



Defensive Security Project

by: Jordan, Eric, Jaz, Franc, & Joel

Table of Contents

This document contains the following resources:

01

**Monitoring
Environment**

02

Attack Analysis

03

**Project Summary
& Future
Mitigations**

Monitoring Environment

Scenario

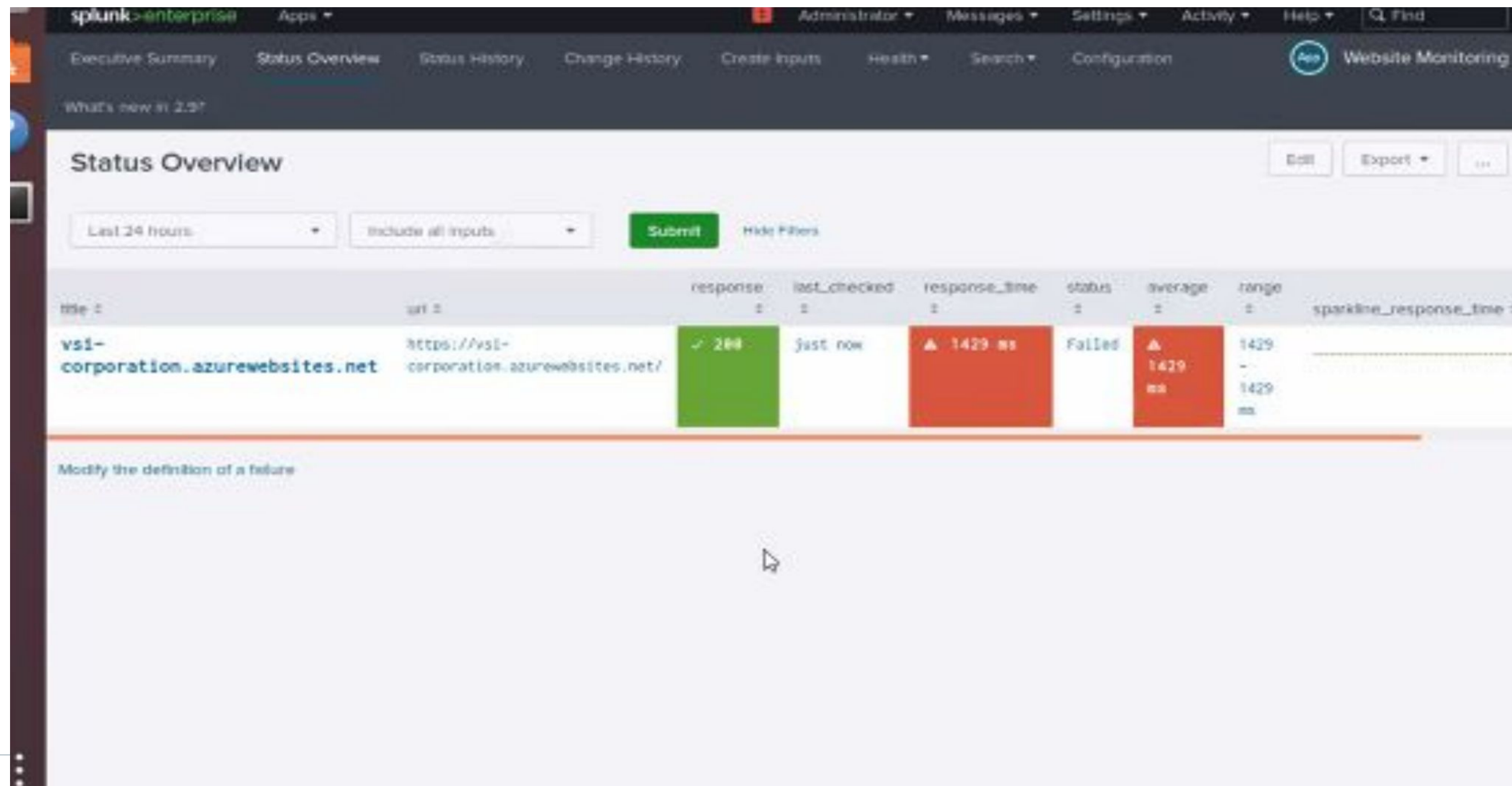
- We are employed at a small company called Virtual Space Industries (VSI) as SOC Analysts
- There are rumors that a competitor might disrupt our business
- We are tasked with using SPLUNK against to monitor against our potential attacks

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and squares, creating a mosaic-like effect.

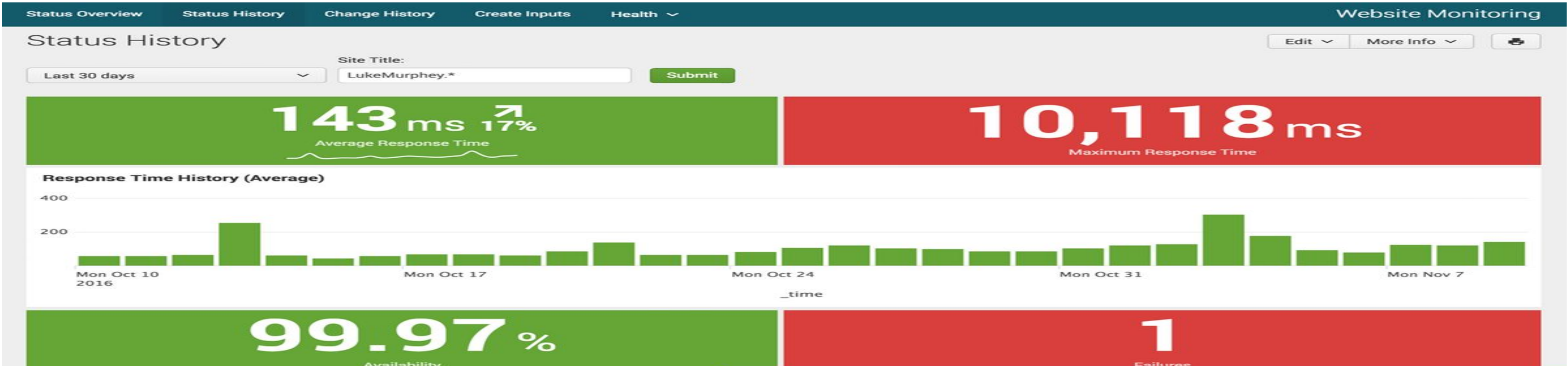
“Add-On” App WEBSITE MONITORING

Website Monitoring

- Monitor websites to detect downtime and performance issues
- You can define the websites you would like to monitor
- This app uses a modular input that can easily be set up in minutes.
- This add-on will help check the availability, performance, and function of a website or web service.



Website Monitoring



Status OverviewStatus HistoryChange HistoryCreate InputsHealth Website Monitoring

Change History

Last 24 hours

Site Title: *

Submit

Change History

	title	url	changed	since_last_changed	last_observed	count
1	Answers.Splunk.com	http://answers.splunk.com/	11/09/2016 16:07:53	4 minutes ago	11/09/2016 16:07:53	1
2	Splunk.com	http://splunk.com	11/09/2016 16:07:47	4 minutes ago	11/09/2016 16:07:47	1
3	LukeMurphey.net	http://LukeMurphey.net	11/09/2016 15:53:01	18 minutes ago	11/09/2016 15:53:01	1
4	LukeMurphey.com	http://LukeMurphey.com	11/09/2016 15:52:55	19 minutes ago	11/09/2016 15:52:55	1
5	Blogs.Splunk.com	http://blogs.splunk.com	11/09/2016 15:52:55	19 minutes ago	11/09/2016 16:07:57	2
6	Answers.Splunk.com	http://answers.splunk.com/	11/09/2016 15:52:51	19 minutes ago	11/09/2016 15:52:51	1
7	Answers.Splunk.com	http://answers.splunk.com/	11/09/2016 15:38:26	33 minutes ago	11/09/2016 15:38:26	1
8	Blogs.Splunk.com	http://blogs.splunk.com	11/09/2016 15:38:25	33 minutes ago	11/09/2016 15:38:25	1
9	LukeMurphey.com	http://LukeMurphey.com	11/09/2016 15:22:59	49 minutes ago	11/09/2016 15:22:59	1
10	LukeMurphey.net	http://LukeMurphey.net	11/09/2016 15:22:58	49 minutes ago	11/09/2016 15:22:58	1

« prev

12345678910

next »

Website Monitoring

Why would web monitoring be important?

