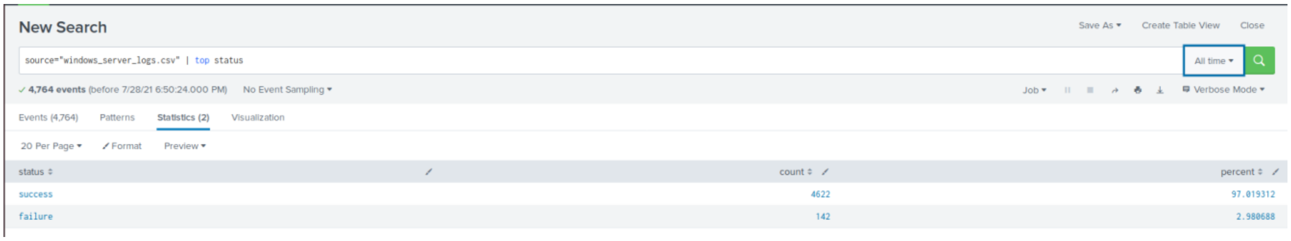
Solution Guide: Part 2 - Defend Your SOC

Windows Server Logs

Report Analysis for Severity

1. Did you detect any suspicious changes in severity?
    a. Yes. The percentages changed from:
        High: 7%
        Informational: 93%



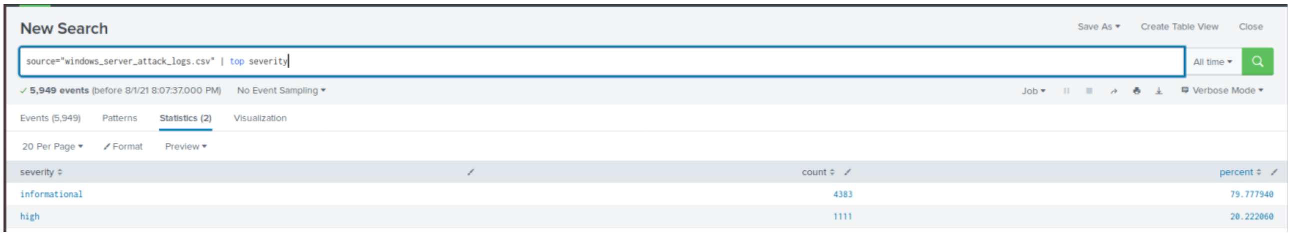
```
source="windows_server_logs.csv" | top status
```

✓ 4,764 events (before 7/28/21 6:50:24.000 PM)

status	count	percent
success	4622	97.019312
failure	142	2.980688

to:

High: 20%
Informational: 80%



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

✓ 5,949 events (before 8/1/21 8:07:37.000 PM)

severity	count	percent
informational	4383	79.777940
high	1111	20.222060

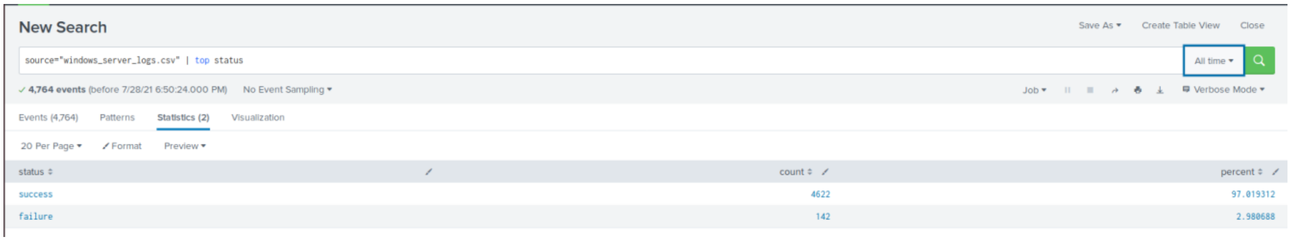
1. **This indicates an increase in the high severity cases.**

Report Analysis for Failed Activities

1. **Did you detect any suspicious changes in failed activities?**
   a. **Yes. The percentages changed from:**

      success: 97%

      failure: 3%



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

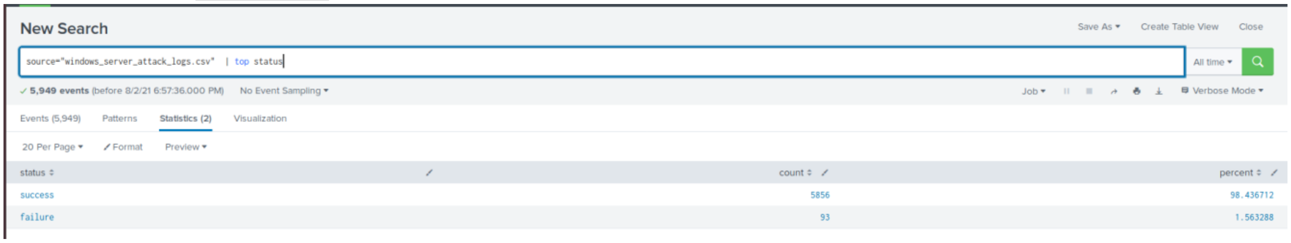
✓ 4,764 events (before 7/28/21 6:50:24.000 PM) No Event Sampling ▾

status	count	percent
success	4622	97.019312
failure	142	2.980688

to:

