

Defensive Security Project by: The Dream Team

Table of Contents

This document contains the following resources:

01

**Monitoring
Environment**

02

Attack Analysis

03

**Project Summary
& Future
Mitigations**

Monitoring Environment

Scenario

- SOC analysts at Virtual Space Industries (VSI) which designs virtual-reality programs for businesses
- VSI hear rumors the a competitor, JobeCorp, may launch cyberattacks to disrupt VSI's businesses
- As SOC analysts, we were tasked with using Splunk to monitor against potential attacks on VSI's systems and applications
- VSI products that we were tasked with monitoring include an administrative webpage, an Apache web server, and a Window's OS
- We reviewed logs from the Windows Server and the Apache Server

["Add-On" App]

Splunk Add-on for Apache Web Server

The Splunk Add-on for Apache Web Server allows a Splunk software administrator to collect and analyze data from Apache Web Server using file monitoring. After the Splunk platform indexes the events, you can analyze the data using the prebuilt panels included with the add-on.

The screenshot shows the Splunk App Store interface. At the top, the navigation bar includes the Splunk logo, 'enterprise' version, and user options like 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. A search bar on the right contains the text 'Find'. Below the navigation bar, the main heading is 'Browse More Apps'. On the left, there is a search input field with 'apache' and a list of categories. The main content area displays '14 Apps' and lists the top results. The first result, 'Splunk Add-on for Apache Web Server', is marked as 'Already Installed'. The second result, 'TA-apache_access_eventgen', has an 'Install' button. The third result, 'ITSI Module for Kafka smart monitoring', and the fourth, 'Kafka Smart Monitoring', also have 'Install' buttons. Each app card includes a description, category, author, and download/release information.

Search Results:

- Search:** apache
- Filters:** CATEGORY (IT Operations, Security, Fraud & Compliance, Business Analytics, Utilities, IoT & Industrial Data, DevOps, Directory Service, Email, Endpoint, Firewall, Generic, Identity Management, Information, Investigative, Network Access Control, Network Device, Network Security)
- Sort:** Best Match, Newest, Popular
- 14 Apps**
- App 1:** **Splunk Add-on for Apache Web Server** (Already Installed)
 - Description: The Splunk Add-on for Apache Web Server allows a Splunk software administrator to collect and analyze data from Apache Web Server using file monitoring. After the Splunk platform indexes the events, you can analyze the data using the prebuilt panels included with the add-on.
 - More: This add-on provides the inputs and CIM-compatible knowledge to use with...
 - Category: IT Operations | Author: Splunk Inc. | Downloads: 23712 | Released: 9 months ago | Last Updated: 4 months ago | [View on Splunkbase](#)
- App 2:** **TA-apache_access_eventgen** (Install)
 - Description: TA-apache_access_eventgen is a custom LOG generator by [Splunk EventGen] (<http://splunk.github.io/eventgen/>). This TA generates continuous event logs of general apache access combined. It can be useful if we want a bunch of continuous sample logs. The most of ip,url,useragent and referer is based on [Splunk Buttercup Games's event data](<http://docs....>) [More](#)
 - Category: IT Operations, Utilities | Author: GoAhead Dev Team | Downloads: 52 | Released: 2 months ago | Last Updated: 2 months ago | [View on Splunkbase](#)
- App 3:** **ITSI Module for Kafka smart monitoring** (Install)
 - Description: The ITSI module for Telegraf Kafka monitoring provides smart insight monitoring for Apache Kafka monitoring, on top of Splunk and ITSI.
- App 4:** **Kafka Smart Monitoring** (Install)
 - Description: The Splunk application for Kafka monitoring with Telegraf leverages the best components to provide monitoring, alerting and reporting on top of Splunk and

Splunk Add-on for Apache Web Server

[Scenario that illustrates benefit of add-on app.]

Splunk Add-on for Apache Web Server

Apps

Showing 1-25 of 27 items

25 per page

« Prev 1 2 Next »

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Splunk Add-on for Apache Web Server	Splunk_TA_apache	2.1.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase

Splunk_TA_apache

[Apps](#) » [Splunk_TA_apache](#)

Name

Give your app a friendly name for display in Splunk Web.

Update checking

☐ No ☒ Yes

Check SplunkApps for updates to this app.

Visible

☒ No ☐ Yes

Only apps with views should be made visible.

Upload asset

Browse...

No file selected.

Can be any html, js, or other file to add to your app.

Cancel

Save

Logs Analyzed

1

Windows Logs

This server contains intellectual property of VSI's next-generation virtual reality programs

2

Apache Logs

This server is used for VSI's main public-facing website, vsi-company.com

Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Signatures and associated signature IDs	To view reports that show the ID number associated with the specific signature for Windows activity.
Severity Levels Count and Percentage	To allow VSI to quickly understand the severity levels of the Windows logs being viewed.
Comparison Between Success and Failure	This report will allow VSI to monitor if there is a suspicious level of failed activities on their server.

Images of Reports—Windows

Signature and Signature ID

All time

✓ 15 events (before 3/7/23 1:13:19.000 AM)

Job

20 per page

i	_time	host	sourcetype	name	signature	signature_id
>	3/24/20 11:59:54.000 PM	windows_server_logs	csv	A user account was deleted	A user account was deleted	4726
>	3/24/20 11:59:53.000 PM	windows_server_logs	csv	A user account was created	A user account was created	4720
>	3/24/20 11:59:31.000 PM	windows_server_logs	csv	A computer account was deleted	A computer account was deleted	4743
>	3/24/20 11:57:54.000 PM	windows_server_logs	csv	An account was successfully logged on	An account was successfully logged on	4624
>	3/24/20 11:57:51.000 PM	windows_server_logs	csv	Special privileges assigned to new logon	Special privileges assigned to new logon	4672
>	3/24/20 11:56:41.000 PM	windows_server_logs	csv	An attempt was made to reset an accounts password	An attempt was made to reset an accounts password	4724
>	3/24/20 11:56:40.000 PM	windows_server_logs	csv	System security access was granted to an account	System security access was granted to an account	4717
>	3/24/20 11:54:46.000	windows_server_logs	csv	A privileged service was called	A privileged service was called	4673

Severity Count and Percent

All time

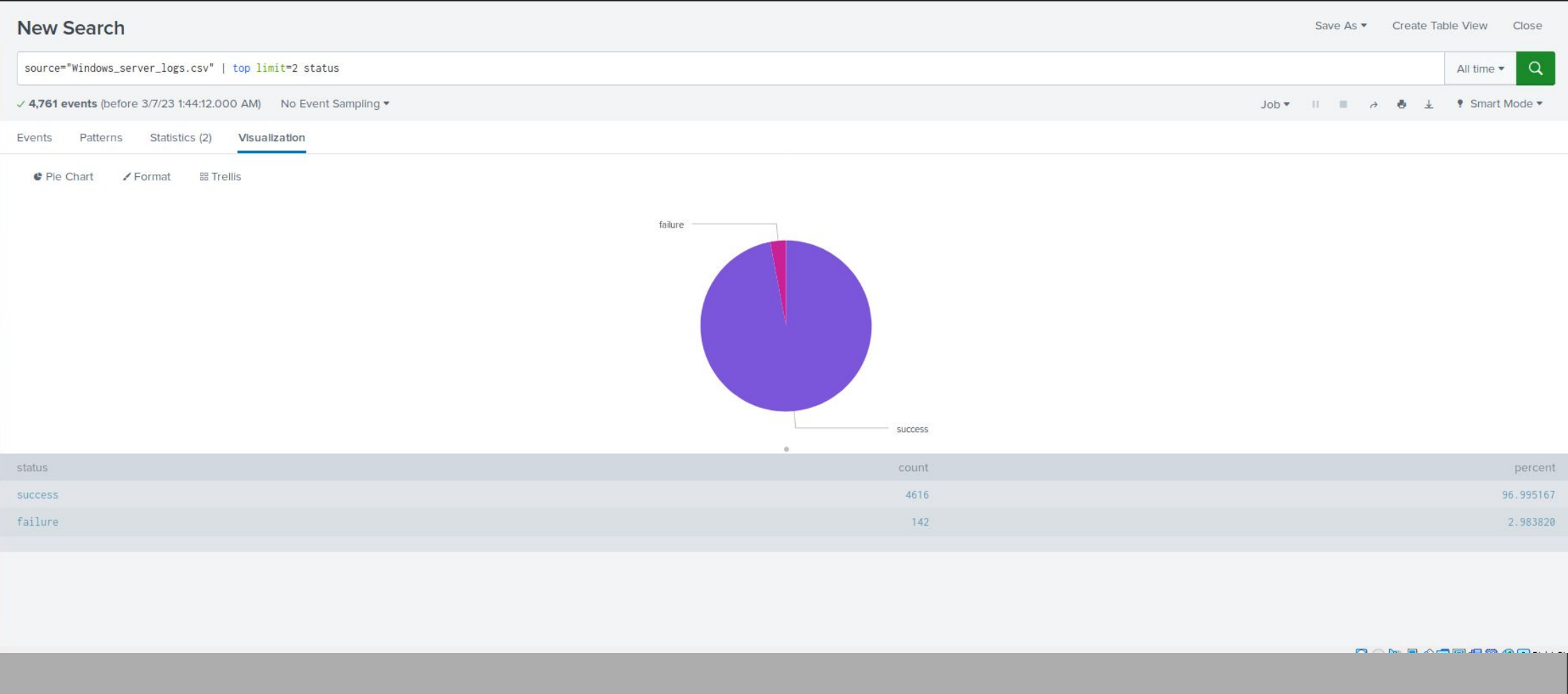
✓ 4,761 events (before 3/7/23 1:41:26.000 AM)

Job

2 results

20 per page

severity	count	percent
informational	4429	93.885338
high	329	6.914670



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	Number of failed Windows activities by hour.	11	20

JUSTIFICATION: We took the average count by hour and made that figure our baseline. We then found the standard deviation of the counts and did the average plus two times the standard deviation to get our threshold.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
An Account Was Successfully Logged On	Alerts when an inordinate amount of logins occur in an hour.	27	39

JUSTIFICATION: We took the average count by hour and made that figure our baseline. We then found the standard deviation of the counts and did the average plus two times the standard deviation to get our threshold.

