Defensive Security Project
by: Manena Long

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Playing the role of an SOC analyst at a small company called **Virtual Space Industries (VSI)**, which designs virtual-reality programs for businesses.
- VSI has heard rumors that a competitor, **JobeCorp**, may launch cyberattacks to disrupt VSI's business.
- As an SOC analyst, you are tasked to develop a defensive solution that utilizes a variety of the Splunk tools to monitor potential attacks and protect the organization.
- The VSI products that you have been tasked with monitoring include:
- ○ An administrative webpage: https://vsi-corporation.azurewebsites.net/
- ○ An Apache web server, which hosts this webpage
- ○ A Windows operating system, which runs many of VSI's back-end operations
- Your networking team has provided you with past logs to help you develop baselines and create reports, alerts, dashboards, and more.
- You've been provided the following logs on your machine:
- **Windows Server Logs**
- ○ This server contains intellectual property of VSI's next-generation virtual-reality programs.
- **Apache Server Logs**
- ○ This server is used for VSI's main public-facing website, vsi-company.com.
- There will be a simulated attack against the organization. You will analyze the reports and dashboards that were created to determine whether the defensive choices protected the organization from these attacks.

Website Monitoring

Website Monitoring

Monitor websites to detect downtime and performance problems. This app uses a modular input that can be setup easily (in 5 minutes or less).

Website Monitoring

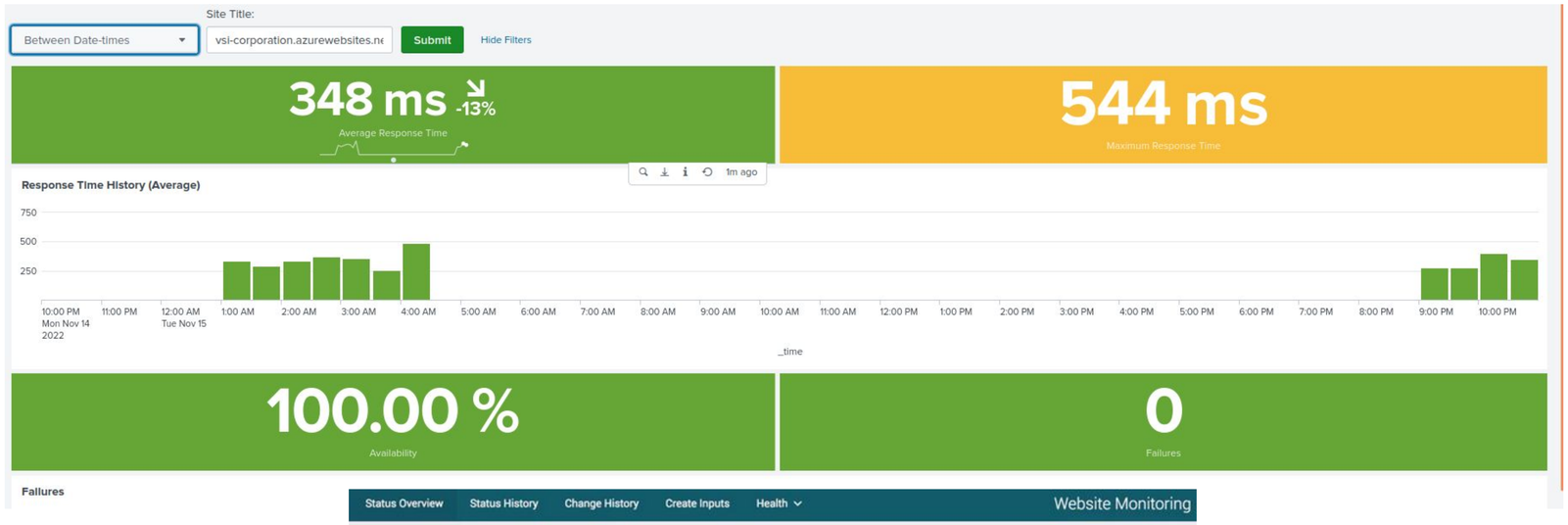
VSI’s website availability, performance, and function are crucial; therefore Website Monitoring is essential.