success: 98%

failure: 2%



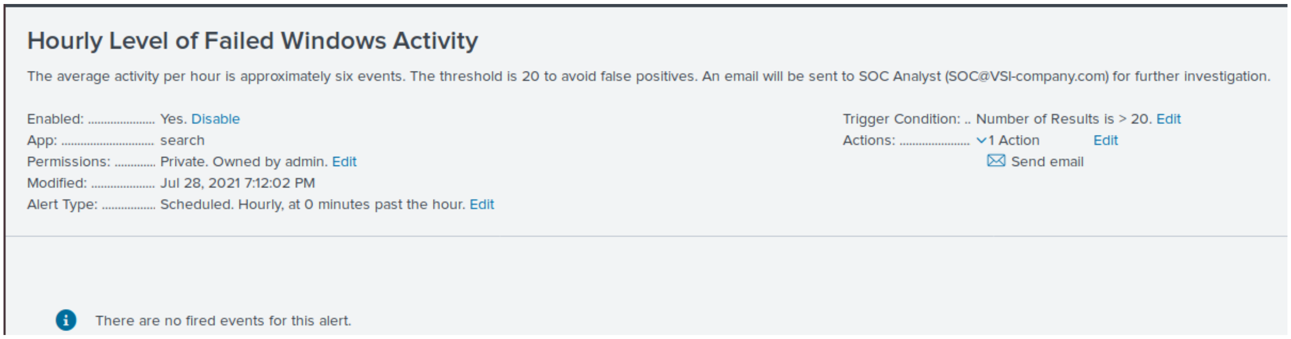
```
source="windows_server_attack_logs.csv"  | top status
```

✓ 5,949 events (before 8/2/21 6:57:36.000 PM) No Event Sampling ▾

status	count	percent
success	5856	98.436712
failure	93	1.563288

2. **This indicates that there is not a major change in the cumulative failure of events.**

Alert Analysis for Failed Windows Activity



Hourly Level of Failed Windows Activity

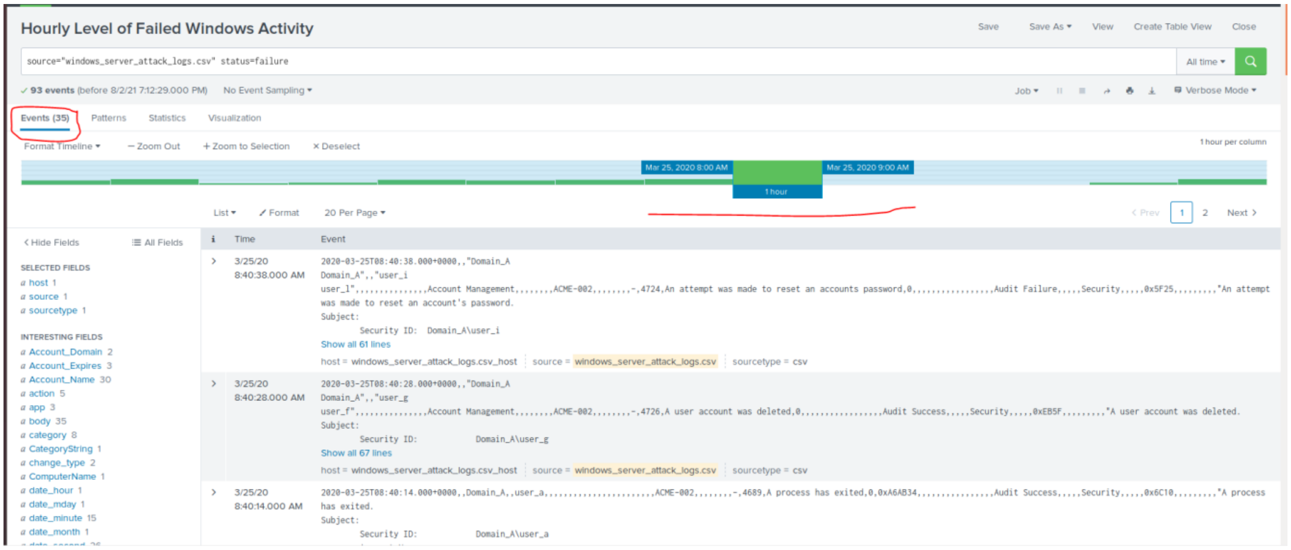
The average activity per hour is approximately six events. The threshold is 20 to avoid false positives. An email will be sent to SOC Analyst (SOC@VSI-company.com) for further investigation.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jul 28, 2021 7:12:02 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

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

ℹ There are no fired events for this alert.

1. **There is some potential suspicious activity for failed activity between 8 a.m. and 9 a.m. on Weds, March 25th.**



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

✓ 93 events (before 8/2/21 7:12:29.000 PM) No Event Sampling ▾

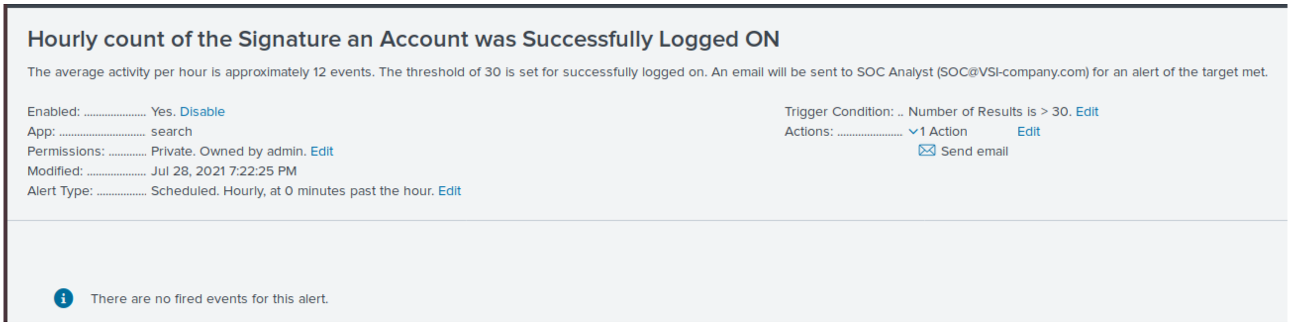
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2
a Account_Expires 3
a Account_Name 30
a action 5
a app 3
a body 35
a category 8
a CategoryString 1
a change_type 2
a ComputerName 1
a date_hour 1
a date_mday 1
a date_minute 15
a date_month 1

i	Time	Event
›	3/25/20 8:40:38.000 AM	2020-03-25T08:40:38.000+0000,,"Domain_A Domain_A",,"user_i user_1",,,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x5F25,,,,,,,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_i Show all 61 lines host = windows_server_attack_logs.csv_host source = windows_server_attack_logs.csv sourcetype = csv
›	3/25/20 8:40:28.000 AM	2020-03-25T08:40:28.000+0000,,"Domain_A Domain_A",,"user_g user_f",,,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xEB5F,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_g Show all 67 lines host = windows_server_attack_logs.csv_host source = windows_server_attack_logs.csv sourcetype = csv
›	3/25/20 8:40:14.000 AM	2020-03-25T08:40:14.000+0000,,Domain_A,,user_a,,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4689,A process has exited,0,0xA6AB34,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x6C10,,,,,,,,,"A process has exited. Subject: Security ID: Domain_A\user_a