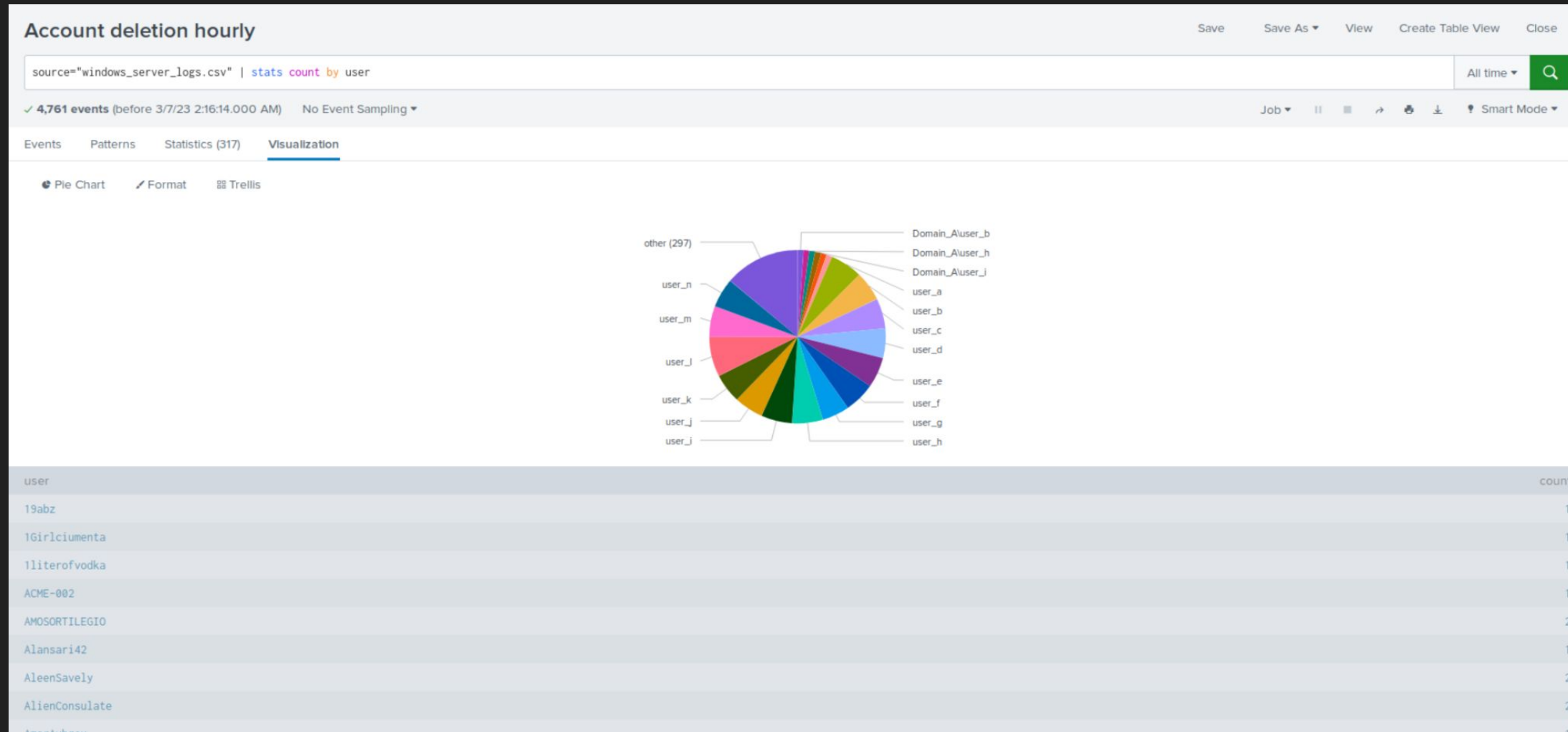
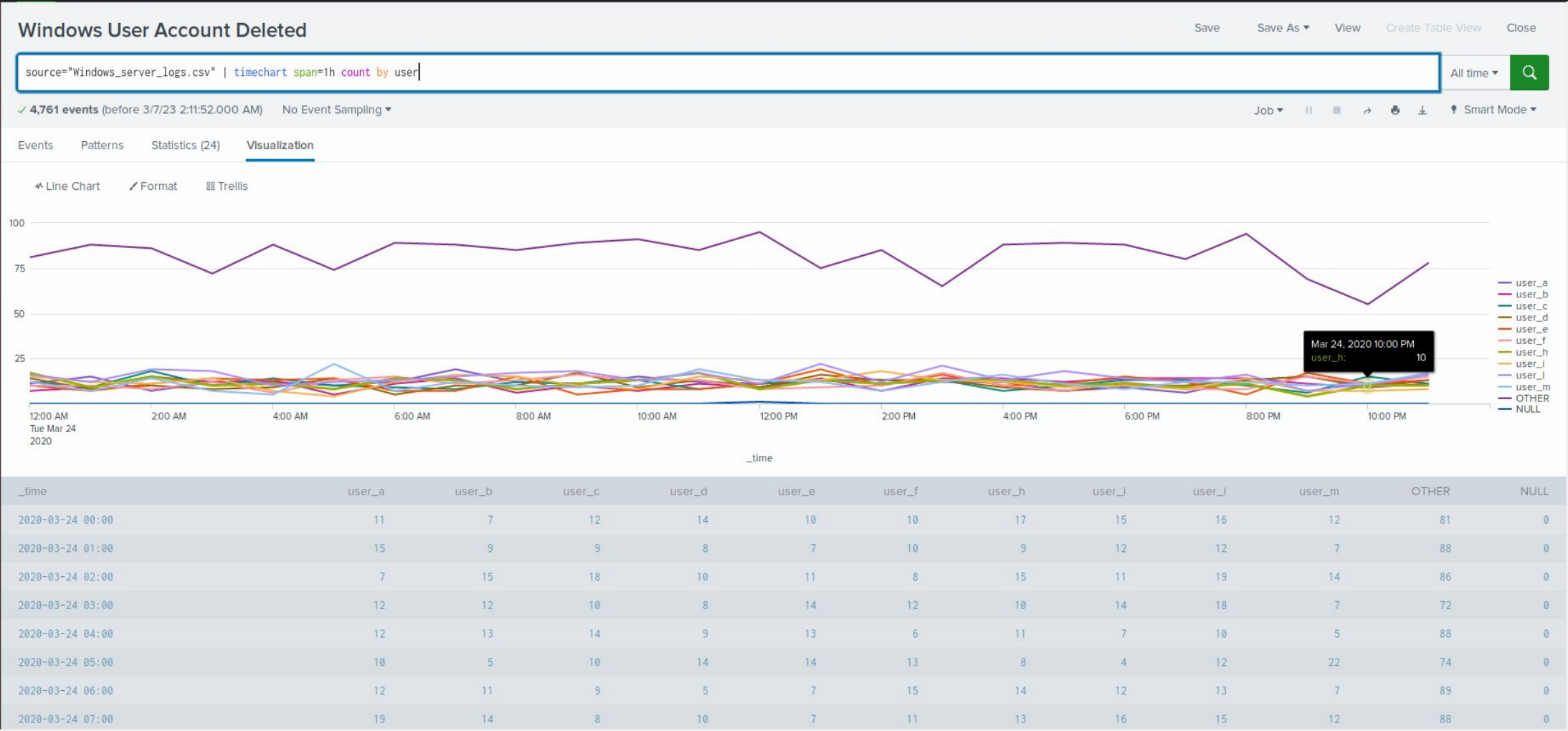
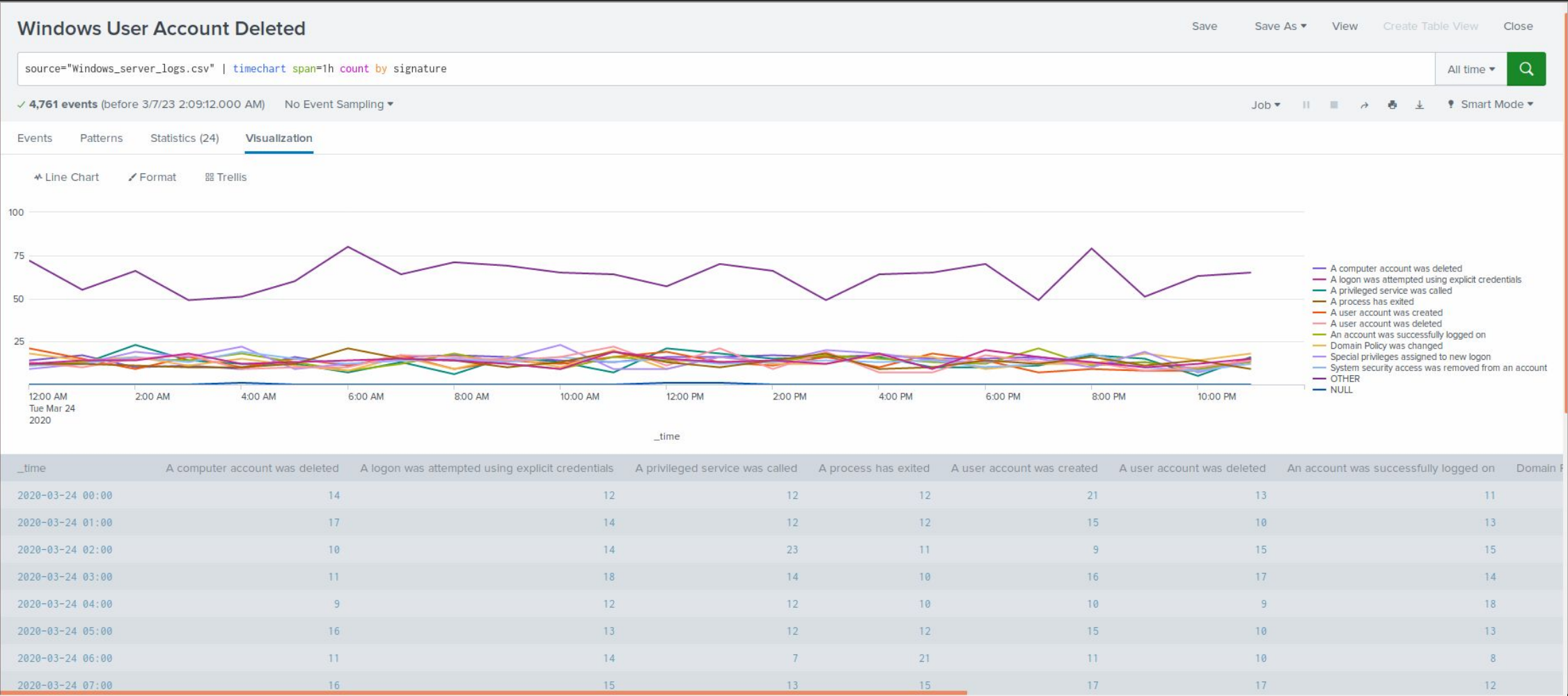
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Accounts Deleted	Alerts when an inordinate amount of user accounts are deleted in an hour.	27	44

JUSTIFICATION: We took the average count by hour and made that figure our baseline. We then found the standard deviation of the counts and did the average plus two times the standard deviation to get our threshold.

