Defensive Security Project

by: Lisa Suzanne, Brenda, Timin, Tom

Table of Contents

This document contains the following resources:

Scenario

- VSI SOC Analyst
- We are monitoring Windows and Apache Logs to prevent JobeCorp from disrupting our business
- The products that we have been tasked to monitor
  - Administrative Webpage
  - Apache Web Server
  - Windows OS running VSI backend

Monitoring Environment

WhoisXMLAPI

Whois XML IP Geolocation API

The Whois XML IP Geolocation API is a web service that provides real-time geolocation data for a given IP address. The API can be used to determine the country, city, region, latitude, longitude, and timezone associated with an IP address, as well as the Autonomous System Number (ASN) and Internet Service Provider (ISP) that owns the IP address.

The Whois XML IP Geolocation API is a useful tool for various use cases, such as fraud detection, website localization, and targeted advertising. With its accurate and up-to-date geolocation data, the API can help businesses improve their customer engagement and security measures.

Whois XML IP Geolocation API

Let’s image VSI wants to expand its customer base by targeting specific regions and countries. Whois XML IP Geolocation API could be incredibly beneficial to the company. By integrating the API into their software, the company could gather detailed information about the location of their potential customers. They could use this information to customize their virtual reality programs to cater to the specific needs of their customers in different regions. For example, they could create programs that highlight cultural differences or emphasize specific products or services that are popular in a particular region.

Furthermore, the API could help the company track the performance of their virtual reality programs in different regions. They could use this information to optimize their programs and make them more effective in specific regions. For example, they could analyze the data to see which regions are showing the most interest in their programs and adjust their marketing strategies accordingly. Overall, by using the Whois XML IP Geolocation API, the small company would be able to make data-driven decisions about how to market their virtual reality programs and which regions to focus on. This could ultimately lead to increased sales and a larger customer base.

Whois XML IP Geolocation API

Logs Analyzed

1 Windows Logs

Windows Server logs

- System events
- Security events
- Application events
- Performance events
- Internet Information Services
- Active Directory events
- DNS events

Windows Server Attack Logs

- Audit policy changes
- Account logon events
- Account management events
- Privilege use events
- Object access events:
- Policy change events

2 Apache Logs

Apache Server Logs

- Access logs:
- Error logs:
- Rewrite logs
- SSL logs
- User-agent logs
- Referrer logs

