Defensive Security Project

By: Room 2,

Fahim Adil
Sam Corn
Sid Choudhuri
Kyra Chow
Melody Galloro
Amanullah Haidary
Hossainul Islam
Justin Legendre
Fatima Mansoor
Ryan Morgen
Daniel Nguyen
Tim Pang
Avram Sachinidis
Gerald Sequeira

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Our employer tasked us with creating a monitoring solution to help protect their Windows and Apache servers against a malicious competitor.
- We were provided with logs of regular activity (which is not typical in the real world).
- We used this crucial information to devise baseline thresholds of suspicious activity within Splunk Enterprise with reports and alerts.
- These alerts are just that; they will notify security personnel of atypical activity but will ***not*** mitigate anything.
- Additionally we created dashboards to quickly and efficiently display data in a streamlined panel of graphs.
- We additionally used **Whois XML IP Geolocation API addon for Splunk to pinpoint physical IP locations.**

Website Monitoring

Website Monitoring

Summary:

Website monitoring apps can be a valuable tool for website owners and administrators, providing real-time monitoring and alerts to help quickly identify and resolve any issues that may arise. This app uses a modular input that can be set up quickly (in 5 minutes or less).

Features:

- **Uptime monitoring:** This feature tracks the website's availability and alerts the user when the website goes down or becomes unavailable.
- **Performance monitoring:** This feature tracks the website's performance, including load times, response times, and server resource usage, and alerts the user when performance falls below a certain threshold.
- **Error rate monitoring:** This feature tracks the number of errors and 404 pages encountered by users, helping to identify and troubleshoot issues with the website.

Website Monitoring

- **Alert notifications:** This feature provides alerts via email, SMS, push notifications, or other channels when the website experiences an issue or goes down.

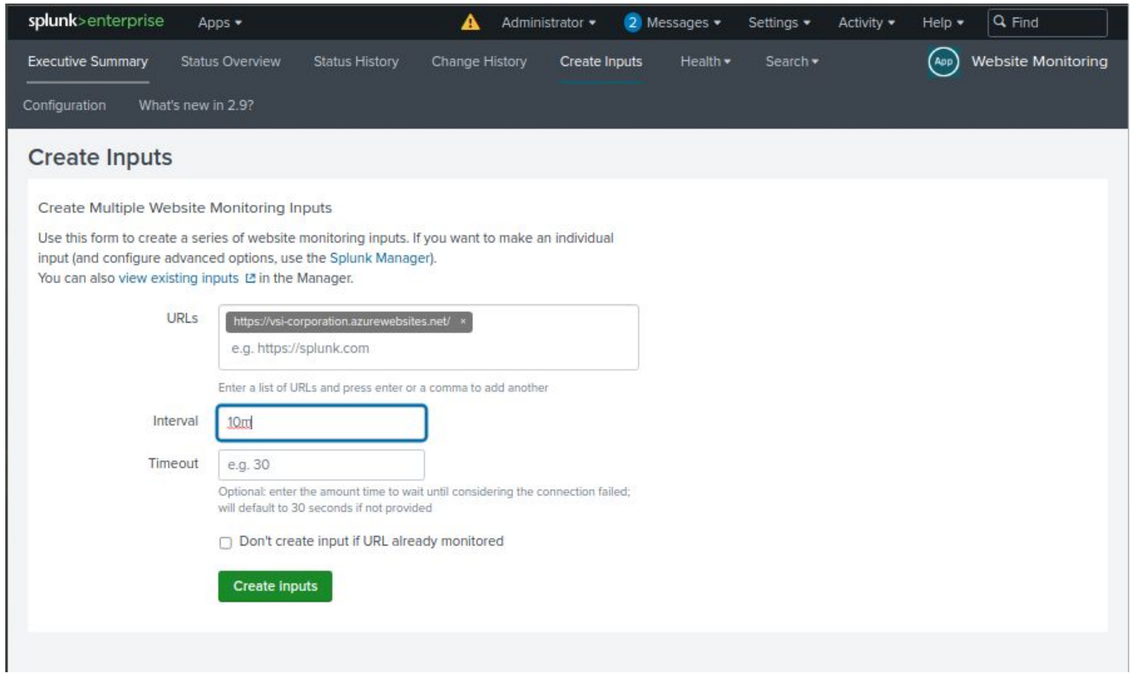
- **Historical data tracking:** This feature provides data on website performance and uptime over time, allowing users to track trends and identify potential issues before they become critical.

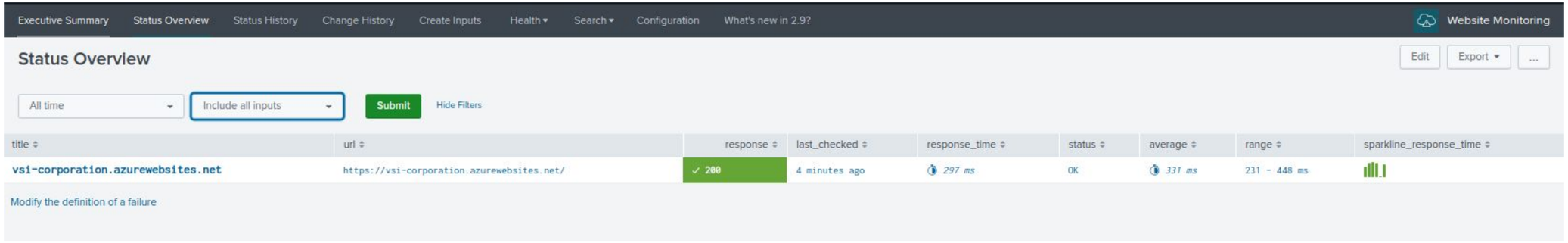
- **Multiple monitoring locations:** This feature allows the user to monitor the accessing website from various locations worldwide, providing a more accurate picture of website performance and availability.

- **Integration with other tools**: Many website monitoring apps integrate with other tools, such as analytics platforms or incident management systems, to provide a more comprehensive view of website performance and streamline the incident resolution process.

These are just a few of the standard features of website monitoring apps. Depending on the user's needs, different apps may provide additional or variations on these core features. Therefore, considering various options and choosing a website monitoring app that provides the features and resources that meet your specific needs is essential.