Dashboards—Windows



Dashboards—Windows



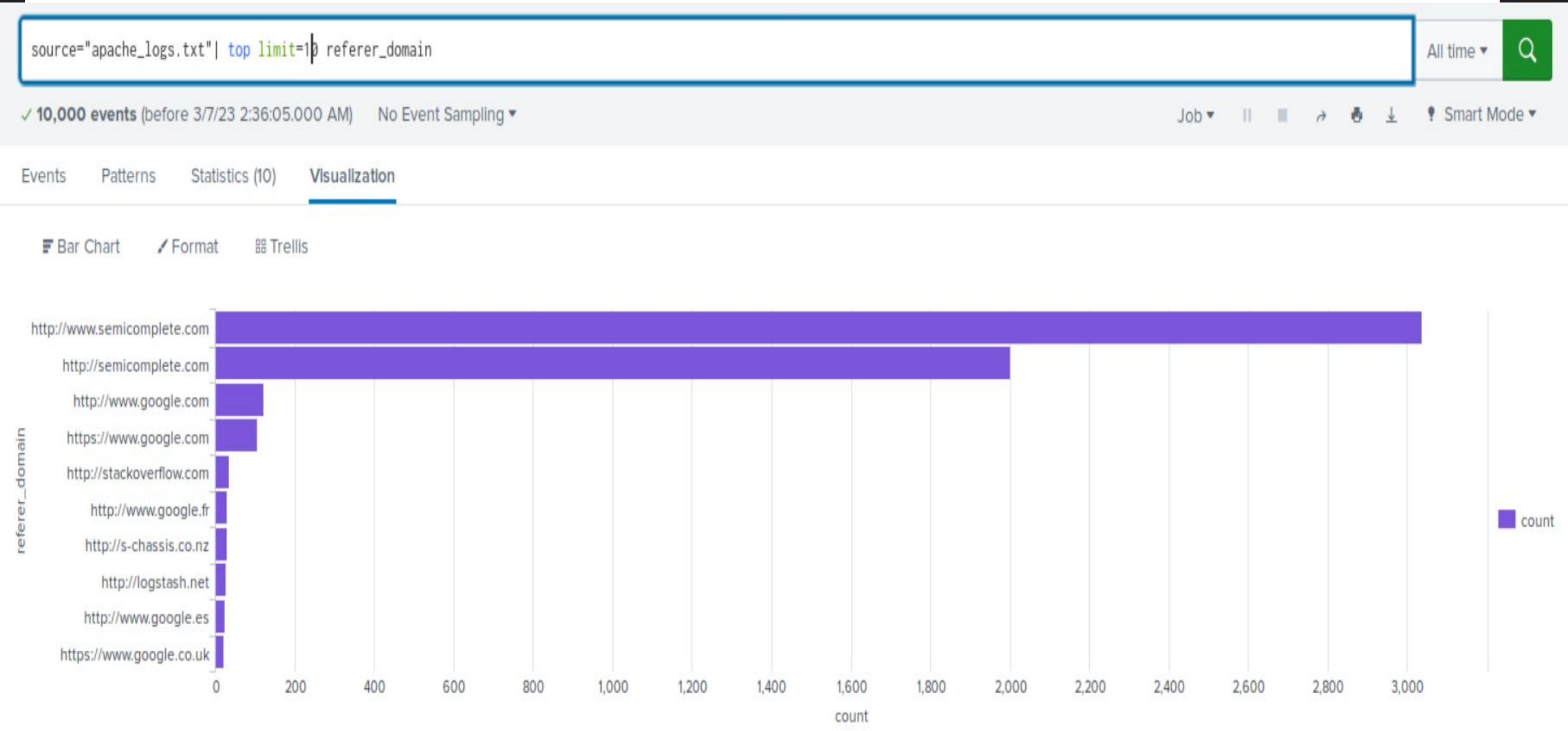
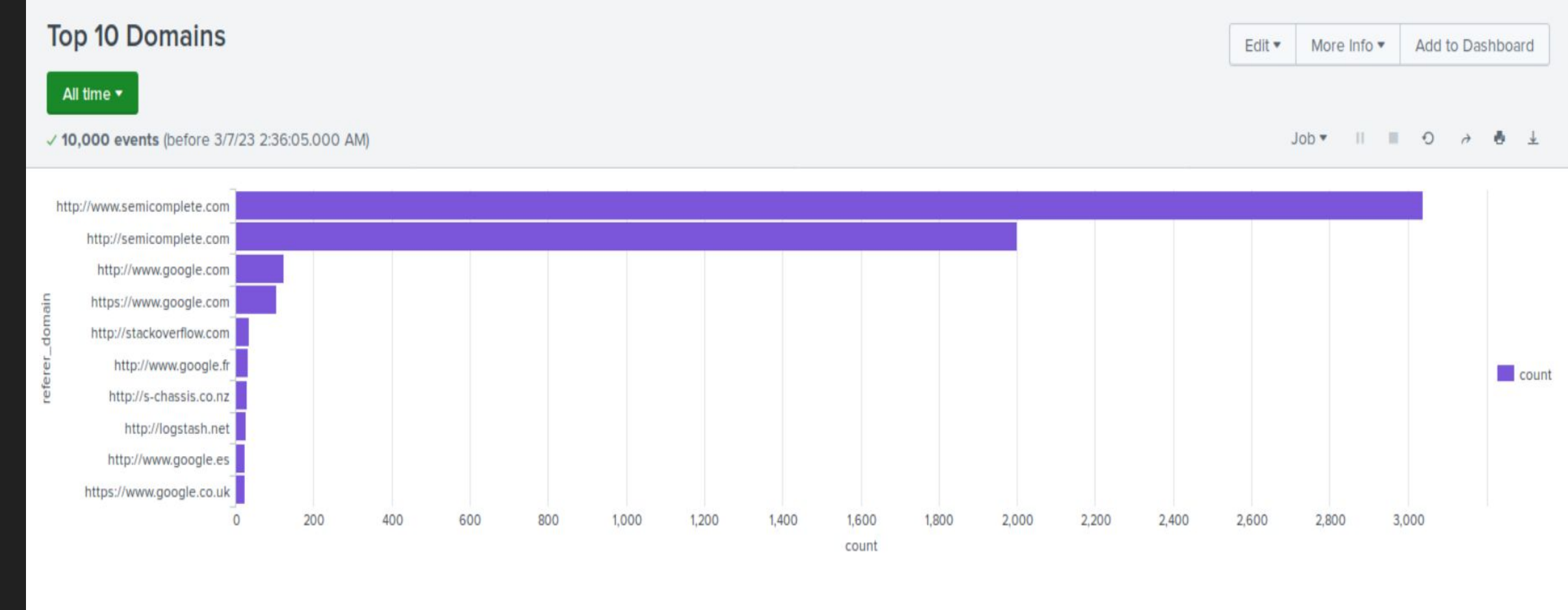
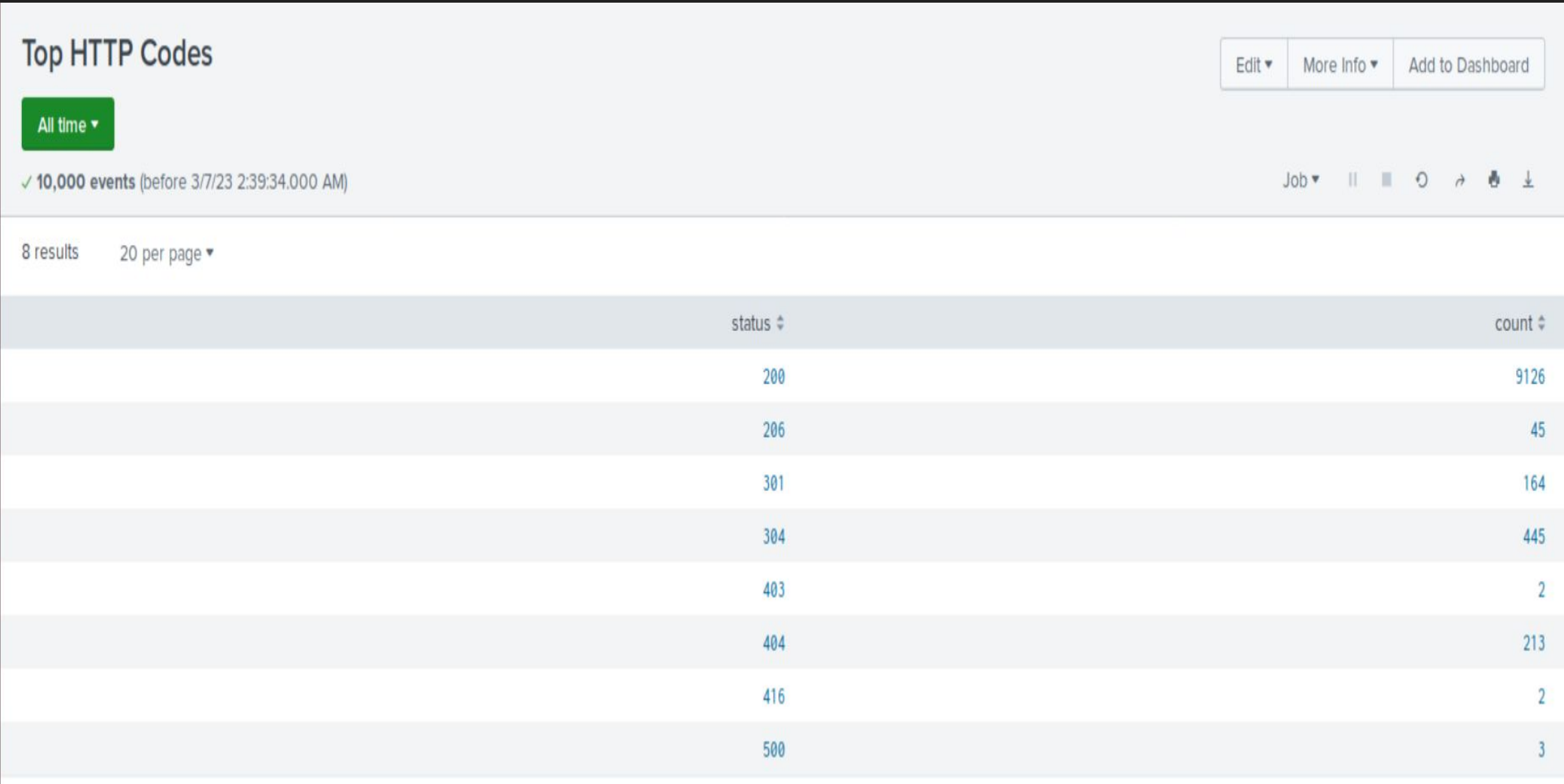
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Method	This will provide insight into the type of HTTP activity being requested against VSI's web server
Top 10 Domains	This will assist VSI with identifying suspicious referrers
Top HTTP Codes	This will provide insight into any suspicious levels of HTTP responses

Images of Reports—Apache



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Exceeded threshold for hourly activity from any country besides the US	Alert emails SOC@VSI-company.com when threshold reached	128	200

JUSTIFICATION: Detect unusual activity towards Apache Server from any country outside the United States

Exceeded threshold for hourly activity from any country besides the United States.

