

Project 3

Defensive Security Project

by: Victor, Raul, Caleb, Emily & Tim



Table of Contents

This document contains the following resources:

01

Monitoring The Environment

- **Add-On App**
- **Windows log Reports**
- **Apache log Reports**
- **Alerts**

02

Attack Analysis

- **Apache Dashboards**
- **Windows Dashboards**
- **Alerts**

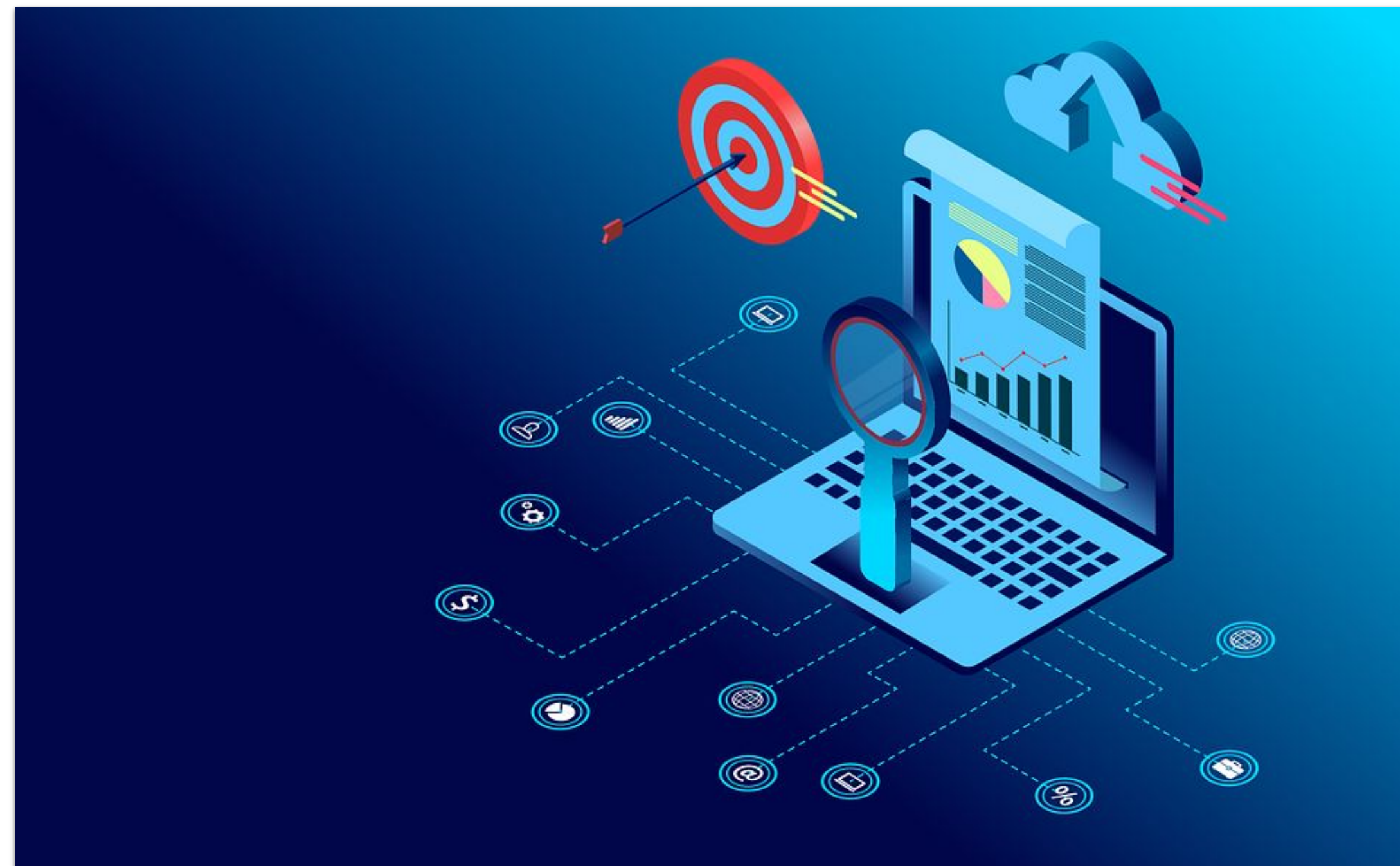
03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

The scenario of our analysis is to monitor against past logs to develop baselines and creating reports, alerts, & dashboards for the company Virtual Space Industries (VSI).



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.

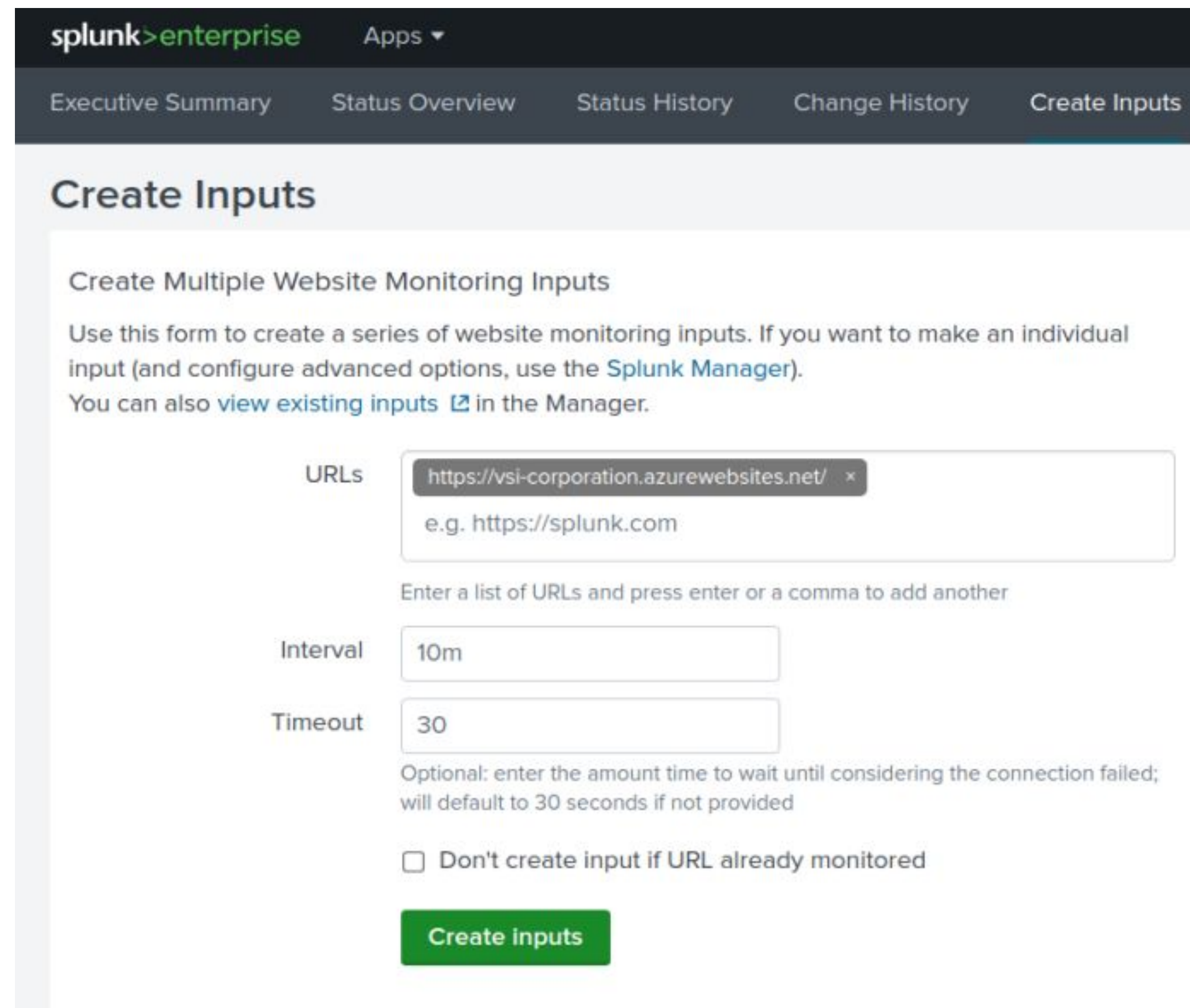
Add-on App Used:
Website Monitoring

Website Monitoring

- **The Website Monitoring app is a tool used to monitor the availability and performance of websites. It provides real-time visibility into the status of web applications and servers and allows administrators to quickly identify and troubleshoot issues.**
- **Benefits:**
 - Real-time monitoring: monitors website performance and availability in real-time and provides alerts when issues arise.
 - Customizable dashboards: allows administrators quickly analyze website performance data.
 - Integration with other Splunk apps: provides a comprehensive view of IT infrastructure.
 - Trend analysis: helps identify performance issues over time.
 - Scalability: can be easily scaled to accommodate large websites or complex web applications.