Website Monitoring





Logs Analyzed

1 Windows Logs

- Windows event changes
  - Account Deleted
  - Account Login Successful
  - Account password reset
- Status logs of success or failures
- List of users who logged on
- Severity/Event status

2 Apache Logs

- Different Logins from different domain locations
- Different HTTP methods/requests to obtain information
- Status of the website
- Different ip addresses that requested

Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Windows Events Signatures	A report with a table of signatures and associated signature IDs.
Windows Events Severity	A report that displays the severity levels, and the count and percentage of each.
Windows Events Status	A report that provides a comparison between the success and failure of Windows activities.

Images of Reports—Windows

Windows Event Signatures

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **4,764 events** (before 2/15/23 12:41:03.000 AM)

Job ▾

15 results 20 per page ▾

signature	signature_id
A computer account was deleted	4743
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A user account was deleted	4726
An attempt was made to reset an accounts password	4724
A user account was created	4720
System security access was removed from an account	4718
System security access was granted to an account	4717
A process has exited	4689
A privileged service was called	4673
Special privileges assigned to new logon	4672
A logon was attempted using explicit credentials	4648
An account was successfully logged on	4624
The audit log was cleared	1102
	100%

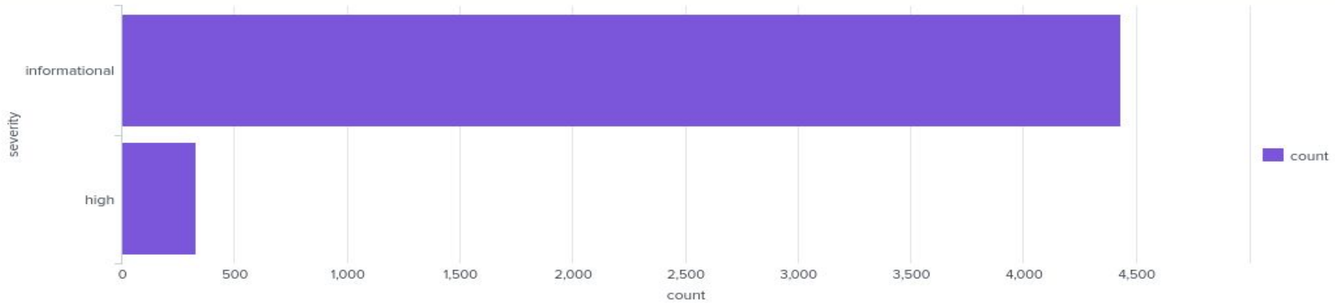
Windows Events Severity

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **4,764 events** (before 2/15/23 12:44:50.000 AM)

Job ▾



2 results 20 per page ▾

severity	count	percent
informational	4435	93.094039
high	329	6.905961
	4764	100
	97.9%	2.1%

Windows Events Status

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **4,764 events** (before 2/15/23 12:54:15.000 AM)

Job ▾

2 results 20 per page ▾

status	count	percent
success	4622	97.019312
failure	142	2.980688
	4764	100
	97.9%	2.1%

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Events Alerts - Failure	Windows failure status threshold = 20 per hour	Min = 2 Max = 10	Threshold = 20

JUSTIFICATION:The max baseline failure rate per hour is 10. I chose a threshold double this value to avoid false positives.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Events Alerts - Successfully logged in	Windows failure status threshold = Greater than 35 per hour	Min = 8 Max = 21	Threshold = 35

JUSTIFICATION: The max baseline failure rate per hour is 21. I chose a threshold of 35, close to double the failure rate, to avoid false positives.