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Mar 7, 2023 2:52:12 AM

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

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Abnormal amount of hourly HTTP POST requests	This alert will notify a VSI SOC Analyst if there are an abnormal amount of HTTP POST requests in an hour	5	10

JUSTIFICATION: Detect an unusual number of POST requests

HTTP POST by Hour

Enabled: Yes. [Disable](#)


Permissions: Private. Owned by admin. [Edit](#)

Modified: Mar 7, 2023 2:56:18 AM

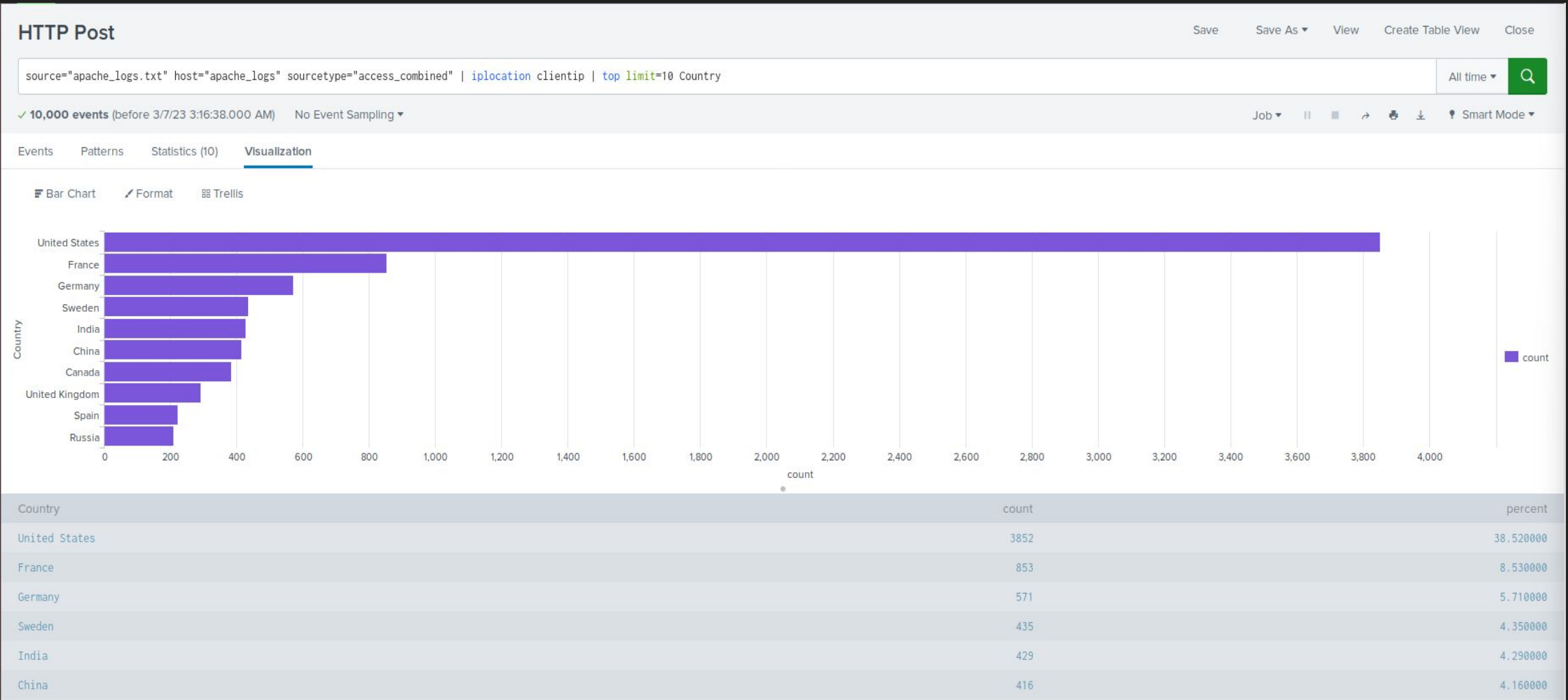
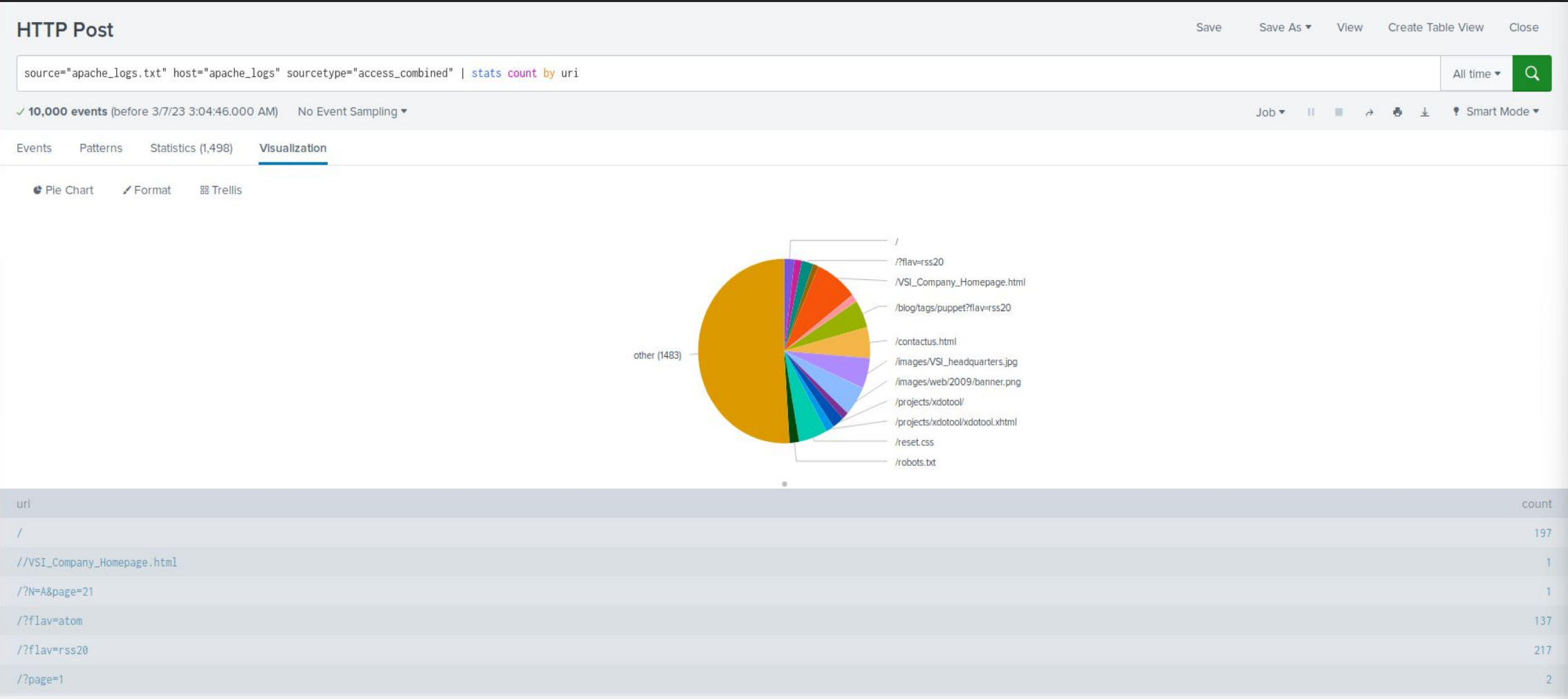
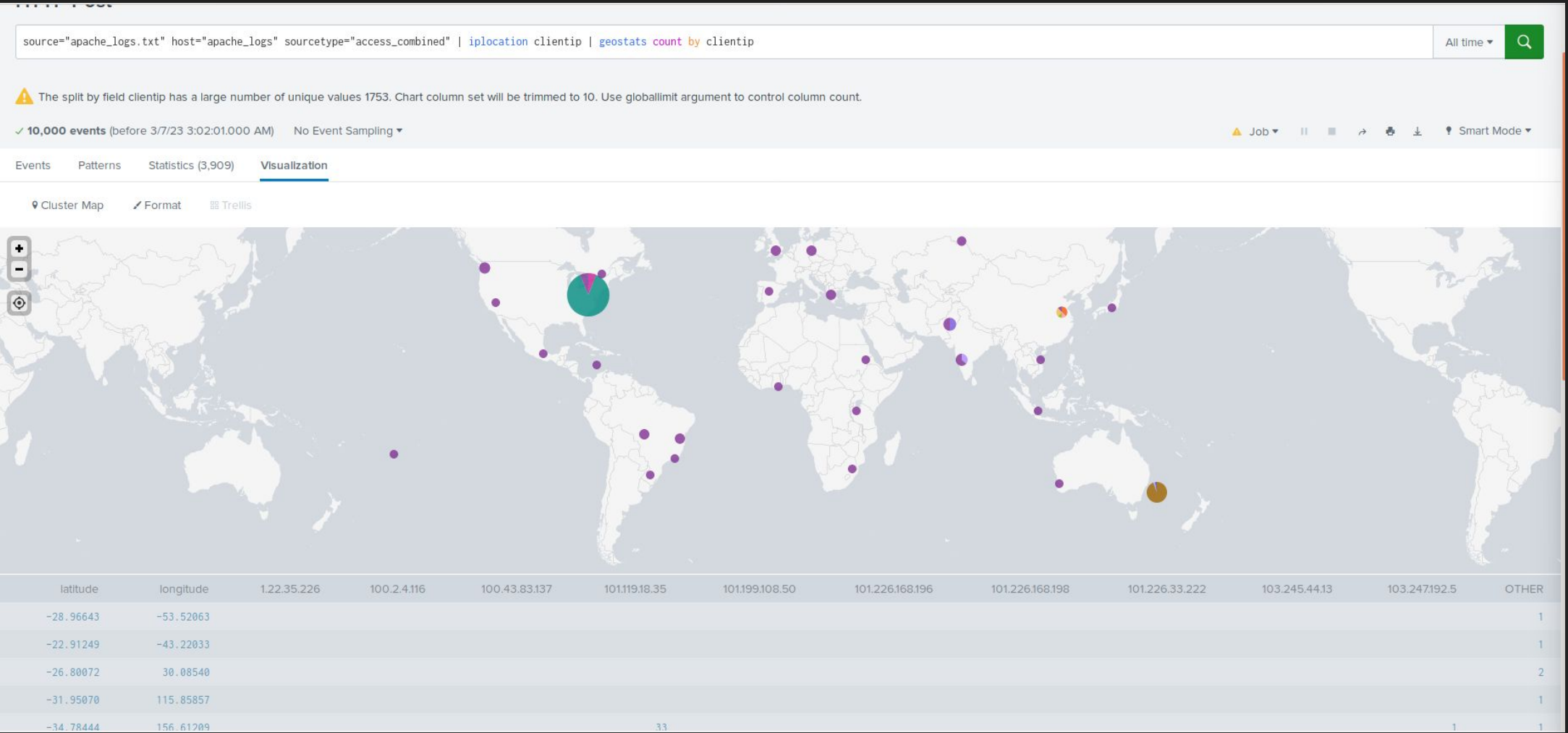
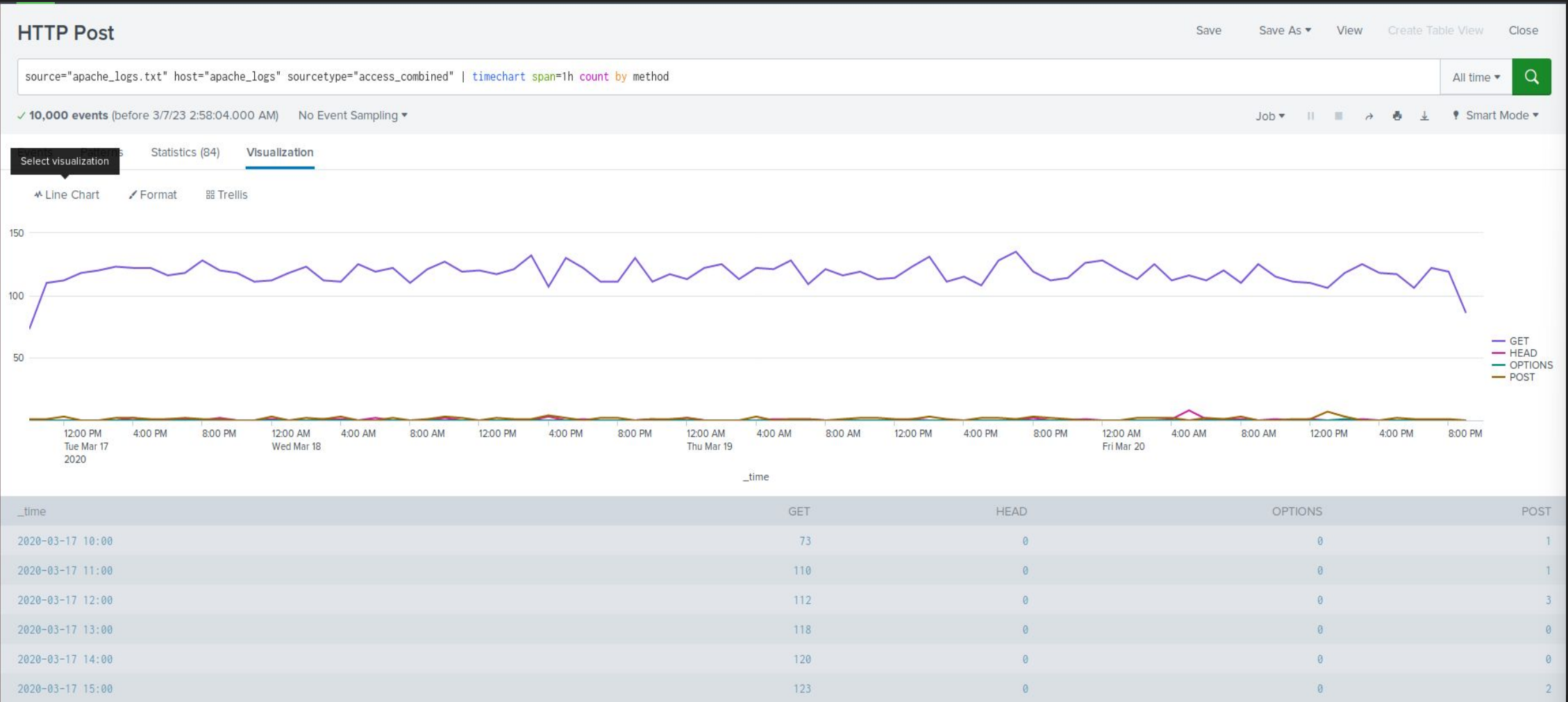
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 10. [Edit](#)

