



Defensive Security Project

by: Cookie Crumbles

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- ❖ We are playing the role of SOC analysts for Virtual Space Industries which designs VR Programs
- ❖ We are tasked with using Splunk to analyze and monitor VSI's environment as there are rumors that our competitor JobeCorp is planning to launch cyber attacks to disrupt business.
- ❖ We have been provided past logs of Apache and Windows Servers that we will use to form baselines, alerts, and reports.
- ❖ We will incorporate an add-on that will help us with monitoring the web application.

["Add-On" App]

Add-On App: Website Monitoring

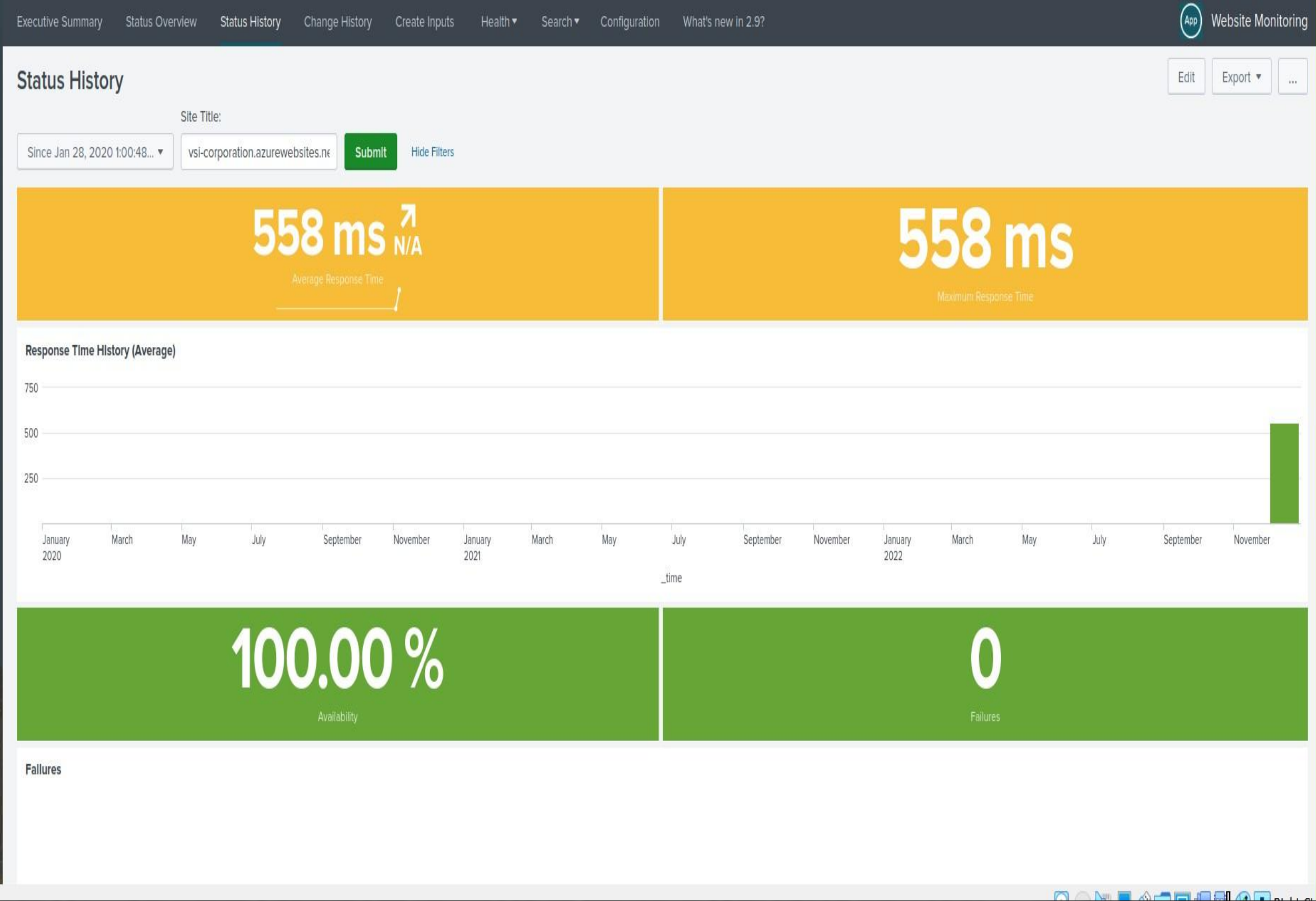
The Website Monitoring app is designed to detect downtime and performance issues. It provides information about past failures and calculates the website's uptime percentage. The app provides email alerts when the website is down or response times are too slow. It also provides response time for the website and gives historical analysis of the sites responsiveness