Apache Attack Logs

- IP addresses
- Requested URLs
- HTTP status codes
- User agents
- Timestamps

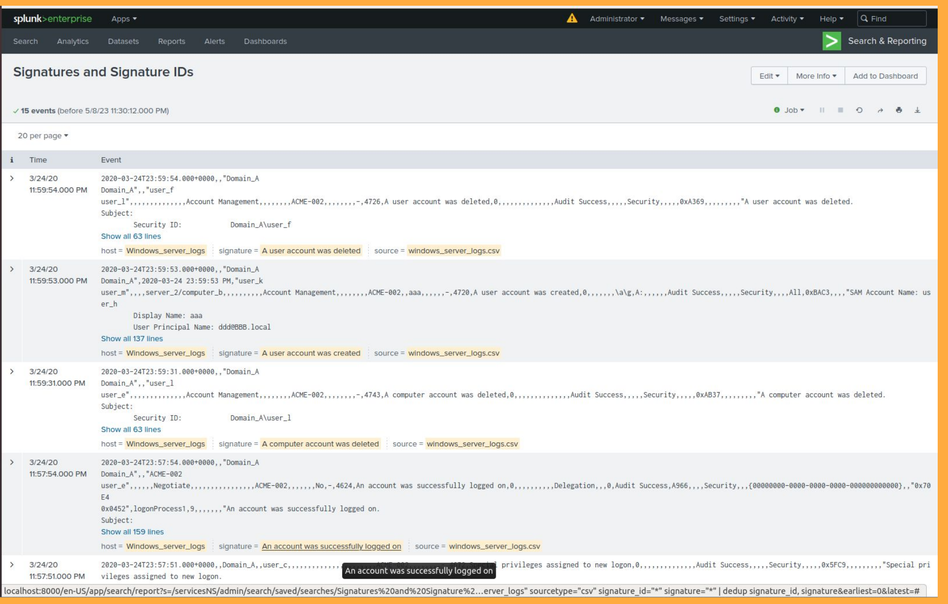
Windows Logs

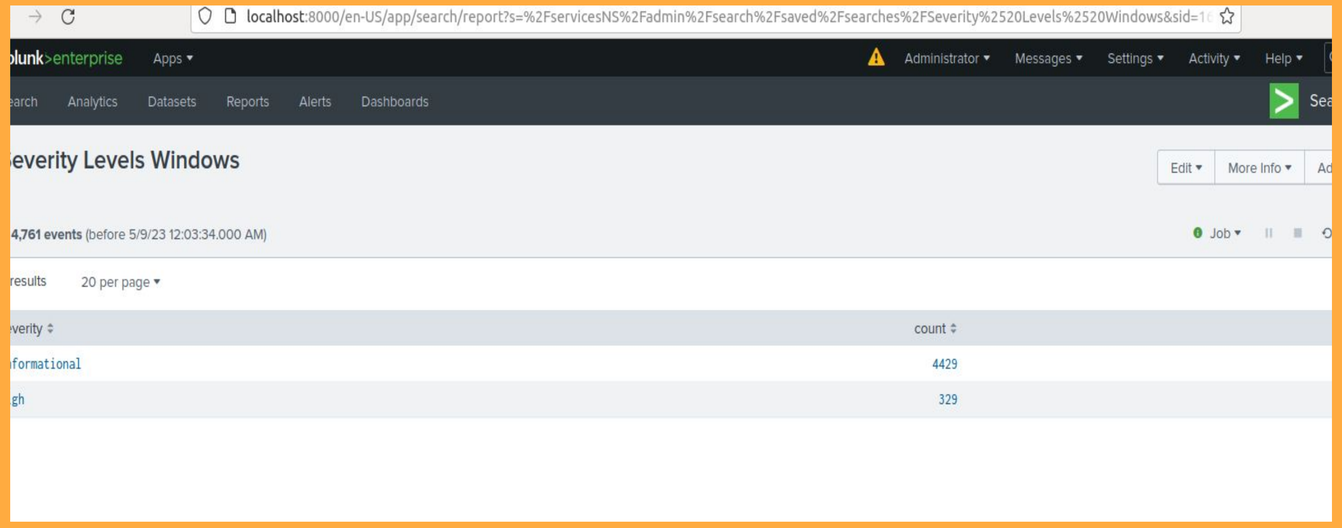
Reports—Windows

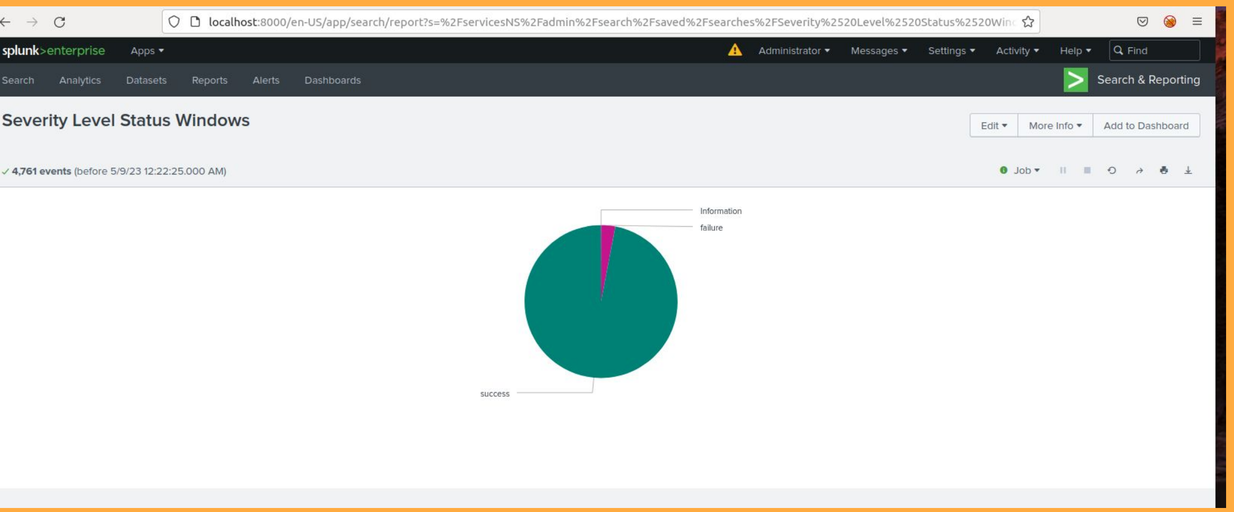
Designed the following reports:

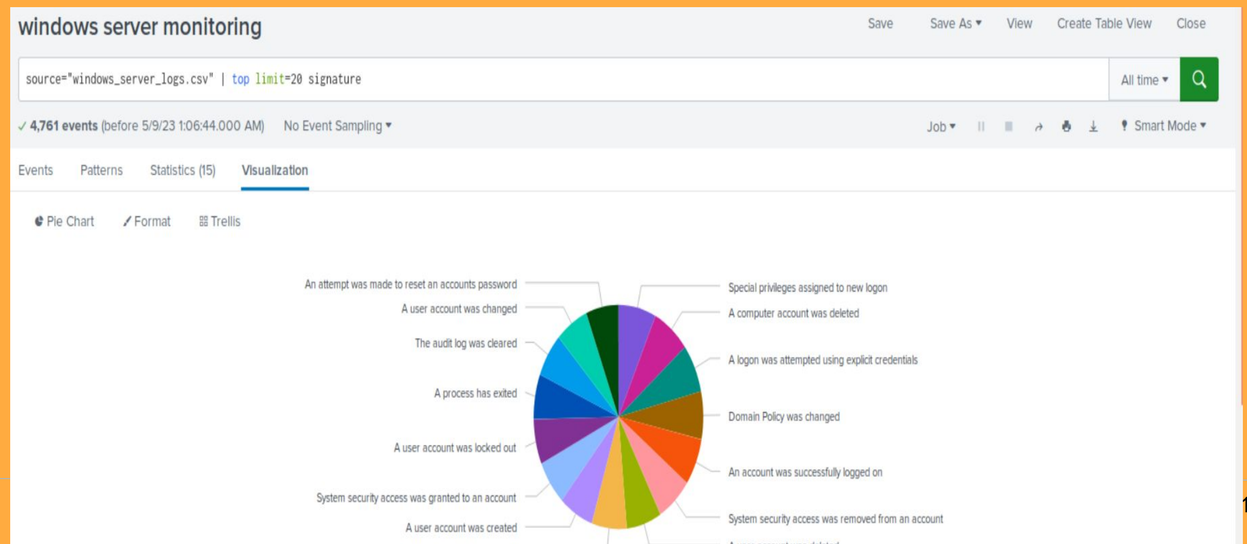
Report Name	Report Description
Signatures and Signature IDs	Table of Signatures and their related Signature IDs
Severity Levels	Severity levels of events and their percentage
Success and Failure of Windows Activities	Pie chart of successful and failed attempts of Windows activity

