Defensive Security Project
by:
InfoSec Chillers Study Group

Gorin, Michael
Kamimura, Matt
Maurer, Chris
Meadow, Michael
Mosburg, Leon
Villanueva, Marc

We doin' big chillin', we securin' all these. (Check 'em out now.) Big chillin' on too many screens.

Table of Contents

This document contains the following resources:

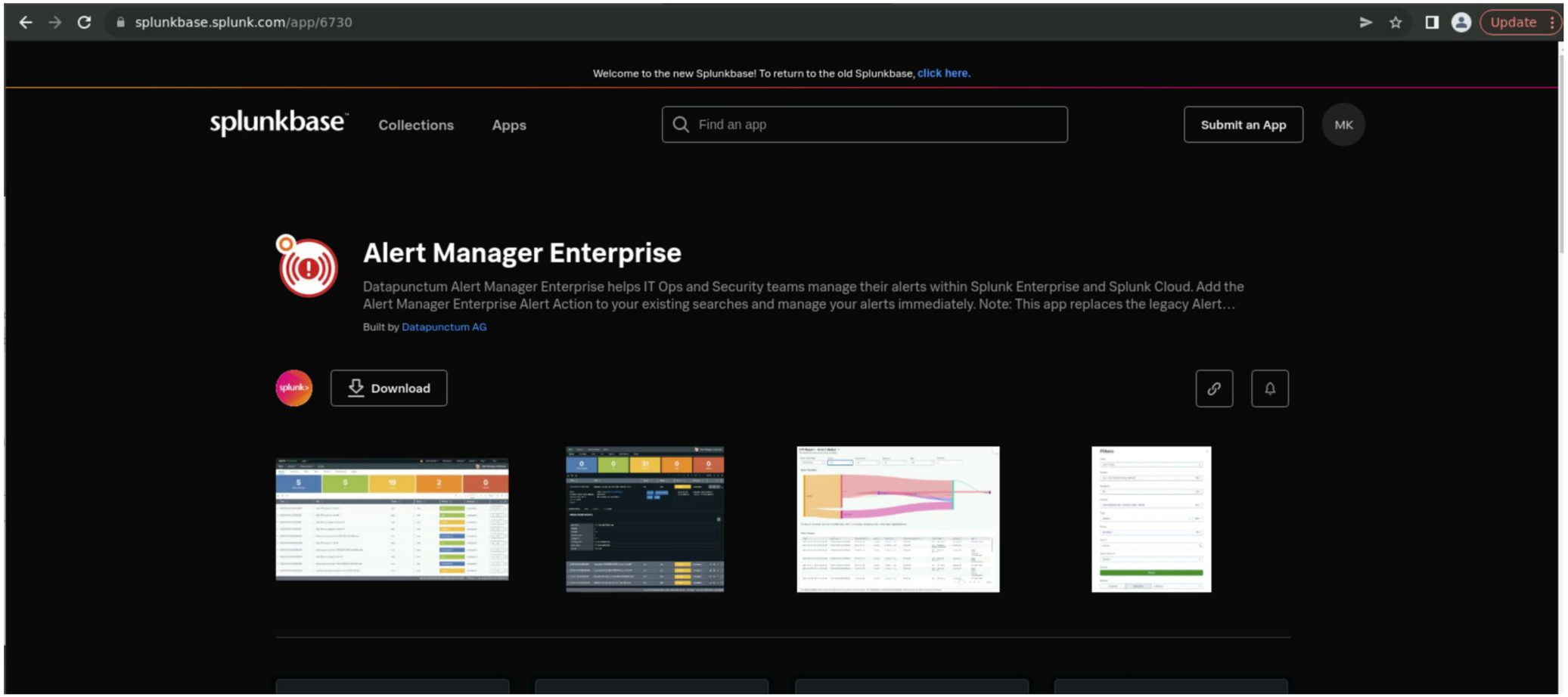
Monitoring Environment

Scenario

- Create a dashboard in Splunk that displays a baseline of statistics for Windows and Apache by using existing data logs to determine what normal daily operations look like for Virtual Space Industries (VSI). The baseline statistics are to then used to compare to data logs captured during and after a cyber attack on VSI.
- Detail mitigations to help prevent future attacks.


["Add-On" App]

[ALERT MANAGER ENTERPRISE]



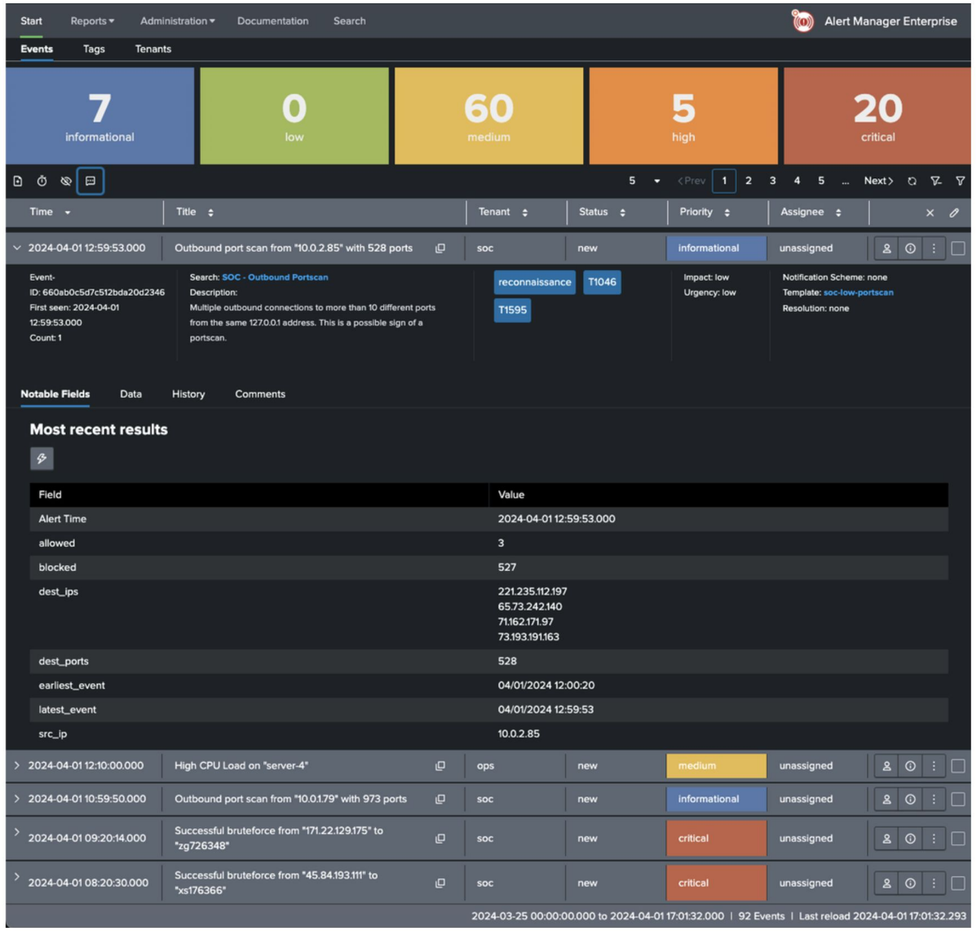
Alert Manager Enterprise

What is Alert Manager Enterprise?

Datapunctum Alert Manager Enterprise (AME) helps IT Ops and Security teams manage their alerts within Splunk Enterprise and Splunk Cloud.

Add the Alert Manager Enterprise Alert Action to your existing searches and manage your alerts immediately.

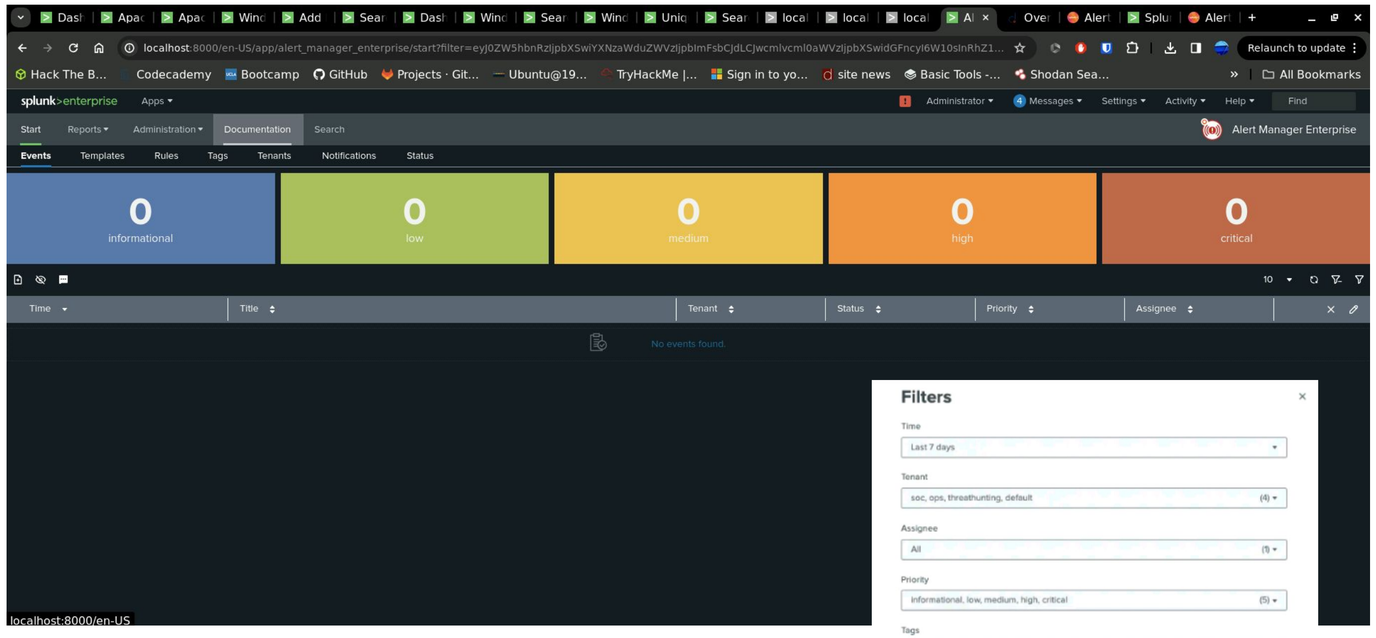
-https://docs.datapunctum.com/ame/

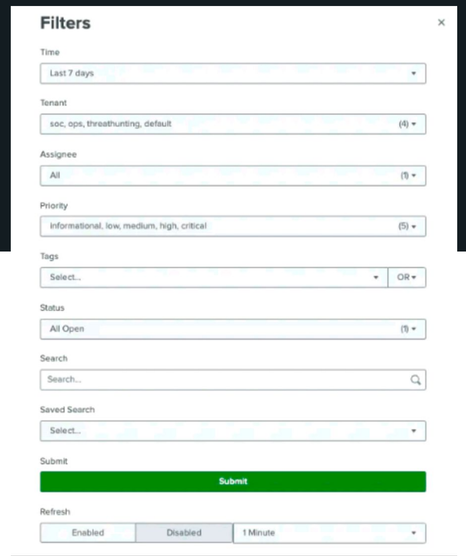


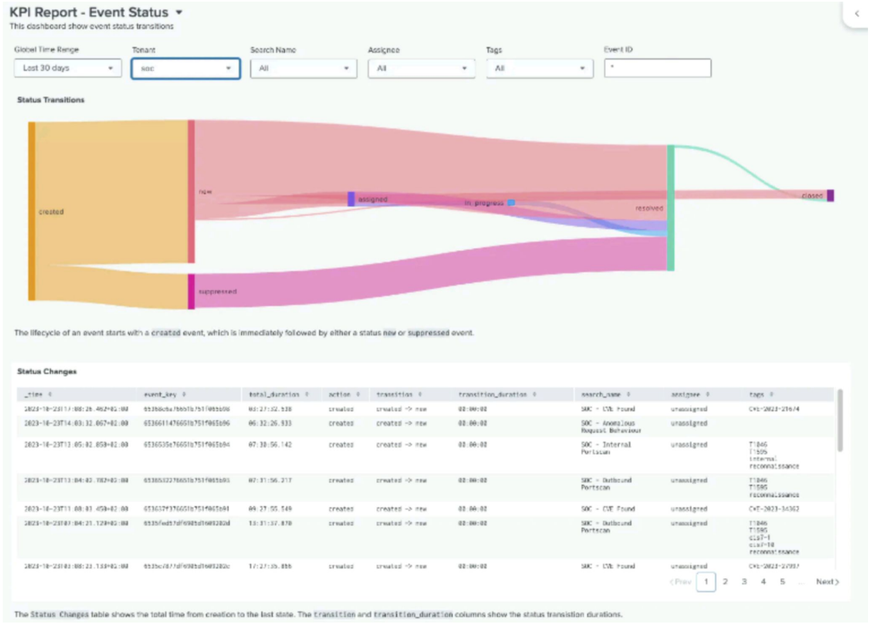
Alert Manager Enterprise

- Useful for organizations handling many alerts.
- Streamlines identification and response to critical issues.
- Provides customizable notifications and access control.
- Helps prioritize and investigate potential threats.
- Enhances security and operational efficiency.
- Moves beyond basic email alerting.
- Integrated notification schemes for targeted communication.