Add-On App: Website Monitoring

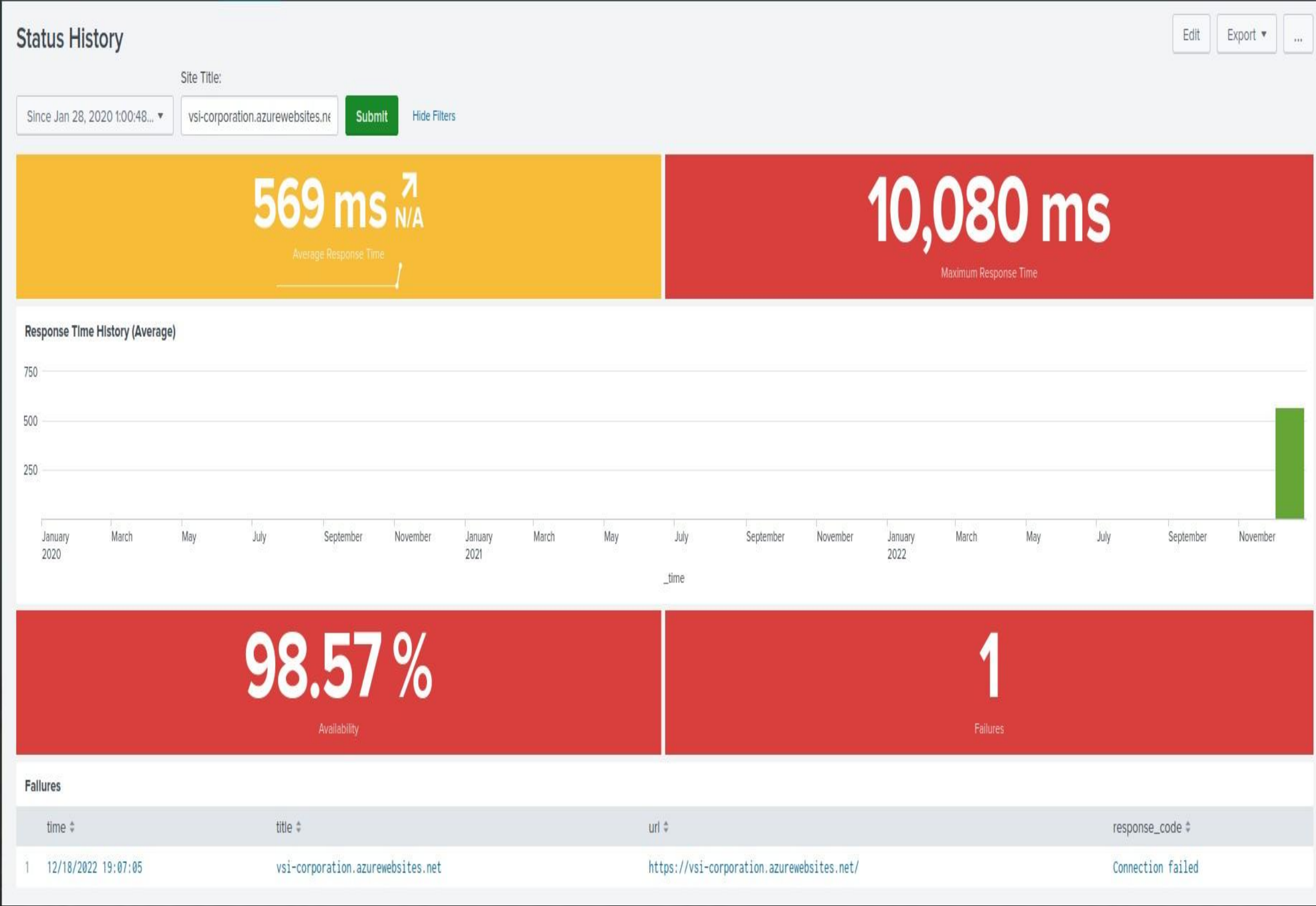
In a scenario in which there is a DDoS attack and the server stops responding or shuts down, the app will send email alerts and the issue can be addressed in a timely manner.

Add-On App: Website Monitoring

Before Attack



After Attack



Logs Analyzed

1

Windows Logs

Windows Server logs that were analyzed contained information about system events on the network:

- ❖ Successful logins and failed events.
- ❖ Creation and deletion of user accounts.
- ❖ Domain policy changes.
- ❖ Modifications to privileges.
- ❖ Severity of each event in the log

2

Apache Logs

Apache logs provided the following information about the web application:

- ❖ HTTP request methods.
- ❖ URI
- ❖ HTTP response types.
- ❖ IP Geolocation.
- ❖ HTTP status codes.
- ❖ Referrer Domains

Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Signature Report	This report displays the signature and the signature ID associated
Severity Report	Provides the severity of each event in the Windows logs
Failure Report	Compares the failure and success rate of windows activities

Images of Reports—Windows

20 per page ▾					
*	🕒 _time	📄 host	📄 signature	# signature_id	📄 source
1	2020-03-24T23:59:54.000Z	windows_server_logs.csv	A user account was deleted	4726	windows_server_logs.csv
2	2020-03-24T23:59:53.000Z	windows_server_logs.csv	A user account was created	4728	windows_server_logs.csv
3	2020-03-24T23:59:31.000Z	windows_server_logs.csv	A computer account was deleted	4743	windows_server_logs.csv
4	2020-03-24T23:57:54.000Z	windows_server_logs.csv	An account was successfully logged on	4624	windows_server_logs.csv
5	2020-03-24T23:57:51.000Z	windows_server_logs.csv	Special privileges assigned to new logon	4672	windows_server_logs.csv
6	2020-03-24T23:56:41.000Z	windows_server_logs.csv	An attempt was made to reset an accounts password	4724	windows_server_logs.csv
7	2020-03-24T23:56:40.000Z	windows_server_logs.csv	System security access was granted to an account	4717	windows_server_logs.csv
8	2020-03-24T23:54:46.000Z	windows_server_logs.csv	A privileged service was called	4673	windows_server_logs.csv
9	2020-03-24T23:54:42.000Z	windows_server_logs.csv	A logon was attempted using explicit credentials	4648	windows_server_logs.csv
10	2020-03-24T23:54:39.000Z	windows_server_logs.csv	A user account was locked out	4740	windows_server_logs.csv
11	2020-03-24T23:54:25.000Z	windows_server_logs.csv	Domain Policy was changed	4739	windows_server_logs.csv
12	2020-03-24T23:50:07.000Z	windows_server_logs.csv	A user account was changed	4738	windows_server_logs.csv
13	2020-03-24T23:48:36.000Z	windows_server_logs.csv	A process has exited	4689	windows_server_logs.csv
14	2020-03-24T23:46:27.000Z	windows_server_logs.csv	The audit log was cleared	1102	windows_server_logs.csv
15	2020-03-24T23:45:36.000Z	windows_server_logs.csv	System security access was removed from an account	4718	windows_server_logs.csv

localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search source%3D"windows_server_logs.csv"%20 | dedup signature signature_id&display.page.search.mode=verbose&dis