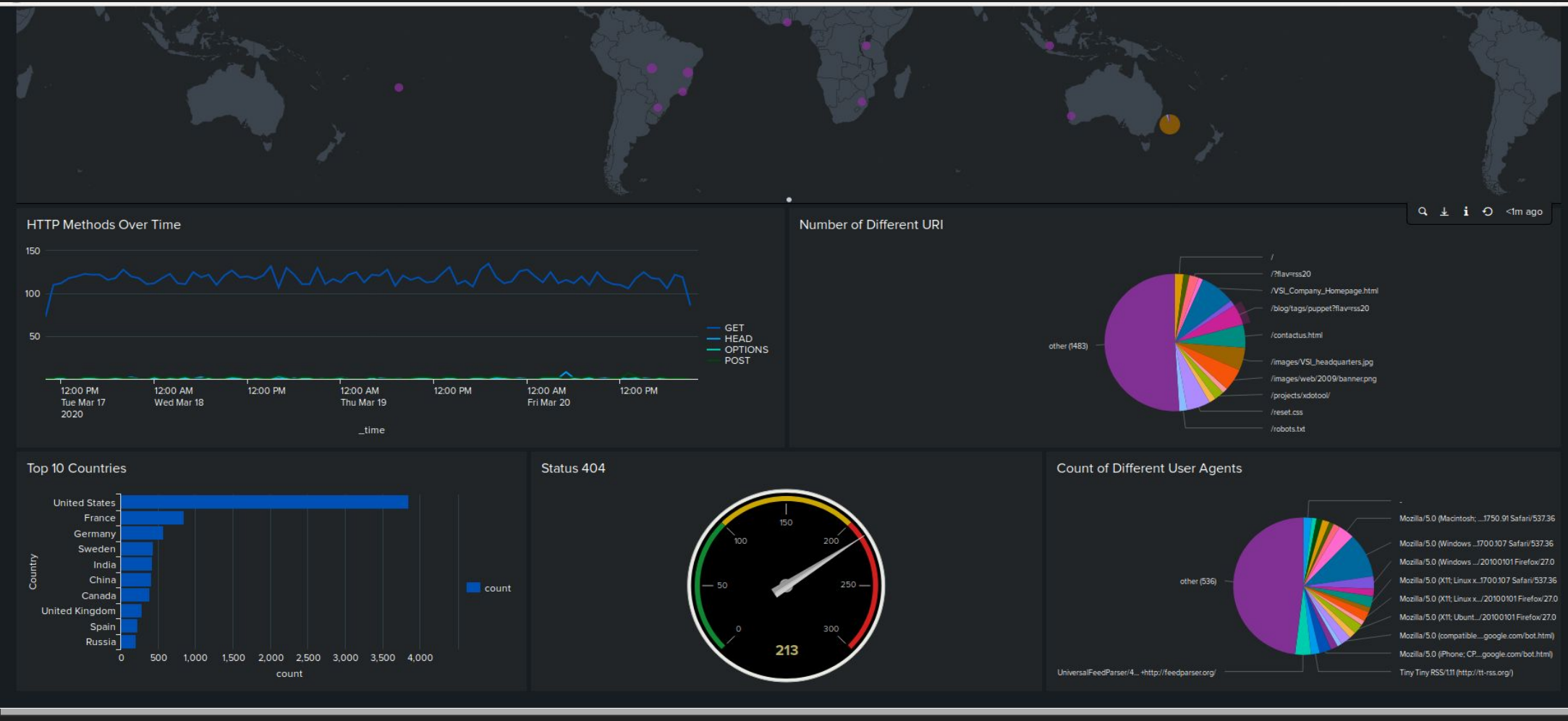
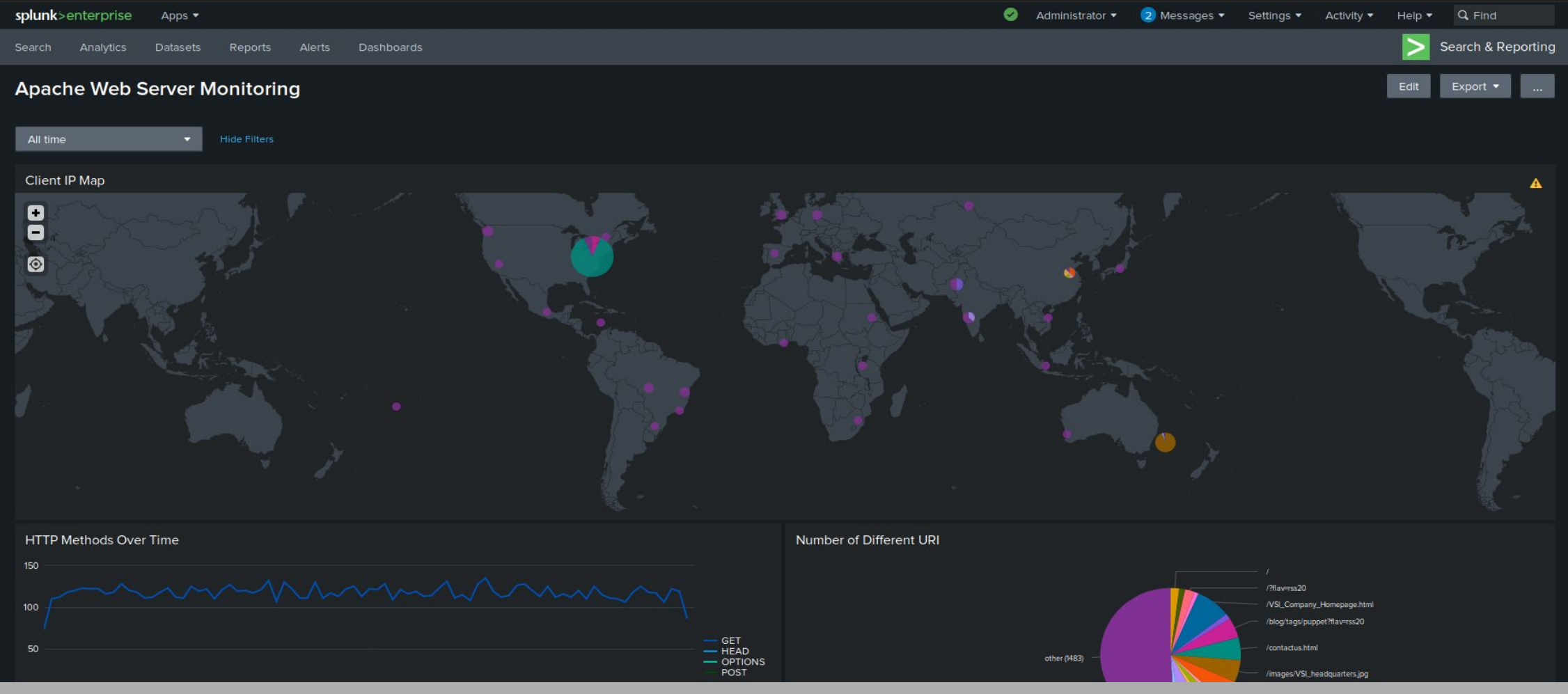
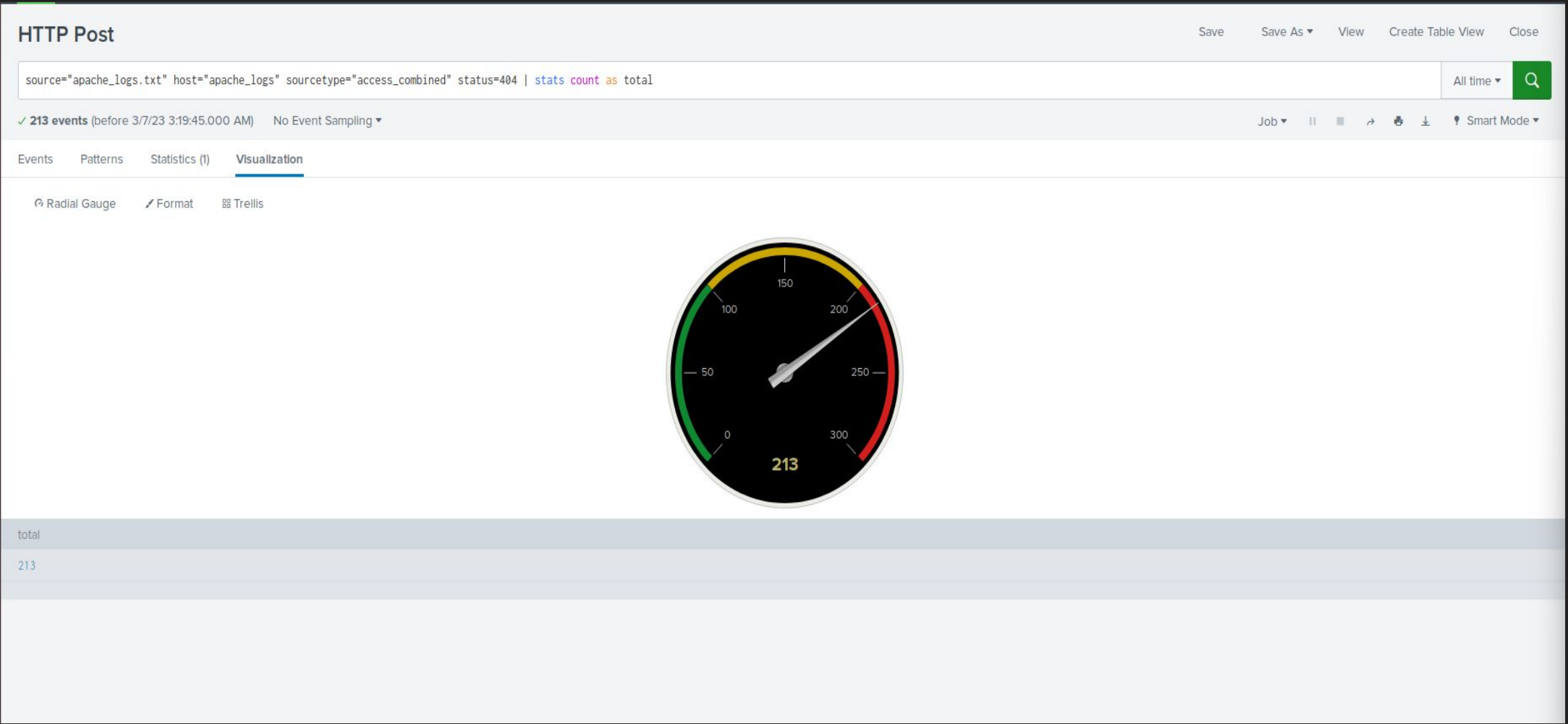
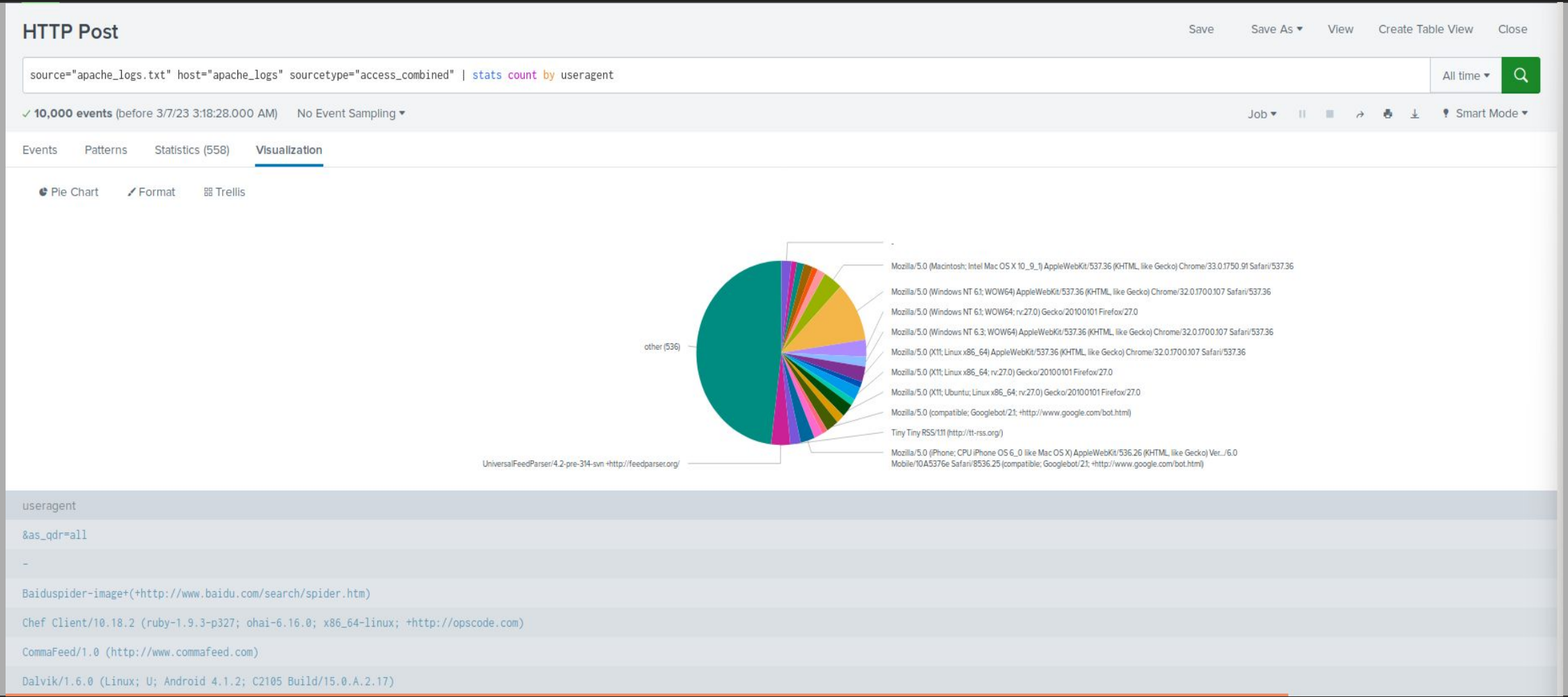
Actions: [▼](#) 1 Action [Edit](#)