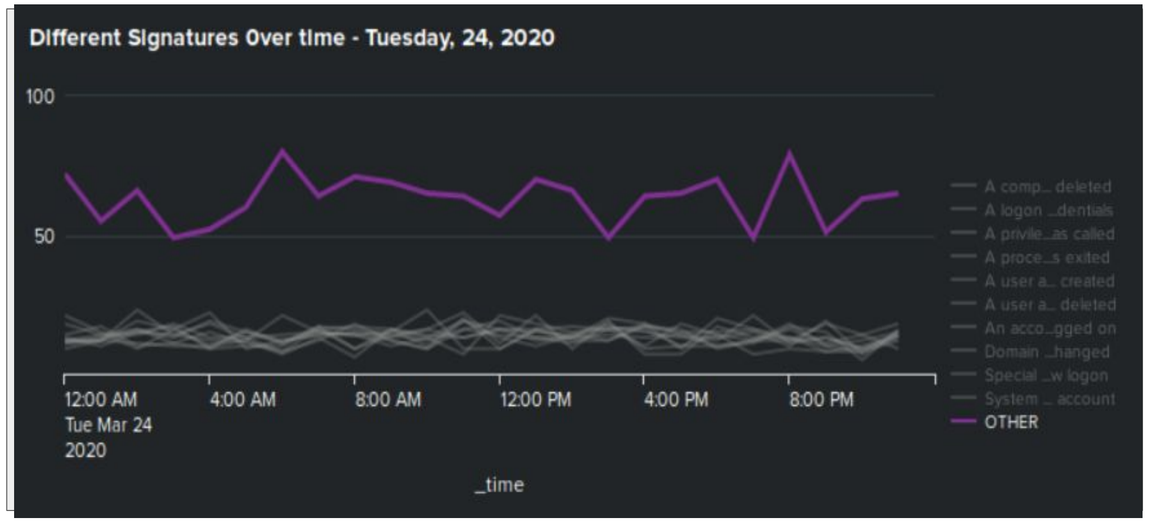
Alerts—Windows

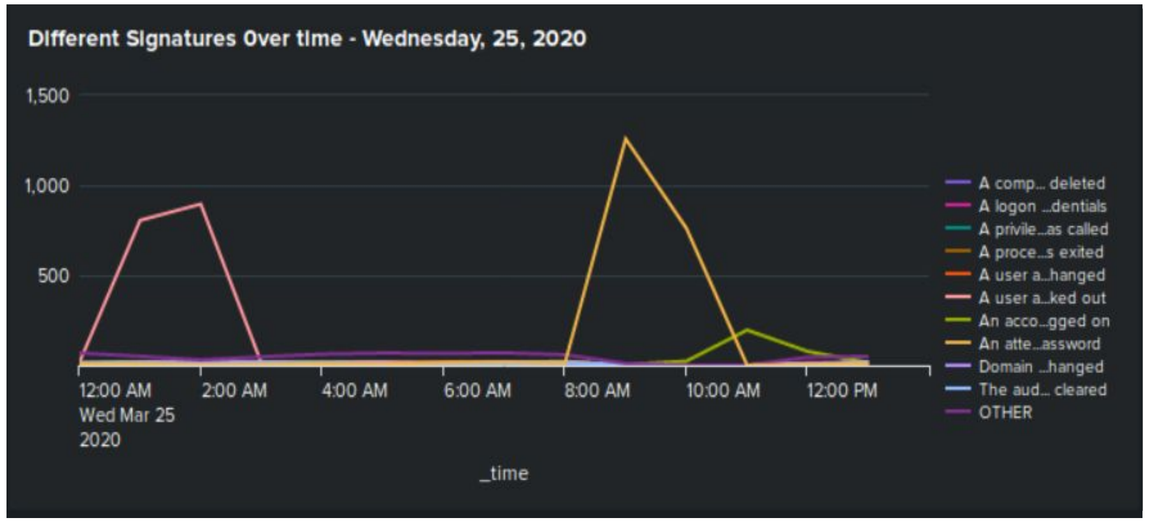
Designed the following alerts:

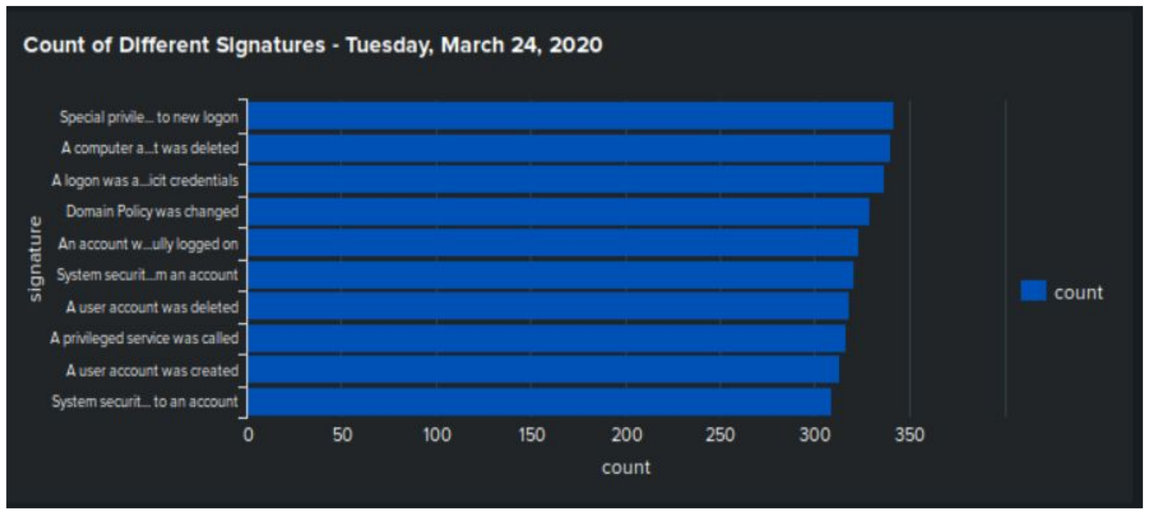
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Events Alerts - Deleted Accounts	Deleted accounts greater than 30 per hour	Min = 7 Max = 22	Threshold = 30

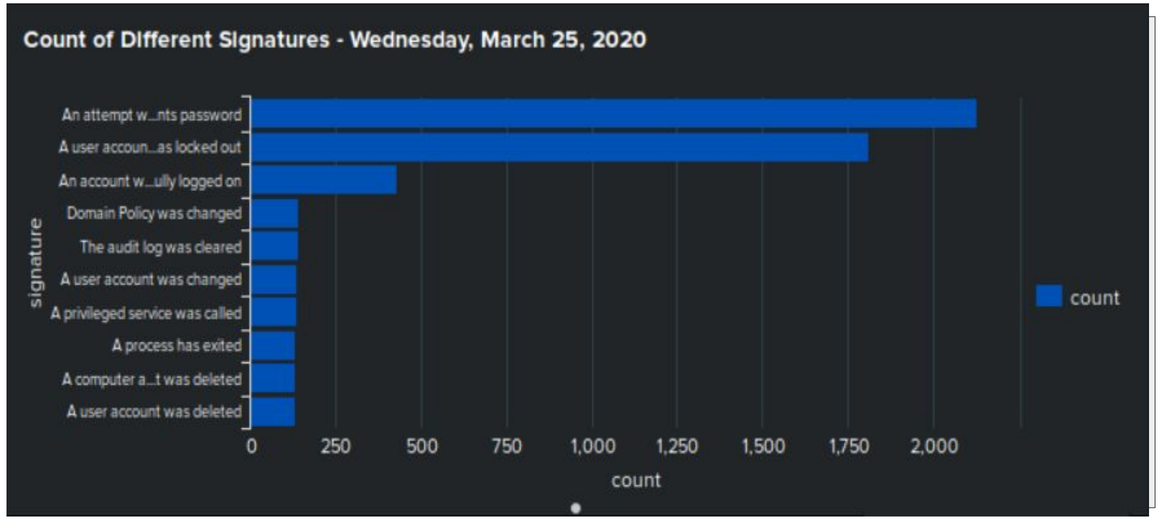
JUSTIFICATION: The max baseline failure rate per hour is 22. I chose a threshold of 30 because account deletion should occur closer to the baseline than double the maximum threshold.