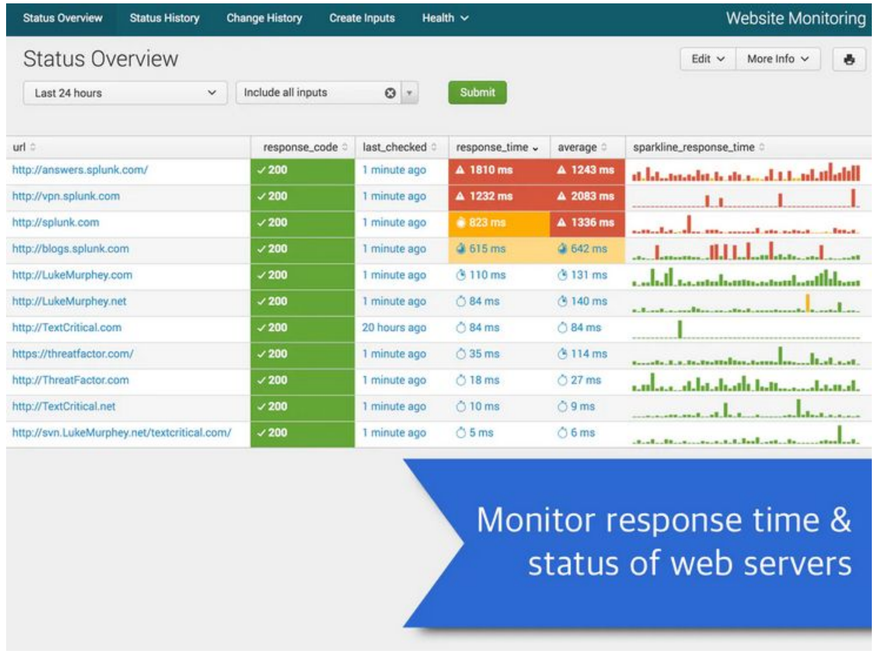
A slow loading site with frequent downtimes can drive visitors away. This can have a negative effect on sales, profits and also impact VSI’s reputation.

The Status Monitoring Dashboard of the Website Monitoring App provides response time for monitored websites and also historical analysis of the site’s responsiveness.

Website Monitoring App can send email alerts if the website is down or responds too slowly, making it easier to be aware of any issues, including potential suspicious activity .

Website Monitoring





Logs Analyzed

1 Windows Logs

The Windows Logs contains intellectual property of VSI's next-generation virtual-reality programs.

2 Apache Logs

The Apache Logs contains data about VSI’s main public-facing website, vsi-company.com

Windows Logs

Reports—Windows

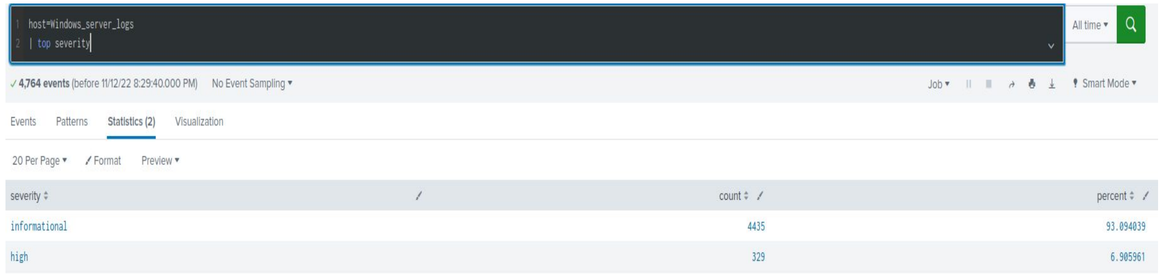
Designed the following Reports:

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

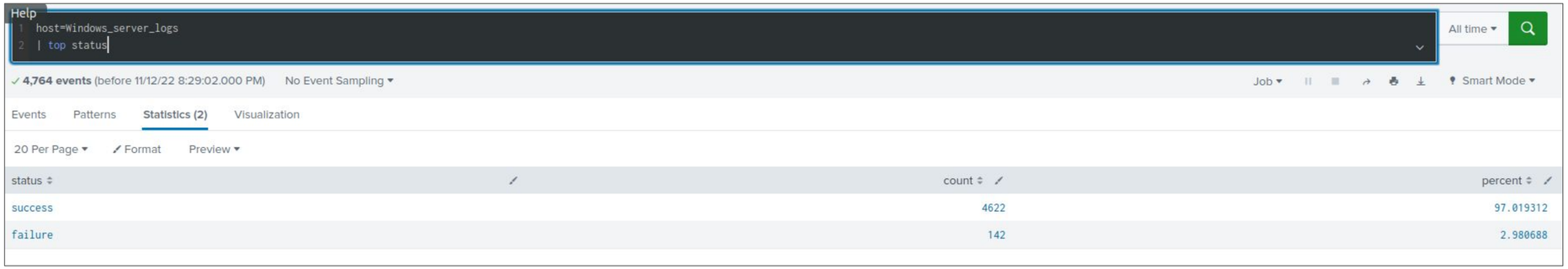
Images of Reports—Windows

Windows Events by Signature

Windows Events by Severity



Windows Events by Status



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Status Failure Alert	This alert triggers when hourly number of failed Windows activity exceeds a certain threshold.	10	> 15

JUSTIFICATION: The largest number of failed Windows activity per hour was determined as 10. This was used as the baseline. The threshold was calculated by multiplying the baseline number by 1.5

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Successful Logon Alert	This alert triggers when the hourly number of the signature “An account was successfully logged on”, exceeds the threshold.	20	> 30

JUSTIFICATION: The largest number of successful logons per hour was determined as 20. This was used as the baseline. The threshold was calculated by multiplying the baseline number by 1.5

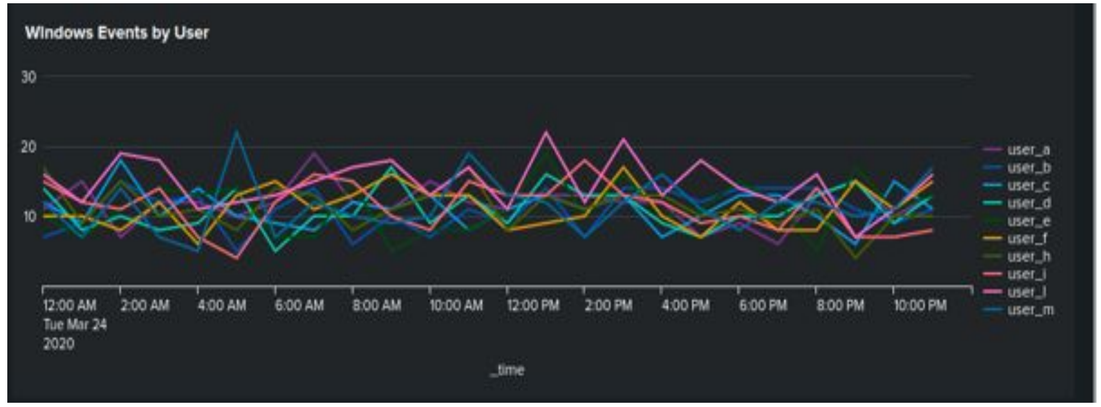
Alerts—Windows

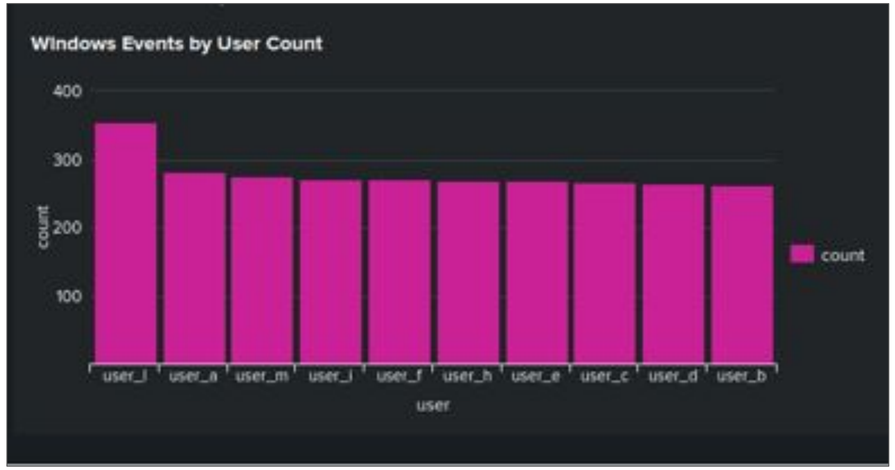
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Deleted Account Alert	This alert triggers when the hourly number of the signature “A user account was deleted”, exceeds the threshold.	20	>31