 Send email

Dashboards—Apache



Dashboards—Apache

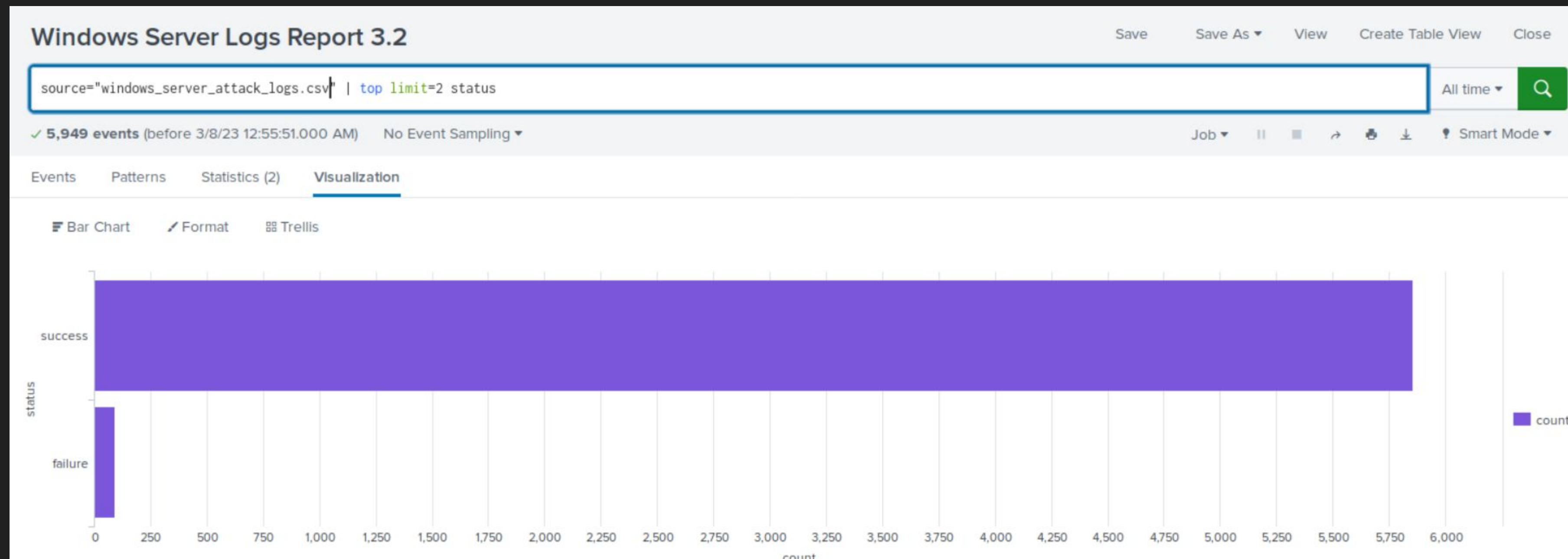


Attack Analysis

Attack Summary—Windows

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

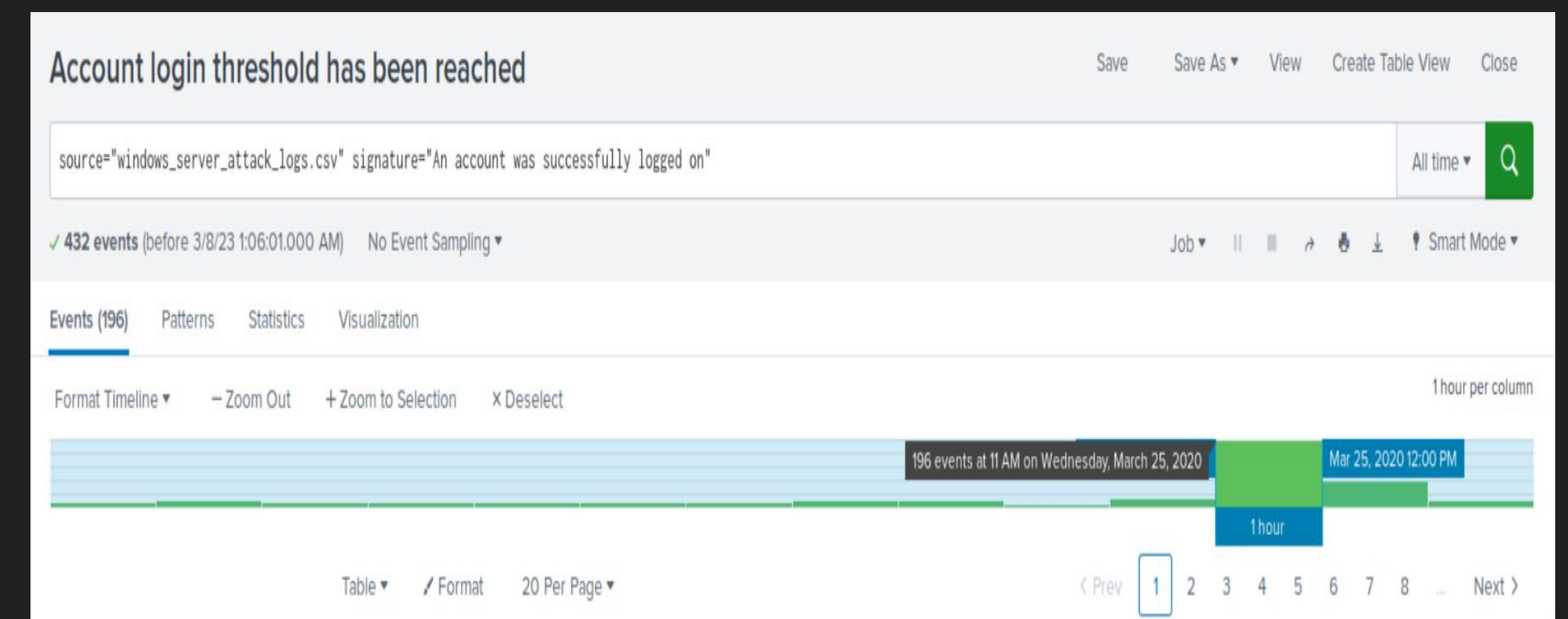
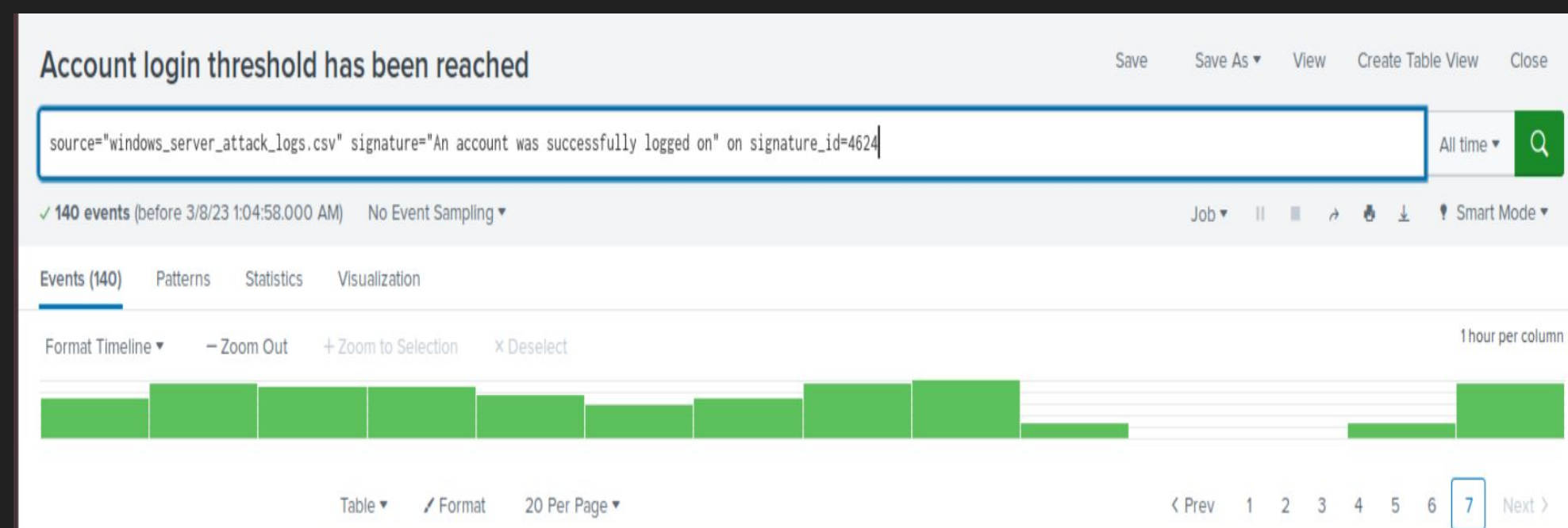
- IT severity count decreased (93% to 80%), while the high severity account increased (7% to 20%)
- Notable changes in failed activities, increase in successes 4616 to 5854 and decrease in fails from 142 to 93.



Attack Summary—Windows

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

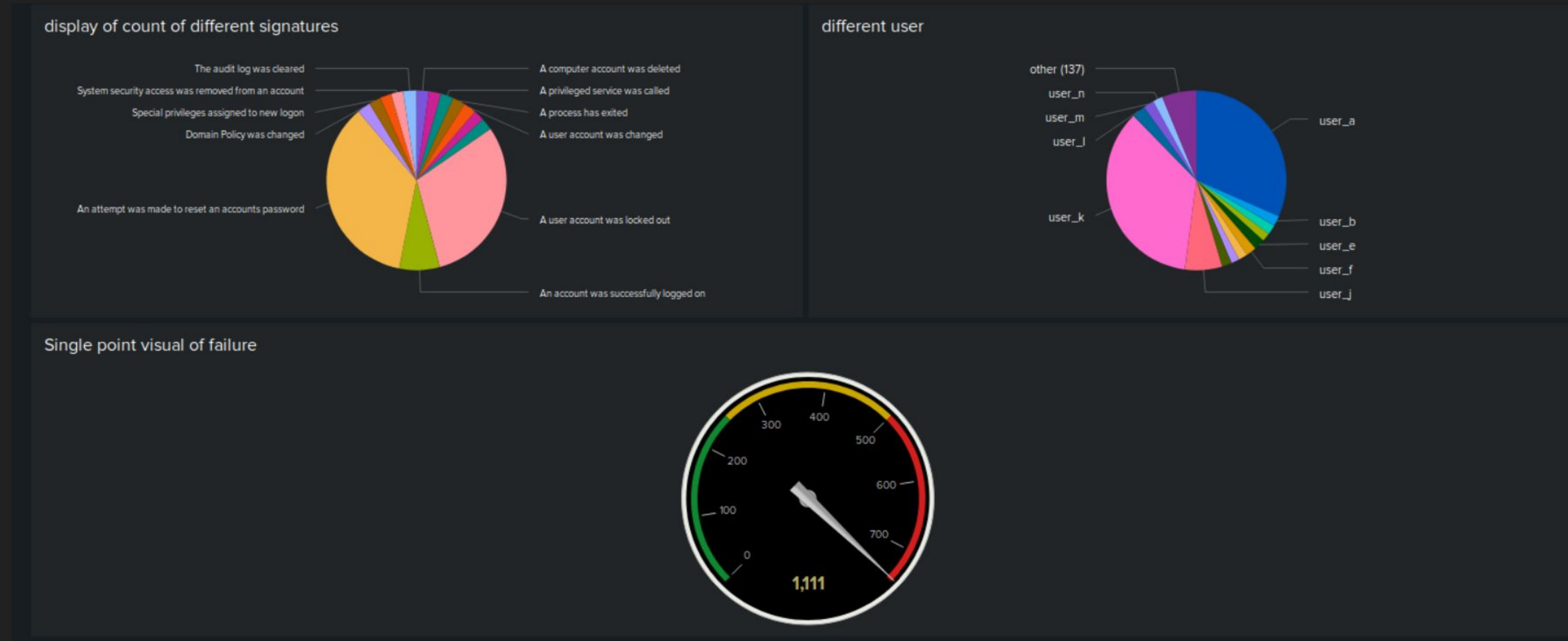
- Alert for suspicious volume of failed activities failed
 - Signature_id 4624 prevents the alert being triggered
- Alert for suspicious volume of deleted accounts succeeded



Attack Summary—Windows

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

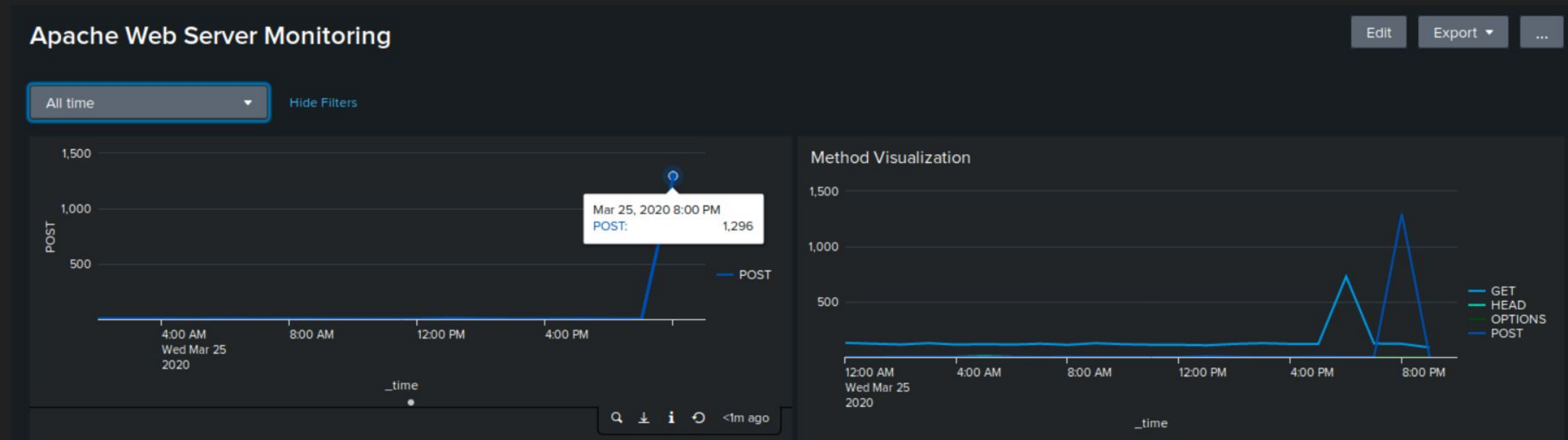
- Suspicious user activity – excessive login attempts by user_a, user_k, and user_j