Website Monitoring

- Using the URL of VSI's website, <https://vsi-corporation.azurewebsites.net/>, we can enter this into the URL box under the “Create Inputs” tab from the toolbar.



The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and an 'Apps' dropdown. Below this is a secondary navigation bar with tabs: 'Executive Summary', 'Status Overview', 'Status History', 'Change History', and 'Create Inputs'. The 'Create Inputs' tab is selected. The main content area is titled 'Create Inputs' and contains the following text: 'Create Multiple Website Monitoring Inputs', 'Use this form to create a series of website monitoring inputs. If you want to make an individual input (and configure advanced options, use the [Splunk Manager](#)).', and 'You can also [view existing inputs](#) in the Manager.' Below this text are three input fields: 'URLs' with a value of 'https://vsi-corporation.azurewebsites.net/' and a placeholder 'e.g. https://splunk.com'; 'Interval' with a value of '10m'; and 'Timeout' with a value of '30'. Below these fields is a checkbox labeled 'Don't create input if URL already monitored'. At the bottom is a green button labeled 'Create Inputs'.

splunk>enterprise Apps ▾

Executive Summary Status Overview Status History Change History Create Inputs

Create Inputs

Create Multiple Website Monitoring Inputs

Use this form to create a series of website monitoring inputs. If you want to make an individual input (and configure advanced options, use the [Splunk Manager](#)).
You can also [view existing inputs](#) in the Manager.

URLs
e.g. https://splunk.com

Enter a list of URLs and press enter or a comma to add another

Interval

Timeout

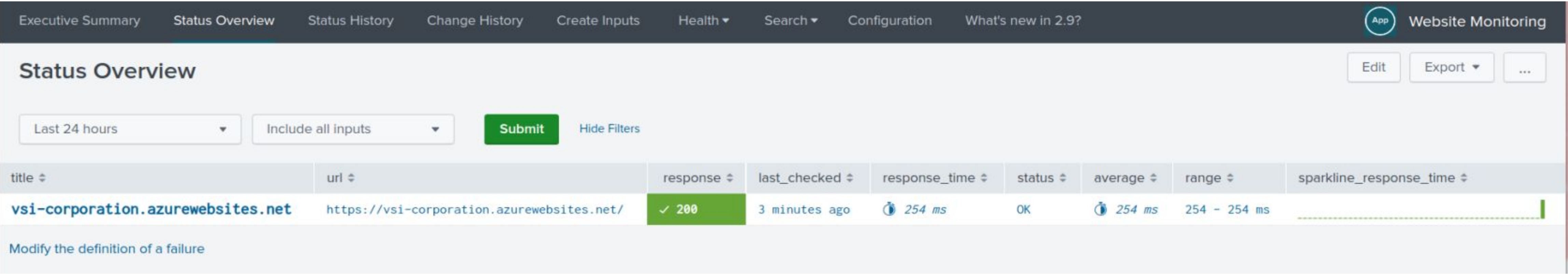
Optional: enter the amount time to wait until considering the connection failed;
will default to 30 seconds if not provided

☐ Don't create input if URL already monitored

Create Inputs

Website Monitoring

- After confirming the input and selecting “Status Overview”, you will be able to see the status of the website, the HTTP response code (200), and its response time.



Logs Analyzed

1

Windows Logs

Windows Logs Data

1. 4672 - new privileges -25 High
2. 4743 - Accounts Deleted - 20 High
3. 4624 - Successful Login - 25 High
4. 4740 - User Locked Out - 23 High
5. 4724 - Attempt To Reset An Account Password - 20 High
6. Failure Status - 15 High
7. Domain_* - 60 High
8. user_*285 excl user_I - 360

2

Apache Logs

Apache Logs Data

1. HTTP Method Count
2. VSI Top 10 Referrer Domains
3. HTTP Response Code Count
4. Get - 118 (constant) - 120 high
Head - 0-1 (inconsistent) - 3 high
Options - 0 - alert on any activity*
Post - 2-3 (inconsistent) - 4 high

Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
signature_id	This report describes the number of reset password attempts that have been made.
signature	Displays successful logins
user	Displays users activity in between times
status	Displays the status of the number of success and failure counts
severity	Defines the impact or importance of an event or case.

Images of Reports—Windows

Signature Report

Edit ▾

More Info ▾

Add to Dashboard

All time ▾

✓ 15 events (before 2/3/23 1:46:13.000 AM)