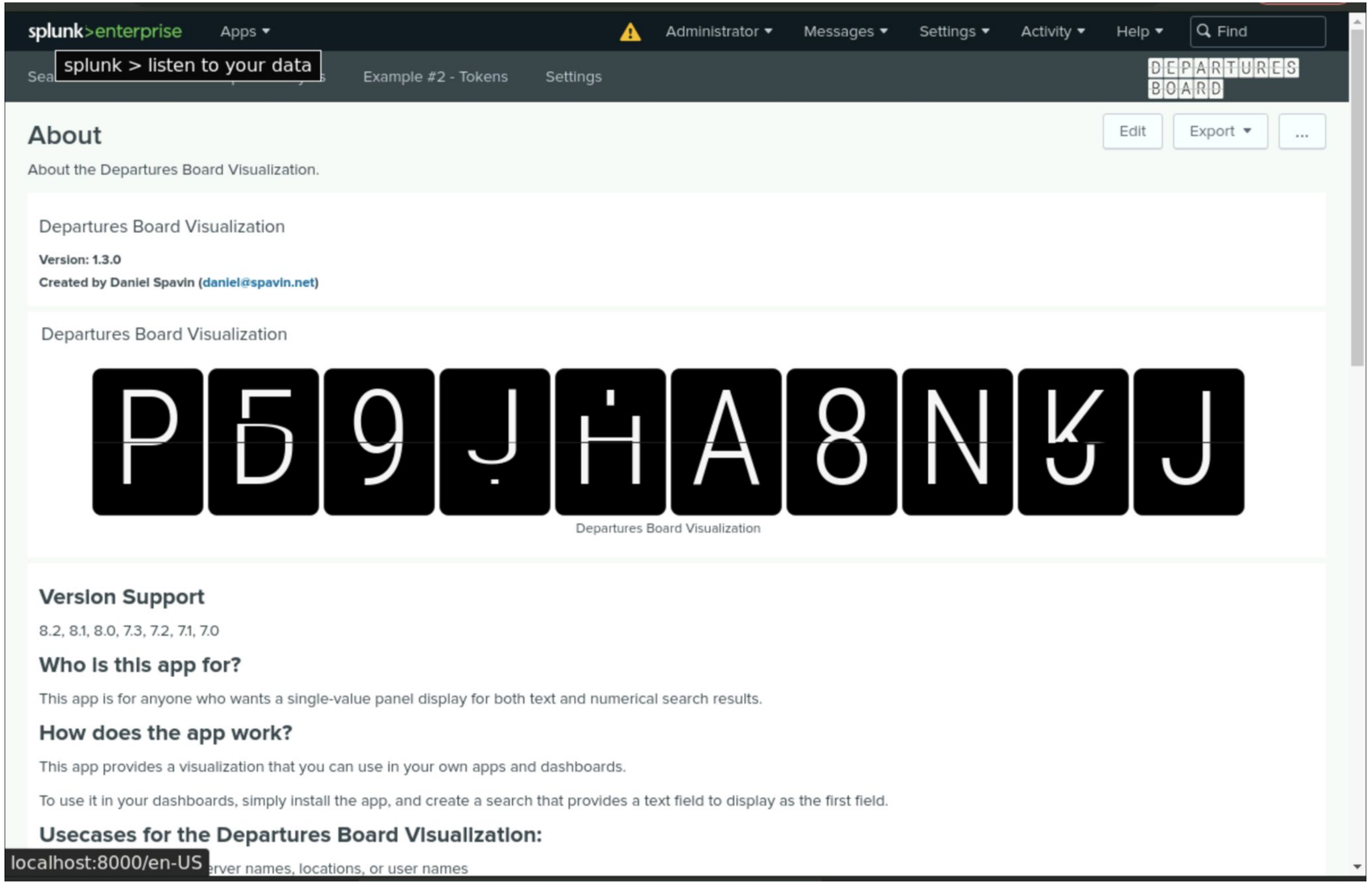
Alert Manager Enterprise







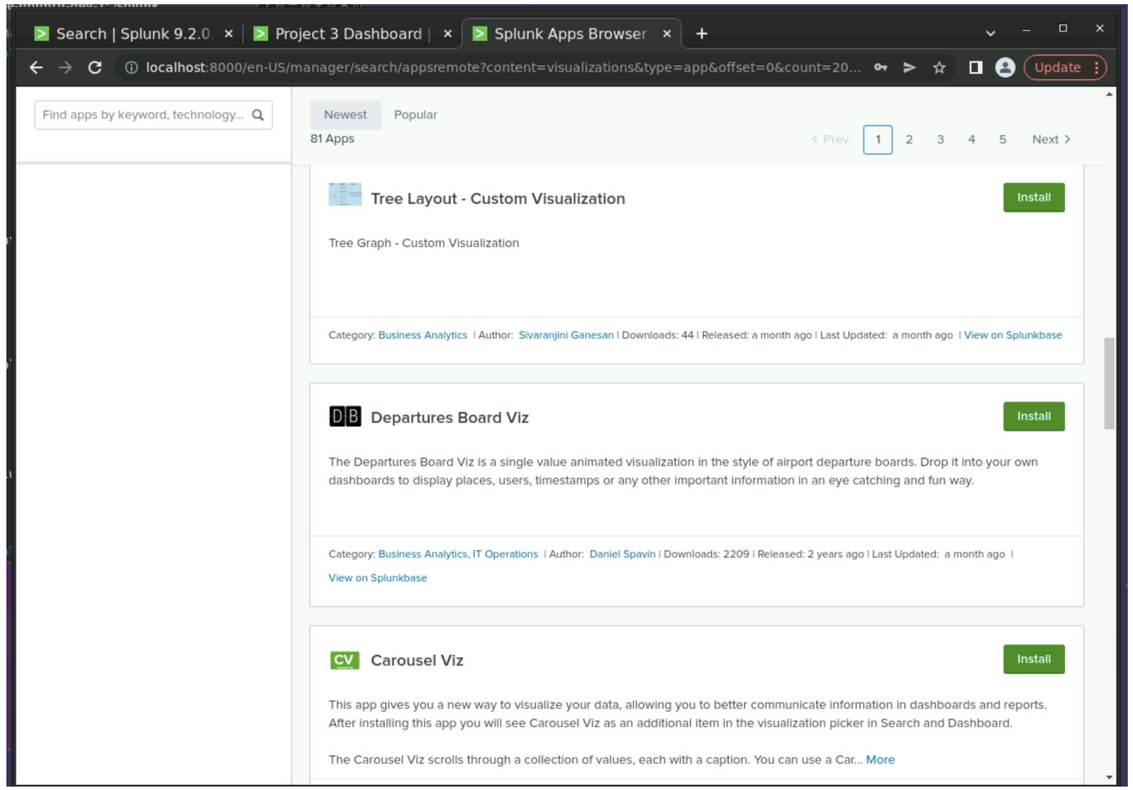
[Departures Board Visualization]



[Departures Board Visualization]

“The Departures Board Viz is a single value animated visualization in the style of airport departure boards. Drop it into your own dashboards to display places, users, timestamps or any other important information in an eye catching and fun way.”

-https://splunkbase.splunk.com/app/4292



[Departures Board Visualization]

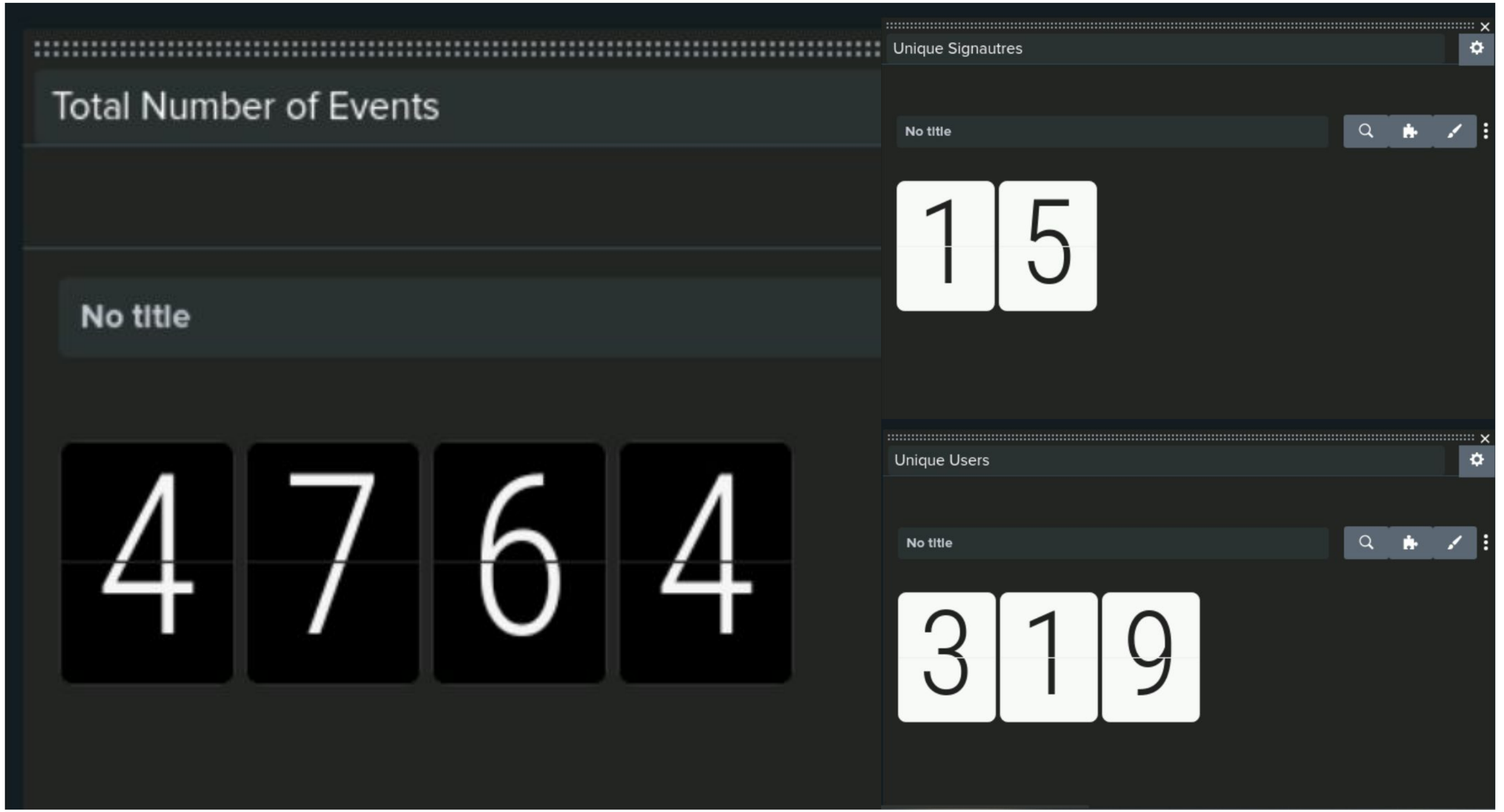
INT. CLASSROOM - NIGHT

A COMPUTER MONITOR sits on a 1950s school desk. The camera pushes in close to the screen, which is playing a video of an old BLACK AND WHITE TELEVISION COMMERCIAL....

MATT

Hello, friends. I’m your Departures Board Visualization guy.
Are you tracking timestamps, user data, and info?
Do you get tired of terminal? Are you untechnical?
The answer to all your problems is in this little add-on:
Departures Board Visualization.
Yes, Departures Board Visualization displays places,
users, timestamps, and any other important information.
Yes, with Departures Board Visualization, you can code your
way to visualizing. All you do is link a big Splunk report
after every data add.
It's so easy, too. It’s just like taking candy from a baby!
So, why don't you join the thousands of happy, peppy people,
and download a great big add-on of
Departures Board Visualization tomorrow.
That's Departures Board Visualization.

[Departures Board Visualization]



Logs Analyzed

1 Windows Logs

The windows logs primarily contain windows security events. Data is provided on existing user accounts, created accounts, deleted accounts, login attempts and successes and so on. The logs also provide potential security compromise data as well as event timings.

2 Apache Logs

HTTP Response Headers, HTTP Request Methods, Referring Domains, HTTP Status Codes, Geographical Location of IP Addresses, Times events occurred.

