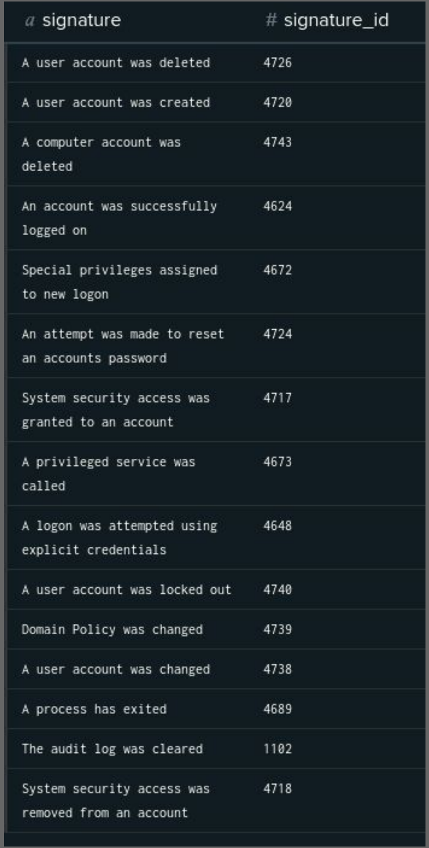
Project 3: Building a Sec Monitoring Env

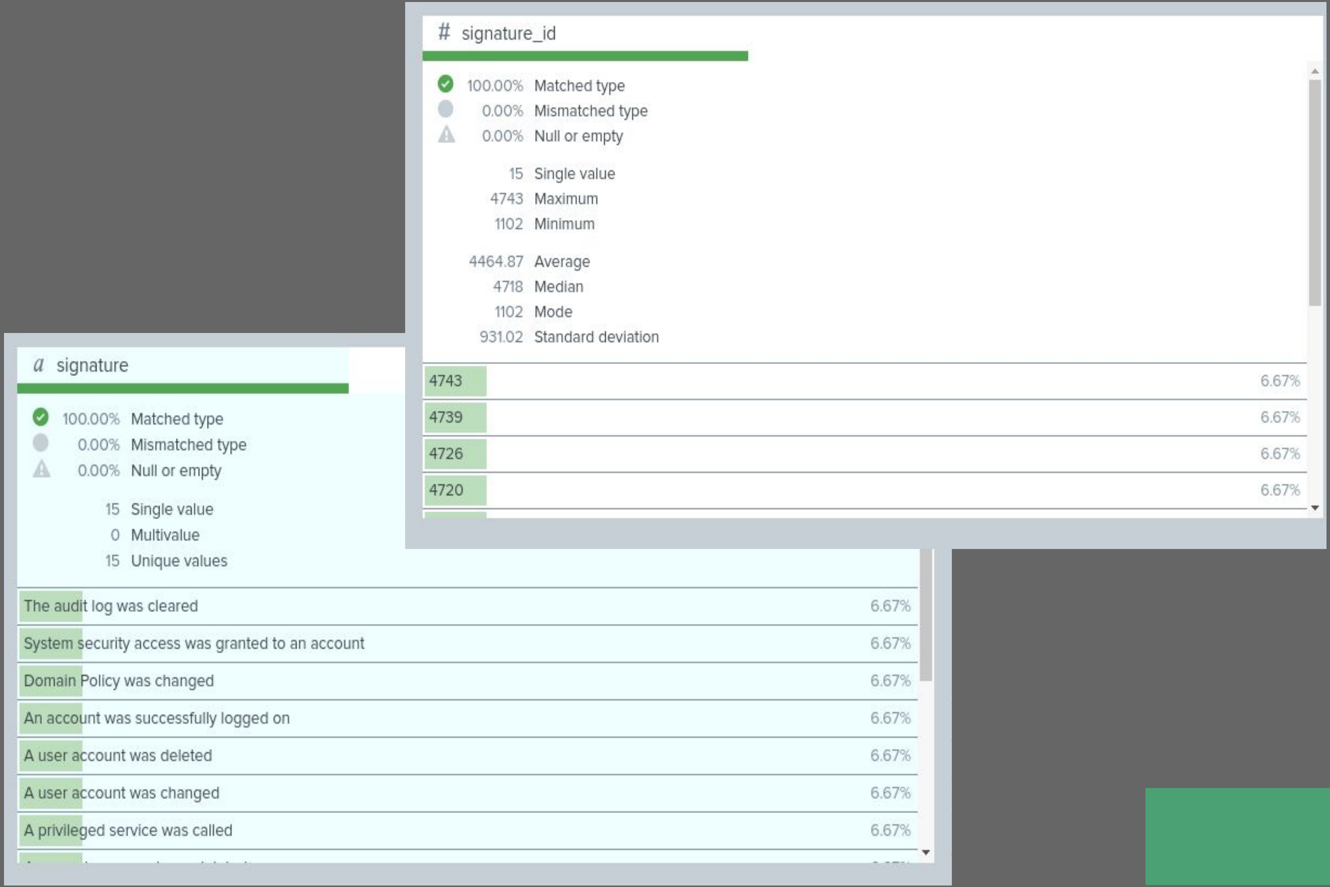
BY: Chase Hancock

Day 1: Designing The Defensive Solution

Part 1: Window Reports



a signature	# signature_id
A user account was deleted	4726
A user account was created	4720
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724
System security access was granted to an account	4717
A privileged service was called	4673
A logon was attempted using explicit credentials	4648
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A process has exited	4689
The audit log was cleared	1102
System security access was removed from an account	4718



signature_id

```
✓ 100.00%  Matched type
●   0.00%  Mismatched type
⚠   0.00%  Null or empty

       15  Single value
     4743  Maximum
     1102  Minimum

  4464.87  Average
     4718  Median
     1102  Mode
   931.02  Standard deviation
```

4743	6.67%
4739	6.67%
4726	6.67%
4720	6.67%

a signature

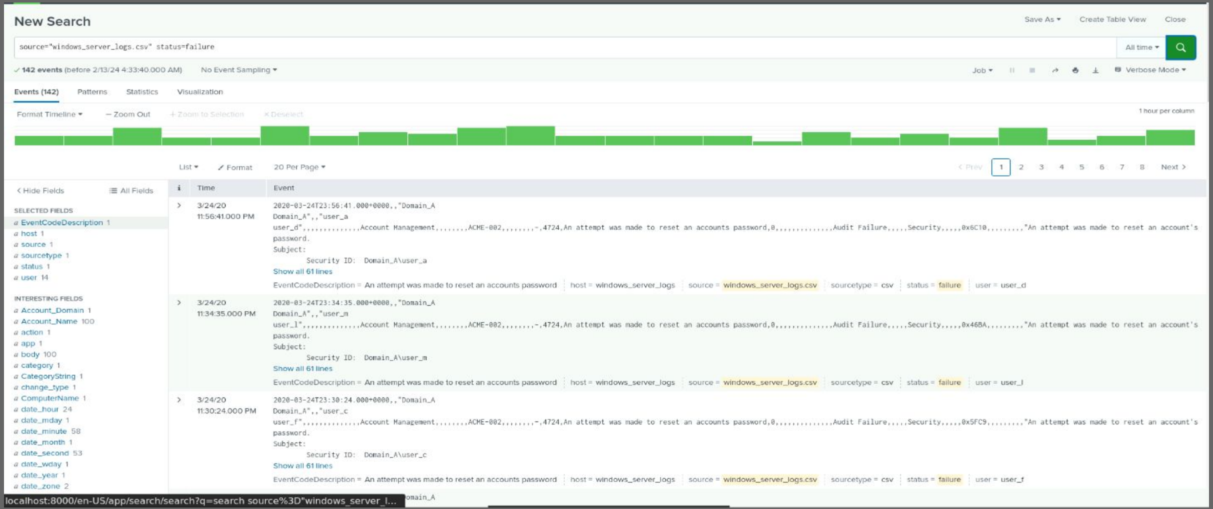
```
✓ 100.00%  Matched type
●   0.00%  Mismatched type
⚠   0.00%  Null or empty

       15  Single value
        0  Multivalue
       15  Unique values
```

The audit log was cleared	6.67%
System security access was granted to an account	6.67%
Domain Policy was changed	6.67%
An account was successfully logged on	6.67%
A user account was deleted	6.67%
A user account was changed	6.67%
A privileged service was called	6.67%

Day 1: Designing The Defensive Solution

Part 2: Windows_server Alert #1 Failed Windows Activity



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

✓ 142 events (before 2/13/24 4:33:40.000 AM)

SELECTED FIELDS

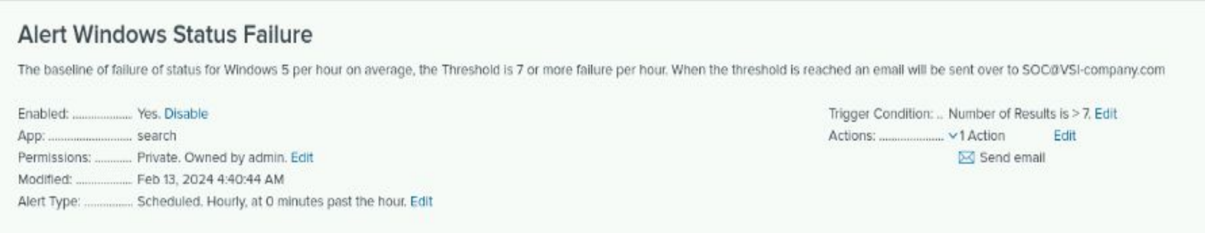
a EventCodeDescription	1
a host	1
a source	1
a sourcetype	1
a status	1
a user	14

INTERESTING FIELDS

a Account_Domain	1
a Account_Name	100
a action	1
a app	1
a body	100
a category	1
a CategoryString	1
a change_type	1
a ComputerName	1
a date_hour	24
a date_mday	1
a date_minute	58
a date_month	1
a date_second	53
a date_wday	1
a date_year	1
a date_zone	2

i	Time	Event
›	3/24/20 11:56:41.000 PM	2020-03-24T23:56:41.000+0000,,"Domain_A Domain_A",,"user_a user_d",,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x6C10,,,,,,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_a Show all 61 lines EventCodeDescription = An attempt was made to reset an accounts password host = windows_server_logs source = windows_server_logs.csv sourcetype = csv status = failure user = user_d
›	3/24/20 11:34:35.000 PM	2020-03-24T23:34:35.000+0000,,"Domain_A Domain_A",,"user_m user_l",,,,,,,,,,,,,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 EventCodeDescription = An attempt was made to reset an accounts password host = windows_server_logs source = windows_server_logs.csv sourcetype = csv status = failure user = user_l
›	3/24/20 11:30:24.000 PM	2020-03-24T23:30:24.000+0000,,"Domain_A Domain_A",,"user_c user_f",,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x5FC9,,,,,,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_c Show all 61 lines EventCodeDescription = An attempt was made to reset an accounts password host = windows_server_logs source = windows_server_logs.csv sourcetype = csv status = failure user = user_f

localhost:8000/en-US/app/search/search?q=search source%3D"windows_server_l...



Alert Windows Status Failure

The baseline of failure of status for Windows 5 per hour on average, the Threshold is 7 or more failure per hour. When the threshold is reached an email will be sent over to SOC@VSI-company.com

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 13, 2024 4:40:44 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 7. Edit
Actions: .... ∨ 1 Action Edit
✉ Send email

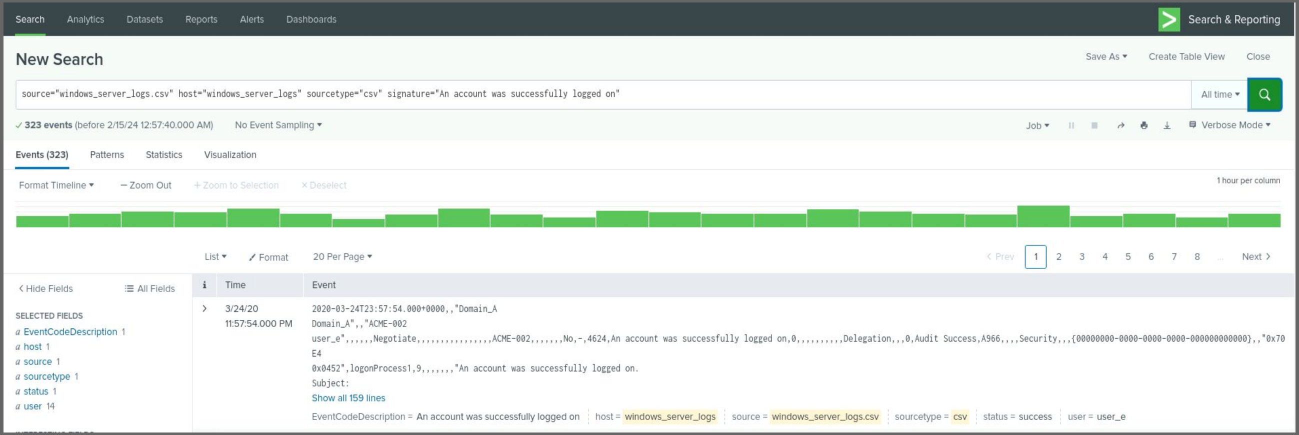
Created an alert to notify VSI of suspicious activity.

Determined that the baseline is 5 per hour and threshold is 7 failed WIndows Activity.