Images of Reports—Windows









Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Login Windows Attempts	Failed Login Windows Activity within 1 hour	5	8

JUSTIFICATION: The average failed attempts per hour is about 5, and the majority of instances where that number exceeds 8 happened outside of business hours.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
USER ACCOUNT DELETED	An alert for accounts deleted being	7	12

JUSTIFICATION: The average accounts deleted per hour is about 7, and the maximum at any given point is around 12.

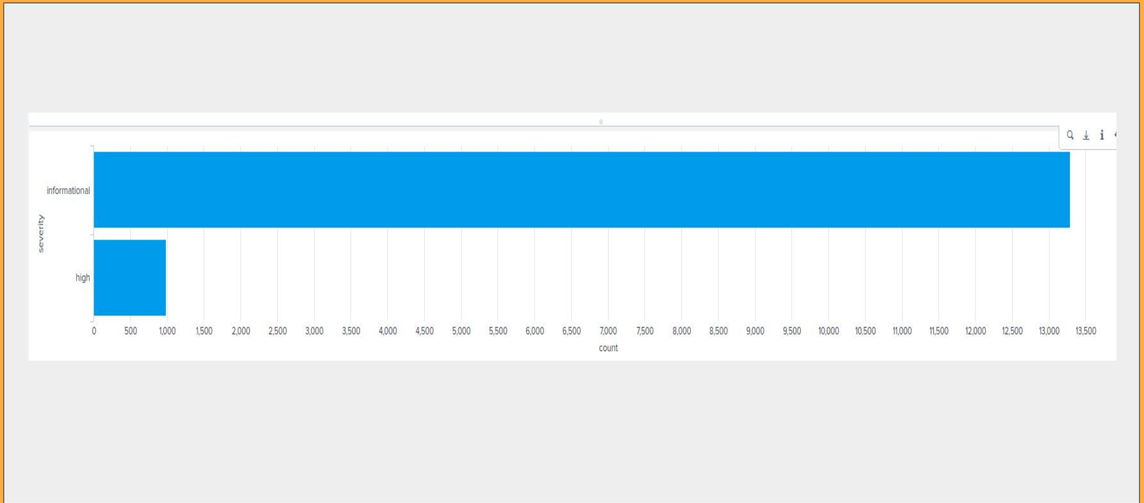
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
An account was successfully logged on	a baseline and threshold for the hourly count of accounts logged on	7	15

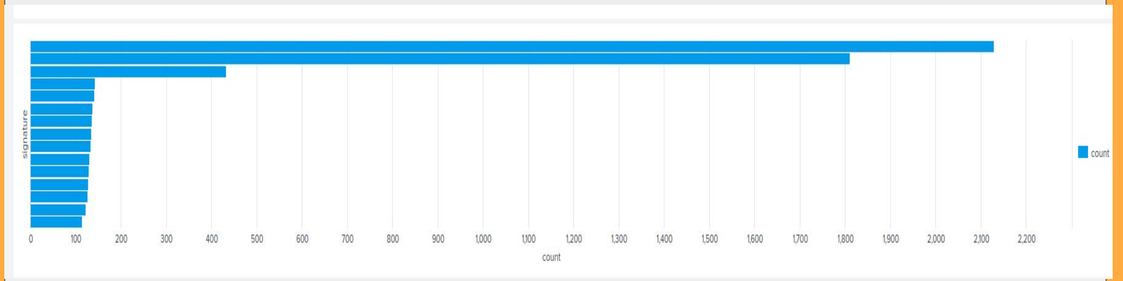
JUSTIFICATION: The average amount of accounts logged on per hour is about 7, and the maximum at any given point is around 15.

Dashboards—Windows



Attack Logs

_time	A computer account was deleted	A privileged service was called	A process has exited	A user account was changed	A user account was deleted	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	NULL
2020-03-24 19:00	19	14	8	10	14	16	11	10	10	12	68	0
2020-03-24 20:00	12	20	13	7	7	805	15	11	16	16	51	0
2020-03-24 21:00	9	3	16	9	5	896	14	3	17	8	27	0
2020-03-24 22:00	13	13	12	16	9	10	14	6	16	14	51	0
2020-03-24 23:00	12	18	8	11	14	12	12	11	10	16	63	0
2020-03-25 00:00	11	14	12	16	17	19	9	8	14	10	62	0
2020-03-25 01:00	9	14	12	17	13	3	11	14	8	13	64	0
2020-03-25 02:00	15	8	15	17	11	11	15	16	20	7	70	1
2020-03-25 03:00	17	13	23	11	11	16	16	12	11	16	59	0
2020-03-25 04:00	5	2	1	3	3	1	4	1258	0	4	12	0
2020-03-25 05:00	0	0	0	0	0	0	23	761	0	0	0	0
2020-03-25 06:00	0	0	0	0	0	0	196	0	0	0	0	0
2020-03-25 07:00	7	9	7	11	13	6	77	6	6	9	46	0
2020-03-25 08:00	4	8	7	9	13	16	15	12	15	17	48	0



