

Solution Guide: Part 1 - Master of the SOC

Windows Server Logs

Reports: Design the following reports to assist VSI with quickly identifying specific information.

1. A report with a table of signatures with associated SignatureID.

○ **source="windows_server_logs.csv" | table signature signature_id | dedup signature**

New Search

Save As Create Table View Close

source="windows_server_logs.csv" | table signature signature_id | dedup signature

All time

4,764 events (before 7/28/21 6:38:07:000 PM) No Event Sampling

Job

Events (4,764) Patterns Statistics (15) Visualization

20 Per Page Format Preview

signature	signature_id
A user account was deleted	4726
A user account was created	4728
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	4748
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

Signatures with associated SignatureID

Edit More Info Add to Dashboard

A report with a table of signatures with associated SignatureID.

All time

4,764 events (before 7/28/21 6:38:07:000 PM)

Job

15 results 20 per page

signature	signature_id
A user account was deleted	4726
A user account was created	4728
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	4748
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

2. A report that provides the count and percent of the severity.
- **source="windows_server_logs.csv" | top severity**

New Search

Save AsCreate Table ViewClose

source="windows_server_logs.csv" | top severity

All time

✓ 4,764 events (before 7/28/21 6:47:12.000 PM) No Event SamplingJob

Events (4,764)PatternsStatistics (2)Visualization

20 Per PageFormatPreview

severity	count	percent
informational	4435	93.094039
high	329	6.905961

Top Severity

EditMore InfoAdd to Dashboard

A report that provides the count and percent of the severity.

All time

✓ 4,764 events (before 7/28/21 6:47:12.000 PM)Job

2 results20 per page

severity	count	percent
informational	4435	93.094039
high	329	6.905961

3. A report that provides a comparison between the success and failure of Windows activities.

- **source="windows_server_logs.csv" | top status**

New Search

Save AsCreate Table ViewClose

source="windows_server_logs.csv" | top status

All time

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

Events (4,764)PatternsStatistics (2)Visualization

20 Per PageFormatPreview

status	count	percent
success	4622	97.019312
failure	142	2.980688

Windows Activities Status

EditMore InfoAdd to Dashboard

A report that provides a comparison between the success and failure of Windows activities.

All time

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

2 results20 per page

status	count	percent
success	4622	97.019312
failure	142	2.980688

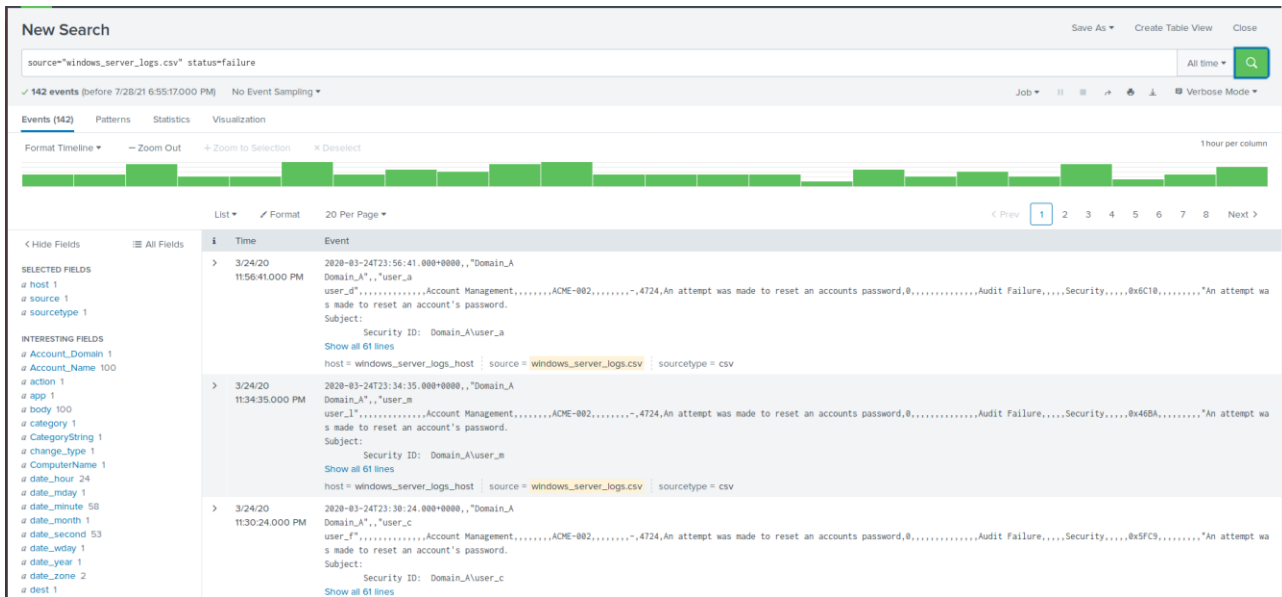
Ketan Vithal Patel

Page 2 of 22

Alerts: Design the following alerts to notify VSI of suspicious activity.

1. Determine an appropriate baseline and threshold for hourly level of failed Windows activity. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.

○ **source="windows_server_logs.csv" status=failure**



- The average activity per hour is approximately six events. The threshold is up to each group, but should be in the range of 15-25 to avoid false positives.
- To create alert, change the search to one hour
- Set to run every hour.
 - Set alert to trigger when count is greater than chosen threshold.
 - Add action Send email to SOC@VSI-company.com.