When the threshold has been reached an alert will be activated and will send an email to SOC@VSI-company.com

Day 1: Designing The Defensive Solution

Part 2: Windows_server Alert #2 Successful Login

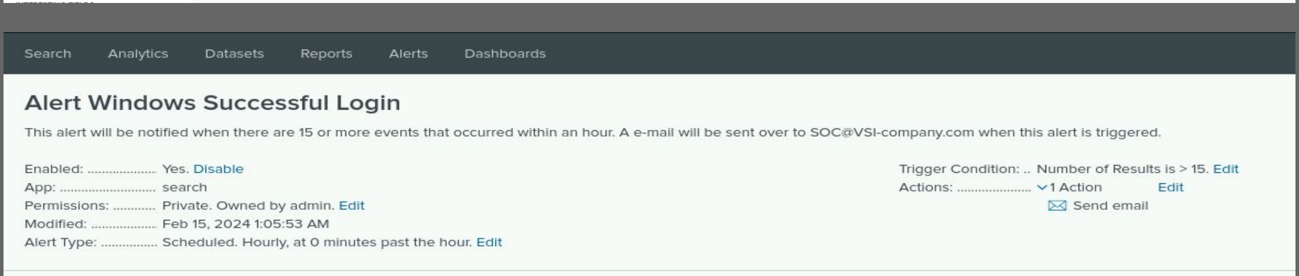


```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" signature="An account was successfully logged on"
```

✓ 323 events (before 2/15/24 12:57:40.000 AM)   No Event Sampling ▾

SELECTED FIELDS
- a EventCodeDescription 1
- a host 1
- a source 1
- a sourcetype 1
- a status 1
- a user 14

i	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},,"0x70 E4 0x0452",logonProcess1,9,,,,,,,"An account was successfully logged on. Subject: Show all 159 lines EventCodeDescription = An account was successfully logged on host = windows_server_logs source = windows_server_logs.csv sourcetype = csv status = success user = user_e



Alert Windows Successful Login

This alert will be notified when there are 15 or more events that occurred within an hour. A e-mail will be sent over to SOC@VSI-company.com when this alert is triggered.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 15, 2024 1:05:53 AM
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

Created an alert to notify VSI of suspicious activity.

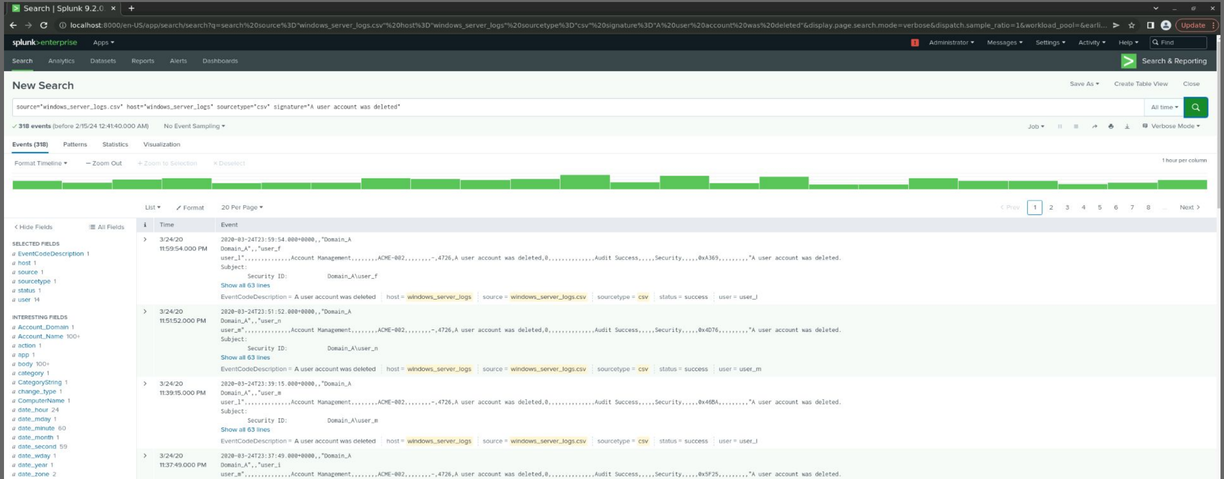
There were 323 events that occurred over 24 hr. period.

Determined that the baseline is 13 per hour and threshold is 15 successful logins.

When the threshold has been reached an alert will be activated and will send an email to SOC@VSI-company.com

Day 1: Designing The Defensive Solution

Part 2: Windows_server Alert #3 User Account was Deleted



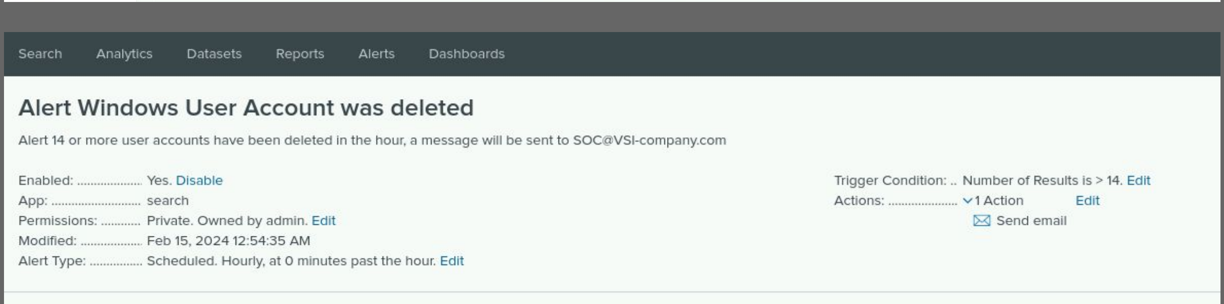
```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" signature="A user account was deleted"
```

✓ 318 events (before 2/15/24 12:41:40.000 AM) No Event Sampling

SELECTED FIELDS
- a EventCodeDescription 1
- a host 1
- a source 1
- a sourcetype 1
- a status 1
- a user 14

INTERESTING FIELDS
- a Account_Domain 1
- a Account_Name 100+
- a action 1
- a app 1
- a body 100+
- a category 1
- a CategoryString 1
- a change_type 1
- a ComputerName 1
- a date_hour 24
- a date_mday 1
- a date_minute 60
- a date_month 1
- a date_second 59
- a date_wday 1
- a date_year 1
- a date_zone 2

i	Time	Event
>	3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,,"Domain_A Domain_A",,"user_f user_l",,,,,,,,,,,,,,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 63 lines EventCodeDescription = A user account was deleted host = windows_server_logs source = windows_server_logs.csv sourcetype = csv status = success user = user_l
>	3/24/20 11:51:52.000 PM	2020-03-24T23:51:52.000+0000,,"Domain_A Domain_A",,"user_n user_m",,,,,,,,,,,,,,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 EventCodeDescription = A user account was deleted host = windows_server_logs source = windows_server_logs.csv sourcetype = csv status = success user = user_m
>	3/24/20 11:39:15.000 PM	2020-03-24T23:39:15.000+0000,,"Domain_A Domain_A",,"user_m user_l",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x46BA,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_m Show all 63 lines EventCodeDescription = A user account was deleted host = windows_server_logs source = windows_server_logs.csv sourcetype = csv status = success user = user_l
>	3/24/20 11:37:49.000 PM	2020-03-24T23:37:49.000+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.



Alert Windows User Account was deleted

Alert 14 or more user accounts have been deleted in the hour, a message will be sent to SOC@VSI-company.com

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 15, 2024 12:54:35 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 14. Edit
Actions: .... 1 Action Edit
Send email

Created an alert to notify VSI of suspicious activity.

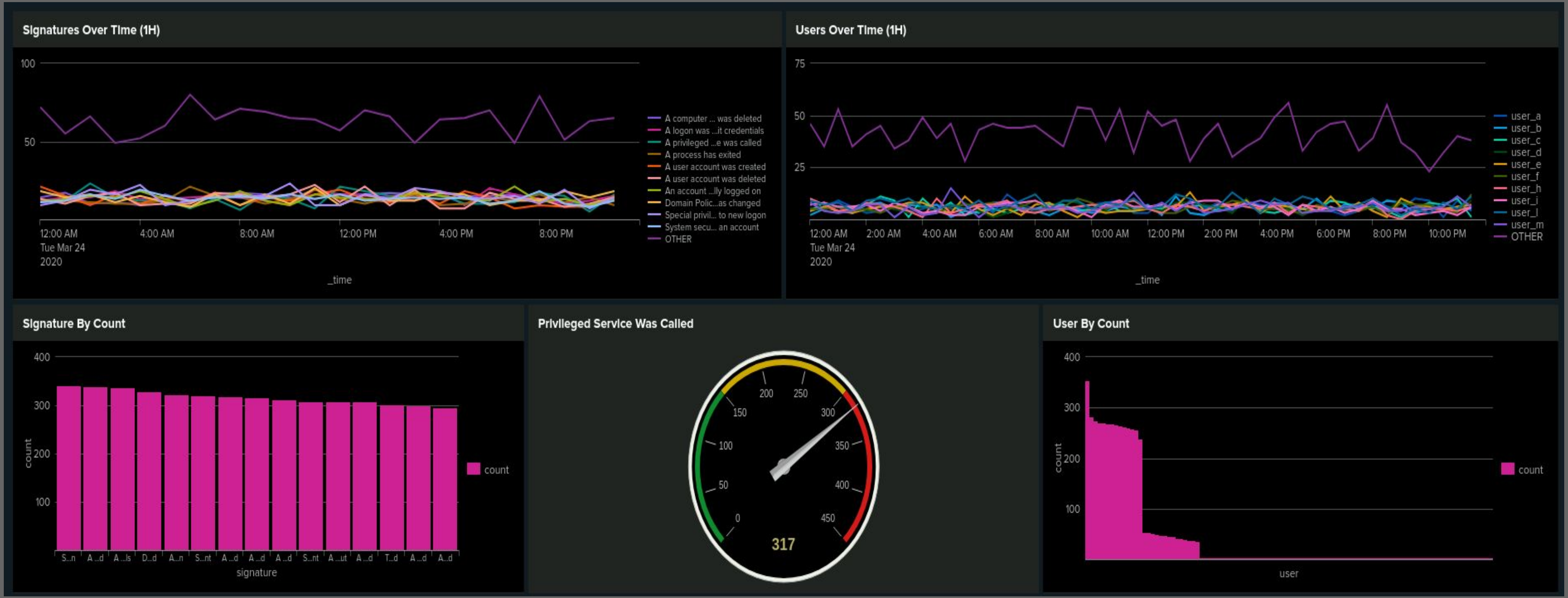
There were 318 events that occurred over 24 hr. period.

Determined that the baseline is 12 per hour and threshold is 14 user account was deleted results.

When the threshold has been reached an alert will be activated and will send an email to SOC@VSI-company.com

Day 1: Designing The Defensive Solution

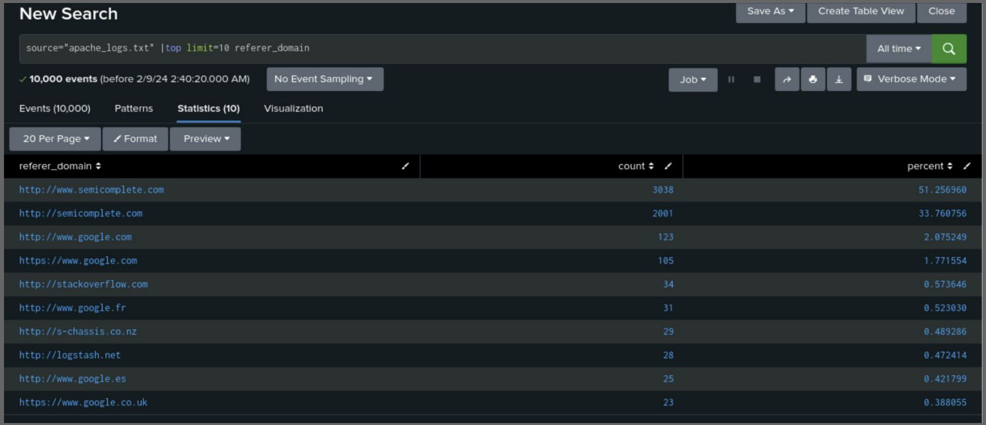
Part 3: Windows Dashboard



Day 1: Designing The Defensive Solution

Part 4: Apache Logs Report

Domains

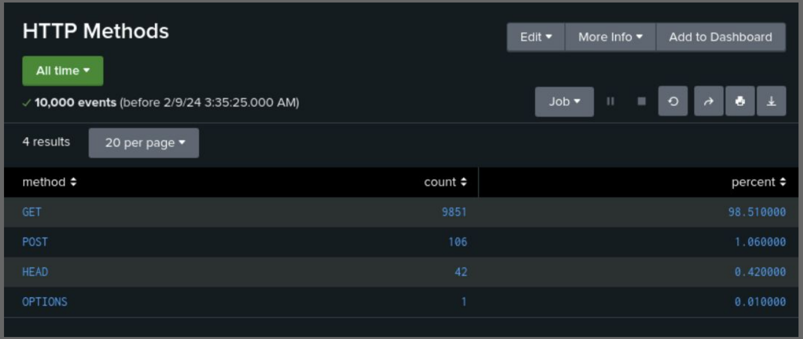


```
source="apache_logs.txt" |top limit=10 referer_domain
```

✓ **10,000 events** (before 2/9/24 2:40:20.000 AM)

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 Methods

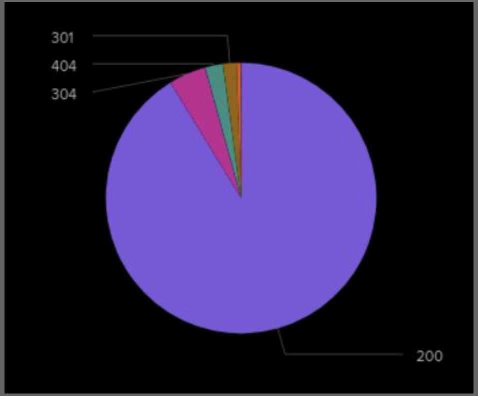


✓ **10,000 events** (before 2/9/24 3:35:25.000 AM)

