Defensive Security Project

by: Liam, Joey, Ryan, Nyantan, Pradeep, Addi, & Davey

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

Project: Defensive Security Monitoring Environment

Objective: Design and implement a custom monitoring environment to protect the fictional organization from cyber attacks.

Research and Design:

Utilize Splunk to research and design a monitoring solution.

Identify and analyze potential security threats and vulnerabilities with reports.

Develop a comprehensive monitoring plan that addresses the identified threats.

Testing and Evaluation:

Implement the designed monitoring solution.

Simulate various cyberattacks and evaluate the effectiveness of the monitoring system in detecting and responding to these attacks.

Identify any gaps or weaknesses in the monitoring solution and make necessary adjustments.

Whois XML IP Geolocation API

Whois XML IP Geolocation API for Splunk - Summary

Whois XML IP Geolocation API is a powerful tool for identifying the geographical location of an IP address. It provides accurate and up-to-date information on the location of an IP address, including country, city, latitude, longitude, and time zone. The API can also be used to identify the ISP and ASN associated with an IP address.

The Whois XML IP Geolocation API is easy to use and can be integrated into a variety of applications such as **Splunk**. It is a valuable tool for security professionals, fraud analysts, and anyone else who needs to identify the location of an IP address.

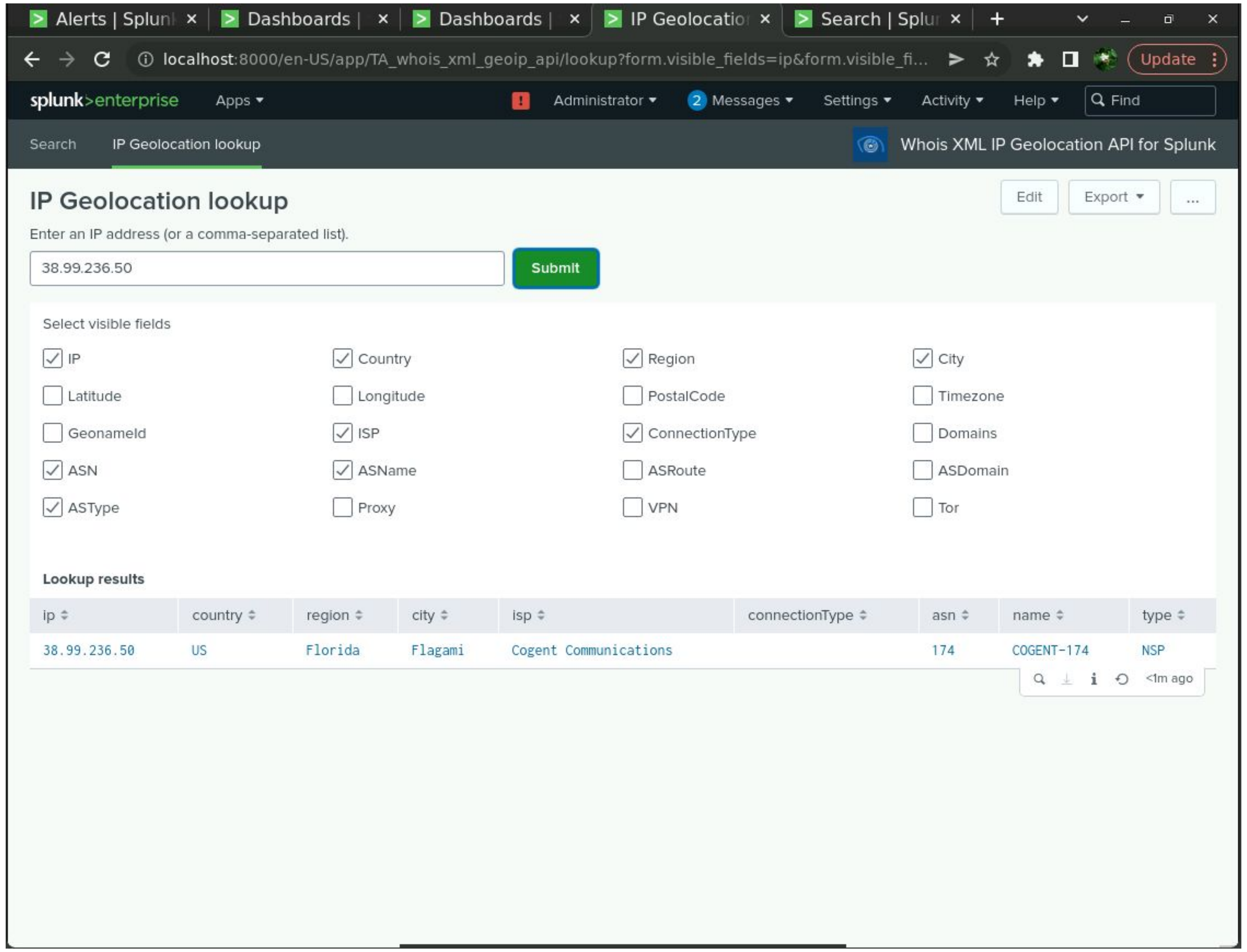
Key Features of Whois XML IP Geolocation API:

- Accurate and up-to-date IP location data
- Support for IPv4 and IPv6 addresses
- XML and JSON output formats
- Easy-to-use API
- Bulk IP geolocation support

Whois XML IP Geolocation API for Splunk - Scenario

A scenario that this app would allow you to benefit from is if you or your company wanted to monitor where the network is being accessed from in order to determine whether or not it was valid, or detect unexpected traffic. With unexpected traffic you can identify where it’s coming from and what events are occurring under that IP.

Whois XML IP Geolocation API for Splunk - Images



IP Geolocation lookup

Enter an IP address (or a comma-separated list).