- 1. To avoid losing money/customers**
- 2. To safeguard your content and data**
- 3. To identify problems with your site or hosting**
- 4. To understand how visitors are interacting with your website**

Logs Analyzed

1

Windows Logs

Signature_ID

Signature

User

Status

Severity

2

Apache Logs

IP Addresses

Https

Windows Logs

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	level of failed Windows activity	7	failed logins is > 10

JUSTIFICATION: The average was about 7 failed logins so we decided more than 10 failed log ins would trigger an alert.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful logins Alert	when a user account successfully logged on	10	Successful logins is >15

JUSTIFICATION: With a baseline of 10 successful logins per hour, we added an alert that would trigger with a threshold of 15 successful logins.

Images of Reports—Windows

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Reporting

Save

Save As

View

Create Table View

Close

source="windows_server_attack_logs.csv" host="windows_server_attack_logs.csv" sourcetype="csv" | stats count by status

All time

17,844 events (before 3/10/23 12:16:14.000 AM)

No Event Sampling

Job

Verbose Mode

Events (17,844)

Patterns

Statistics (2)

Visualization

20 Per Page

Format

Preview

status	count
failure	279
success	17562

Activities

Google Chrome

Mon 20:55

Splunkbase | Apps

Thank You for Download

Search | Splunk 9.0.4

127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D"windows_server_logs.csv" host%3D"windows_server_logs" sourcetype="csv" | stats count by status

Update

< Hide Fields

All Fields

20 Per Page

signature

15 Values, 100% of events

Selected Yes No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values

Count

%

Special privileges assigned to new logon	342	7.179%
A computer account was deleted	340	7.137%
A logon was attempted using explicit credentials	337	7.074%
Domain Policy was changed	329	6.906%
An account was successfully logged on	323	6.78%
System security access was removed from an account	321	6.738%
A user account was deleted	318	6.675%
A privileged service was called	317	6.654%
A user account was created	313	6.57%
A process has exited	309	6.486%

127.0.0.1:8000/en-US/app/search/search?q=search source%3D"windows_server_logs.csv" host%3D"windows_server_logs" sourcetype="csv" | stats count by status

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User account deletion	when deleted account users are greater than 20	11	>20

JUSTIFICATION: The baseline showed an average of 11 user accounts deleted, so the threshold of 20 user account deletions will trigger the alert.

