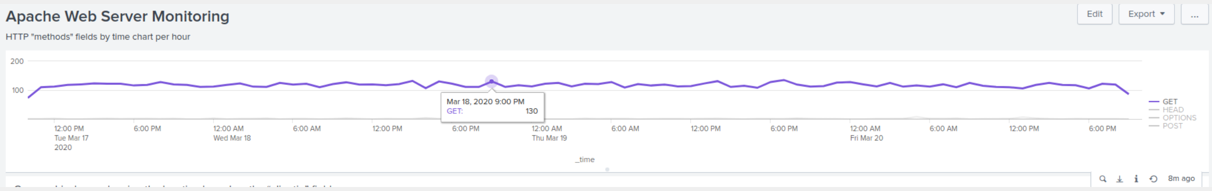
- After reviewing, would you change the threshold that you previously selected?

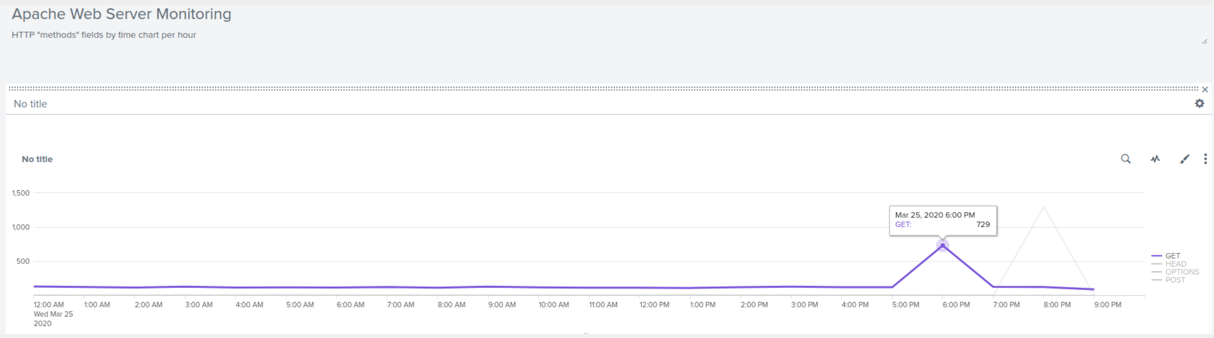
```
No, I would not change the threshold.
```