2. **The count of activity is 35 events during this hour, A privileged service was called, where the user account was deleted, Domain Policies were changed, A user account was created, an attempt was made to reset an accounts password, and a computer account was deleted.**

Alert Analysis for Successful Logons



Hourly count of the Signature an Account was Successfully Logged ON

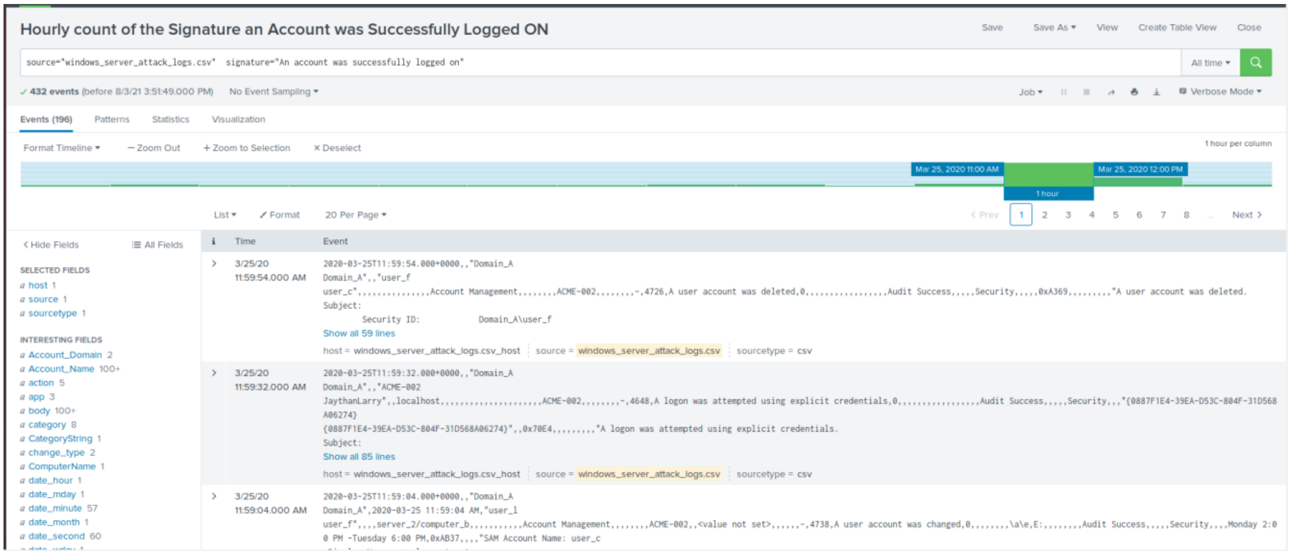
The average activity per hour is approximately 12 events. The threshold of 30 is set for successfully logged on. An email will be sent to SOC Analyst (SOC@VSI-company.com) for an alert of the target met.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jul 28, 2021 7:22:25 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 30. Edit
Actions: .... ∨1 Action Edit
✉ Send email

ℹ There are no fired events for this alert.

1. **There is some potential suspicious activity for successful logons activity between 11 a.m and 12 p.m. on Weds, March 25th.**



```
source="windows_server_attack_logs.csv"  signature="An account was successfully logged on"
```

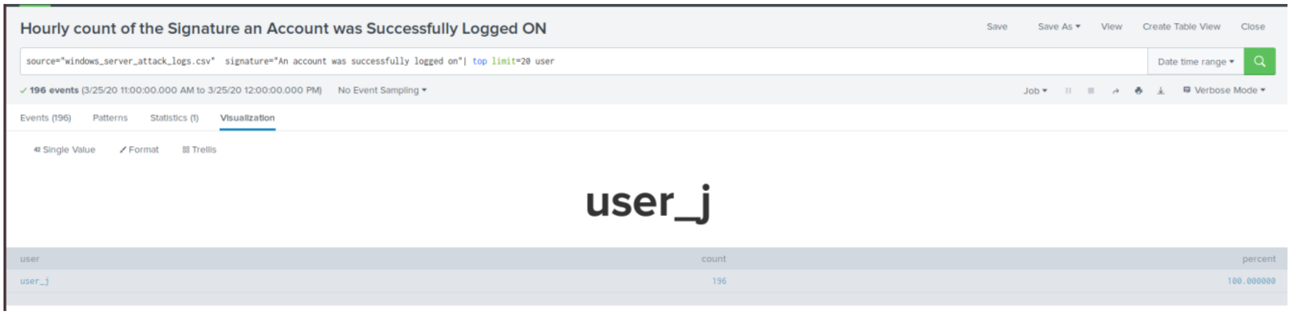
✓ 432 events (before 8/3/21 3:51:49.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2
a Account_Name 100+
a action 5
a app 3
a body 100+
a category 8
a CategoryString 1
a change_type 2
a ComputerName 1
a date_hour 1
a date_mday 1
a date_minute 57
a date_month 1
a date_second 60

```
i  Time                  Event
>  3/25/20               2020-03-25T11:59:54.000+0000,,"Domain_A
   11:59:54.000 AM       Domain_A",,"user_f
                         user_c",,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A user account was deleted.
                         Subject:
                                 Security ID:            Domain_A\user_f
                         Show all 59 lines
                         host = windows_server_attack_logs.csv_host | source = windows_server_attack_logs.csv | sourcetype = csv
>  3/25/20               2020-03-25T11:59:32.000+0000,,"Domain_A
   11:59:32.000 AM       Domain_A",,"ACME-002
                         JaythanLarry",,localhost,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4648,A logon was attempted using explicit credentials,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,"{0887F1E4-39EA-D53C-804F-31D568
                         A06274}
                         {0887F1E4-39EA-D53C-804F-31D568A06274}",,0x70E4,,,,,,,,,"A logon was attempted using explicit credentials.
                         Subject:
                         Show all 85 lines
                         host = windows_server_attack_logs.csv_host | source = windows_server_attack_logs.csv | sourcetype = csv
>  3/25/20               2020-03-25T11:59:04.000+0000,,"Domain_A
   11:59:04.000 AM       Domain_A",2020-03-25 11:59:04 AM,"user_l
                         user_f",,,,server_2/computer_b,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,<value not set>,,,,,,-,4738,A user account was changed,0,,,,,,,,\a\e,E:,,,,,,,,,Audit Success,,,,,Security,,,,Monday 2:0
                         0 PM -Tuesday 6:00 PM,0xAB37,,,,"SAM Account Name: user_c
```