Dashboards—Windows

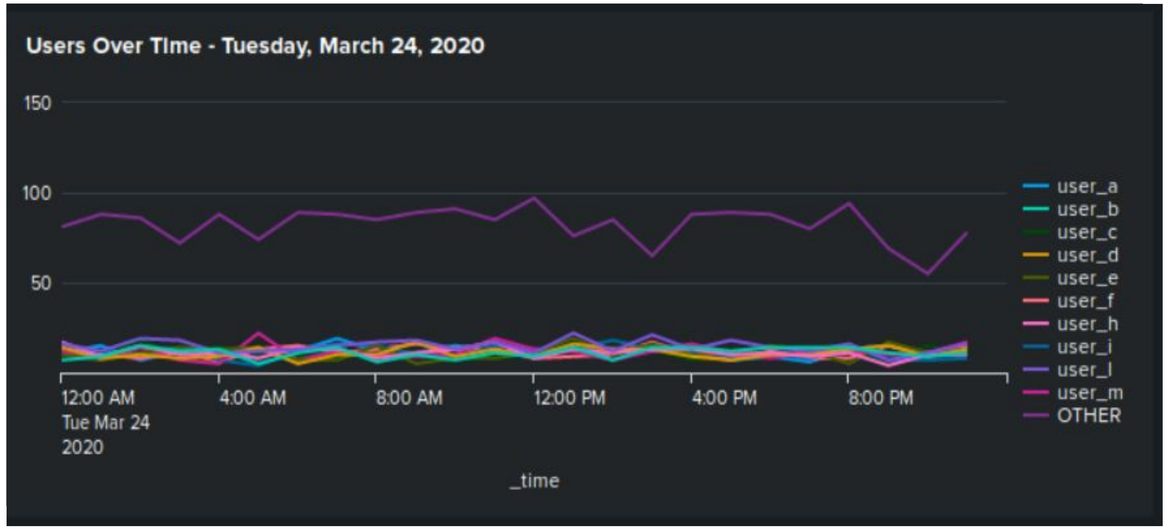


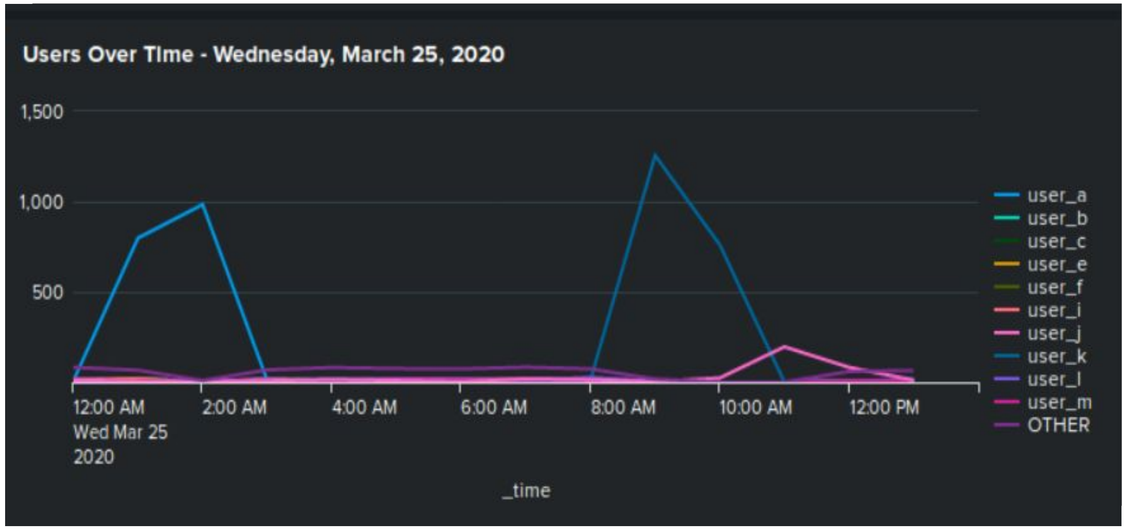


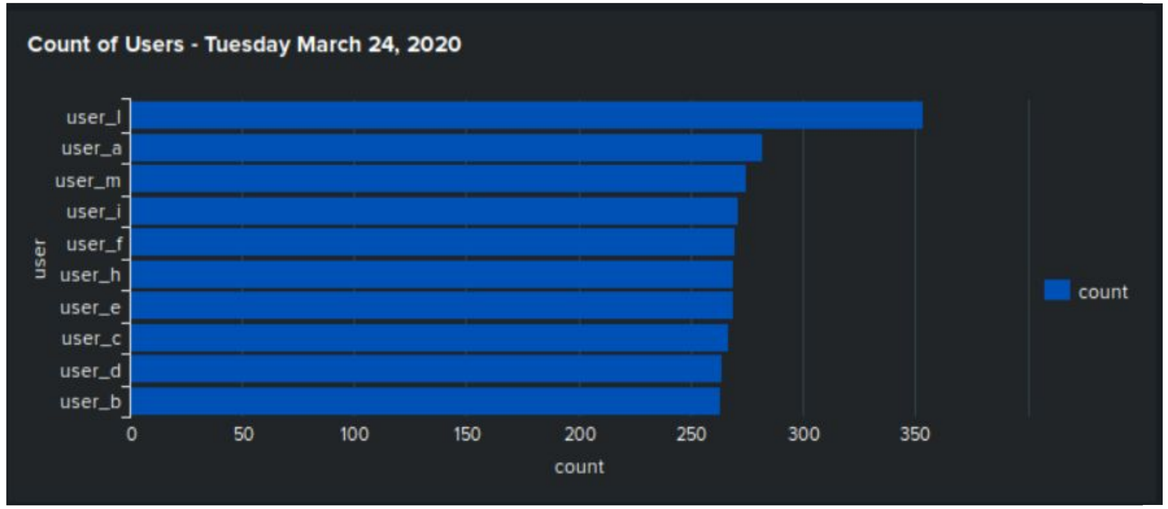


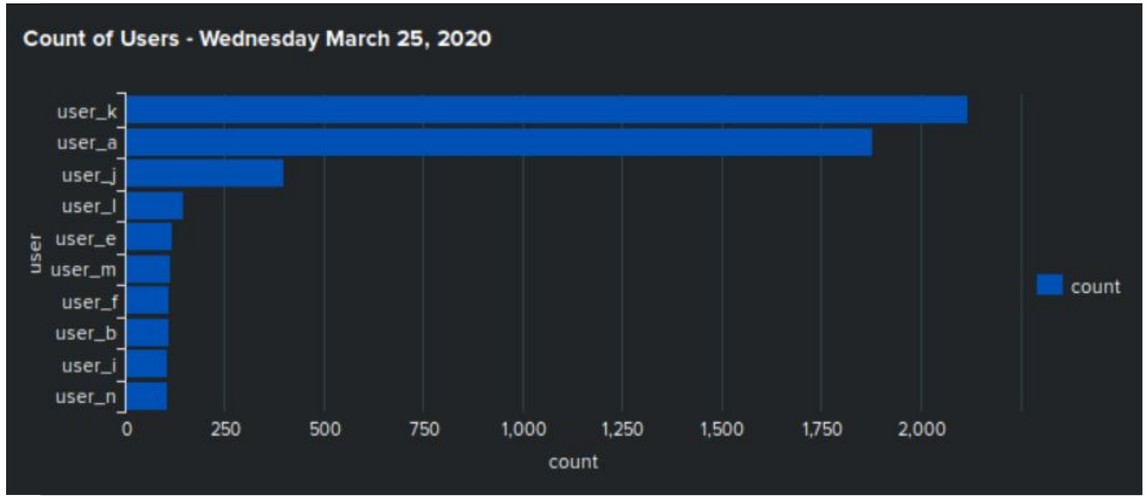


Dashboards—Windows









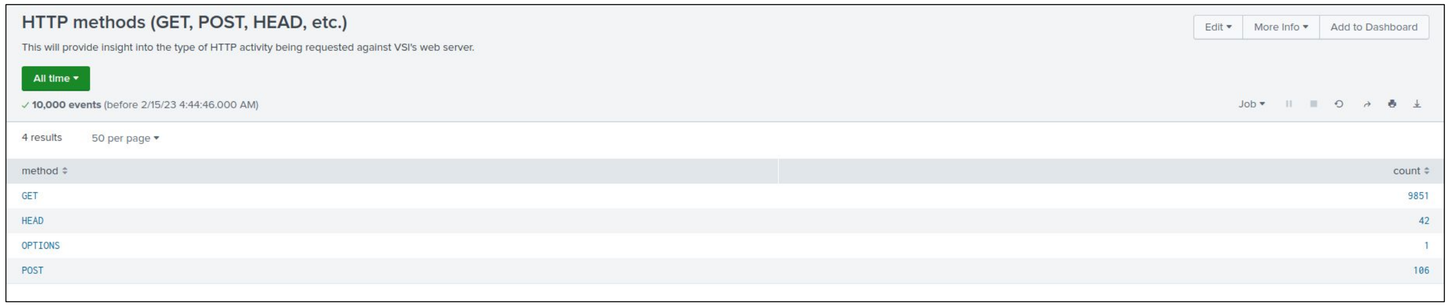
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods TABLE	HTTP activity status count of the type of GET, POST, HEAD and OPTIONS activity being requested against the VSI web server.
Top 10 VSI Domain Referrers	A list of the top 10 referring domains to identify any suspicious referring sites to VSI's websites.
HTTP Response Codes	A report showing the count of each HTTP response code to provide insight into any suspicious levels of HTTP responses.

Images of Reports—Apache



HTTP methods (GET, POST, HEAD, etc.)

This will provide insight into the type of HTTP activity being requested against VSI's web server.

Edit | More Info | Add to Dashboard

All time

✓ 10,000 events (before 2/15/23 4:44:46.000 AM)

Job

4 results 50 per page

method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106

Top 10 domains that refer to VSI's website