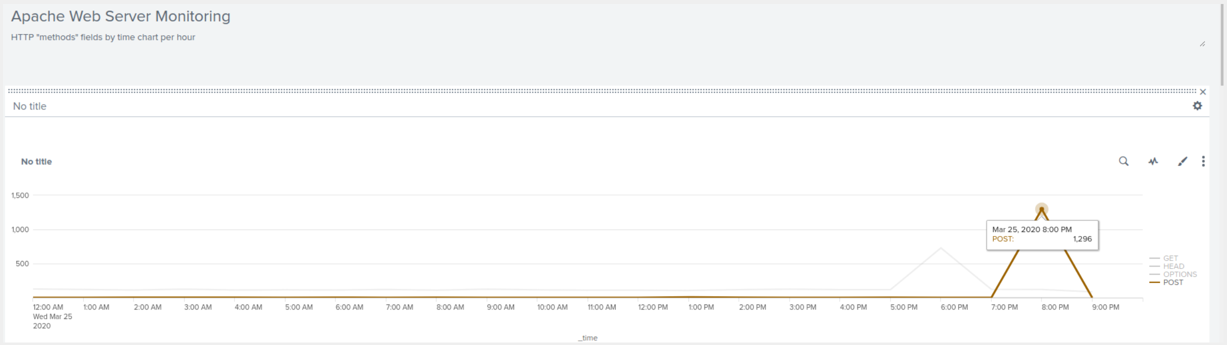
Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, the HTTP POST method is utilized significantly during the attack.
```







- Which method seems to be used in the attack?

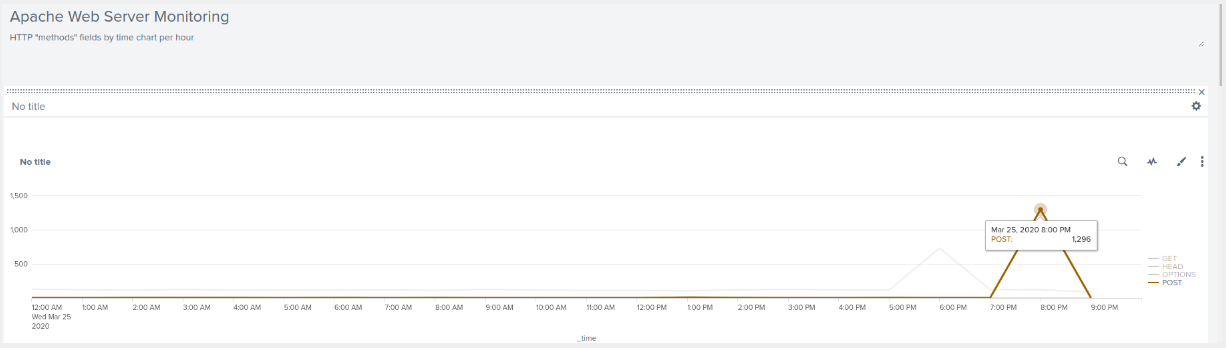
The HTTP POST method seems to be used in the attack.

- At what times did the attack start and stop?

The attack started at 7:00 PM and Stopped at 9:00 PM on March 25,2020

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

The peak count of the HTTP POST method during the attack is 1296 per hour.



Apache Web Server Monitoring

HTTP "methods" fields by time chart per hour

No title

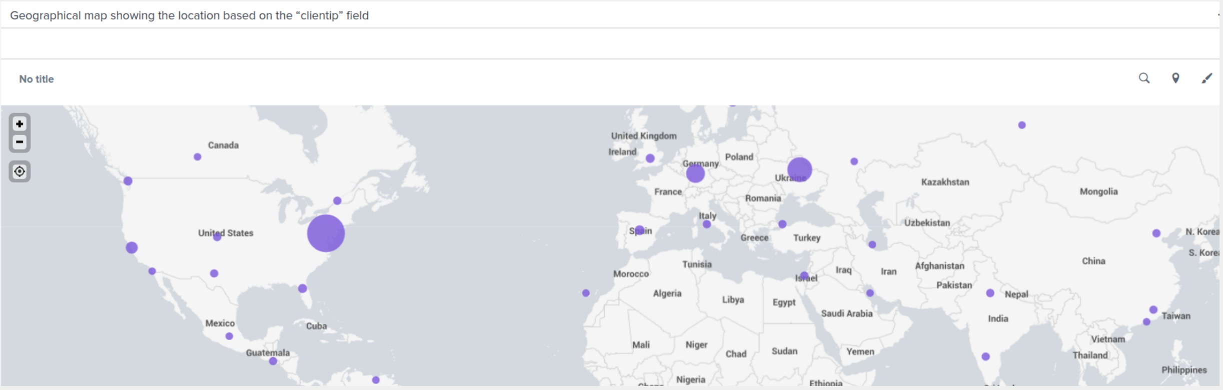
No title

Mar 25, 2020 8:00 PM
POST: 1,296

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

It is true that there is a significant amount of activity originating from Ukraine, as well as the United States, which is highly suspicious.



Geographical map showing the location based on the “clientip” field

No title

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

On the map, Ukraine and The United States has a high volume of activity.

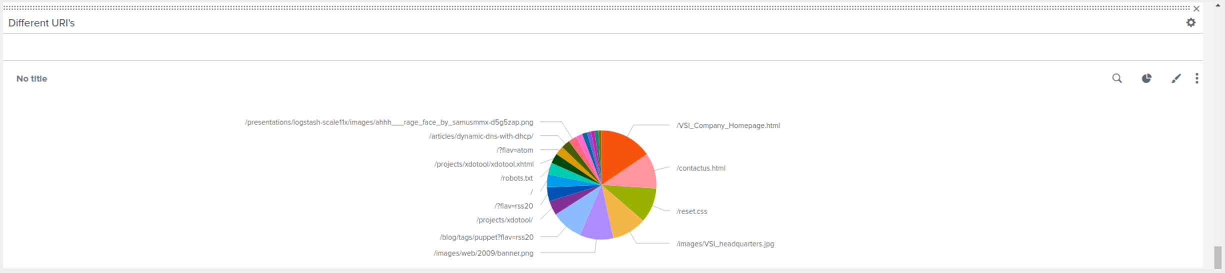
- What is the count of that city?

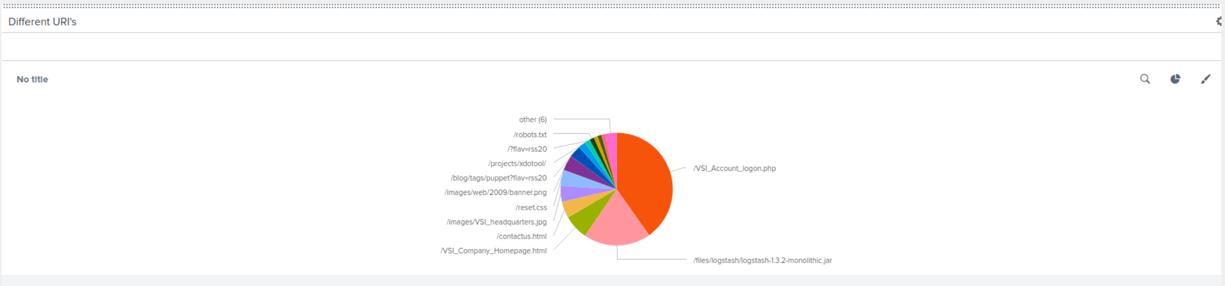
The count is 1296.