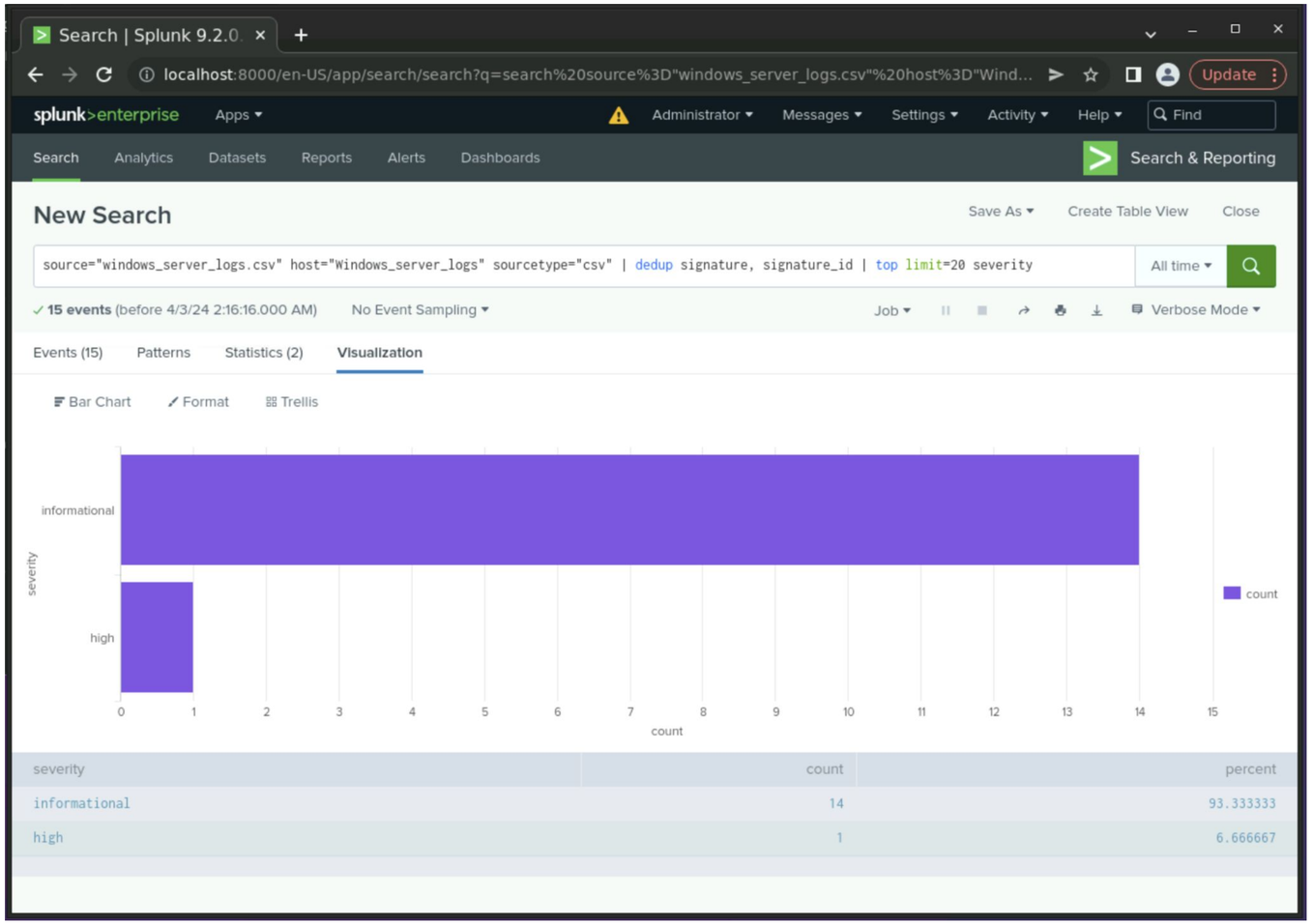

Windows Logs

Reports—Windows

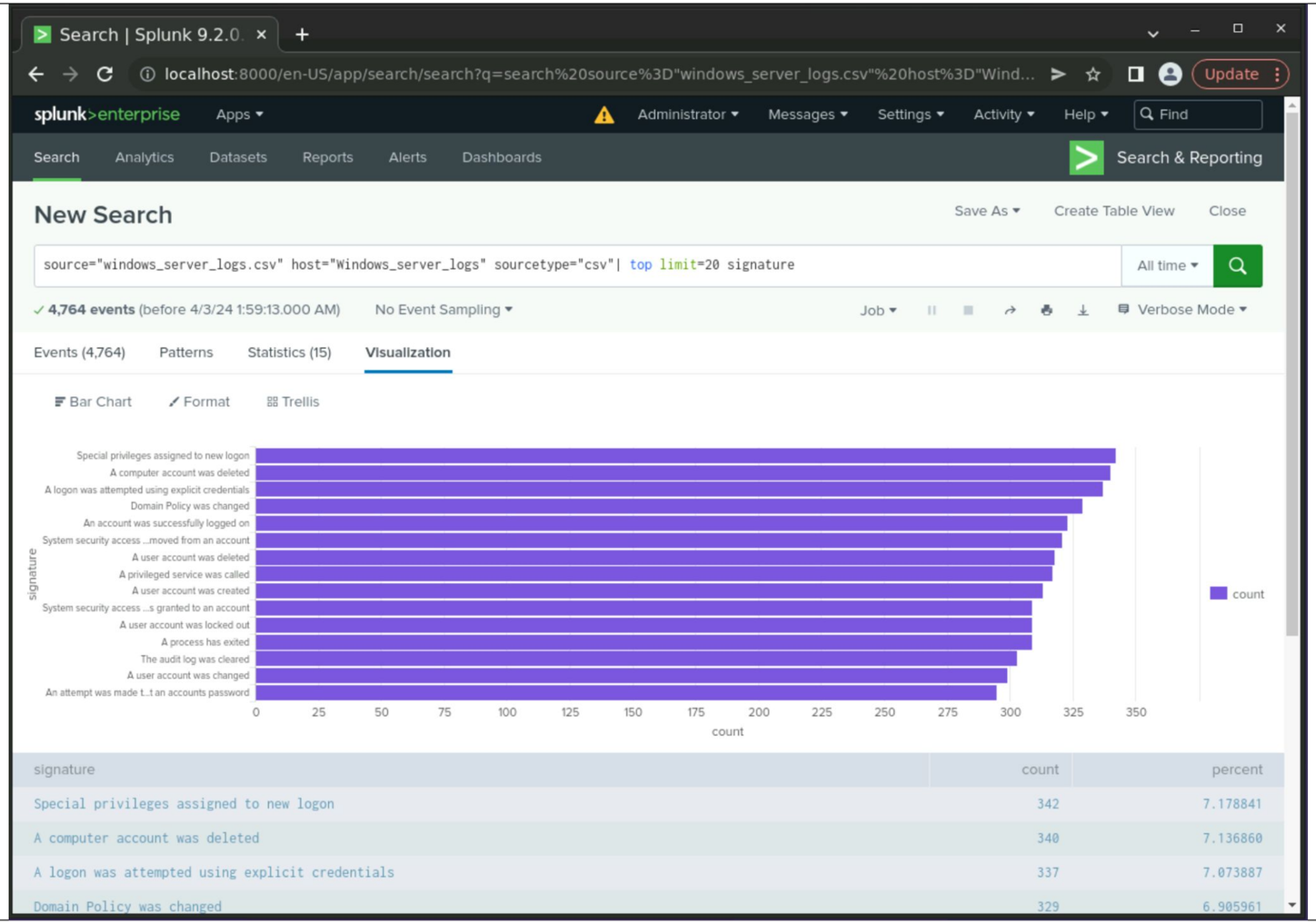
Designed the following reports:

Report Name	Report Description
Security Levels (Count & Percentage) REPORT	Bar chart showing various security events throughout a span of time by severity.
Signature & Signature ID REPORT	Bar chart that shows the counts and percentages of various system events as labelled by their Signature_ID.
Signature & Signature ID Stats REPORT	Statistics showing what system events the Signature_ID's are tied to.
Success and Failure of Signature REPORT	Statistics showing the counts and percentages of various system events based whether they successfully or unsuccessfully executed.
Total Number of Events REPORT	The total number of events throughout the given report.
Unique Signatures REPORT	The amount of overall unique signatures throughout the report.
Unique Users REPORT	The amount of unique user accounts recorded throughout the report.
Users Over Time REPORT	A Linechart representing user logins over the span of an hour.