2. **The count of activity is 196 between 11 a.m. and 12 p.m.**
3. **The primary user logging in is user j.**



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

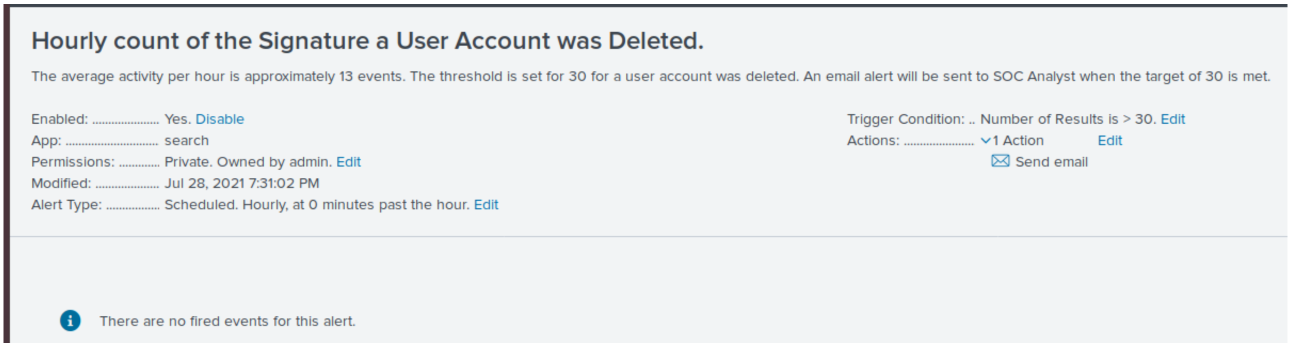
✓ 196 events (3/25/20 11:00:00.000 AM to 3/25/20 12:00:00.000 PM) No Event Sampling ▾

user	count	percent
user_j	196	100.000000

4. **Yes, it would have alerted the SOC Analyst of the suspicious logons.**
5. **No, it is set appropriately for the hourly settings, it would have also triggered an alert for the activity for the second hour from 12 p.m. to 1 p.m. on the same day.**

Alert Analysis for Deleted Accounts

Did you detect a suspicious volume of deleted accounts?



Hourly count of the Signature a User Account was Deleted.

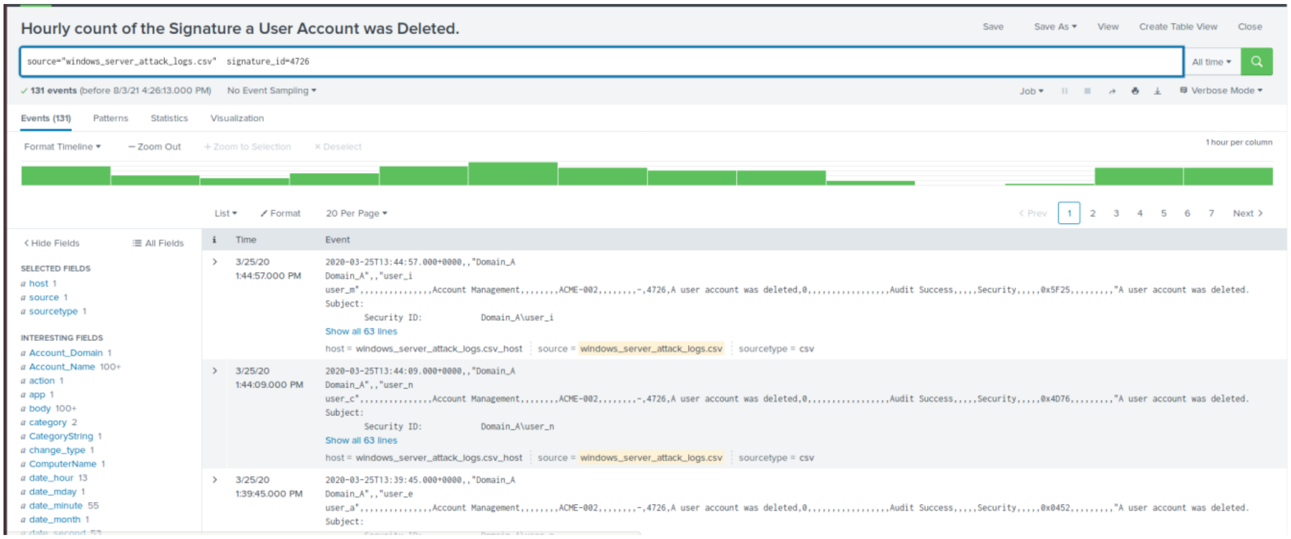
The average activity per hour is approximately 13 events. The threshold is set for 30 for a user account was deleted. An email alert will be sent to SOC Analyst when the target of 30 is met.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jul 28, 2021 7:31:02 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 30. Edit
Actions: .... 1 Action Edit
✉ Send email

There are no fired events for this alert.