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](#)

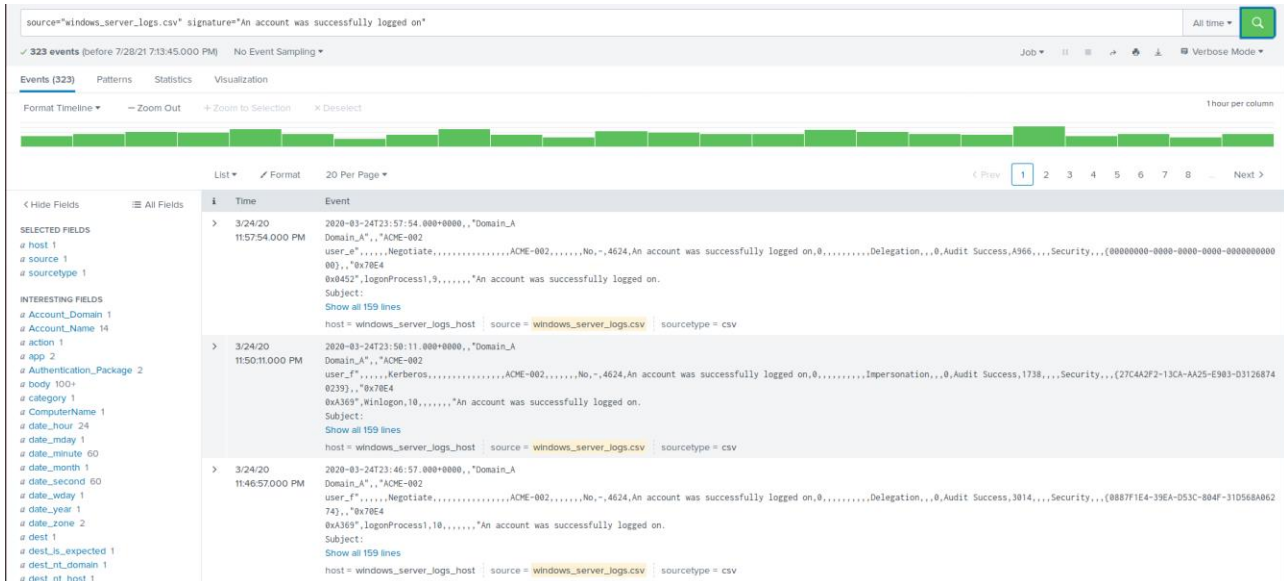
Actions: 1 Action [Edit](#)

[Send email](#)

There are no fired events for this alert.

2. Determine a baseline and threshold for hourly count of the signature an account was successfully logged on. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.

- **source="windows_server_logs.csv" signature="An account was successfully logged on"**



- The average activity per hour is approximately 12 events. The threshold is up to each group, but should be in the range of 30-50.
- To create alert, change the search to one hour and click Save As > Alert.
- Set to run every hour.
- Set alert to trigger when count is greater than chosen threshold.
- Add action Send email to SOC@VSI-company.com.

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](#)



There are no fired events for this alert.

- Determine a baseline and threshold for hourly count of the signature a user account was deleted. Design the alert based on the corresponding SignatureID. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.

○ [source="windows_server_logs.csv" signature_id=4726](#)

New Search Save As Create Table View Close

source="windows_server_logs.csv" signature_id=4726 All time Q

✓ 318 events (before 7/28/21 7:24:10.000 PM) No Event Sampling

Events (318) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 Next

Time	Event
3/24/20 11:59:54.000 PM	2828-83-24723:59:54.000+0000,,Domain_A Domain_A", "user_f user_1", "Account Management,,,,,ACME-002,,,,,4726,A user account was deleted,0,,,,,Audit Success,,,,Security,,,,0x4369,,,,,"A user account was deleted. Subject: Security ID: Domain_A/user_f Show all 63 lines host = windows_server_logs_host source = windows_server_logs.csv sourcetype = csv
3/24/20 11:51:52.000 PM	2828-83-24723:51:52.000+0000,,Domain_A Domain_A", "user_n user_m", "Account Management,,,,,ACME-002,,,,,4726,A user account was deleted,0,,,,,Audit Success,,,,Security,,,,0x4076,,,,,"A user account was deleted. Subject: Security ID: Domain_A/user_n Show all 63 lines host = windows_server_logs_host source = windows_server_logs.csv sourcetype = csv
3/24/20 11:39:15.000 PM	2828-83-24723:39:15.000+0000,,Domain_A Domain_A", "user_m user_1", "Account Management,,,,,ACME-002,,,,,4726,A user account was deleted,0,,,,,Audit Success,,,,Security,,,,0x468A,,,,,"A user account was deleted. Subject: Security ID: Domain_A/user_m Show all 63 lines host = windows_server_logs_host source = windows_server_logs.csv sourcetype = csv

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 1
a CategoryString 1
a change_type 1
a ComputerName 1
a date_hour 24
a date_minute 60
a date_month 1
a date_second 59
a date_wday 1
a date_year 1
a date_zone 2

- The average activity per hour is approximately 13 events.
- The threshold range should be between 30-50.
- To create alert, change the search to one hour and click Save As > Alert.
- Set to run every hour.
- Set alert to trigger when count is greater than chosen threshold.
- Add action Send email to SOC@VSI-company.com.

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](#)

i There are no fired events for this alert.