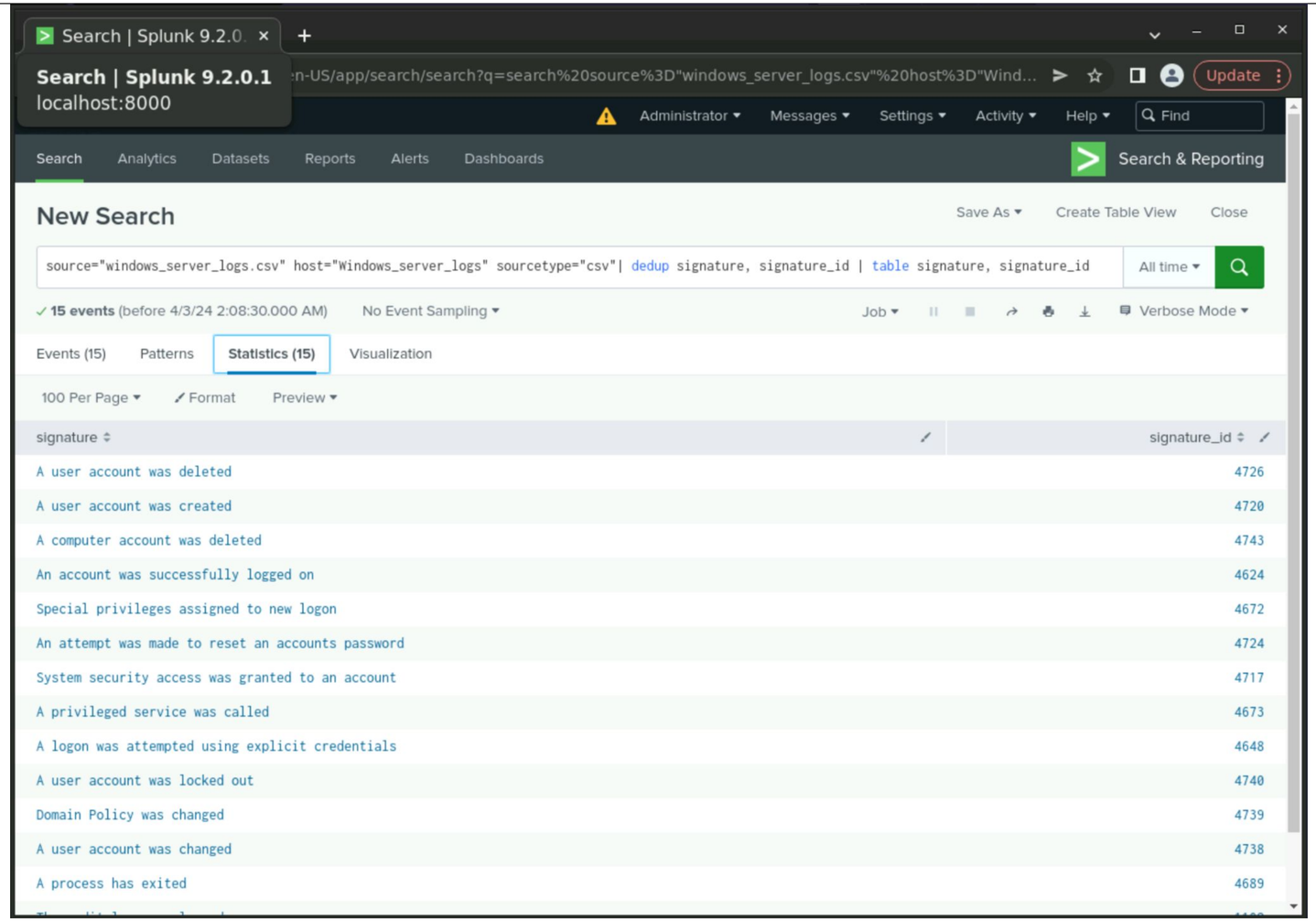
Images of Reports—Windows



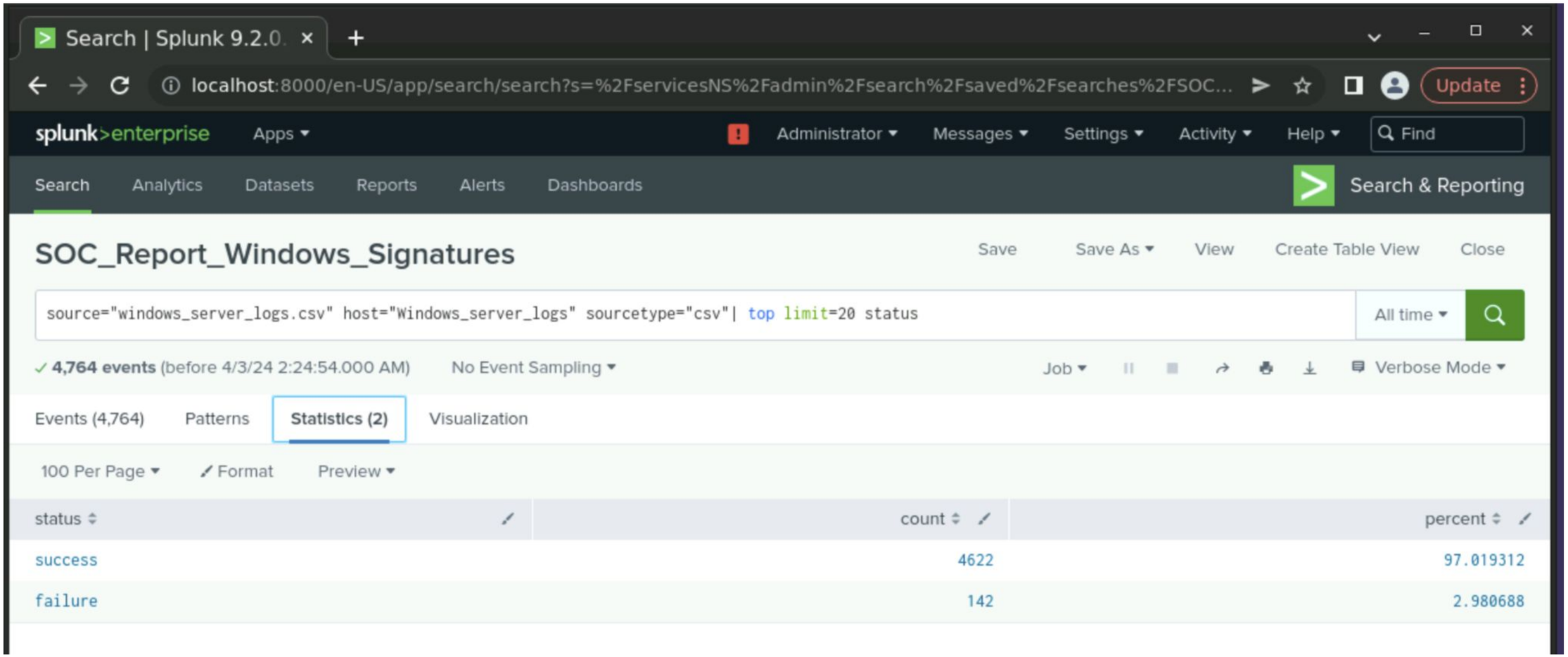
Images of Reports—Windows



Images of Reports—Windows



Images of Reports—Windows

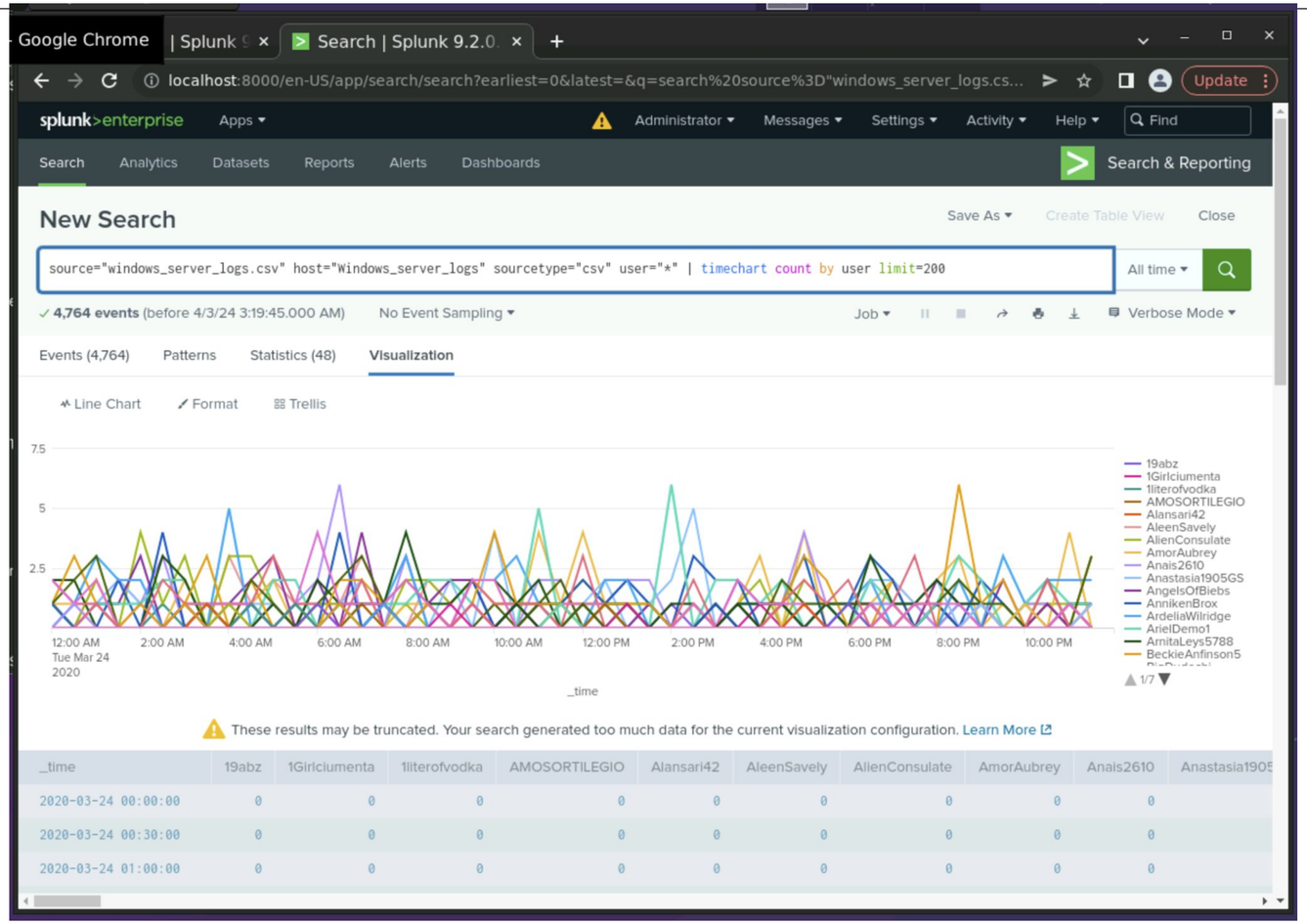


Images of Reports—Windows

Images of Reports—Windows

Images of Reports—Windows

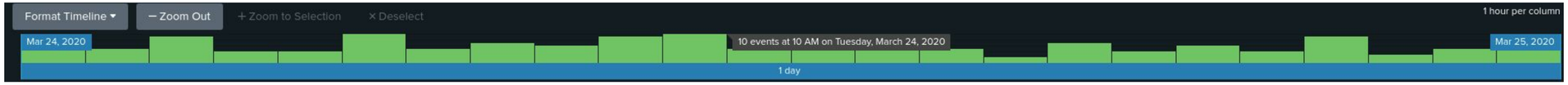
Images of Reports—Windows

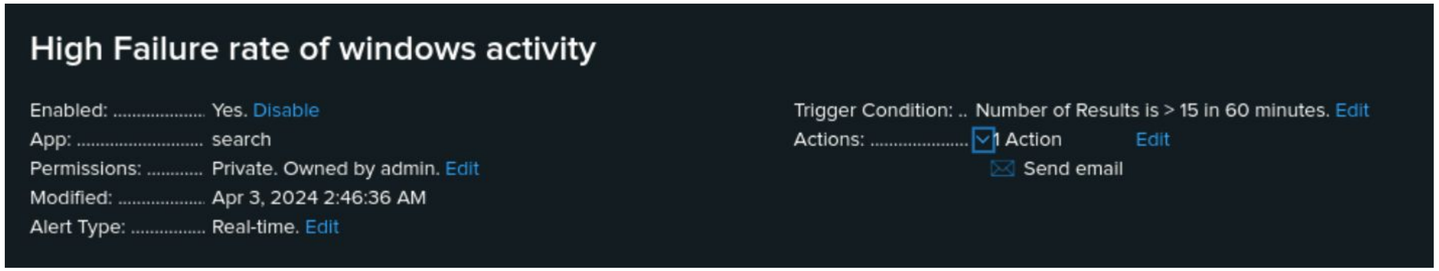


Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Failure Rate of Windows Activity	[Send e-mail to: SOC@VSI-company.com]	[10]	[>15 in 60 minutes]



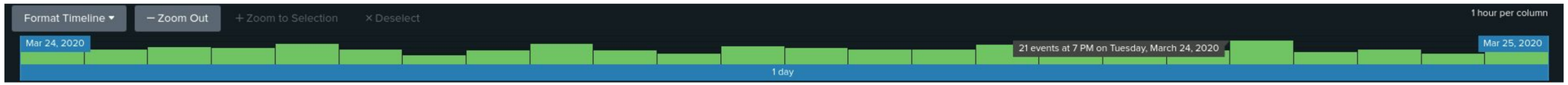


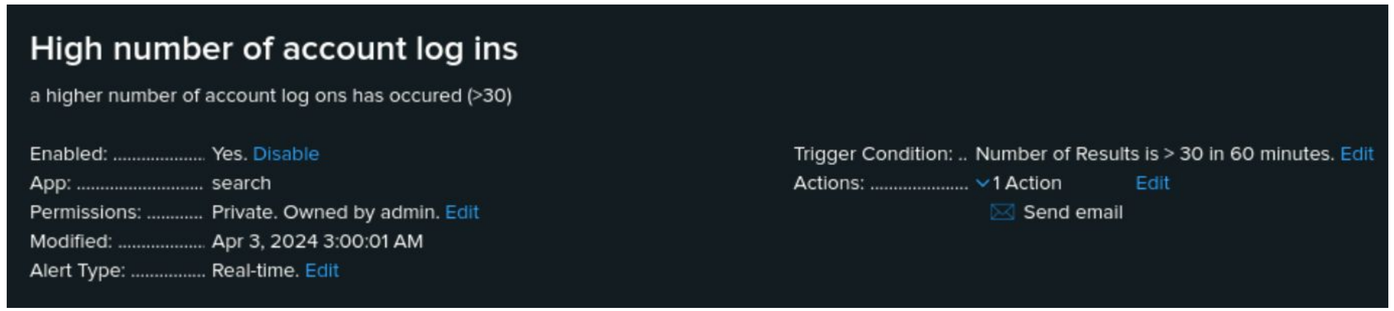
JUSTIFICATION: [Highest number hit was 10 over 24 hours.]

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Number of Account Logins	[Send e-mail to: SOC@VSI-company.com]	[21]	[>30 in 60 minutes]





JUSTIFICATION: [Highest number of log in an hour was 21 over 24 hours.]

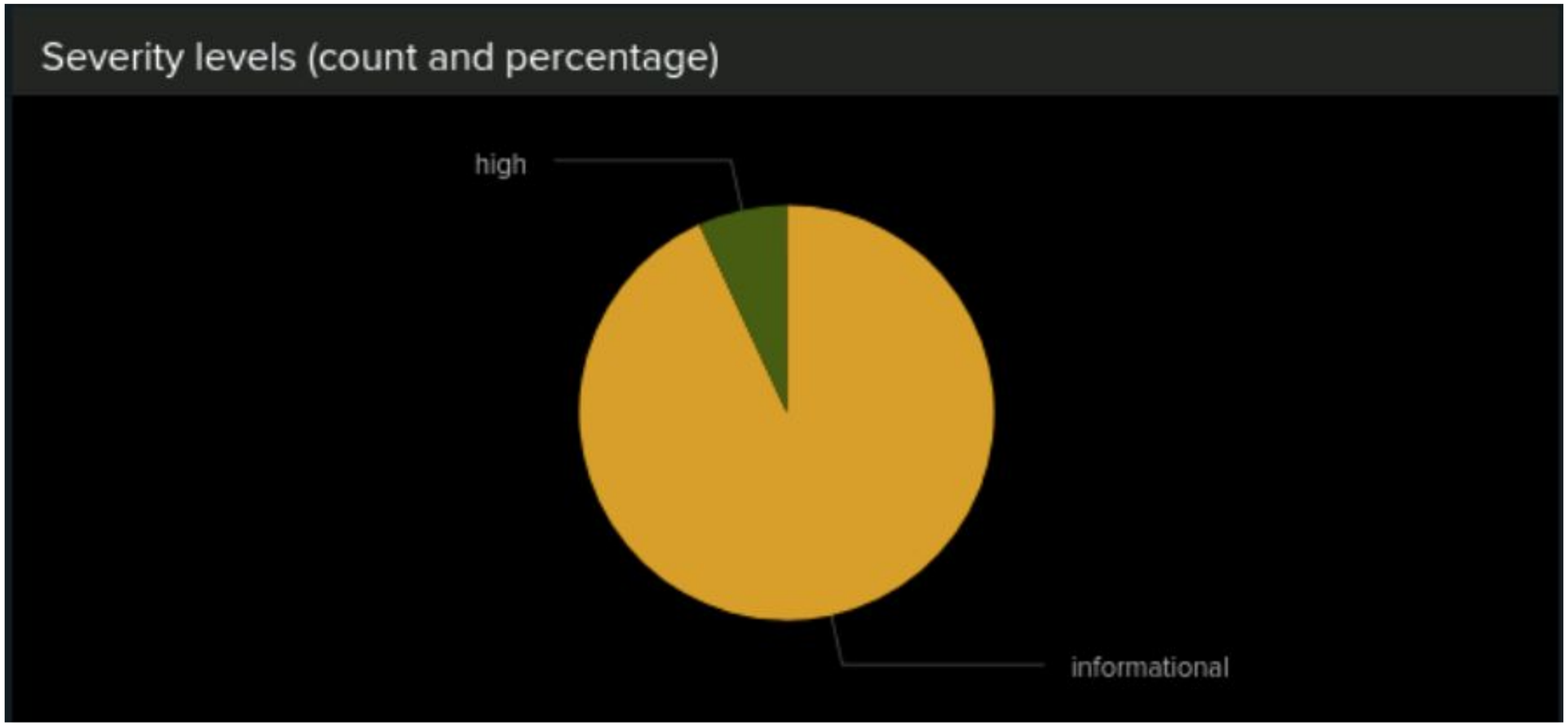
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Amount of User Accounts Deleted	[Send e-mail to: SOC@VSI-company.com]	[22]	[>30 in 60 minutes]

JUSTIFICATION: [Highest number of deleted users signatures did not surpass 22/hour in 24 hours.]

Dashboards—Windows



Security Levels (Count & Percentage) DASHBOARD

Dashboards—Windows

Dashboards—Windows

signature	signature_id	count	percent
Special privileges assigned to new logon	4672	342	7.178841
A computer account was deleted	4743	340	7.136860
A logon was attempted using explicit credentials	4648	337	7.073887
Domain Policy was changed	4739	329	6.905961
An account was successfully logged on	4624	323	6.780017
System security access was removed from an account	4718	321	6.738035
A user account was deleted	4726	318	6.675063
A privileged service was called	4673	317	6.654072
A user account was created	4720	313	6.570109
System security access was granted to an account	4717	309	6.486146

« Prev 1 2 Next »