1. **There was no suspicious activity of deleted accounts.**



Hourly count of the Signature a User Account was Deleted.

```
source="windows_server_attack_logs.csv"  signature_id=4726
```

✓ 131 events (before 8/3/21 4:26:13.000 PM)   No Event Sampling

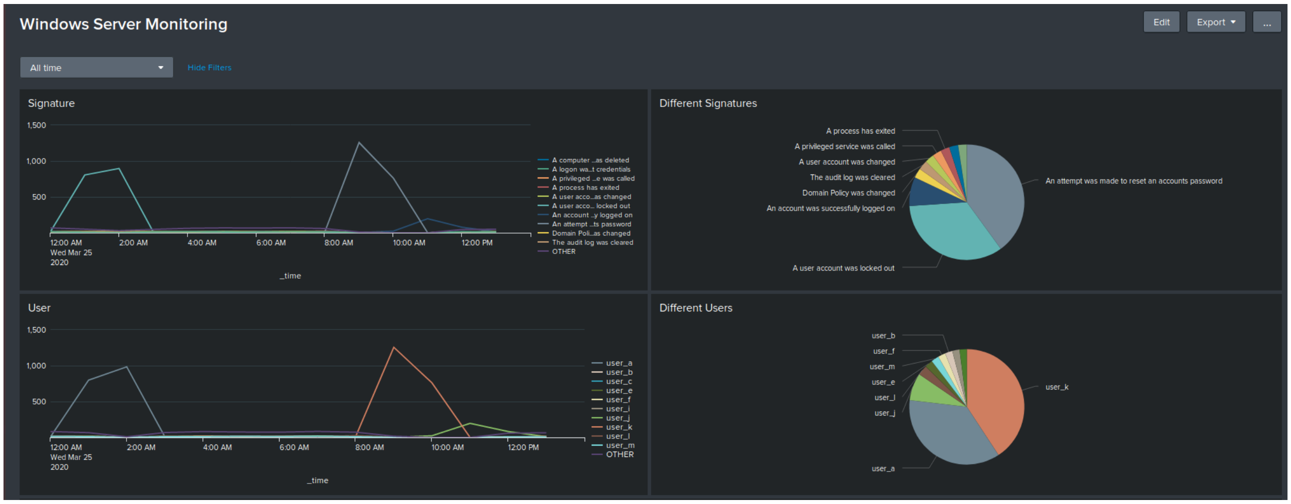
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 1
a Account_Name 100+
a action 1
a app 1
a body 100+
a category 2
a CategoryString 1
a change_type 1
a ComputerName 1
a date_hour 13
a date_mday 1
a date_minute 55
a date_month 1

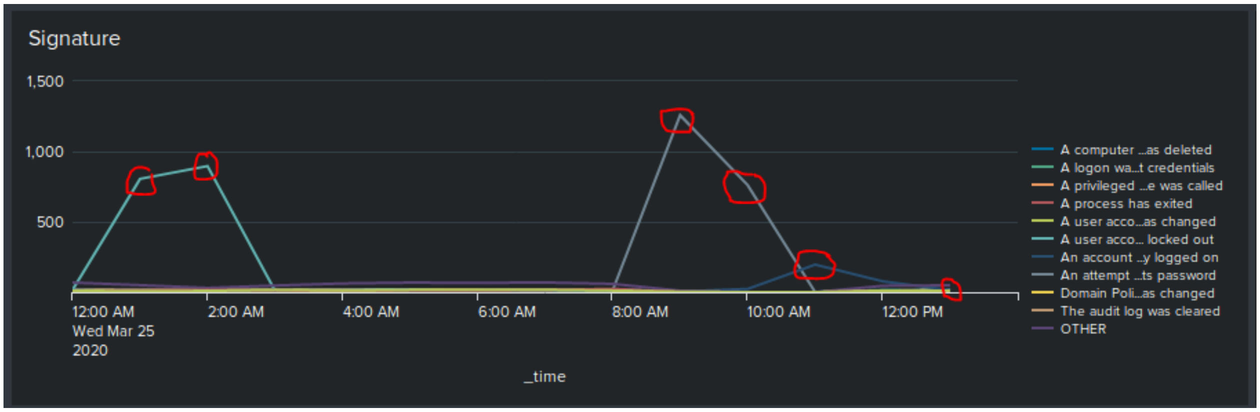
i	Time	Event
›	3/25/20 1:44:57.000 PM	2020-03-25T13:44:57.000+0000,,"Domain_A Domain_A",,"user_i user_m",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x5F25,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_i Show all 63 lines host = windows_server_attack_logs.csv_host source = windows_server_attack_logs.csv sourcetype = csv
›	3/25/20 1:44:09.000 PM	2020-03-25T13:44:09.000+0000,,"Domain_A Domain_A",,"user_n user_c",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x4D76,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_n Show all 63 lines host = windows_server_attack_logs.csv_host source = windows_server_attack_logs.csv sourcetype = csv
›	3/25/20 1:39:45.000 PM	2020-03-25T13:39:45.000+0000,,"Domain_A Domain_A",,"user_e user_a",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x0452,,,,,,,,,"A user account was deleted. Subject:

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious? What signatures stand out?
    1. **Yes, the signatures that have suspicious activity are: An attempt was made to reset a users password (39.955%), A user account was locked out (34.003%), and An account was successfully logged on (8.111%).**