38.99.236.50

Submit

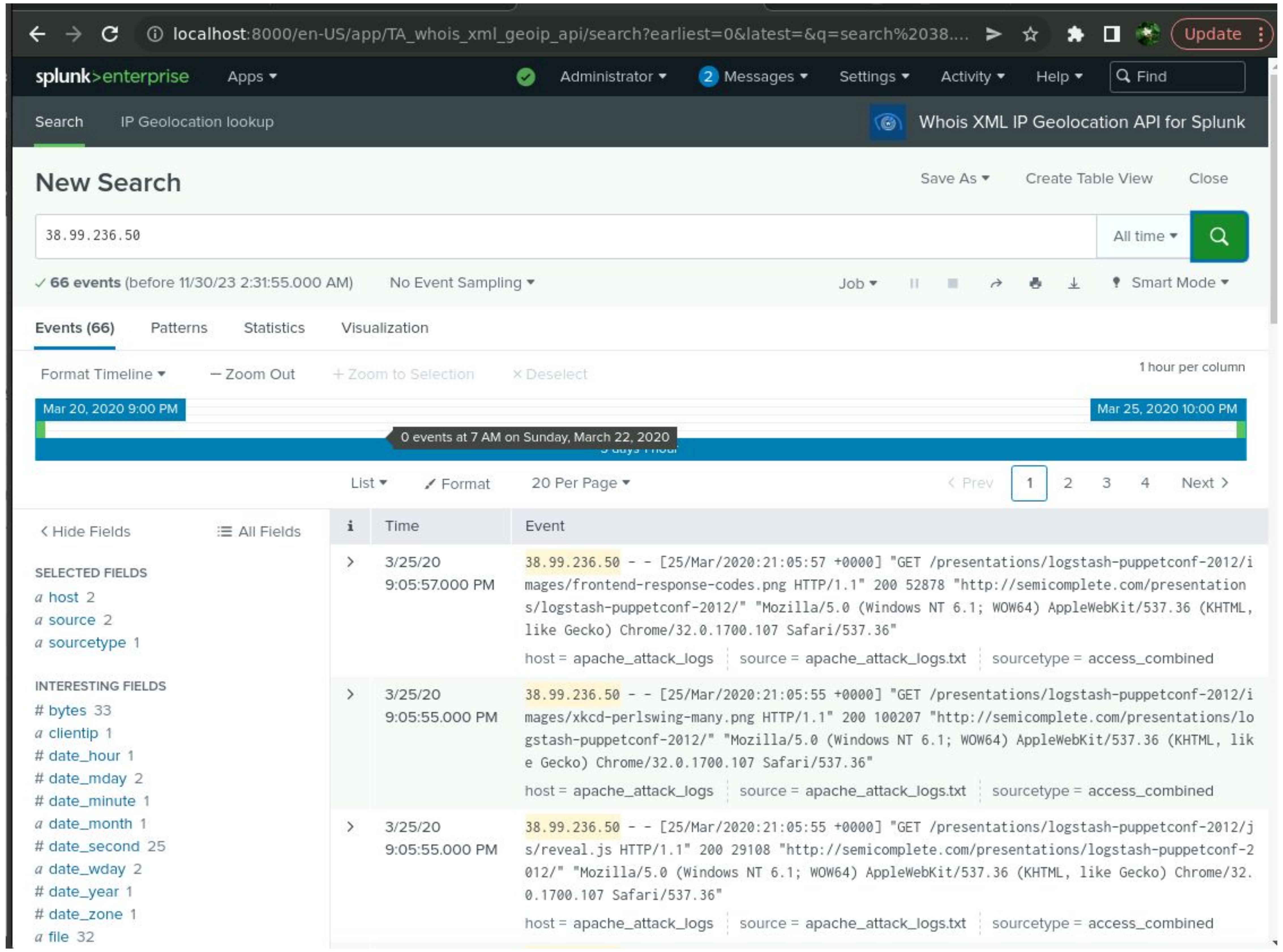
Select visible fields

☑ IP	☑ Country	☑ Region	☑ City
□ Latitude	□ Longitude	□ PostalCode	□ Timezone
□ GeonameId	☑ ISP	☑ ConnectionType	□ Domains
☑ ASN	☑ ASName	□ ASRoute	□ ASDomain
☑ ASType	□ Proxy	□ VPN	□ Tor

Lookup results

ip	country	region	city	isp	connectionType	asn	name	type
38.99.236.50	US	Florida	Flagami	Cogent Communications		174	COGENT-174	NSP

<1m ago



New Search

38.99.236.50 — All time

✓ 66 events (before 11/30/23 2:31:55.000 AM) — No Event Sampling

Events (66) | Patterns | Statistics | Visualization

Mar 20, 2020 9:00 PM — Mar 25, 2020 10:00 PM

0 events at 7 AM on Sunday, March 22, 2020

SELECTED FIELDS
- a host 2
- a source 2
- a sourcetype 1

INTERESTING FIELDS
- # bytes 33
- a clientip 1
- # date_hour 1
- # date_mday 2
- # date_minute 1
- a date_month 1
- # date_second 25
- a date_wday 2
- # date_year 1
- a date_zone 1
- a file 32

i	Time	Event
›	3/25/20 9:05:57.000 PM	38.99.236.50 - - [25/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = apache_attack_logs source = apache_attack_logs.txt sourcetype = access_combined
›	3/25/20 9:05:55.000 PM	38.99.236.50 - - [25/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/images/xkcd-perlswing-many.png HTTP/1.1" 200 100207 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = apache_attack_logs source = apache_attack_logs.txt sourcetype = access_combined
›	3/25/20 9:05:55.000 PM	38.99.236.50 - - [25/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/js/reveal.js HTTP/1.1" 200 29108 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = apache_attack_logs source = apache_attack_logs.txt sourcetype = access_combined

Logs Analyzed

1 Windows Logs

- Signature ID- An identification number for the event that occurred.
- Signature- Description of the event that occurred.
- User- The user associated with that event.
- Status- Whether the intent of the event succeeded or failed.
- Severity- Level of severity of the event that occurred.

2 Apache Logs

- Method- HTTP method associated with the event.
- Referer Domain- Domain name involved with the event.
- Status- HTTP response code for the event.
- Client IP- IP address involved with the event.
- User agent- Web browser, email client, download manager, etc. that was used in the event.

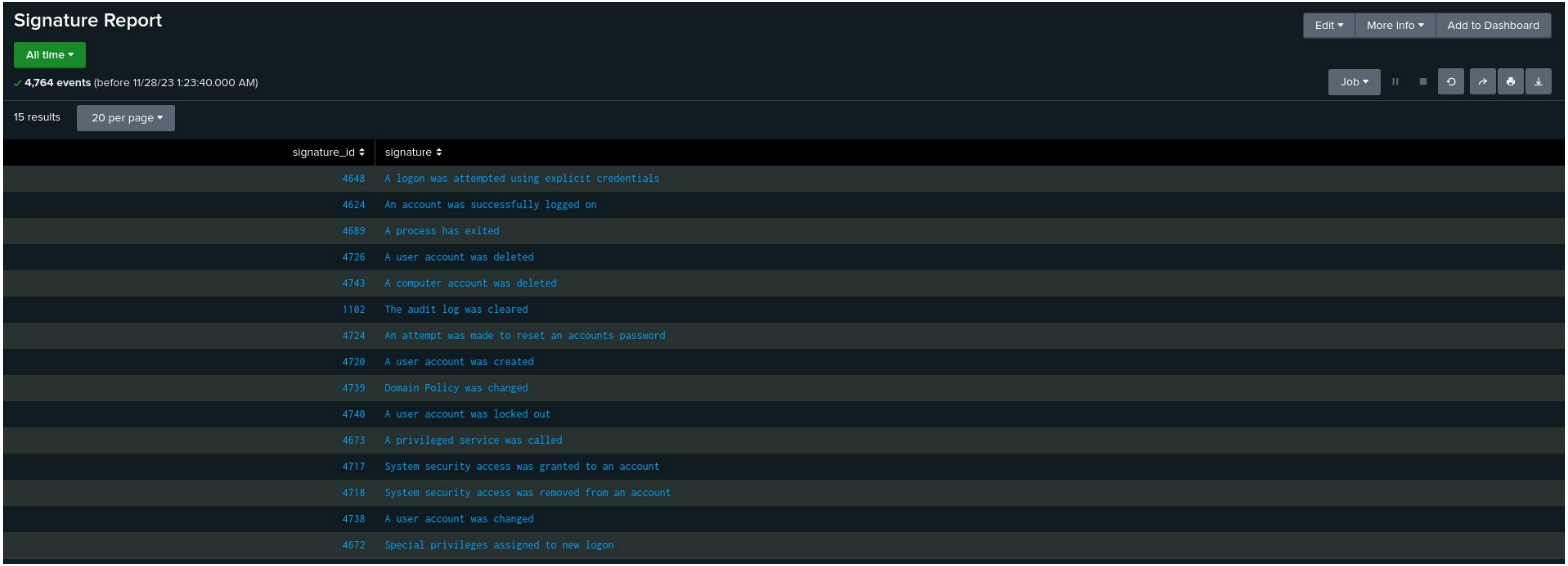
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signature Report	Shows signatures along with their respective IDs
Severity Report	Shows Informational and High Severities along with counts and percentages
Status Report	Shows Successes and Failures of logons in the form of a bar graph