Dashboards—Windows

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

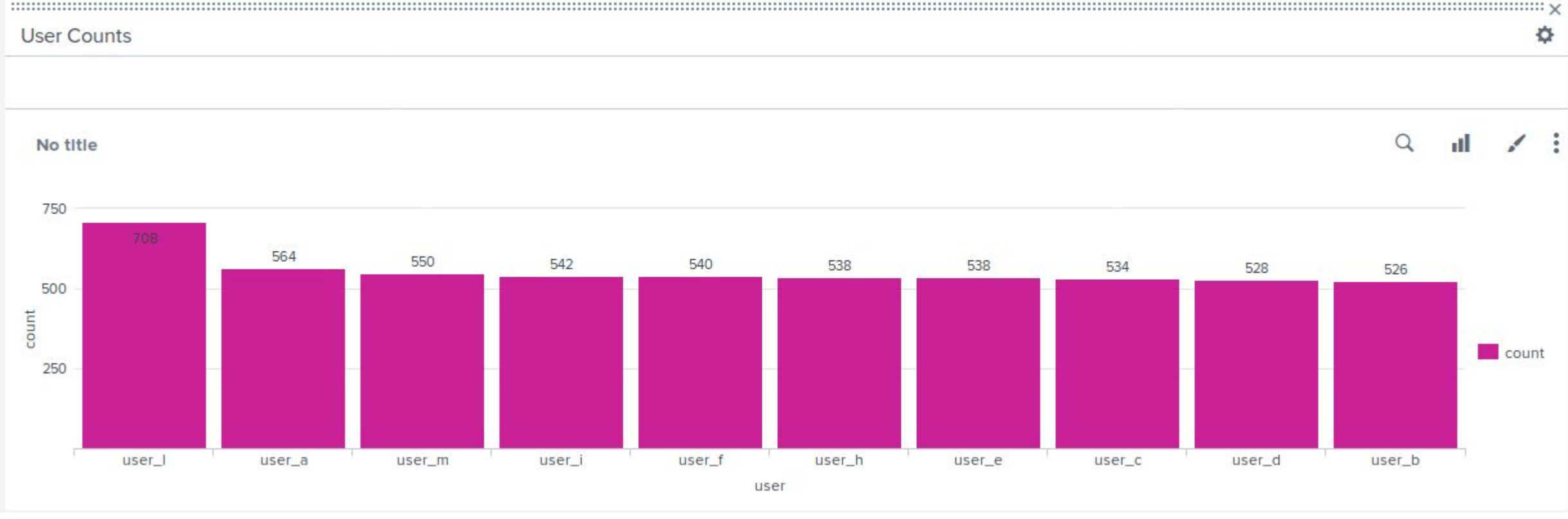
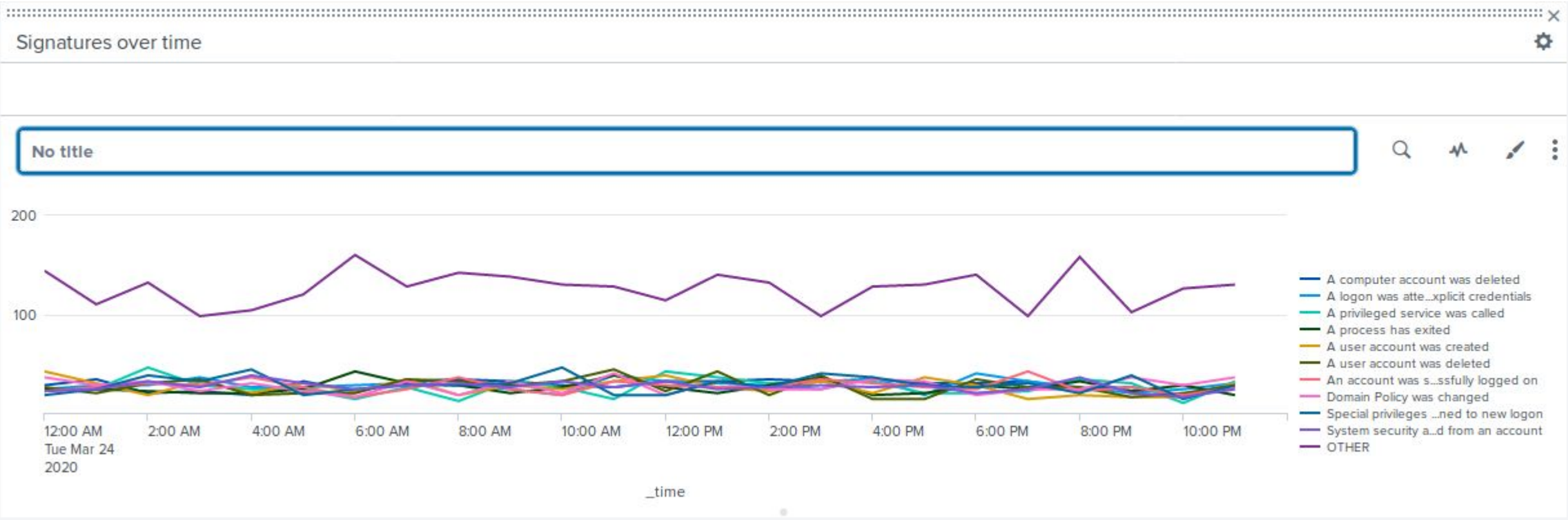
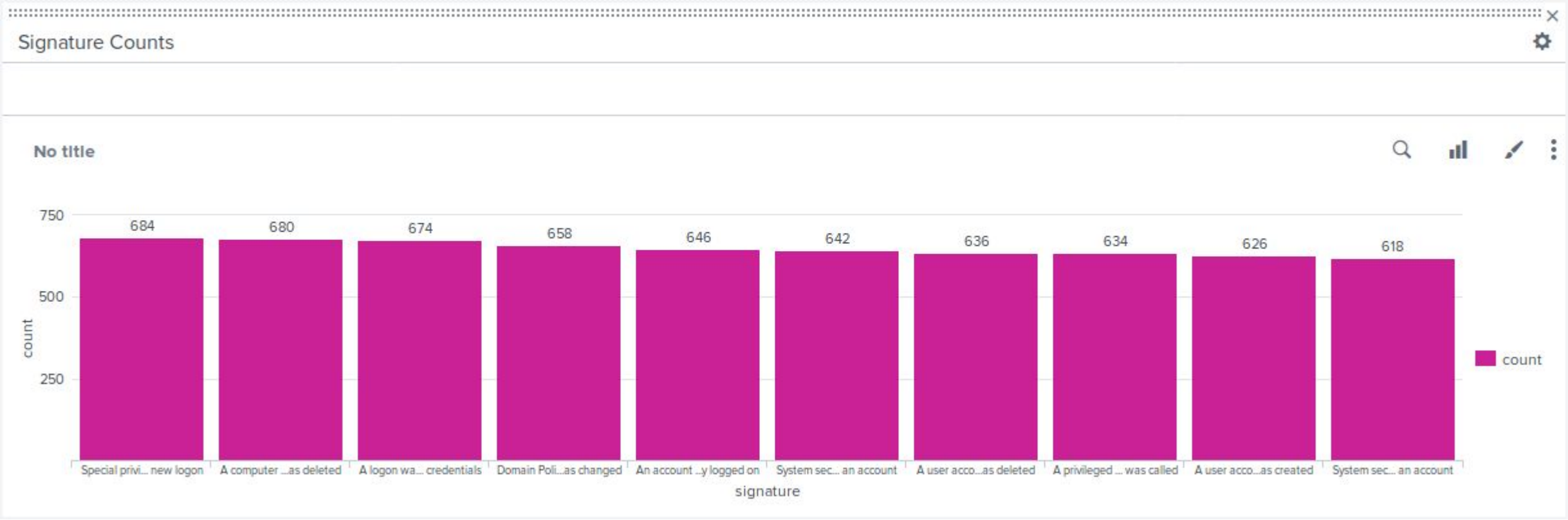
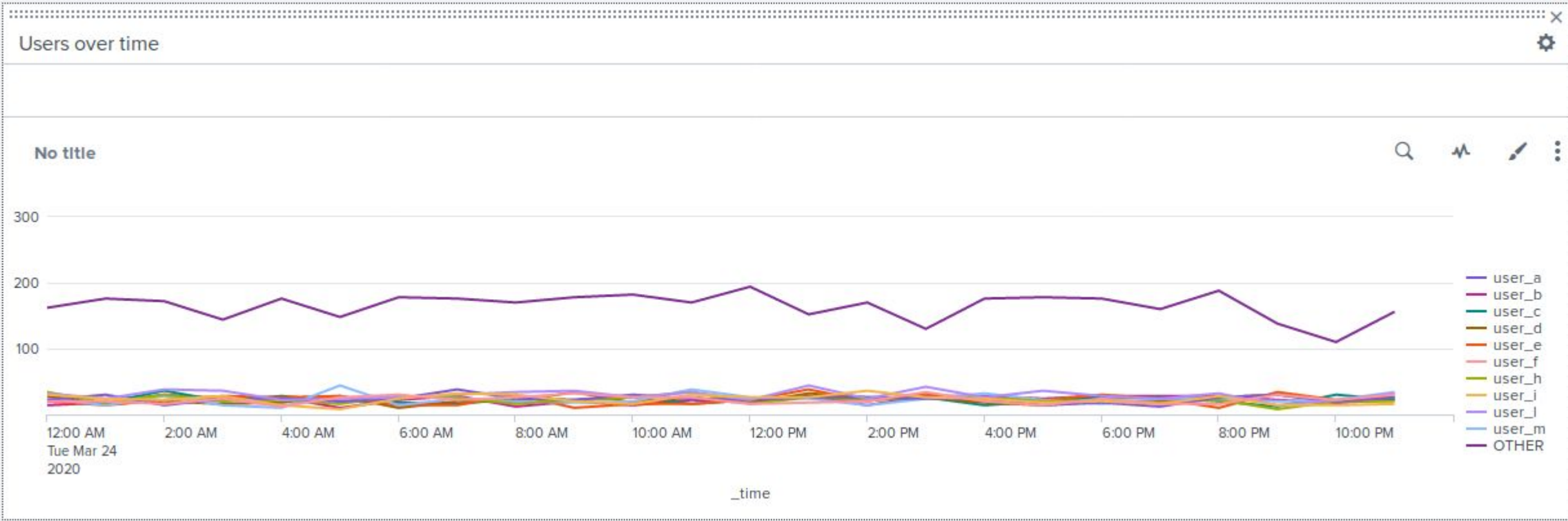
> Search & Reporting

Failed hourly threshold metEdit

Enabled: Yes.DisableTrigger Condition: Number of Results is > 40.EditApp: searchActions: 1 Action EditPermissions: Private. Owned by admin.EditModified: Mar 8, 2023 7:30:19 PMAlert Type: Scheduled. Hourly, at 0 minutes past the hour.Edit

There are no fired events for this alert.

Dashboard - Windows



Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
Apache HTTP Methods	Provides insight into the type of HTTP activity that is being requested against VSI’s web server
Apache Top 10 Domains	Highlights the top ten domains that refer to VSI’s website
Apache Total Response Codes	Highlights the total number of each response code, and can help with analyzing for suspicious levels of HTTP responses

Images of Reports—Apache

The screenshot shows the Splunk web interface in a Mozilla Firefox browser. The page title is 'Apache_log_Report_Methods | Splunk 9.0.4 - Mozilla Firefox'. The browser address bar shows the URL 'localhost:8000/en-US/app/search/report?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2F...'. The Splunk navigation bar includes 'splunk>enterprise', 'Apps', and a user profile 'Administrator'. The main navigation menu has 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search & Reporting' section is active, showing the report 'Apache_log_Report_Methods'. A green button indicates 'All time' and a status bar shows '10,000 events (before 3/10/23 1:00:58.000 AM)'. The report shows 4 results with 20 per page. The data is as follows:

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

Apache_logs_Report_Top10Domains | Splunk 9.0.4 - Mozilla Firefox

Apache_logs_Report_Top10Domains X +

localhost:8000/en-US/app/search/report?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2F

...

