Defensive Security Project
by: Lian Canda, Matt Dunton, Peter Nguyen, & Ben Spidle

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- We played the role of a SOC team at a company called Virtual Space Industries, which build designs for virtual-reality programs.
- Competition soon arises as VSI competitor, JobeCorp, launches attacks to disrupt VSI’s flow and to ruin their reputation.
- We were tasked to use SIEM tools, via Splunk, to build reports, alerts, and dashboards to monitor for attacks on our systems and applications. These includes:
  - An administrative webpage
  - An Apache Server
  - A Windows Server

[“Add-On” App]

IPInfo App for Splunk

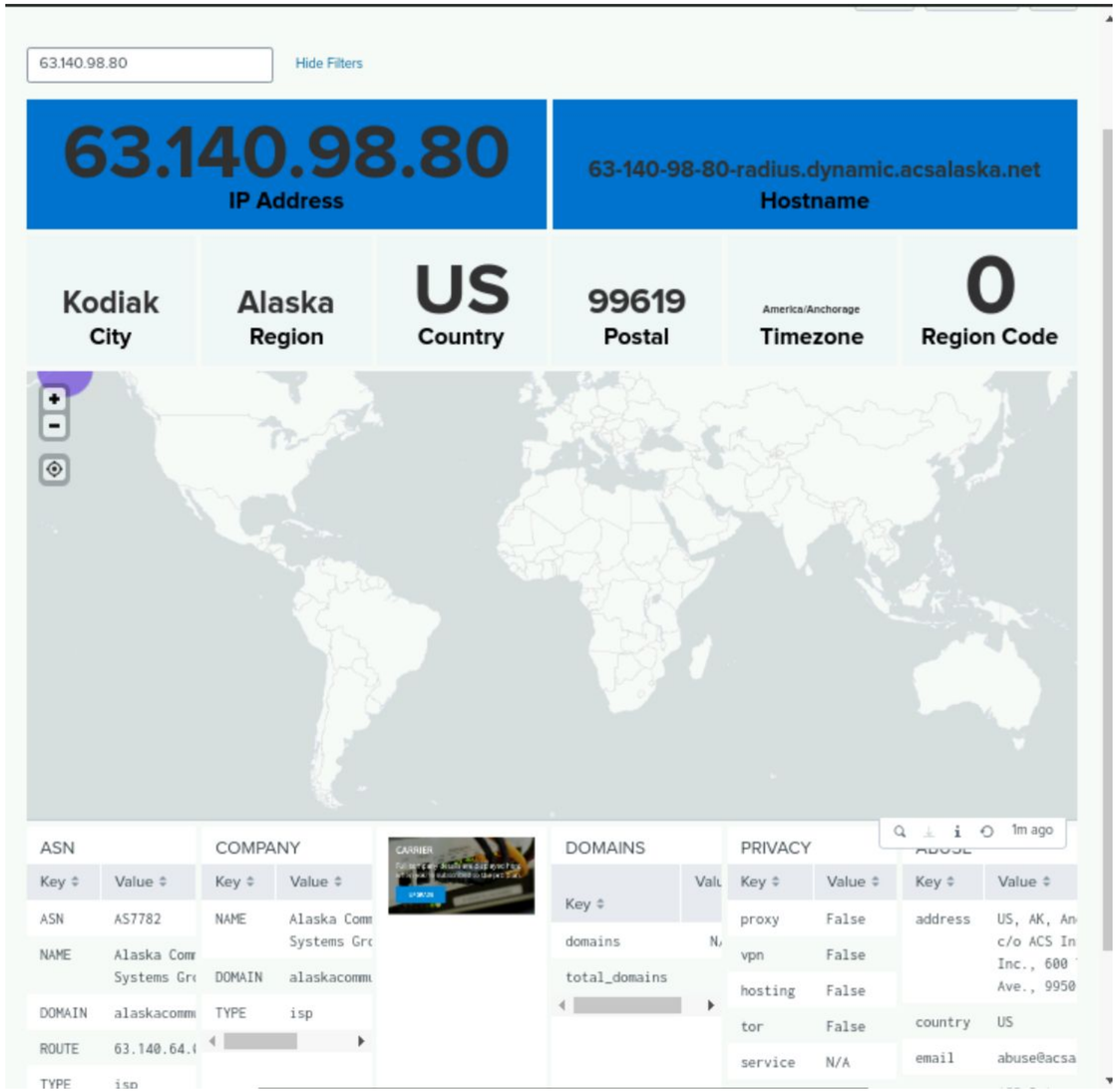
IPinfo offers the most accurate IP address data available anywhere. There's a paid and free option for users to use to find all information related to IPs:

- IP to Geolocation
- IP to Mobile
- IP to Company
- IP Whois
- IP Ranges
- Privacy Detection
- Hosted Domains
- ASN Data
- Abuse Contract

Users have 50,000 free IP to Geolocation API requests per month and a free IP database. IPinfo's users deliver reliable use cases including:

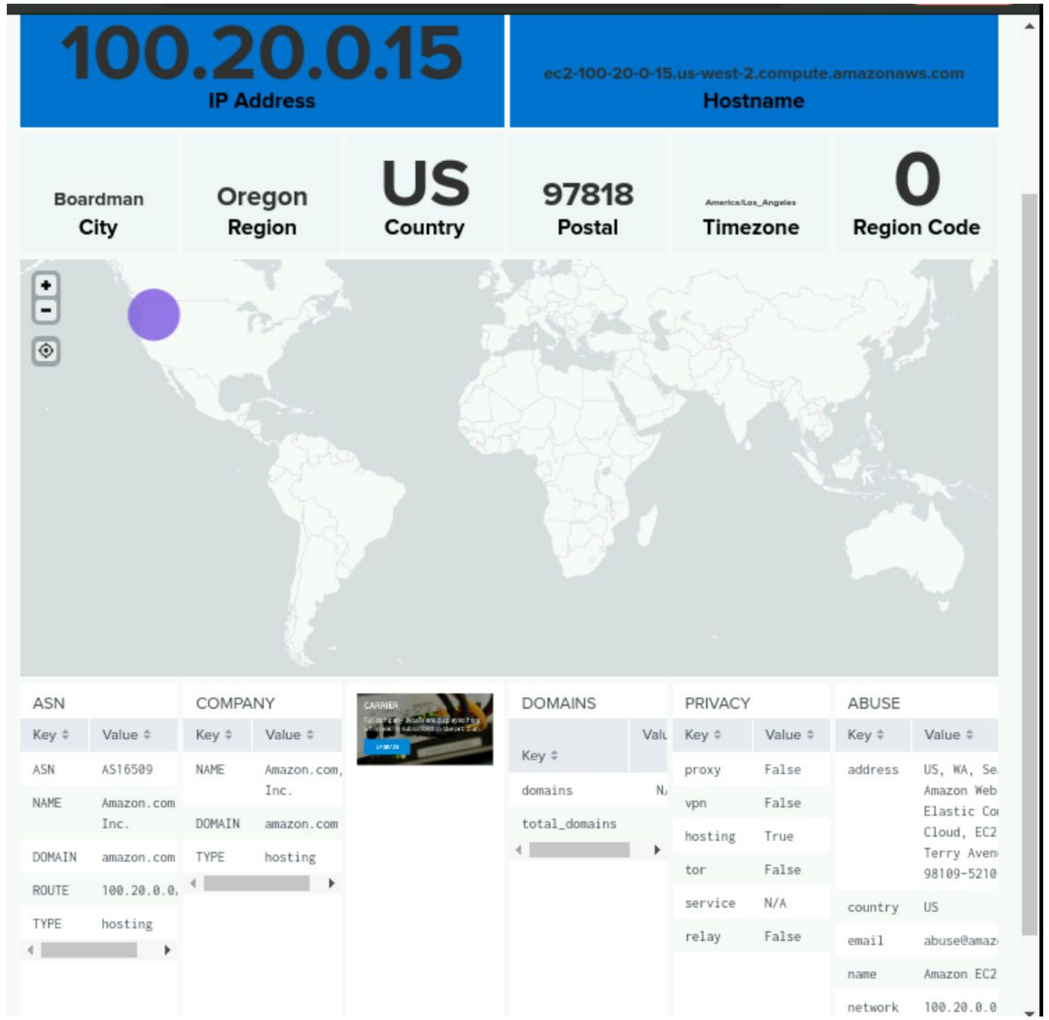
- Threat Detection & Intelligence
- Critical Infrastructure Security
- Utilities
- Security Compliance & Risk Management
- Fraud Prevention
- And many more :)