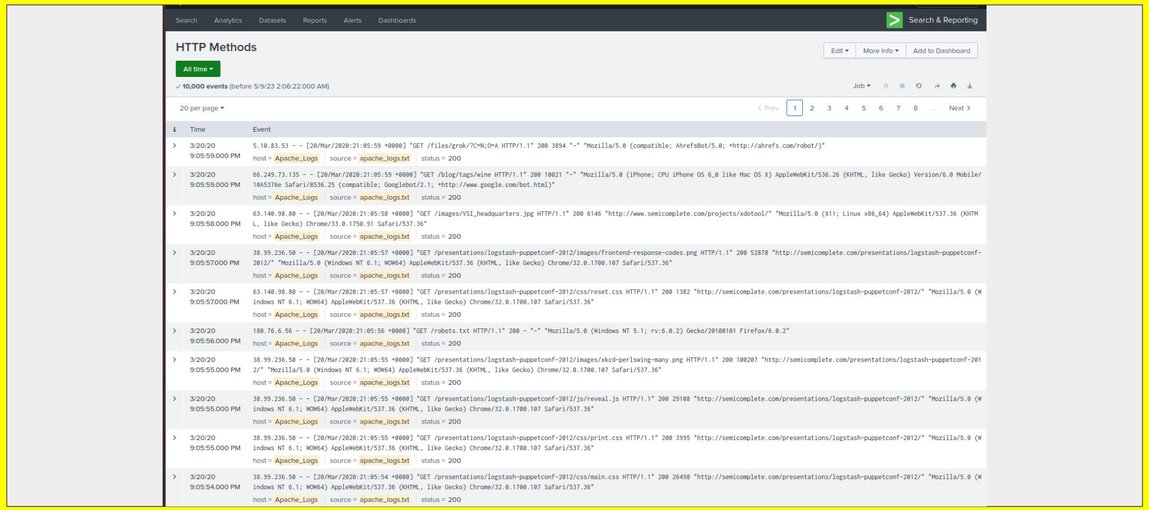
Apache Logs

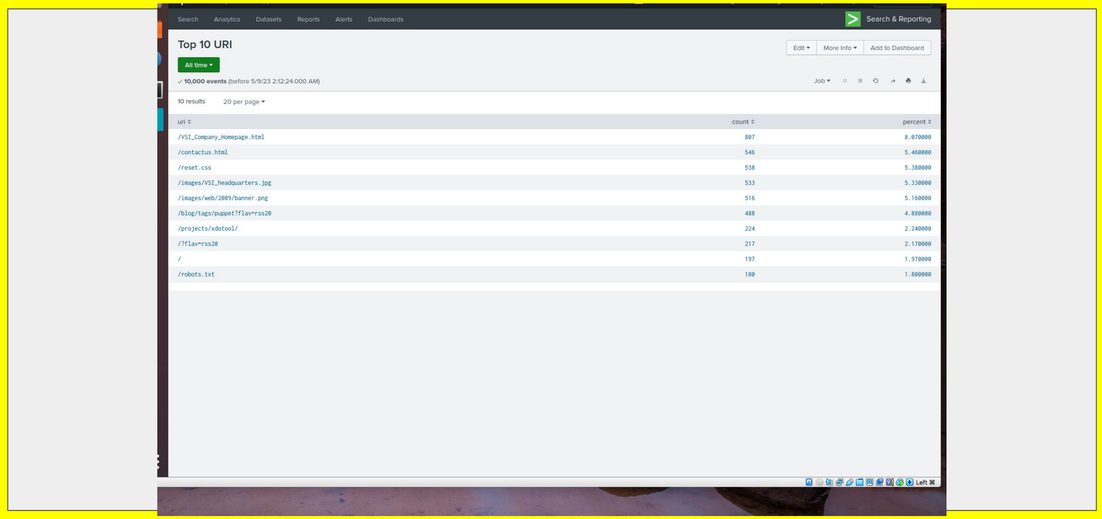
Reports—Apache

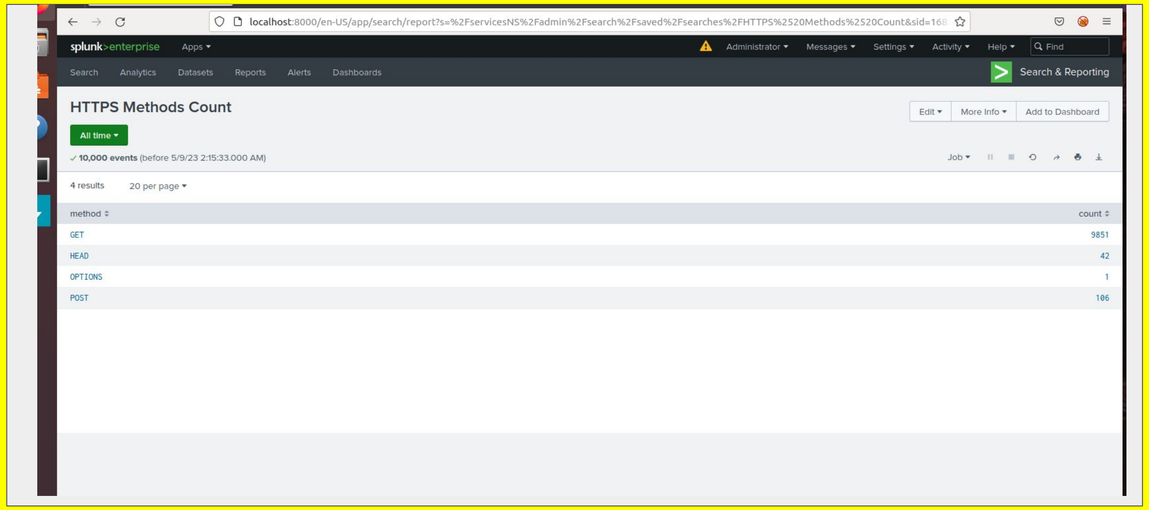
Designed the following reports:

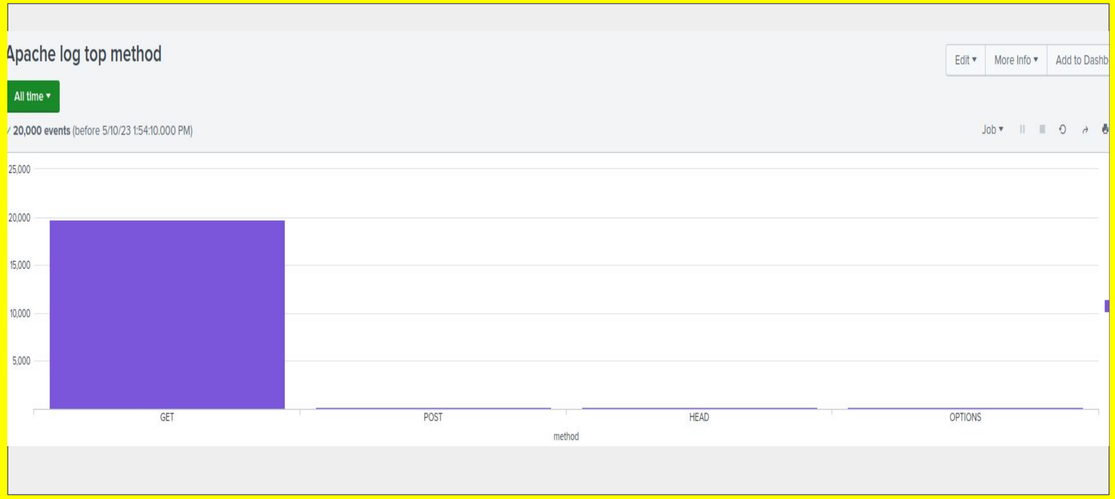
Report Name	Report Description
HTTP Methods	Table of all HTTP Methods
Top 10 Referrer Domains	Table of the top 10 Referrer Domains that refer to VSI’s website
HTTP Response Code Counts	Table showing the count of each HTTP response code

Images of Reports—Apache









Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Threshold of high HTTP Posts	Alert if hourly count of the HTTP Post method exceeds the threshold.	3	5

JUSTIFICATION: Most events were consistent around 3. Setting threshold to 5 will capture all events out of “normal” range.