JUSTIFICATION: The largest number of a user account being deleted per hour was determined as 20. This was used as the baseline. The threshold was calculated by multiplying the baseline number by 1.5

Dashboards—Windows





Apache Logs

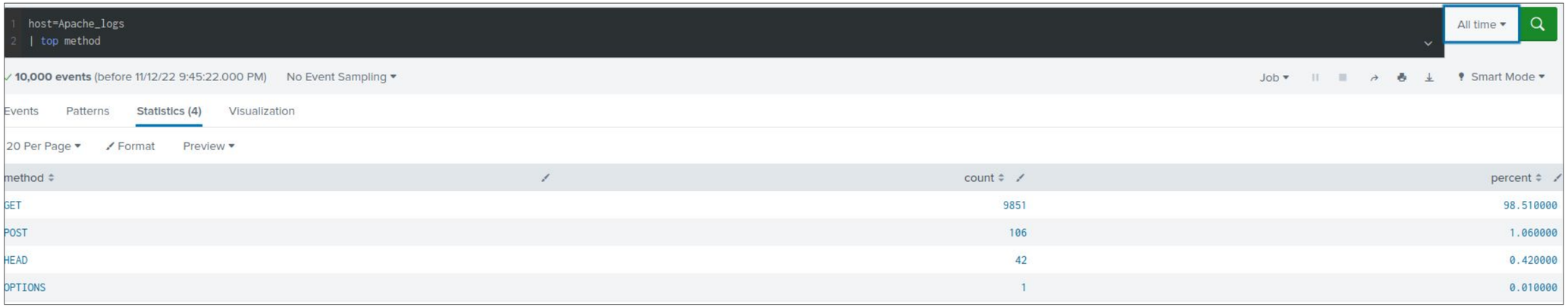
Reports—Apache

Designed the following reports:

Report Name	Report Description
Web Server Events by Method Report	A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc)
Web Server Events by Referrer Report	A report that shows the top 10 domains that refer to VSI’s website
Web Server Events by Response Code Report	A report that shows the count of each HTTP response code