- High number of attempts to reset account passwords (2128)
- High number of accounts locked out (1811)



Attack Summary—Apache

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

- There were a significant increase in POST requests (from 104 to 1324)
- There were sa significant decline in referrals from websites
- The amount of 404 status code responses increased by 466 responses while all other response codes decreased



Attack Summary—Apache

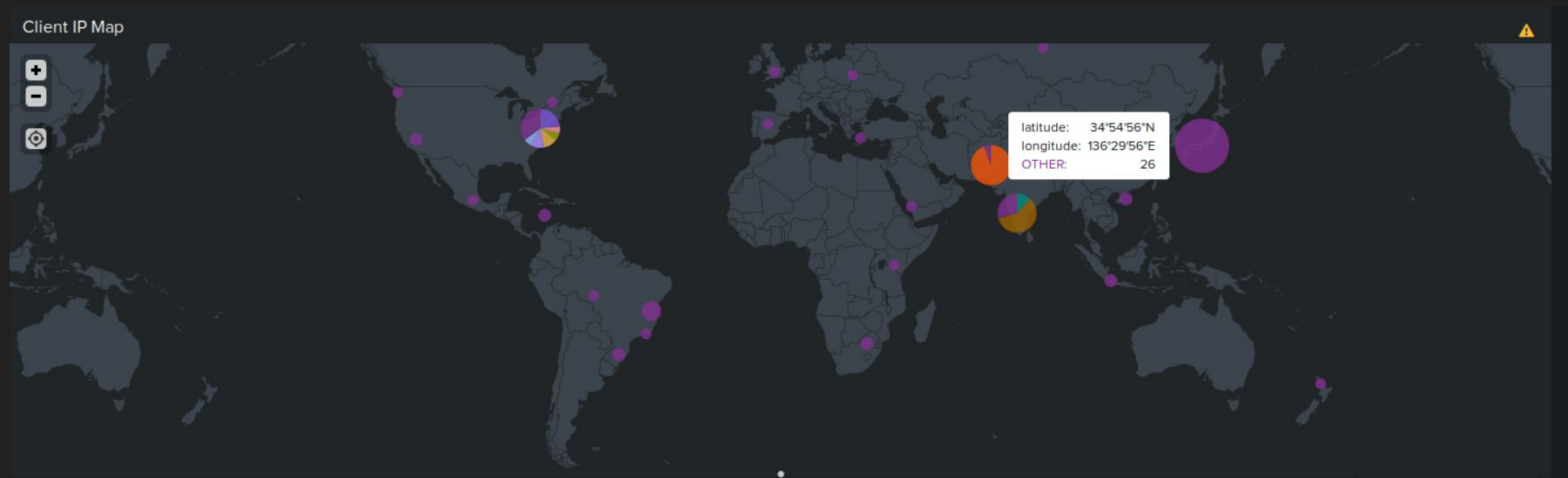
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- There was a stark increase in international activity at 20:00 on Wednesday March 25, 2020; 939 activities. The threshold of 334 would have successfully notified us of the suspicious activity.
- A suspicious volume of HTTP POST requests were detected on 20:00 on Wednesday March 25, 2020. There were 1296 POST requests made. Our threshold was set to 10, and it would have detected this volume of POST requests.