New Search

Save AsCreate Table ViewClose

source="windows_server_logs.csv" | dedup signature signature_id

All time

15 events (before 12/18/22 8:43:23.000 PM)No Event Sampling

Job

Verbose Mode

Events (15)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect

1 minute per column

4

3

2

1

11:45 PM
Tue Mar 24
2020

11:50 PM

11:55 PM

4

3

2

1

Show FieldsListFormat50 Per Page

i	Time	Event
>	3/24/20 11:59:54.000 PM	<div>2020-03-24T23:59:54.000+0000,, "Domain_A Domain_A",, "user_f user_l",,,,,,,,,,Account Management,,,,,,,,,ACME-002,,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_f Show all 63 lines host = windows_server_logs.csv source = windows_server_logs.csv sourcetype = windows_server_logs.csv</div>
>	3/24/20 11:59:53.000 PM	<div>2020-03-24T23:59:53.000+0000,, "Domain_A Domain_A",2020-03-24 23:59:53 PM, "user_k user_m",,,,server_2/computer_b,,,,,,,,,Account Management,,,,,,,,,ACME-002,,,aaa,,,,,,,,,-,4720,A user account was created,0,,,,,,\a\g,A:,,,,,Audit Success,,,,,Security,,,,,All,0xBAC3,,,,"SAM Account Name: user_h Display Name: aaa User Principal Name: ddd@BBB.local Show all 137 lines host = windows_server_logs.csv source = windows_server_logs.csv sourcetype = windows_server_logs.csv</div>
>	3/24/20 11:59:31.000 PM	<div>2020-03-24T23:59:31.000+0000,, "Domain_A Domain_A",, "user_l user_e",,,,,,,,,,Account Management,,,,,,,,,ACME-002,,,,,,,,,-,4743,A computer account was deleted,0,,,,,,,,,Audit Success,,,,,Security,,,,,0xAB37,,,,,,,,,"A computer account was deleted. Subject:</div>

13

Create Table View

Cancel

source="windows_server_logs.csv" host="windows_server_logs.csv" sourcetype="windows_server_logs.csv" severity="*" | top limit=20 severity



Select existing fields

Filter existing fields



+ Add a missing existing field

- ✓ all fields
- ✓ count
- ✓ percent
- ✓ severity




✓ Previewing 4,764 events (1/28/20 1:00:48.000 PM to 12/15/22 1:02:47.000 AM) Event Limiting: ~100,000 ▼

*	# count	# percent	a severity
1	4435	93.094039	informational
2	329	6.905961	high

Done

Create Table View

Save

History	SPL		Edit ▾	Sort ▾	Filter ▾	Clean ▾	Summarize ▾	Add New ▾	 Rows	 Summary
✓ Previewing 4,764 events (1/28/20 1:00:48.000 PM to 12/15/22 1:09:11.000 AM) Event Limiting: ~100,000 ▾										
	*	# count	# percent	a status						
1	4622	97.019312	success							
2	142	2.980688	failure							

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Events	Alert notifies SOC of failed events that exceed threshold within 1 hour period.	12 events	20 events

JUSTIFICATION: When reviewing the logs for failed login attempts the average number of unsuccessful logins was 12. We set the threshold at 20 events because it was noted as the high for the day but was not considered suspicious activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins - 4624	Alert SOC when login attempts exceed 25 per hour	24	25

When reviewing the logs for successful login attempts the average number of unsuccessful logins was 24. We set the threshold at 25 events because it was noted as the high for the day but was not considered suspicious activity.

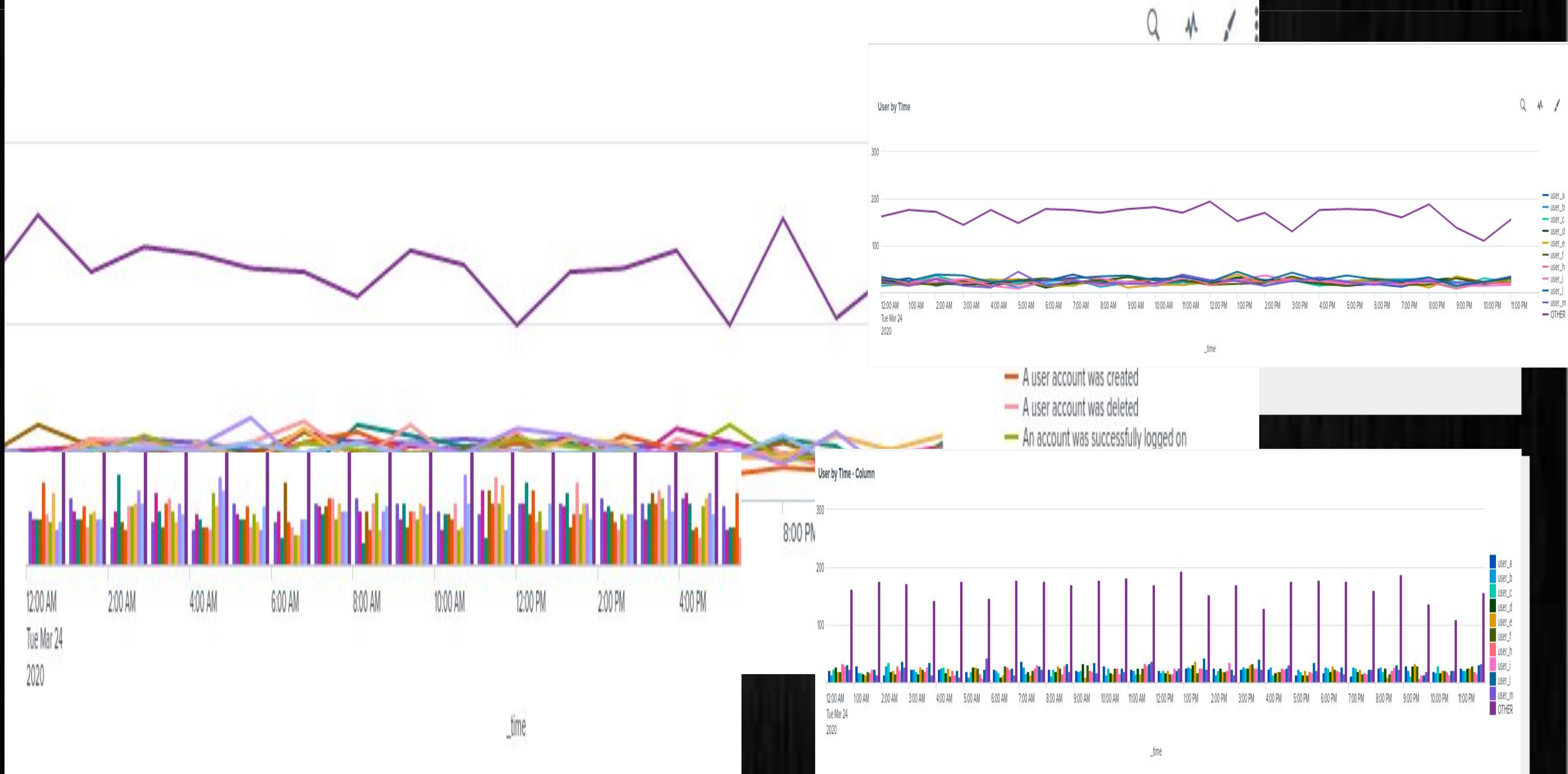
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Accounts Deleted - 4726	Alert when attempts to delete a user account exceeds 19	17	22