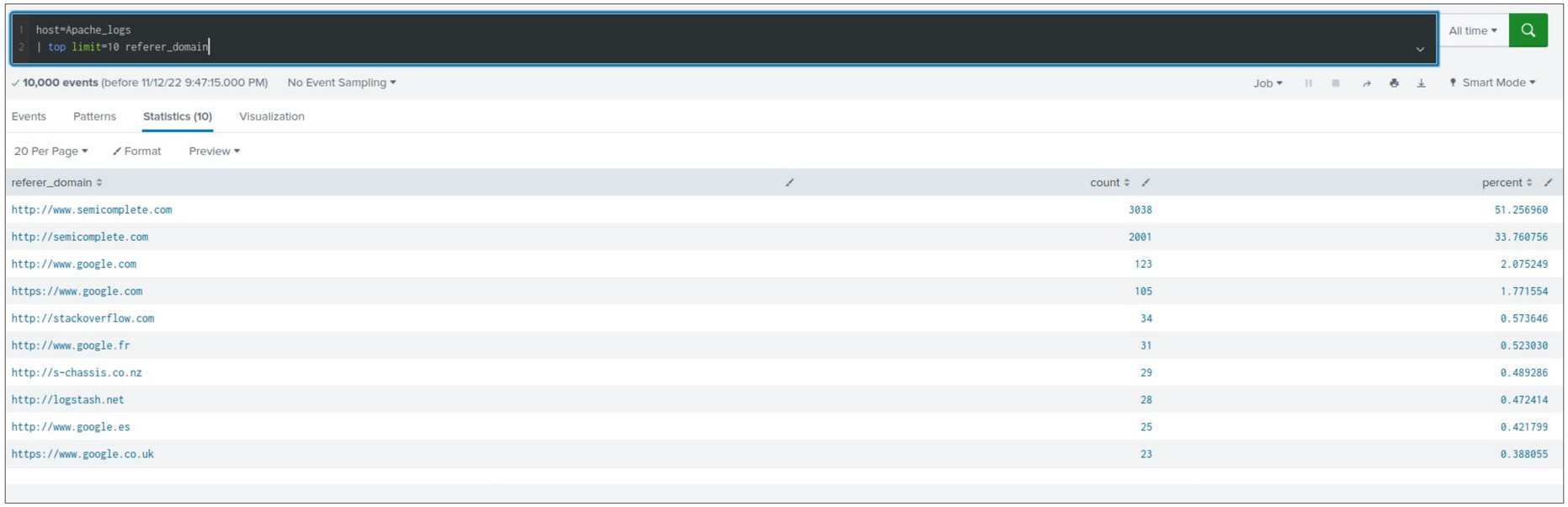
Images of Reports—Apache

Web Server Events by Method



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

Web Server Events by Referrer



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

Images of Reports—Apache

Web Server Events by Response Code

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

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache Logs International Activity Alert	This alert triggers when the hourly activity from any country besides the United States reaches a predefined threshold	120	180

JUSTIFICATION: The largest number of international activity per hour was determined as 120 and was used as the baseline. The threshold was calculated by multiplying the baseline number by 1.5

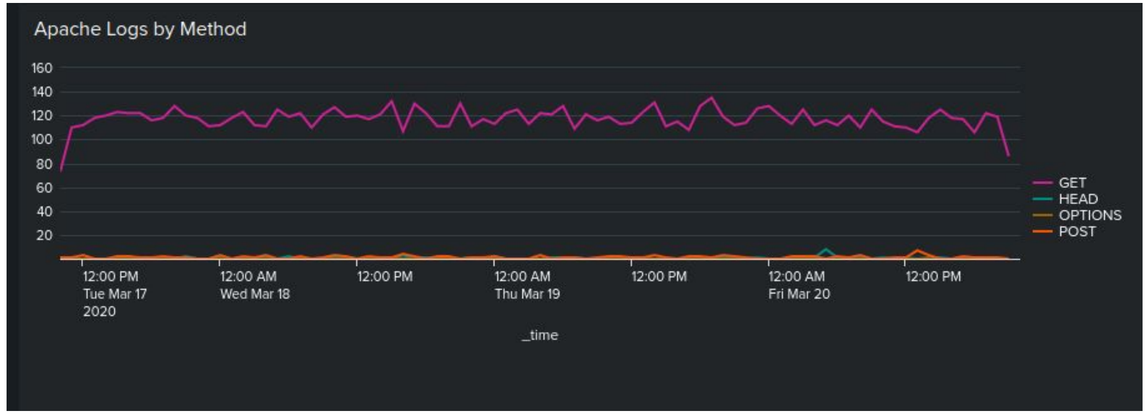
Alerts—Apache

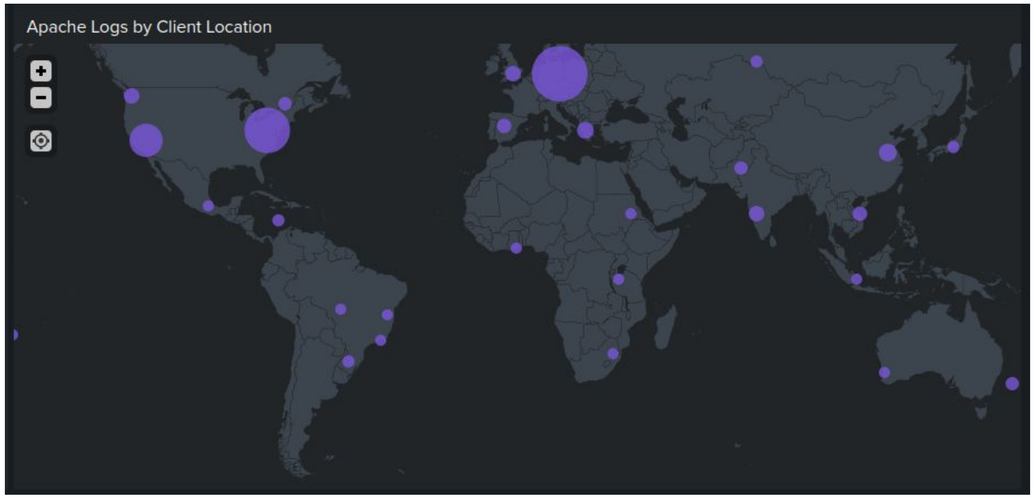
Designed the following alerts:

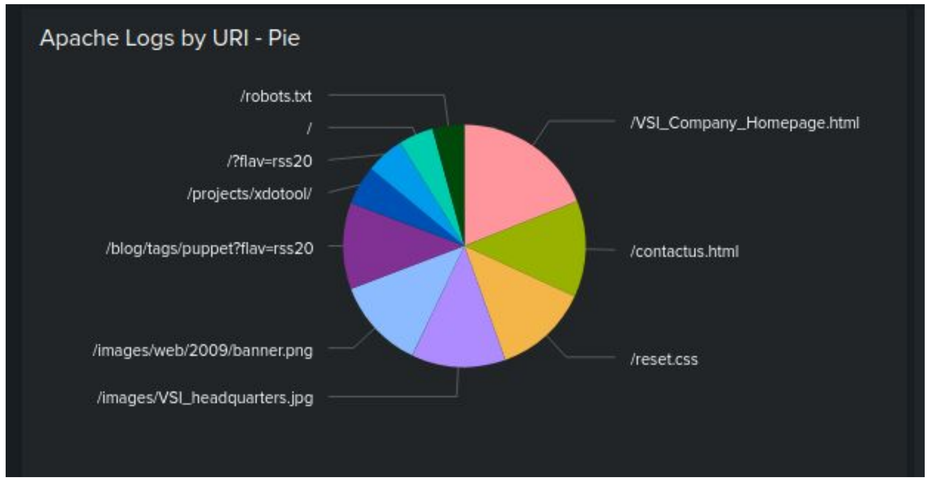
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache Logs HTTP POST Alert	This alert triggers when the hourly count for the HTTP POST method method reaches a predefined threshold	8	> 12

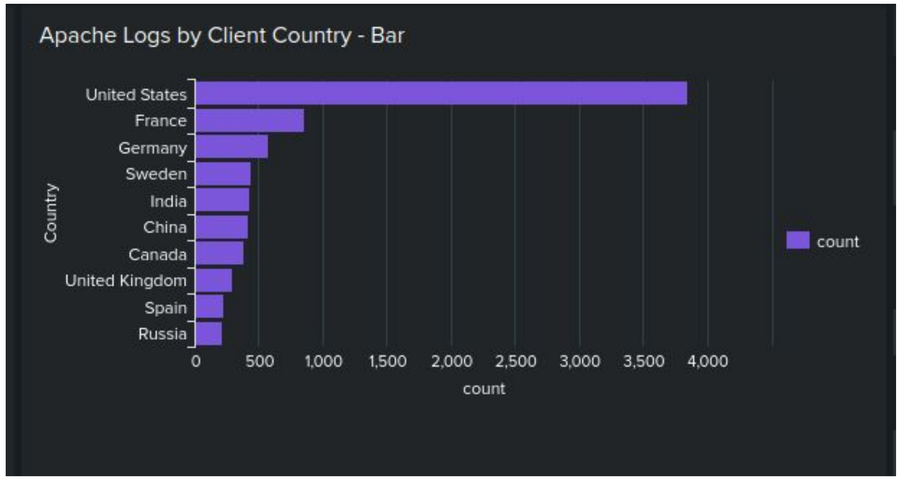
JUSTIFICATION: The largest number of HTTP POST per hour was determined as 8 and was used as the baseline. The threshold was calculated by multiplying the baseline number by 1.5

Dashboards—Apache









Attack Analysis

Attack Summary—Windows

REPORTS

- Report Analysis for **Severity** indicates an increase in the high severity cases by percentage.