Job ▾

⏸

■

🔄

➡

🖨

⬇

15 results

20 per page ▾

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

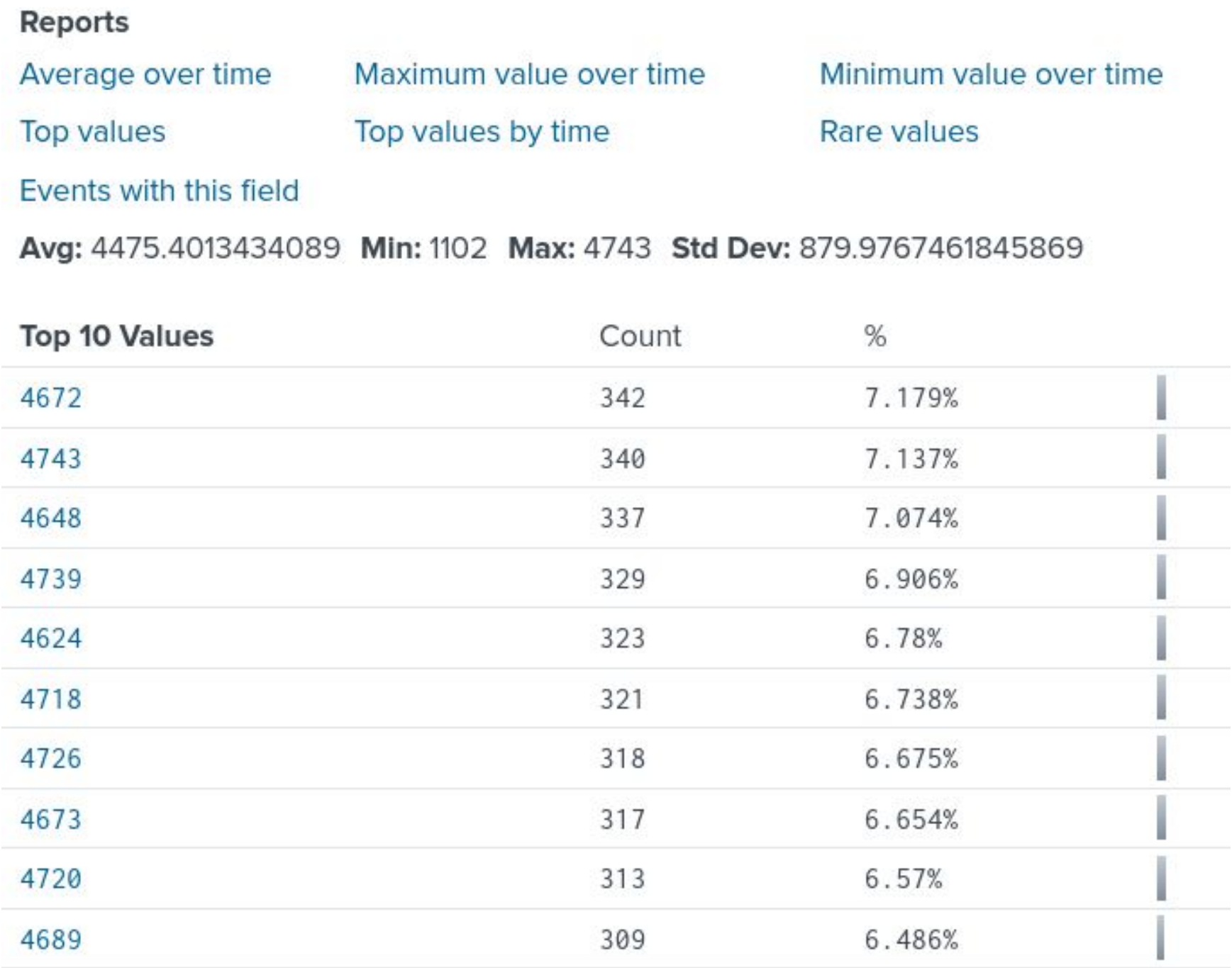
</

signature report

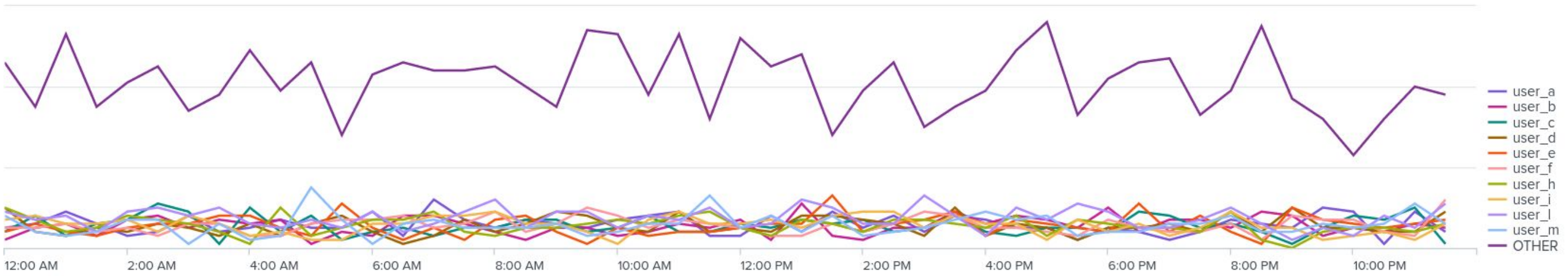
Top 10 Values	Count	%	
Special privileges assigned to new logon	342	7.179%	
A computer account was deleted	340	7.137%	
A logon was attempted using explicit credentials	337	7.074%	
Domain Policy was changed	329	6.906%	
An account was successfully logged on	323	6.78%	
System security access was removed 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%	