JUSTIFICATION: In the event captured the baseline was between 17-19 attempts to delete a user account. 22 was chosen as the threshold because it seems as though this is a small deviation from the norm. Anything above 22 would be flagged as suspicious behavior.

D



Apache Logs

https://docs.google.com/presentation/d/1lKn9nynttrfn1RZuLI-DfBSbsaSDVcfa04dZ3_jB6ZTeU/edit?usp=sharing

Designed the following reports:

Report Name	Report Description
HTTP requests by method	Parses the HTTP requests and counts of each request.
Top 10 URI	Displays info about the top 10 domains that refer to VSI's website
HTTP response code	Displays type and count of HTTP response code

Images of Reports—Apache

source="apache_logs.txt" | stats count by method

Select existing fields

Filter existing fields

+ Add a missing existing field

✓ all fields

✓ count

✓ method

✓ Previewing 20,000 events (1/28/20 1:00:48.000 PM to 12/19/22 10:37:13.000 PM)

Event Limiting: ~100,000

*	a count	a method
1	19702	GET
2	84	HEAD
3	2	OPTIONS
4	212	POST

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

Select existing fields

Filter existing fields

+ Add a missing existing field

✓ all fields

✓ count

✓ percent

✓ referer_domain

✓ Previewing 20,000 events (1/28/20 1:00:48.000 PM to 12/19/22 8:53:49.000 PM)

Event Limiting: ~100,000

*	# count	# percent	a referer_domain
1	6076	51.256960	http://www.semicomplete.com
2	4002	33.760756	http://semicomplete.com
3	246	2.075249	http://www.google.com
4	210	1.771554	https://www.google.com
5	68	0.573646	http://stackoverflow.com
6	62	0.523030	http://www.google.fr
7	58	0.489286	http://s-chassis.co.nz
8	56	0.472414	http://logstash.net
9	50	0.421799	http://www.google.es
10	46	0.388055	https://www.google.co.uk

http response table view

All time

✓ 10,000 events (before 12/16/22 12:42:42.000 AM)

20 per page

Job

Rows

Summary

1

2

3

4

5

6

7

8

Next

*	@_time	a host	a source	a sourcetype	# status
1	2020-03-20T21:05:59.000Z	Apache_logs	apache_logs.txt	access_combined	200
2	2020-03-20T21:05:59.000Z	Apache_logs	apache_logs.txt	access_combined	200
3	2020-03-20T21:05:58.000Z	Apache_logs	apache_logs.txt	access_combined	200
4	2020-03-20T21:05:57.000Z	Apache_logs	apache_logs.txt	access_combined	200
5	2020-03-20T21:05:57.000Z	Apache_logs	apache_logs.txt	access_combined	200
6	2020-03-20T21:05:56.000Z	Apache_logs	apache_logs.txt	access_combined	200
7	2020-03-20T21:05:55.000Z	Apache_logs	apache_logs.txt	access_combined	200
8	2020-03-20T21:05:55.000Z	Apache_logs	apache_logs.txt	access_combined	200
9	2020-03-20T21:05:55.000Z	Apache_logs	apache_logs.txt	access_combined	200
10	2020-03-20T21:05:54.000Z	Apache_logs	apache_logs.txt	access_combined	200
11	2020-03-20T21:05:53.000Z	Apache_logs	apache_logs.txt	access_combined	200
12	2020-03-20T21:05:53.000Z	Apache_logs	apache_logs.txt	access_combined	200
13	2020-03-20T21:05:53.000Z	Apache_logs	apache_logs.txt	access_combined	200
14	2020-03-20T21:05:52.000Z	Apache_logs	apache_logs.txt	access_combined	200
15	2020-03-20T21:05:50.000Z	Apache_logs	apache_logs.txt	access_combined	200

Create Table View

History

SPL

Edit

Sort

Filter

Clean

Summarize

Add New

Selected Data

✓ Previewing 20,000 events (1/28/20 1:00:48.000 PM to 12/19/22 8:53:47.000 PM)

Event Limiting: ~100,000

*	# count	# percent	a referer_domain	a uri
1	1614	8.070000	null	/VSI_Company_Homepage.html
2	1092	5.460000	null	/contactus.html
3	1076	5.380000	null	/reset.css
4	1066	5.330000	null	/images/VSI_headquarters.jpg
5	1032	5.160000	null	/images/web/2009/banner.png
6	976	4.880000	null	/blog/tags/puppet?flav=rss20
7	448	2.240000	null	/projects/xdotool/
8	434	2.170000	null	?flav=rss20
9	394	1.970000	null	/
10	360	1.800000	null	/robots.txt

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Country outside of US	Send an alert if access exceeds 10 events.	8	11

JUSTIFICATION: When reviewing the logs for access outside the US the number of events was between 6 and 9 for a normal day. We set the threshold at 11 events because anything outside of that would could be considered suspicious activity.