4 results

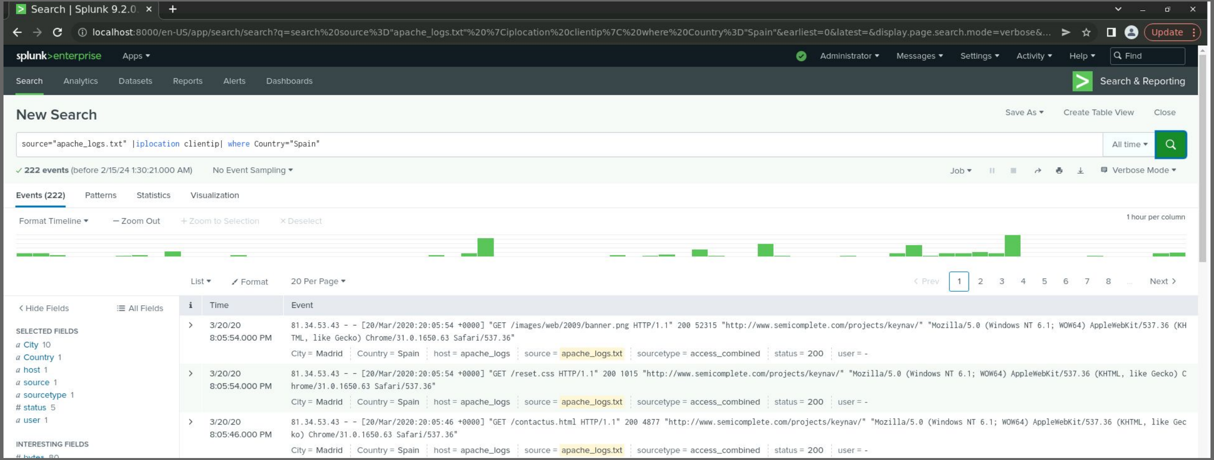
method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

Status Codes



Day 1: Alert HTTP POST Apache Logs

Part 4: Alert: Activity from Any Other Country besides the United States



New Search

```
source="apache_logs.txt" |iplocation clientip| where Country="Spain"
```

✓ **222 events** (before 2/15/24 1:30:21.000 AM) No Event Sampling

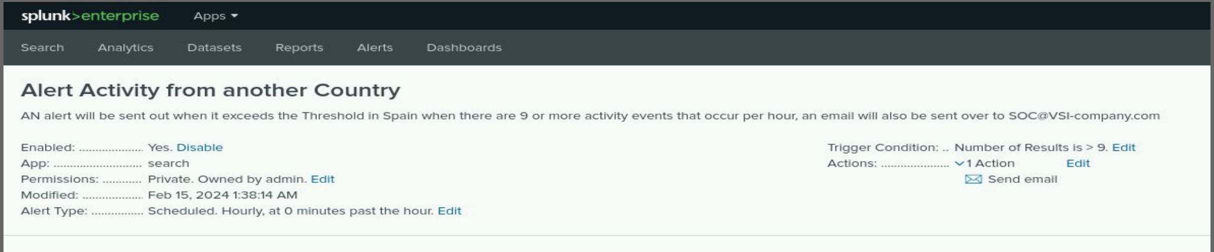
Events (222)

SELECTED FIELDS

a City	10
a Country	1
a host	1
a source	1
a sourcetype	1
# status	5
a user	1

INTERESTING FIELDS

i	Time	Event
>	3/20/20 8:05:54.000 PM	81.34.53.43 - - [20/Mar/2020:20:05:54 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/projects/keynav/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36" City = Madrid Country = Spain host = apache_logs source = apache_logs.txt sourcetype = access_combined status = 200 user = -
>	3/20/20 8:05:54.000 PM	81.34.53.43 - - [20/Mar/2020:20:05:54 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/keynav/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36" City = Madrid Country = Spain host = apache_logs source = apache_logs.txt sourcetype = access_combined status = 200 user = -
>	3/20/20 8:05:46.000 PM	81.34.53.43 - - [20/Mar/2020:20:05:46 +0000] "GET /contactus.html HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/keynav/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36" City = Madrid Country = Spain host = apache_logs source = apache_logs.txt sourcetype = access_combined status = 200 user = -



Alert Activity from another Country

AN alert will be sent out when it exceeds the Threshold in Spain when there are 9 or more activity events that occur per hour, an email will also be sent over to SOC@VSI-company.com

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 15, 2024 1:38:14 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

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

Created an alert to notify VSI of suspicious activity.

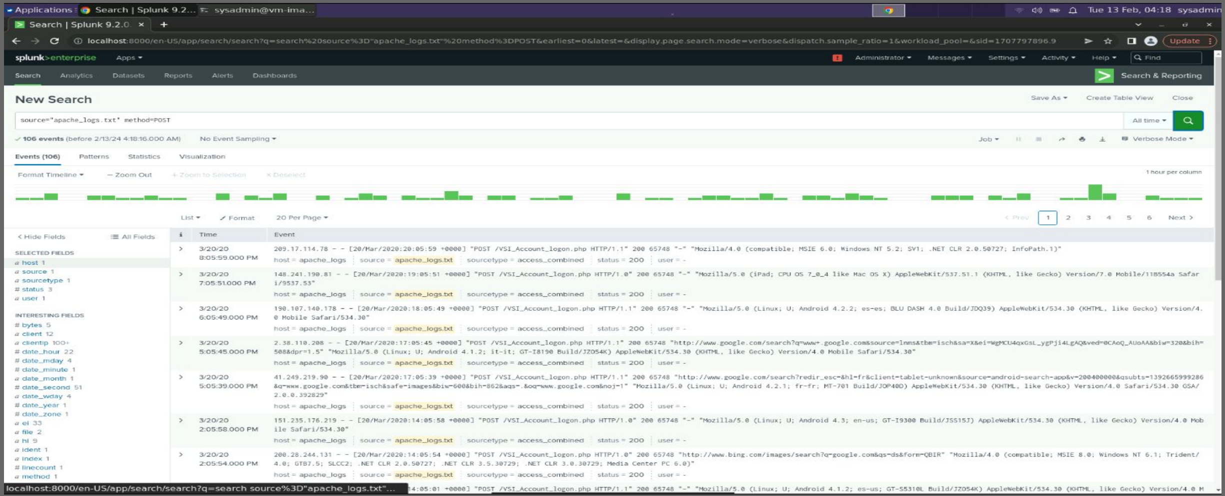
There were 222 events that occurred in Spain.

Determined that the baseline is 6 per hour and threshold is 9.

When the threshold has been reached an alert will be activated and will send an email to SOC@VSI-company.com

Day:1 Alert HTTP POST Apache Logs

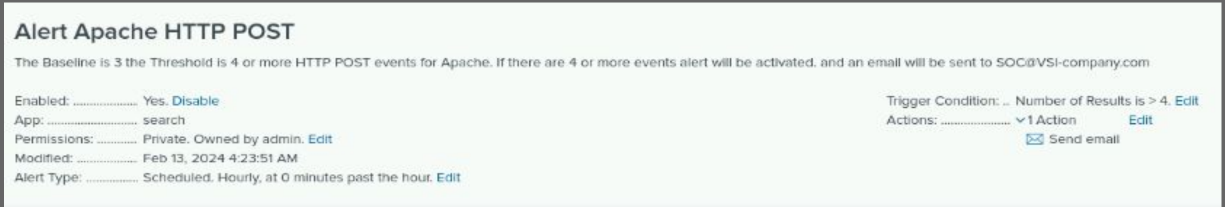
Part 4: Alert: HTTP POST



```
source="apache_logs.txt" method=POST
```

✓ 106 events (before 2/13/24 4:18:16.000 AM)   No Event Sampling

```
i  Time          Event
>  3/20/20       209.17.114.78 - - [20/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 2.0.50727; InfoPath.1)"
   8:05:59.000 PM  host = apache_logs   source = apache_logs.txt   sourcetype = access_combined   status = 200   user = -
>  3/20/20       148.241.190.81 - - [20/Mar/2020:19:05:51 +0000] "POST /VSI_Account_logon.php HTTP/1.0" 200 65748 "-" "Mozilla/5.0 (iPad; CPU OS 7_0_4 like Mac OS X) AppleWebKit/537.51.1 (KHTML, like Gecko) Version/7.0 Mobile/11B554a Safar
   7:05:51.000 PM  i/9537.53"
                 host = apache_logs   source = apache_logs.txt   sourcetype = access_combined   status = 200   user = -
>  3/20/20       190.107.140.178 - - [20/Mar/2020:18:05:49 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/5.0 (Linux; U; Android 4.2.2; es-es; BLU DASH 4.0 Build/JDQ39) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.
   6:05:49.000 PM  0 Mobile Safari/534.30"
                 host = apache_logs   source = apache_logs.txt   sourcetype = access_combined   status = 200   user = -
>  3/20/20       2.38.110.208 - - [20/Mar/2020:17:05:45 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "http://www.google.com/search?q=www+.google.com&source=lnms&tbm=isch&sa=X&ei=WgMCU4qxGsL_ygPji4LgAQ&ved=0CAoQ_AUoAA&biw=320&bih=
   5:05:45.000 PM  508&dpr=1.5" "Mozilla/5.0 (Linux; U; Android 4.1.2; it-it; GT-I8190 Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30"
                 host = apache_logs   source = apache_logs.txt   sourcetype = access_combined   status = 200   user = -
>  3/20/20       41.249.219.90 - - [20/Mar/2020:17:05:39 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "http://www.google.com/search?redir_esc=&hl=fr&client=tablet-unknown&source=android-search-app&v=200400000&qsubts=1392665999286
   5:05:39.000 PM  &q=www.google.com&tbm=isch&safe=images&biw=600&bih=862&aqs=.&oq=www.google.com&noj=1" "Mozilla/5.0 (Linux; U; Android 4.2.1; fr-fr; MT-701 Build/JOP40D) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Safari/534.30 GSA/
                 2.0.0.392829"
                 host = apache_logs   source = apache_logs.txt   sourcetype = access_combined   status = 200   user = -
>  3/20/20       151.235.176.219 - - [20/Mar/2020:14:05:58 +0000] "POST /VSI_Account_logon.php HTTP/1.0" 200 65748 "-" "Mozilla/5.0 (Linux; U; Android 4.3; en-us; GT-I9300 Build/JSS15J) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mob
   2:05:58.000 PM  ile Safari/534.30"
                 host = apache_logs   source = apache_logs.txt   sourcetype = access_combined   status = 200   user = -
>  3/20/20       200.28.244.131 - - [20/Mar/2020:14:05:54 +0000] "POST /VSI_Account_logon.php HTTP/1.0" 200 65748 "http://www.bing.com/images/search?q=google.com&qs=ds&form=QBIR" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/
   2:05:54.000 PM  4.0; GTB7.5; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)"
                 host = apache_logs   source = apache_logs.txt   sourcetype = access_combined   status = 200   user = -
                 4:05:01 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/5.0 (Linux; U; Android 4.1.2; es-us; GT-S5310L Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 M
```



Alert Apache HTTP POST

The Baseline is 3 the Threshold is 4 or more HTTP POST events for Apache. If there are 4 or more events alert will be activated. and an email will be sent to SOC@VSI-company.com

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 13, 2024 4:23:51 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 4. Edit
Actions: .... 1 Action Edit
Send email

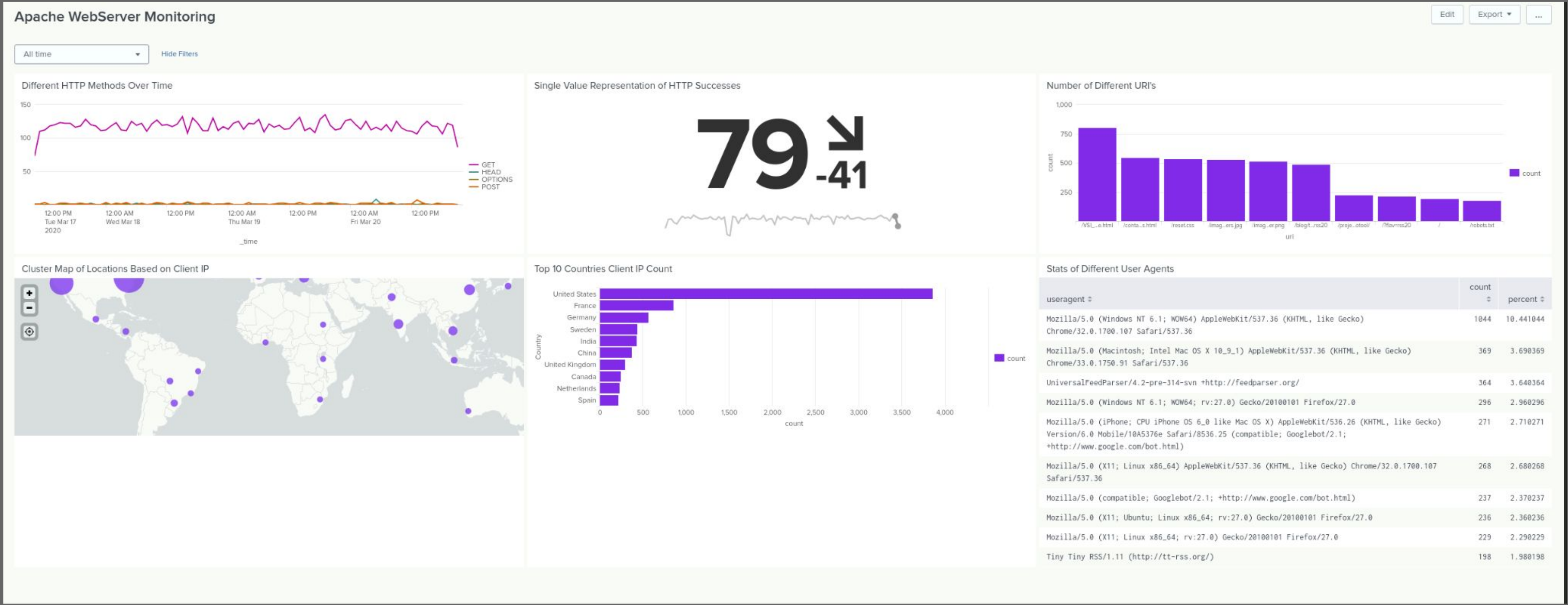
Created an alert to notify VSI of suspicious activity.