🔒

☆

📑

📄

🌐

☰

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Apache_logs_Report_Top10Domains

Edit More Info Add to Dashboard

All time

✓ 10,000 events (before 3/9/23 10:49:29.000 PM)

Job || ⏏ ↺ ↻ 🖨 ⬇

10 results 20 per page

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

Apache_logs_Report_ResponseCodes | Splunk 9.0.4 - Mozilla Firefox

Apache_logs_Report_Re X

+

←

→

↺

🏠

localhost:8000/en-US/app/search/report?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2F

⋮

🔒

☆

📖

📄

👤

☰

splunk>enterprise

Apps ▾

⚠

Administrator ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

🔍 Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

➤

Search & Reporting

Apache_logs_Report_ResponseCodes

Edit ▾

More Info ▾

Add to Dashboard

All time ▾

✓ 10,000 events (before 3/9/23 10:52:43.000 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

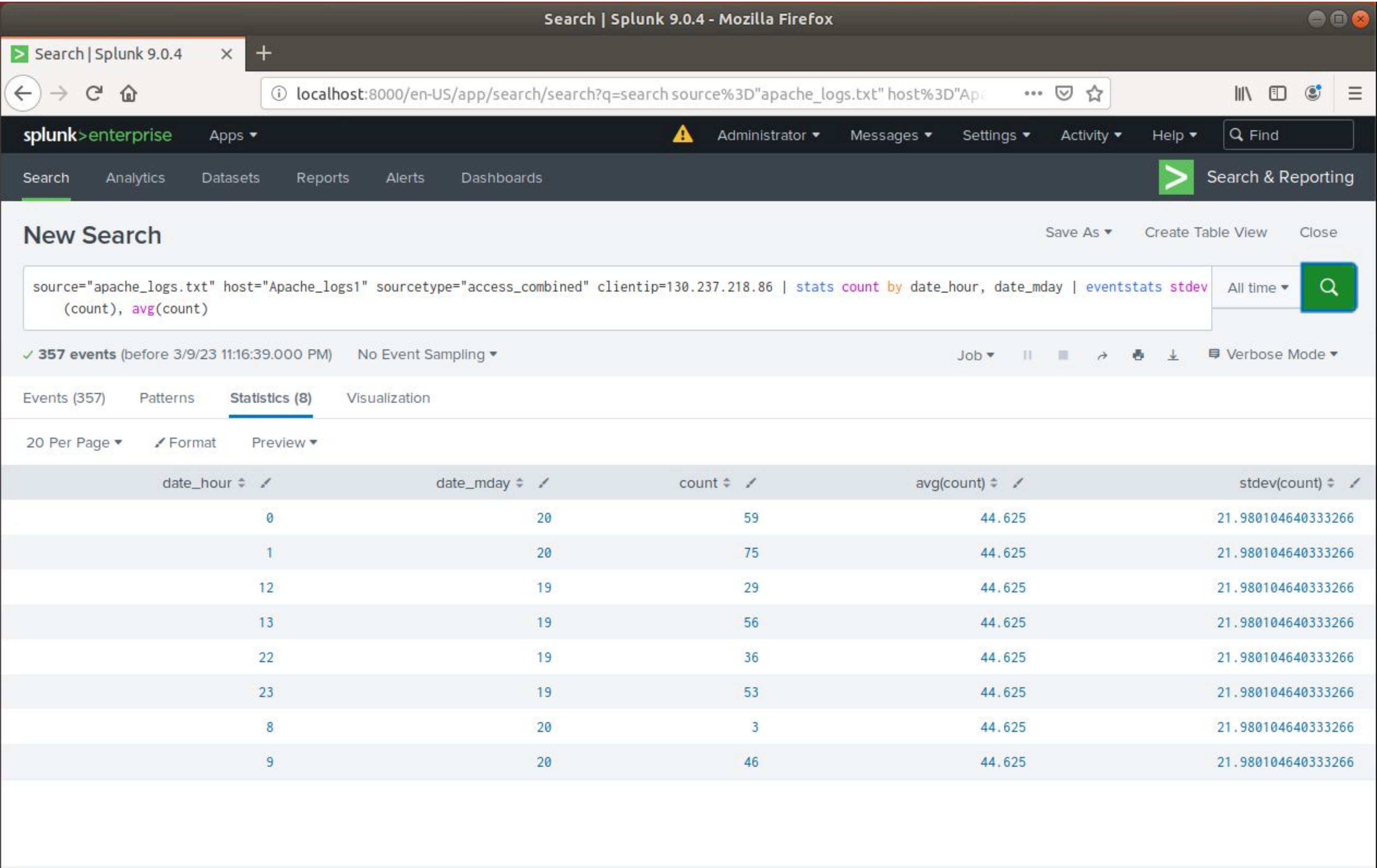
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache Logs on ClientIP-Germany	This alert is triggered when the hourly activity in Germany surpasses the threshold	~44	>88

Justification: The normal activity showed us hourly activity in Germany ranging from 3 to 75 with an average baseline of 44. We decided to set the threshold at 88 because with the standard deviation at 21.9 we doubled the standard deviation (~44) and added it to the baseline (~44).

Germany Hourly Activity Alert



Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Logs on POST Method	When the amount of POST request exceed the count of threshold (11) we will send an alert email to SOC management whenever the hourly rate is exceeded.	5	>11

Justification: With the baseline being at 5 and our threshold being at 11 the alert would've been triggered. I got 11 for my threshold with standard deviation of my baseline number(5) and that number was 12. With that I chose 11 to be my threshold because I felt that 12 was to much of a risk.