IPInfo App for Splunk



- By running an IP scan against an IP founded in one of the files, we were able to pinpoint exactly where the requests were made from. The information provided gave us which city, region, country, and zip code.
- With further analysis, additional information gives us what the IP is tied to.
  - Is the IP connected to a company?
  - Is there a domain listed under the IP?
  - Is a VPN or proxy set up with the IP?

IPInfo App for Splunk



Showing results for 100.20.0.15

Copy API link | Copy complete JSON

Geolocation

Copy JSON

```
hostname  "ec2-100-20-0-15.us-west-2.compute.amazonaws.com"
city      "Boardman"
region    "Oregon"
country   "US"
loc       "45.8399,-119.7006"
org       "AS16509 Amazon.com, Inc."
postal    "97818"
timezone  "America/Los_Angeles"
```

ASN

Copy JSON

```
asn     "AS16509"
name    "Amazon.com, Inc."
domain  "amazon.com"
route   "100.20.0.0/14"
type    "hosting"
```

Company

Copy JSON

```
name    "Amazon.com, Inc."
domain  "amazon.com"
type    "hosting"
```

Privacy

Copy JSON

```
vpn    false
proxy  false
```

Logs Analyzed

1 Windows Logs

- The Windows Server contains back-end operation trade secrets.

2 Apache Logs

- The Apache Server contains logs for Virtual Space Industries website.

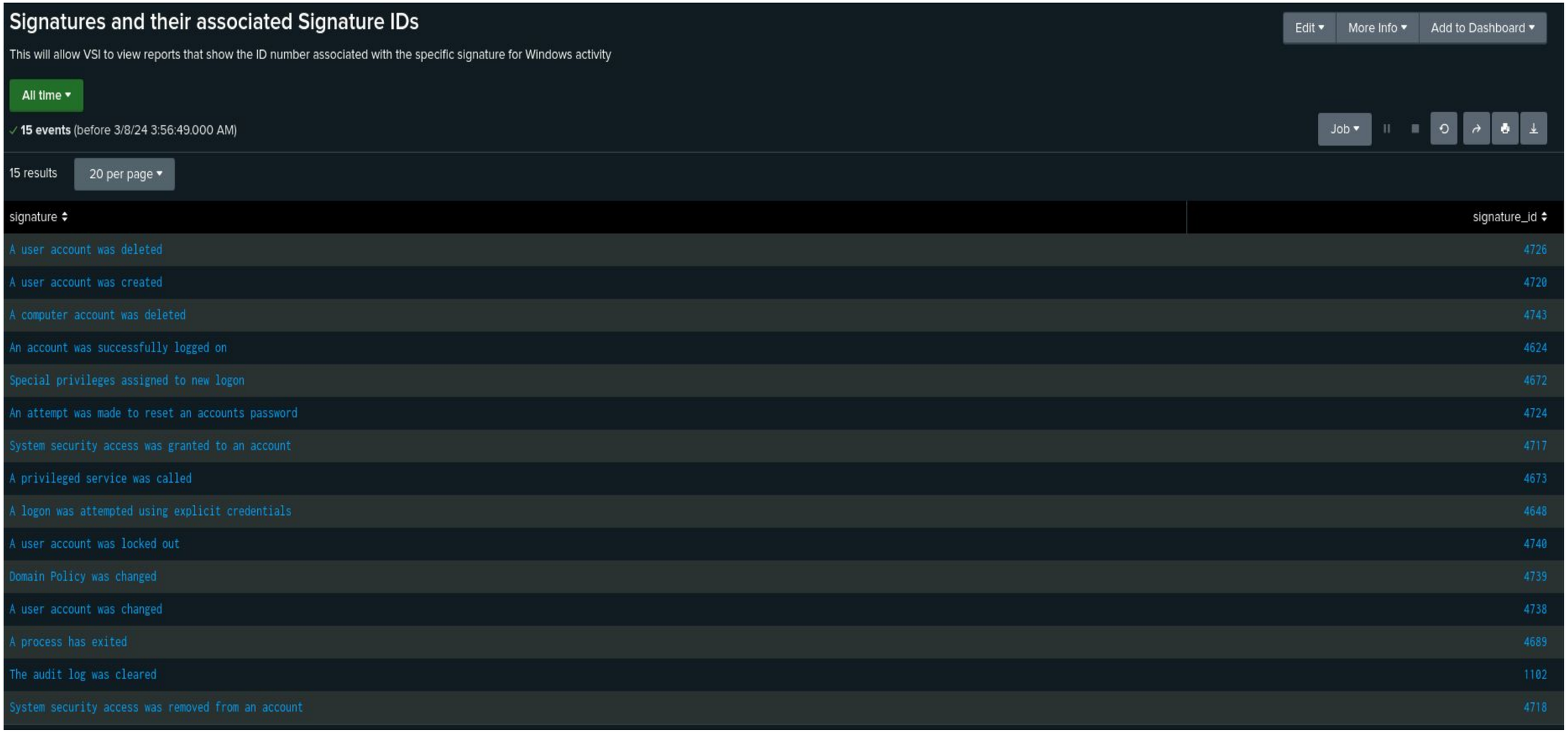
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signatures and their associated Signature IDs	This allows VSI to view reports that show the ID number associated with the specific signature for Windows activity
Count and Percentage of Severity Levels	This allows VSI to understand the severity levels of the Windows logs being viewed
Comparison of “Success” and “Failure” Status	This shows VSI if there is a suspicious level of failed activities on their Windows server

Images of Reports—Windows Report 1



Signatures and their associated Signature IDs

Edit ▾ | More Info ▾ | Add to Dashboard ▾

This will allow VSI to view reports that show the ID number associated with the specific signature for Windows activity