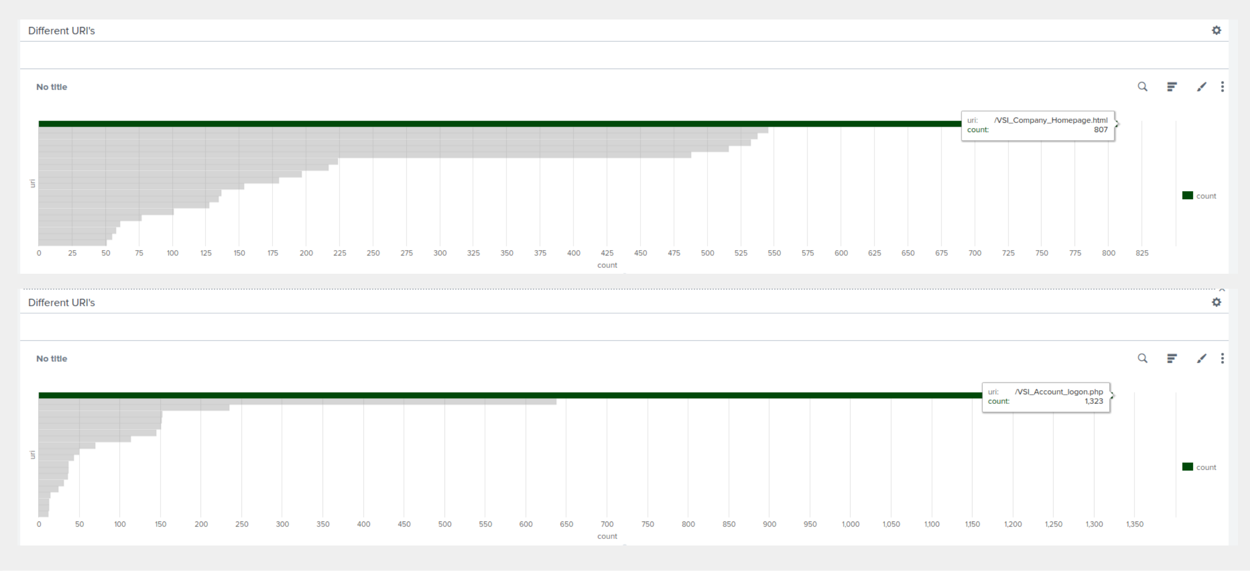
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yeah, the one that stands out is the VSI account logon.php, which has the most entries in the chart of the Apache attack logs.


Different URI's
No title
/presentations/logstash-scale11x/images/ahhh___rage_face_by_samusmmx-d5g5zap.png
/articles/dynamic-dns-with-dhcp/
/?flav=atom
/projects/xdotool/xdotool.xhtml
/robots.txt
/
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/VSI_Company_Homepage.html
/contactus.html
/reset.css
/images/VSI_headquarters.jpg


Different URI's
No title
other (6)
/robots.txt
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/reset.css
/images/VSI_headquarters.jpg
/contactus.html
/VSI_Company_Homepage.html
/VSI_Account_logon.php
/files/logstash/logstash-1.3.2-monolithic.jar



- What URI is hit the most?

```
The URI that is hit the most is “VSI_Account_logon.php”.
```

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

```
The VSI account logon.php indicates that the user is trying to log into the
account. A brute force attack is when the user tries to guess the user’s
password.

The high number of requests for a POST server indicates that the user wants
to send data to the server. A POST server typically sends data (such as a
password) to the server.
```