Top Ten Values

Images of Reports—Windows

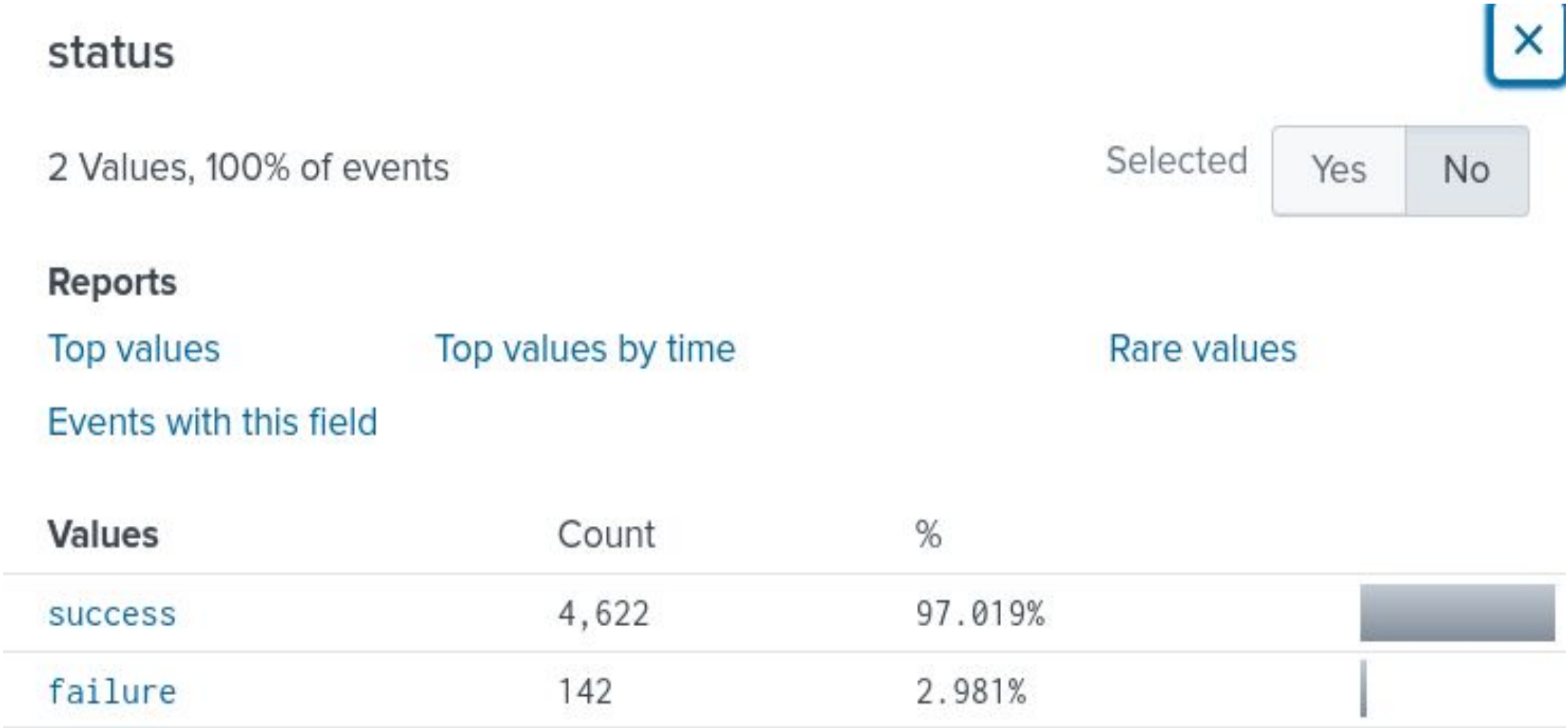


signature_id image

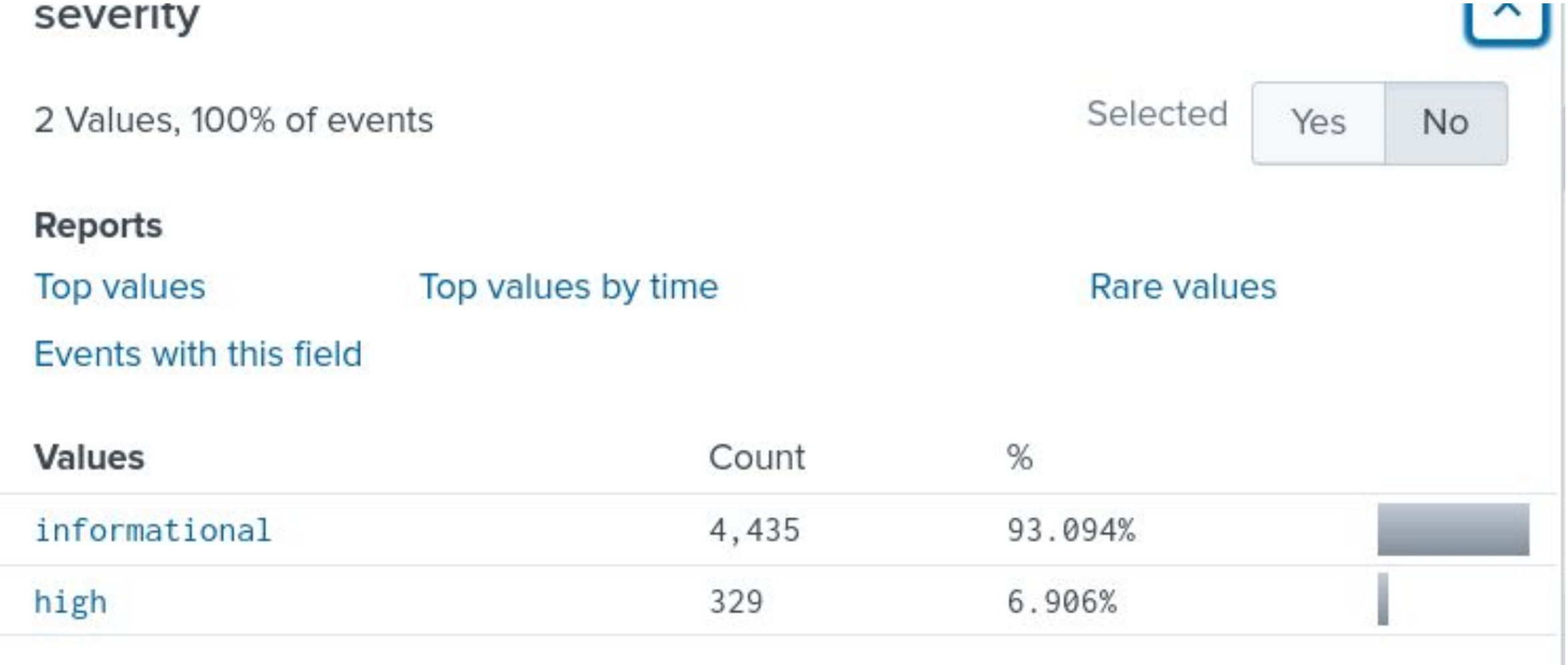


user graph chart image

Images of Reports—Windows



status image



severity image

Images of Reports—Windows

15 results 20 per page ▼

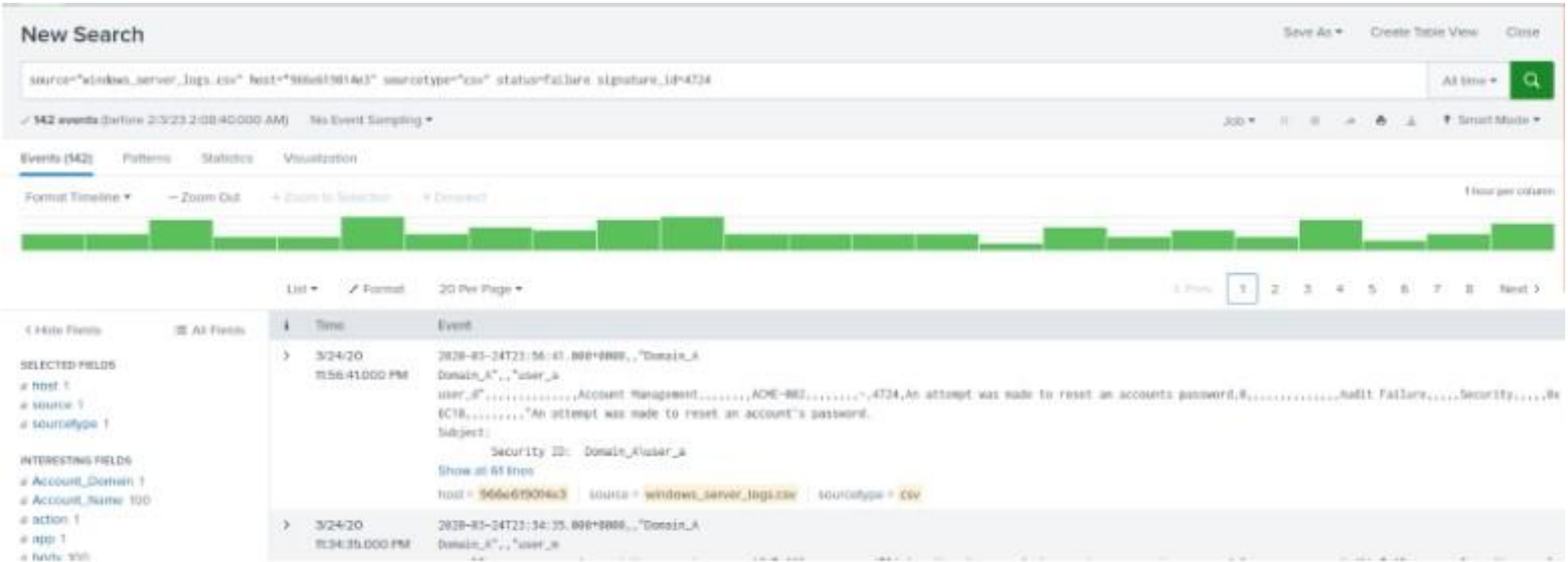
signature ↕	signature_id
A user account was deleted	47
A user account was created	47
A computer account was deleted	47
An account was successfully logged on	46
Special privileges assigned to new logon	46
An attempt was made to reset an accounts password	47
System security access was granted to an account	47
A privileged service was called	46
A logon was attempted using explicit credentials	46
A user account was locked out	47
Domain Policy was changed	47
A user account was changed	47
A process has exited	46
The audit log was cleared	11

The Whole Windows Log Report

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
signature	Reset Account Password Attempts	[Baseline]	20 High



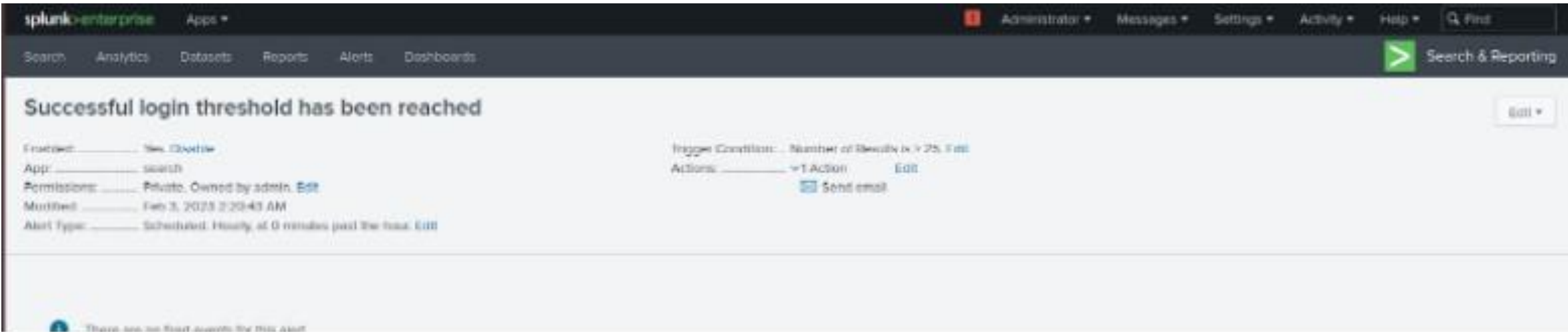
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
signature_id	shows successful logins	[Baseline]	25

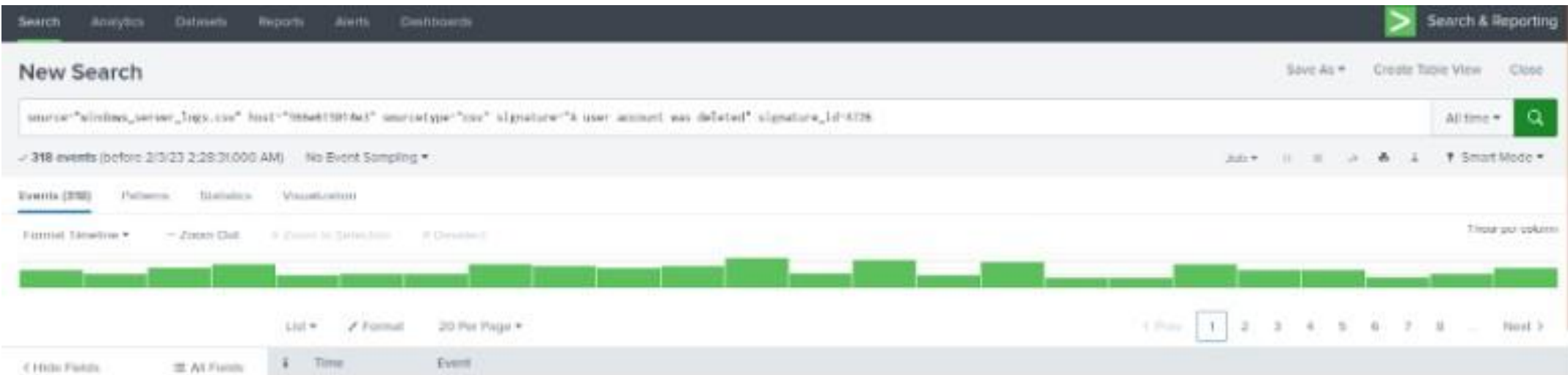


This chart displays the normal baseline of successful logins. A threshold has been created