Determined that the baseline is 3 per hour and threshold is 4 failed HTTP POST Activity.

When the threshold has been reached an alert will be activated and will send an email to SOC@VSI-company.com

Day 1: Designing The Defensive Solution

Part 4: Visualisations and Dashboards Apache Web Server Monitoring



Apache WebServer Monitoring

Different HTTP Methods Over Time

Single Value Representation of HTTP Successes

Number of Different URI's

Cluster Map of Locations Based on Client IP

Top 10 Countries Client IP Count

Stats of Different User Agents

useragent ⇕	count ⇕	percent ⇕
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	1044	10.441044
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	369	3.690369
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	364	3.640364
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	296	2.960296
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	271	2.710271
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	268	2.680268
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	237	2.370237
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	236	2.360236
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	229	2.290229
Tiny Tiny RSS/1.11 (http://tt-rss.org/)	198	1.980198

Day:1 Part 5 [Add-On The Watch v2]

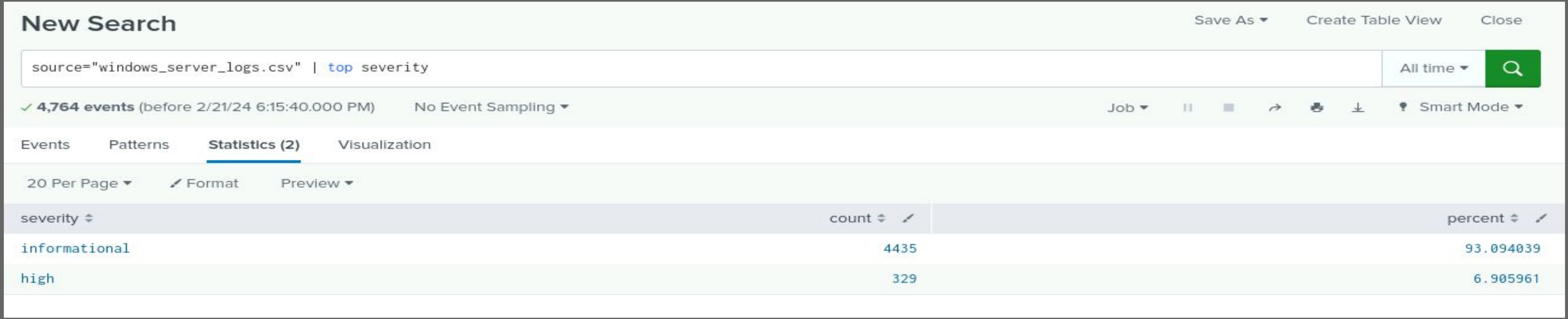
Summary - This application aims to enhance Splunk Enterprise by providing SIEM-like functionality for teams that do not have Splunk Enterprise Security. The main concept of this tool is to streamline the identification of events from known information without the need to create new searches for each artifact. It also aims to capitalize on the time spent on investigations by improving alert handling and automation.

Scenario - The Watch v2 add-on empowers the team to establish live monitoring on essential data sources like database access logs and user authentication events. They can specify conditions, such as repeated failed login attempts or unauthorized access to restricted files, to promptly trigger alerts.

Day 2: Monitoring and Analyzing Attacks

Report Analysis: Severity

Before:

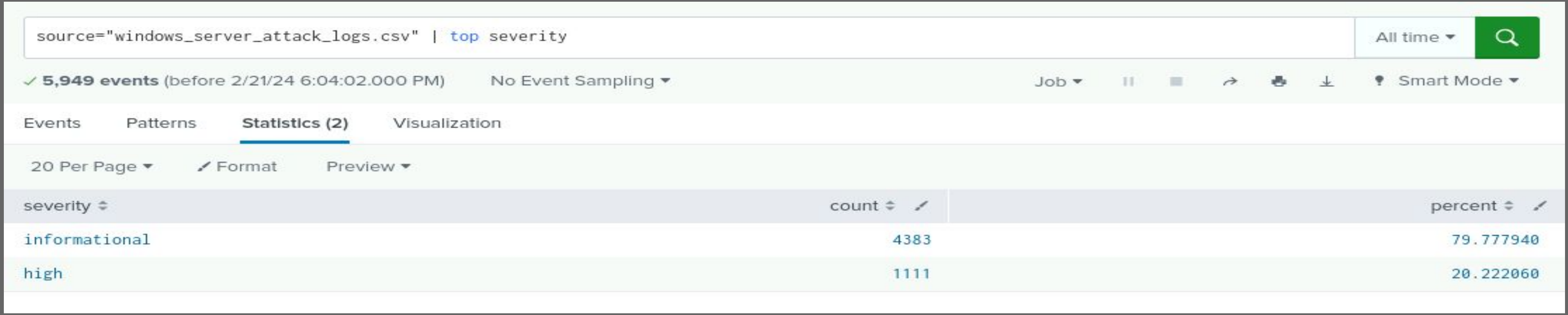


```
source="windows_server_logs.csv" | top severity
```

✓ **4,764 events** (before 2/21/24 6:15:40.000 PM)

severity	count	percent
informational	4435	93.094039
high	329	6.905961

After:



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

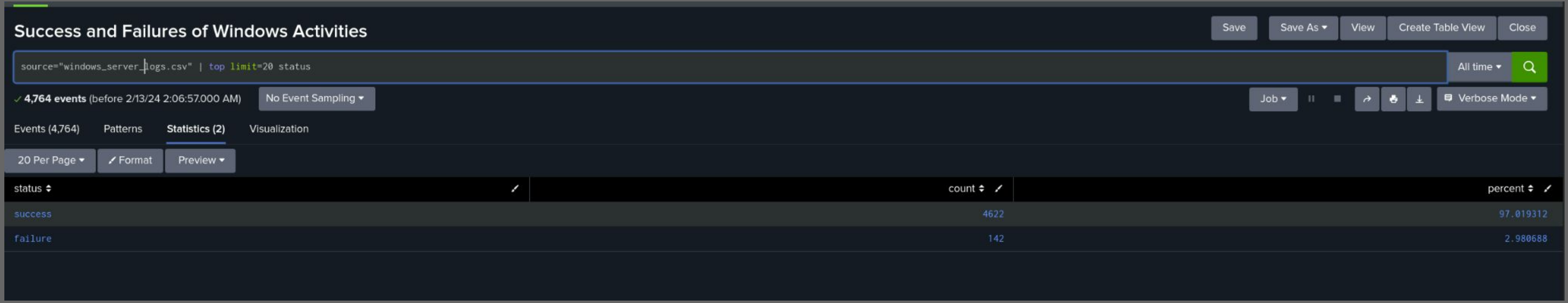
✓ **5,949 events** (before 2/21/24 6:04:02.000 PM)

severity	count	percent
informational	4383	79.777940
high	1111	20.222060

Day 2: Monitoring and Analyzing Attacks

Report Analysis: Windows Failed Activities

Before:



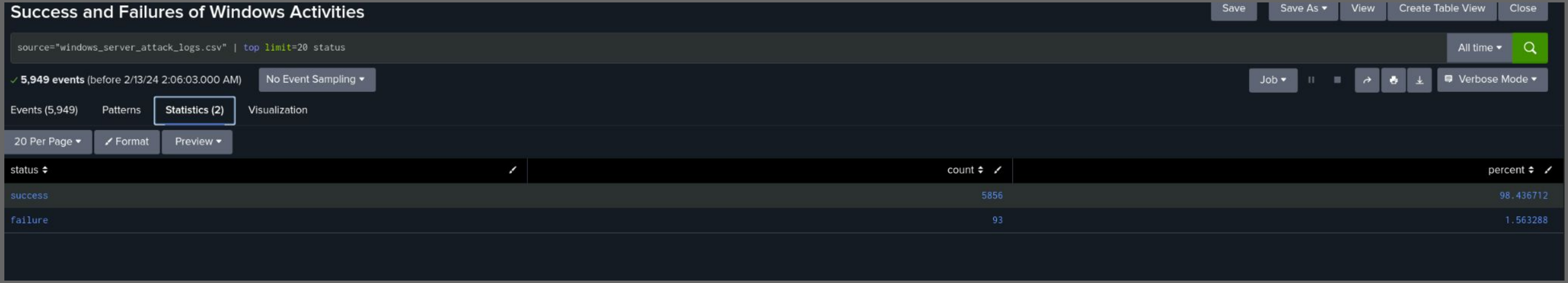
Success and Failures of Windows Activities

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

✓ **4,764 events** (before 2/13/24 2:06:57.000 AM)

status	count	percent
success	4622	97.019312
failure	142	2.980688

After:



Success and Failures of Windows Activities

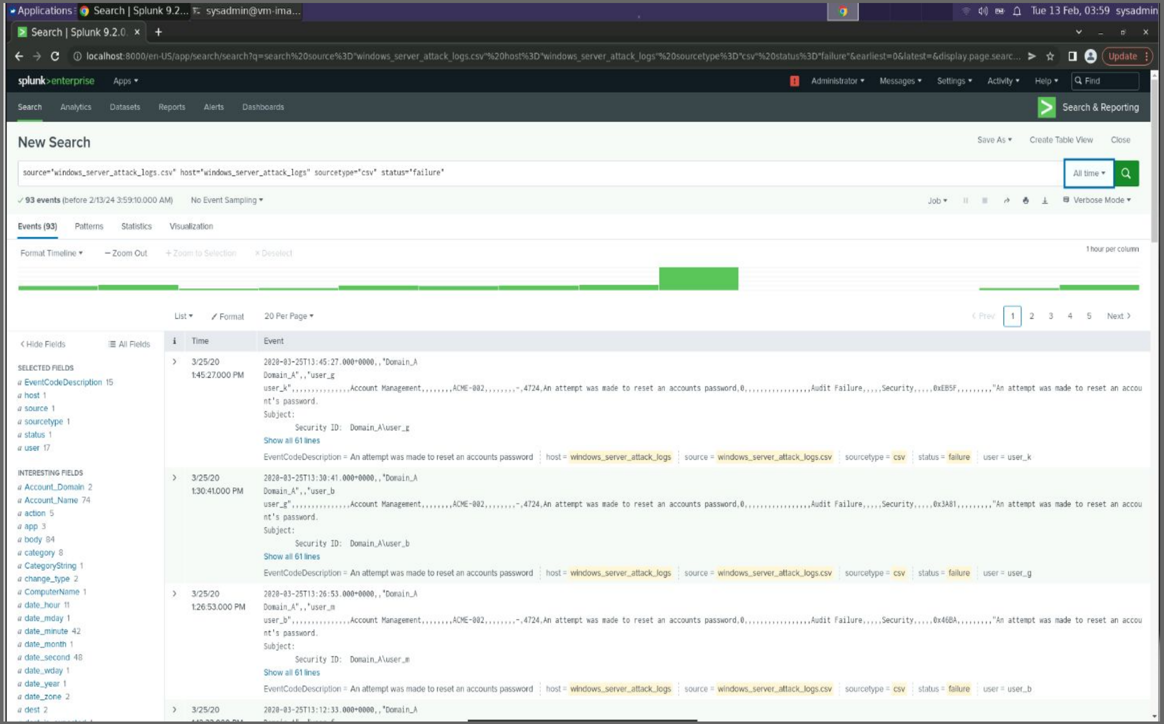
```
source="windows_server_attack_logs.csv" | top limit=20 status
```

✓ **5,949 events** (before 2/13/24 2:06:03.000 AM)

status	count	percent
success	5856	98.436712
failure	93	1.563288

Day 2: Monitoring and Analyzing Attacks

Alert Analysis for Failed Windows Activity



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

✓ 93 events (before 2/13/24 3:59:10.000 AM) No Event Sampling

SELECTED FIELDS
- a EventCodeDescription 15
- a host 1
- a source 1
- a sourcetype 1
- a status 1
- a user 17

INTERESTING FIELDS
- a Account_Domain 2
- a Account_Name 74
- a action 5
- a app 3
- a body 84
- a category 8
- a CategoryString 1
- a change_type 2
- a ComputerName 1
- a date_hour 11
- a date_mday 1
- a date_minute 42
- a date_month 1
- a date_second 48
- a date_wday 1
- a date_year 1
- a date_zone 2
- a dest 2

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 accou
nt's password.
Subject:
        Security ID:  Domain_A\user_g
```

Show all 61 lines

EventCodeDescription = An attempt was made to reset an accounts password | host = windows_server_attack_logs | source = windows_server_attack_logs.csv | sourcetype = csv | status = failure | user = user_k

3/25/20 1:30:41.000 PM

```
2020-03-25T13:30:41.000+0000,,"Domain_A
Domain_A",,"user_b
user_g",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x3A81,,,,,,,,,"An attempt was made to reset an accou
nt's password.
Subject:
        Security ID:  Domain_A\user_b
```

Show all 61 lines

EventCodeDescription = An attempt was made to reset an accounts password | host = windows_server_attack_logs | source = windows_server_attack_logs.csv | sourcetype = csv | status = failure | user = user_g

3/25/20 1:26:53.000 PM