Visualizations and Dashboards: Design the following visualizations and add them to a dashboard called Windows Server Monitoring:

1. A line chart that displays the different `signature` field values over time.

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

New Search Save As Create Table View Close

source="windows_server_logs.csv" | timechart span=1h count by signature All time Q

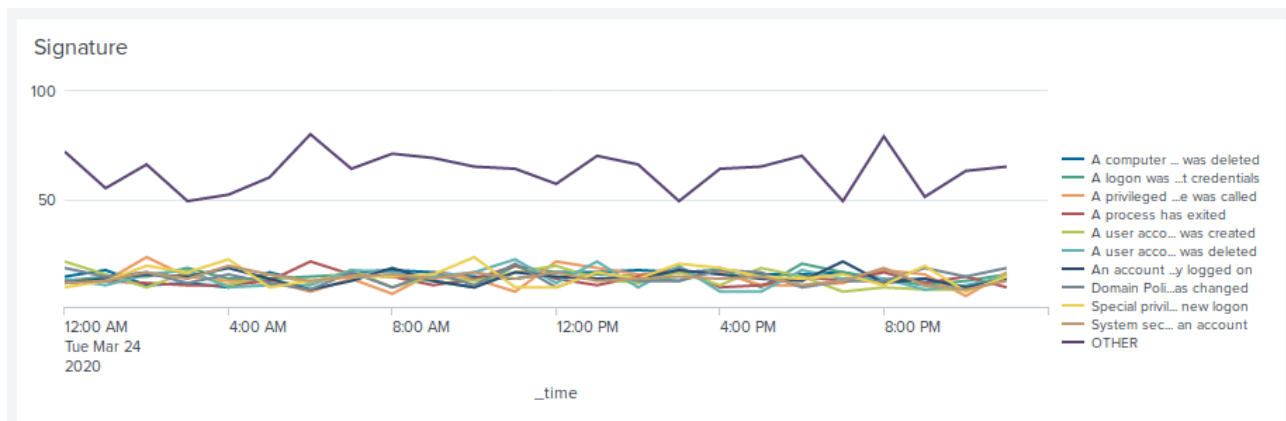
✓ 4,764 events (before 7/31/21 8:17:16.000 PM) No Event Sampling

Events (4,764) Patterns **Statistics (24)** Visualization

20 Per Page Format Preview Prev 1 2 Next

_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was created	A user account was deleted	An account was successfully logged on	Domain Policy was changed	Special privileges assigned to new logon	System security access was removed from an account	OTHER
2020-03-24 00:00	14	12	12	12	21	13	11	18	9	11	72
2020-03-24 01:00	17	14	12	12	15	10	13	14	12	12	55
2020-03-24 02:00	10	14	23	11	9	15	15	16	19	16	66
2020-03-24 03:00	11	18	14	10	16	17	14	11	16	13	49
2020-03-24 04:00	9	13	12	10	10	9	18	15	22	19	52
2020-03-24 05:00	16	13	12	12	15	10	13	11	9	15	60
2020-03-24 06:00	11	14	7	21	11	10	8	8	12	12	80
2020-03-24 07:00	16	15	13	15	17	17	12	16	14	14	64
2020-03-24 08:00	17	14	6	14	9	16	18	9	14	15	71
2020-03-24 09:00	16	12	16	10	14	14	12	16	15	13	69
2020-03-24 10:00	14	9	13	13	12	16	9	10	23	16	65
2020-03-24 11:00	13	19	7	19	16	22	16	20	9	13	64
2020-03-24 12:00	16	16	21	13	19	11	14	9	9	16	57
2020-03-24 13:00	16	15	18	10	13	21	13	16	16	12	70
2020-03-24 14:00	17	14	15	14	11	9	13	12	13	13	66

○ Select Visualizations > Line Chart.



2. A line chart that displays the different `user` field values over time.

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

New Search

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

4,764 events (before 7/31/21 8:20:40.000 PM)

No Event Sampling

Job

Verbose Mode

Events (4,764)

Patterns

Statistics (24)

