Defensive Security Project

by: Natasha Harris, Shawn Bandy, Sarbjit Singh, Jackie Koh, Steve Herrera, Aiser Tiomico, Nicole Ramirez, Siavash Etesham

Table of Contents

This document contains the following resources:

Monitoring Environment

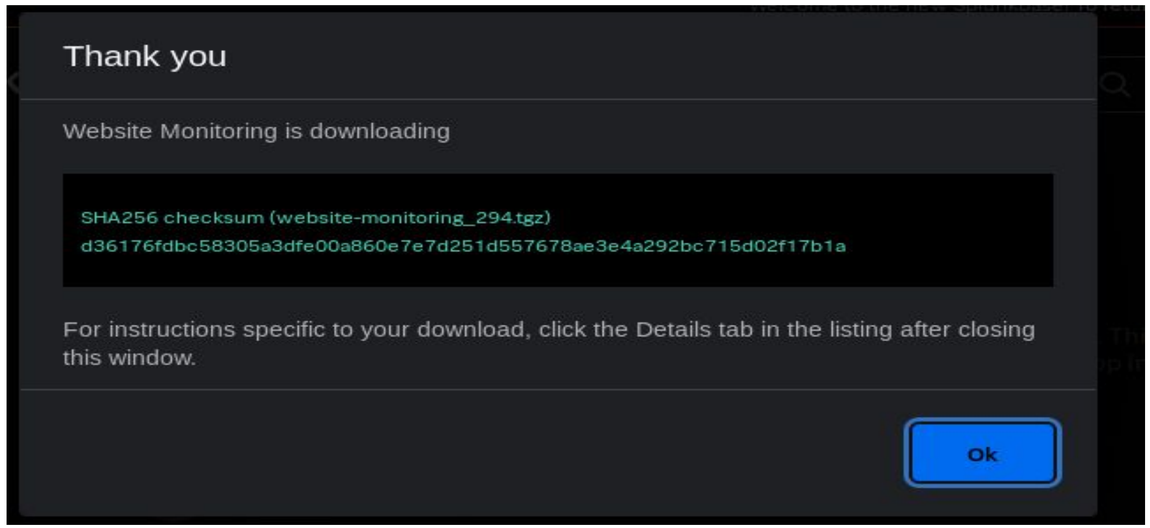
Scenario

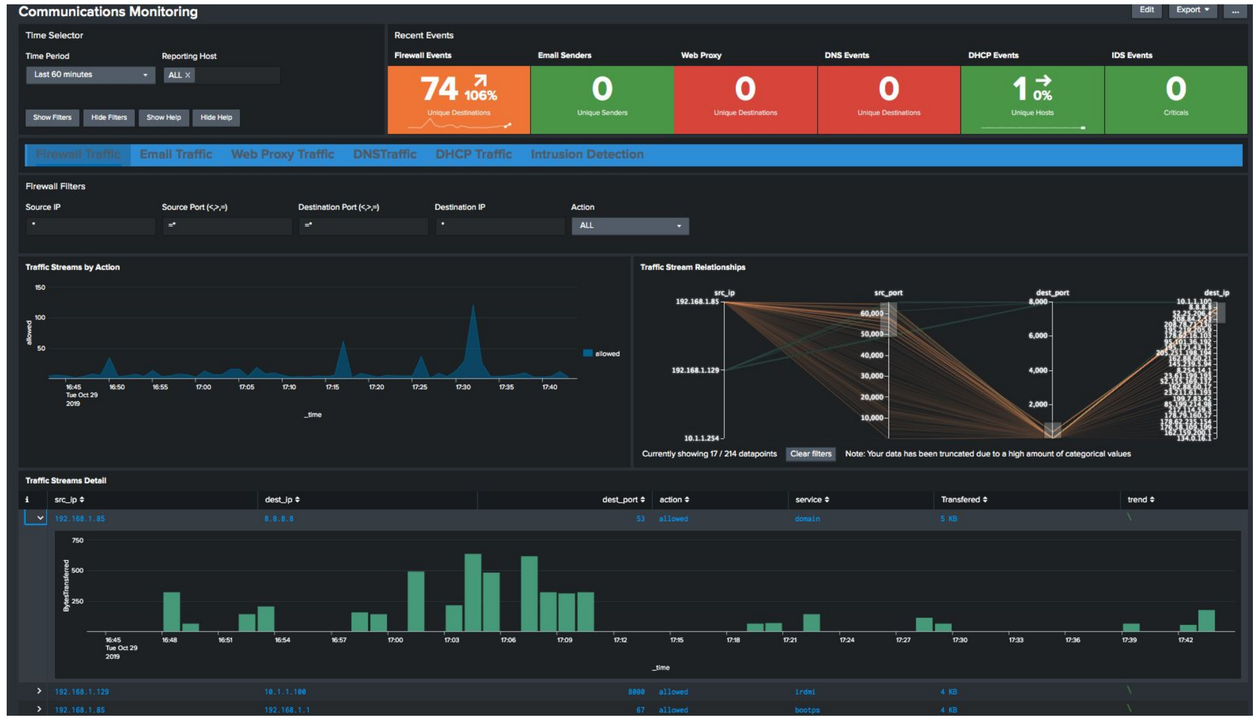
- VSI acting under a tip is aware that its competitor, jobcorp, might attempt a cyberattack on the website and infrastructure. As soc analysts, we have created an environment to monitor attacks with their linux apache server that hosts their public-facing web page and Windows network—used for their company information and data. We provided general baselines and post-attack logs to review their environment and determine if the attack occurred.