```
2020-03-25T13:26:53.000+0000,,"Domain_A
Domain_A",,"user_m
user_b",,,,,,,,,,,,,,,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 accou
nt's password.
Subject:
        Security ID:  Domain_A\user_m
```

Show all 61 lines

EventCodeDescription = An attempt was made to reset an accounts password | host = windows_server_attack_logs | source = windows_server_attack_logs.csv | sourcetype = csv | status = failure | user = user_b

3/25/20

```
2020-03-25T13:12:33.000+0000,,"Domain_A
```

We did detect a suspicious volume of failed activity

The count of events was 93 that occurred over 14 hours.

It occurred on 8AM Wed. March 25th 2020 with 35 events.

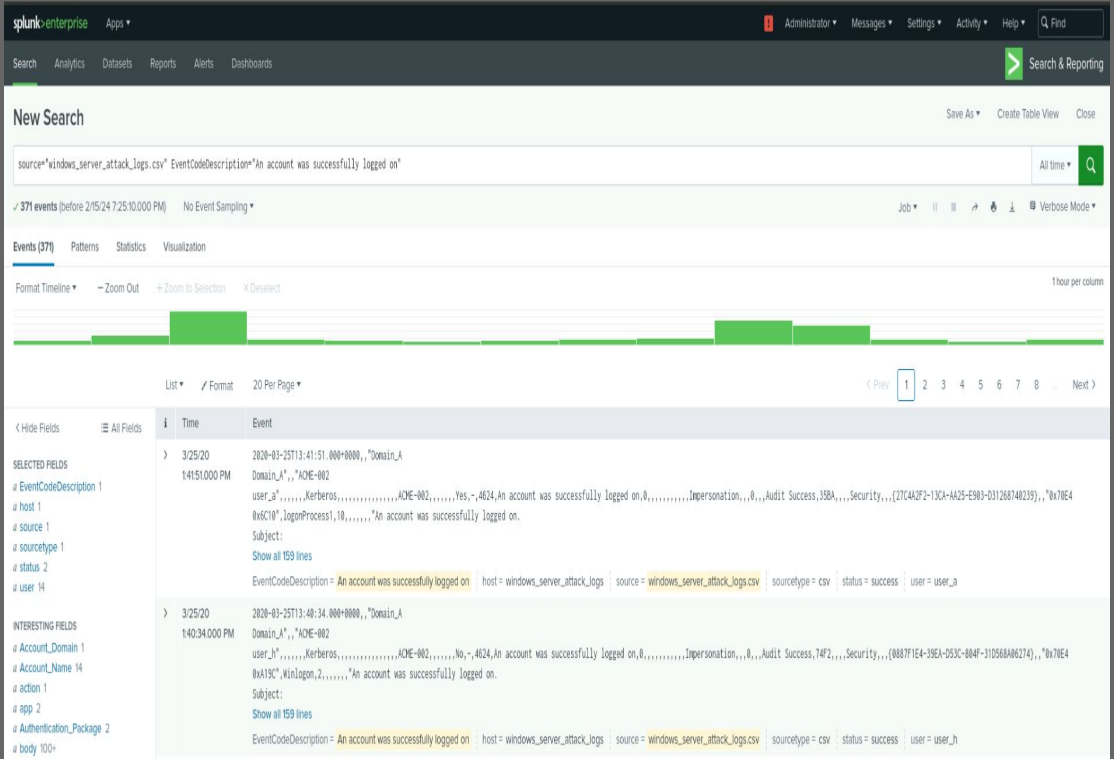
The alert would be triggered for this activity.

After reviewing the results I would keep my threshold the same.

HM

Day 2: Monitoring and Analyzing Attacks

Alert Analysis for Successful Logins Windows Activity



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

✓ 371 events (before 2/15/24 7:25:10.000 PM)

i	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 EventCodeDescription = An account was successfully logged on host = windows_server_attack_logs source = windows_server_attack_logs.csv sourcetype = csv status = success user = user_a
›	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 EventCodeDescription = An account was successfully logged on host = windows_server_attack_logs source = windows_server_attack_logs.csv sourcetype = csv status = success user = user_h

We did detect a suspicious volume of failed activity

The count of events was 371 that occurred over 14 hours.

It occurred 4 times on Wednesday 25 March 2020:

- **1 AM 25 events,**
- **2 AM 94 events.**
- **9 AM 70 events,**
- **10 AM 54 events.**

The alert would be triggered for this activity.

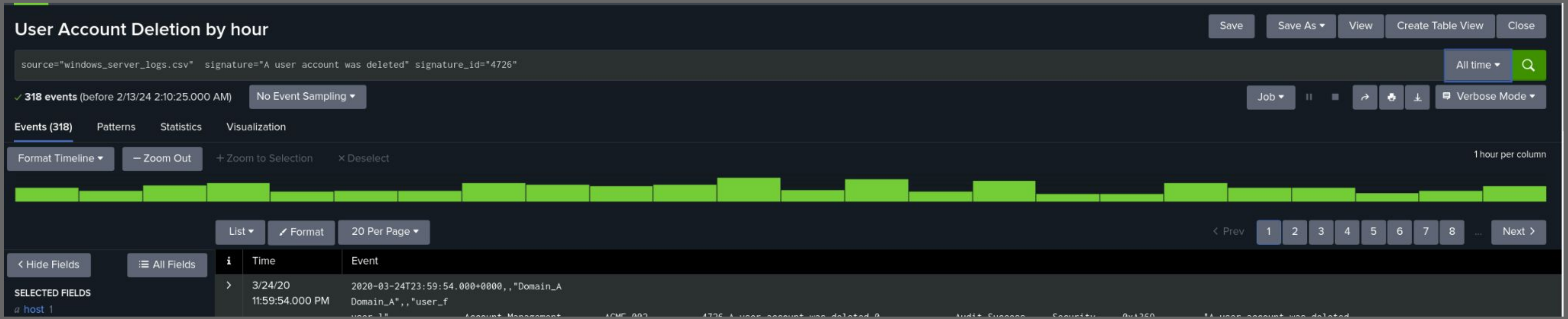