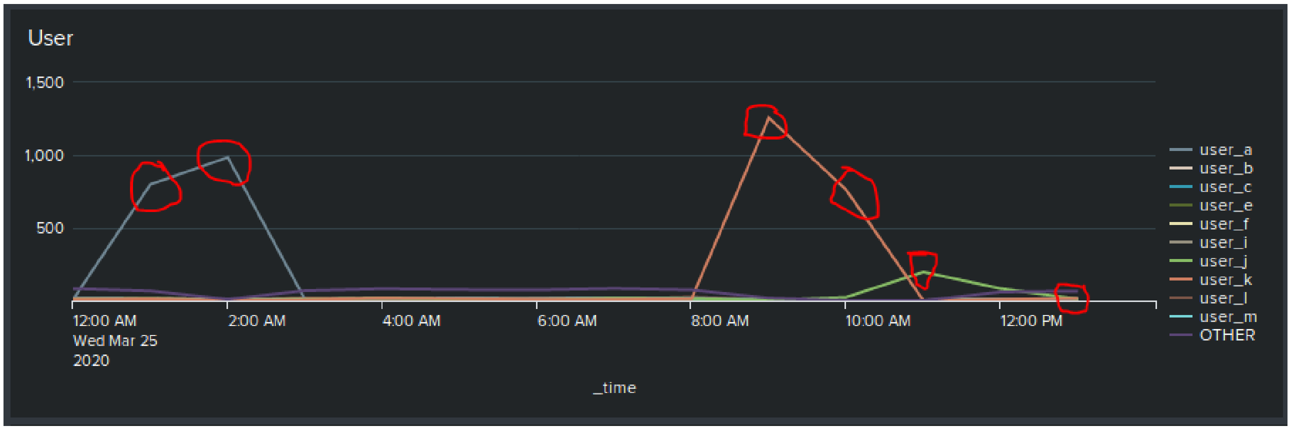


- What time did it start and stop for each signature? What is the peak count of the different signatures?
    2. **A user account was locked out: Started around 1 a.m. and ended at 3 a.m. on March 25th. The peak count was 896, and the total for the two hours was (805 + 896 = 1701).**
    3. **An attempt was made to reset a users password: Started around 9 a.m. and ended at 11 a.m. on March 25th. The peak count was 1,258, and the total for the two hours was (1258 + 761 = 2019)**
    4. **The account was successfully logged on: Started around 11 a.m. and ended at 1 p.m. on March 25th. The peak count was 196, and the total for the two hours was (196 + 77 = 273).**



Dashboard Analysis for Users

- Does anything stand out as suspicious? Which users stand out?
    1. **Yes, the users that have suspicious activity are users A, K, and J.**
- What time did it begin and stop for each user? What is the peak count of the different user?
    2. **User A: Started around 1 a.m. and ended at 3 a.m. on March 25th. Peak count was 984, and the total for the two hours was (799 + 984 = 1783).**
    3. **User K: Started around 9 a.m. and ended at 11 AM on March 25th. Peak count was 1,256, and the total for the two hours was (1256 + 761 = 2017).**
    4. **User J: Started around 11 a.m. and ended at 1 p.m. on March 25th. Peak count was 196, and the total for the two hours was (196 + 82 = 278).**



Dashboard Analysis for Signatures with Bar, Graph, Pie Charts

1. **All Charts are showing the same information as above for the Signatures.**

Dashboard Analysis for Users with Bar, Graph, Pie Charts

1. **All Charts are showing the same information as above for the Users.**

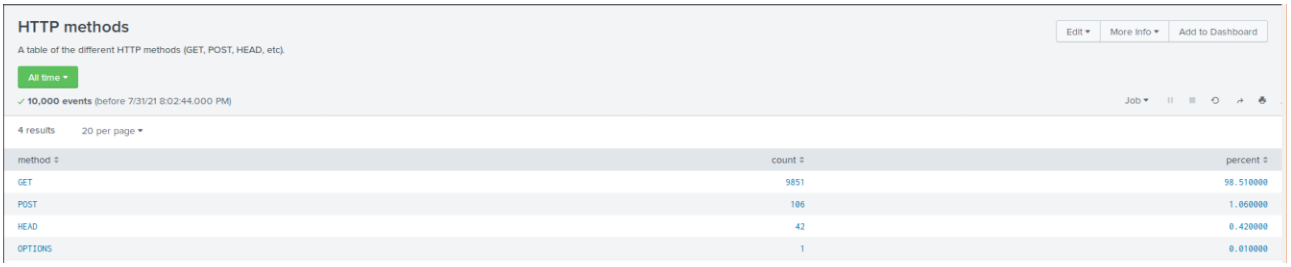
Dashboard Analysis for Users with Statistical Chart

- What would be the advantage/disadvantage of using this report, compared to the other user panels you created?
    - **There is only one advantage of the stats chart, as it will only give the total count of the users activity or the percentage of the activity. However, the disadvantage of the stats chart compared to a chart will show a cumulative perspective, while a time chart shows the suspicious activity over a more specific, and shorter time frame.**

Apache WebServer Logs

Report Analysis for Methods

1. Did you detect any suspicious changes in HTTP methods? If so, which one?
    - **Yes, a suspicious change in the HTTP POST method was raised from 1% to 29%.**



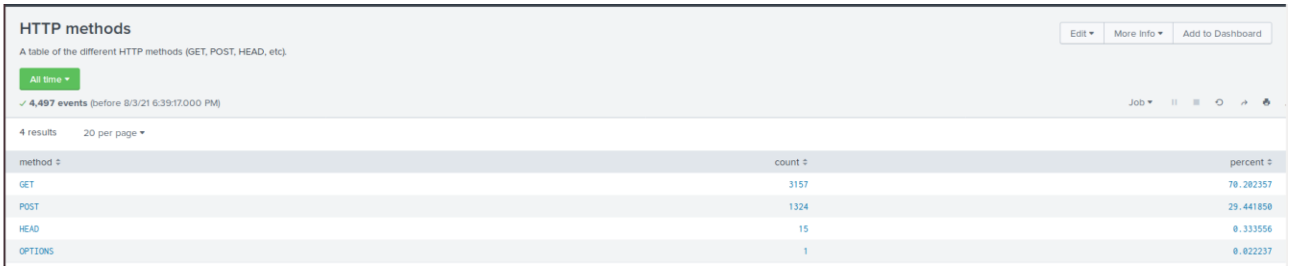
HTTP methods

A table of the different HTTP methods (GET, POST, HEAD, etc).