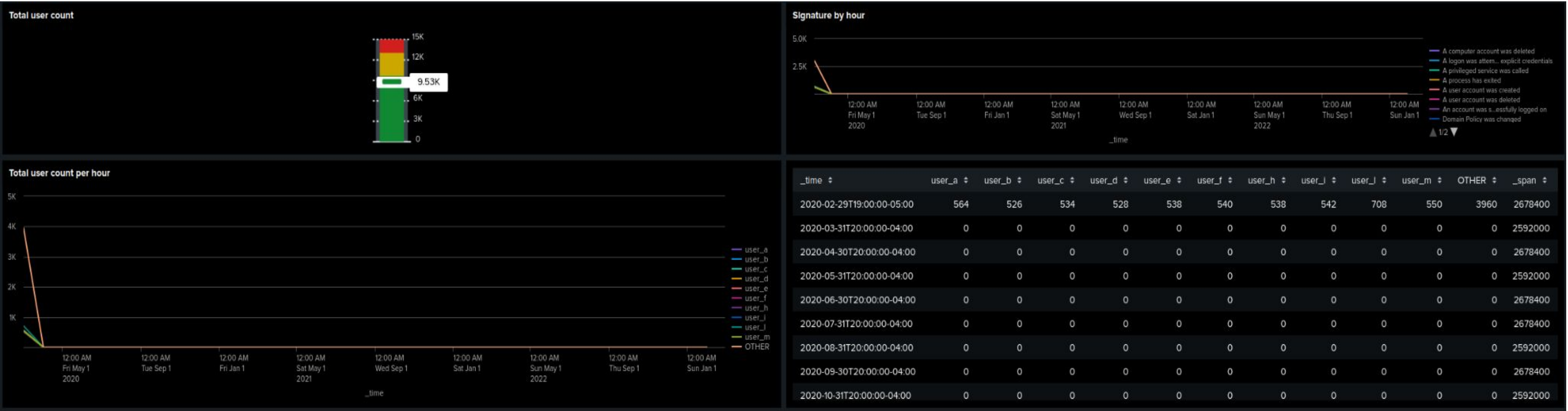


Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
user	user account deletion	[Baseline]	23



Dashboards—Windows



Total user number
source="windows_server_logs.csv"
host="966e619014e3" sourcetype="csv" | top
limit=10000 user | stats sum(count) AS total

Signature by hour:
source="windows_server_logs.csv"
host="966e619014e3" sourcetype="csv" | timechart
count by signature limit=10

Total user count per hour
source="windows_server_logs.csv"
host="966e619014e3" sourcetype="csv" | timechart
count by user limit=10



Total signature
source="windows_server_logs.csv"
host="966e619014e3" sourcetype="csv" | top
limit=50 signature