After reviewing the results I would change the threshold to 16 events or more before the threshold is triggered.

HM

Day 2: Monitoring and Analyzing Attacks

Alert Analysis: Windows Alert for Deleted Account

Before:



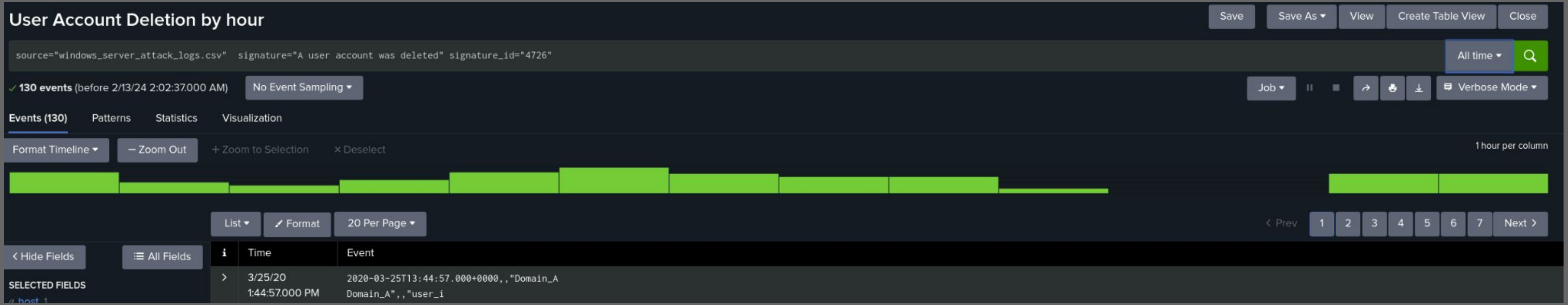
User Account Deletion by hour

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

✓ **318 events** (before 2/13/24 2:10:25.000 AM)

i	Time	Event
>	3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,,"Domain_A Domain_A",,"user_f

After:



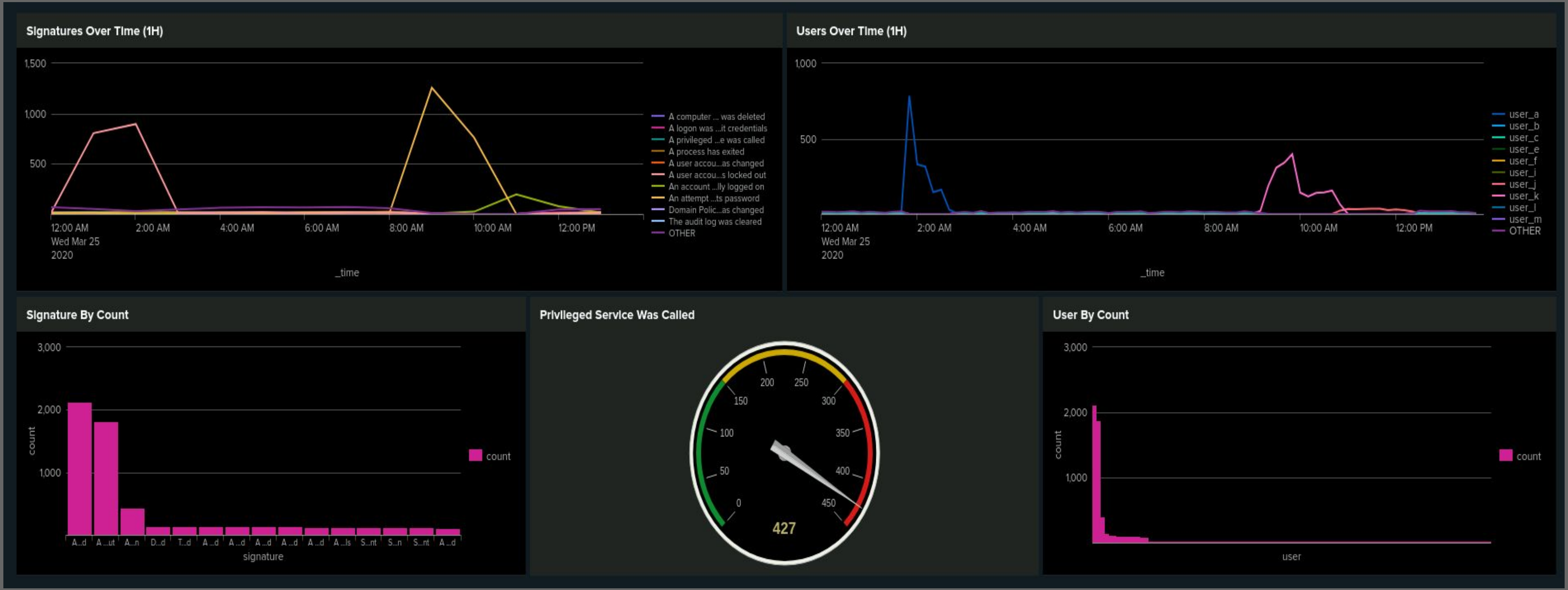
User Account Deletion by hour

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

✓ **130 events** (before 2/13/24 2:02:37.000 AM)

i	Time	Event
>	3/25/20 1:44:57.000 PM	2020-03-25T13:44:57.000+0000,,"Domain_A Domain_A",,"user_i

Day 2: Monitoring and Analyzing Attacks
Dashboard Analysis: Windows Server (Signatures)


Signatures Over Time (1H)

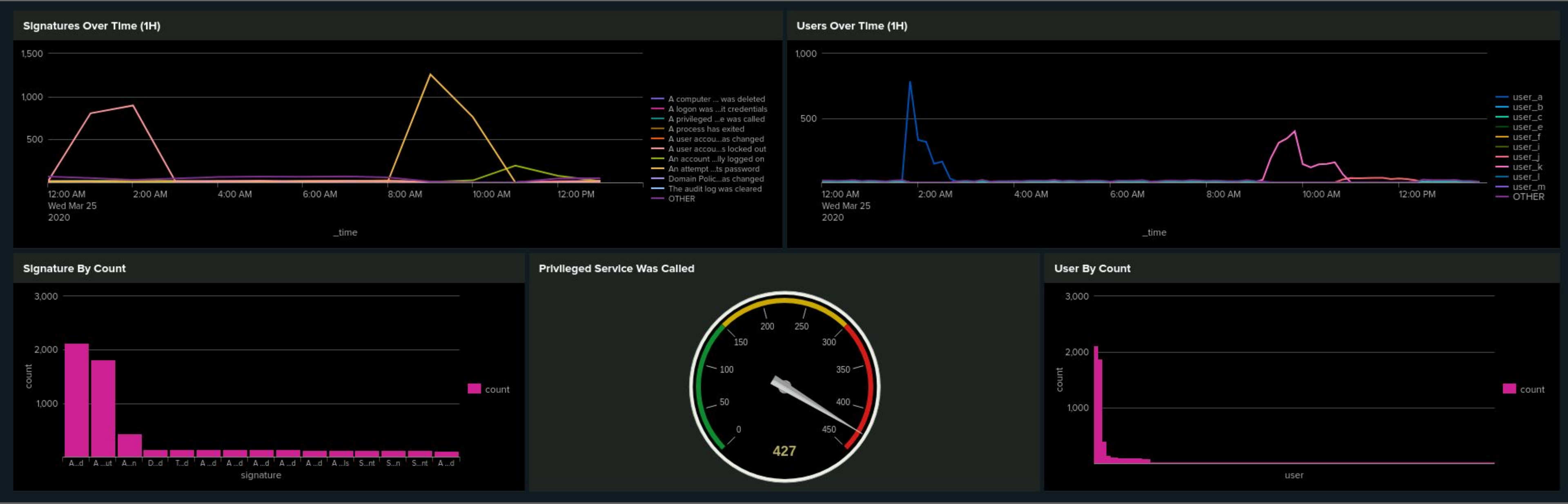
Users Over Time (1H)

Signature By Count

Privileged Service Was Called

User By Count

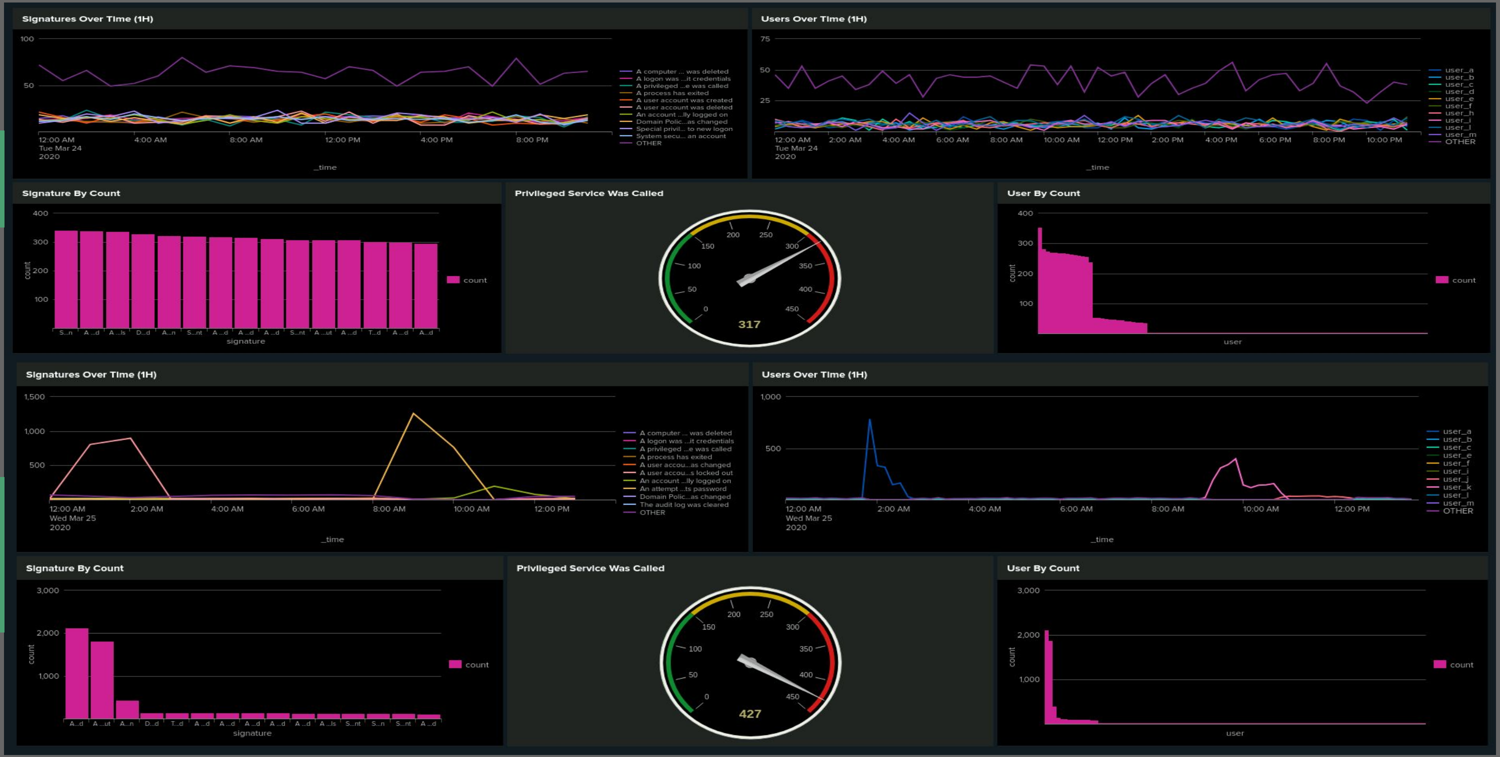
Day 2: Monitoring and Analyzing Attacks
Dashboard Analysis: Windows Server (Users)



Day 2: Monitoring and Analyzing Attacks
Dashboard Analysis: Windows Server (SIDE BY SIDE)

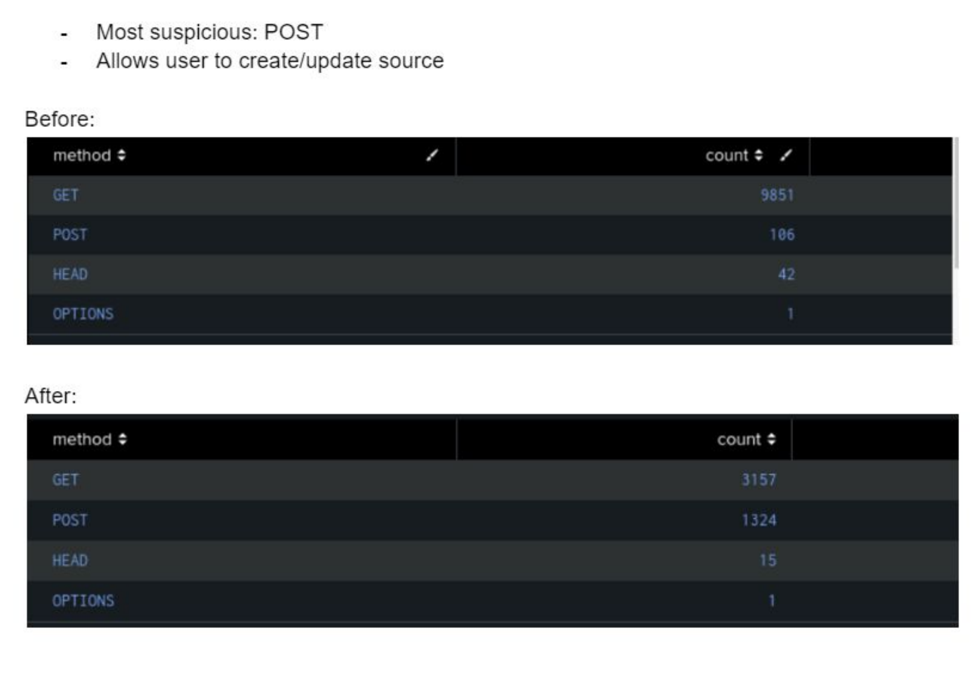
Baseline:

During Attack:



Day 2: Monitoring and Analyzing Attacks

Part 4: Report Analysis: HTTP Methods



- Most suspicious: POST
- Allows user to create/update source

Before:

method	count
GET	9851
POST	106
HEAD	42
OPTIONS	1

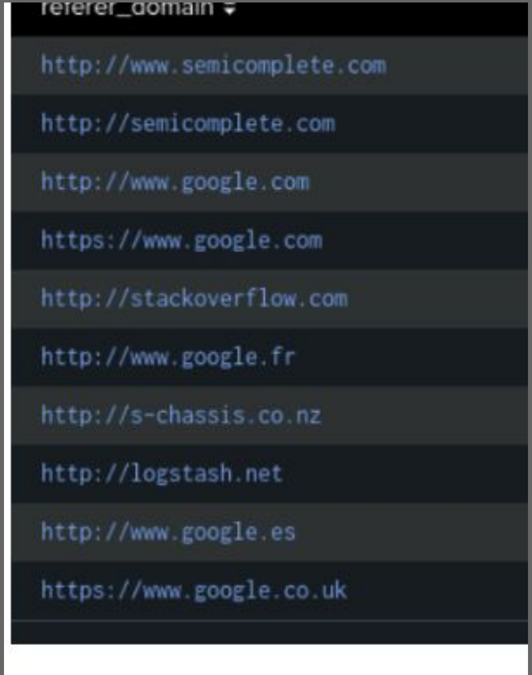
After:

method	count
GET	3157
POST	1324
HEAD	15
OPTIONS	1

Day 2: Monitoring and Analyzing Attacks

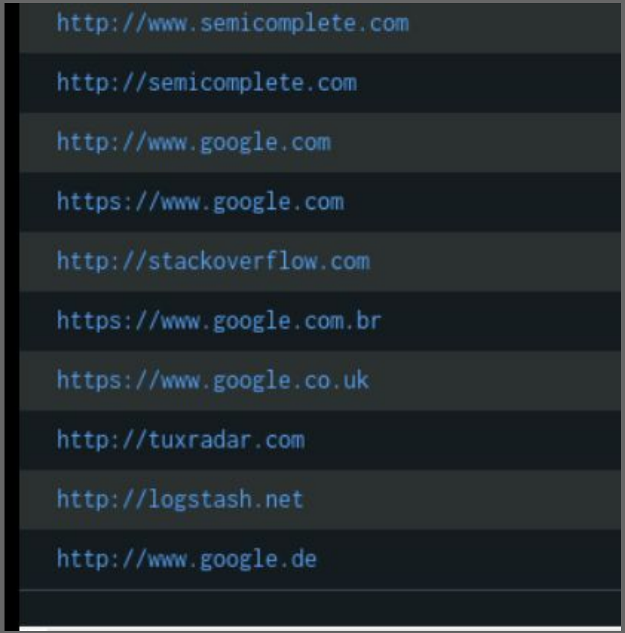
Part 4: Report Analysis: Referrer Domains

BEFORE THE ATTACK



referer_domain
http://www.semicomplete.com
http://semicomplete.com