Add-On App - Website Monitoring

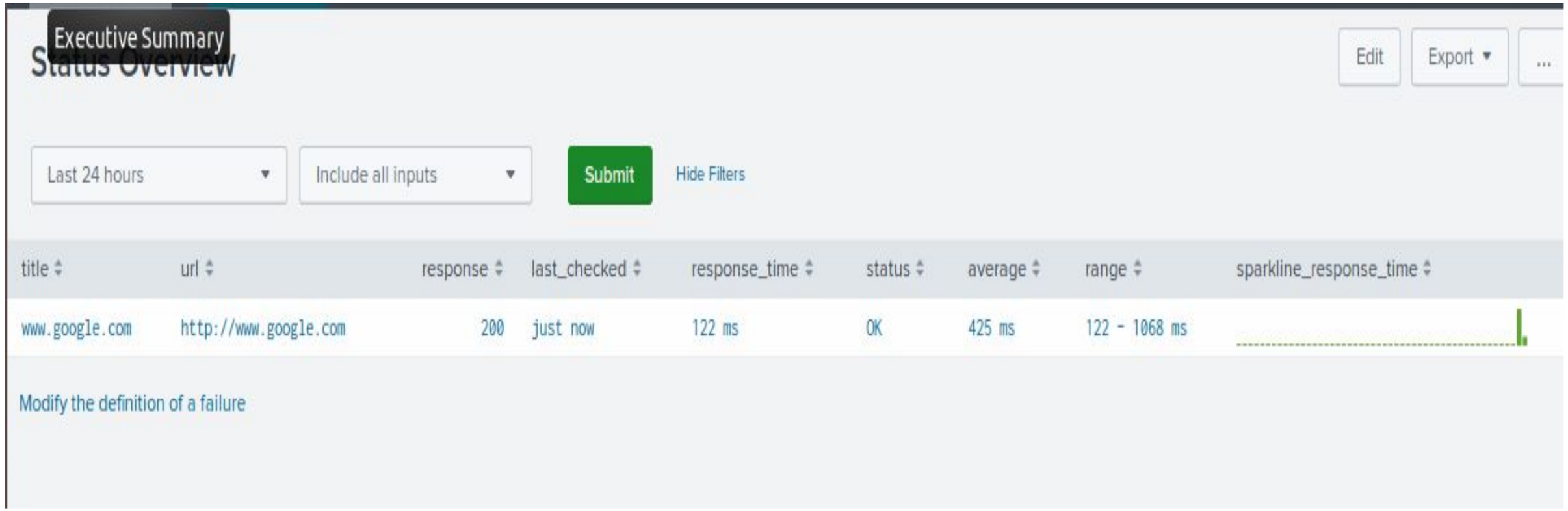
Website monitoring

Chose web site monitoring app to check how the website is performing and regularly perform checks to ensure website stability.
Features Communications Monitoring which will show various types of relevant traffic.





[Website Monitoring]



[Website Monitoring]

The best use case for this service is to ensure our website's overall availability and quality. If your website goes down, it can automate sending an email to notify you. If your site has stability issues, you can actively track its performance. Tracking changes to a website allows Splunk to follow if they are unintended.

Logs Analyzed

1 Windows Logs

[Windows Logs contain information regarding various topics, including specific computers within their local network and activities. The critical information in these logs is the host, domains, time zones, destinations, windows, event codes, and event IDs.]

2 Apache Logs

[Apache Logs contains information regarding VSI's web server; it holds client IP addresses, specific flies requested by clients, referring domains, HTTP request methods, request times, URI, and information status.]