splunk>enterprise

Apps ▾

Administrator ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

> Search & Reporting

Apache Logs Method Post

Edit

Ubuntu Software

App: search

Permissions: Private. Owned by admin. Edit

Modified: Mar 14, 2023 3:22:19 AM

Alert Type: Scheduled. Hourly, at 30 minutes past the hour. Edit

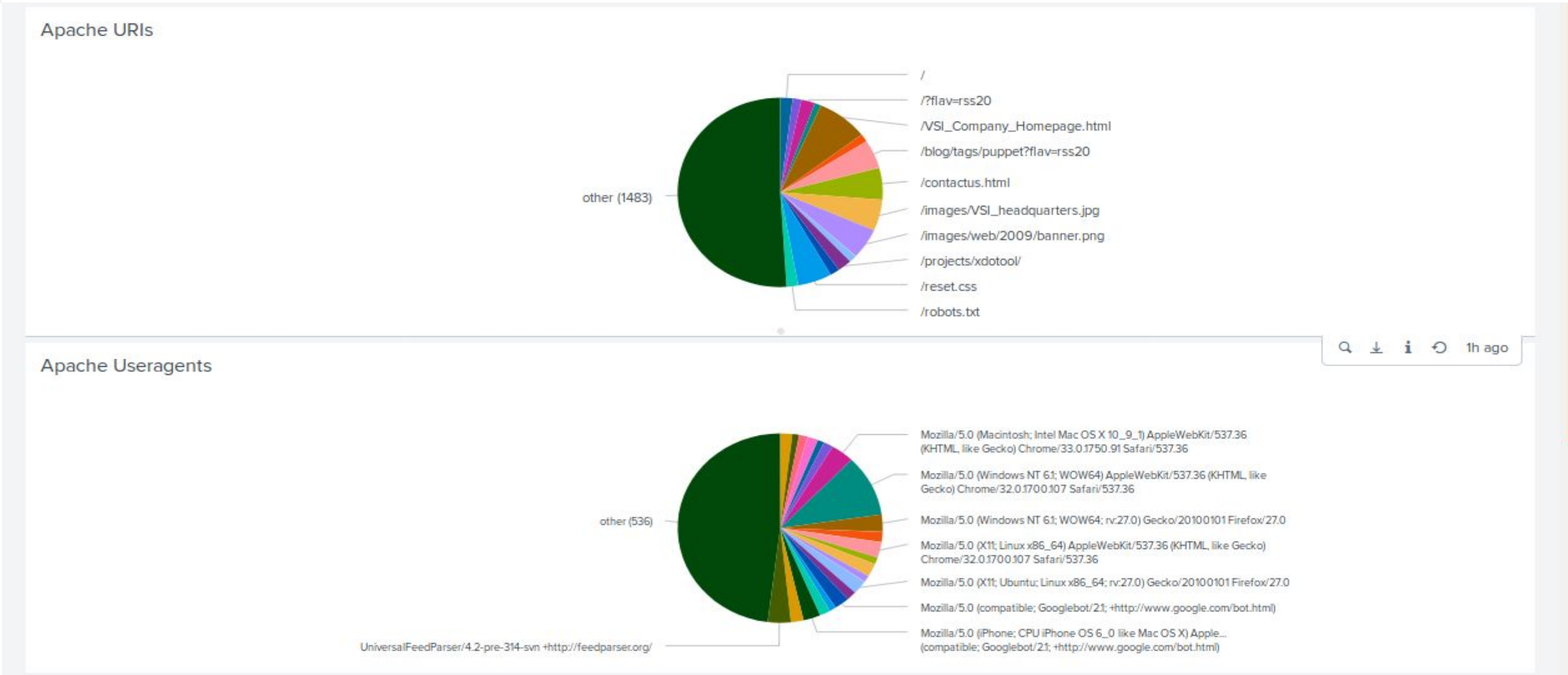
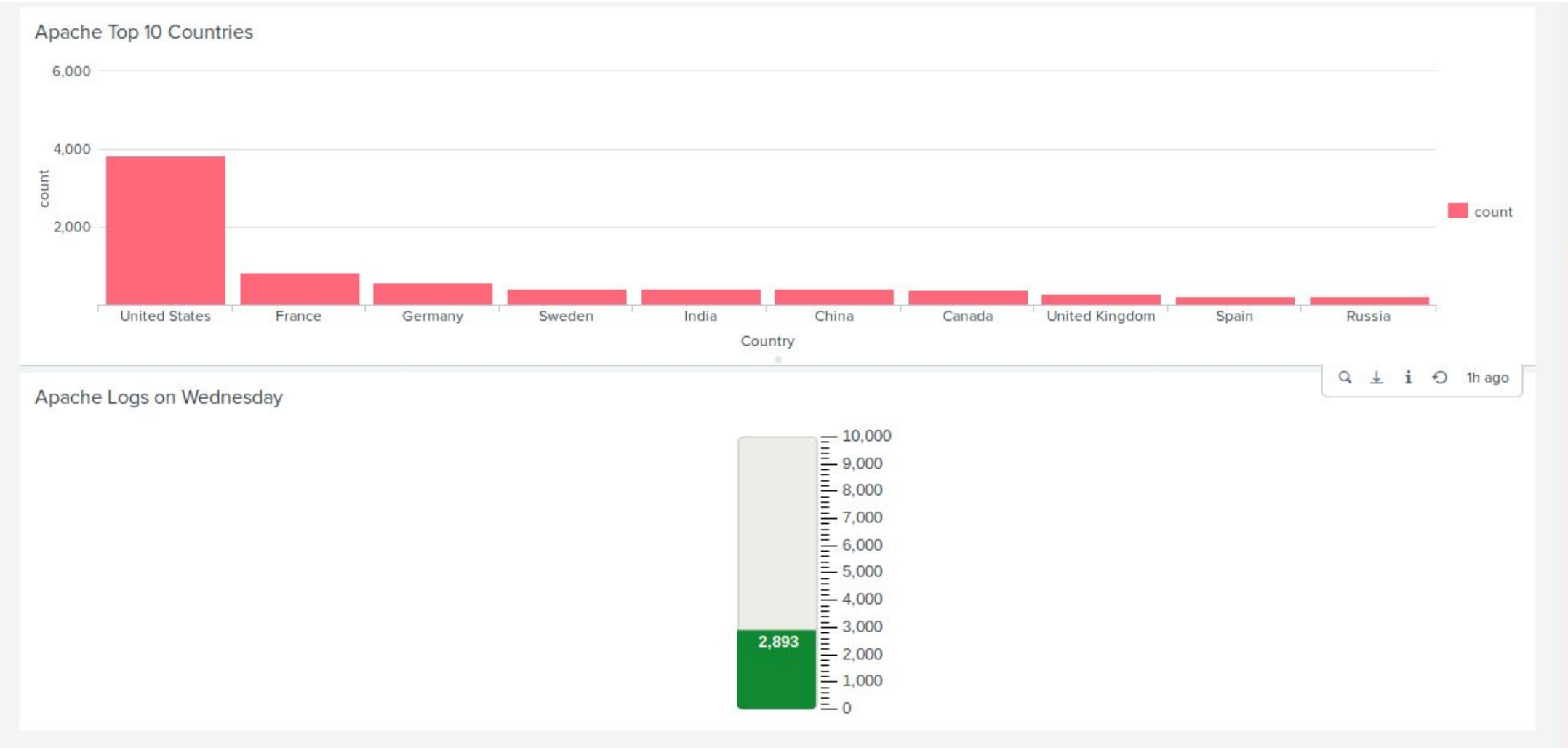
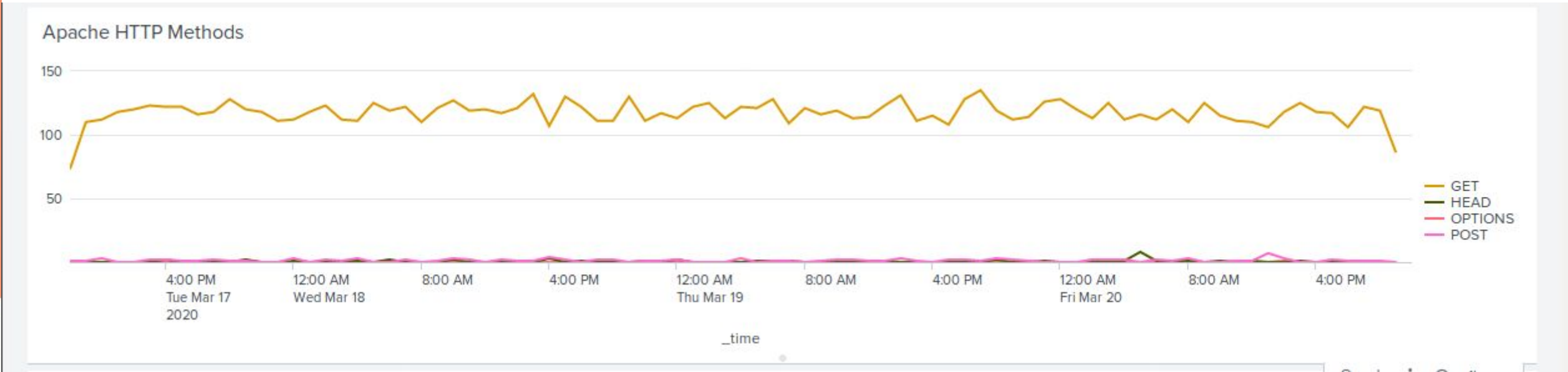
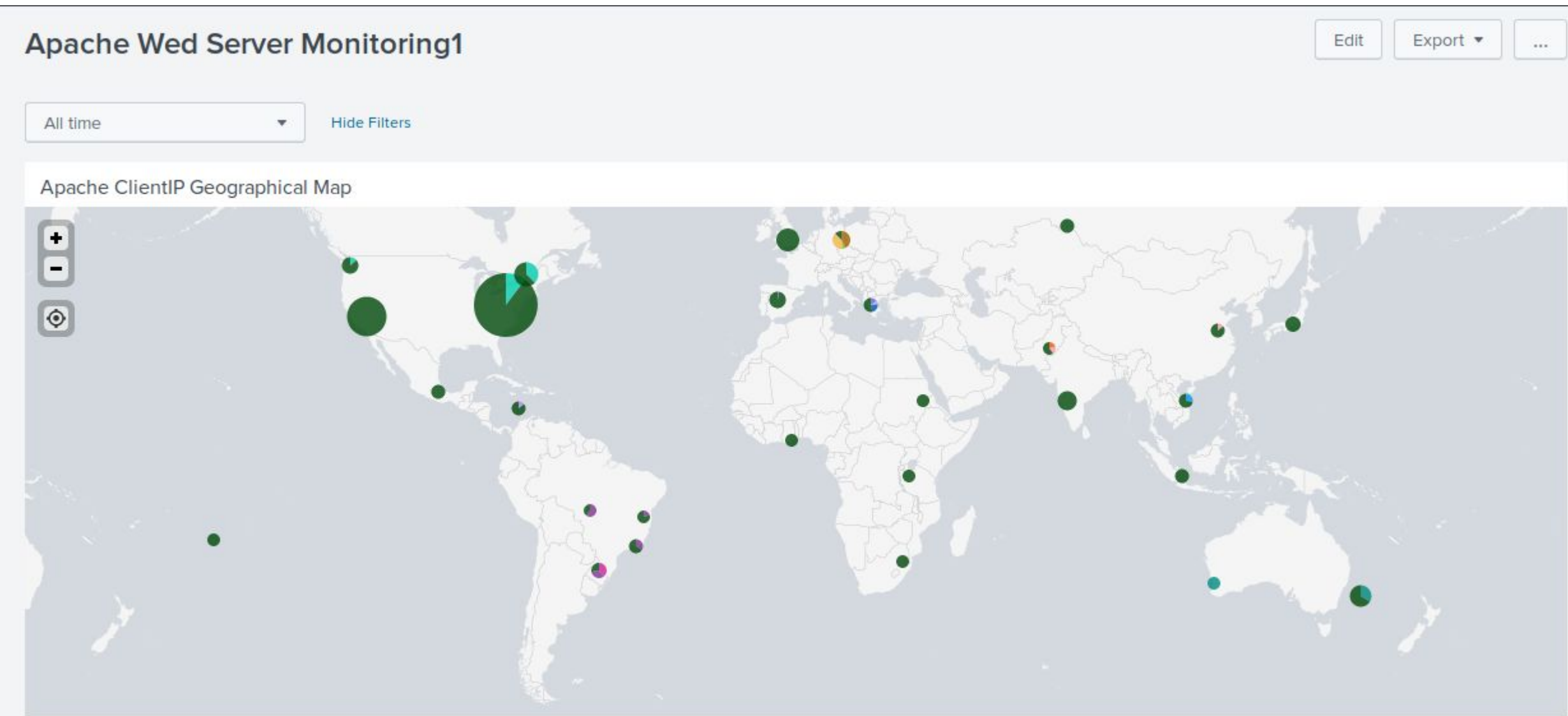
Trigger Condition: .. Custom. "search count > 11". Edit