http://www.google.com
https://www.google.com
http://stackoverflow.com
http://www.google.fr
http://s-chassis.co.nz
http://logstash.net
http://www.google.es
https://www.google.co.uk

AFTER THE ATTACK

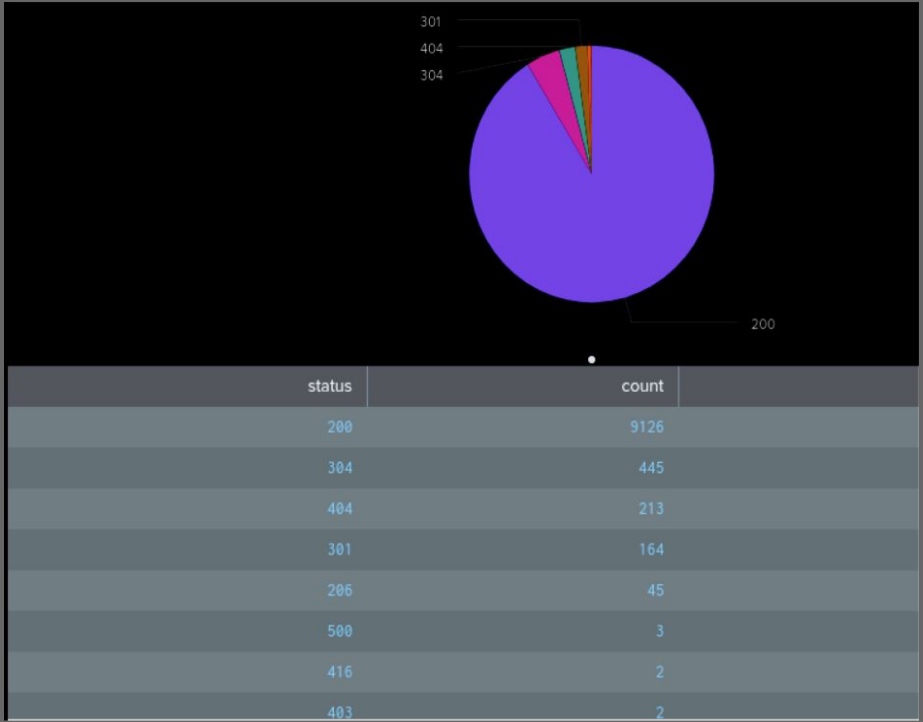


http://www.semicomplete.com
http://semicomplete.com
http://www.google.com
https://www.google.com
http://stackoverflow.com
https://www.google.com.br
https://www.google.co.uk
http://tuxradar.com
http://logstash.net
http://www.google.de

Day 2: Monitoring and Analyzing Attacks

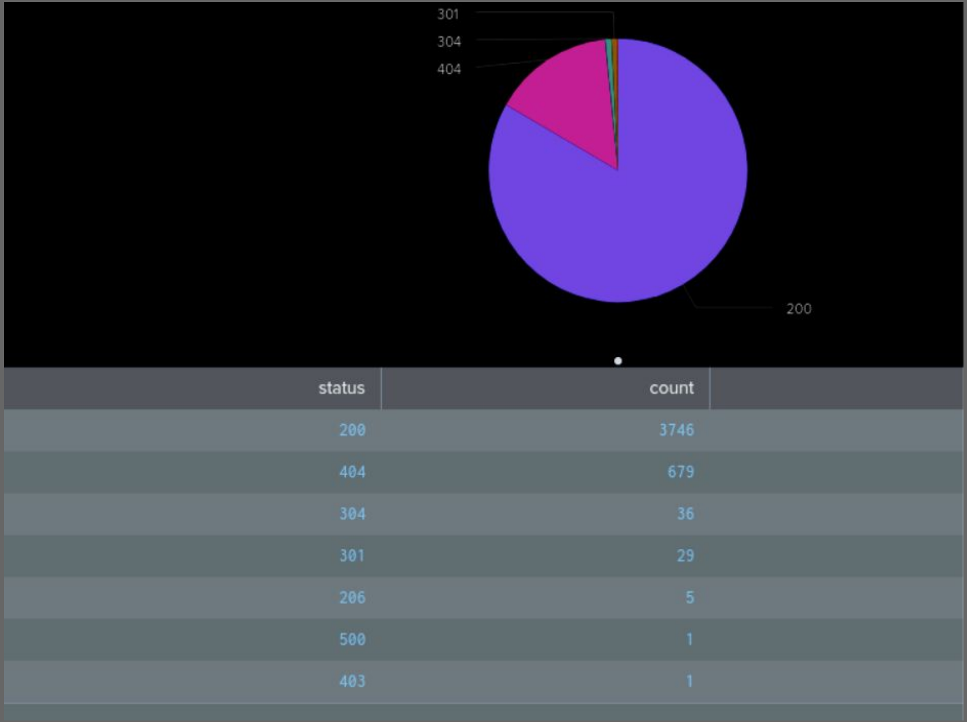
Part 4: Report Analysis: HTTP Response Codes

Before the Attack:



status	count
200	9126
304	445
404	213
301	164
206	45
500	3
416	2
403	2

After the Attack:

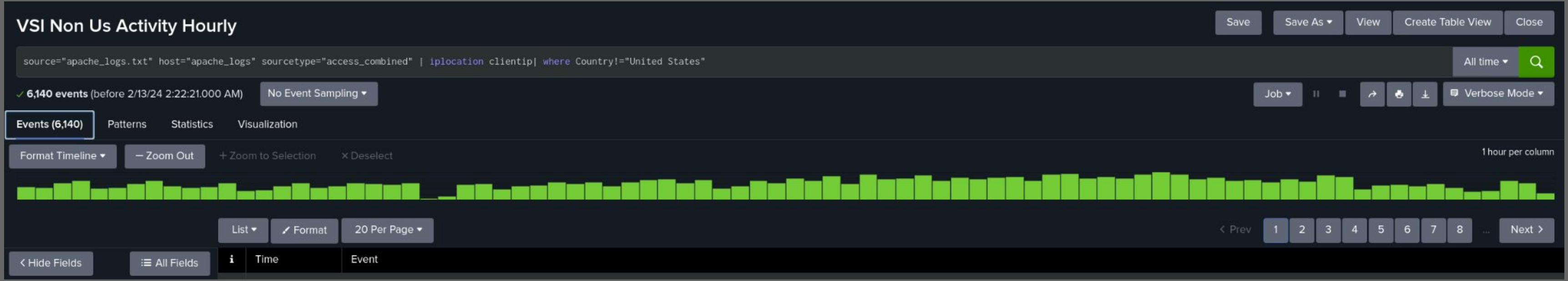


status	count
200	3746
404	679
304	36
301	29
206	5
500	1
403	1

Day 2: Monitoring and Analyzing Attacks

Part 4: Alert Analysis: Alert Analysis for International Activity

Before:

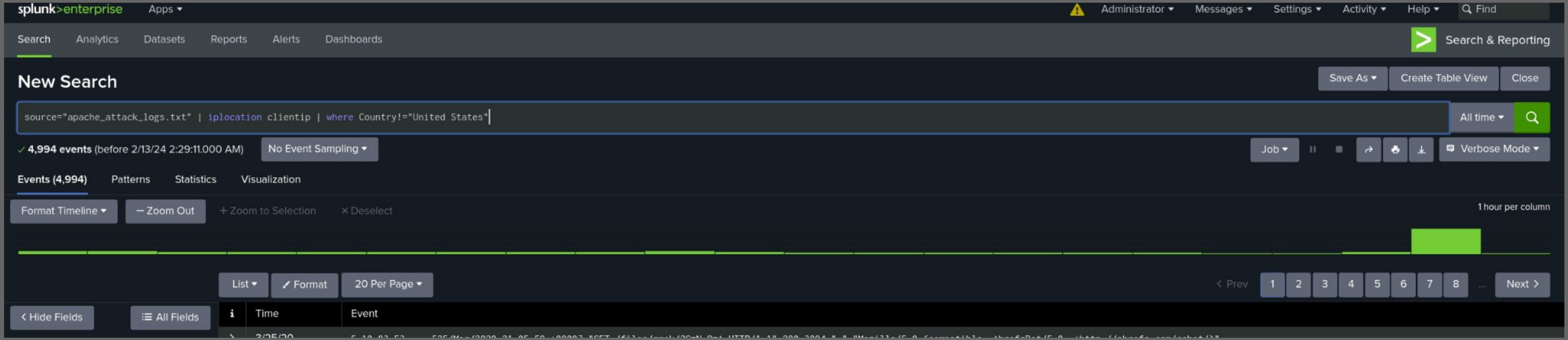


VSI Non Us Activity Hourly

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

✓ 6,140 events (before 2/13/24 2:22:21.000 AM)

After:



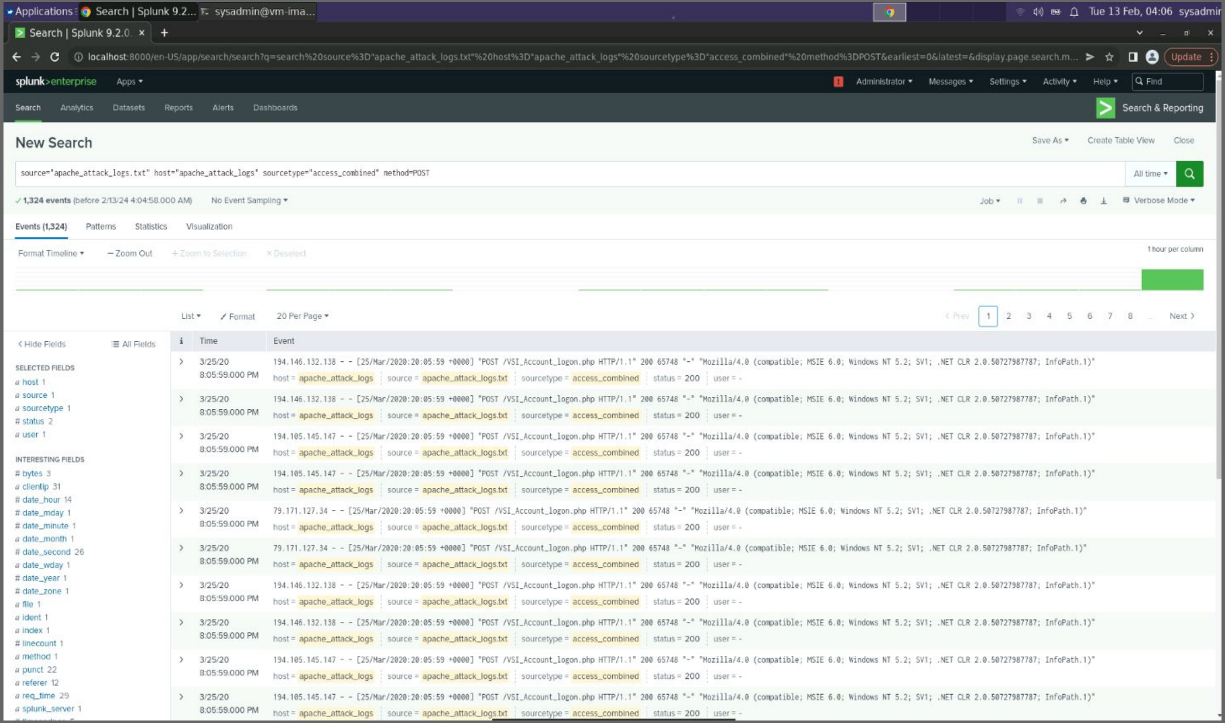
New Search

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

✓ 4,994 events (before 2/13/24 2:29:11.000 AM)

Day 2: Monitoring and Analyzing Attacks

Part 4: Alert Analysis for HTTP POST Activity



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

✓ 1,324 events (before 2/13/24 4:04:58.000 AM) No Event Sampling

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1
# status 2
a user 1

INTERESTING FIELDS

bytes 3
a clientip 31
# date_hour 14
# date_mday 1
# date_minute 1
a date_month 1
# date_second 26
a date_wday 1
# date_year 1
# date_zone 1
a file 1
ident 1
a index 1
# linecount 1
a method 1
a punct 22
a referer 12
a req_time 29
a splunk_server 1