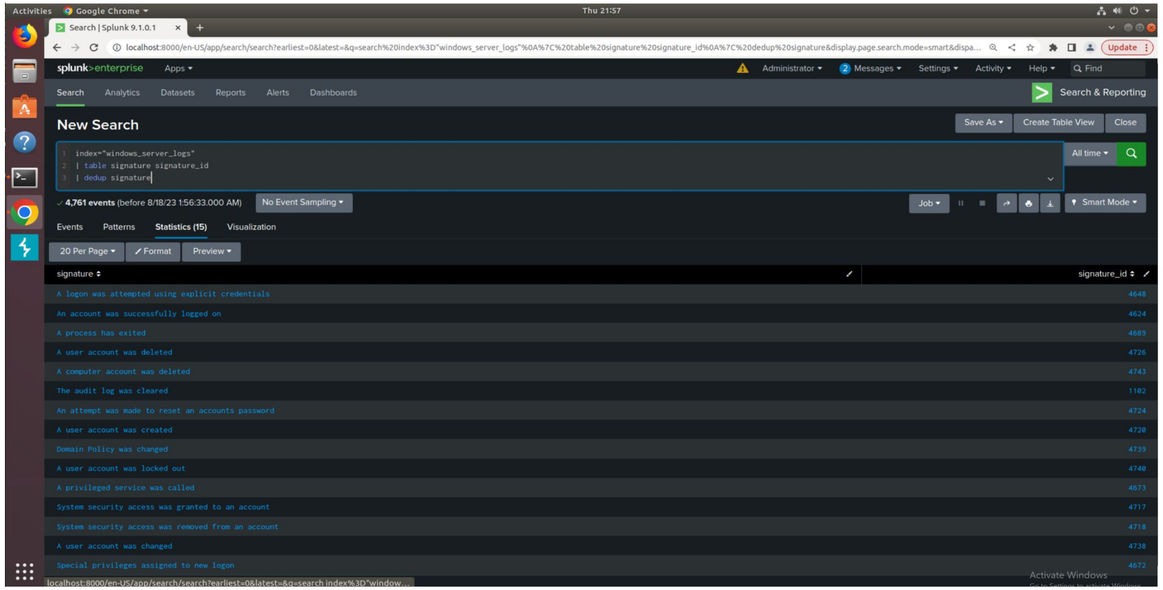
Windows Logs

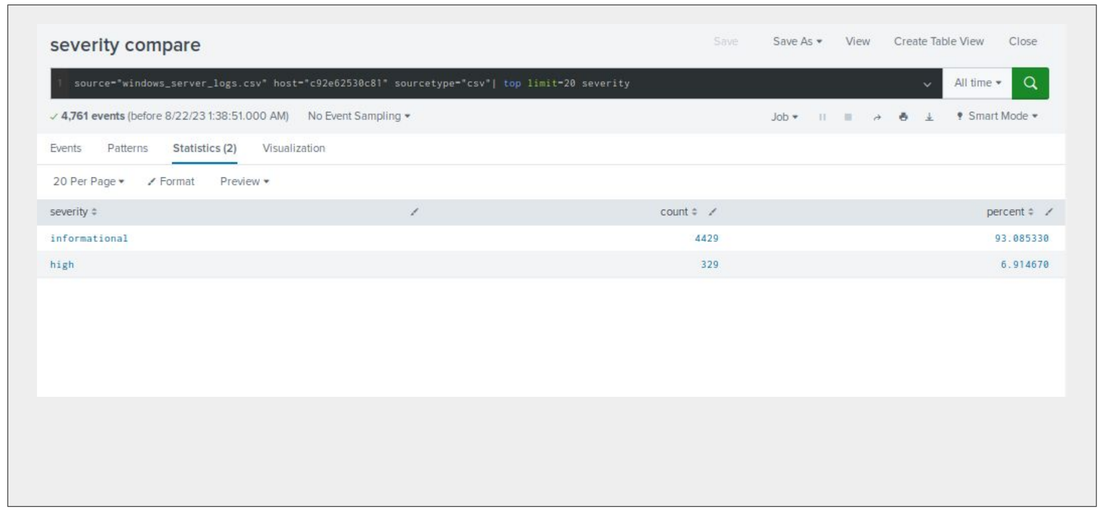
Reports—Windows

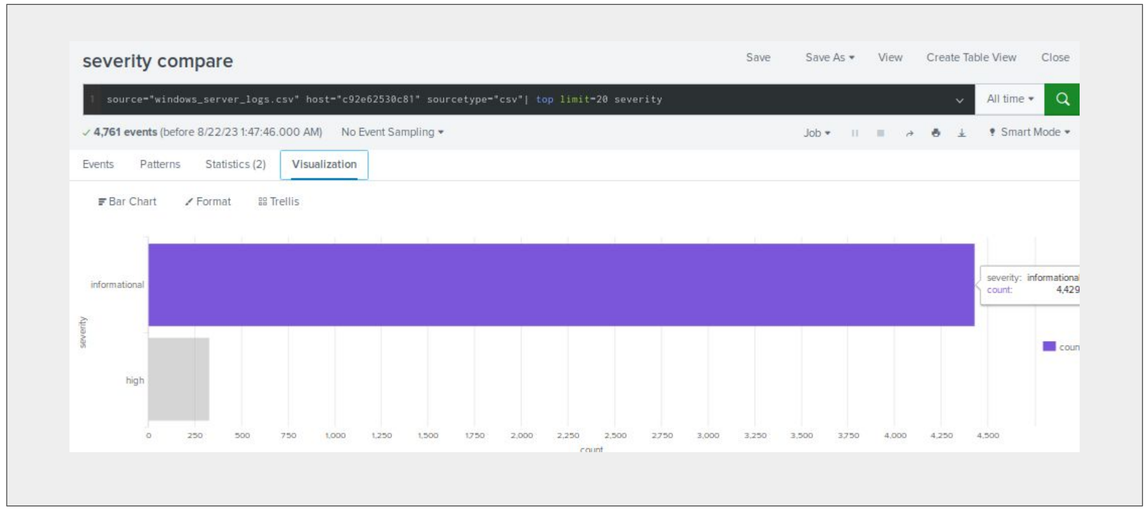
Designed the following reports:

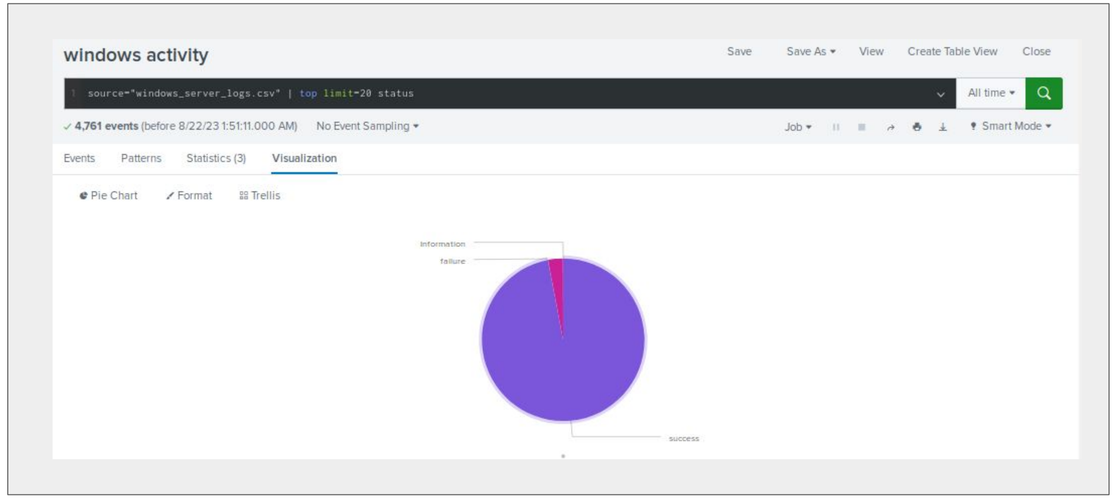
Report Name	Report Description
Signatures & ID’s	Table of Signatures & Assoc. ID’s
Windows Severity	Report of Windows Severity Rate
Windows Success & Failure	Comparison of Success & Failure Rate

Images of Reports—Windows









Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Failed Activity	track activity failure rate	6	13

JUSTIFICATION: 1.5 rule was chosen as an adequate method to account for a 50% increase in expected traffic

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deletion	tracks volume of account deletion	13	20

JUSTIFICATION: 1.5 rule was chosen as an adequate method to account for a 50% increase in expected traffic