All time ▾

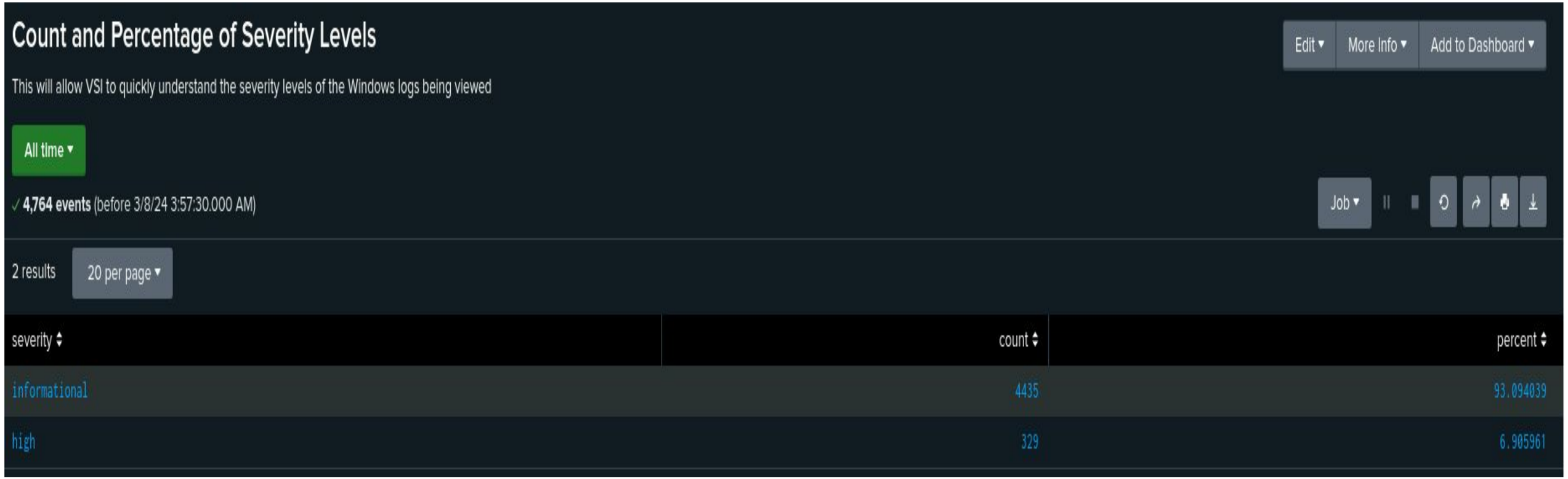
✓ **15 events** (before 3/8/24 3:56:49.000 AM)

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
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

Images of Reports—Windows Report 2



Images of Reports— Windows Report 3

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Login Attempts Reached	The threshold for the hourly level of failed Windows Activity has been reached	7	15

JUSTIFICATION:
The estimated average to determine the baseline for the “normal” amount of failed login attempts was 7 per hour.
The threshold should be 15 failed login attempts because the highest “normal” amount of failed login attempts was 10 during some hours.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Accounts Successfully Logged On	The threshold of successfully logged on accounts has been reached.	15	35

JUSTIFICATION:
The estimated average to determine the baseline for the normal amount of successful login was 15 per hour.
The threshold should be 35 successful login because the highest “normal” amount of successful logins was 21 during some hours

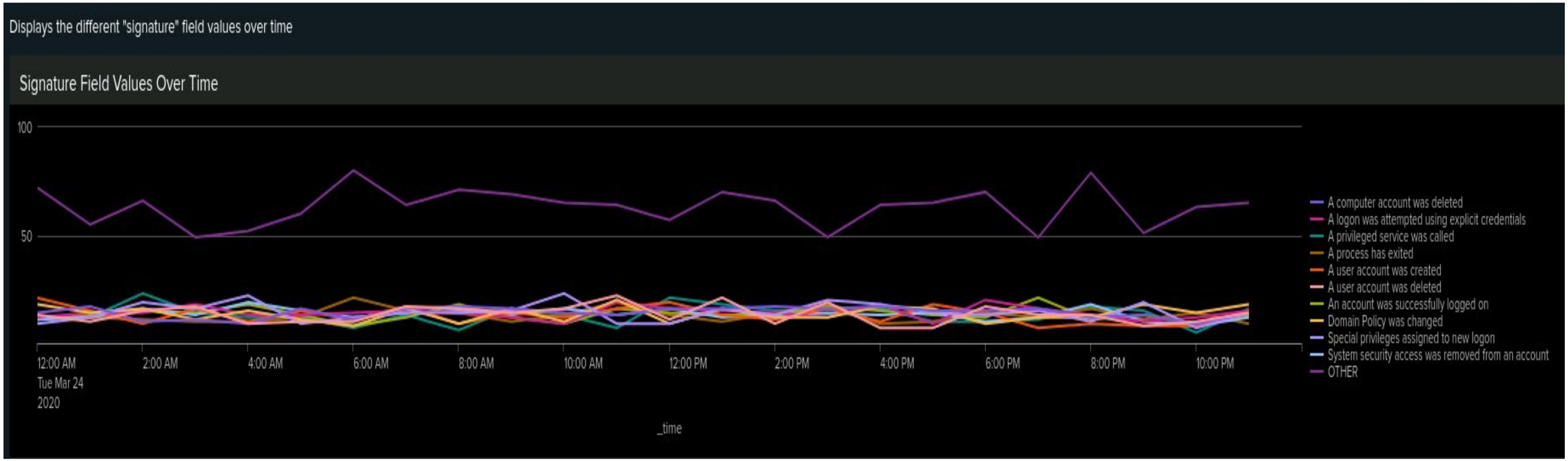
Alerts—Windows

Designed the following alerts:

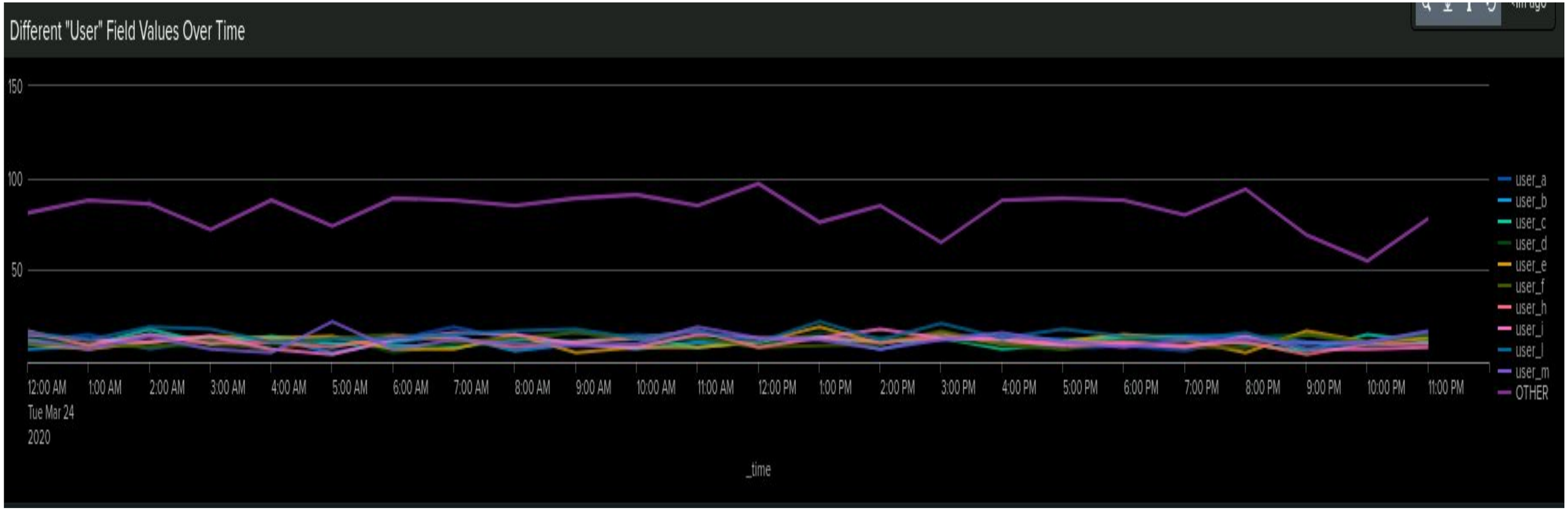
Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Deleted User Accounts	The threshold of deleted user accounts has been reached.	15	35