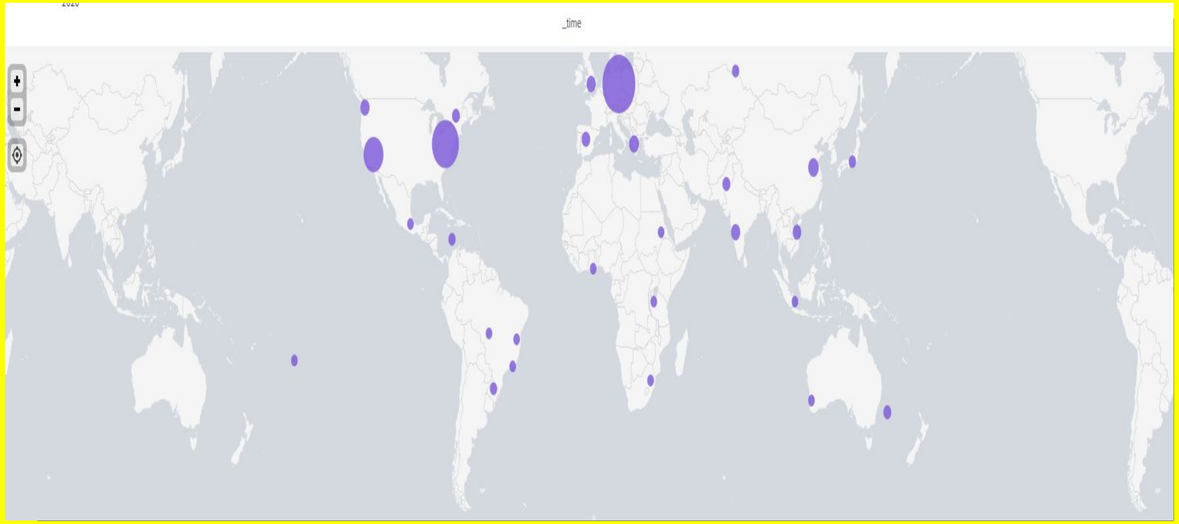
Alerts—Apache

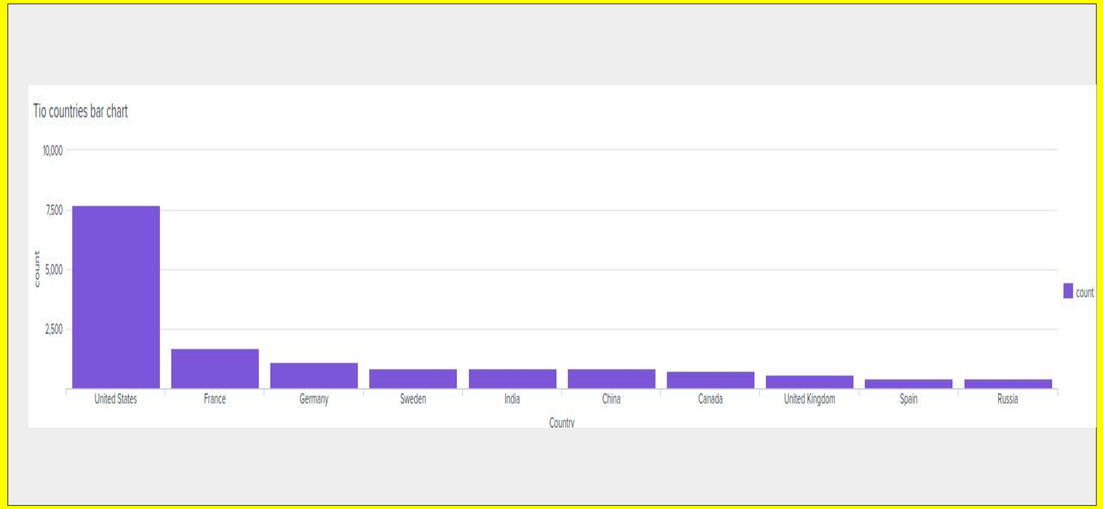
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly activity from Country outside US	Set alert to capture influx of traffic outside of US hourly	90	180

JUSTIFICATION: Events in normal range seem to be between 90 and 170. If we capture anything over 180, we will capture suspicious activity.

Dashboards—Apache





Attack Analysis-Windows

Attack Summary—Windows

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

1. Report analysis for “failure” activity has no significant changes
    a. Windows logs show 2.98% failure and Windows attack logs 1.56%
2. Time Charts indicate suspicious activity was high for “Reset Passwords” and “User account lockouts”.
    a. Highest lock out peaked from 7-10PM on March 24
        i. 896 incidents
    b. Highest attempts to reset password peaked from 3-6 AM on March 25
        i. 1258 highest

Attack Summary—Windows

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

- Alert set for “4726” -User Deleted threshold set for events greater than 10
  - Not a significant change-Threshold set correctly.
  - There was a slight uptick in deleted accounts On March 24 7-10PM Tuesday March 25th and another slight increase 2-3AM Wednesday March 25th.
- Alert set for An Account was successfully logged on. Peak was 196 Events
  - Set at threshold of 15.
  - Threshold set correctly as we would have received notification. Perhaps increasing it to reduce alert fatigue would be best action.

Attack Summary—Windows

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

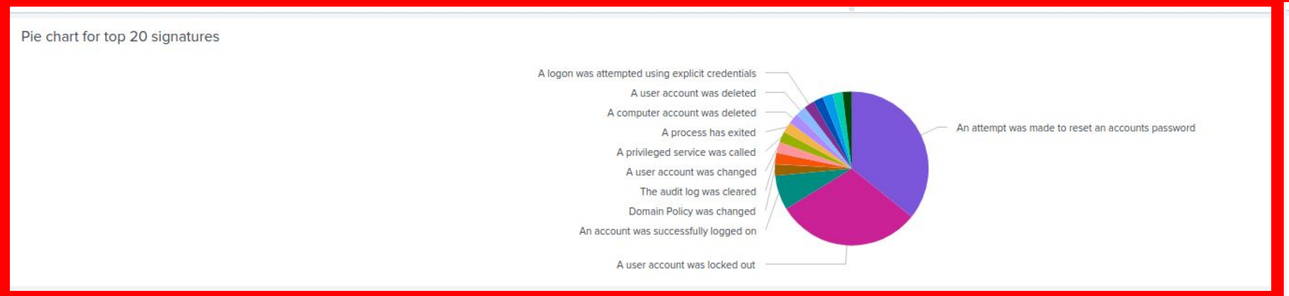
- There was suspicious activity noted in our signatures
  - “An Attempt was made to reset an account password”
    - 1258 highest volume
    - Attempts were at peak from 3-6am March 25th
  - “A user account was locked out”
    - 896 highest volume
    - Attempts were at peak from 7-10PM March 24th