Visualization

20 Per Page

Format

Preview

Prev

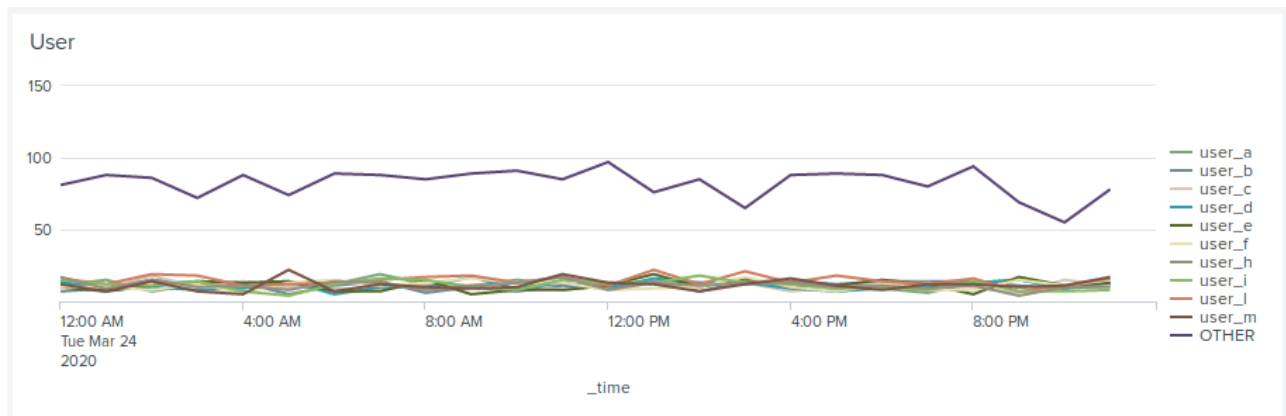
1

2

Next

_time	user_a	user_b	user_c	user_d	user_e	user_f	user_h	user_j	user_k	user_m	OTHER
2020-03-24 00:00	11	7	12	14	10	10	17	15	16	12	81
2020-03-24 01:00	15	9	9	8	7	10	9	12	12	7	88
2020-03-24 02:00	7	15	18	10	11	8	15	11	19	14	86
2020-03-24 03:00	12	12	10	8	14	12	10	14	18	7	72
2020-03-24 04:00	12	13	14	9	13	6	11	7	11	5	88
2020-03-24 05:00	10	5	10	14	14	13	8	4	12	22	74
2020-03-24 06:00	12	11	9	5	7	15	14	12	13	7	89
2020-03-24 07:00	19	14	8	10	7	11	13	16	15	12	88
2020-03-24 08:00	12	6	12	10	15	13	8	15	17	10	85
2020-03-24 09:00	11	10	11	17	5	16	11	10	18	9	89
2020-03-24 10:00	15	7	13	9	8	13	13	8	13	10	91
2020-03-24 11:00	12	11	8	13	8	13	17	15	17	19	85
2020-03-24 12:00	11	9	11	9	11	8	8	13	11	13	97
2020-03-24 13:00	13	14	13	16	19	9	13	13	22	12	76
2020-03-24 14:00	13	7	11	13	10	10	11	18	12	7	85
2020-03-24 15:00	12	14	13	13	16	17	13	13	21	12	60

- Select Visualizations > Line Chart.



4. A bar, column, or pie chart that illustrates the count of different users.

○ **source="windows_server_logs.csv" | top limit=10 user**

New Search Save As Create Table View Close

source="windows_server_logs.csv" | top limit=10 user All time Q

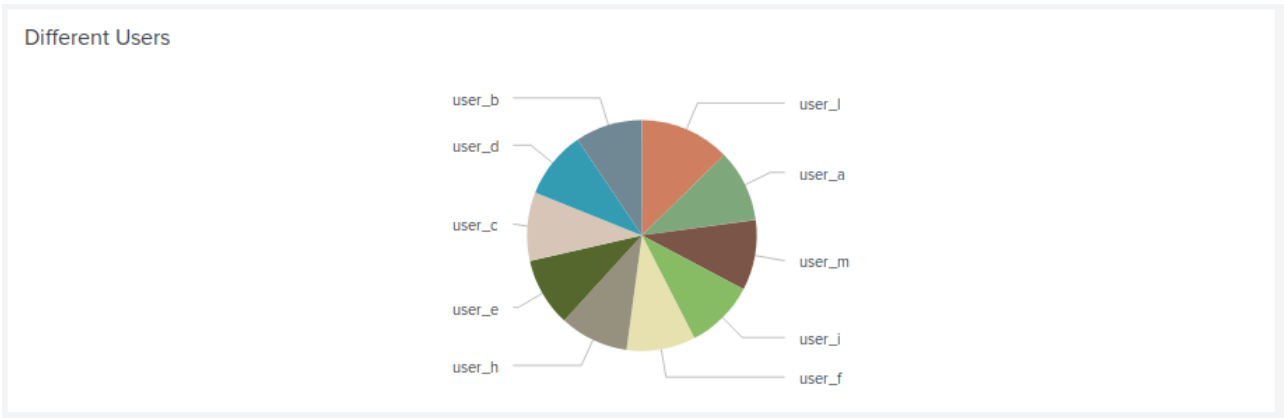
✓ 4,764 events (before 7/31/21 8:25:48.000 PM) No Event Sampling Job || → ⚙ ⬇ Verbose Mode

Events (4,764) Patterns **Statistics (10)** Visualization

20 Per Page Format Preview

user	count	percent
user_l	354	7.430730
user_a	282	5.919395
user_m	275	5.772460
user_i	271	5.688497
user_f	270	5.667506
user_h	269	5.646516
user_e	269	5.646516
user_c	267	5.604534
user_d	264	5.541562
user_b	263	5.520571

○ Select Visualizations > Bar/Column/Pie Chart.



5. A statistical chart that illustrates the count of different users.

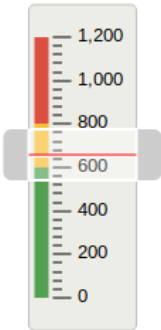
- `source="windows_server_logs.csv" | top limit=10 user`

Different Users Stats		
user	count	percent
user_l	354	7.430730
user_a	282	5.919395
user_m	275	5.772460
user_i	271	5.688497
user_f	270	5.667506
user_h	269	5.646516
user_e	269	5.646516
user_c	267	5.604534
user_d	264	5.541562
user_b	263	5.520571

6. One single value visualization of your choice: radial gauge, marker gauge, etc.

- Answers will vary.