Actions: 1 Action Edit

Send email

There are no fired events for this alert.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

Summarize your findings from your reports when analyzing the attack logs.

- It appeared that Users A and K were working together performing a brute force attack on the Windows Server.
- User A performed their attack from 0140am-0240am. During this time they were performing a bruteforce attack and our threshold alert was tripped.
- User K performed their part of the attack from 0910am-1100am and were attempting to reset account passwords.
- User J started rapidly logging on from 1000am-0100pm

Attack Summary—Windows

Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

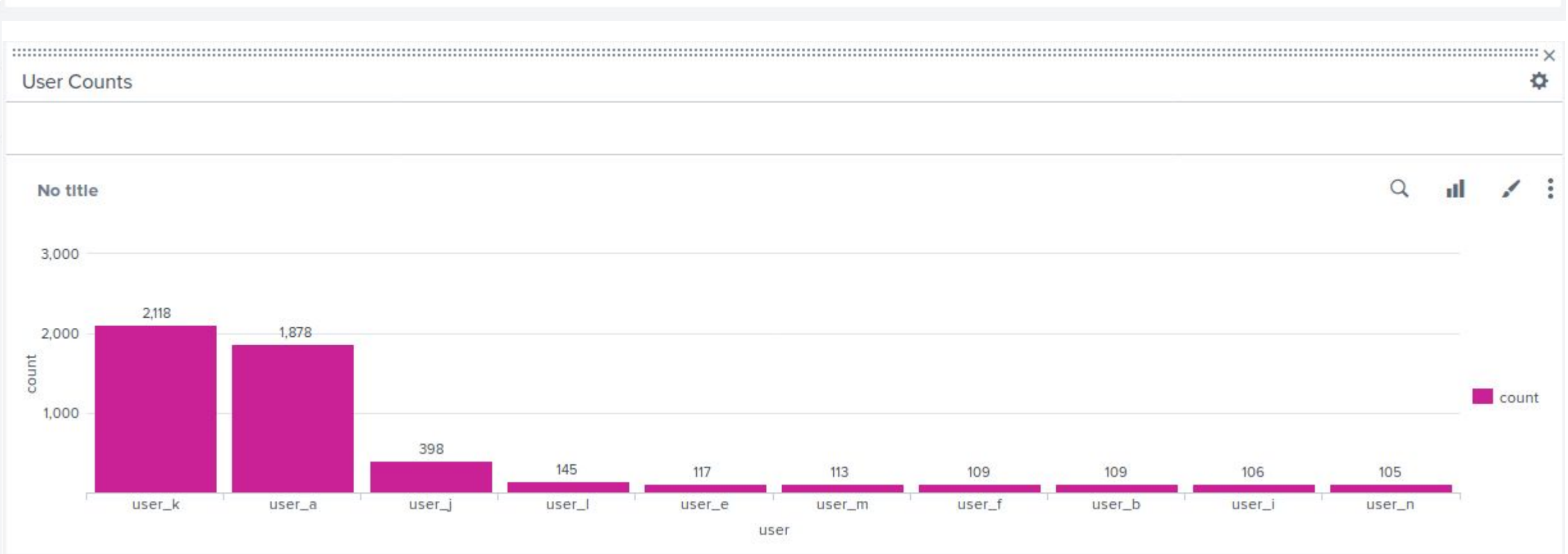
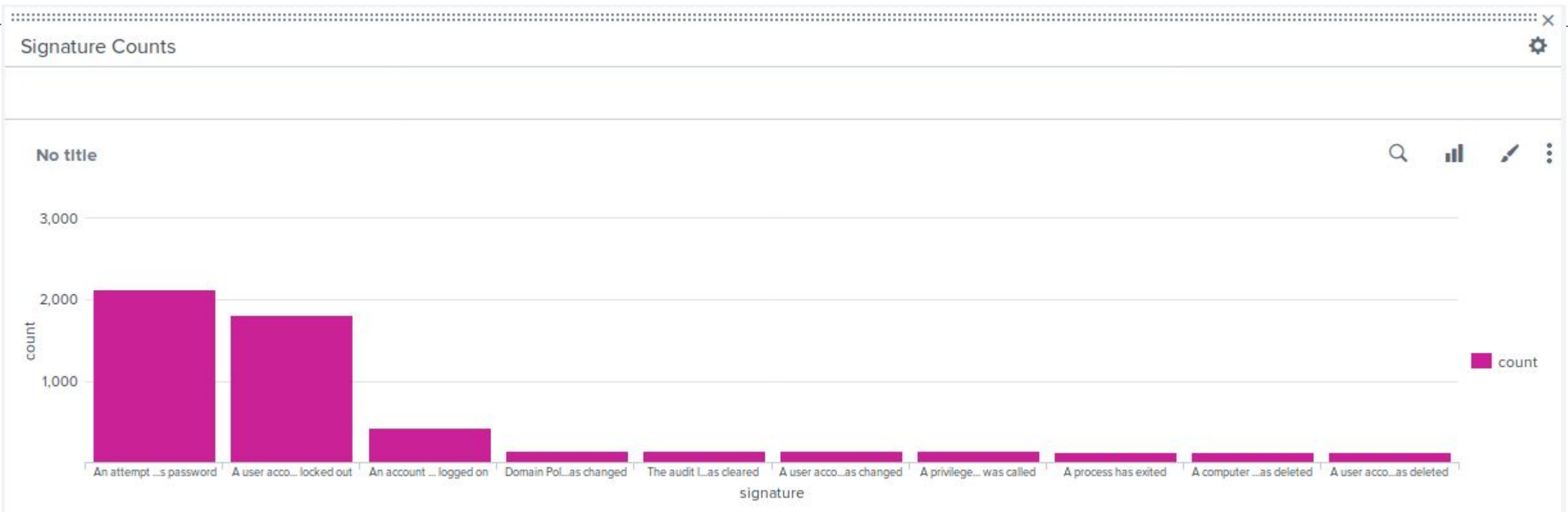
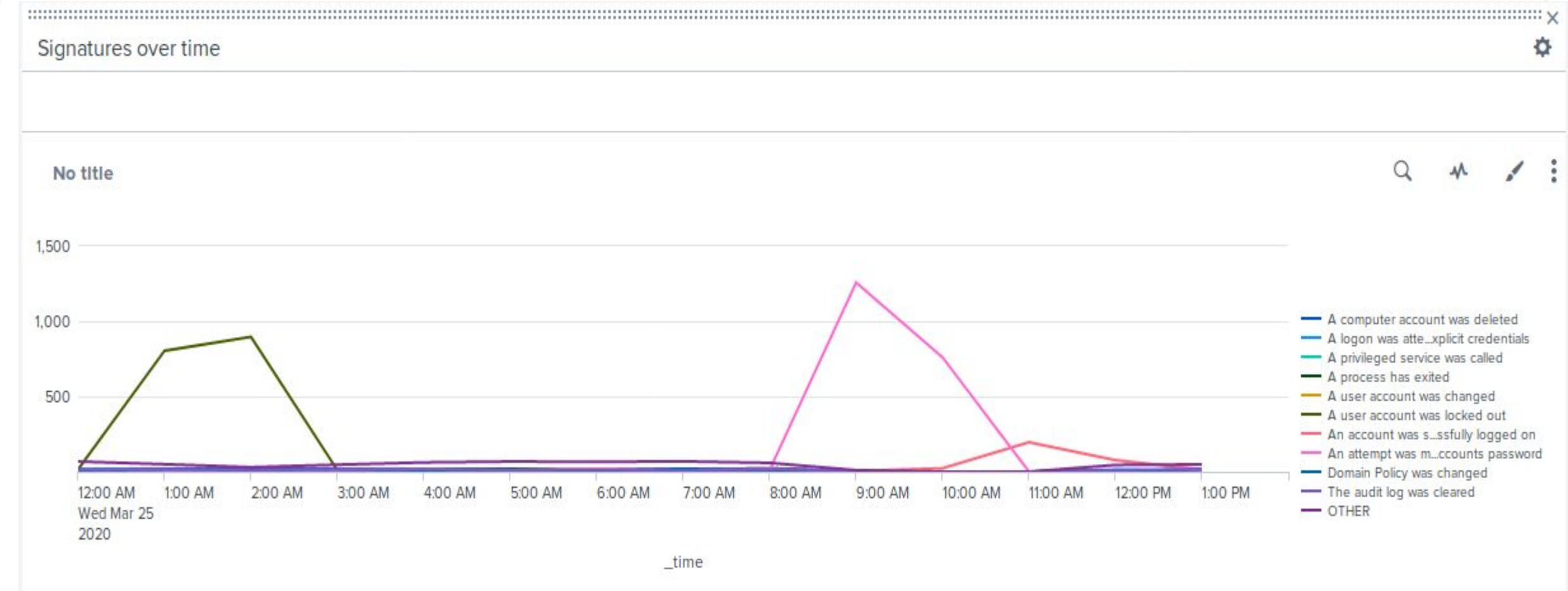
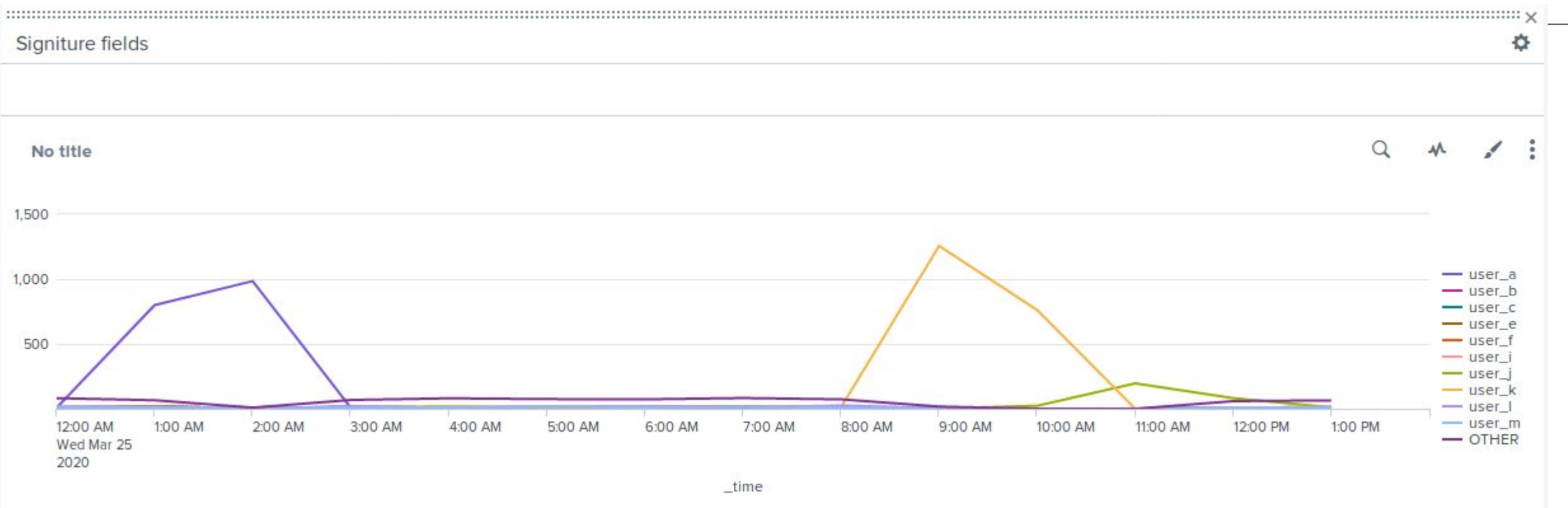
- Our failure alert worked properly. Since our threshold was set at >25.
- Our success alert also worked properly and was tripped since our threshold was set at >300.