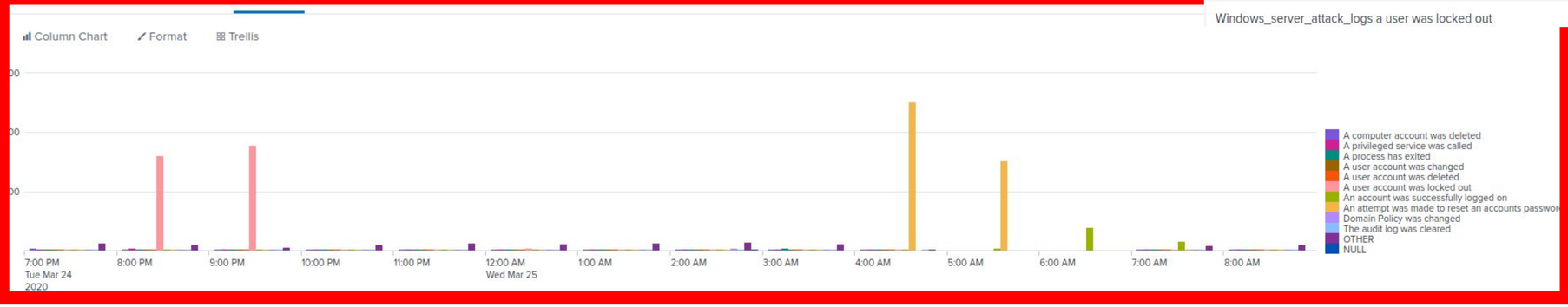
Attack Summary—Windows

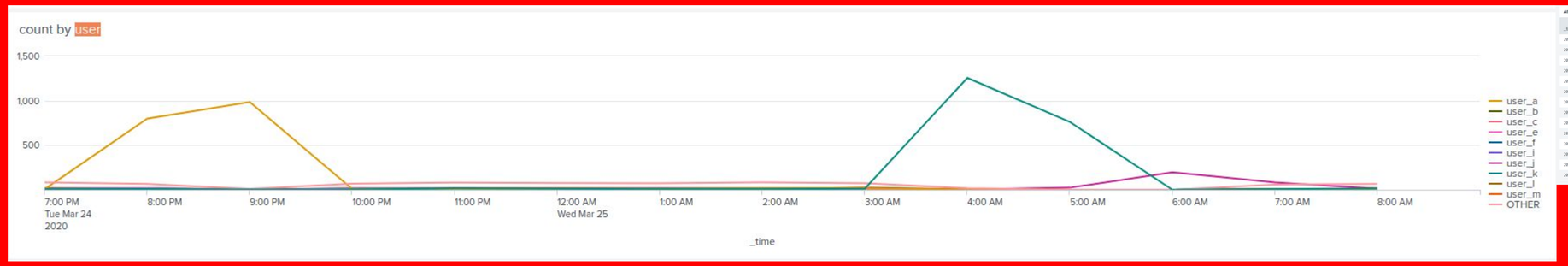
Summarize your findings from your dashboards when analyzing the attack logs.

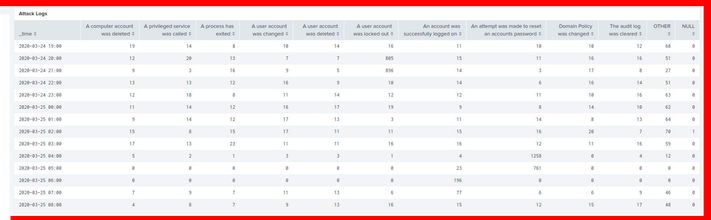
- Two users show suspicious activity
  - User A Peak time was March 24th 7PM-10PM
    - 984 incidents
  - User K Peak time was March 25th 3AM-6AM
    - 1256 incidents

Screenshots of Attack Logs









Attack Analysis-Apache

Attack Summary—Apache

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

- For the report analysis of methods we found that here was a spike in GET from 6am to 7am with 729 and POST from 8pm to 9pm with 1,296
- For the report analysis for referrer domain we found that both www.semicomplete.com and semicomplete.com were the top two hits with counts of 764 and 572
- for the report analysis for HTTP response codes we found that a jump in status code 200 to 3,746 and in status code 404 to 679

Attack Summary—Apache

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

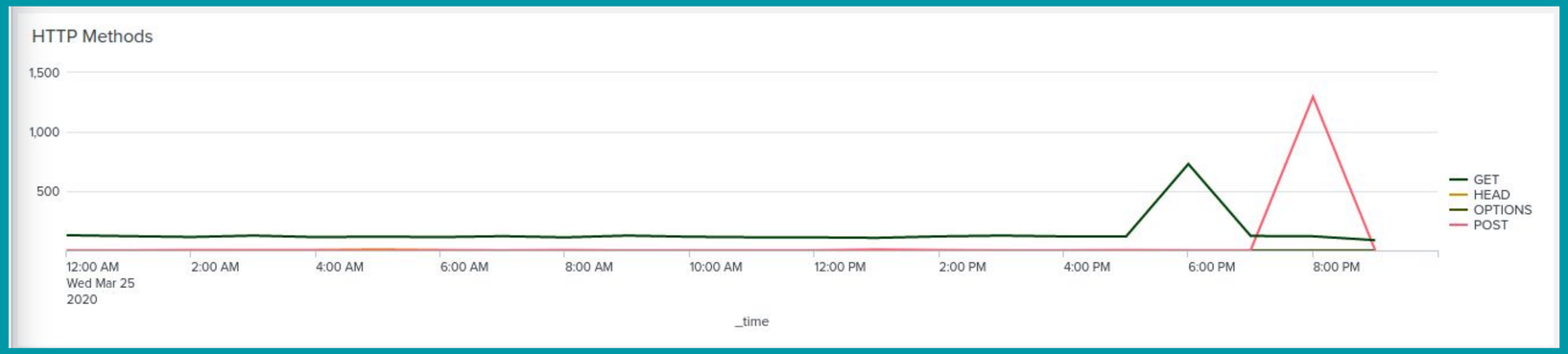
- Alert set for Hourly activity outside of the US, baseline: 90, threshold: 180
  - Yes, our threshold would have been set off by the attack and not by any other hour
- Alert set for HTTP Post activity, baseline: 2, threshold: 5
  - Our threshold would have been set off, but it would have also set off an alert at 1pm on March 25th. We could raised our threshold to about 10 to avoid false positives.