JUSTIFICATION:
The estimated average to determine the baseline for the normal amount of deleted user accounts was 15 per hour.
The threshold should be 35 deleted user accounts, because the highest “normal” amount of successful logins was 22 during some hours

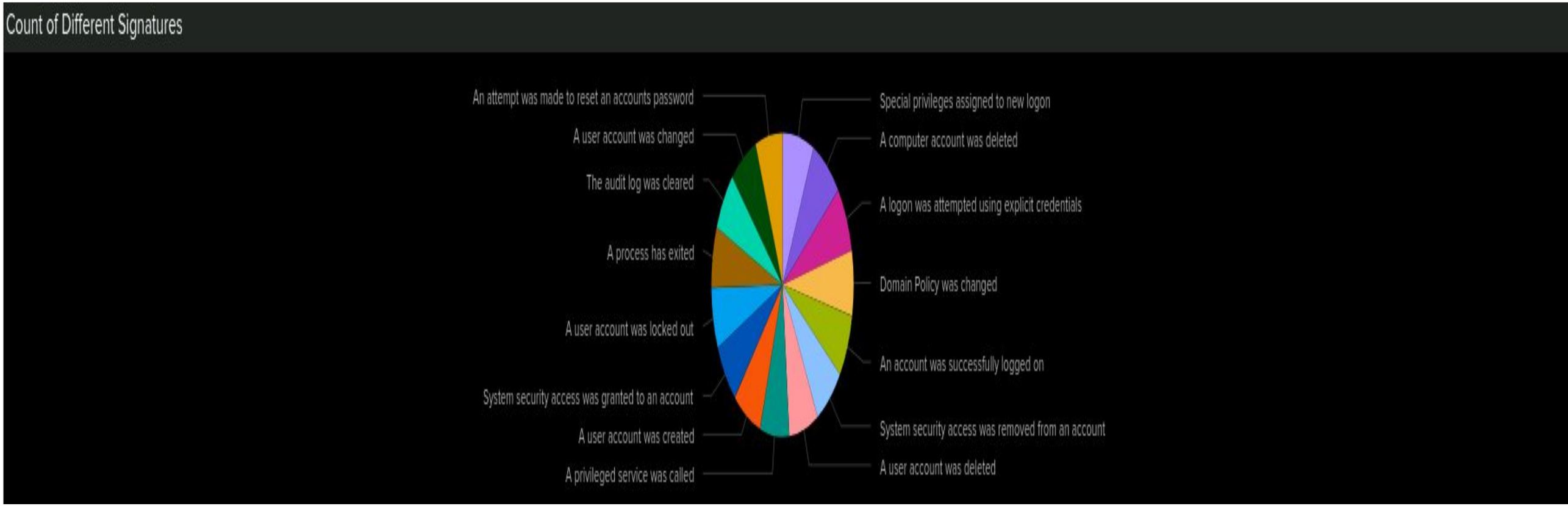
Dashboards—Windows-Signature Field Values Over Time



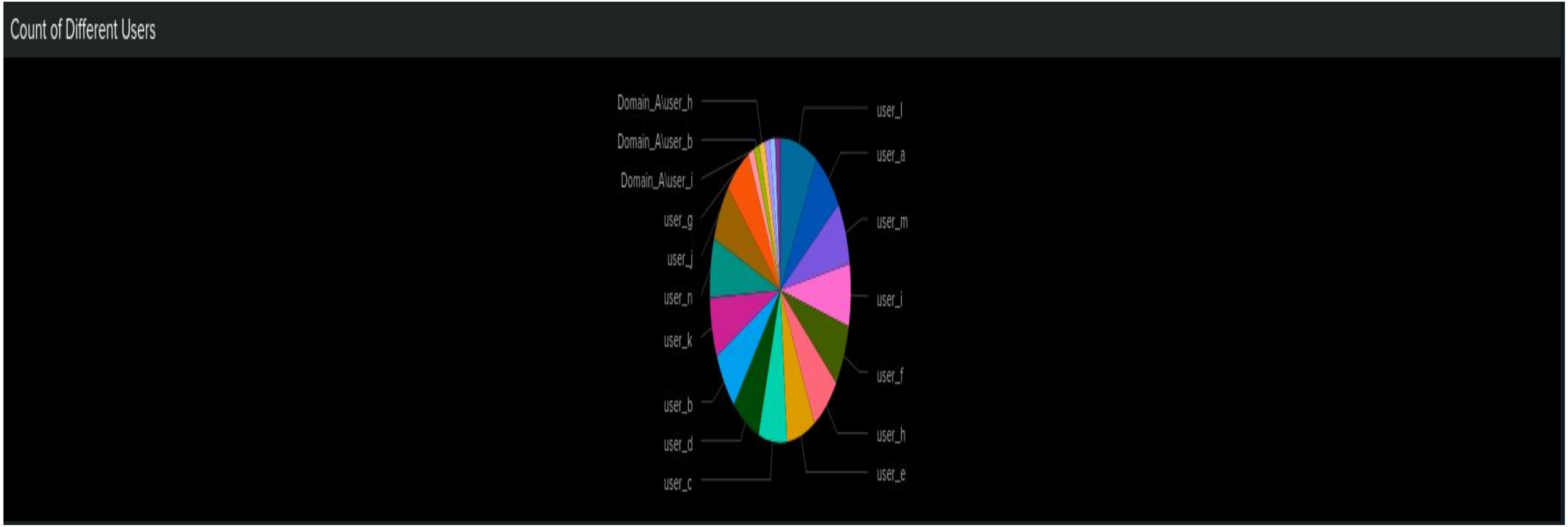
Dashboards—Windows-Different User Fields Over Time