✓ **10,000 events** (before 7/31/21 8:02:44.000 PM)

4 results 20 per page ▾

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



HTTP methods

A table of the different HTTP methods (GET, POST, HEAD, etc).

✓ **4,497 events** (before 8/3/21 6:39:17.000 PM)

4 results 20 per page ▾

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

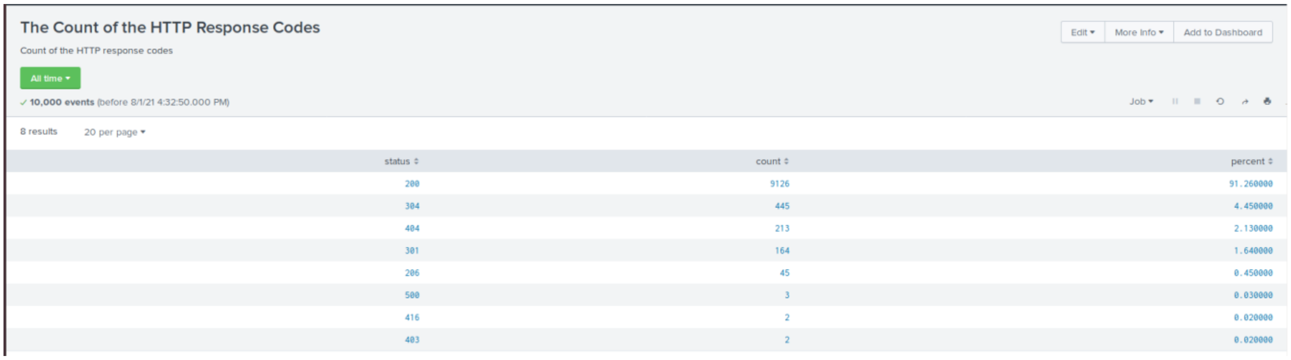
2. What is that method used for?
    - **POST is used to submit or update information to a web server.**

Report Analysis for Referrer Domains

1. Did you detect any suspicious changes in referrer domains?
    - **There were no major suspicious referrers during the attack. Only minor changes to the first two domains by a couple of percentages.**

Report Analysis for HTTP Response Codes

1. Did you detect any suspicious changes in HTTP response codes?
   - **There are several small changes, but the most prominent is the 404 response code, which increased from 2% to 15%. The 200 response code went down from 91% to 83%.**



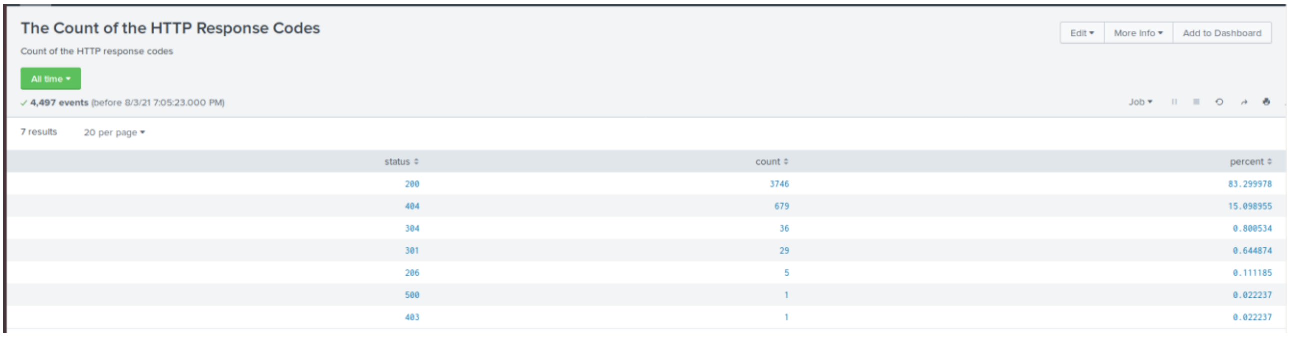
The Count of the HTTP Response Codes

Count of the HTTP response codes

✓ **10,000 events** (before 8/1/21 4:32:50.000 PM)

8 results

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



The Count of the HTTP Response Codes

Count of the HTTP response codes

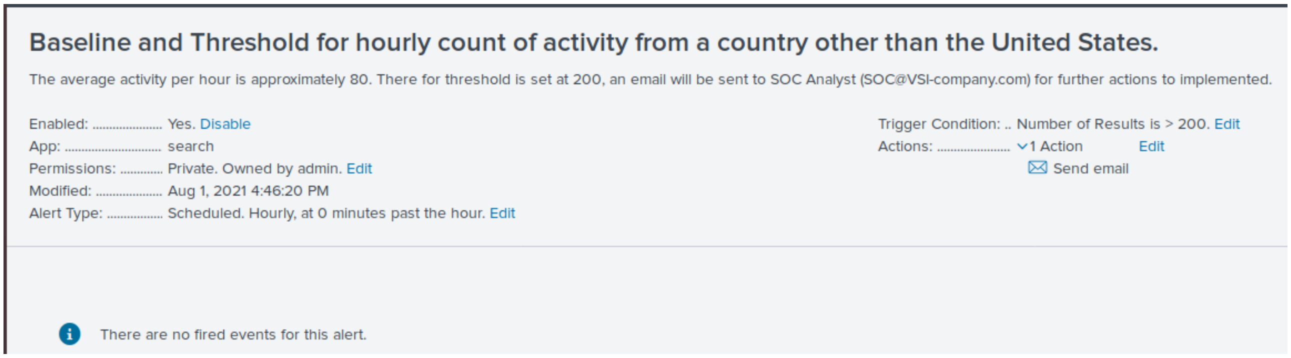
✓ **4,497 events** (before 8/3/21 7:05:23.000 PM)