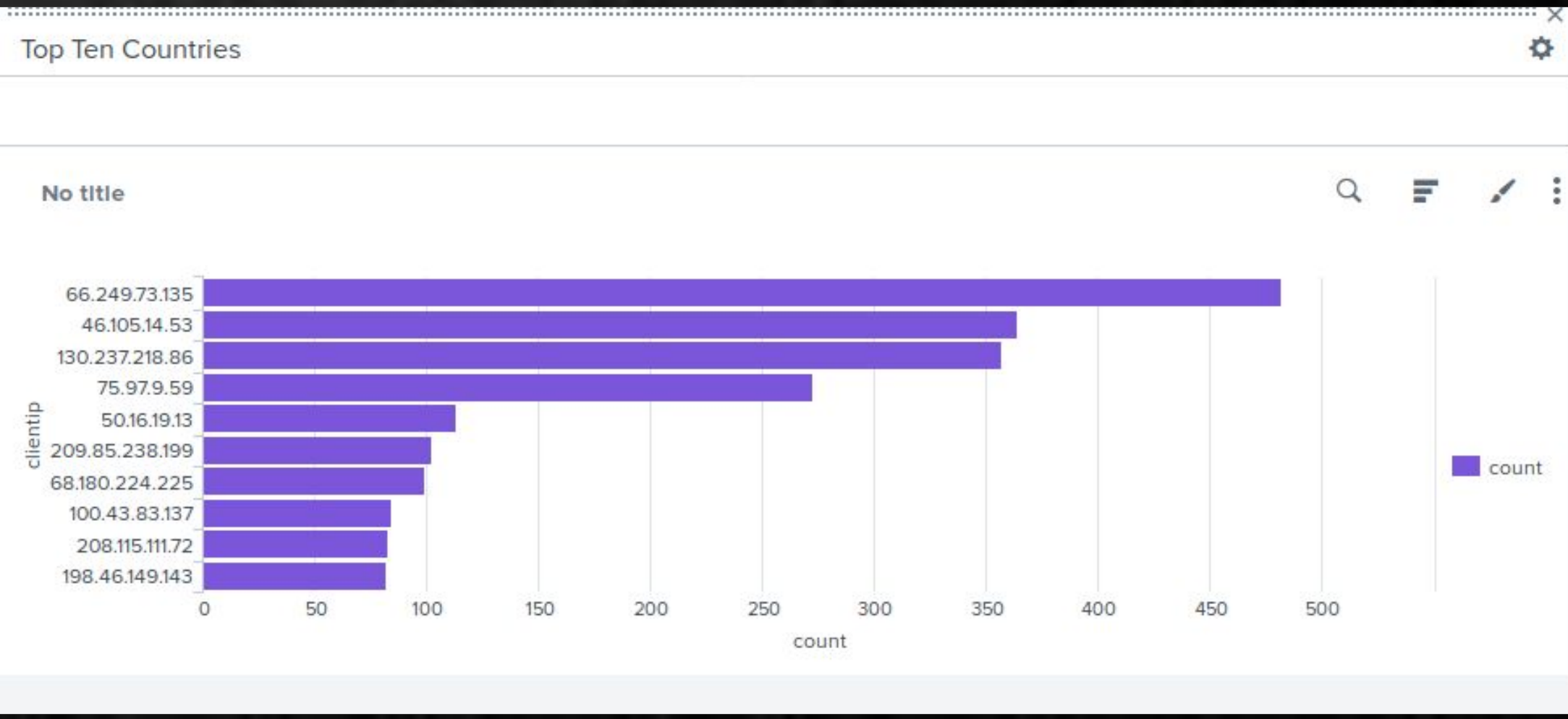
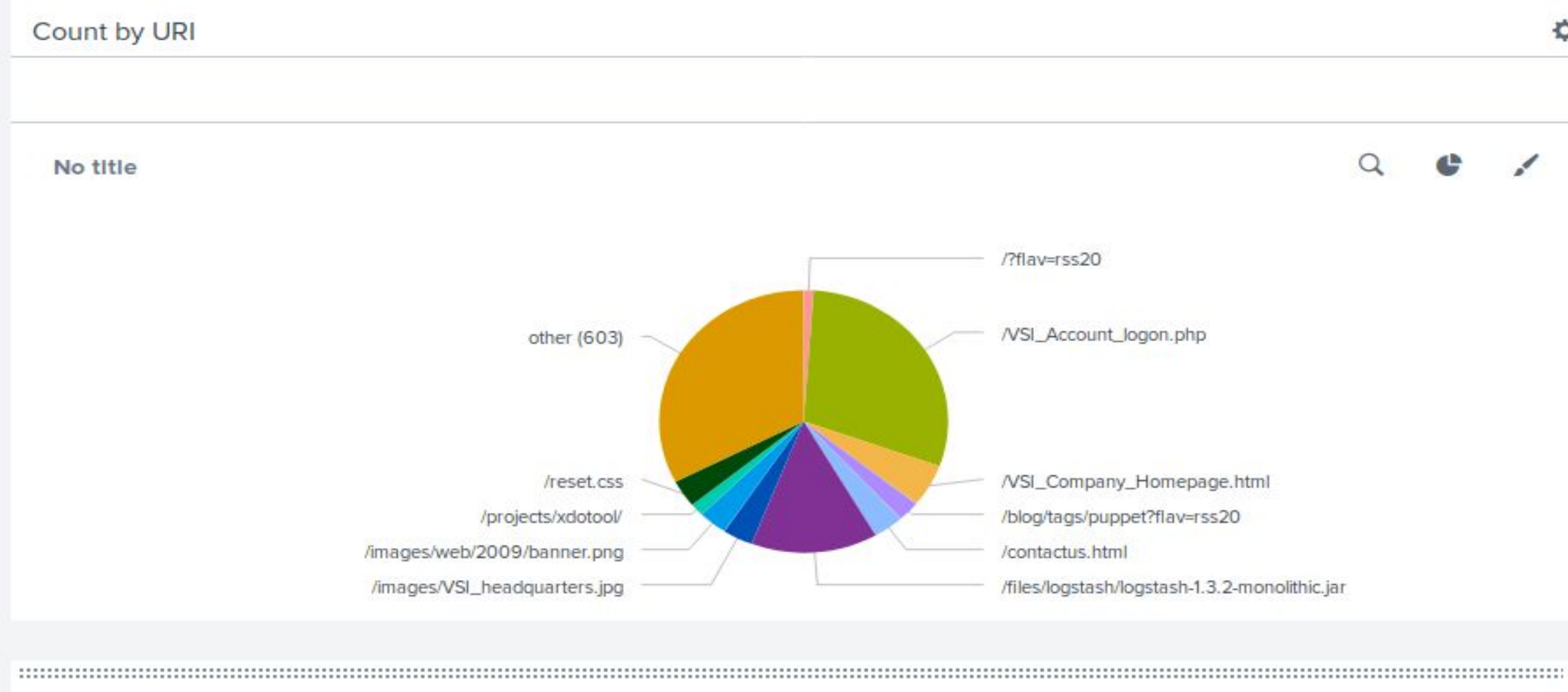
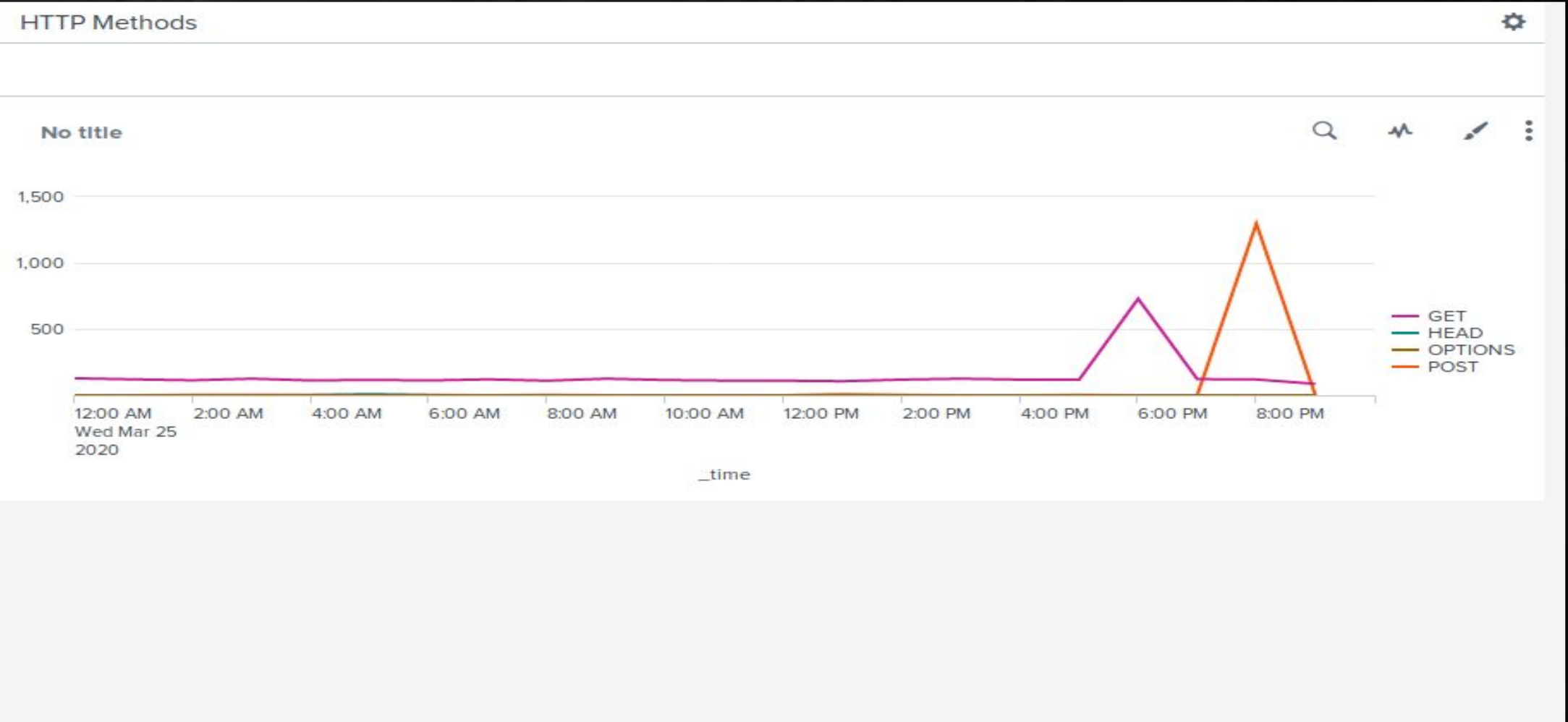