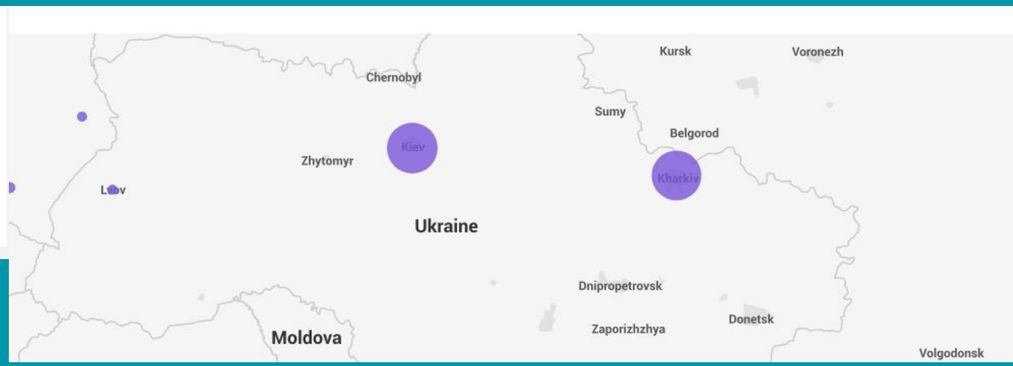
Attack Summary—Apache

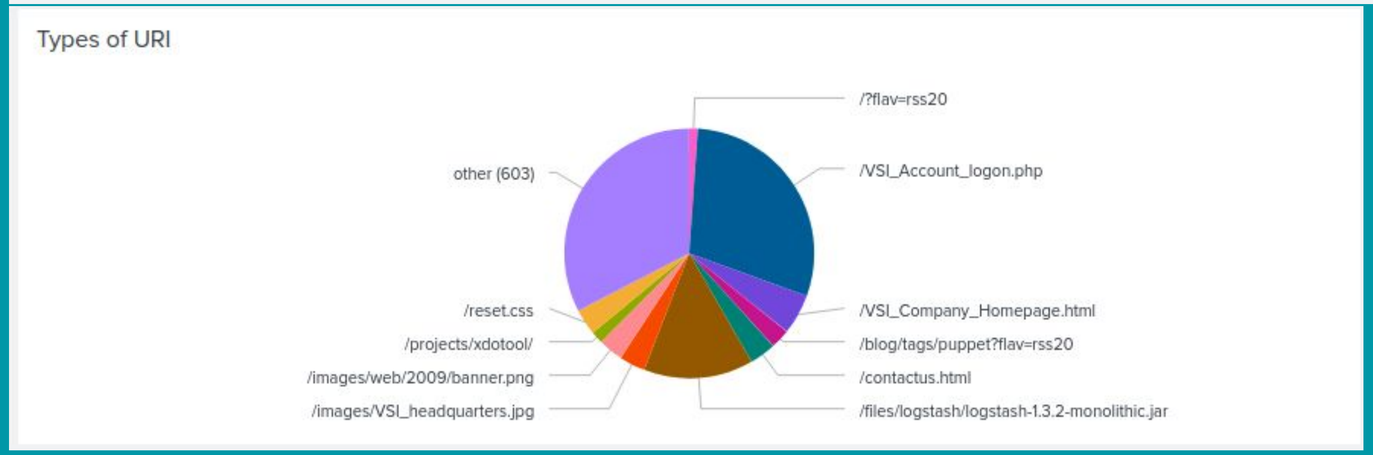
Summarize your findings from your dashboards when analyzing the attack logs.

- Time Chart of HTTP Methods: There was a spike in GETs at 6pm to 729 and a spike in POSTs at 8pm to 1,296
- Cluster Map of Logins: There was a spike of logins from Ukraine, Kiev and Kharkiv, to 877
- Top URI Pie Chart: The VSI_Account_logon.php page was the most used with a count of 1323, leading to believe that some kind of attack occurred on this page. Brute Force, Password Guessing, Command Injection, Local File Inclusion, XSS, SQL Injections, amongst others are all possibilities of the attack.

Screenshots of Attack Logs







Summary and Future Mitigations

Project 3 Summary & Mitigation

- Majority of attacks seem to be coming in from Ukraine.
- To protect VSI from future attacks - Additional security measure proposal:
  - To limit successful brute force attacks, implement increases security around credentials
    - Limit login attempts to 5
    - Increase password complexity with characters, numbers, letters.
    - Implement MFA and/or Captcha
  - Implement firewall rules
    - Block all traffic coming in from various countries
  - To limit XSS, File Inclusion, SQL Injections, and Command Injection
    - Input Validation
    - Output Encoding
    - Store Files in Database
    - Parameterized Queries
    - Server Side Validation