Dashboards—Windows-Count of Different Signatures



Dashboards—Windows-Count of Different Users



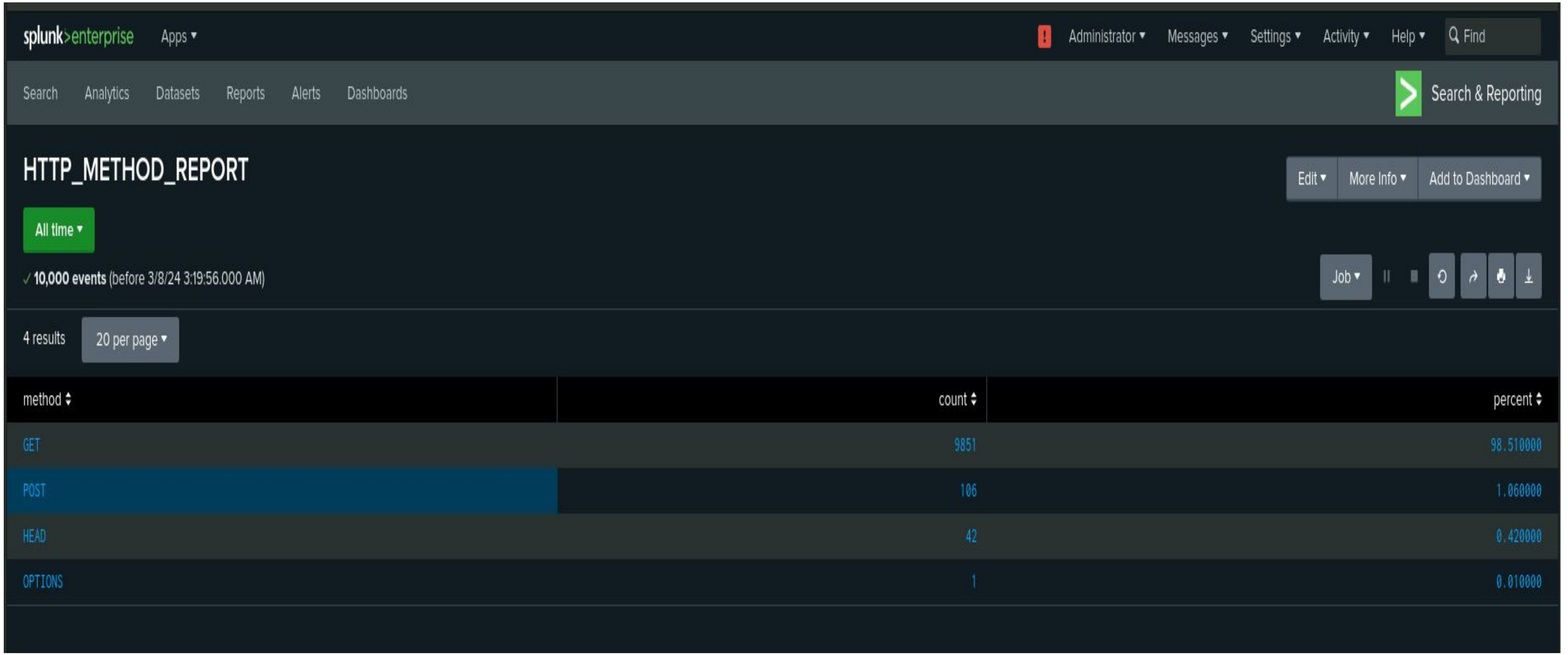
Apache Logs

Reports—Apache

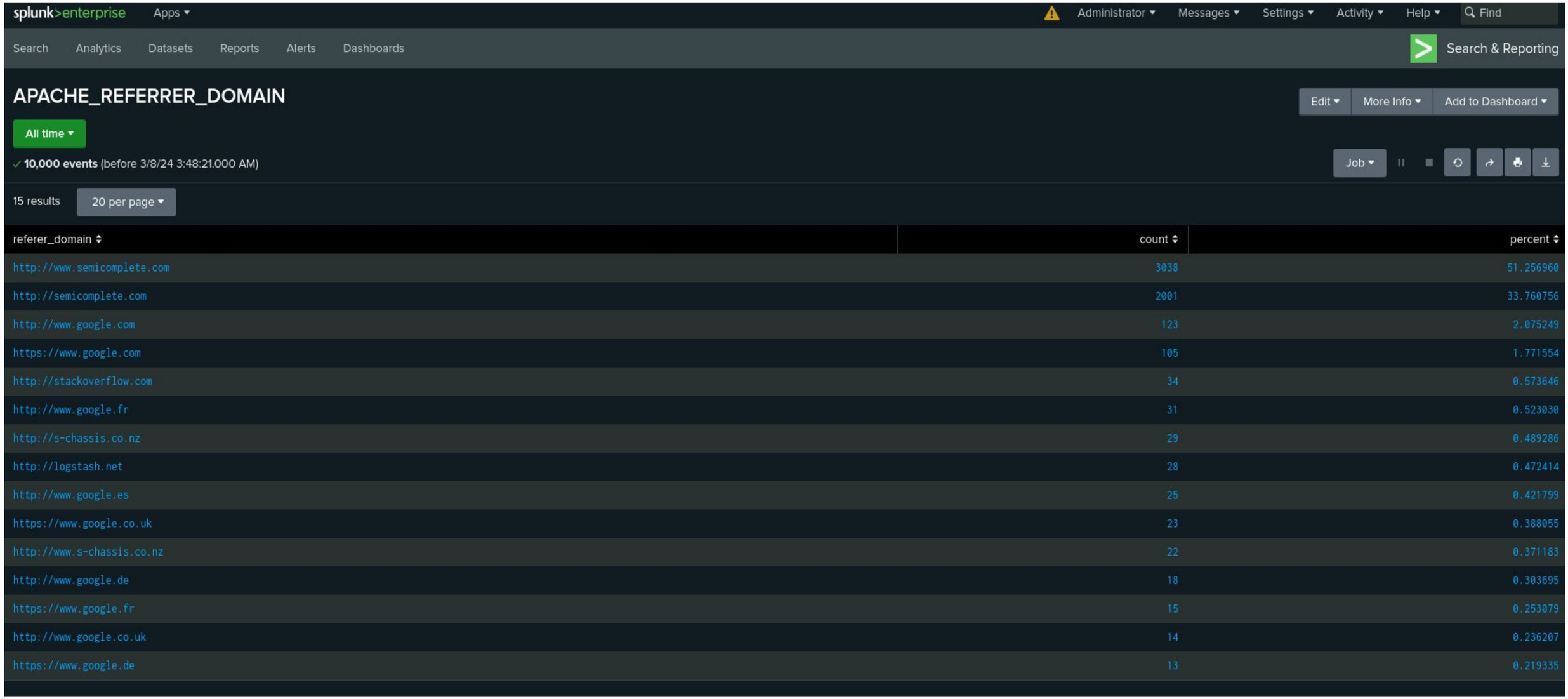
Designed the following reports:

Report Name	Report Description
HTTP_METHOD_REPORT	Shows the different types of HTTP responses against the website which can provide insight into the type of activity being requested.
APACHE_REFERRER_DOMAIN	Shows the top 15 domains that refer to VSI's website and the count for how many times it occurred.
APACHE_STATUS_REPORT	Shows the count of each specific HTTP response code and provides insight into any suspicious activity from them.