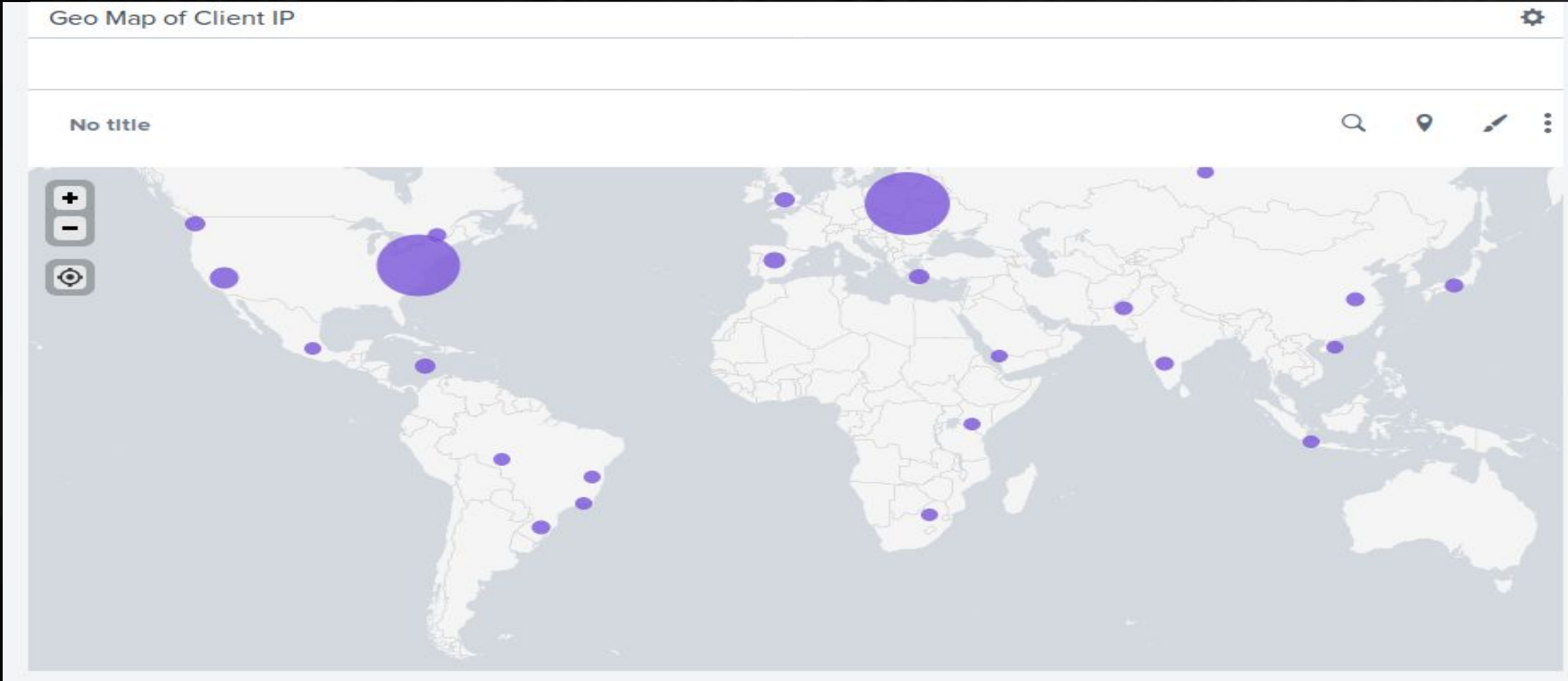
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Method	Send an alert if POST request exceed 6	4	6