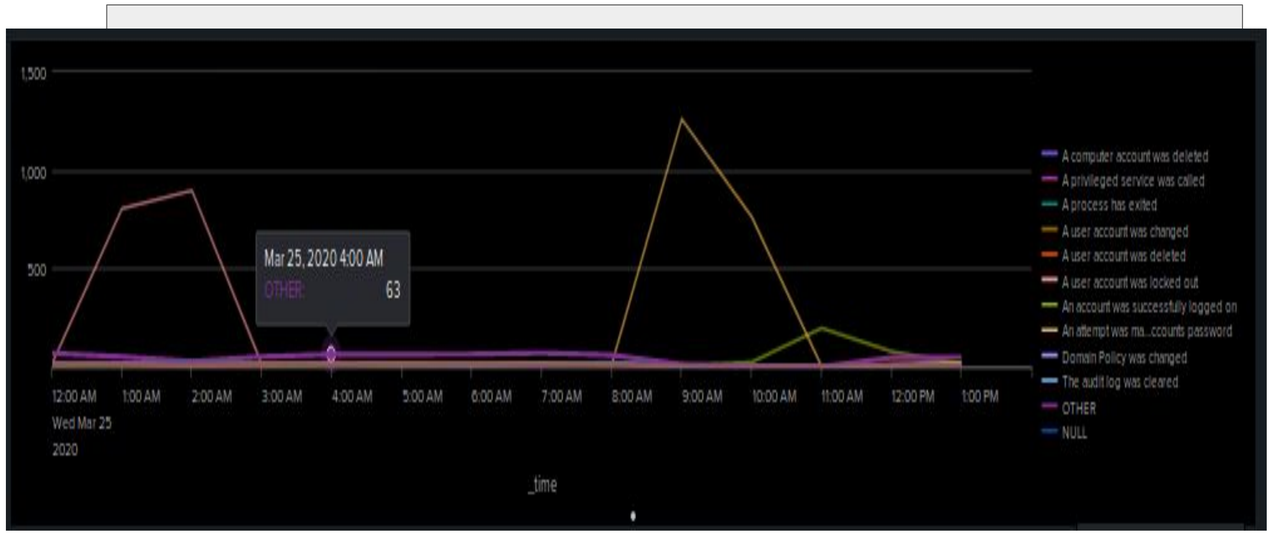
Alerts—Windows

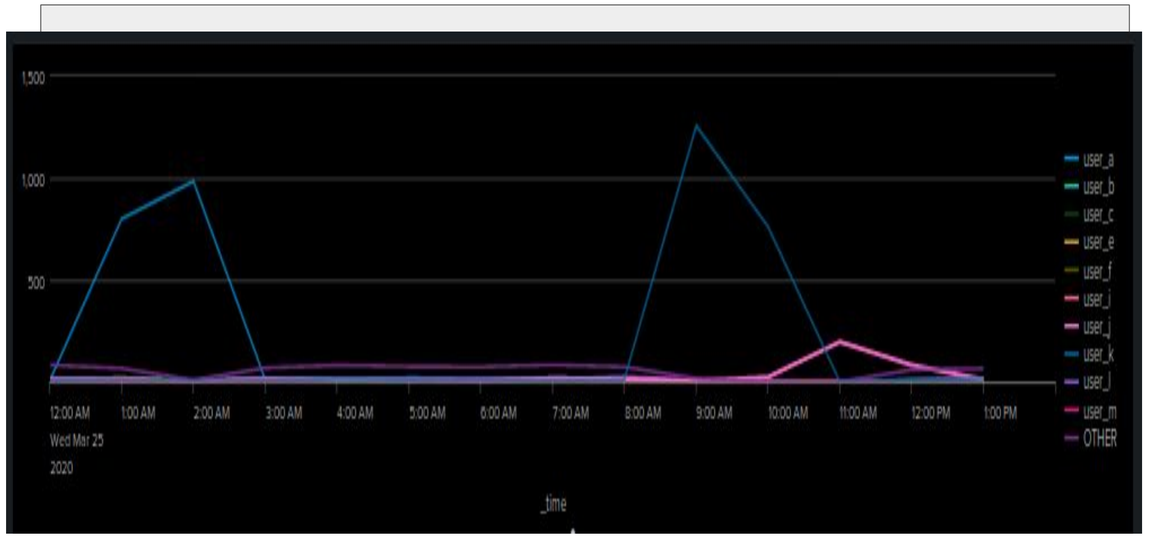
Designed the following alerts:

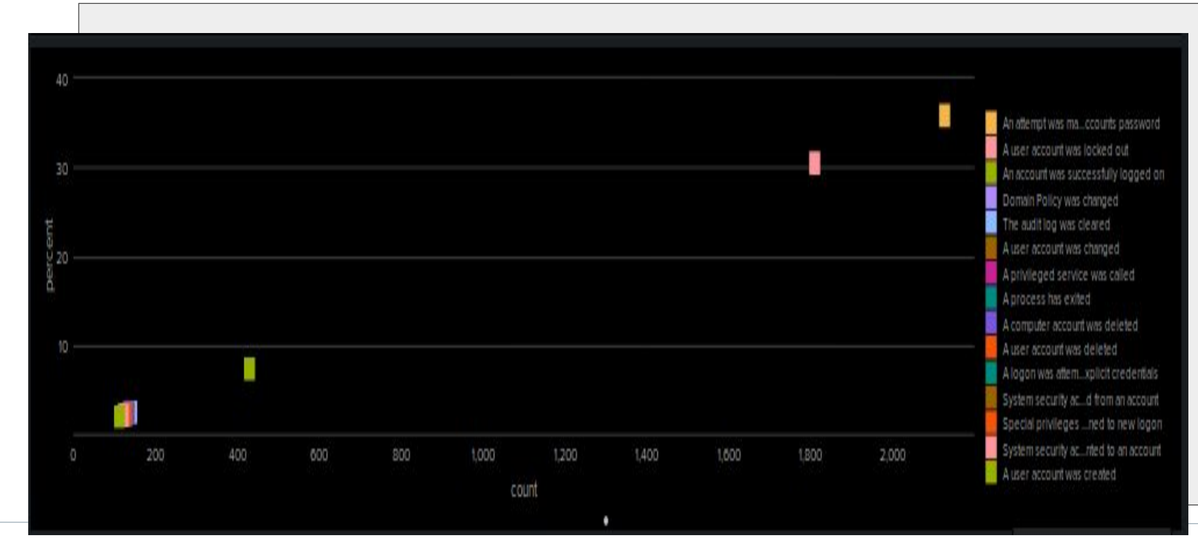
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive Logins	Alert an Abnormal amount of Successful logins within an hourly period.	27.3 hr	32 hr