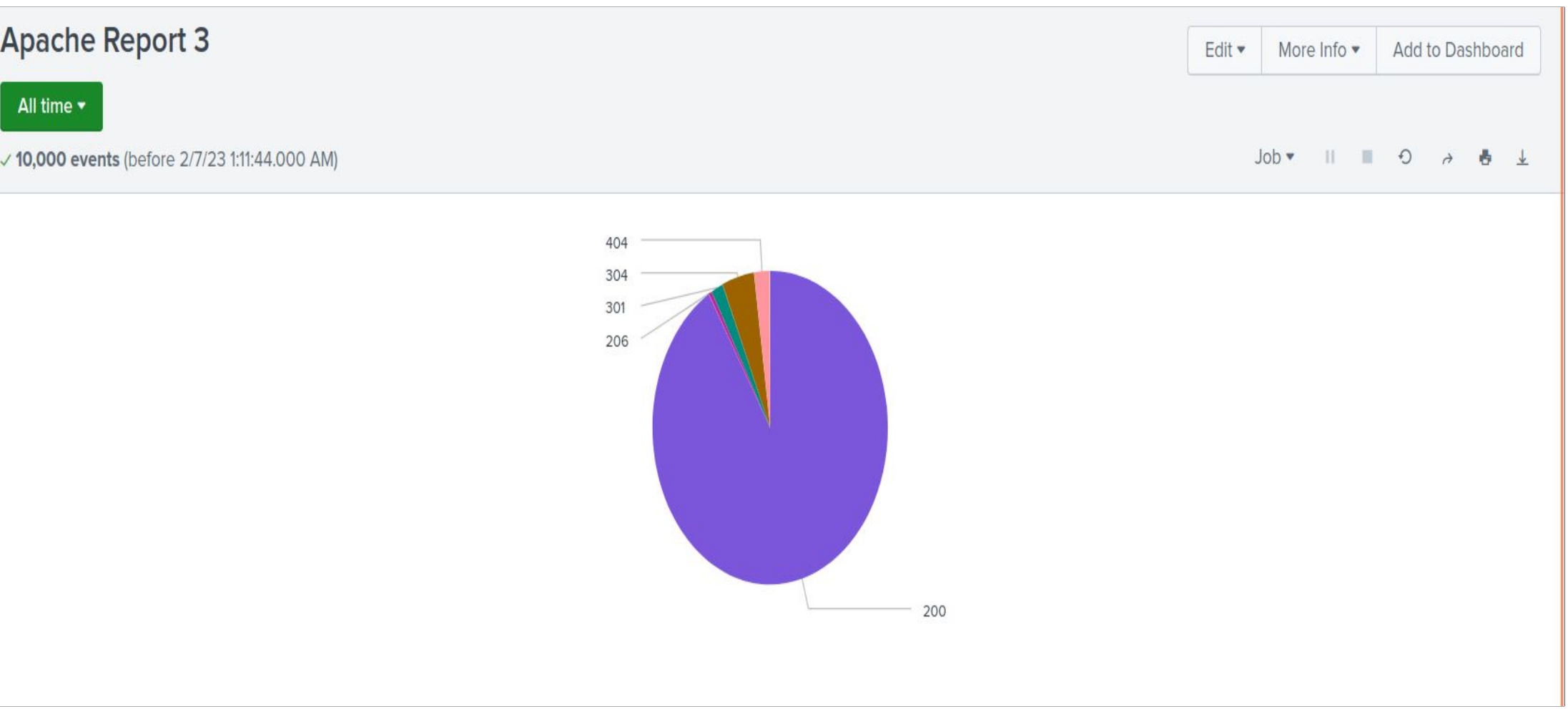
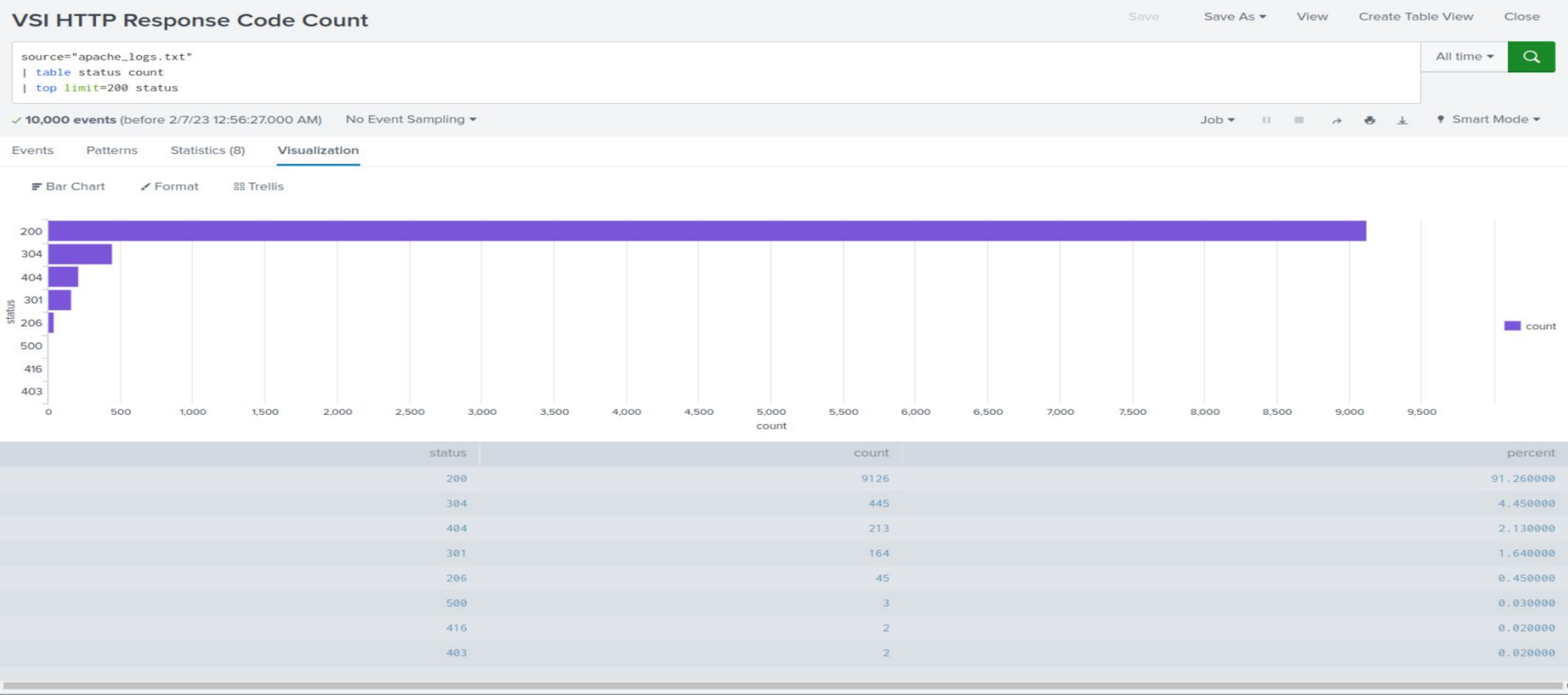
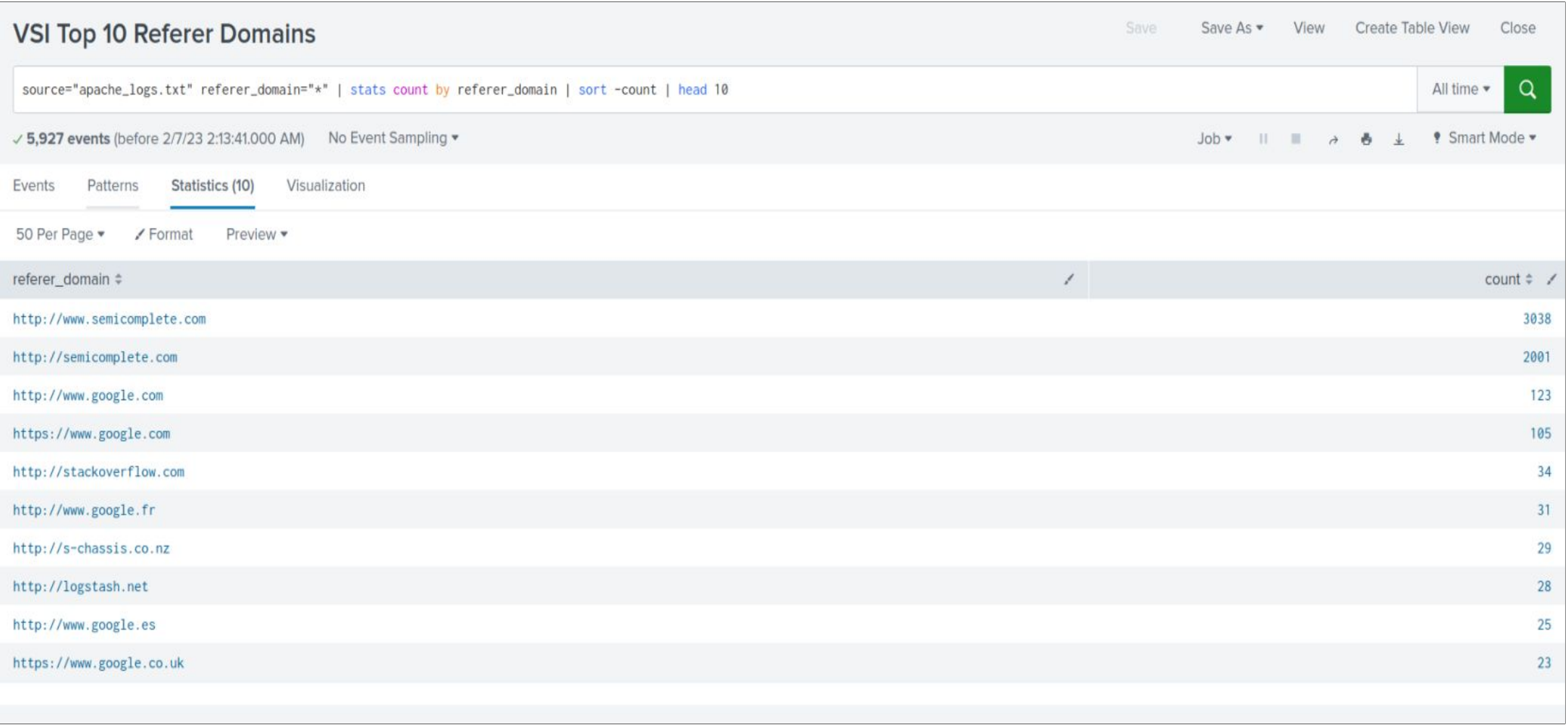
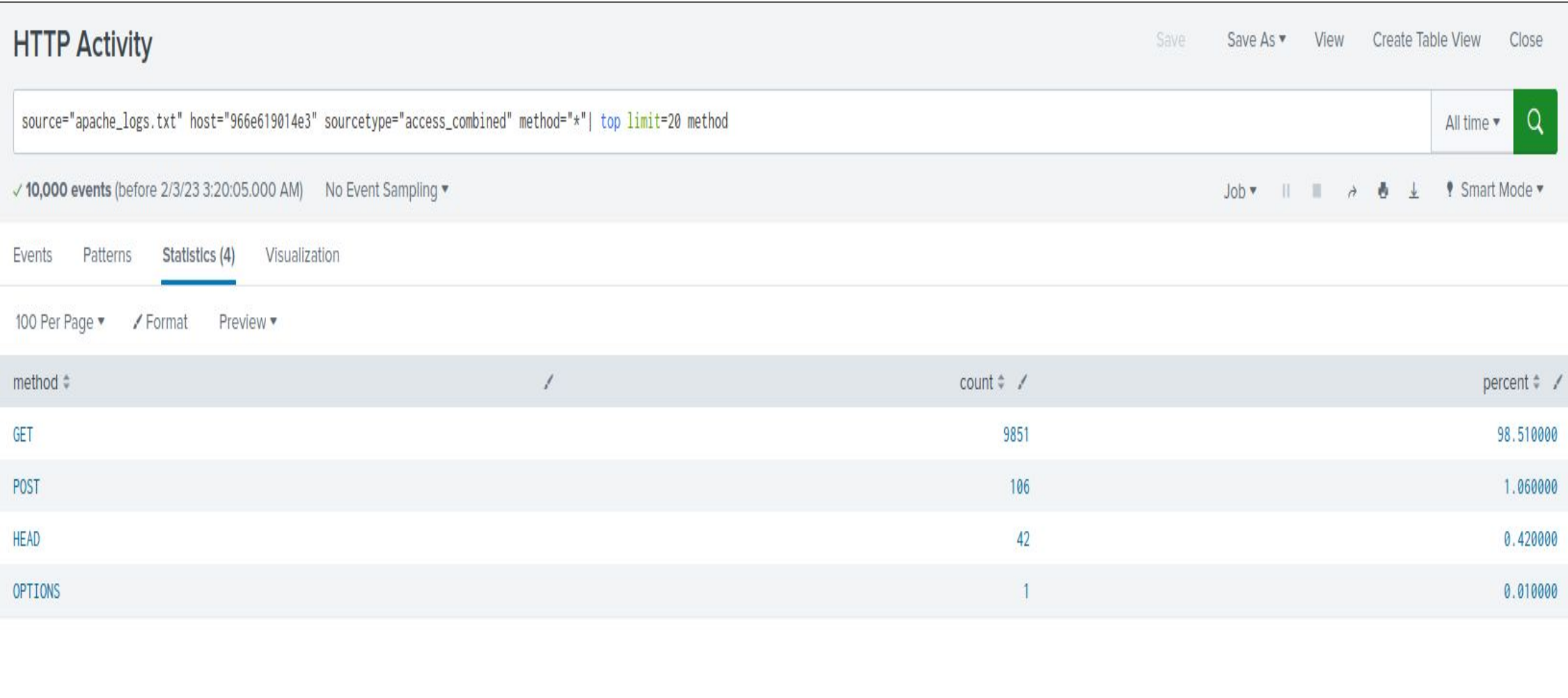
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Method Count	Provides insight for types of HTTP activity requested from the Web Server
VSI Top 10 Referrer Domains	Used to assist in identifying suspicious referrer domains
HTTP Response Code Count	Provides insight on any suspicious levels of HTTP responses