Images of Reports—Apache HTTP Methods

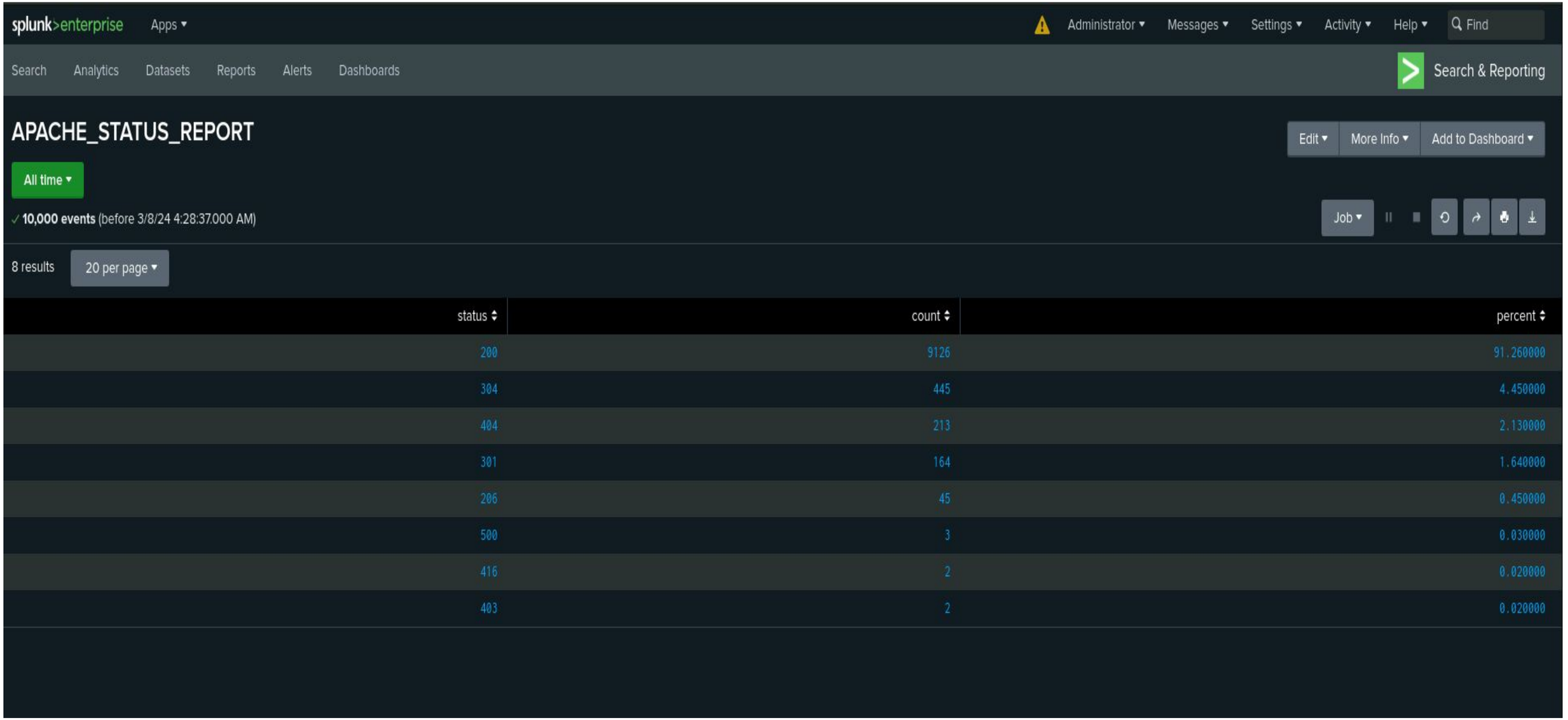


Images of Reports—Apache Top 15 Domains



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
http://www.s-chassis.co.nz	22	0.371183
http://www.google.de	18	0.303695
https://www.google.fr	15	0.253079
http://www.google.co.uk	14	0.236207
https://www.google.de	13	0.219335

Images of Reports—Apache HTTP Status Report



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Non-US Activity	The threshold of Non-US Activity has been Reached.	85	180

JUSTIFICATION: The estimated average to determine the baseline for the “normal” amount of non-US activity was 85 per hour.
The threshold should be 180 non-US activity because the highest “normal” amount of non-US activity was 120 during some hours.

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI - HTTP POST Count	Threshold for hourly HTTP POST has been reached.	2	15

JUSTIFICATION: The estimated average to determine the baseline for the “normal” amount of HTTP POST requests was 2 per hour. The threshold should be 15 POST requests hourly because the highest “normal” amount of POST requests was 7 during some hours.

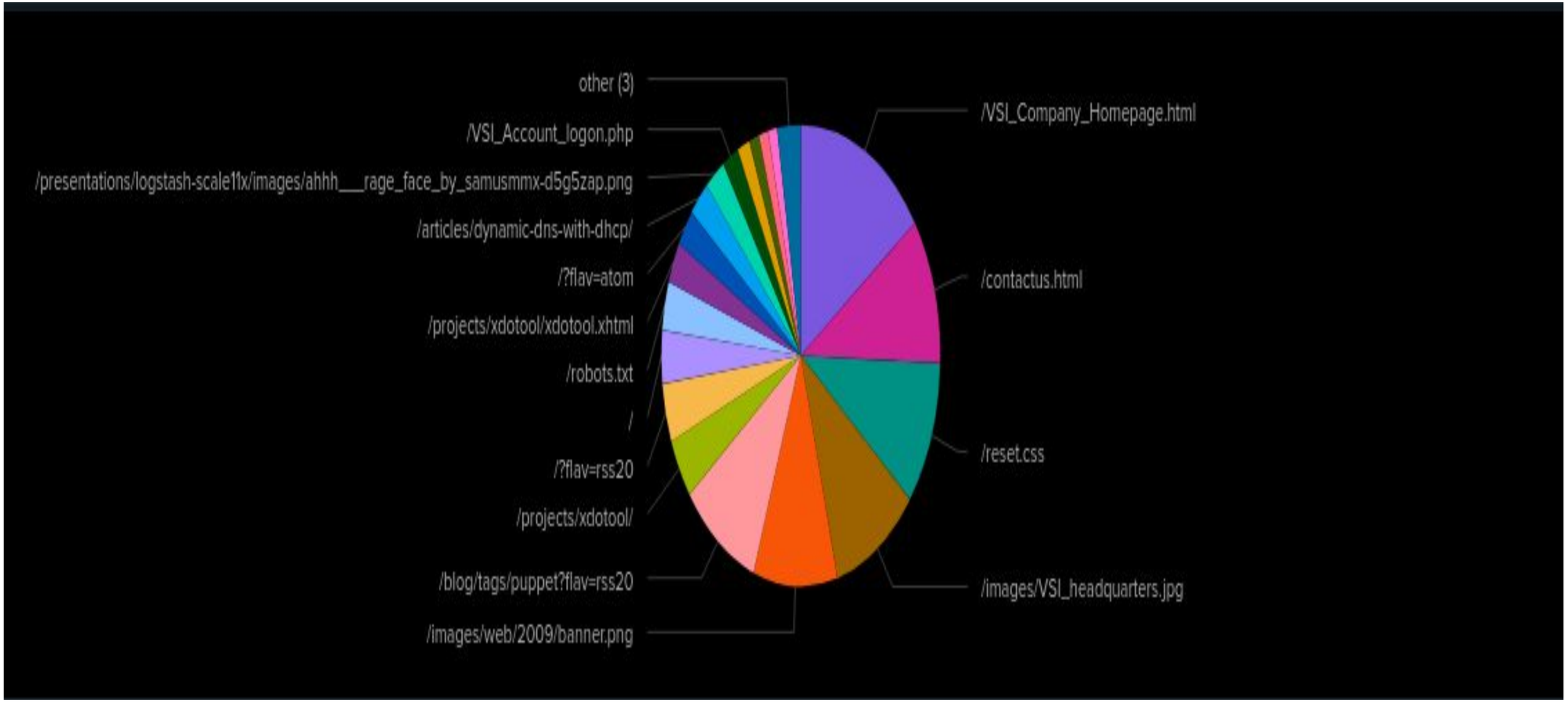
Dashboards—Apache HTTP Methods Over Time

Number of HTTP requests over time and the different HTTP methods used in the requests