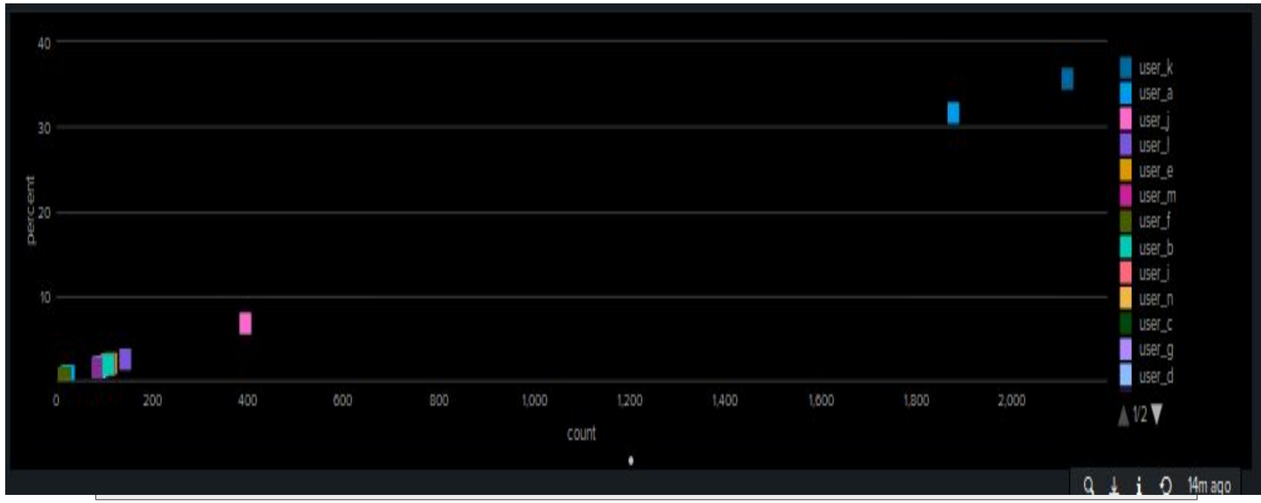
JUSTIFICATION: Baseline is the average per hour. Threshold is anything above 1 standard deviation. (4.6)