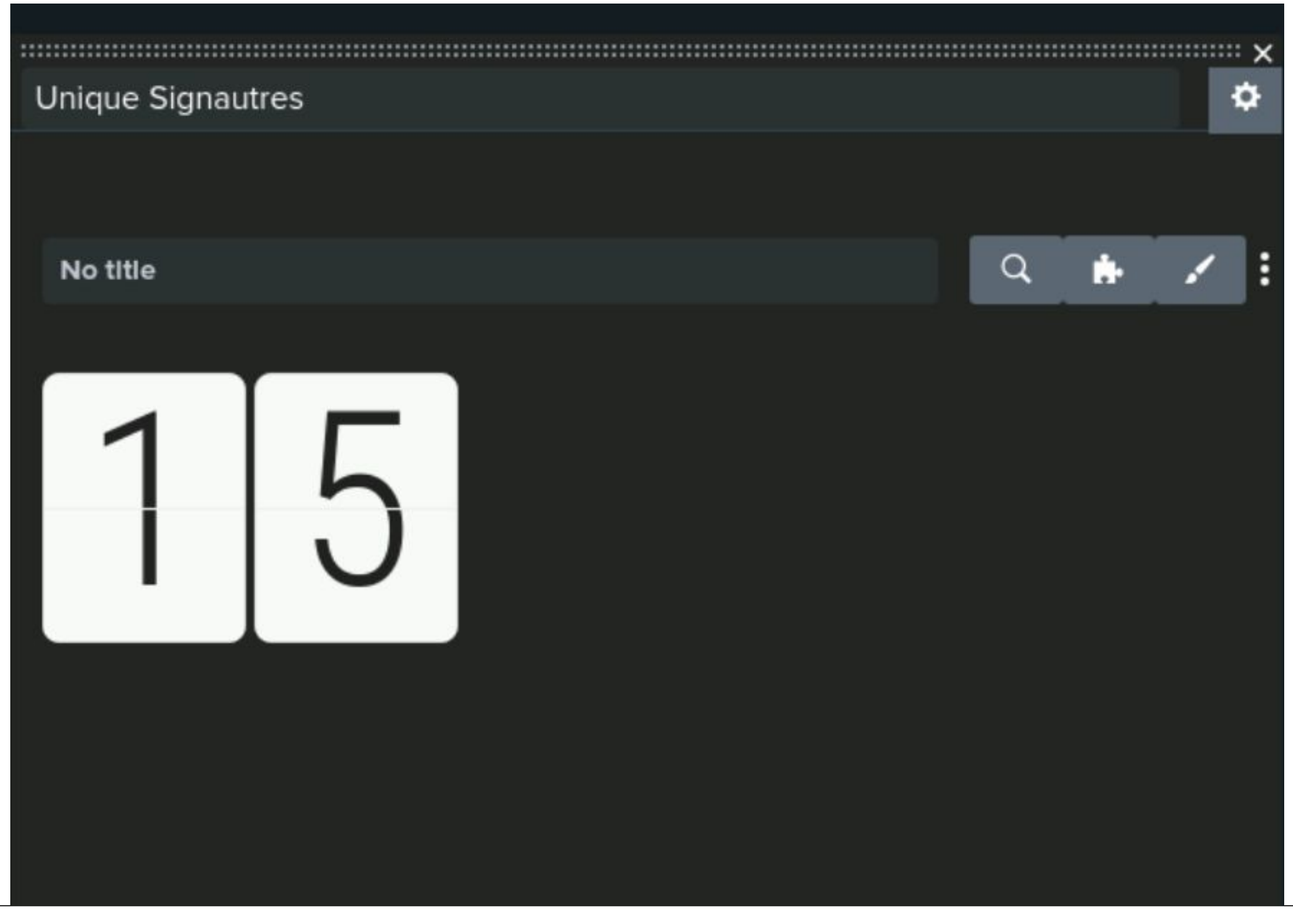
Dashboards—Windows

Success & Failure of Signature DASHBOARD

Dashboards—Windows

Total Number of Events DASHBOARD

Dashboards—Windows



Dashboards—Windows

Dashboards—Windows

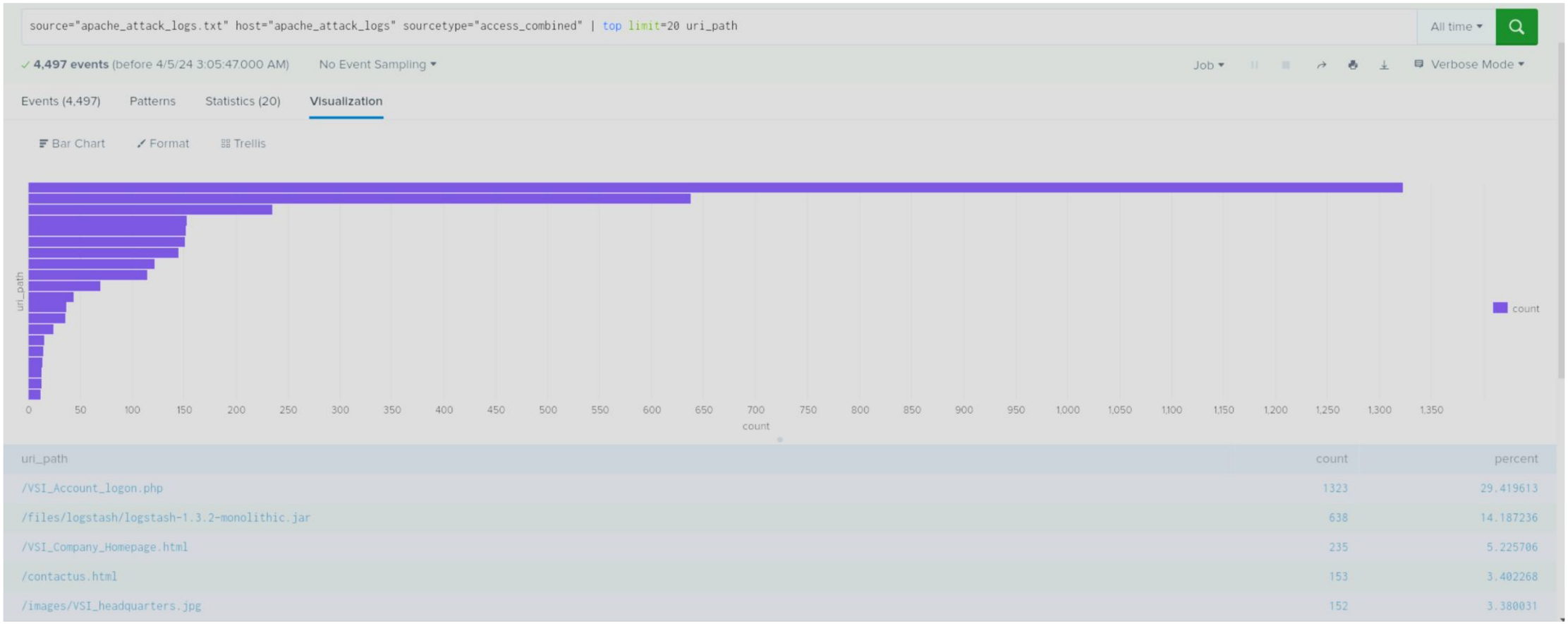

Apache Logs

Reports—Apache

Designed the following reports:

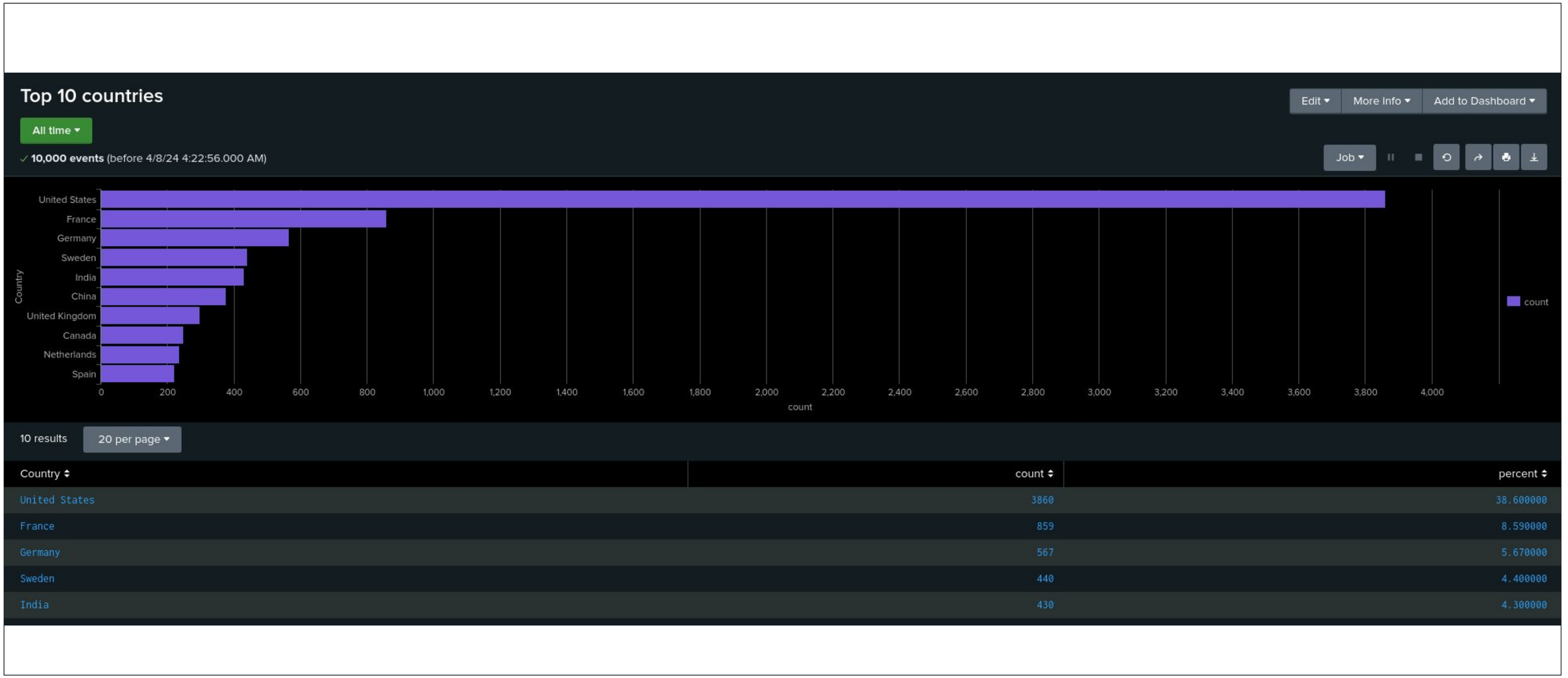
Report Name	Report Description
Unique URI REPORT	Bar Chart showing the count and percentage of each URI visitations.
Top 10 Countries REPORT	Bar Chart showing the top 10 countries with the highest login counts to the server.
IP By Location REPORT	A map visualization which illustrates the geographical sources of the IP logins.
HTTP Methods Over One Hour REPORT	Column Chart showing the most commonly used HTTP Methods over the span of an hour.
HTTP Response Code REPORT	BarChart illustrating the most common response code response for various HTTP methods.
HTTP Methods Pie Chart REPORT	A Pie chart illustrating the most common HTTP Methods.
Top Ten Referrer By Domain REPORT	Barchart that shows the 10 referrer domains.
Unique Referrers REPORT	Departures Board Visualization of the unique Referrers.