Images of Reports—Windows

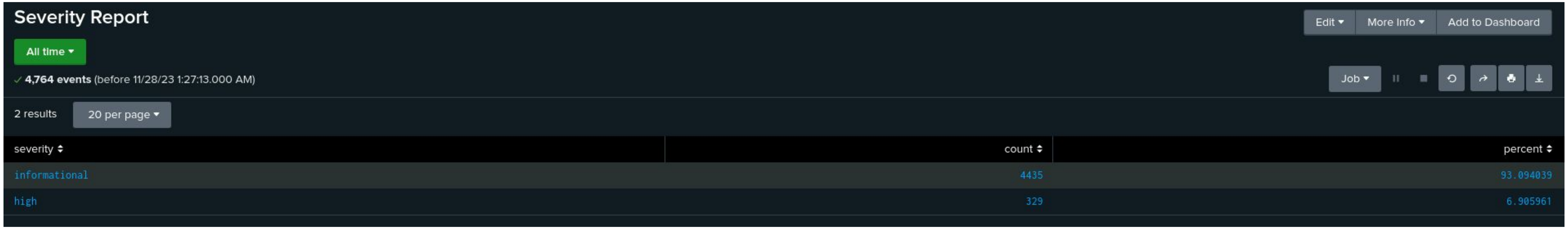


✓ **4,764 events** (before 11/28/23 1:23:40.000 AM)

15 results

signature_id	signature
4648	A logon was attempted using explicit credentials
4624	An account was successfully logged on
4689	A process has exited
4726	A user account was deleted
4743	A computer account was deleted
1102	The audit log was cleared
4724	An attempt was made to reset an accounts password
4720	A user account was created
4739	Domain Policy was changed
4740	A user account was locked out
4673	A privileged service was called
4717	System security access was granted to an account
4718	System security access was removed from an account
4738	A user account was changed
4672	Special privileges assigned to new logon

Images of Reports—Windows

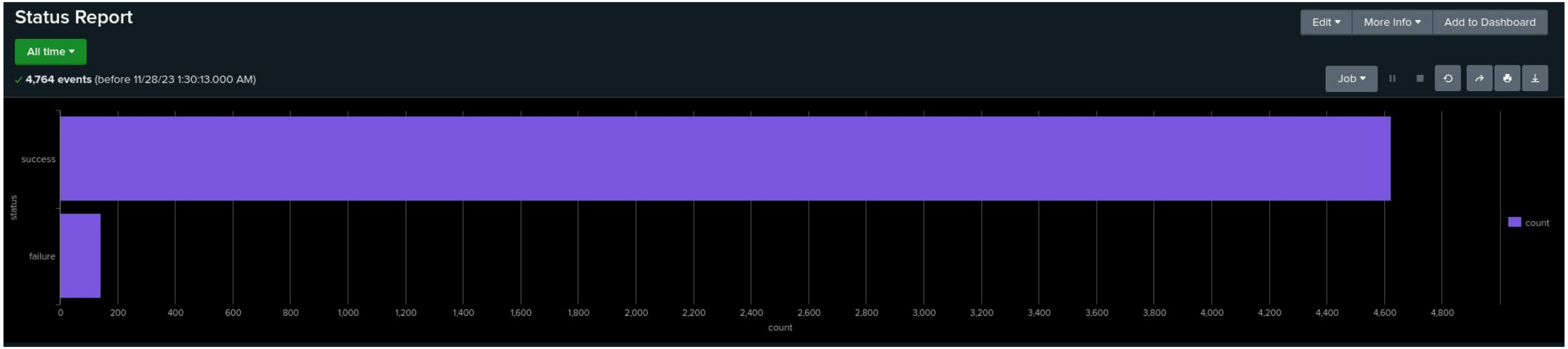


Severity Report

✓ **4,764 events** (before 11/28/23 1:27:13.000 AM)

2 results

severity	count	percent
informational	4435	93.094039
high	329	6.905961



Status Report

✓ **4,764 events** (before 11/28/23 1:30:13.000 AM)

Alerts—Windows

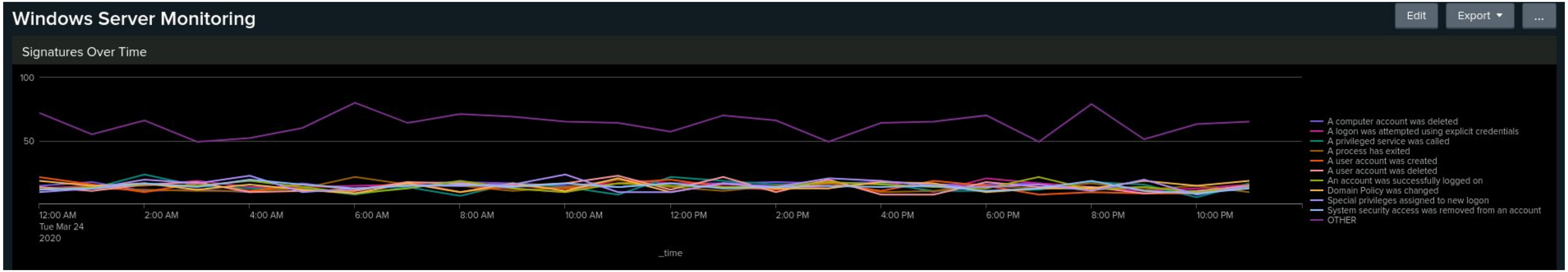
Designed the following alerts:

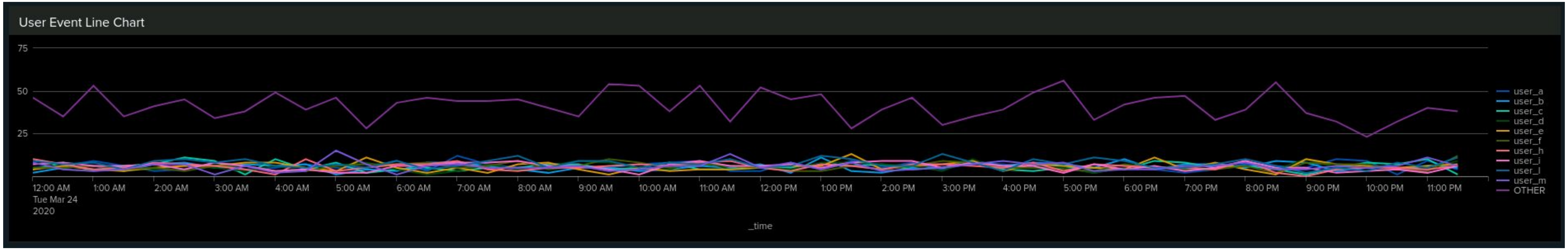
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	Send email to SOC@VSI-company.com when hourly failed activity exceeds threshold	6	15
Successful Logins	Send email to SOC@VSI-company.com when single-account login activity within an hour exceeds threshold	13	25
Accounts Deleted	Send email to SOC@VSI-company.com when number of accounts deleted within an hour exceeds threshold	14	25

JUSTIFICATION: When viewing the normal activity logs we saw, over a 24 hour period:

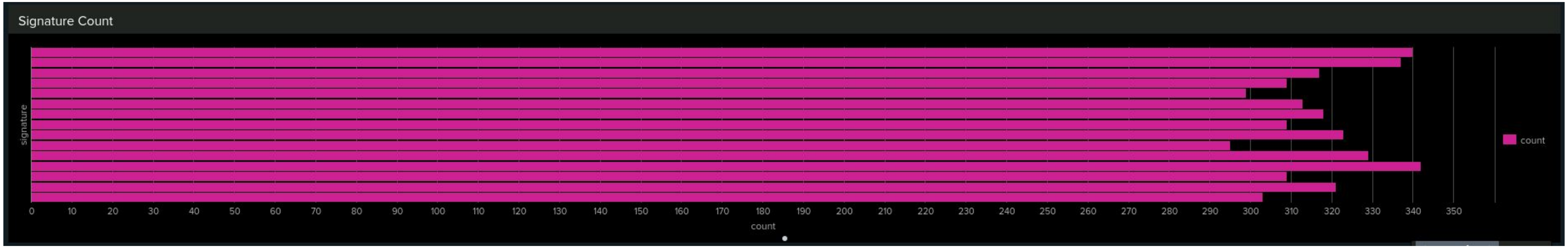
- 142 failure events (142/24=5.91 baseline)
- 323 successful login events (323/24=13.458 baseline)
- 318 account deletions (318/24=13.25 baseline)

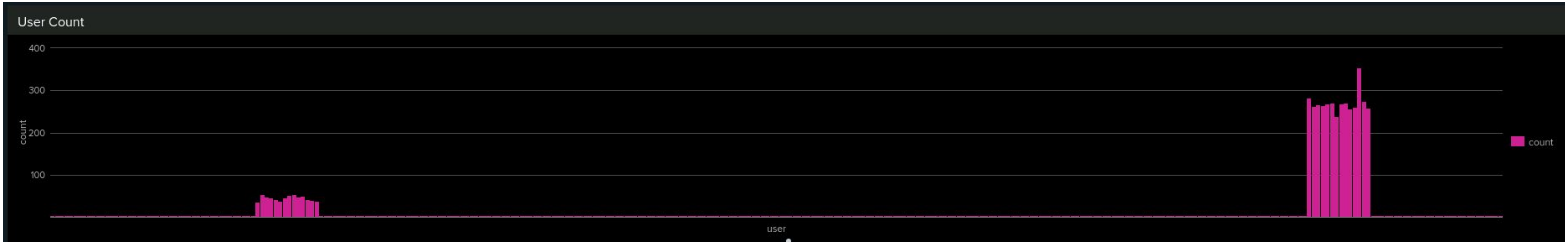
Dashboards—Windows


Windows Server Monitoring
Edit
Export ▾
...
Signatures Over Time
100
50
12:00 AM
Tue Mar 24
2020
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
10:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER

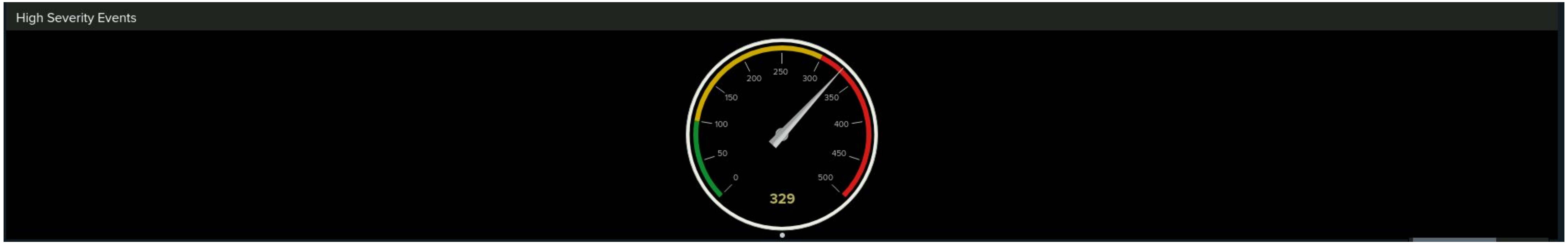


Dashboards—Windows





Dashboards—Windows



High Severity Events

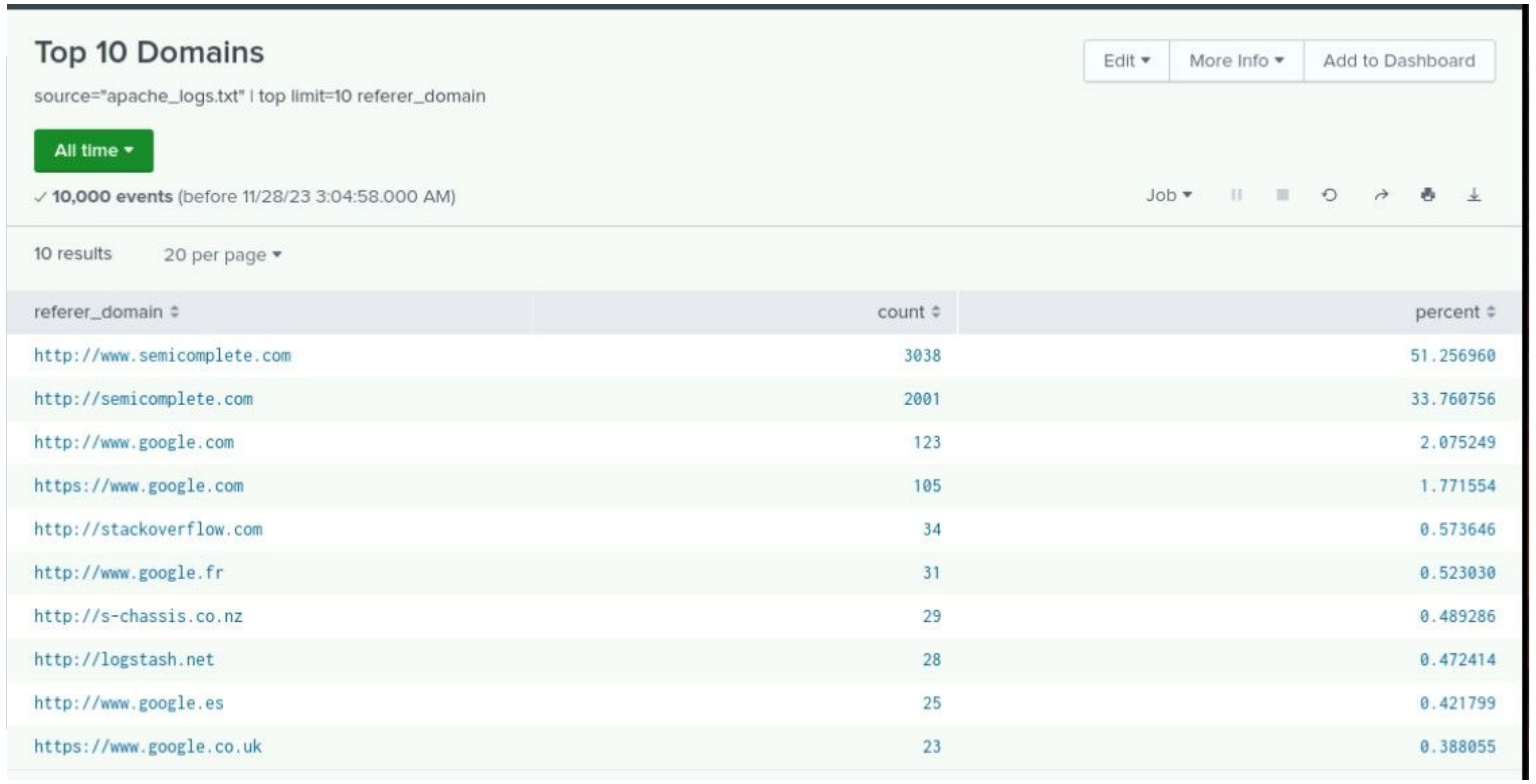
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Report detailing the top HTTP methods (i.e. GET, POST, HEAD, OPTIONS) including the count and percentage of each method
HTTP Response Codes	Report detailing the HTTP response code statuses, counts and percentage of each code
Top 10 Domains	Report detailing the top referrer domains (i.e. http://www.semicomplete.com) including the count and percentage of each domain