This will provide insight into the type of HTTP activity being requested against VSI's web server.

Edit | More Info | Add to Dashboard

All time

✓ 10,000 events (before 2/15/23 4:48:51.000 AM)

Job

10 results 50 per page

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 code

shows the count of each HTTP response code.

Edit | More Info | Add to Dashboard

All time

✓ 10,000 events (before 2/15/23 5:20:45.000 AM)

Job

8 results 50 per page

status	count
200	9126
206	45
301	164
304	445
403	2
404	213
416	2
500	3

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Country Activity	Threshold from countries not including the US	125	150

JUSTIFICATION: The average hourly activity from other countries is roughly 125. this was found by taking the lowest and highest hourly activity and averaging them. We set our threshold at 150, to allow room for company growth and to not have alert fatigue. If attacks like a DDoS were to take place it would go well over the alert threshold.

Alerts—Apache

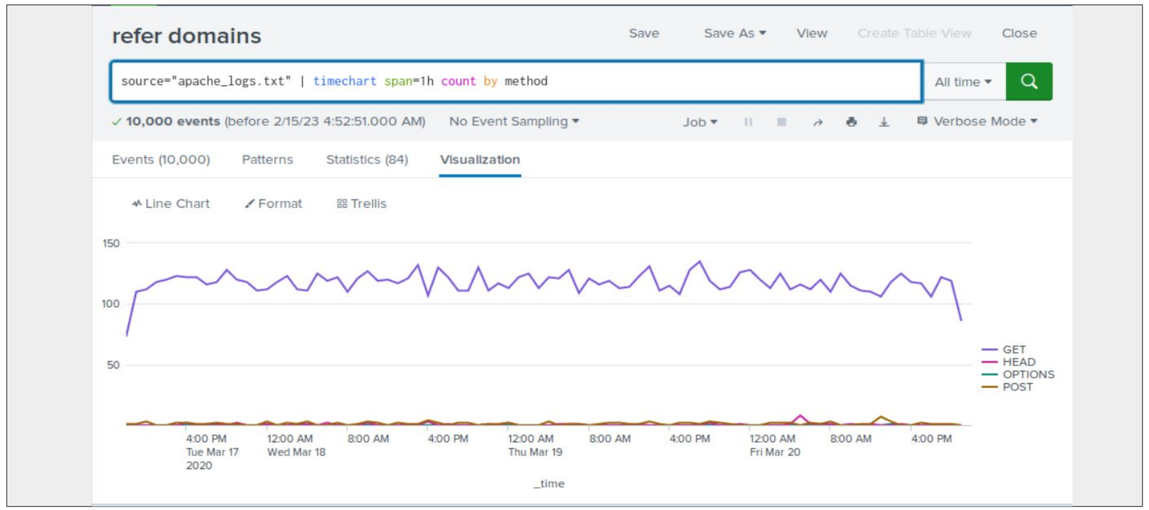
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST ALERT	HTTP POST Threshold >10 per hour	5	10