Images of Reports—Apache

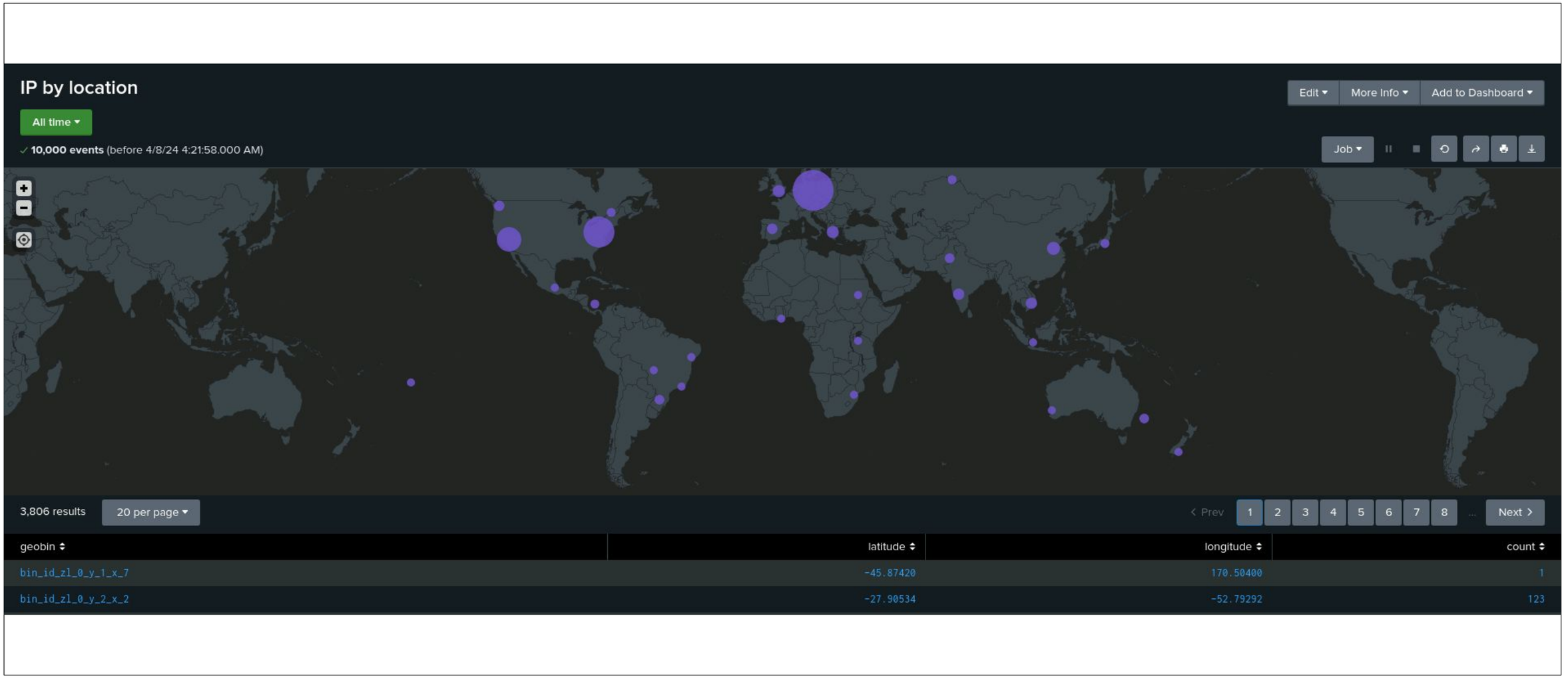


Unique URI REPORT

Images of Reports—Apache

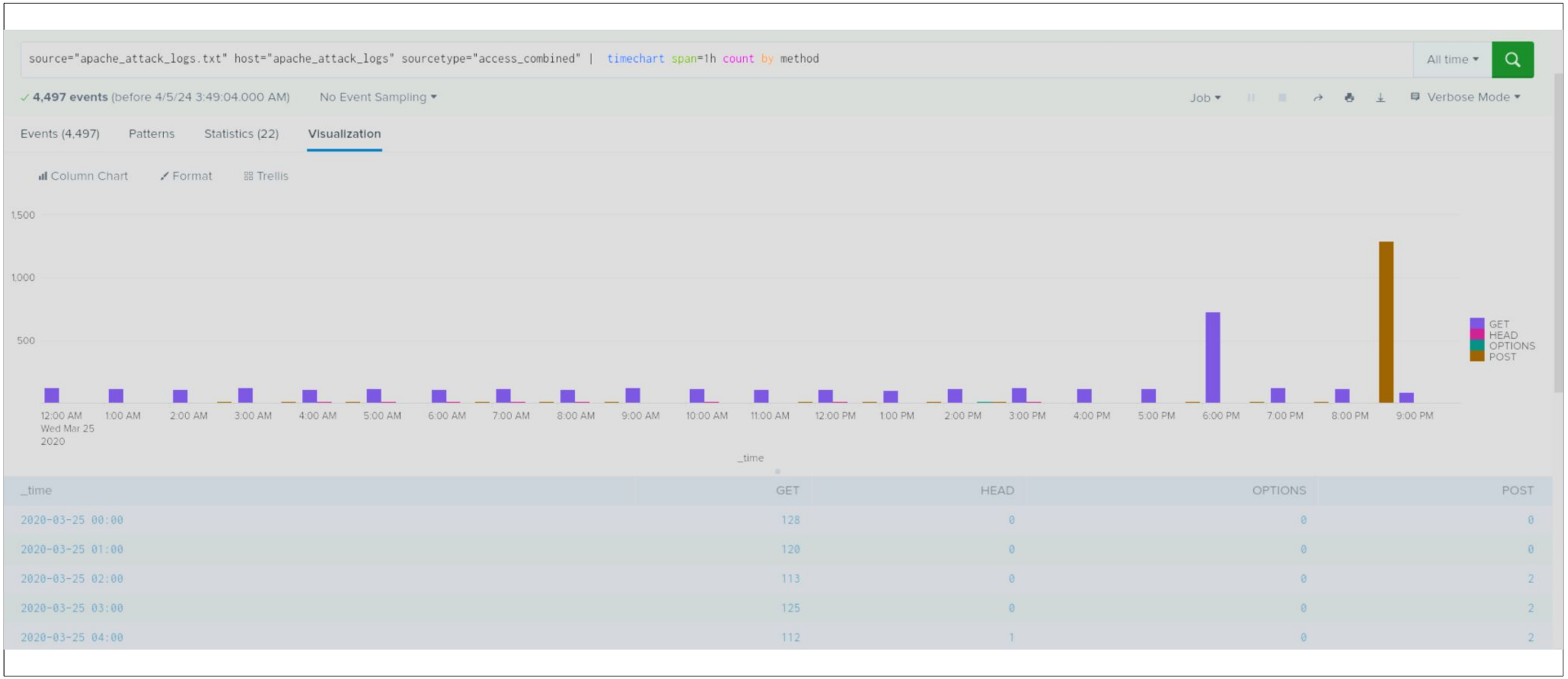


Images of Reports—Apache



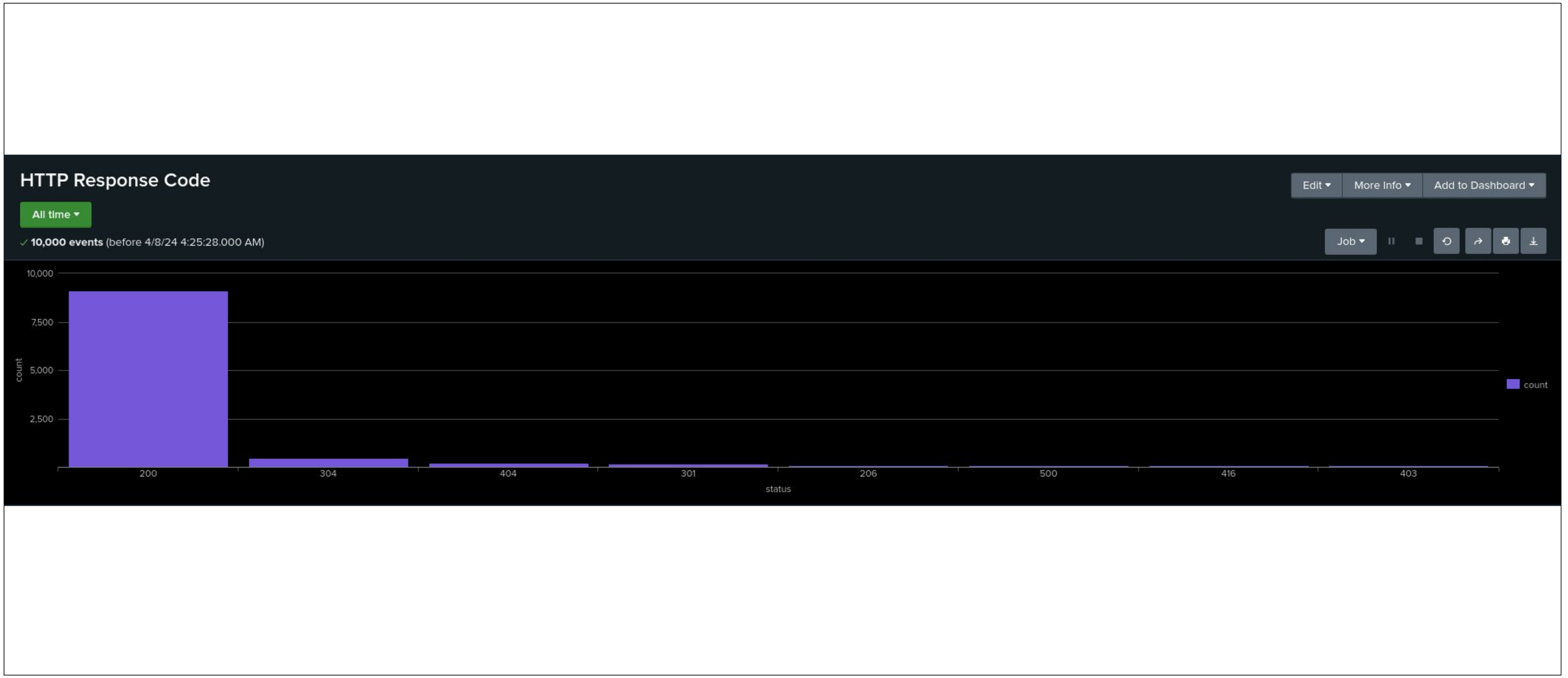
geobin	latitude	longitude	count
bin_id_zl_0_y_1_x_7	-45.87420	170.50400	1
bin_id_zl_0_y_2_x_2	-27.90534	-52.79292	123

Images of Reports—Apache

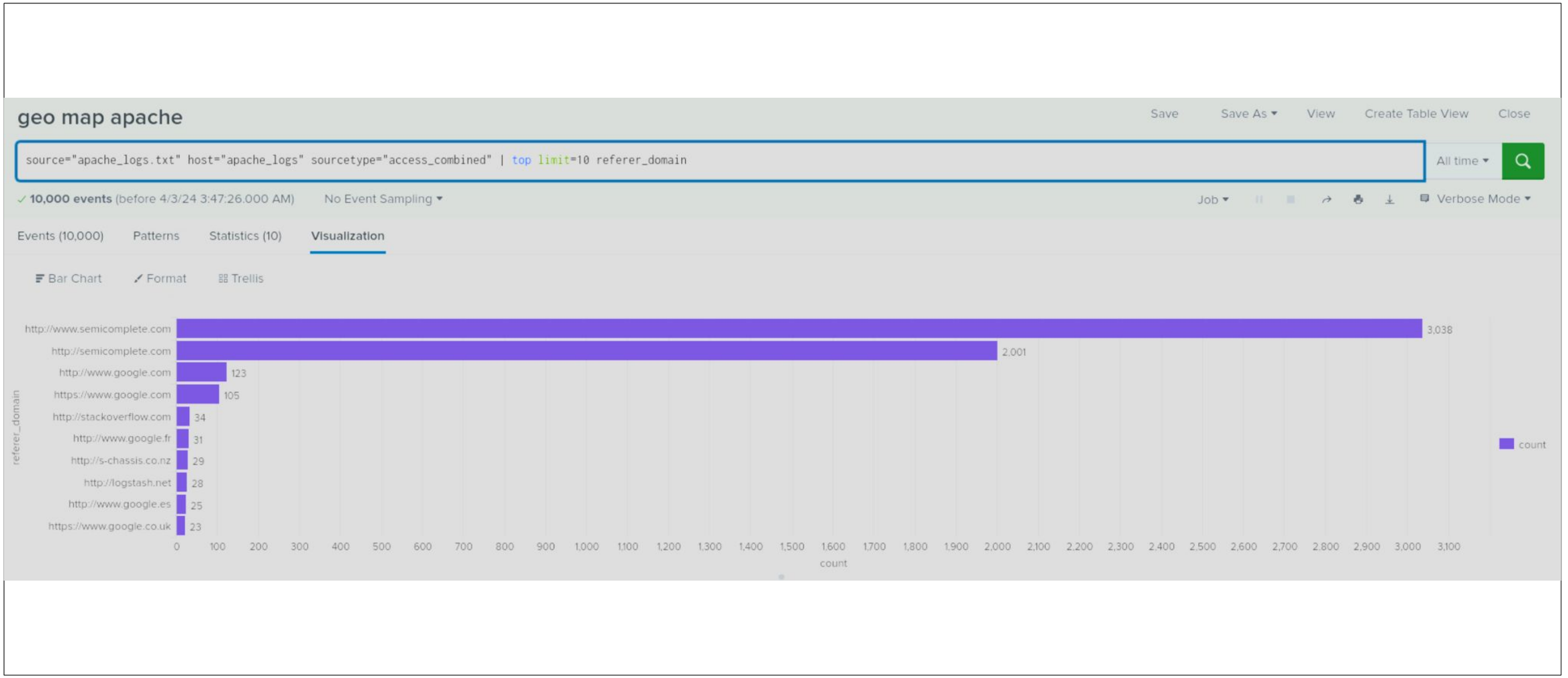


_time	GET	HEAD	OPTIONS	POST
2020-03-25 00:00	128	0	0	0
2020-03-25 01:00	120	0	0	0
2020-03-25 02:00	113	0	0	2
2020-03-25 03:00	125	0	0	2
2020-03-25 04:00	112	1	0	2

Images of Reports—Apache



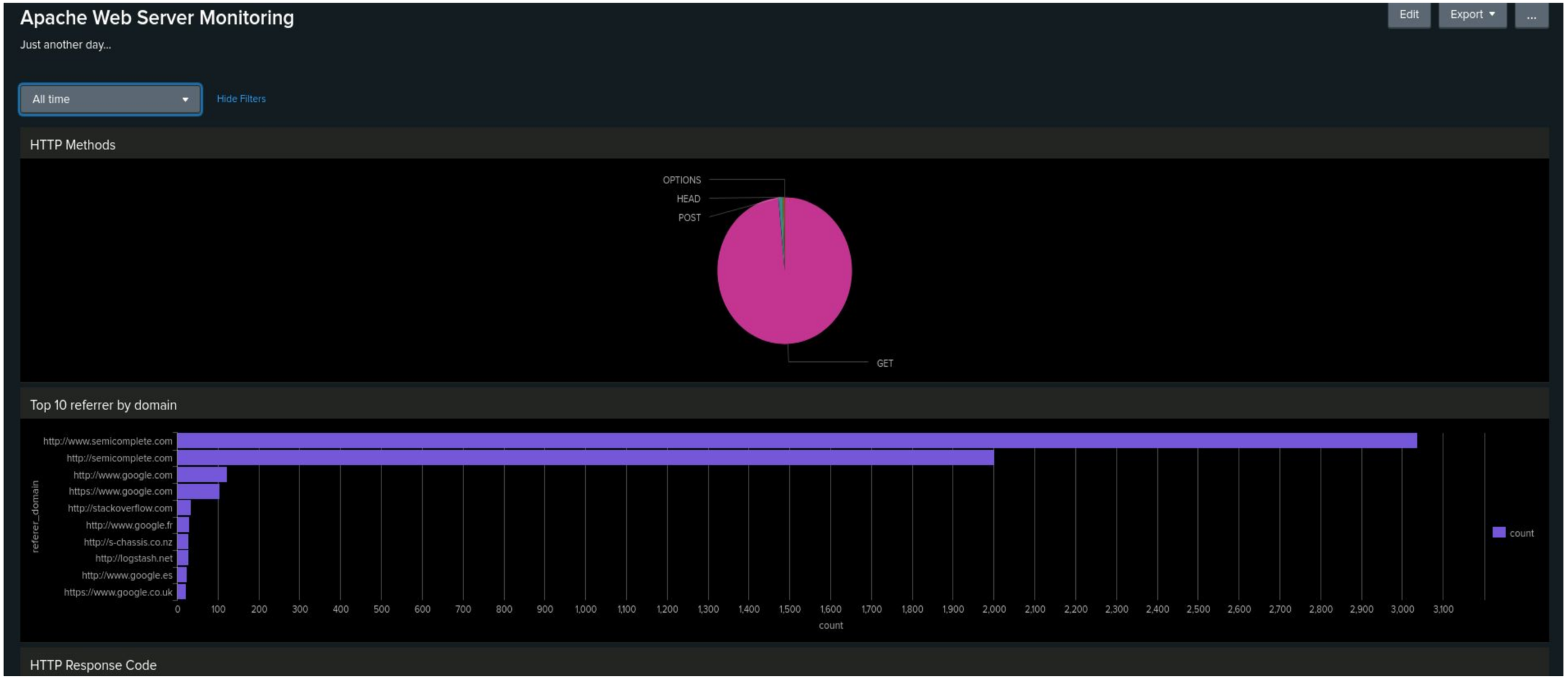
Images of Reports—Apache



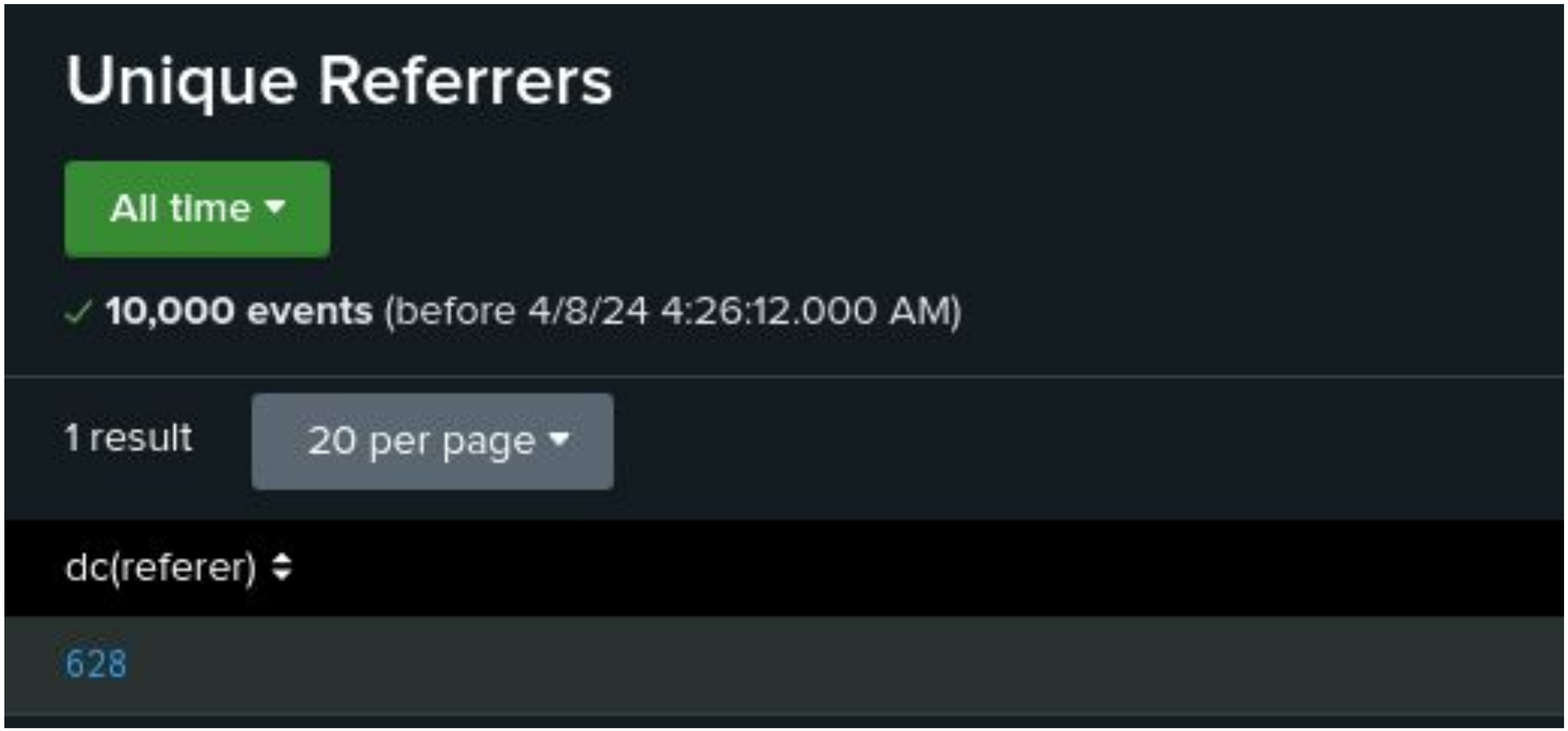
Top Ten Referrer By Domain REPORT

Images of Reports—Apache

Dashboards—Apache



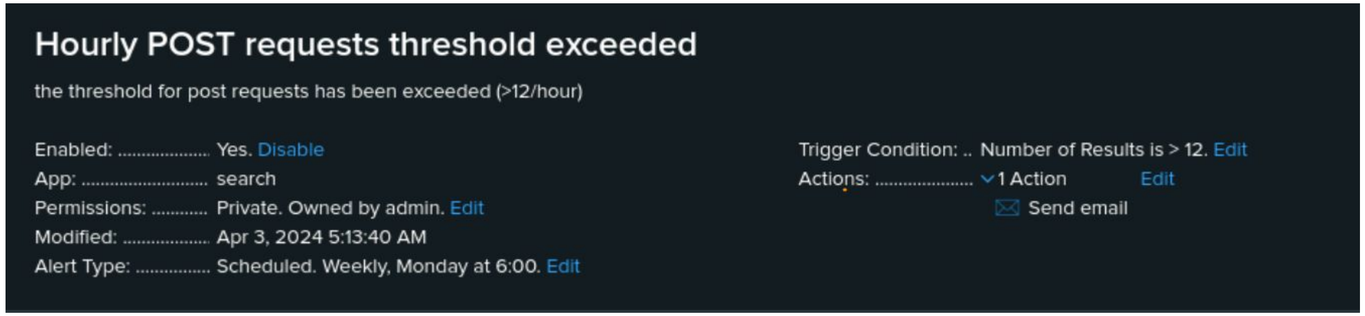
Images of Reports—Apache



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[Hourly POST Requests]	[Send e-mail to: SOC@VSI-company.com]	[~7]	[>12]



JUSTIFICATION: [Highest number of POST requests was 7/hour over 24 hours.]