Dashboards—Apache IP Locations

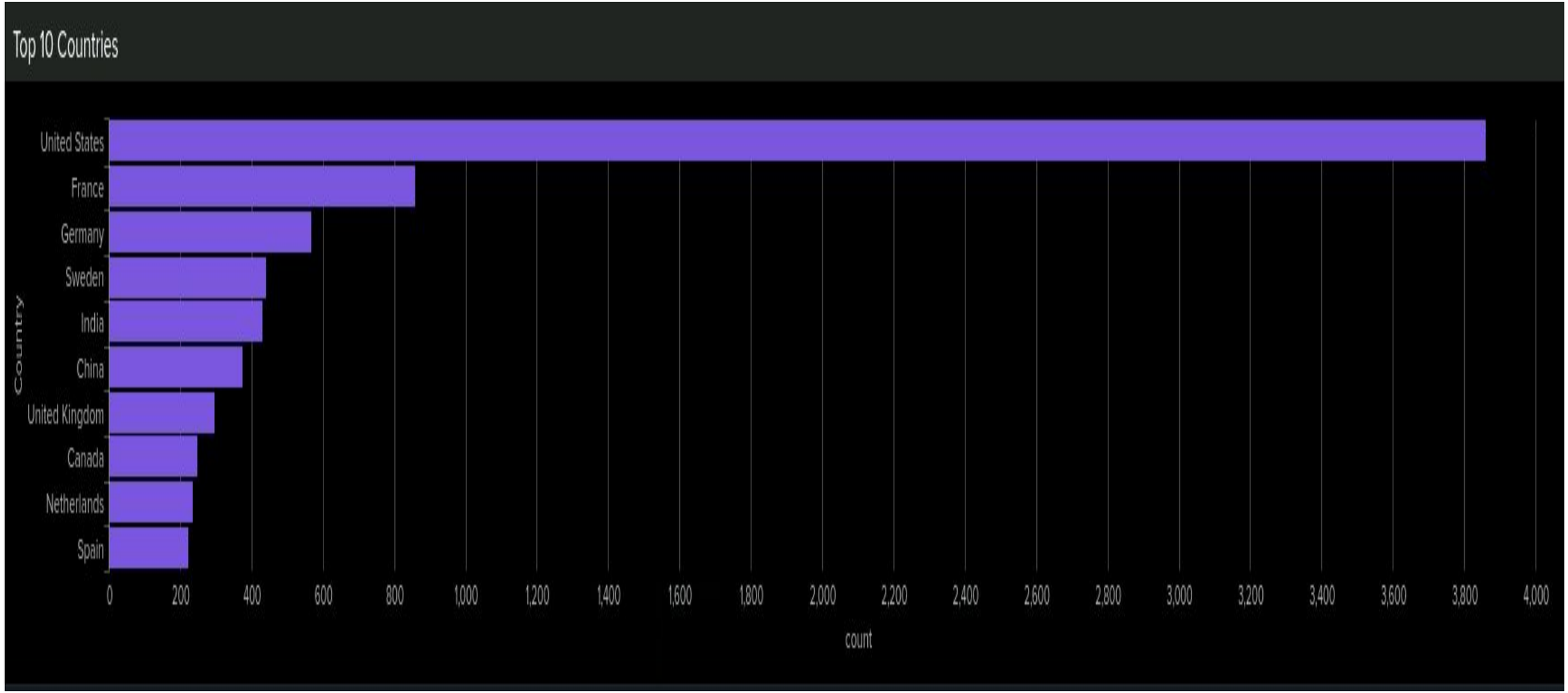
Activity on the web server laid out by IP Address location showing the usage of the web server in different countries

Dashboards—Apache URI Values



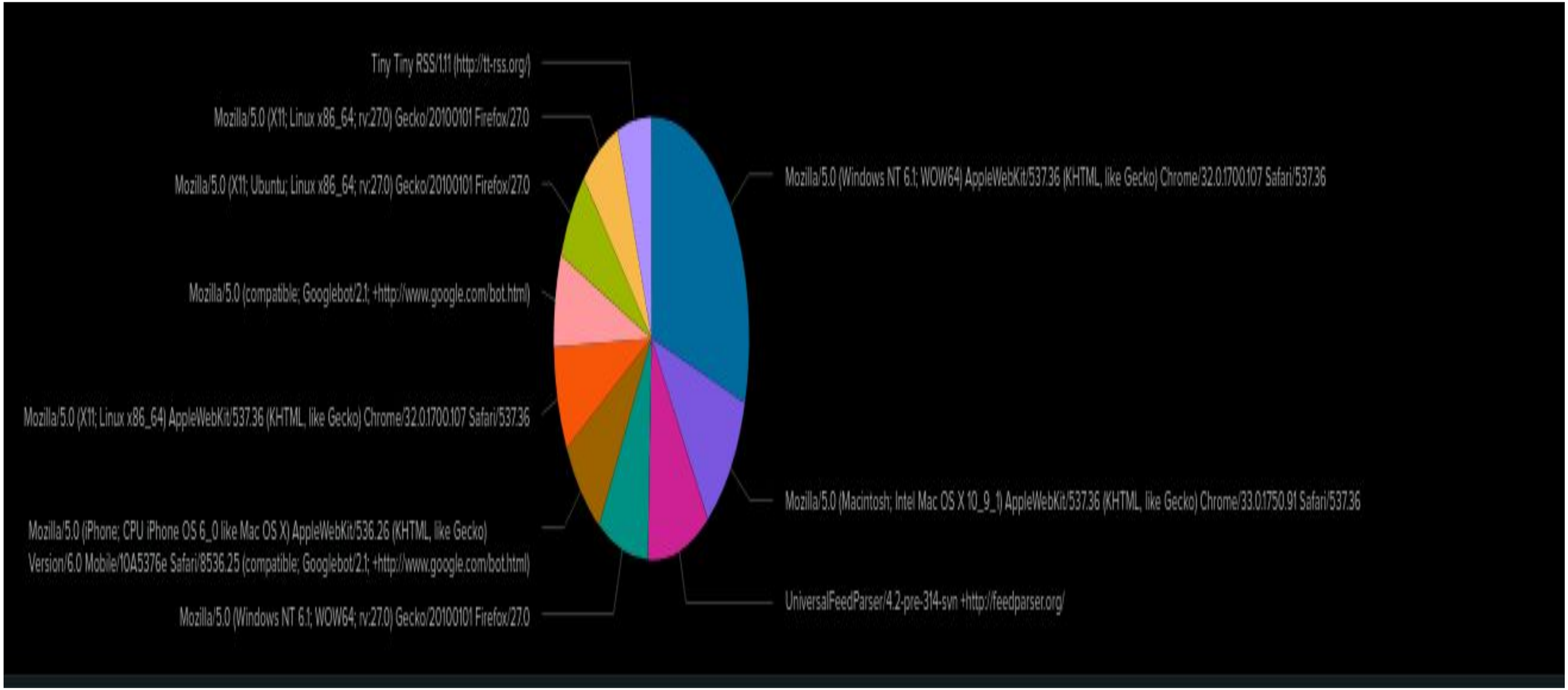
Shows the different URIs used on the web server ("other" had 1000+ so I made it to only show a few)

Dashboards—Apache Top 10 Countries



Distribution of user countries

Dashboards—Apache Top 10 User Agents



The top used user agents on the web server

Dashboards—Apache Status Code 404

number of errors users received on the web server

Attack Analysis

Attack Summary—Windows

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

- In the “severity” report, the original “informational” severity was 93.09 percent while the “high” severity was 6.9 percent. This changed to about 80 percent “informational” and about 20 percent “high” in the attack logs.
- In the “failed activities” report, the original failed activities was about 3 percent. The attack logs state that failed activities is now about 1.5 percent.