Images of Reports—Apache



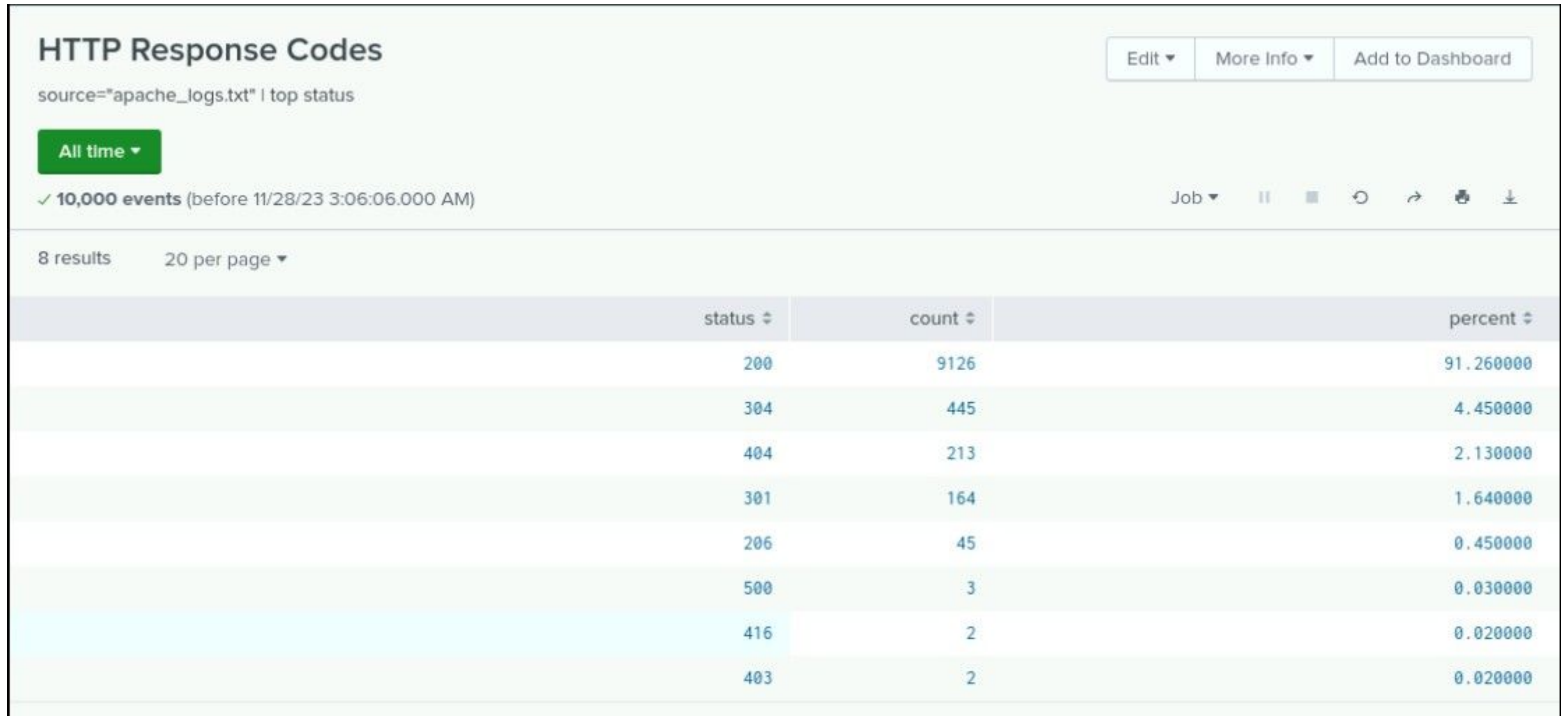
Top 10 Domains

source="apache_logs.txt" | top limit=10 referer_domain

✓ **10,000 events** (before 11/28/23 3:04:58.000 AM)

10 results

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



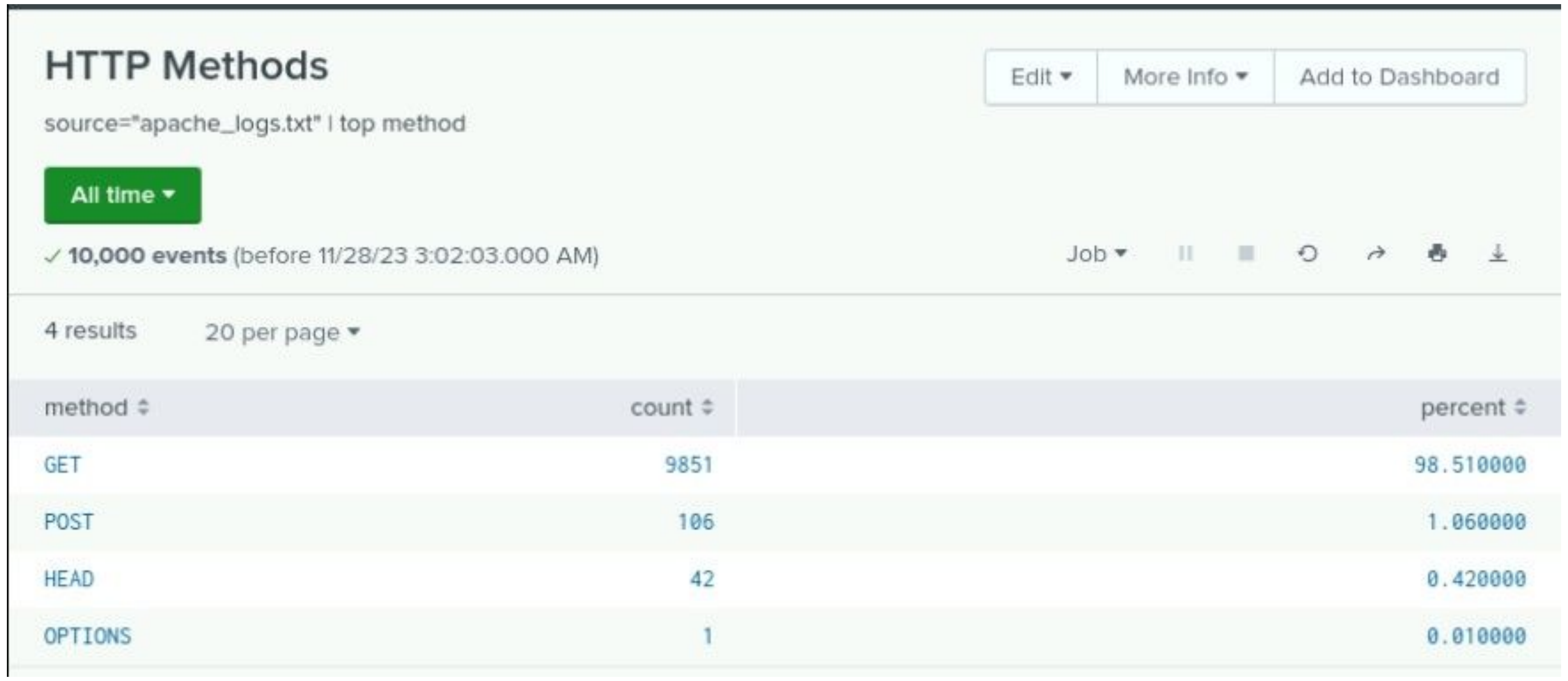
HTTP Response Codes

source="apache_logs.txt" | top status

✓ **10,000 events** (before 11/28/23 3:06:06.000 AM)