Alerts—Apache

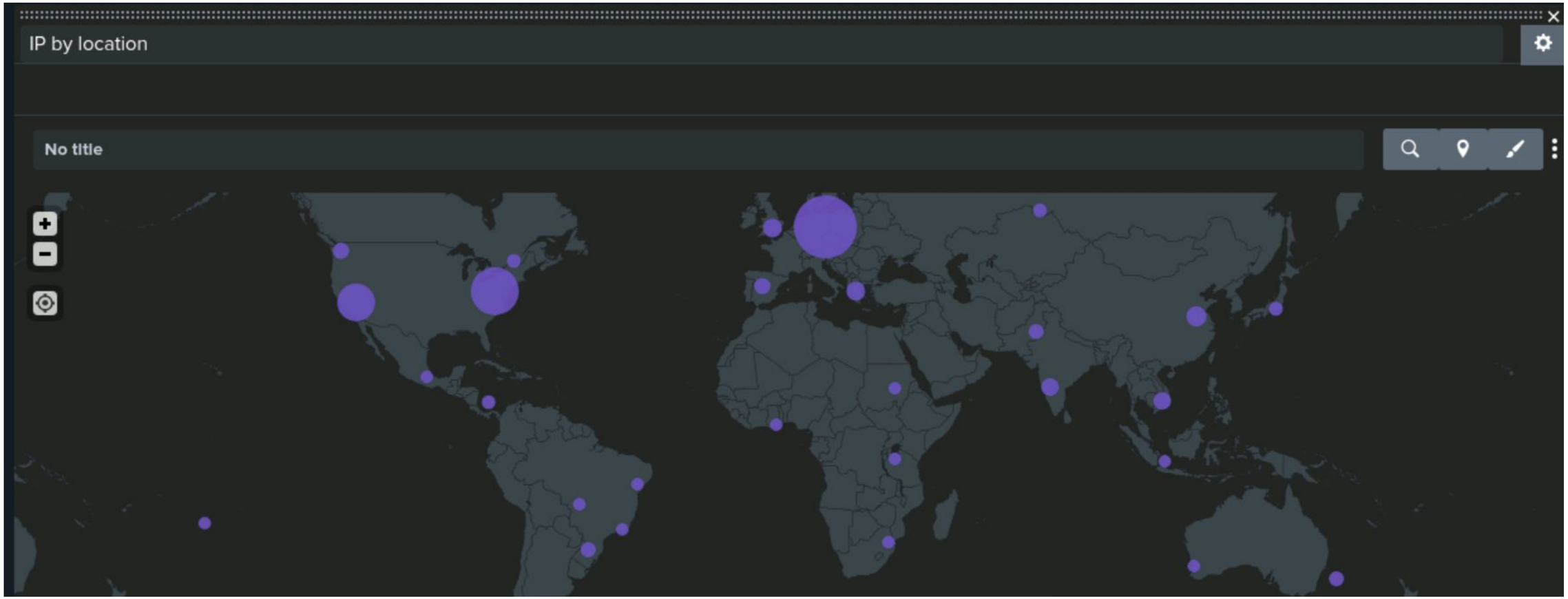
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[Hourly Traffic From Outside US]	[Send e-mail to: SOC@VSI-company.com]	[120]	[>200 in 60 min.]

JUSTIFICATION: [Traffic from outside the US peaked at 120/hour over 24 hours.]