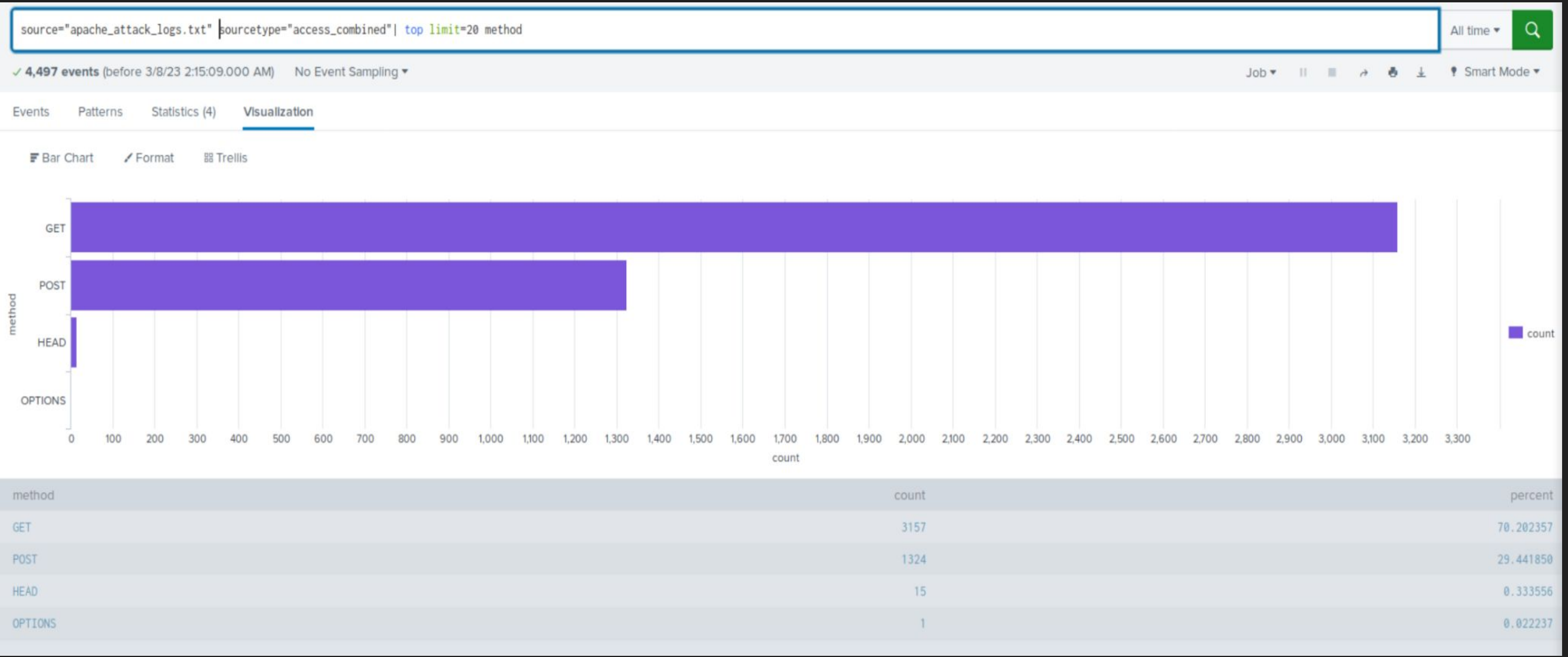
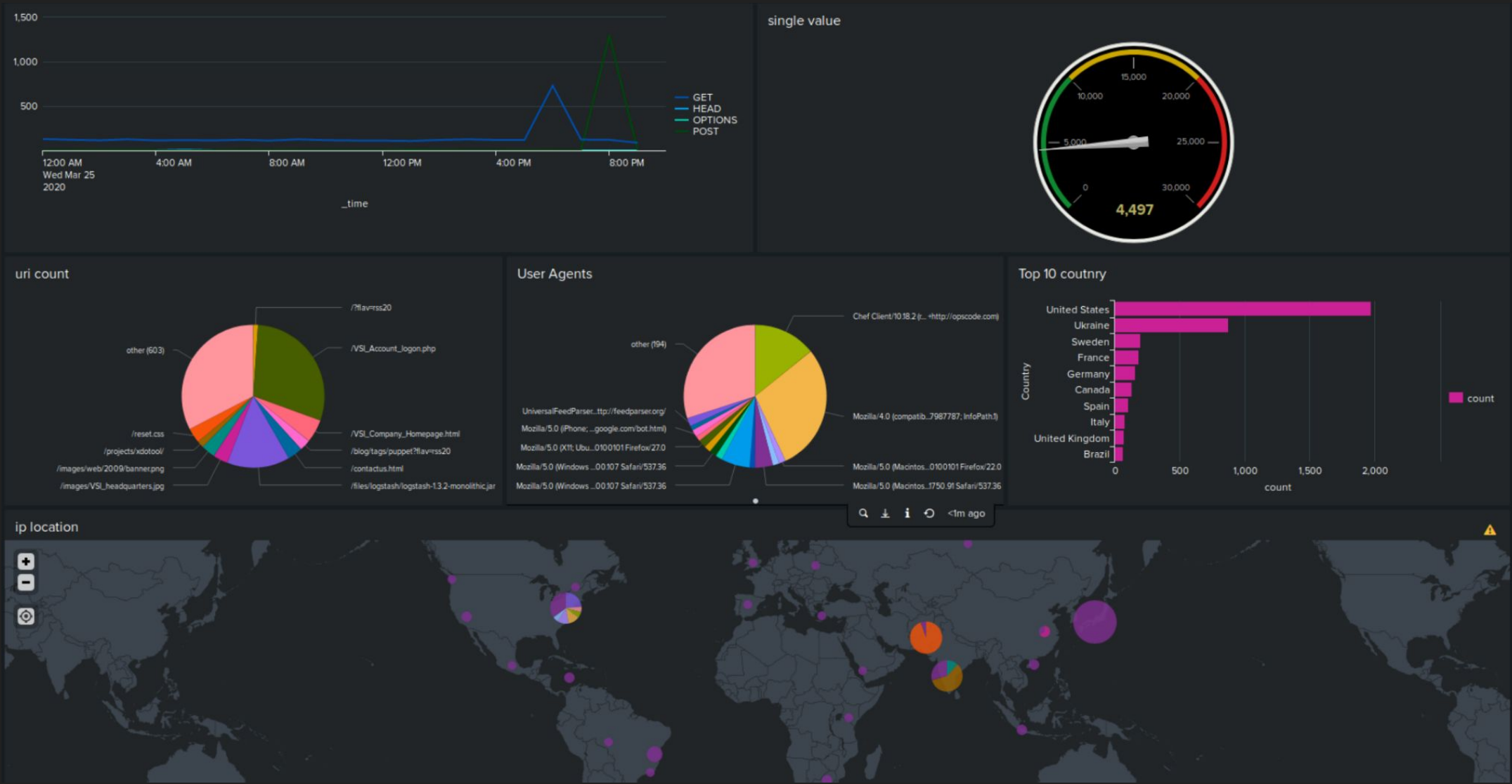
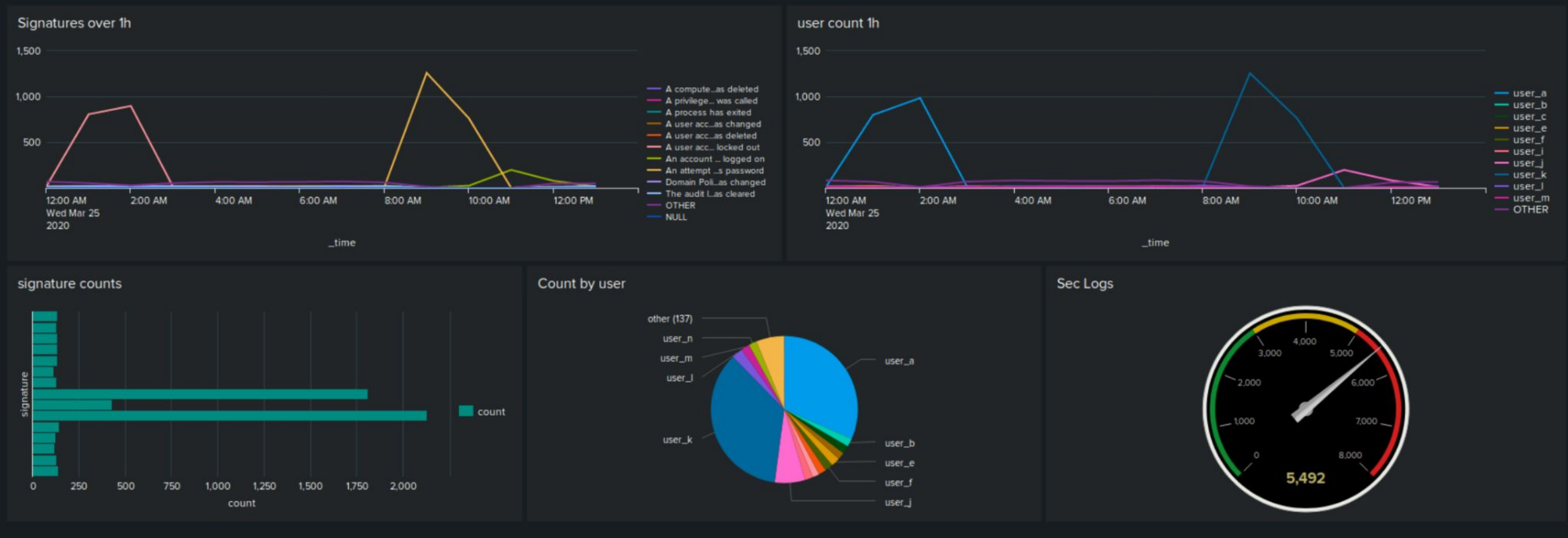
Attack Summary—Apache

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

- Suspicious spike in POST and GET requests on 03/25/20
- Non-US country login attempts with high rates in Kiev, Ukraine
- High rates of VSI account logon (1323)



Screenshots of Attack Logs



Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?

Windows Server:

- Unusual account logins from users a, k, and j
- Suspicious attempts to reset passwords and user lockout

Apache Server:

- Attacker in Ukraine attempting Brute Force Attack at the VSI website

- To protect VSI from future attacks, what future mitigations would you recommend?
 - Restrict high levels of account logins and password resets