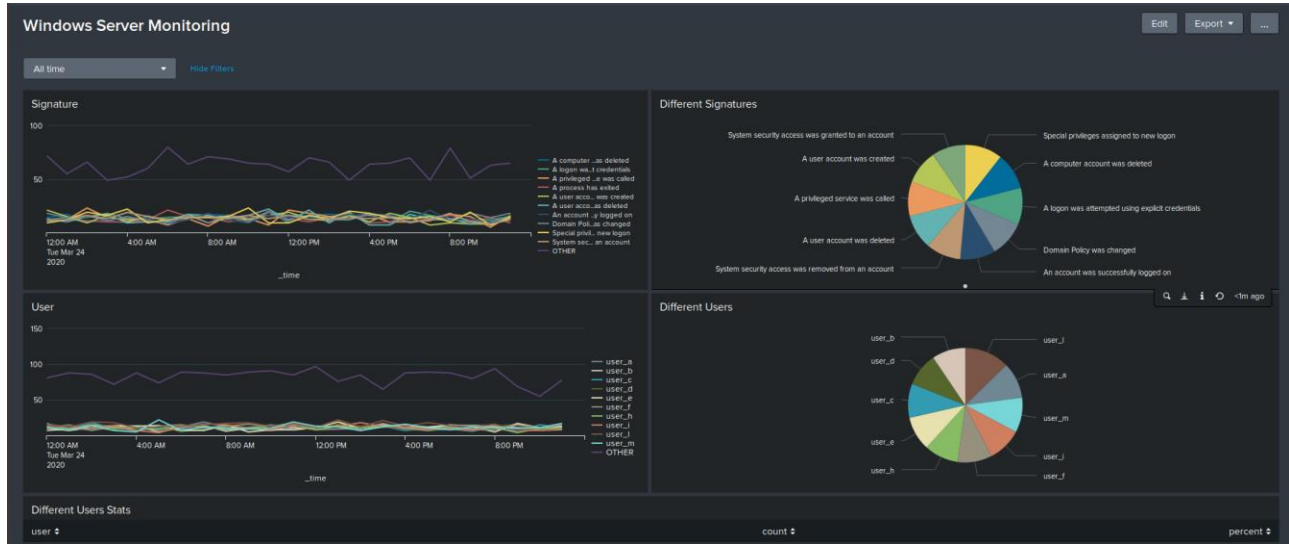
Action=Deleted



EventCode=4672



On your dashboard, add the ability to change the time range for all your visualizations.



Apache Web Server Logs

Reports: Design the following reports to assist VSI with quickly identifying specific information.

1. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc).

○ [source="apache_logs.txt" | top method](#)

New Search Save As Create Table View Close

source="apache_logs.txt" | top method All time Q

✓ 10,000 events (before 7/31/21 8:02:44.000 PM) No Event Sampling

Events (10,000) Patterns **Statistics (4)** Visualization

20 Per Page Format Preview

method	count	percent
GET	9851	98.510000
POST	186	1.860000
HEAD	42	0.420000
OPTIONS	1	0.010000

HTTP methods Edit More Info Add to Dashboard

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

All time

✓ 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	186	1.860000
HEAD	42	0.420000
OPTIONS	1	0.010000

- A report that shows the top 10 domains that referred to VSI's website.

○ [source="apache_logs.txt" | top limit=10 referer_domain](#)

New Search Save As Create Table View Close

source="apache_logs.txt" | top limit=10 referer_domain All time Q

✓ 10,000 events (before 7/31/21 8:06:47.000 PM) No Event Sampling

Events (10,000) Patterns **Statistics (10)** Visualization

20 Per Page Format Preview

referer_domain	count	percent
http://www.semicomplete.com	3838	51.256960
http://semicomplete.com	2901	33.760756
http://www.google.com	123	2.075249
https://www.google.com	185	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

Top 10 Domains			Edit More Info Add to Dashboard
The top 10 domains that referred to VSZ's website.			
All time			
✓ 10,000 events (before 7/31/21 8:06:47:000 PM)			Job ↶ ↷
10 results 20 per page			
referer_domain	count	percent	
http://www.semicomplete.com	3038	51.256960	
http://semicomplete.com	2001	33.768756	
http://www.google.com	123	2.075249	
https://www.google.com	185	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	

2. A report that shows the count of the HTTP response codes.
- `source="apache_logs.txt" | top status`

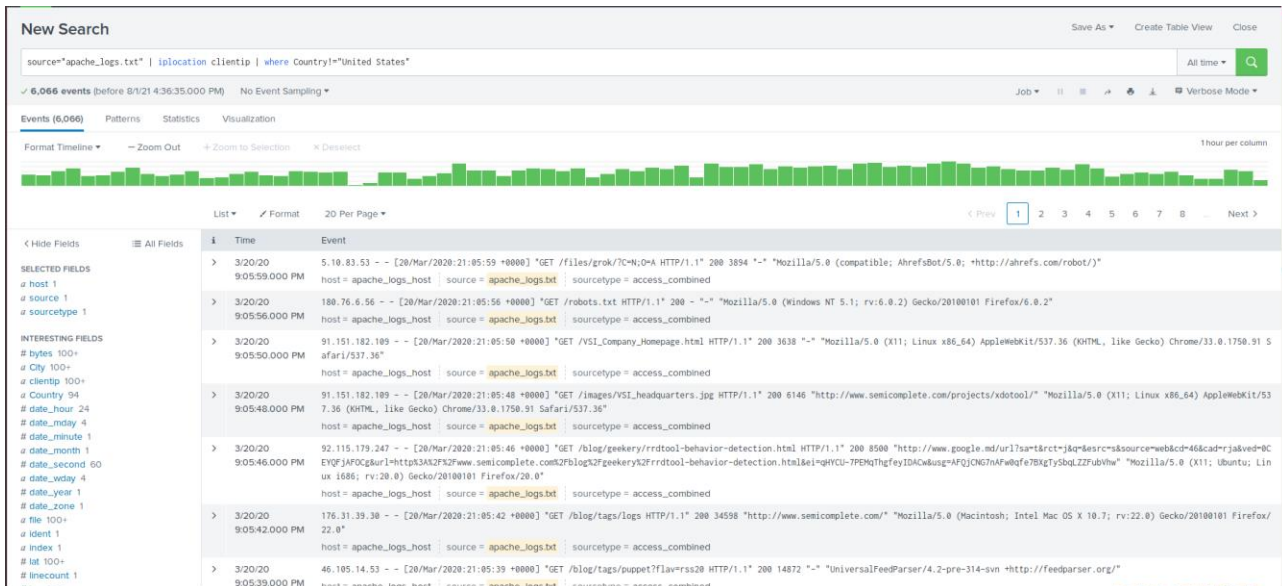
New Search			Save As Create Table View Close
<input type="text" value="source='apache_logs.txt' top status"/>			All time Q
✓ 10,000 events (before 8/1/21 4:32:50.000 PM) No Event Sampling			Job ↶ ↷ ⬇ ⬆ Verbose Mode
Events (10,000)	Patterns	Statistics (8)	Visualization
20 Per Page	Format	Preview	
status	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			Edit More Info Add to Dashboard
Count of the HTTP response codes			
All time			
✓ 10,000 events (before 8/1/21 4:32:50.000 PM)			Job ↶ ↷
8 results 20 per page			
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	