Dashboards—Windows









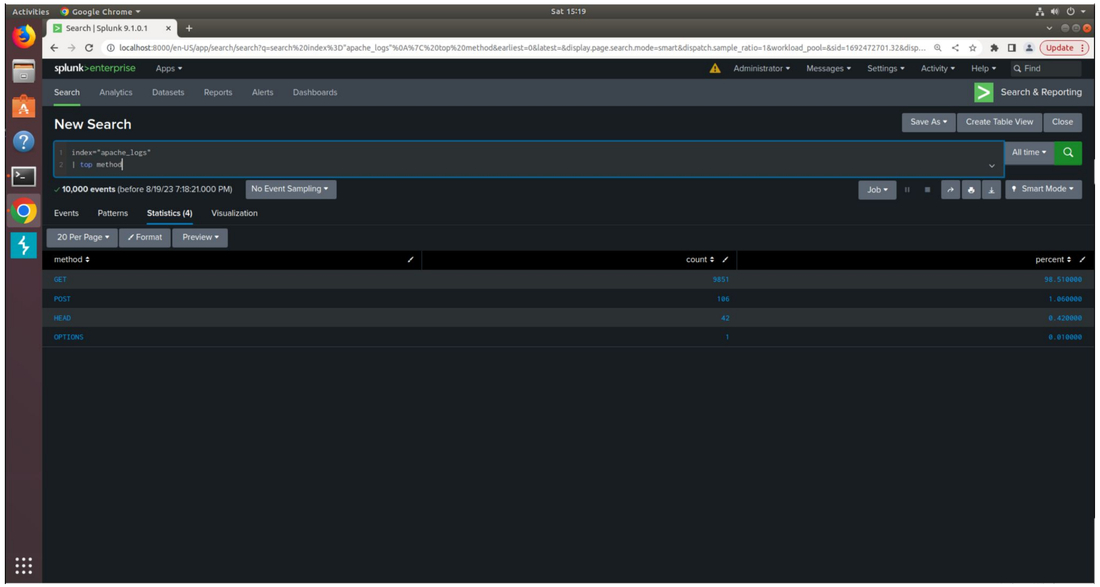
Apache Logs

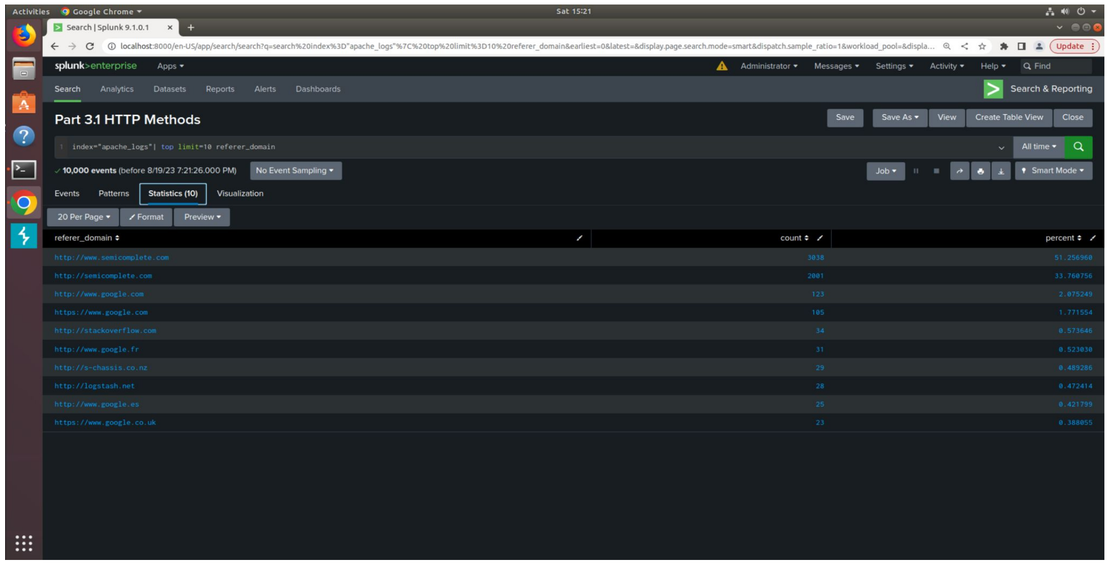
Reports—Apache

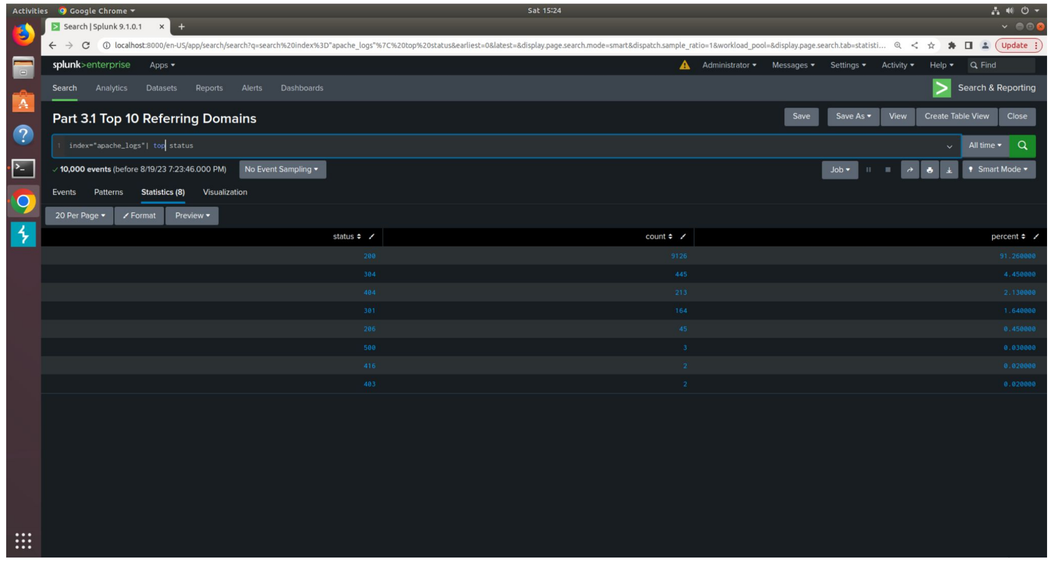
Designed the following reports:

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 Comments	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 averaged around three. Choosing five will capture those instances where the events exceed the average threshold.

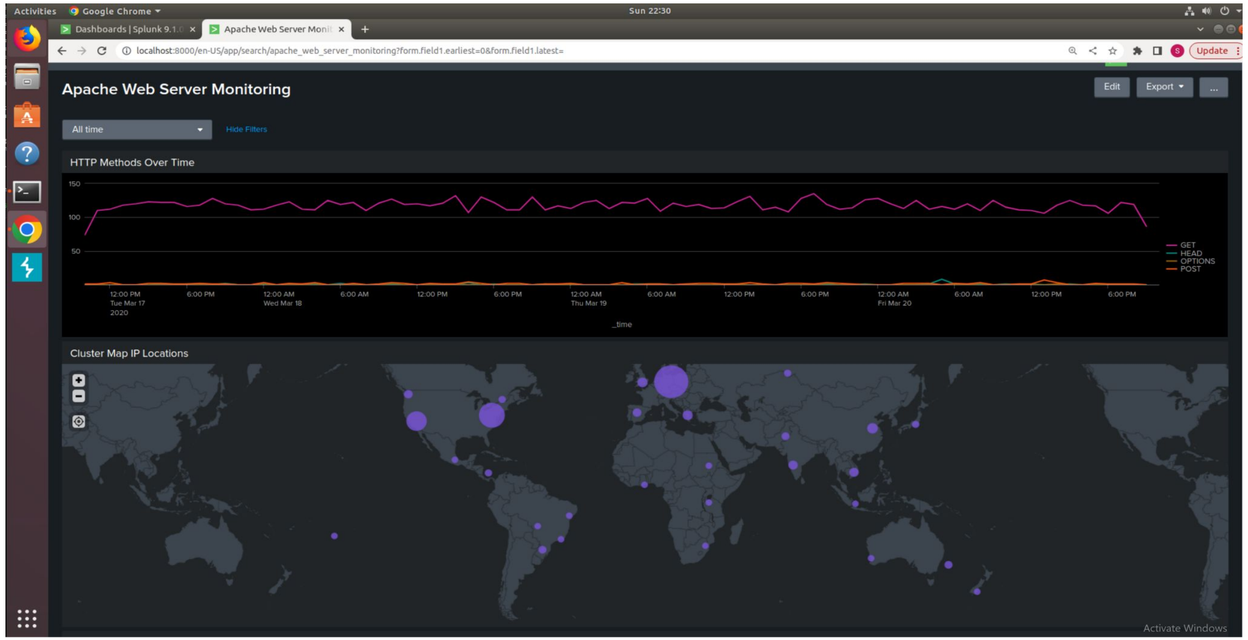
Alerts—Apache

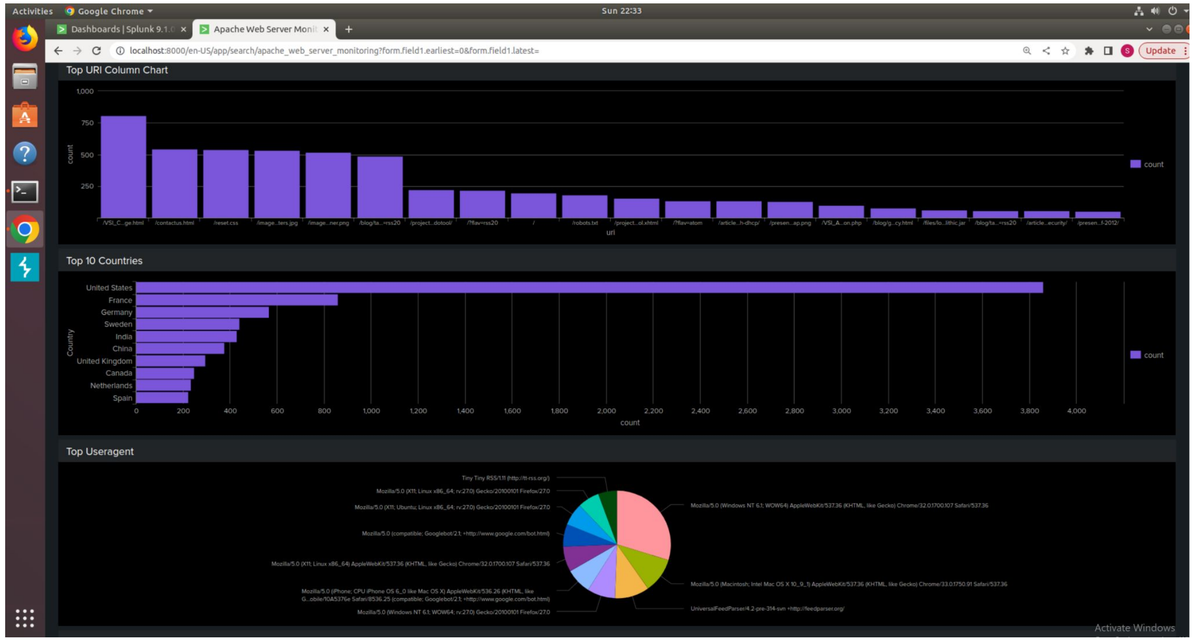
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
apache alert	tracks international activity	73	110

JUSTIFICATION: The 1.5 rule accounts for a 50% increase in expected traffic compared to the baseline.