- Report Analysis for **Failed Activities** indicates that there is not a major change in the cumulative failure of events.

Attack Summary—Windows

ALERTS

- Alert Analysis for Failed Windows Activity: There is some potential suspicious activity of 35 events at 8 a.m. on Weds, March 25th. The threshold of greater than 15 events was correct.

- Alert Analysis for Successful Logins: There is some potential suspicious activity at 11 AM and 12 PM on Weds, March 25th. The count of activity is 196 at 11 a.m. and 77 at 12 p.m. The primary user logging in is user j. The threshold of greater than 30 events was correct.

- Alert Analysis for Deleted Accounts: There was no suspicious activity of deleted accounts.

Attack Summary—Windows

DASHBOARDS

- Time Chart of Signatures - Three signatures have suspicious activity:
  - A user account was locked out. Started after 12 AM and ended by 3 AM on March 25th. The peak count was 896
  - An attempt was made to reset an account password. Started after 8 AM and ended by 11 AM on March 25th. The peak count was 1,258.
  - An account was successfully logged on. Started after 10 AM and ended by 1PM on March 25th. The peak count was 196.

Attack Summary—Windows

DASHBOARDS

- Dashboard for Users - Three users have suspicious activity:
  - User A: Started after 12 AM and ended by 3 AM on March 25th. Peak count was 984.
  - User K: Started after 8 AM and ended by 11 AM on March 25th. Peak count was 1,256.
  - User J: Started after 10 AM and ended by 1PM on March 25th. Peak count was 196.

Screenshots of Attack Logs

Attack Summary—Apache

REPORTS

- Report Analysis for Methods - there was a suspicious change in the HTTP POST method, which increase from 1% to 29%.

- Report Analysis for Referrer Domain - there were no suspicious referrers during the attack.

- Report Analysis for HTTP Response Codes - There are several small changes, but the most prominent is the 404 response code, which increased from 2% to 15%

Attack Summary—Apache

ALERTS

- Alert Analysis for International Activity: There was activity from Ukraine at 8 PM. on Weds, March 25th, with a count of 935 events. The threshold of greater than 180 events per hour was correct.

- Alert Analysis for HTTP POST Activity: There was a spike in POST method activity at 8 PM on Weds, March 25th, with a count of 1,296 events. The threshold of greater than 12 events per hour was correct.

Attack Summary—Apache

DASHBOARDS

- Dashboard Analysis for Time Chart of HTTP methods - there were increases in the POST and GET methods:

  - The POST method was used, starting after 7 PM and ending by 9 PM. The peak count was 1,296.
  - THE GET method was used, starting after 5 PM and ending by 7 PM. The peak count was 729.

- Dashboard Analysis for Client Country - there was a suspicious increase in IP location of clients from Ukraine.