Alerts: Design the following alerts:

1. Determine a baseline and threshold for hourly count of activity from a country other than the United States. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.

○ **source="apache_logs.txt" | iplocation clientip | where Country!="United States"**



- The average activity per hour is approximately 80.
- The threshold should range between 170-250.
- To create an alert, change the search to one hour.
- Set to run every hour.
- Set alert to trigger when count is greater than chosen threshold.
- Add action Send email to SOC@VSI-company.com.

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: [v](#) 1 Action [Edit](#)

[✉](#) Send email



There are no fired events for this alert.

2. Determine a baseline and threshold for hourly count of the HTTP POST method. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.

- **source="apache_logs.txt" method=POST**



- The average activity per hour is approximately two.
- The threshold should be between 12-20.
- To create an alert, change the search to one hour.
- Set to run every hour.
- Set alert to trigger when count is greater than chosen threshold.
- Add action Send email to SOC@VSI-company.com.

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

i There are no fired events for this alert.

Visualizations and Dashboards: Design the following visualization and add them to a dashboard called Apache WebServer Monitoring.

1. A line chart that displays the different HTTP `methods` field over time.

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

New Search Save As Create Table View Close

source="apache_logs.txt" | timechart span=1h count by method All time Q

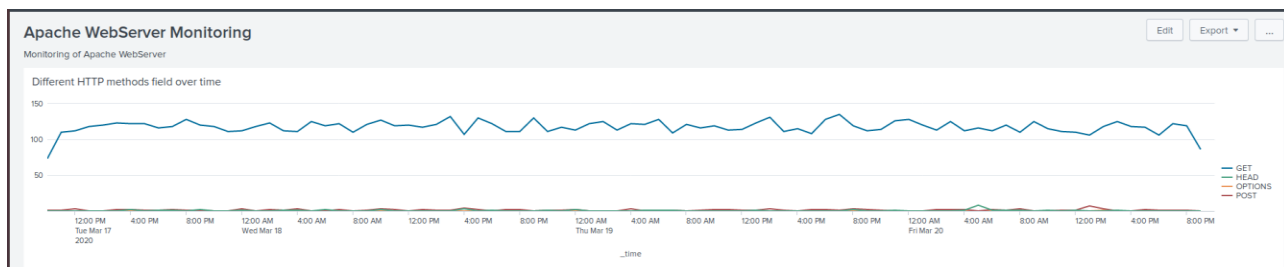
✓ 10,000 events (before 8/1/21 7:01:22.000 PM) No Event Sampling

Events (10,000) Patterns **Statistics (84)** Visualization

20 Per Page Format Preview Prev 1 2 3 4 5 Next

_time	GET	HEAD	OPTIONS	POST
2020-03-17 10:00	73	0	0	1
2020-03-17 11:00	110	0	0	1
2020-03-17 12:00	112	0	0	3
2020-03-17 13:00	118	0	0	0
2020-03-17 14:00	120	0	0	0
2020-03-17 15:00	123	0	0	2
2020-03-17 16:00	122	2	0	2
2020-03-17 17:00	122	0	0	1
2020-03-17 18:00	116	1	0	1
2020-03-17 19:00	118	1	0	2
2020-03-17 20:00	128	0	0	1
2020-03-17 21:00	120	2	0	1
2020-03-17 22:00	118	0	0	0
2020-03-17 23:00	111	0	0	0
2020-03-18 00:00	112	1	0	3
2020-03-18 01:00	118	0	0	0

- Select Visualizations > Line Chart.

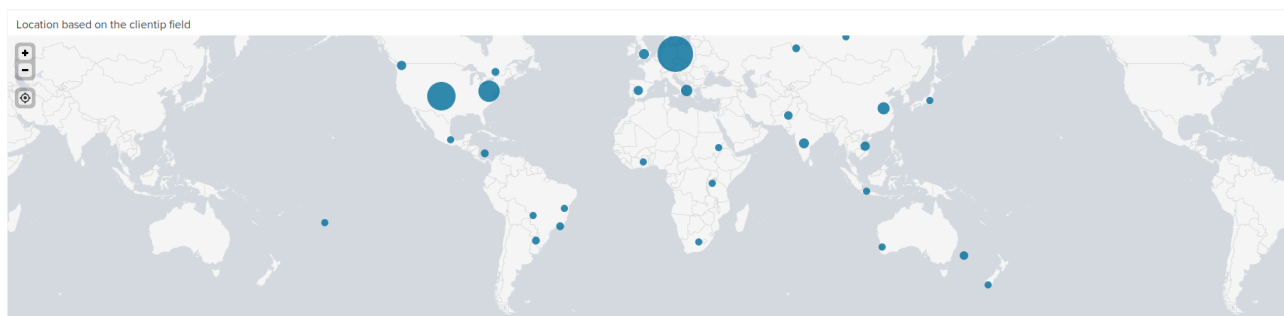


2. A geographical map showing the location based on the `clientip` field.

- `source="apache_logs.txt" | iplocation clientip | geostats count`

[illegible]

- Select Visualizations > Line Chart.