Dashboards—Apache





Attack Analysis

Attack Summary—Windows

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

- Saw an increase of roughly 12% in HIGH severity alerts during time of attack.
  - This could indicate that the system experienced a higher number of serious issues or threats during the attack.
- A 1% increase in failed Windows activity wouldn't necessarily mean an attack. However, the count of failed activities at 08:00 on 2020-03-25 is significantly higher than any other hour in the standard and attack log files.

Attack Summary—Windows

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

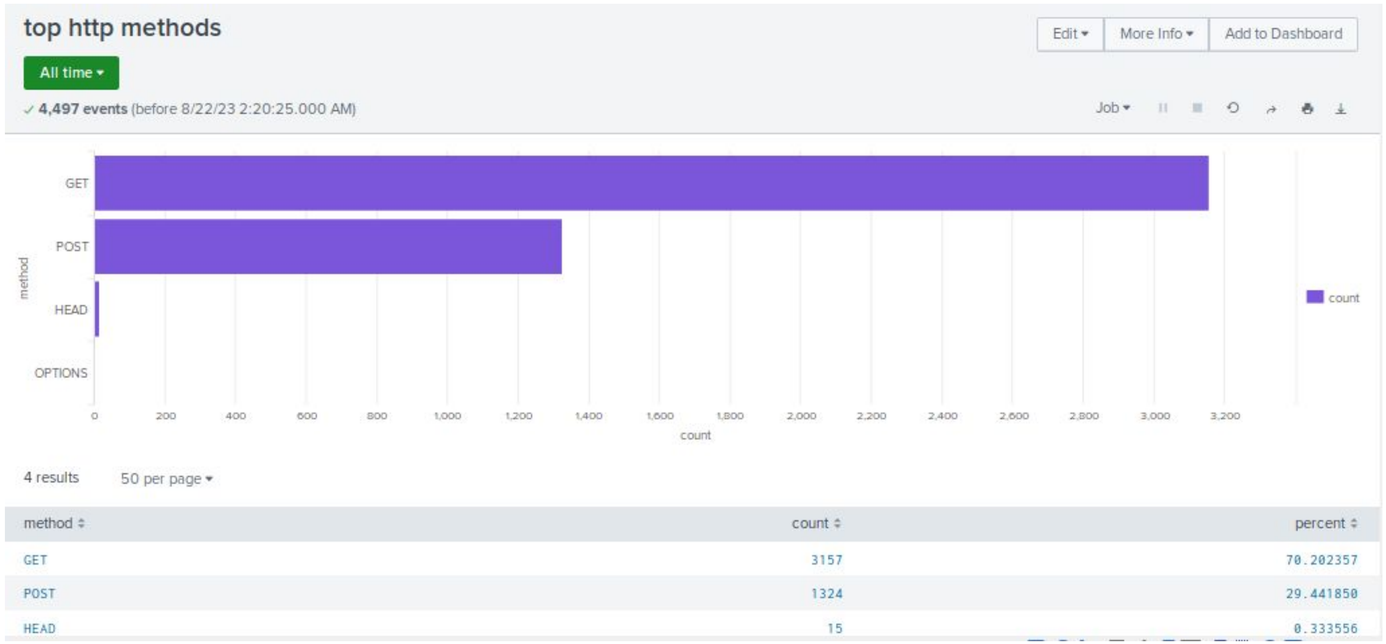
- 18% DECREASE in user account deletions which can indicate a change in normal user activity.
- There were 35 activity failures during the attack at 8am. Before the attack, the normal number of activity failures were 6 at 8am indicating an increase of 29 failed activities.

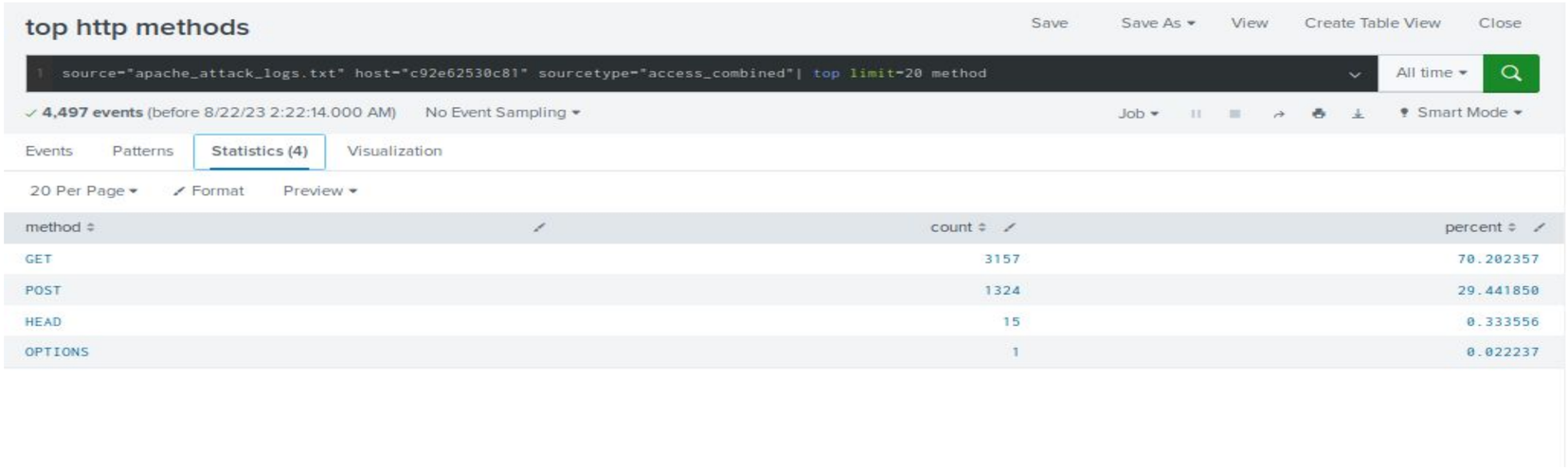
Attack Summary—Windows

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

- Increase of user_k and user_a account utilization.
  - user_k - before attack: 260; during attack: 2,118.
  - user_a - before attack: 282; during attack: 1,878
- 1258 attempts were made to reset passwords on accounts during the time of attack which could indicate that attackers were trying to gain access to VSI systems using user_a and user_k accounts.