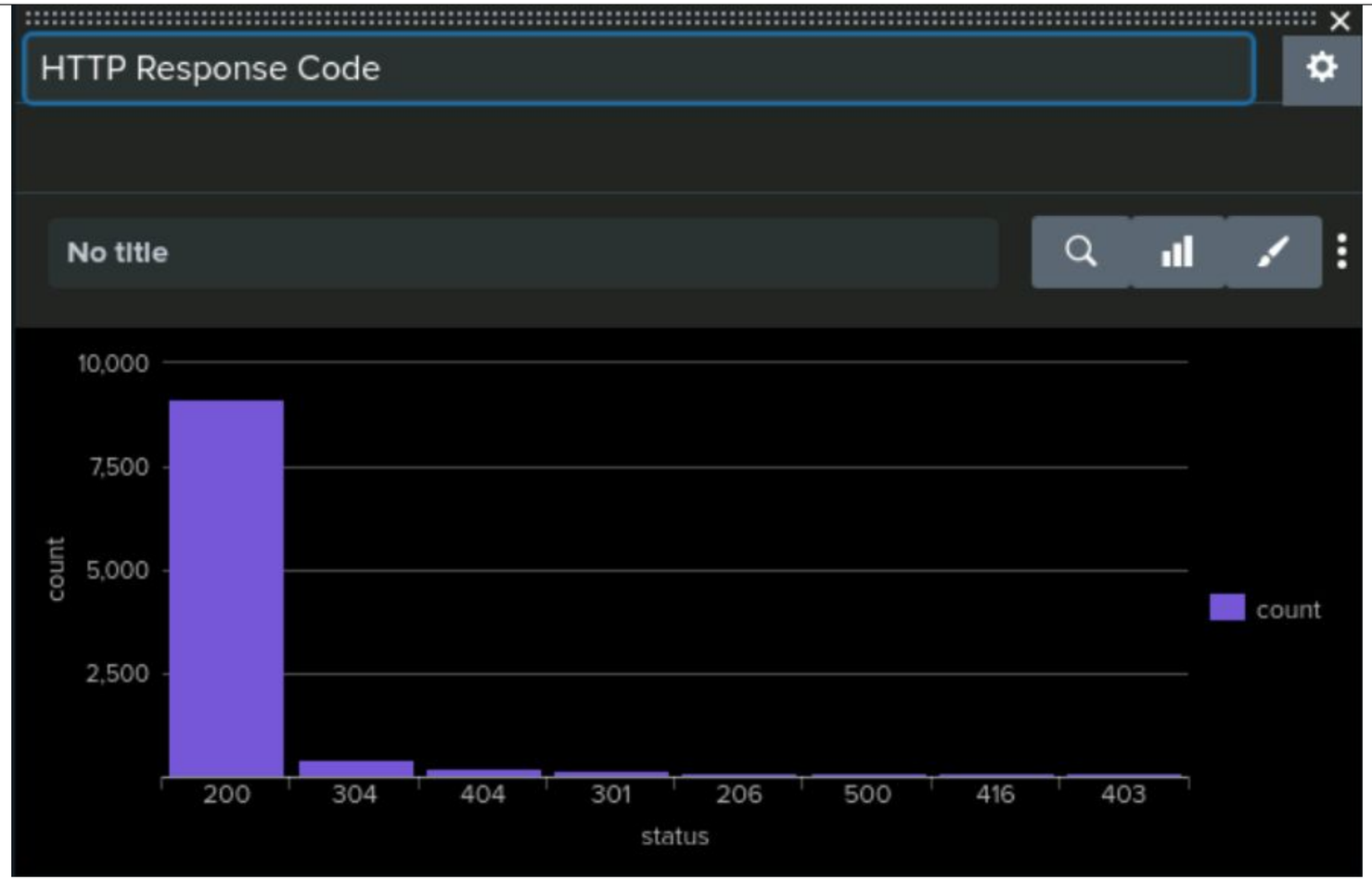
Dashboards—Apache

Dashboards—Apache



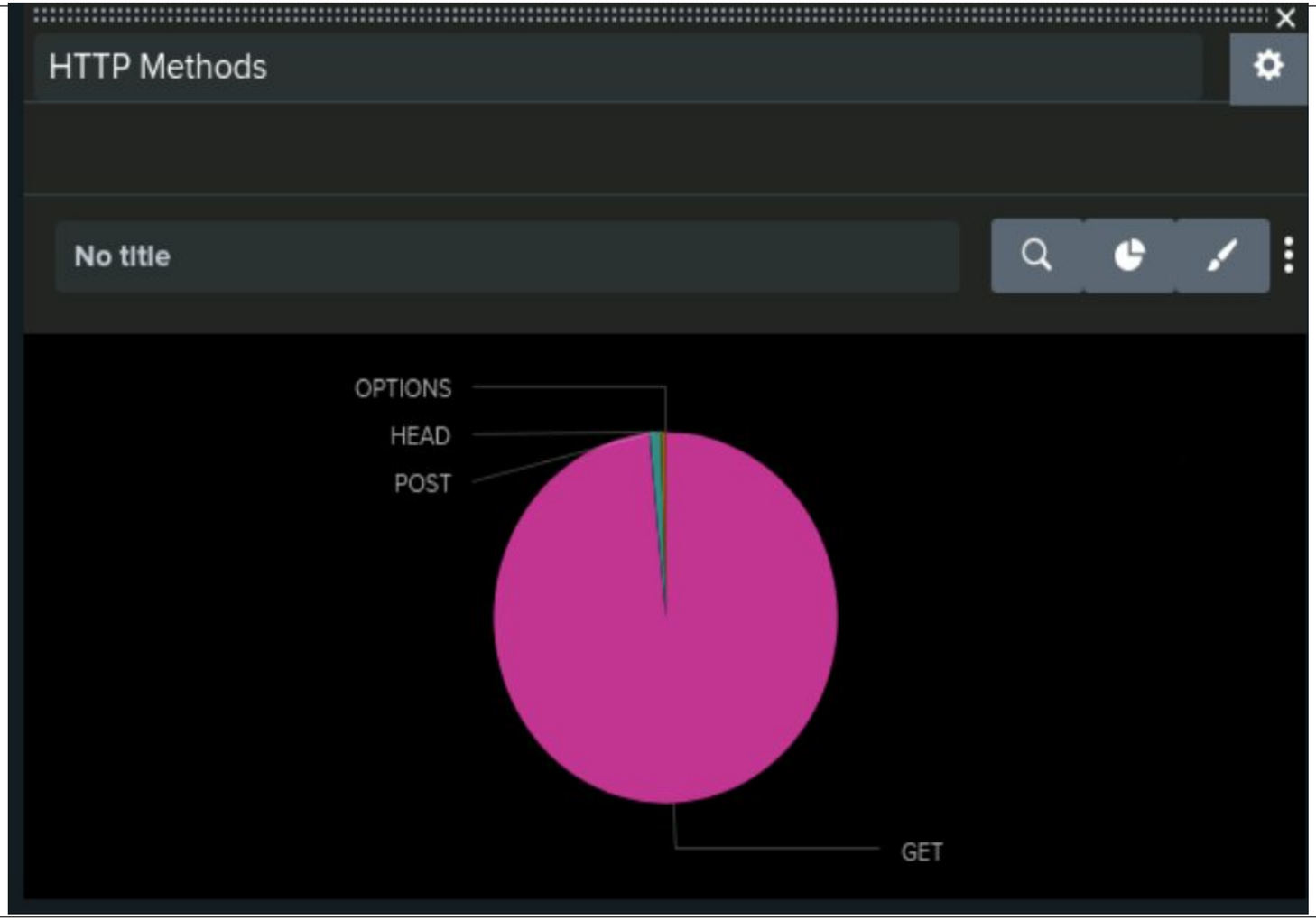
Dashboards—Apache

Dashboards—Apache



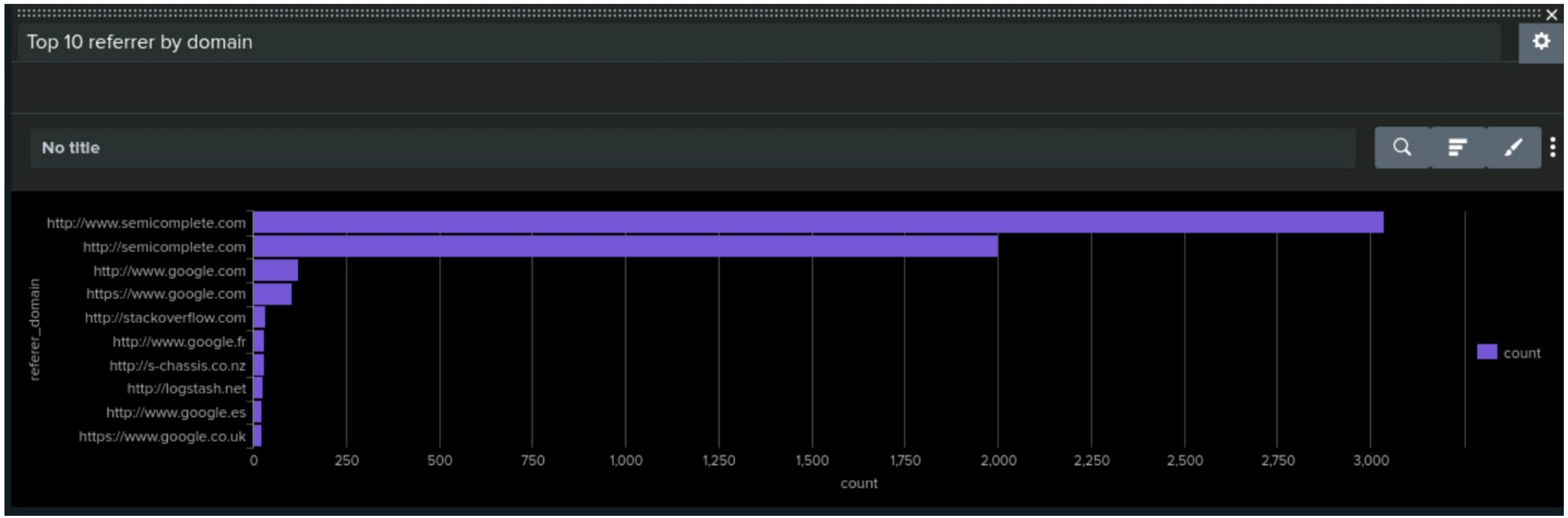
HTTP Response Code DASHBOARD

Dashboards—Apache



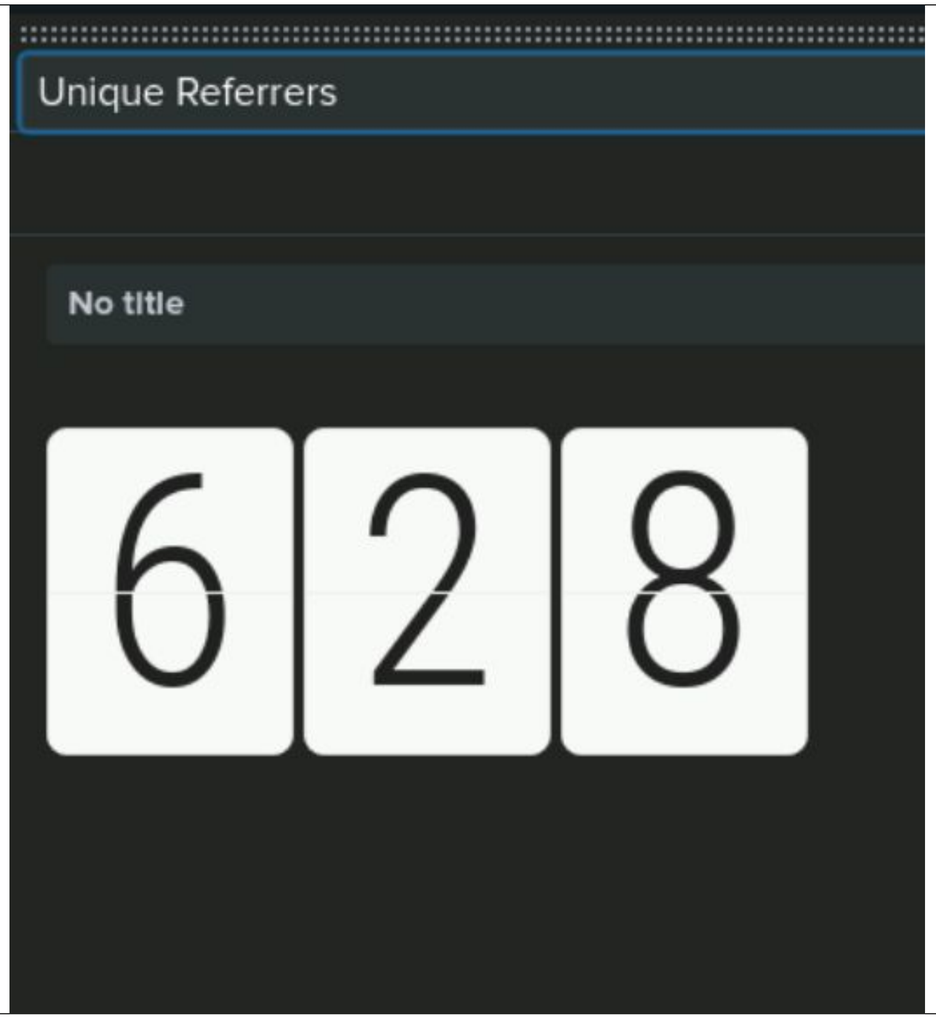
HTTP Methods Pie Chart DASHBOARD

Dashboards—Apache



Top Ten Referrer By Domain DASHBOARD

Dashboards—Apache



Unique Referrers DASHBOARD


Attack Analysis

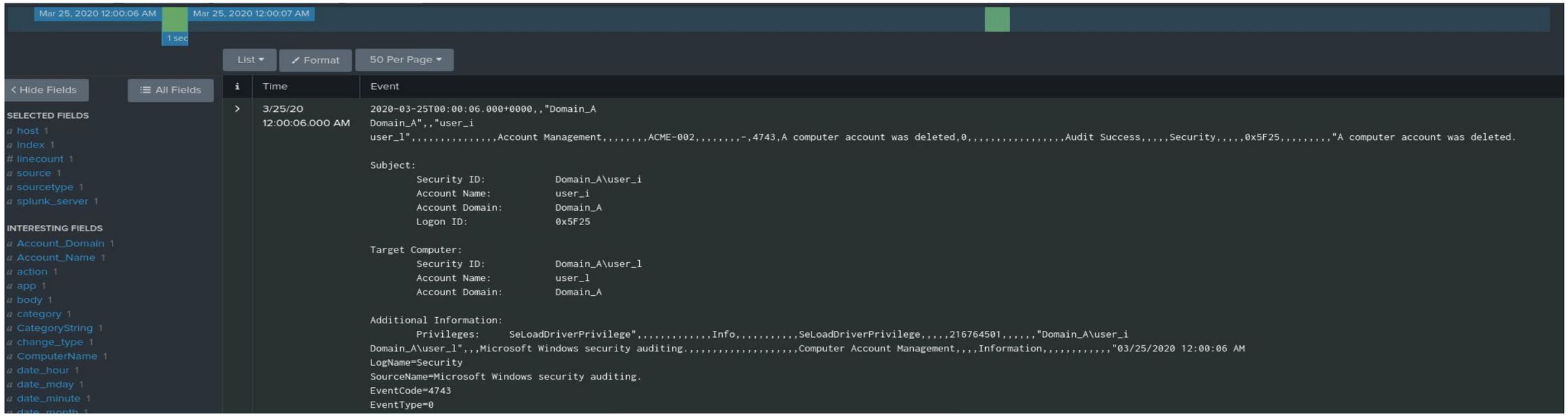
Attack Summary—Windows

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

- At 12:00:06 AM splunk reported computer account “user_l” deleting computer account “user_i”.
- By 2:00:00 AM these “alphabet users” would continue to self propagate and follow a series of repetitious actions involving resetting account passwords, changing domain password policy (changed to be between 6-8 characters), changing user accounts, clearing audit logs before deleting itself.
- These users were seemingly executed by a piece of malware “example_*.exe” following this same alphabet naming convention.
- The final event took place at 1:45:27 PM when the attack stopped.

Screenshots of Attack Logs

Initial anomalous event:



Attack Summary—Windows

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

- [OH YEAH]

Attack Summary—Windows

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

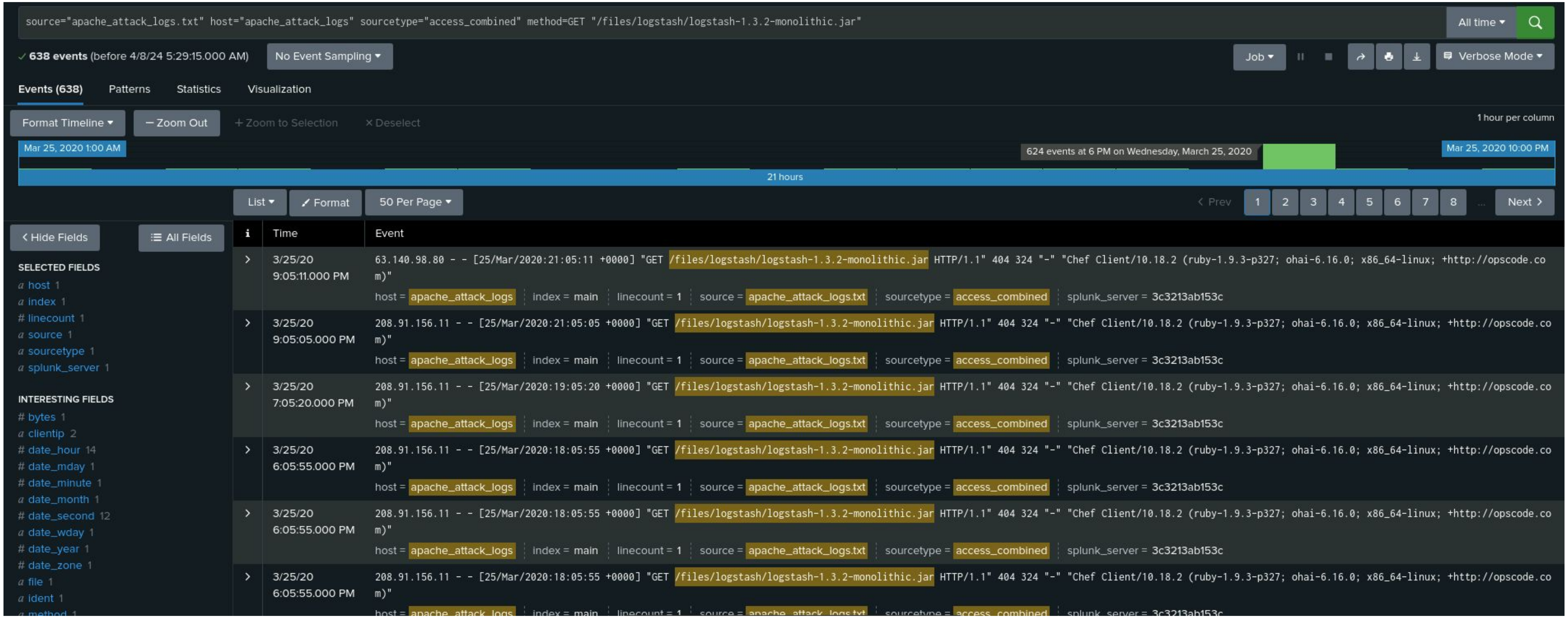
- [Dashboards were very helpful when trying to correlate data to understand the timing and methods of attack.]

Attack Summary—Apache

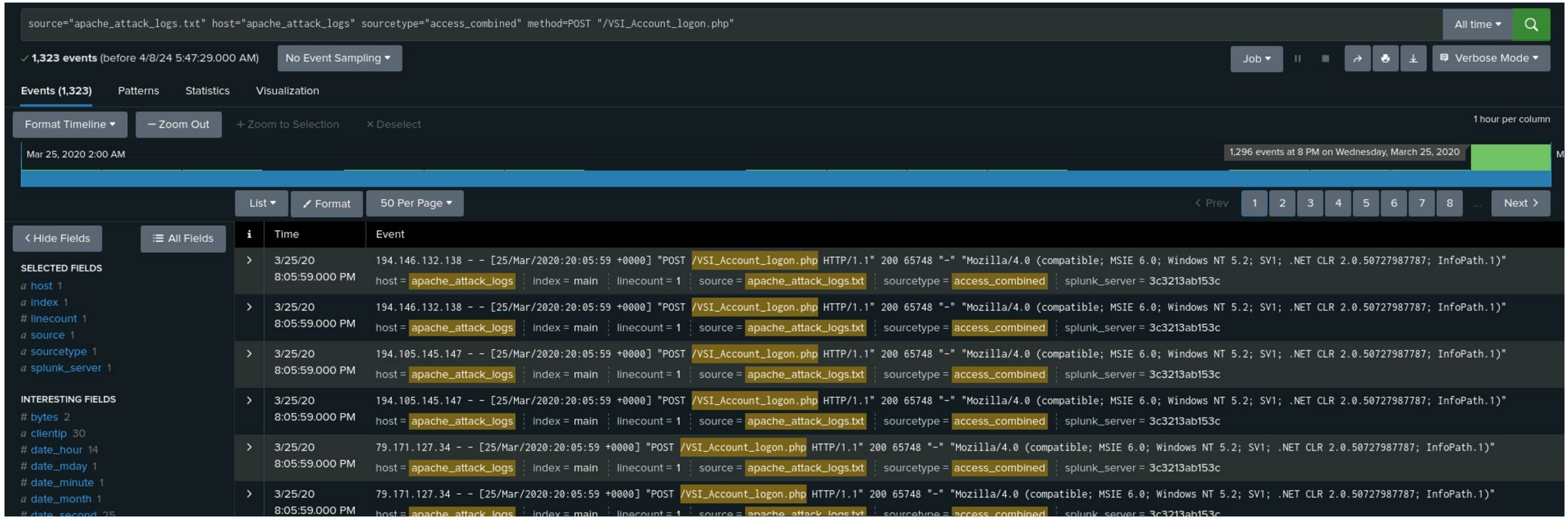
Summarize your findings from your reports when analyzing the attack logs.

- at 6PM a suspicous amount of GET requests for /files/logstash/logstash-1.3.2-monolithic.jar from a Chef Client executing a ruby script via ohai based from of opscode.com
- at 8PM a suspicious amount of POST requests hit /VSI_Account_logon.php, indicative of a brute force log on attack.

Screenshots of Attack Logs



Screenshots of Attack Logs



Attack Summary—Apache

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

- [OH YEAH]

Attack Summary—Apache

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

- The dashboards were very helpful in identifying not only the times and potential types of attacks taking place, but the geolocate function of splunk allowed us to see where the attacks were coming from.

Summary and Future Mitigations

Project 3 Summary

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

On Wednesday March 25th 2020, from 12am to 9pm an attack originating from Ukraine hit first VSI's Windows server, and later that same day VSI's Apache web servers. The attackers leveraged malware and botnets to manipulate logs and change domain policy for passwords, reset passwords, create new accounts, delete accounts and assign special privileges to new users. The attacks then pivoted to the the Apache web server where a very large number of GET requests pulling logs from the web server, followed by a large number of POST requests allowing the login page to be easily brute forced due to the policy password changes (6-8 characters) and resets. Due to the logs being pulled from the Apache server and the log in being brute forced, these systems should be considered compromised. Similarly, due to log erasure and an unknown executable being present on the windows server, these machines should also be considered compromised.

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

- The attack seemingly started from a piece of malware that was present on the windows servers, all staff should be trained against phishing attempts and on site security should be reviewed to discover where the malware originated.
- Firewalls should be in place and updated to stop brute force attempts.
- Firewalls should be in place to screen potentially malicious IPs.
- Lock out on too many password attempts in X amount of time to stop brute force.
- Logs should not be accessible from the web API.

Project 3 (Q&A)

Project 3 Ending