3. A bar, column, or pie chart that displays the count of different URIs.

- `source="apache_logs.txt" | top limit=10 uri`

New Search Save As Create Table View Close

source="apache_logs.txt" | top limit=10 uri All time 🔍

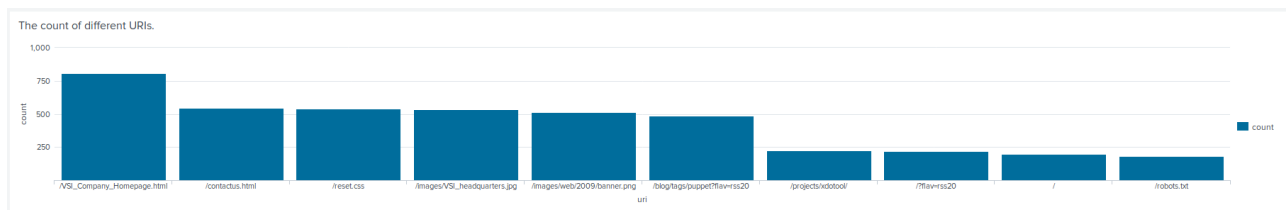
✓ 10,000 events (before 8/1/21 7:13:26.000 PM) No Event Sampling Job || → 📄 📄 Verbose Mode

Events (10,000) Patterns Statistics (10) Visualization

20 Per Page Format Preview

uri	count	percent
/VSI_Company_Homepage.html	887	8.870000
/contactus.html	546	5.460000
/reset.css	538	5.380000
/images/VSI_headquarters.jpg	533	5.330000
/images/web/2009/banner.png	516	5.160000
/blog/tags/puppet?flav=rss20	488	4.880000
/projects/xdotool/	224	2.240000
/?flav=rss20	217	2.170000
/	197	1.970000
/robots.txt	188	1.880000

- Select Visualizations > Bar/Column/Pie Chart.

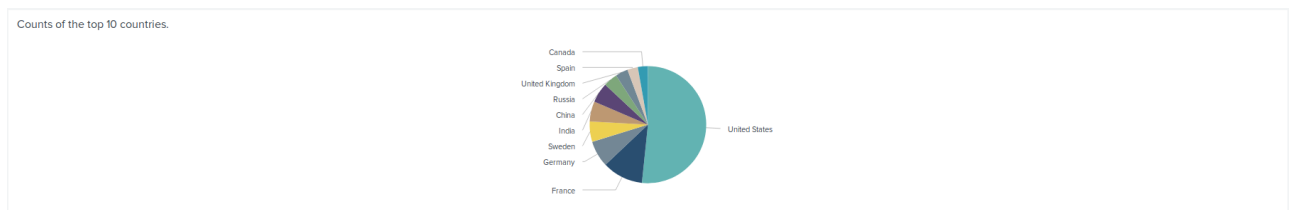


4. A bar, column, or pie chart that displays the counts of the top 10 countries.

- **source="apache_logs.txt" | iplocation clientip | top limit=10 Country**

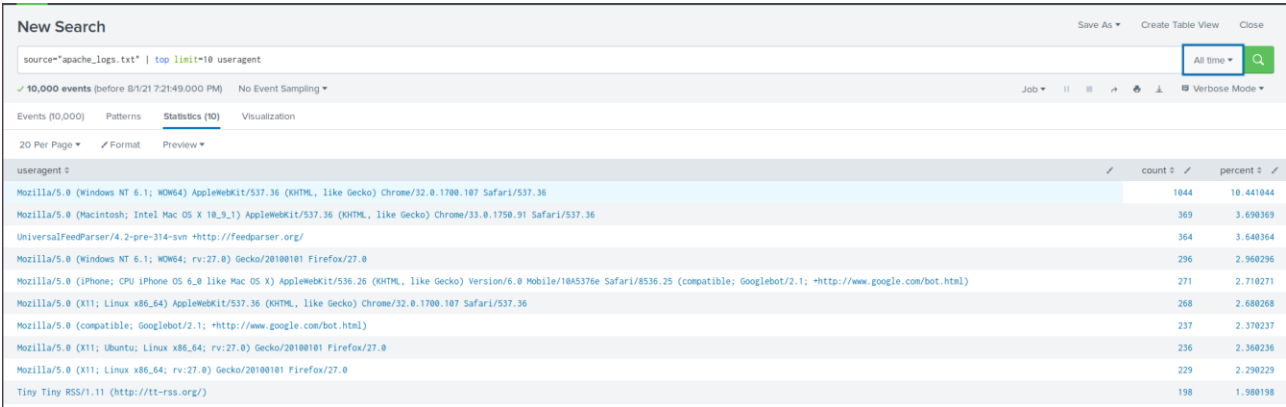
New Search			
source="apache_logs.txt" iplocation clientip top limit=10 Country			
✓ 10,000 events (before 8/3/21 7:19:28.000 PM) No Event Sampling			
Events (10,000) Patterns Statistics (10) Visualization			
20 Per Page Format Preview			
Country	count	percent	
United States	3934	39.340000	
France	863	8.630000	
Germany	553	5.530000	
Sweden	429	4.290000	
India	422	4.220000	
China	418	4.180000	
Russia	298	2.980000	
United Kingdom	264	2.640000	
Spain	222	2.220000	
Canada	212	2.120000	

- Select Visualizations > Bar/Column/Pie Chart.