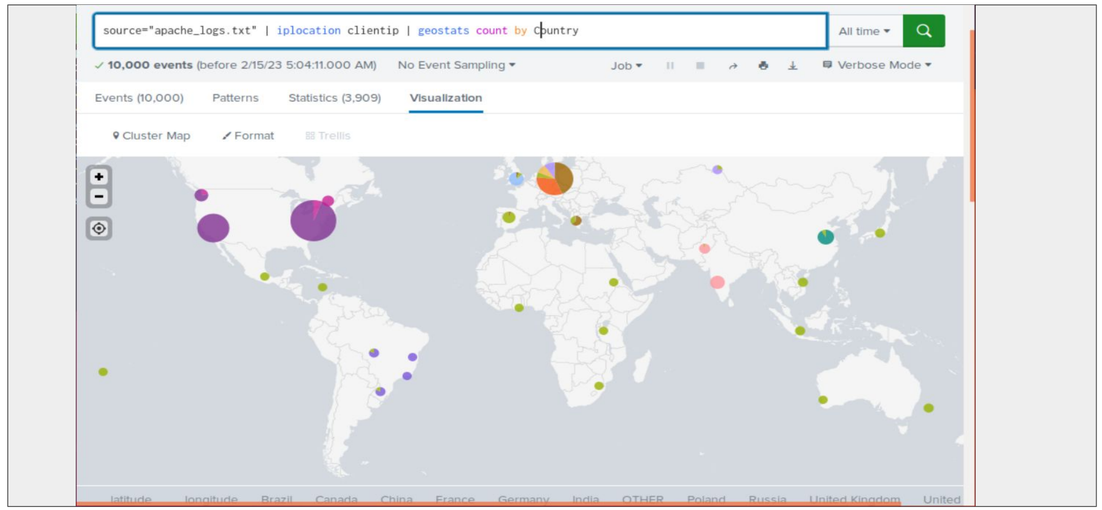
JUSTIFICATION: Since POST's per hour on an average day, can be as low as 0, or as high as 7. we can see an average baseline of roughly 4-5. having the Alert threshold at 10 will allow for those peaks of 7, and alert us if something unexpected could be going on.

Dashboards—Apache

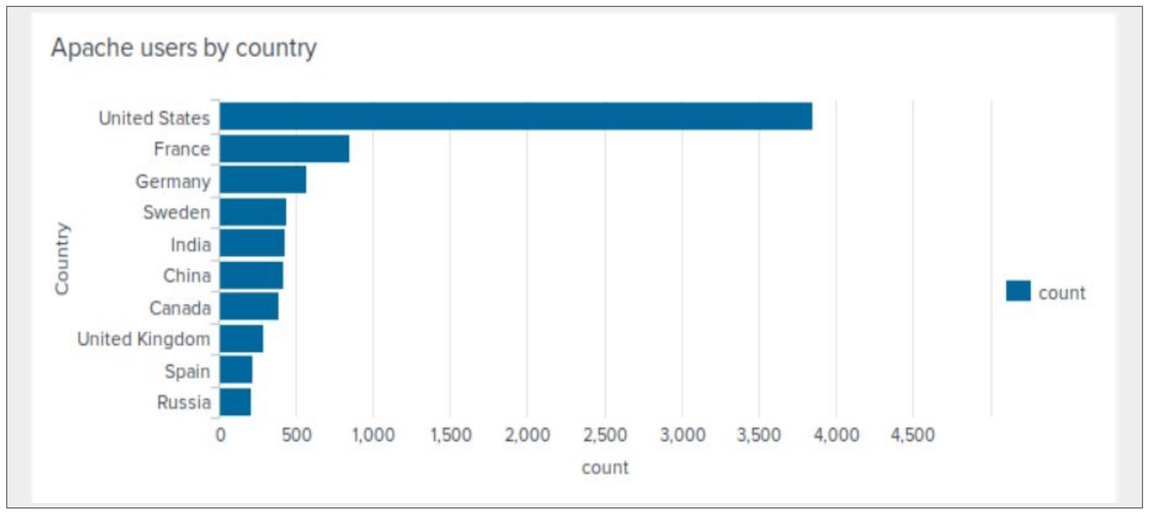
HTTP methods field values over time



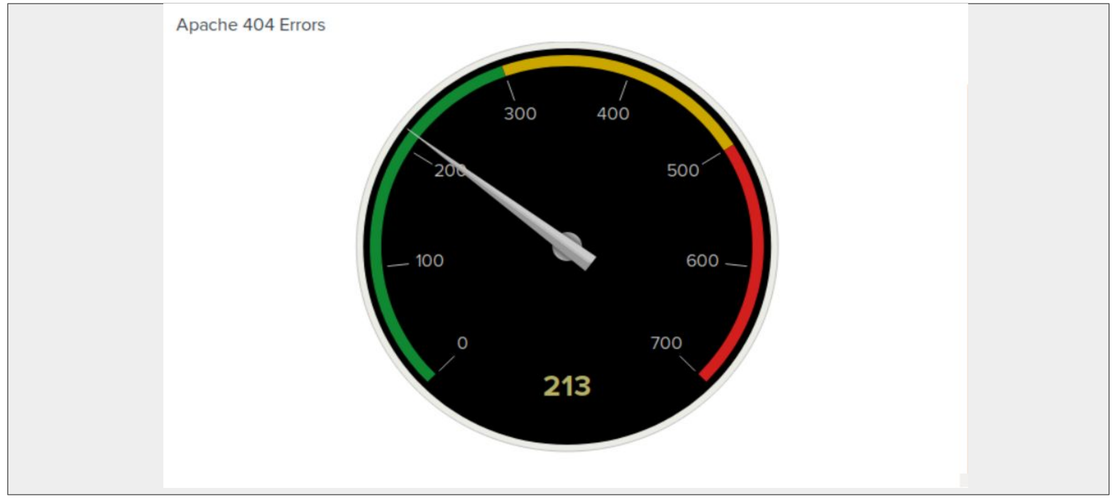
Map of Clientip locations



Top 10 Countries by Users



404 Errors



Attack Analysis

Attack Summary—Windows

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

- **Report analysis for severity: Suspicious**
  - Severity in total count in the column: High, greatly increased
  - 329 in the day 1 server logs in comparison to 1111 in the attack logs

- **Report analysis for failed activities: Not Suspicious**
  - failed activities were found to be lower