Images of Reports—Apache



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI International Threshold Reached	The hourly threshold of use outside the United States has been reached	120 events per hr	240 events per hr

JUSTIFICATION: The baseline represents the average amount of events that occur in an hour, and the threshold was set as twice the amount of average events in an hour.

Alerts—Apache

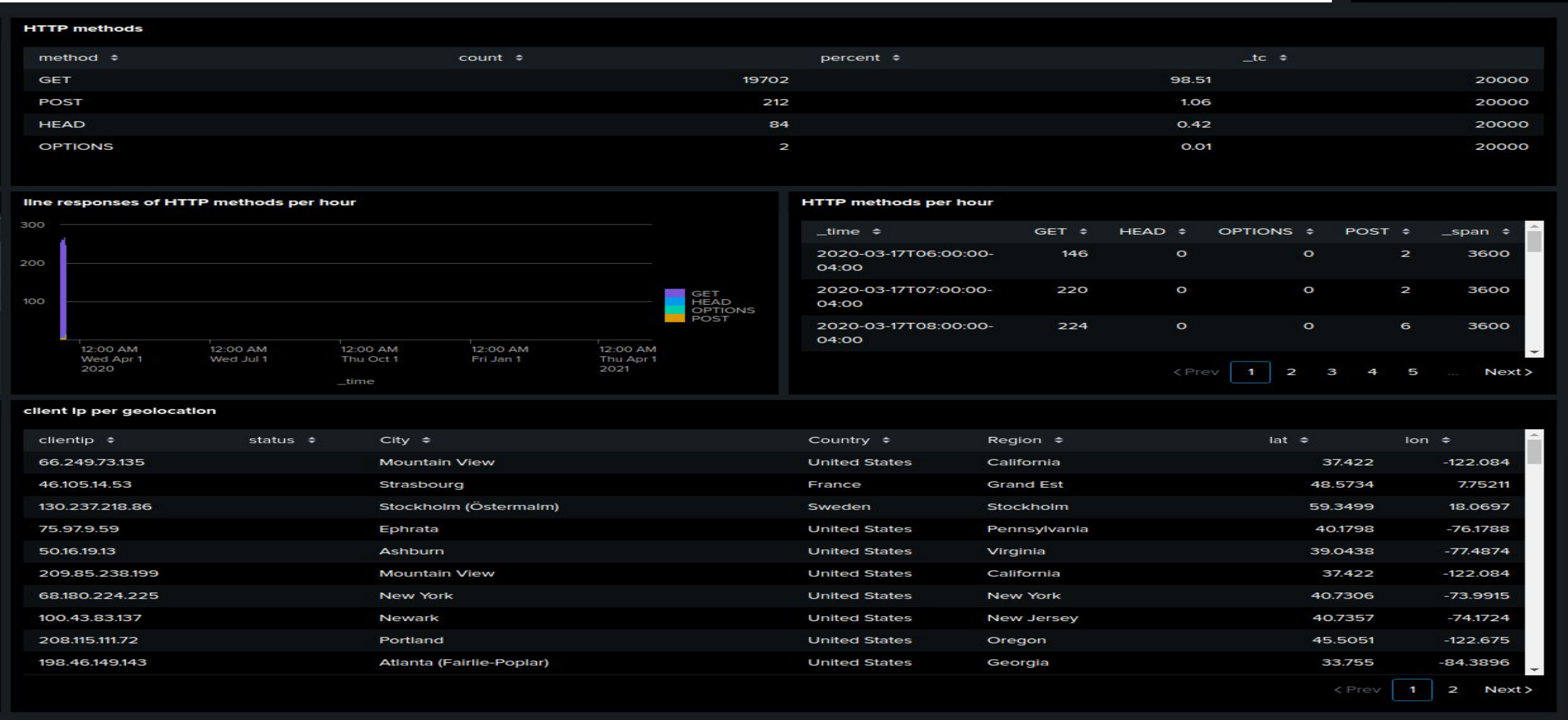
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Threshold Reached	The threshold of POST methods was reached.	1.27 events per hour	12 events per hour

JUSTIFICATION: The baseline represents the average amount of events in an hour, and the threshold was determined by multiplying the average amount of events by ten the rounding.

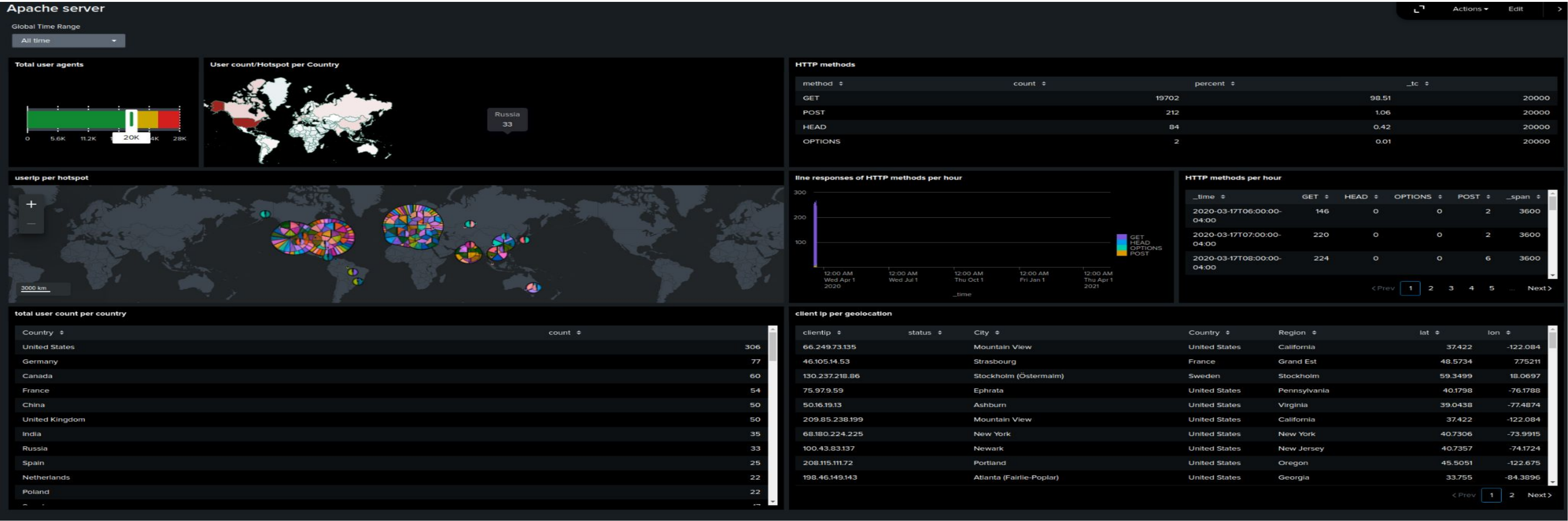
Dashboards—Apache

- User count/Hotspot per Country
- Total user agents
- total user count per country



- client ip per geolocation
- HTTP methods per hour/line responses of HTTP methods per hour