5. A statistical chart that illustrates the count of different user agents.

- **source="apache_logs.txt" | top limit=10 useragent**



- Click the following: Save As > Dashboard Panel > Existing > Apache WebServer Monitoring > Create Title for Panel > Save as Statistics Table

The count 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	1844	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

6. One single value visualization of your choice: radial gauge, marker gauge, etc.

New Search

source="apache_logs.txt" method="GET" | stats count as total

✓ 9,851 events (before 8/1/21 7:36:18.000 PM)

No Event Sampling ▾

Events (9,851)

Patterns

Statistics (1)

Visualization

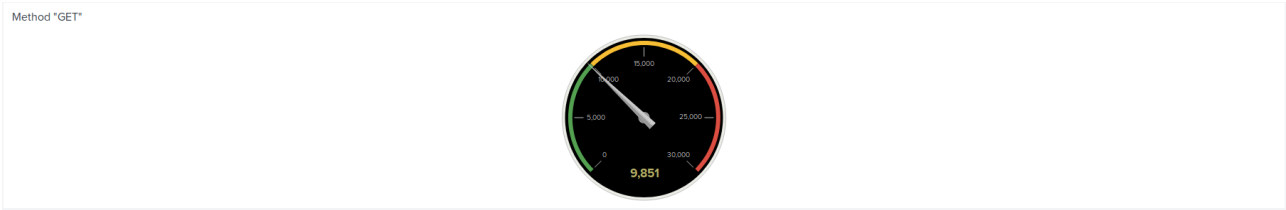
20 Per Page ▾

✎ Format

Preview ▾

total ↕

9851



New Search

source="apache_logs.txt" status="404" | stats count as total

✓ 213 events (before 8/1/21 7:47:44.000 PM)

No Event Sampling ▾

Events (213)

Patterns

Statistics (1)

Visualization

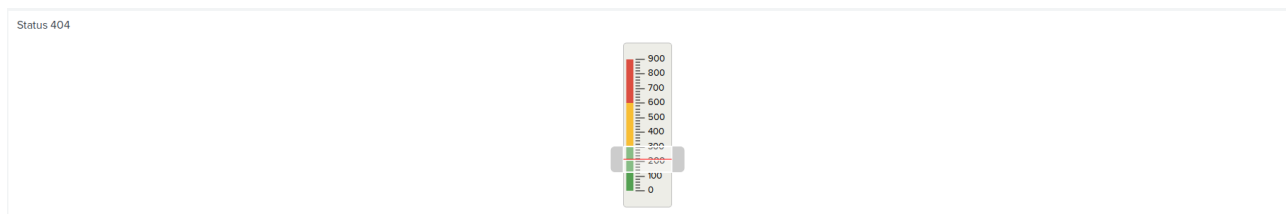
20 Per Page ▾

✎ Format

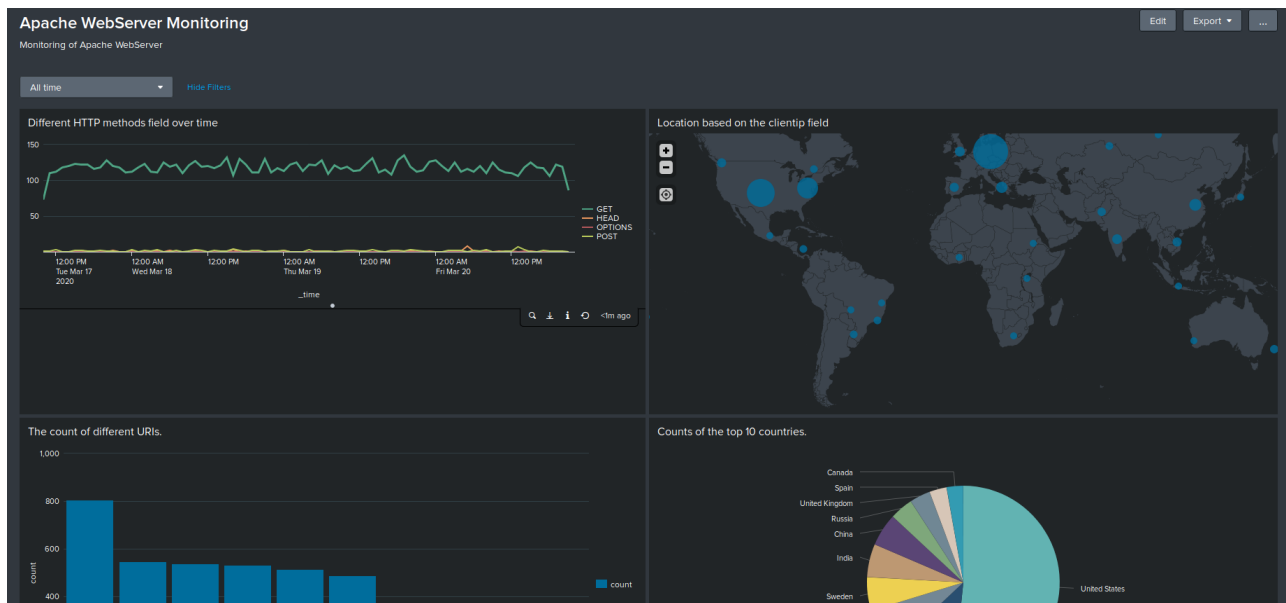
Preview ▾

total ↕

213



On your dashboard, add the ability to change the time range for all your visualizations.



© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.