Screenshots of Attack Logs





Attack Summary—Apache

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

- Our report analysis of methods saw a spike in GET 6am-7am with the total of 729 and POST from 8pm-9pm with a total of 1,296
- Our referrer domain report analysis helped us determine that the top two hits where www.semicomplete.com and semicomplete.com with counts of 764 and 572.
- Our HTTP response codes report showed 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?

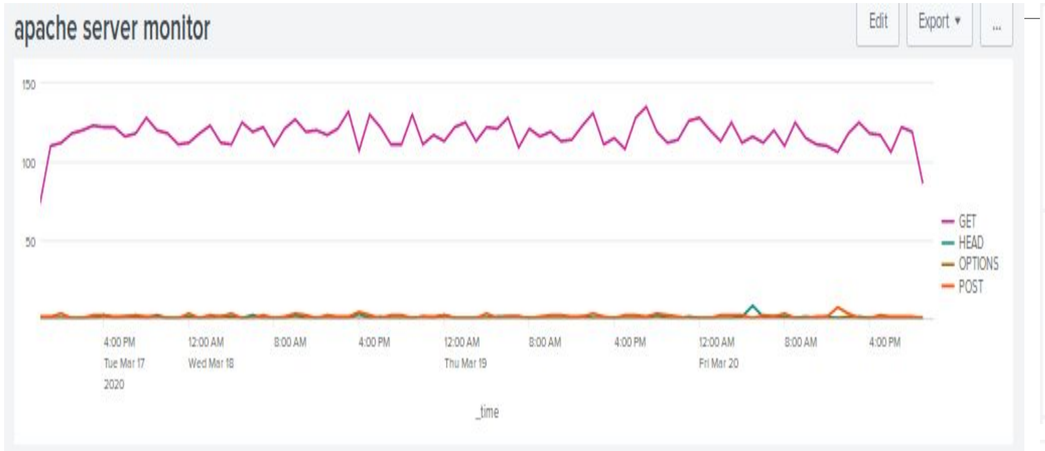
- Alert was set for Hourly activity outside the US. Our baseline was 90 and threshold was 180
- Alert was set for HTTP Post activity. Our baseline was 2 and threshold was 10.

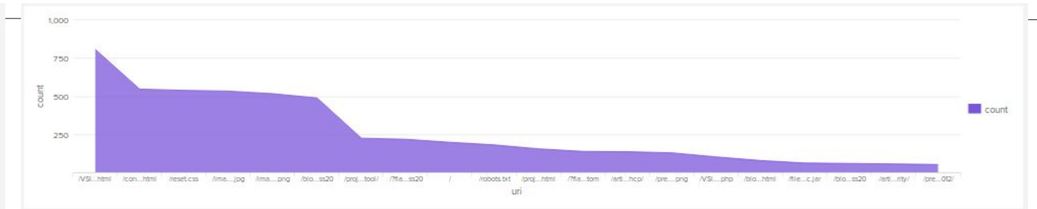
Attack Summary—Apache

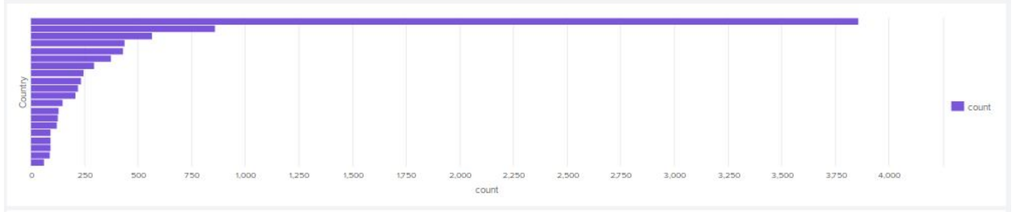
Summarize your findings from your dashboards when analyzing the attack logs.

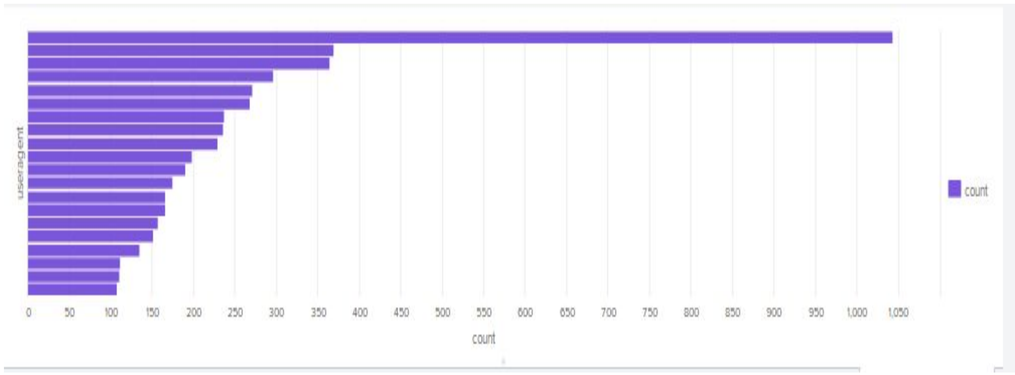
- Time Chart of HTTP Methods: We saw a spike in GETs at 6pm to 729 and a spike in POSTs at 8pm to 1,296
- Cluster Map of Logins: A spike of logins came from Kiev and Kharkiv, Ukraine up to 877
- Top URI Pie Chart: Our VSI_Account_logon.php page with a count of 1323. With that big of a number an attack probably occurred on the page. The possibilities of the attack could have been an LFI, Brute Force, Command Injection,XSS, SQL Injection, and other possible attacks.

Screenshots of Attack Logs









Summary and Future Mitigations

Project 3 Summary

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

  The Apache server experienced a DDOS attack, a majority of the attacks being from Ukraine.

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

Future mitigations against brute force attacks are limiting login attempts to five, increasing password complexity, and implementing Captcha. Blocking incoming traffic from countries that aren't needed is another sound mitigation. We could add input validation, output encoding, and server-side validation for XSS, File Inclusion, SQL Injections, and Command Injection.