JUSTIFICATION: When reviewing the logs for POST request the number of request was between 1-3 for a normal event with random outliers of 7 and 8. We set the threshold at 6 events because anything higher would be considered suspicious activity.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

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

- ❖ While analyzing the attack logs, we noticed a spike of volume of activity from Signature values at 12:00 AM to 3:00 AM and 8:00 AM to 11:00 AM
- ❖ High Severity Levels increased from 7% before the attack to 20% after
- ❖ There was no suspicious activity from the success and failure of Windows activities report.

Attack Summary—Windows

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

- ❖ The successful login, failed events, and deleted account alerts would have been emailed out as all thresholds were exceeded during these attacks.
- ❖ We may consider raising thresholds as volume greatly exceeded each alert.

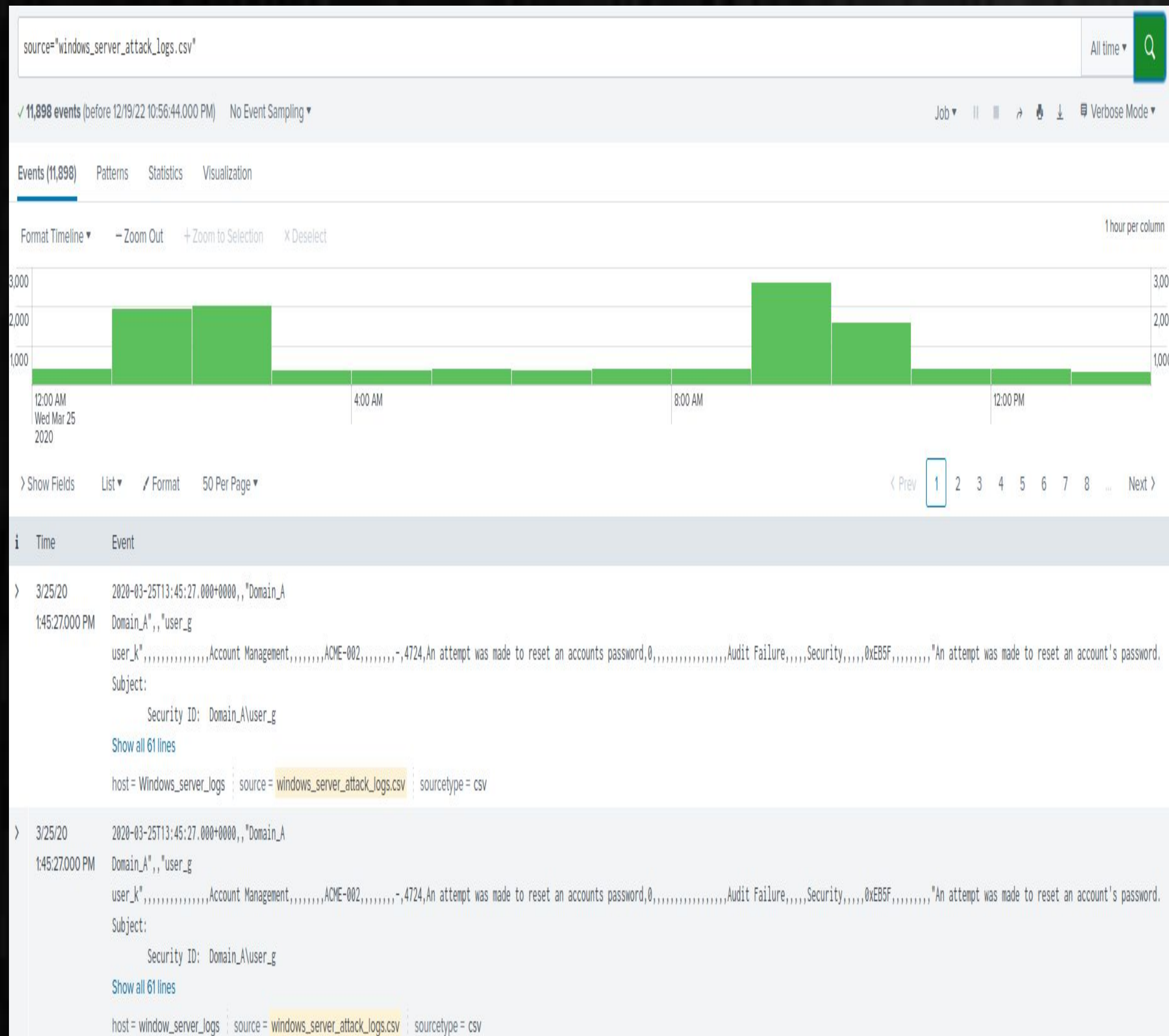
Attack Summary—Windows

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

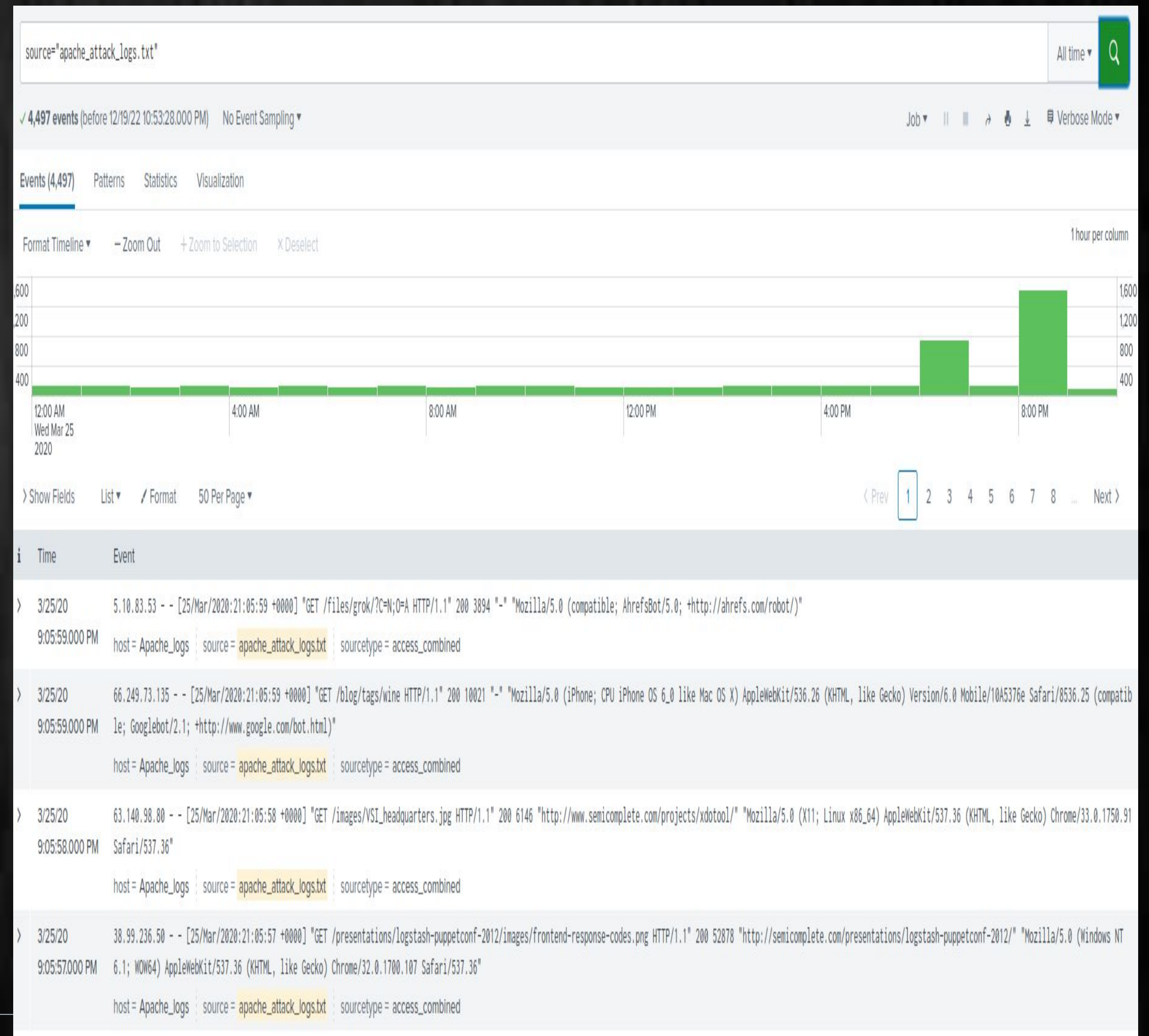
- ❖ While no signature value stood out before the attack, there were 896 instances of a user being locked out from 12:00 AM to 3:00 AM and 1258 instances of a password being reset from 8:00 AM to 11:00 AM.
- ❖ Similar to the signature values no users stood out before the attack. User_a and user_k volume increased to 984 and 1256 during the previously mentioned times.
- ❖ The count of users showed an increase from 260-280 for users A and K to 1800-2100.

Screenshots of Attack Logs

Windows Attack Logs



Apache Attack Logs



Attack Summary—Apache

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

- ❖ The HTTP Method report showed a spike in volume for GET method between 5:00 PM and 7:00 PM and POST method between 7:00 PM and 9:00 PM