8 results

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



HTTP Methods

source="apache_logs.txt" | top method

✓ **10,000 events** (before 11/28/23 3:02:03.000 AM)

4 results

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

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Activity Outside U.S.	An hourly alert that sends an email to SOC@VSI-company.com for suspicious activity outside of the US with over 100 events	73	100
HTTP POST Activity	An hourly alert that sends an email to SOC@VSI-company.com for suspicious POST activity resulting in over 5 events	1.277	5

JUSTIFICATION: When viewing the normal activity logs we saw, over a 84 hour period:

- 6,140 foreign IP events (6,140/84 hours=73.095 baseline)
- 106 POST events (106/83 hours=1.277 baseline*)

**Method search had a timeline of 83 hours instead of the normal 84)*

Dashboards—Apache

Apache Web Server Monitoring

HTTP Methods over time

Last 24 hours

Edit
Export ▾
...
Hide Filters
HTTP Methods Over time
150
100
50
GET
HEAD
OPTIONS
POST
12:00 PM Tue Mar 17 2020
12:00 AM Wed Mar 18
12:00 PM
12:00 AM Thu Mar 19
12:00 PM
12:00 AM Fri Mar 20
12:00 PM
_time
Number of URIs
other (1483)
/
/?flav=rss20
/VSI_Company_Homepage.html
/blog/tags/puppet?flav=rss20
/contactus.html
/images/VSI_headquarters.jpg
/images/web/2009/banner.png
/projects/xdotool/
/projects/xdotool/xdotool.xhtml
/reset.css
/robots.txt
Client IP location
+
-
Top 10 Countries
6,000
4,000
2,000
count
count
United States
France
Germany
Sweden
India
China
United Kingdom
Canada
Netherlands
Spain
Country
Count Different User Agents
other (536)
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536...fari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Single Value Data point
0
2
4
6
8
10
12
14
16
18
20
1

Attack Analysis

Attack Summary—Windows

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

- For the report regarding signatures, there was a significant increase in account lockout and password reset attempts with a slight increase in successful logins
- For the report regarding severity-level analysis, the percentage of ‘high’ level severity event percentage increased from 6.906%-20.222% between the original ‘windows_server_logs.csv’ to the ‘windows_server_attack_logs.csv’.
- For the report regarding failed activity, there was a higher level of overall activity, but not an increase in failed activity.

Attack Summary—Windows

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

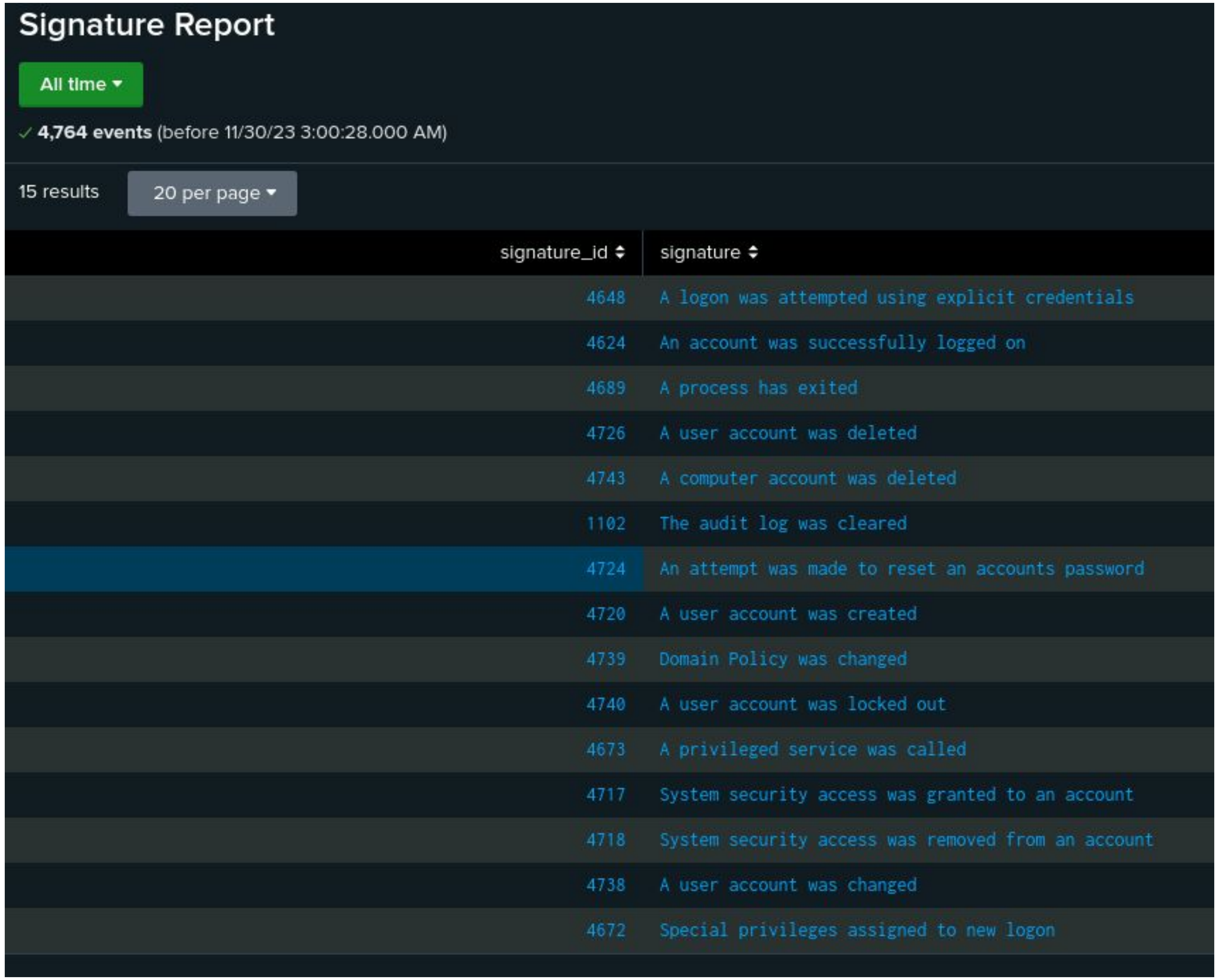
- For the alert regarding failed activity, there was a spike in activity on Wednesday, March 25, 2020 at 8AM resulting in an occurrence of 35 events. Our priorly created threshold would have been triggered for this event.
- For the alert regarding successful login activity, there was a spike in activity on Wednesday, March 25, 2020 at 11AM resulting in 196 events with the most common signature ID being 4624, and the most common user being user_j. Our alert threshold would've been met and triggered by this event.
- For the alert regarding deleted account events, there was not a suspicious amount of deleted accounts. The alert threshold would not have been triggered for these events.