Attack Summary—Windows

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

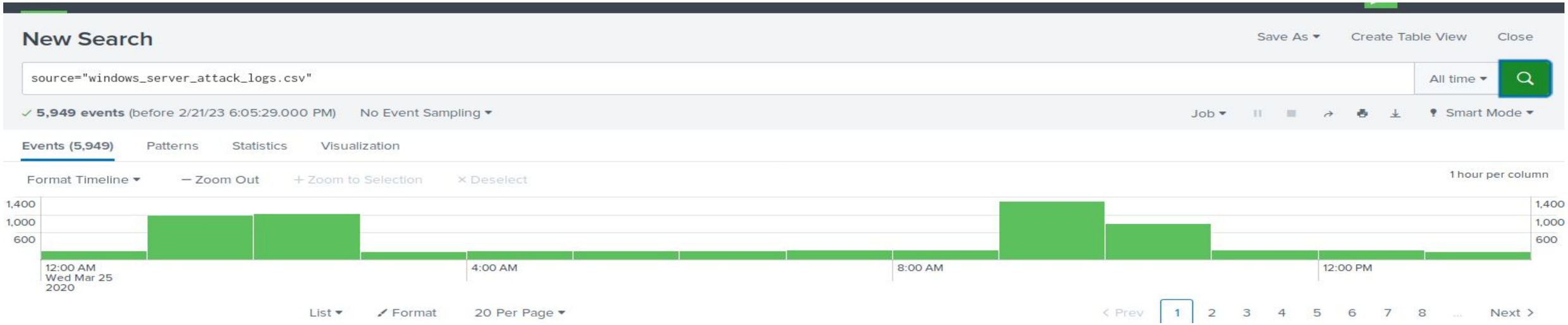
- **Alert analysis for failed windows activity: Suspicious**
  - The total count of events in the hours it occurred was 35. The times being between 8am - 9am
  - Our alert would’ve been triggered for this event. Threshold was correct
  - **Alert analysis for successful logins: Suspicious**
    - The total count of events in the hours it occurred was 196. The primary user being user_j, at the times between 11am - 12pm
    - Our alert would’ve triggered for this event. However, threshold was too low
  - **Alert analysis for user account deleted:**
    - No suspicious volumes of accounts deleted

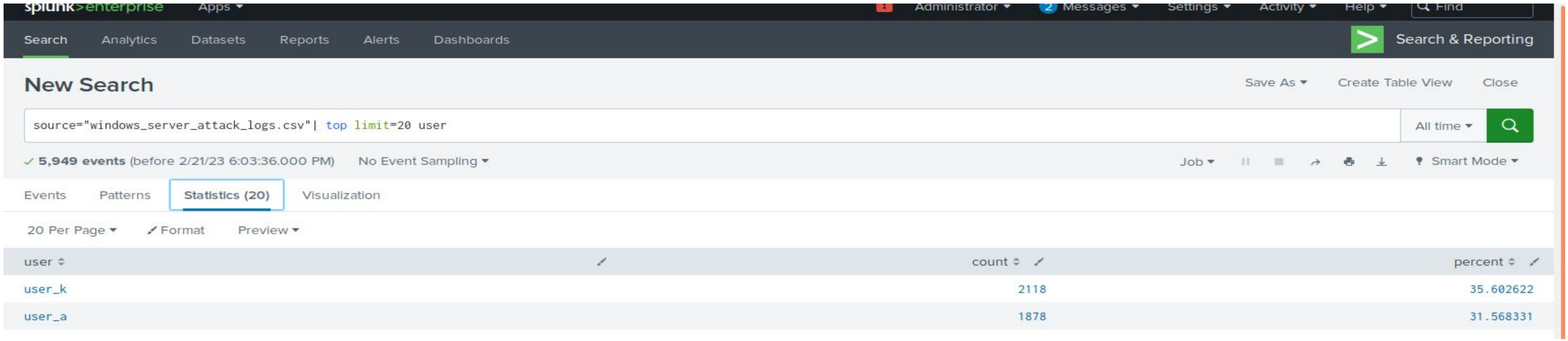
Attack Summary—Windows

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

- Suspicious activity noted 2 users, User_A & User K
- Start time and Stop time: User_A 1:40 am - 2:40 am | User_K 9:10 am - 11:00 am
- Peak Count of different users: User_A 785 | User_K 397
- Suspicious activity found with the signatures, specifically, “A user account was locked out” and “An attempt was made to reset an accounts password” as both had very high volumes of activity.
- “A user account…” peaked at a count of 785 and “An attempt…” peaked at 397.