```
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_attack_logs | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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_attack_logs | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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 | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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 | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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_attack_logs | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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_attack_logs | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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_attack_logs | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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_attack_logs | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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 | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -

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 | source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = -
```

Yes we did detect suspicious volume of HTTP POST activity.

1,324 events occurred over an 18 hour period.

It occurred at 8PM March 25th 2020 with 1,296 events.

I would change the threshold from notifying at 4 events to 3 events.

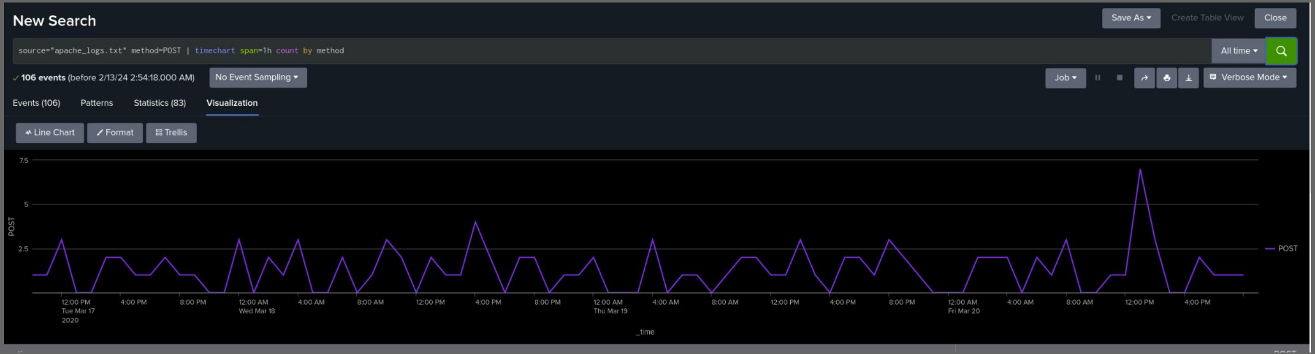
There were only 4 other times when the numbers reached higher than 2 events per hour.

HM

Day 2: Monitoring and Analyzing Attacks

Dashboard Analysis: HTTP POST Method

Before:

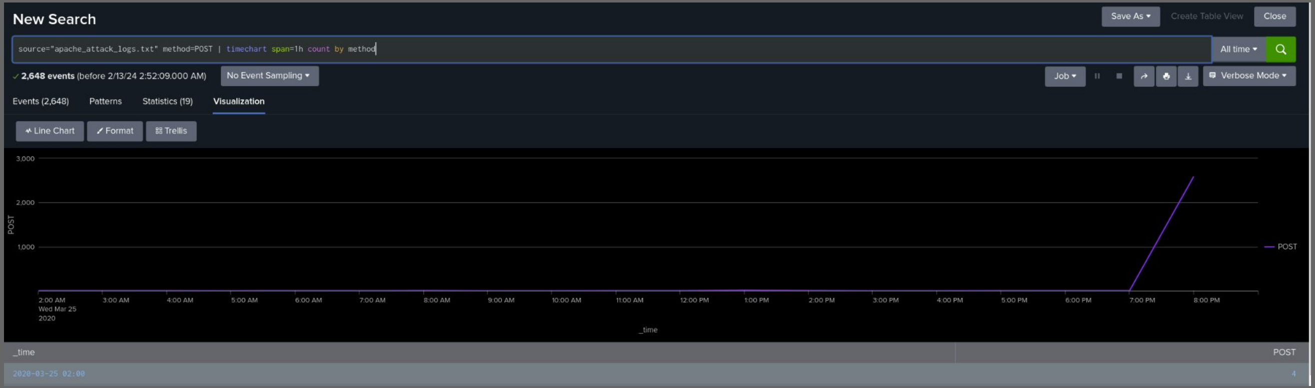


New Search

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

✓ 106 events (before 2/13/24 2:54:18.000 AM)

After:



New Search

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

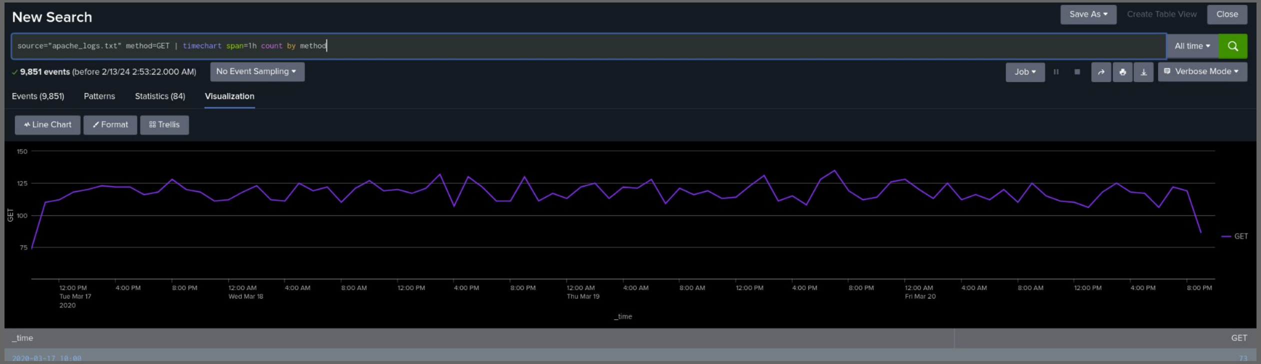
✓ 2,648 events (before 2/13/24 2:52:09.000 AM)

_time	POST
2020-03-25 02:00	4

Day 2: Monitoring and Analyzing Attacks

Dashboard Analysis: HTTP GET Method

Before:



New Search

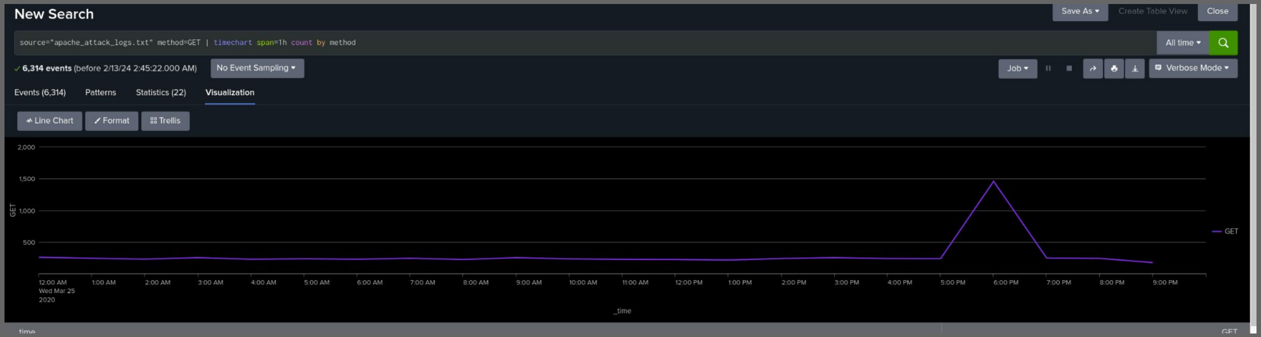
```
source="apache_logs.txt" method=GET | timechart span=1h count by method
```

✓ **9,851 events** (before 2/13/24 2:53:22.000 AM)

Events (9,851) Patterns Statistics (84) **Visualization**

_time	GET
2020-03-17 10:00	73

After:



New Search

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

✓ **6,314 events** (before 2/13/24 2:45:22.000 AM)

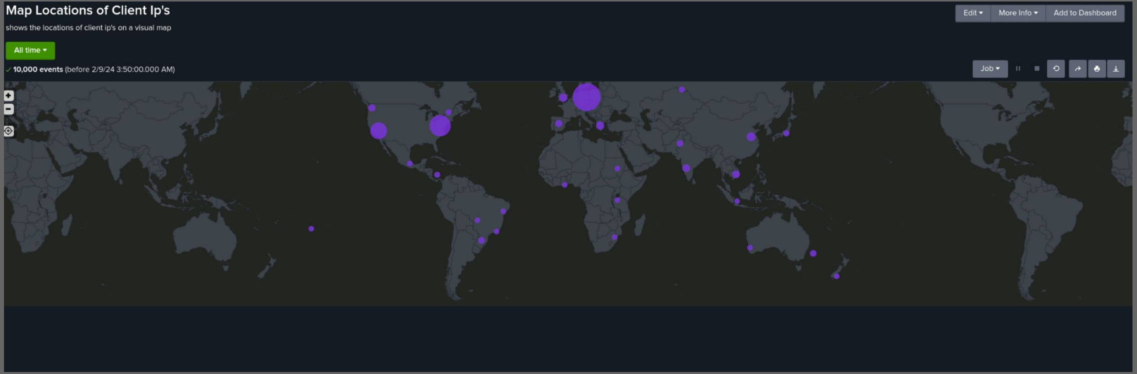
Events (6,314) Patterns Statistics (22) **Visualization**

_time	GET

Day 2: Monitoring and Analyzing Attacks

Dashboard Analysis: Cluster Map

Before:



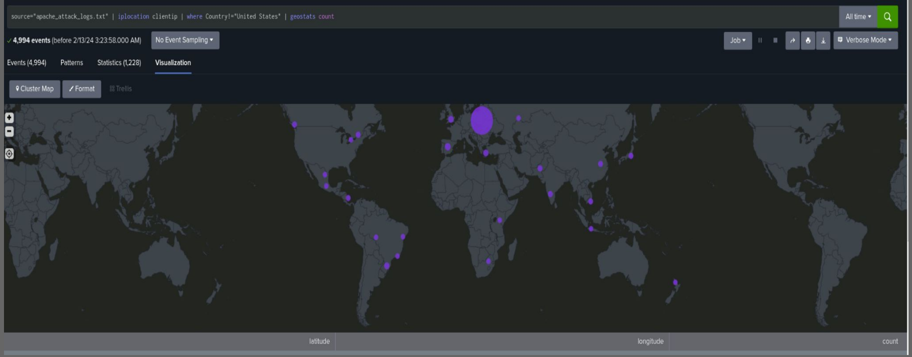
Map Locations of Client Ip's

shows the locations of client ip's on a visual map

All time ▾

✓ 10,000 events (before 2/9/24 3:50:00.000 AM)

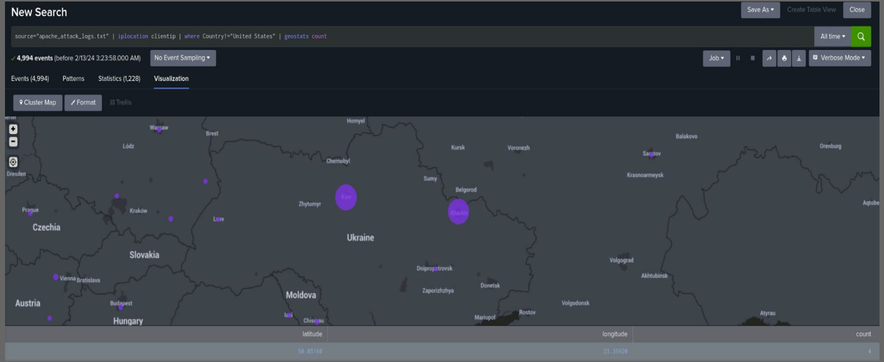
After:



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

✓ 4,994 events (before 2/13/24 3:23:58.000 AM)

latitude	longitude	count



New Search

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

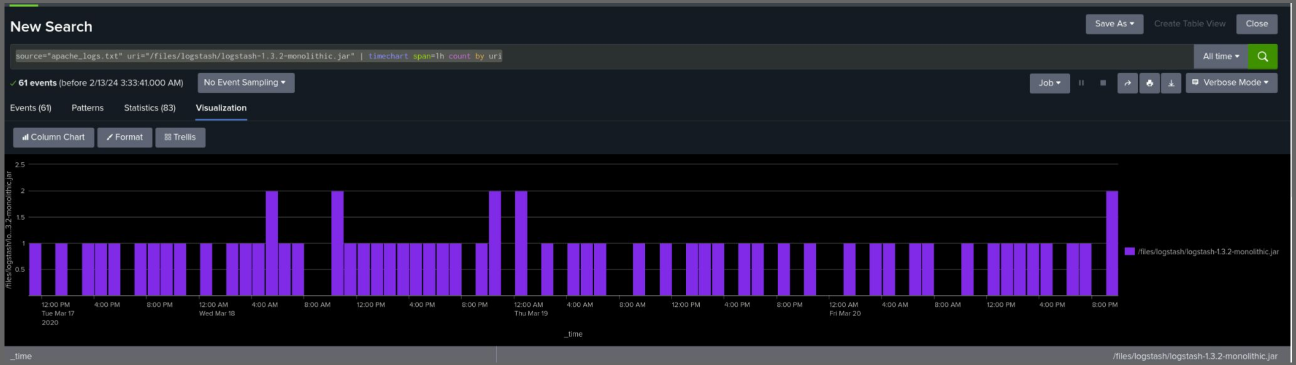
✓ 4,994 events (before 2/13/24 3:23:58.000 AM)

latitude	longitude	count
50.85160	23.35920	4

Day 2: Monitoring and Analyzing Attacks

Dashboard Analysis: Apache URI Data

Before:

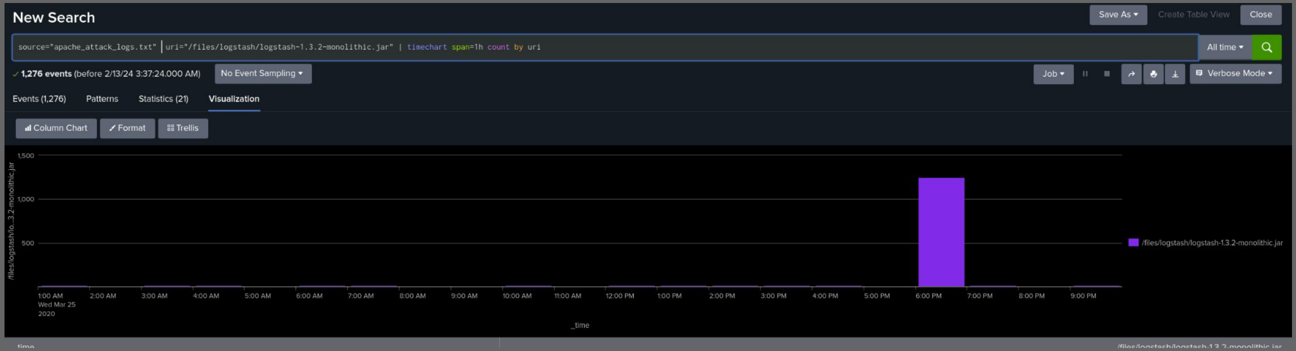


New Search

```
source="apache_logs.txt" uri="/files/logstash/logstash-1.3.2-monolithic.jar" | timechart span=1h count by uri
```

✓ 61 events (before 2/13/24 3:33:41.000 AM)

After:



New Search

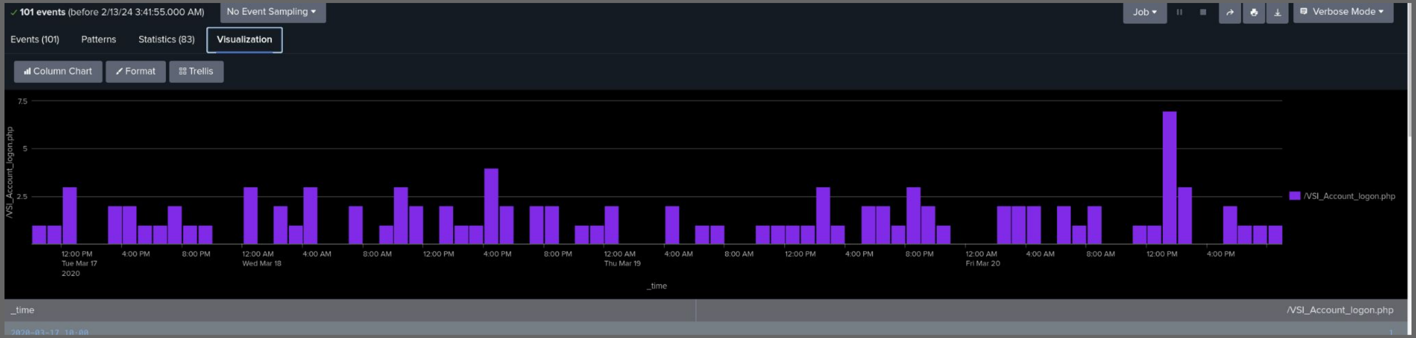
```
source="apache_attack_logs.txt" uri="/files/logstash/logstash-1.3.2-monolithic.jar" | timechart span=1h count by uri
```

✓ 1,276 events (before 2/13/24 3:37:24.000 AM)

Day 2: Monitoring and Analyzing Attacks

Dashboard Analysis: Apache URI Data

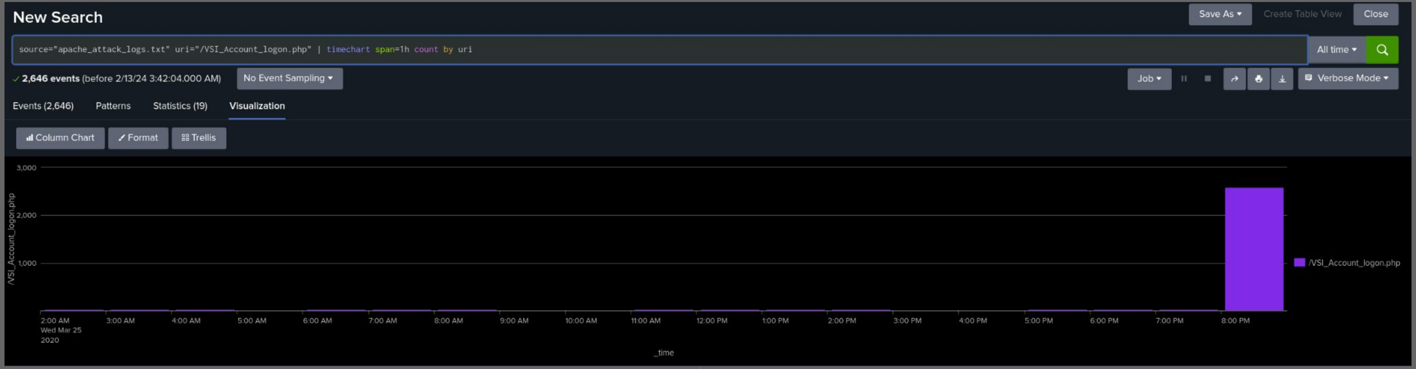
Before:



✓ **101 events** (before 2/13/24 3:41:55.000 AM)

_time	/VSI_Account_logon.php
2020-03-17 10:00	1

After:



New Search

```
source="apache_attack_logs.txt" uri="/VSI_Account_logon.php" | timechart span=1h count by uri
```

✓ **2,646 events** (before 2/13/24 3:42:04.000 AM)

Overview of Project 3

MILESTONES

Day 1

- Loaded and analyzed Windows Logs
- Created reports, alerts, and dashboards for the WIndows Logs
- Loaded and analyzed Apache Logs
- Created reports, alerts, and dashboards for Apache Logs
- Installed an add-on Splunk application for additional monitoring

Day 2

- Loaded Windows Attack Logs
- Analyzed Windows Attack Logs
- Loaded Apache Attack Logs
- Analyzed Apache attack Logs