Attack Summary—Windows

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

- Regarding the analysis for time chart of signatures, there were two signatures that mainly stood out which were “a user was locked out” and “an attempt was made to reset an account password” as well as another signature that seemed relevant to the first two being “an account was successfully logged on”. The first signature’s spike was between 12 and 3AM with the event count being 896, the second’s was 8 to 11AM with a count of 1,258, and the third’s was from 10AM to 1PM with a count of 196.
- Regarding the analysis for users, there were two users that stood out the most, with a third having less activity, but more than the average user. The first most-occurring user was user_k, second was user_a and last was user_j. User_a had the most activity between 12-3AM with peak event count of 984, the second was most active between 8-11AM with a count of 1,256, and the last user was active between 10AM-1PM with a count of 196.
- Regarding the analysis for signatures with the multiple visualizations, there was suspicious activity that was visible in these graphs/charts that was reflective of the activity we were seeing in the time charts.
- Regarding the analysis for users with statistical charts, advantages would be that it’s easy to identify top contributors and their values due to the table style of data. Metrics are also easily readable. A disadvantage would be that it may be more difficult to understand the data as a whole in this format, as opposed to a visualization that is fitting for the data that could help to showcase different aspects that may not necessarily be apparent in a different format.

Screenshots of Attack Logs



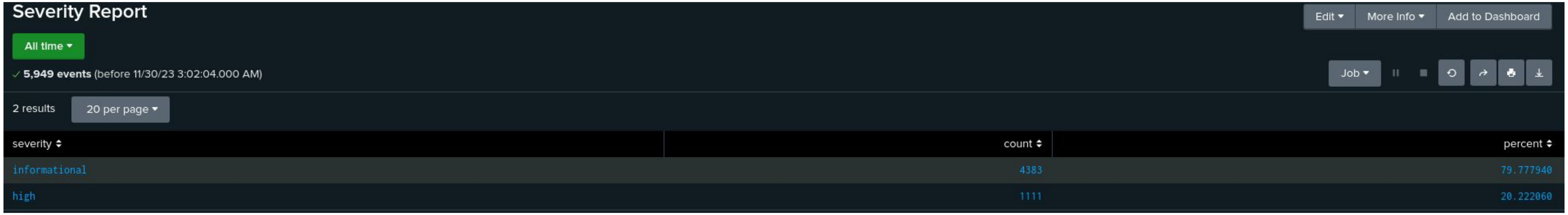
Signature Report

✓ **4,764 events** (before 11/30/23 3:00:28.000 AM)

15 results

signature_id	signature
4648	A logon was attempted using explicit credentials
4624	An account was successfully logged on
4689	A process has exited
4726	A user account was deleted
4743	A computer account was deleted
1102	The audit log was cleared
4724	An attempt was made to reset an accounts password
4720	A user account was created
4739	Domain Policy was changed
4740	A user account was locked out
4673	A privileged service was called
4717	System security access was granted to an account
4718	System security access was removed from an account
4738	A user account was changed
4672	Special privileges assigned to new logon

Screenshots of Attack Logs

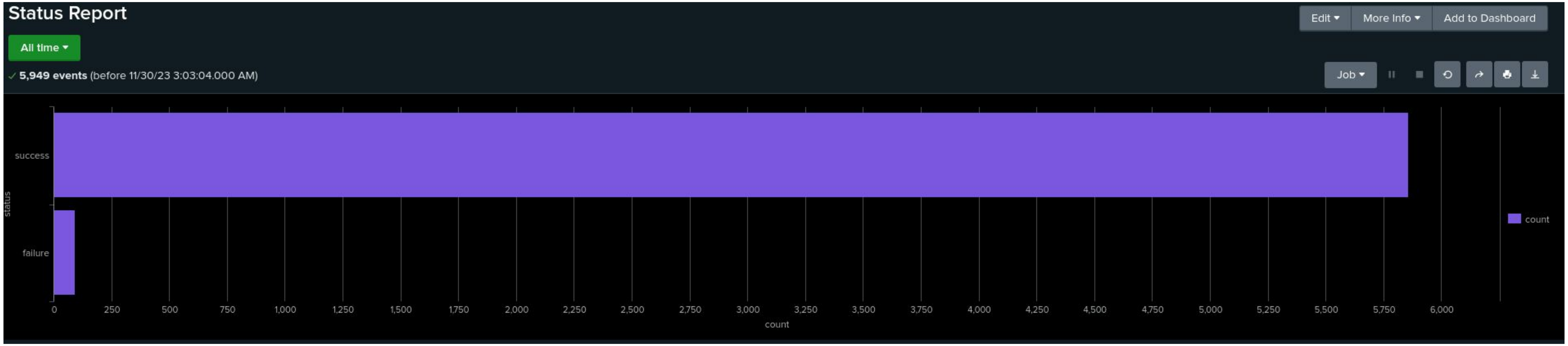


Severity Report

✓ **5,949 events** (before 11/30/23 3:02:04.000 AM)

2 results

severity	count	percent
informational	4383	79.777940
high	1111	20.222060



Status Report

✓ **5,949 events** (before 11/30/23 3:03:04.000 AM)

Screenshots of Attack Logs

Windows Server Monitoring
Edit
Export ▾
...
All time ▾
Hide Filters
Signatures Over Time
1,500
1,000
500
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was changed
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts password
Domain Policy was changed
The audit log was cleared
OTHER
User Event Line Chart
1,000
500
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
_time
user_a
user_b
user_c
user_e
user_f
user_i
user_j
user_k
user_l
user_m
OTHER

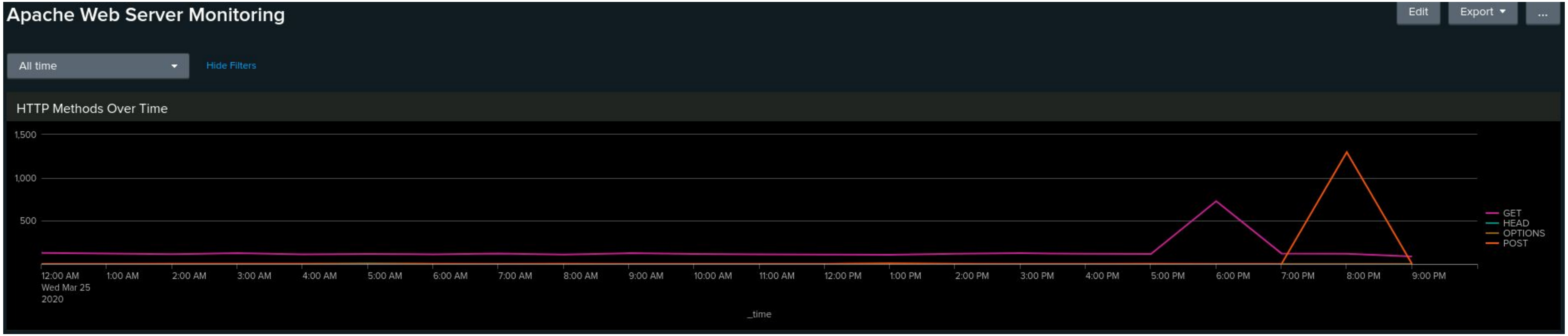
Screenshots of Attack Logs

Signature Count
signature
0
100
200
300
400
500
600
700
800
900
1,000
1,100
1,200
1,300
1,400
1,500
1,600
1,700
1,800
1,900
2,000
2,100
2,200
count
count
User Count
3,000
2,000
1,000
count
user
count