Apache DashBoard



User count/Hotspot per Country:
source="apache_logs.txt" host="966e619014e3" | top limit=1000 clientip | table clientip, status, City, Country, count | iplocation clientip | stats count by Country | sort - count | geom geo_countries featureIdField="Country"

userip per hotspot:
source="apache_logs.txt" host="966e619014e3"| top limit=200 clientip | table clientip, status, City, Country | iplocation clientip | geostats count by clientip globallimit=300

Total user agents
source="apache_logs.txt" host="966e619014e3" useragent="*" | top limit=1000 useragent | stats sum(count) AS total

HTTP methods:
source="apache_logs.txt" host="966e619014e3" sourcetype="access_combined" method="*" | top limit=20 method

HTTP methods per hour/line responses of HTTP methods per hour:
source="apache_logs.txt" host="966e619014e3" sourcetype="access_combined" method="*" | timechart span=1h count by method

total user count per country
source="apache_logs.txt" host="966e619014e3" | top limit=1000 clientip | table clientip, status, City, Country, count | iplocation clientip | stats count by Country | sort - count

client ip per geolocation
source="apache_logs.txt" host="966e619014e3"| top limit=200 clientip | table clientip, status, City, Country | iplocation clientip

Attack Analysis

Attack Summary—Windows

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

Baselines:

Total 220 events

Total 20 events severity=high

4672 - new privileges - 25 high

4743 - account deleted - 20 high

4624 - successful login - 25 high

4740 - user locked out - 23 high

4724 - attempt to reset an account password -20 high

Failure status - 15 high

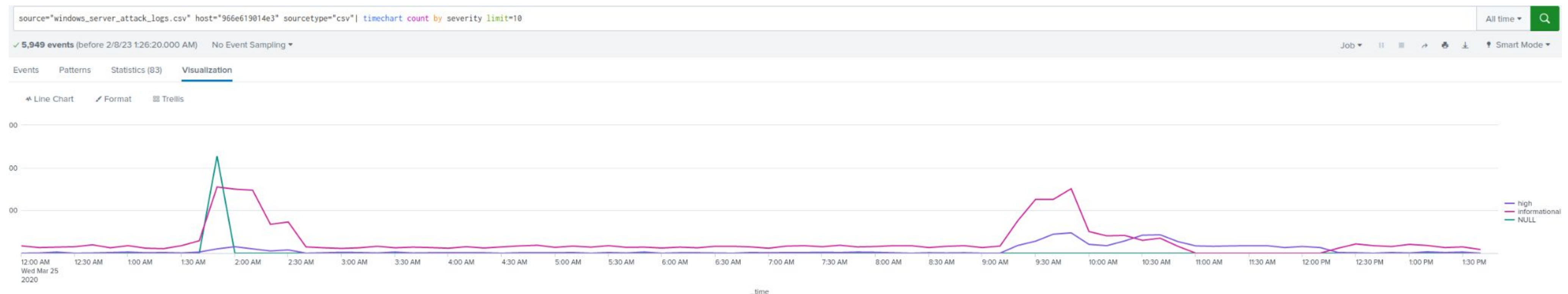
Domain_* - 60 high

user_*285 excl user_I - 360

Attack Summary—Windows

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

- We had a failure on our reports because of a Null signature show from 1:30am to 2:00am where over 400 events happened outside our baseline.
- We had a higher threshold for high severity which caused a late report.
- Overall our other levels and baselines showed a good levels and worked well.



Attack Summary—Apache

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

Method Baselines:

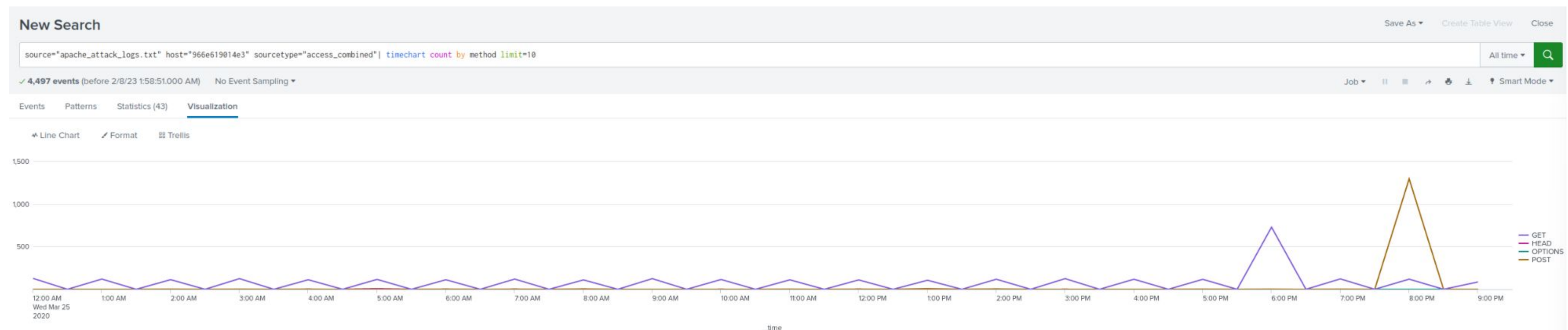
Base lines

Get - 118 (constant) - 120 high

Head - 0-1 (inconsistent) - 5 high

Options - 0 - alert on any activity*

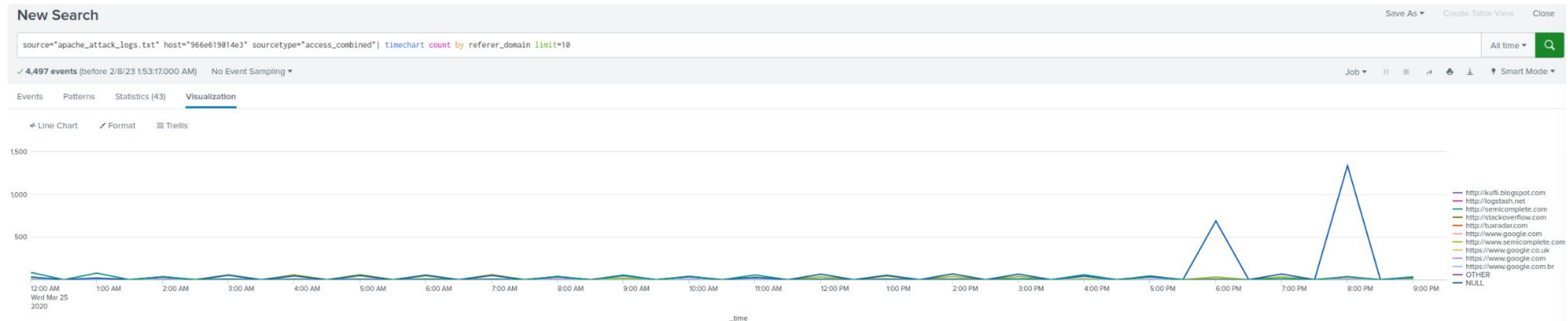
Post - 2-3 (inconsistent) - 5 high



Attack Summary—Apache

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

- Null and unread readings Spike from 5:30pm to 8:30pm
- All other domains kept under same conditions.



Attack Summary—Apache

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

- On the Apache dashboards, you can see the number of Users and Hotspots per country. The dashboards also show the Client IP per Geolocation and HTTP Methods. There was a significant change in the HTTP Response Codes especially in the increase of response code 404 and the decrease of 200. There was suspicious volume of HTTP POST activity. This suspicious volume occurred at 8PM with 1,296 events in just that hour. After further review, the threshold should be raised to 20-30 events an hour.

Summary and Future Mitigations

Project 3 Summary

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

- Multiple different attacks throughout the day. There were user account changes. Peaking use and user actions from a different country and ip unknown. There was suspicious volume of HTTP POST activity. This suspicious volume occurred at 8PM with 1,296 events in just that hour. Null signature show from 1:30am to 2:00am where over 400 events happened.

To protect VSI from future attacks, what future mitigations would you recommend?

- Correct add-ons and features to help identify and respond to attacks accordingly
- Further Access Denial
- Solid and equal monitoring during dead hours and working hours as attacks did not discriminate on time. As well as having world wide times.
- A good core of protection on the apache server to mitigate possible Ddos attacks.
- We can show that with the correct baselines and response we can mitigate a good majority of the attacks.
- Account protection - password changes and lockout standard work