Attack Summary—Windows

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

- The thresholds were correct and would have alerted against these attacks, however the thresholds would have to be increased to accommodate for new data.
- A suspicious volume of failed windows activity occurred with a count of 70 events at 8 AM on March 25th, 2020.
- A suspicious volume of successful logins occurred with a count of 784 to 1293 at time ranges spanning from 1 AM to 2 AM and 9 AM to 10 AM on March 25th, 2020

Attack Summary—Windows

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

- In the findings from ***Signatures*****,** “A user account was locked out” and “An attempt was made to reset an accounts password” take up the majority of data.
- This data also aligns with the findings from ***Users*** where users “A” and “K” take up the majority of data, and we can see that “User A” contributed towards “A user account was locked out” and “User K” contributed towards “An attempt was made to reset an account’s password.”

Screenshot of Attack Logs– Windows Server Monitoring

Attack Summary—Apache

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

- The attack logs reports found some suspicious activity in the HTTP requests as well as the response codes on the web server.
  - GET requests had decreased by about 28.3% while POST requests had increased by 28.3%.
  - There were also slight changes in the HTTP response codes: response 200 had decreased by about 8% while response 404 had increased by about 13%.
    - While the changes in the 200 response code may not be significant, the increase in 404 responses could be seen as suspicious albeit being not as significant as well.

Attack Summary—Apache

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

- The thresholds were correct and would have been alerted to these attacks. No necessary changes to the alerts would be required, as the attacks were grossly over the baseline of 180 and 15.
- A suspicious volume of non-US activity occurred on 8 AM on March 25th, 2020 with a peak count of 1,296.
  - Attacks were primarily centralized in the region of Ukraine.

Attack Summary—Apache

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

- After analyzing the dashboards, there was suspicious activity noted in the GET and POST requests on the web server as well as a suspicious increase in request coming in from a new location.
  - GET and POST requests seemed to have an increase surge on Wednesday March 25th.
    - The GET request surge lasted from 5pm to 7pm with a peak count of 729 and the POST request surge followed from 7pm to 9pm with a peak count of 1296.
  - Activity also increased in a new location, Ukraine, with activity centralizing in the cities of Kiev and Kharkiv.
    - Kiev had and activity count of 440 while Kharkiv had a count of 432

Attack Summary—Apache

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

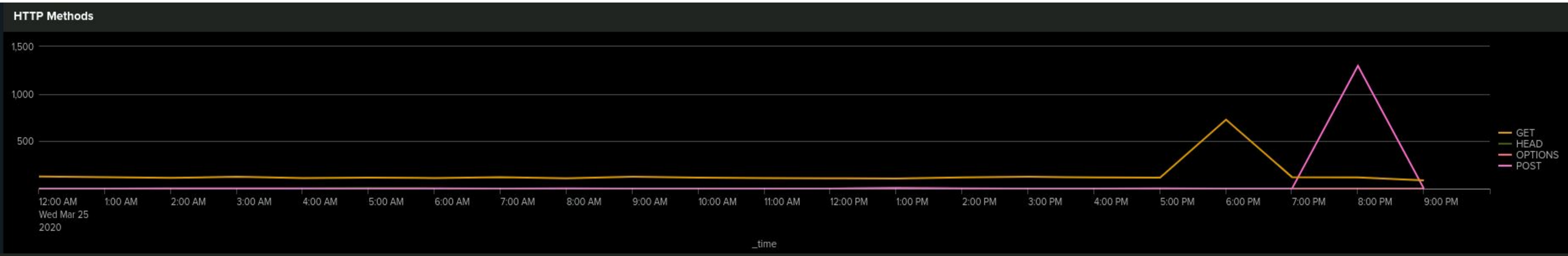
- Along with the HTTP requests and the activity in Ukraine, there was also suspicious activity noted in the URI Data on the server.
  - There was an increase on the /VSI_Account_logon.php URI from a count of 101 to a count of 1323.
  - There was an increase on the /files/logstash/logstash-1.3.2-monolithic.jar URI from a count of 61 to a count of 638.
- This data shows us that the attacker is most likely trying to access the logon page of the web server and using a brute force attack to get in.

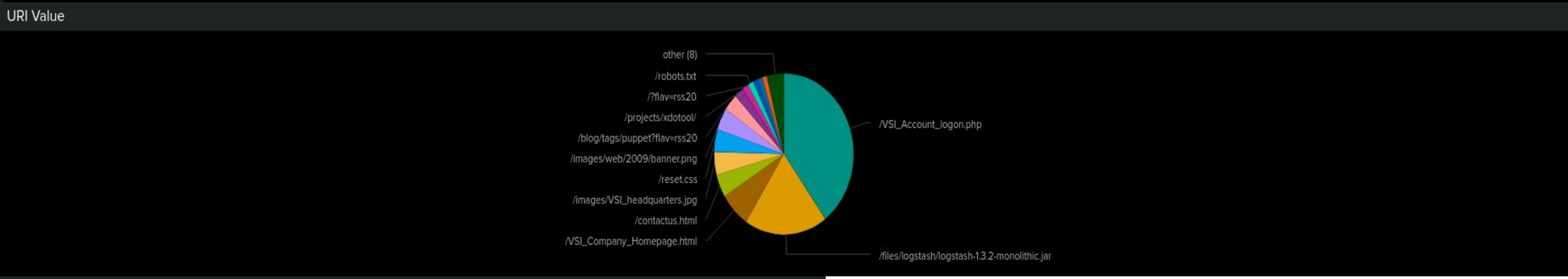
Screenshots of Attack Logs - Reports

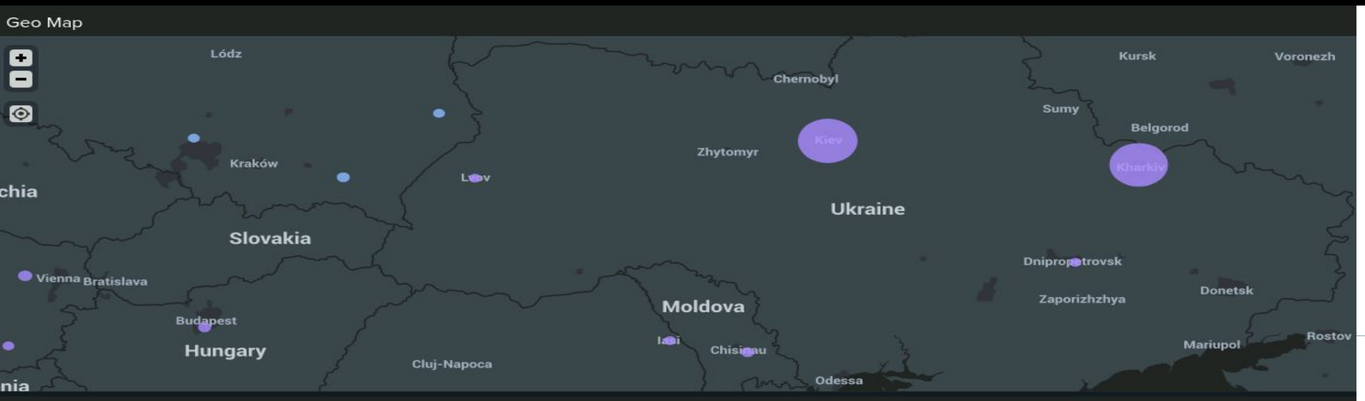
method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237

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

Screenshots of Attack Logs - Dashboard







Summary and Future Mitigations

Project 3 Summary

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

Our overall findings found that March 25th, VSI corporation had multiple attacks on their Apache and Windows servers. The primary form of these attacks involved the brute force attacks, originating from various regions and countries worldwide.

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

Some future mitigations we would recommend includes:

- Limit the number of login attempts
- Implement strong password requirements
- Use two-factor authentication
- Set up IP Access restrictions