Attack Summary—Windows

Summarize your findings from your dashboards when analyzing the attack logs.

- The Windows attack logs show an increase in activity on our “User Counts” and “Signature counts” graphs
- There is also more activity for certain users in successful account logins, attempted reset of passwords, and users accounts being locked out
- User_j and primarily logging in, and users “a” and “k” had high signature counts of attempting password resets/accounts locked out

Screenshots of Windows Attack Dashboard



Attack Summary—Apache

Summarize your findings from your reports when analyzing the attack logs.

- We noticed a increase in HTTP POST request. From a count of 106 to 1,324 on the 25th of March.
- The team found a significant decrease in website referrals from the Apache logs to Apache attack logs.
- There was a increase in international traffic from Germany on the 25th of March. With an increase of 404 response codes showing there was a DDoS attack.

Attack Summary—Apache

Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

Apache Logs compared to Apache attack logs

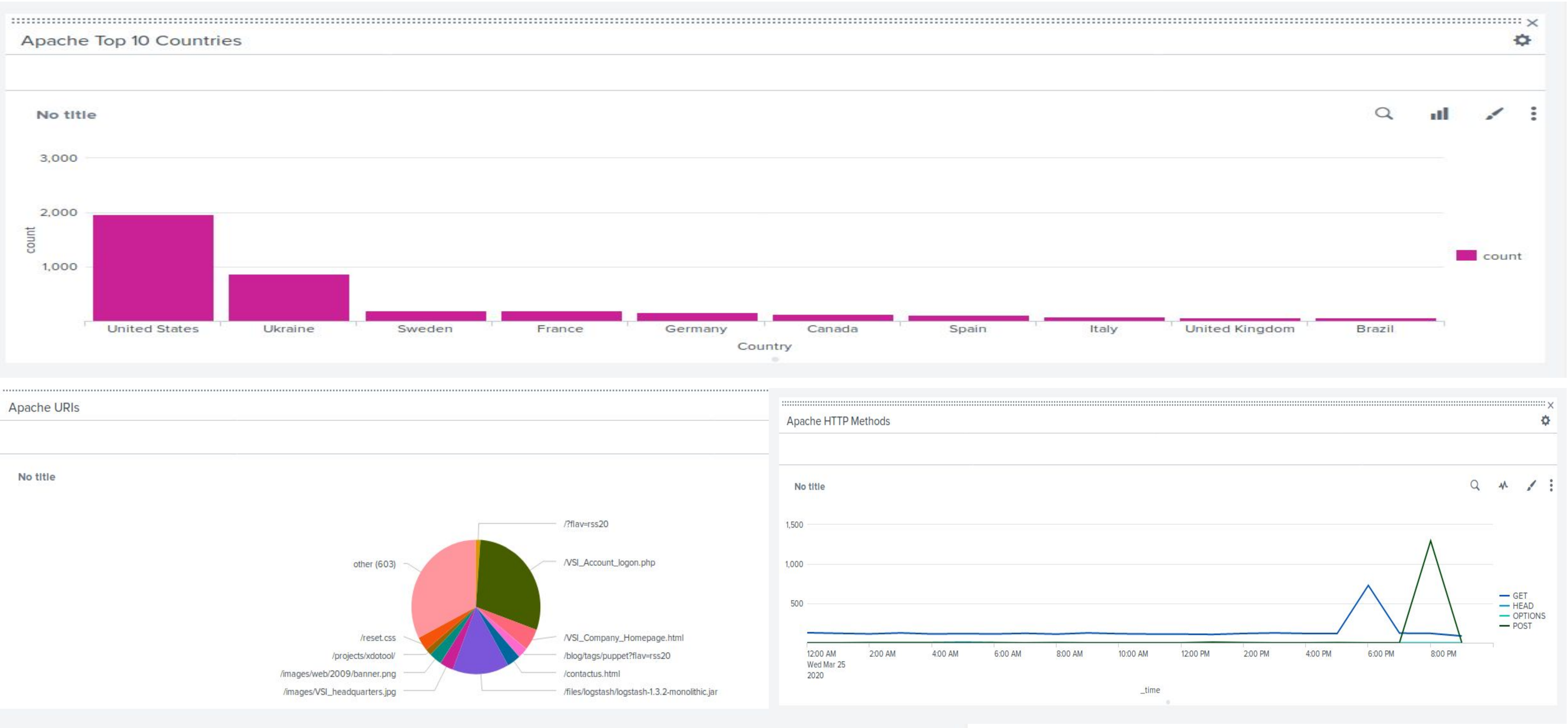
- We noticed a 28% decrease from the apache_logs to the apache_attacker_logs in the GET request. But a 28% increase in POST request. When you're receiving a HTTP response flood like this it most likely intels a DDoS attack. Our alert threshold was set to 11 requests with the baseline being 5. With this alert threshold in place it would detect this attack against the Apache servers.
- There was a difference between the two Apache logs with a decent increase of international client activity from Ukraine during the time of the attack from 791 to 1425 on March 25th.

Attack Summary—Apache

Summarize your findings from your dashboards when analyzing the attack logs.

- After comparing the original dashboard to the dashboard containing the attack log data we realized a significant increase in HTTP POST requests that happened between the hours of 5:00 pm and 7:00 pm.
- We noticed that on our URI graph the number one URI was “/VSI_Account_logon.php” as opposed to just “/VSI_Company_Homepage.html” which was the primary URI before the attack.
- For the top ten countries, we noticed that Ukraine, which was not in the top ten before, now had the second most behind the United States.

Screenshots of Attack Dashboard



Apache HTTP Methods

No title

GET

HEAD

OPTIONS

POST

time

12:00 AM

2:00 AM

4:00 AM

6:00 AM

8:00 AM

10:00 AM

12:00 PM

2:00 PM

4:00 PM

6:00 PM

8:00 PM

1,500

1,000

500

Status Overview | Splunk

Add Data - Select Source

Search | Splunk 9.0.4

localhost:8000/en-US/app/search/search?q=s

67%

splunk>enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Reporting

New Search

Save As

Create Table View

Close

source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined" | top limit=20 method

All time

4,497 events

(before 3/9/23 10:18:53.000 PM)

No Event Sampling

Job

Smart Mode

Events

Patterns

Statistics (4)

Visualization

20 Per Page

Format

Preview

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

Compared to average statistics:

10,000 events

(before 3/10/23 1:00:58.000 AM)

Job

4 results

20 per page

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

36

Status Overview | Splunk XAdd Data - Select Source XSearch | Splunk 9.0.4 X+

localhost:8000/en-US/app/search/search?q=s67%

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboardsSearch & Reporting

New SearchSave As>Create Table ViewClose

source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined" | top limit=20 statusAll time

4,497 events (before 3/9/23 10:47:51.000 PM)No Event SamplingJobVerbose Mode

Events (4,497)PatternsStatistics (7)Visualization

20 Per PageFormatPreview

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

localhost:8000/en-US/app/search/search?q=s 67%

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

Ubuntu Software

source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined" | top limit=10 referer_domain All time

✓ 4,497 events (before 3/9/23 10:43:11.000 PM) No Event Sampling Job Smart Mode

Events Patterns **Statistics (10)** Visualization

20 Per Page Format Preview

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

Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
- Brute force attacks took place in Windows.
- DDoS attacks took place on Apache.
- To protect VSI from future attacks, what future mitigations would you recommend?
- User accounts should be locked out after 5 incorrect attempts
- Consecutive brute forcing attempts from the same IP Address should be locked out permanently
- Implementing multi- factor authentication