Screenshots of Attack Logs





Attack Summary—Apache

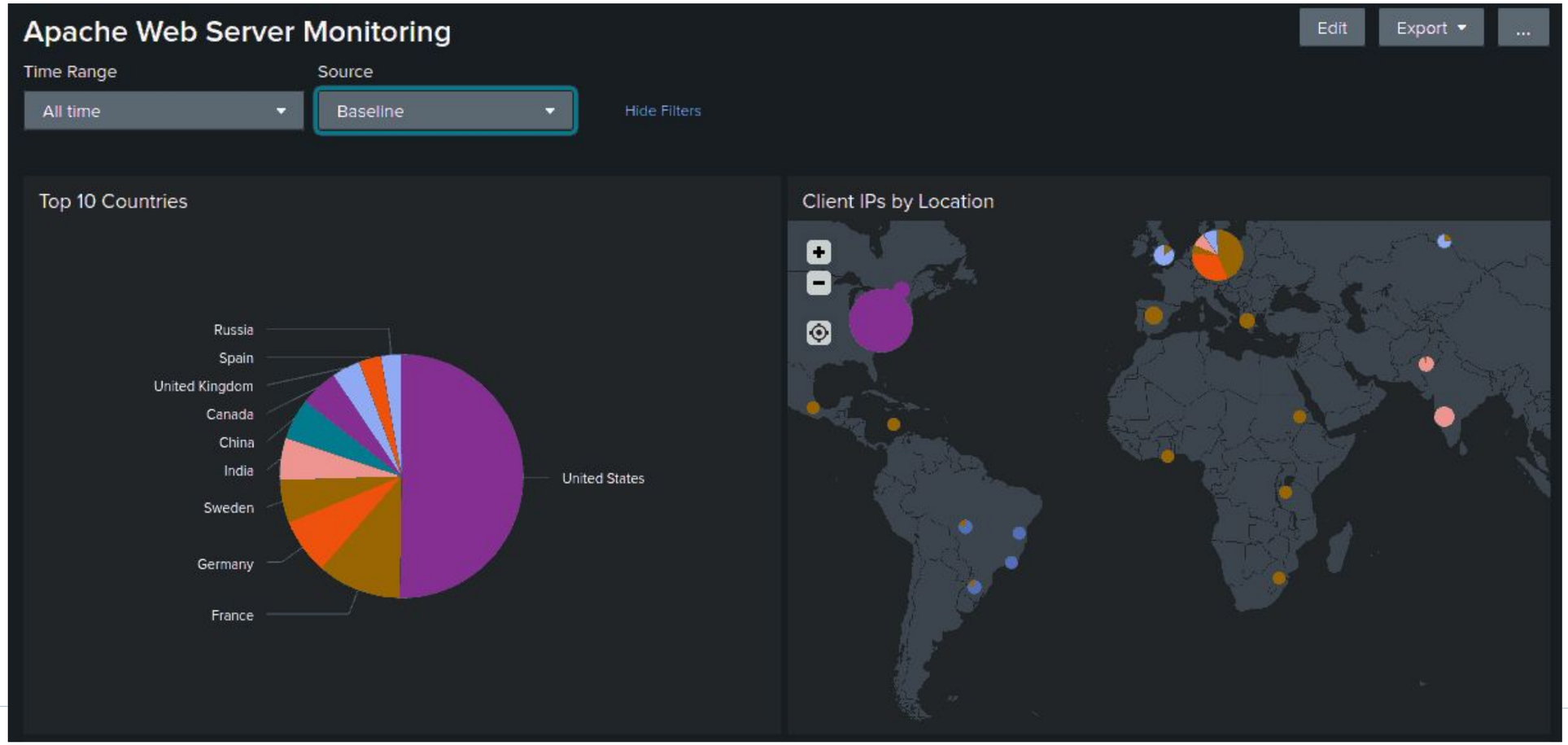
Apache Web Server - HTTP Methods

An extreme volume of GET and POST methods, far above the baseline, occurred from 5pm to 9pm. **The volume of POSTs is far more than GETs from 7pm to 9pm. The peak count of POSTs is 1296 during the attack at 8pm.**

Attack Summary—Apache

Apache Web Server - Client IP - Countries

There is a drastic growth in the volume of IPs belonging to “OTHER” during the attack period **which resolves to Ukraine, specifically the cities Kiev & Kharkiv.**

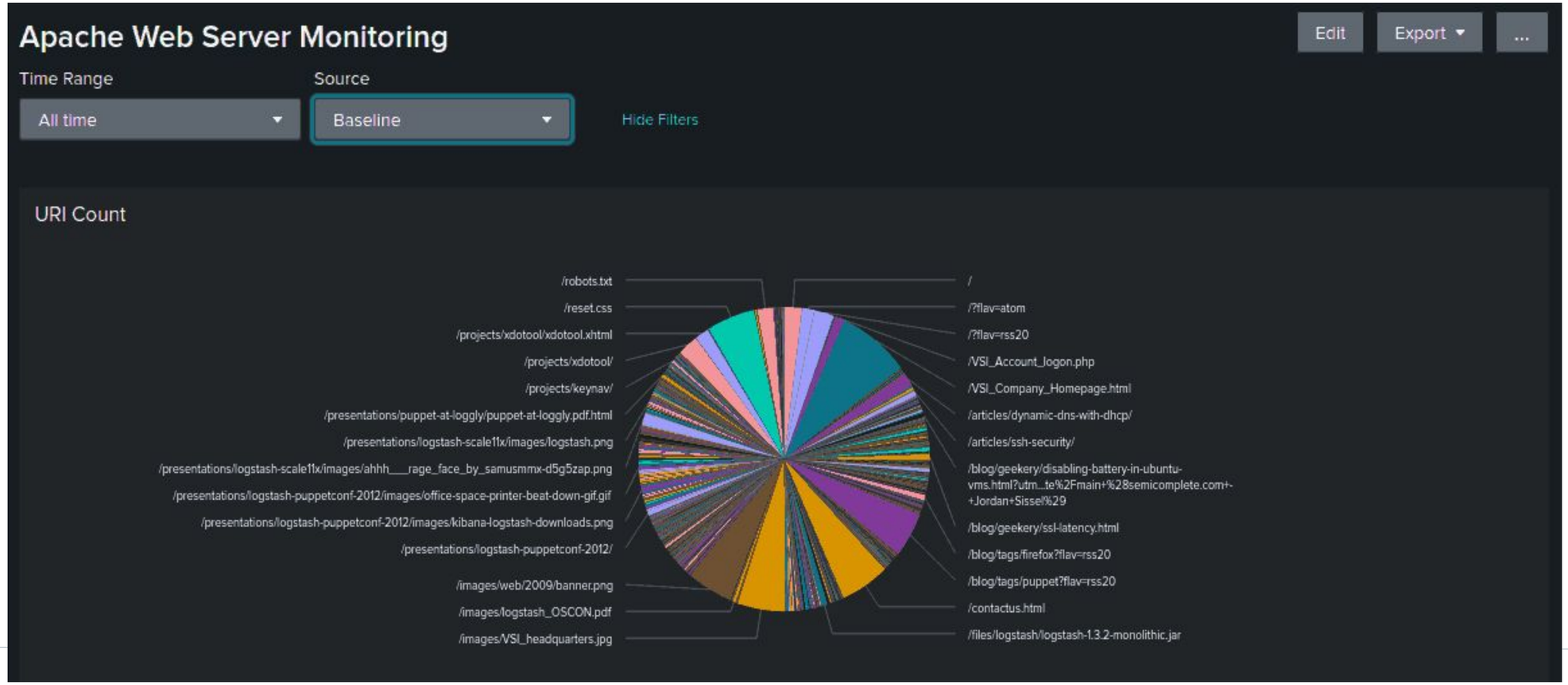


Attack Summary—Apache

Apache Web Server - URI Count

A very large volume of hits to 2 URIs occurred on the attack day:

1323, /VSI_Account_logon.php



Attack Summary—Apache

The attacker seems to be DDoSing and brute forcing the login portal for VSI.

Summary and Future Mitigations

Project 3 Summary

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

This attack was focused on windows and apache servers. The attacker used **IPs that were pointing to Ukraine cities (Kiev and Kharkiv)**. The attacker **focused on two specific URIs** (*/VSI_Account_logon.php* and */files/logstash/logstash-1.3.2-monolithic.jar*) one of them being the **login portal for VSI and was likely the target of a brute force attack**.

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

- Implementing a Web Application Firewall (WAF) that can better detect and block these abnormal traffic patterns (like abnormally high GET and POST requests)
- Using IP filtering to block the addresses where the attacks originated (“Other” category)
- use multi-factor authentication to make it harder to brute force passwords in the future
- regularly review the logs for suspicious and unusual activity