7 results

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

1. Did you detect any suspicious volume of international activity? If so, what was the count of the hour it occurred in?
    - **There was activity in Ukraine between 8 p.m. and 9 p.m. on Weds, March 25th, and had a count of 935 events.**
    - **Yes, as the threshold was set at 200, so this activity would be triggered as part of the alert.**
    - **No, as it's above the activity set threshold.**



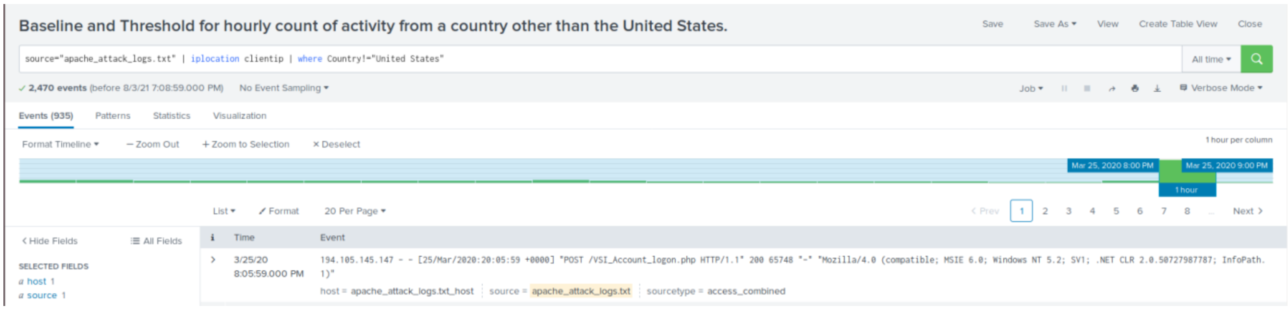
Baseline and Threshold for hourly count of activity from a country other than the United States.

The average activity per hour is approximately 80. There for threshold is set at 200, an email will be sent to SOC Analyst (SOC@VSI-company.com) for further actions to implemented.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 1, 2021 4:46:20 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 200. Edit
Actions: .... 1 Action Edit
✉ Send email

There are no fired events for this alert.



Baseline and Threshold for hourly count of activity from a country other than the United States.

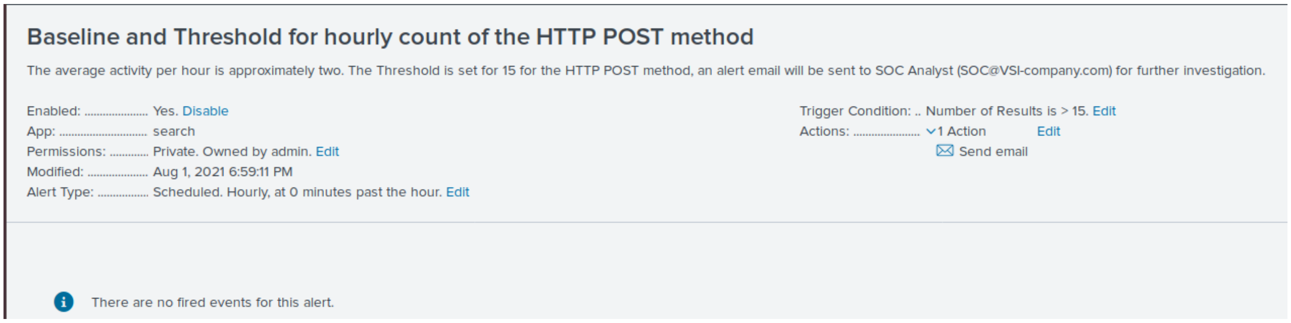
```
source="apache_attack_logs.txt" | iplocation clientip | where Country!="United States"
```

✓ 2,470 events (before 8/3/21 7:08:59.000 PM) No Event Sampling ▾

i	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_attack_logs.txt_host source = apache_attack_logs.txt sourcetype = access_combined

Alert Analysis for HTTP POST Activity

1. Did you detect any suspicious volume of HTTP POST activity? If so, what was the count of the hour it occurred in and when did it occur?
   - **There was a spike in POST method activity between 8 p.m. and 9 p.m. on Weds, March 25th, and had a count of 1,296 events.**
   - **No, the threshold set is at 15 counts, this would have been triggered.**



Baseline and Threshold for hourly count of the HTTP POST method

The average activity per hour is approximately two. The Threshold is set for 15 for the HTTP POST method, an alert email will be sent to SOC Analyst (SOC@VSI-company.com) for further investigation.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 1, 2021 6:59:11 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... 1 Action Edit
✉ Send email

There are no fired events for this alert.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?
  - **Yes, there were suspicious activities of the POST and GET method.**
- What was the method that seems to be used in the attack? What time did it begin and end, and what was the peak count?
  - **The POST method was used, starting at 8 p.m. and ending at 9 p.m. The peak count was 1,296.**
  - **THE GET method was used, starting at 6 p.m. and ending at 7 p.m. The peak count was 729.**

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious? What new country, city on the map has a high volume of activity?
  - **Yes, there is suspicious activity in Ukraine.**
- What is the count of that country, city?
  - **When zoomed in, we can see the cities in Ukraine are:**
    - **Kiev: Count of 439**
    - **Kharkiv: Count of 433**
    - **Lvov: 5**

Dashboard Analysis for URI Data

- Does anything stand out as suspicious? What URI is being hit the most?
  - **Yes, there is suspicious activity against the main VSI logon page: /VSI_Account_logon.php (count of 1323).**
- Based on the URI being accessed, what could the attacker potentially be doing?
  - **The attacker may be trying to brute force the VSI logon page.**