Screenshots of Attack Logs

High Severity Events
0
50
100
150
200
250
300
350
400
450
500
1,111

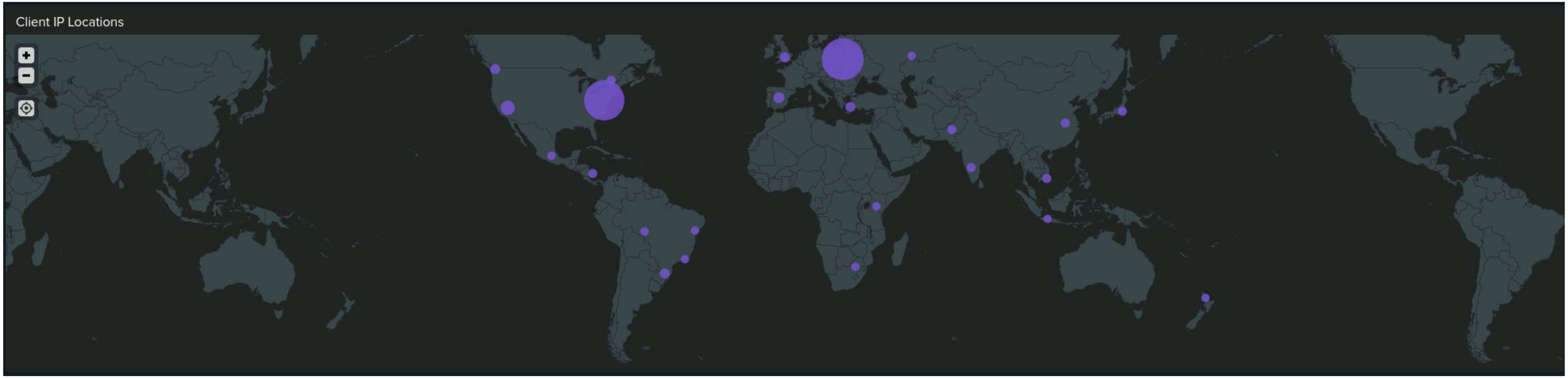
Screenshots of Attack Logs



Apache Web Server Monitoring

All time

HTTP Methods Over Time

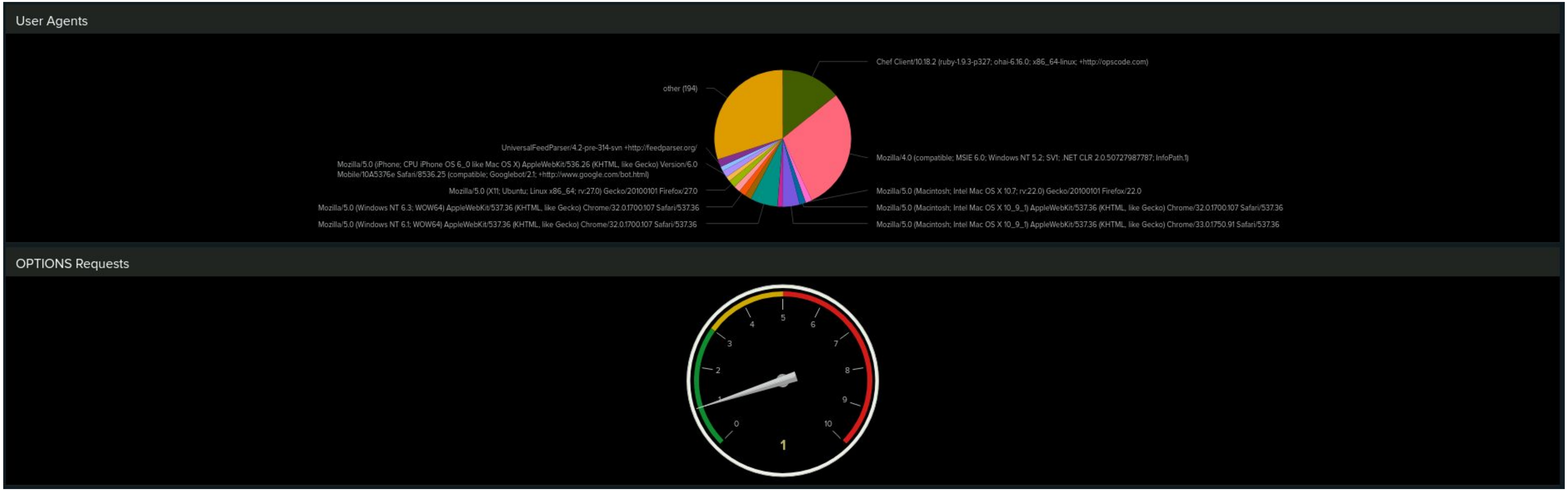


Client IP Locations

Screenshots of Attack Logs

Stats Count by URI
/?flav=rss20
other (603)
/VSI_Account_logon.php
/reset.css
/VSI_Company_Homepage.html
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/contactus.html
/images/VSI_headquarters.jpg
/files/logstash/logstash-1.3.2-monolithic.jar
Top 10 Countries
3,000
2,000
1,000
count
count
United States
Ukraine
Sweden
France
Germany
Spain
Canada
Italy
United Kingdom
Brazil
Country

Screenshots of Attack Logs


User Agents
other (194)
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:22.0) Gecko/20100101 Firefox/22.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
OPTIONS Requests
0
1
2
3
4
5
6
7
8
9
10
1

Attack Summary—Apache

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

- We detected sudden decreases in all of the activities within the referrer domains.
- We detected suspicious changes within the HTTP Response code as well; number of 200 responses greatly decrease, while number of 404 responses increased.
- Reports for methods, we found an increase count in HTTP POST that appeared suspicious with 1,296 events on March 25th, 2020 at 8PM.
- We detected suspicious volume of international activity with the highest count of 937 events on March 25th, 2020 at 8PM.

Attack Summary—Apache

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

On March 25, 2020, a suspicious volume of international activity and HTTP POST activity was detected. The count of international events was 937 at 8:00 PM, and the count of HTTP POST events was 1,296 at 8:00 PM. The alert threshold for international activity will not be changed, but the alert threshold for HTTP POST activity will be increased to 20 to avoid false alerts.

Recommendations:

Investigate the source of the suspicious international activity.

Monitor HTTP POST activity for further suspicious activity.

Additional Notes:

The suspicious activity may be the result of a coordinated attack.

The increased alert threshold for HTTP POST activity may result in some legitimate activity being missed.

Attack Summary—Apache

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

- Regarding the analysis for Cluster Map, we detected high volumes of activity from Ukraine. Further investigation leads to its city, Kiev, with the highest count of 439.
- Regarding the analysis for Time Chart of HTTP methods, we could see a rise in POST events from 7pm to 9pm with a peak of 1,296 events
- Regarding the analysis for URI data, we saw an unusually high percentage with VSI_Account_Logon.php which suggests a brute force attack

Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
  - VSI has experienced a series of attacks on its Windows and Apache servers. The attacks have involved spamming the servers with requests and using brute force methods to attempt to gain unauthorized access.
  - The reports that VSI had, helped to identify the attack patterns.
  - The alerts with optimal threshold did fire alerts to SOC.

- To protect VSI from future attacks, what future mitigations would you recommend?
  - Implement rate limiting: Rate limiting can be used to limit the number of requests that a single IP address can make to a server within a given time period. This can help to prevent attackers from flooding the server with requests.
  - Implement strong password policies: Strong password policies can help to prevent attackers from guessing user passwords. These policies should require users to create passwords that are at least 8 characters long and that contain a mix of upper and lowercase letters, numbers, and symbols.