Attack Summary—Apache

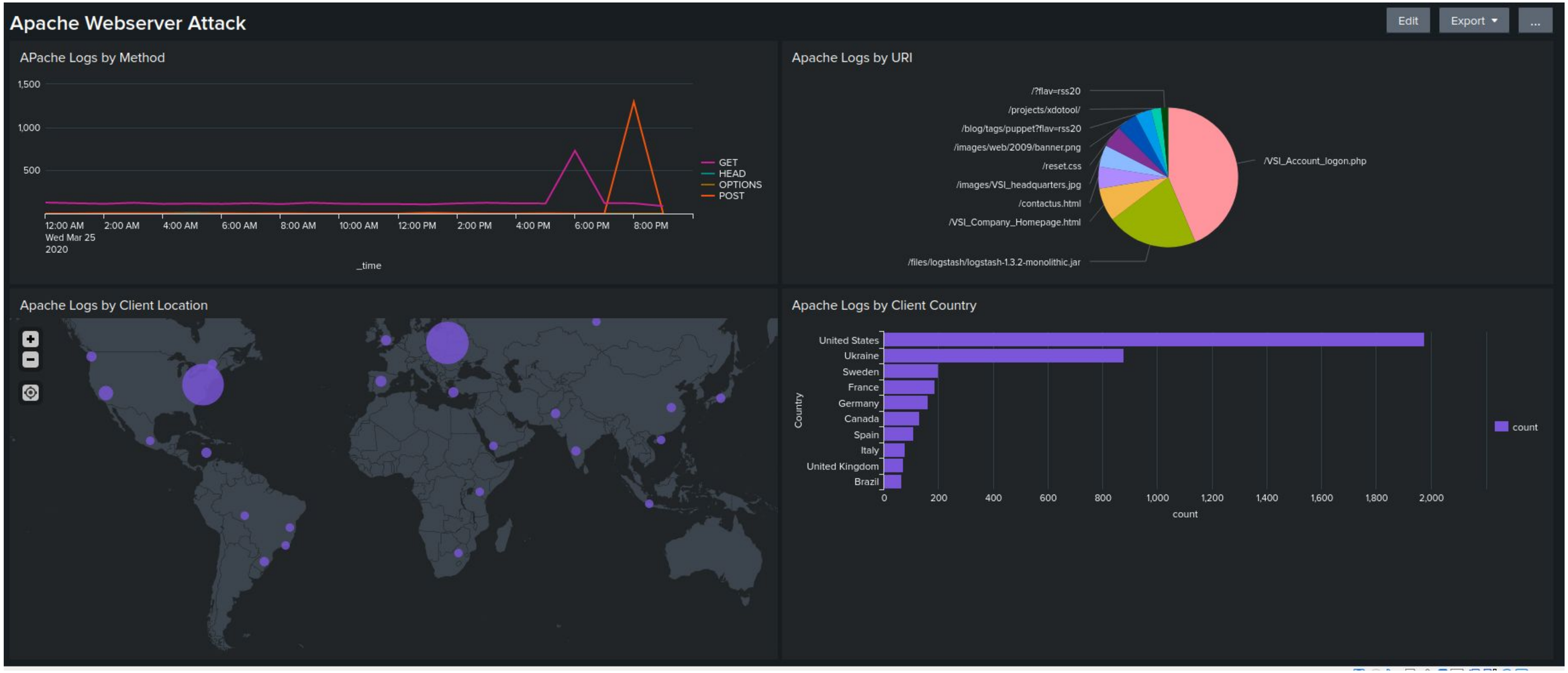
DASHBOARDS

- Dashboard Analysis for Cluster Map- there was suspicious activity from Ukraine.

  - Kyiv(formerly Kiev): Count of 439
  - Kharkiv: Count of 433

- Dashboard Analysis for URI Data - there was suspicious activity against the main VSI logon page: /VSI_Account_logon.php.

Screenshots of Attack Logs



Summary and Future Mitigations

Project 3 Summary

- Attack on the Windows Server: The information that was gathered indicate a potential brute force attack.

  - User “a” showed a high increase of activity that correlates with the same time when the signature “A user account was locked out” increased. This took place after 12 AM and ended by 3 AM on March 25th.
  - User “k” showed a suspicious increase of activity during the same time as when the signature “An attempt was made to reset an account password” activity spiked. This took place after 8 AM and ended by 11 AM on March 25th.
  - User “j” showed a suspicious increase of activity during the same time when the signature “An account was successfully logged on” activity spiked. This took place after 10 AM and ended by 1PM on March 25th.

- The totality of the attack started around 12 AM and ended around 1PM on March 25th.

Summary -continued

- Attack on the Apache Web Server: The information that was gathered indicate a potential brute force attack.
  - There was a suspicious increase in the POST method, at 8 PM on March 25th.
  - Based on IP locations there was suspicious high volume of activity from Ukraine.
  - Analysis of URI data showed suspicious activity against the main VSI logon page: /VSI_Account_logon.php.
  - Since the POST method is used to submit or update information to a web server, the attacker may have been trying to brute force the VSI logon page.

Mitigation Recommendations

- Windows Server
  - Require stronger passwords with 12 characters, including one capital and one special character.
  - Require two-factor authentication.
  - Add an account lockout policy that does not allow for more than 3 incorrect logon attempts.

- Apache Web Server
  - Add strong input validation for fields that require user input.