- ❖ While the US remained over half of the Top 10 countries, Ukraine increased to almost 25% of total users
- ❖ The amount of 404 error messages increased from 2% of all HTTP Response codes to 15%.

Attack Summary—Apache

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

- ❖ The Activity from other countries and HTTP POST method count alerts would have been emailed out as all thresholds were exceeded during these attacks.
- ❖ We may consider raising thresholds as volume greatly exceeded each alert.

Attack Summary—Apache

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

- ❖ While analyzing the attack logs, we noticed a spike in volume of activity from 5:00 PM to 9:00 PM
- ❖ Most of the volume came on the VSI_Account_logon.php page with the POST HTTP method
- ❖ The ClientIP Map lead us to believe we were under a brute force attack from a visitor in another country.

Summary and Future Mitigations

Project 3 Summary

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

- ❖ On or about March 25, 2020 , there were an excessive amount of login attempts, specifically from the Country of Ukraine. Upon further investigation it was determined that there were several successful login attempts as well as some new accounts created, deletion of accounts, and attempted password resets. The Windows server experienced zero activity between the hours of 9 am and 11 am. The excessive amount of GET request in such a short time span would indicate a DDoS attack. The hardest hit URI was VSI_Account_Login.php.

Project 3 Summary

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

- ❖ To protect from future attacks, VSI should implement 2-Factor Authentication. In the event of a successful login, a second form of authentication is still required. It may be helpful to install an IPS to assist in notifying in real time so that events are mitigated faster.