Defensive Security Project
by: Aiden, Howard, Baljeet, Ashley

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- We are SOC analysts 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, we are tasked with using Splunk to monitor against potential attacks on VSI’s systems and application
- 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
- Ouur networking team has provided you with past logs to help you develop baselines and create reports, alerts, dashboards, and more!

The following logs have been provided for us:

- **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.

Website Monitoring: App to monitor VSI’s web app

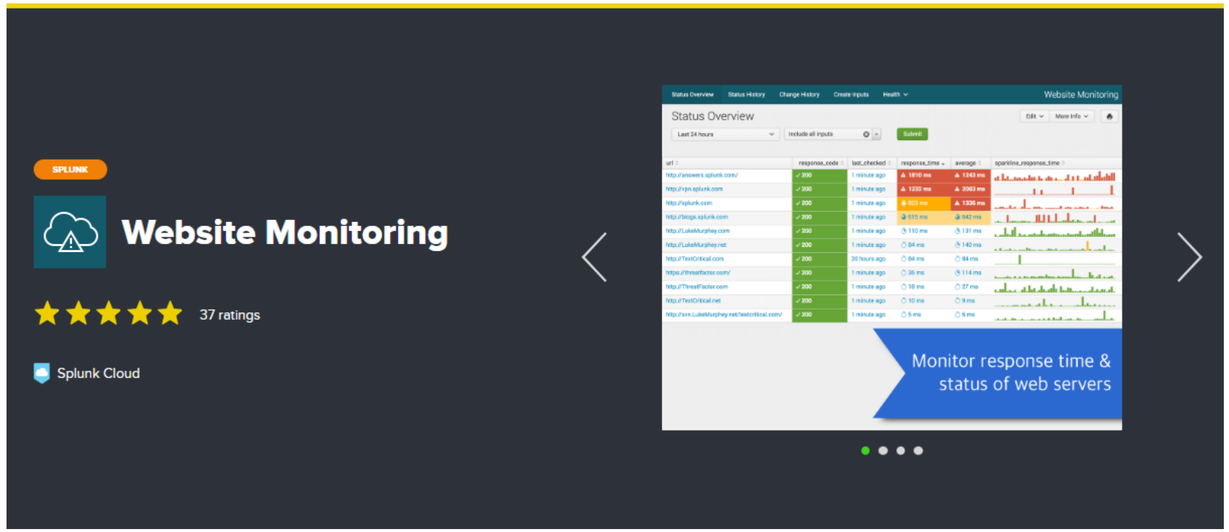
Website Monitoring: App to monitor VSI’s web app

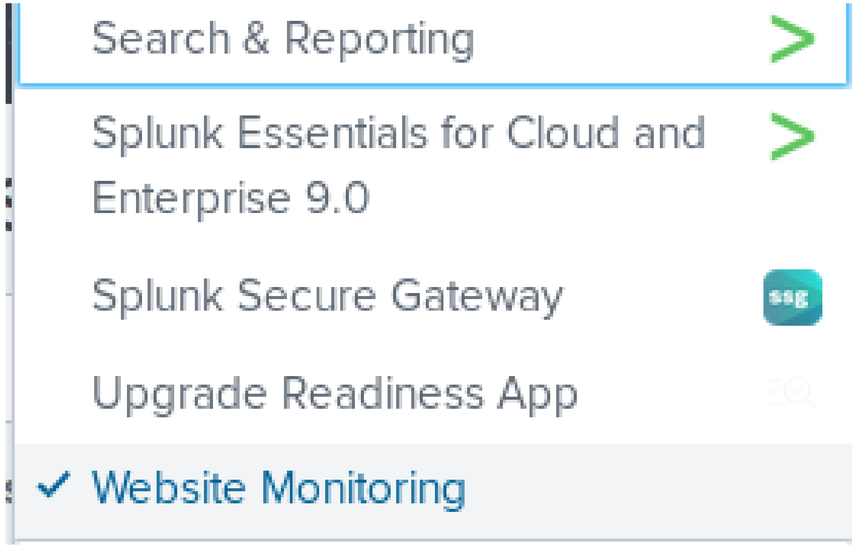
- **Monitor websites to detect downtime and performance problems.**
- **This app uses a modular input that can be setup easily (in 5 minutes or less).**

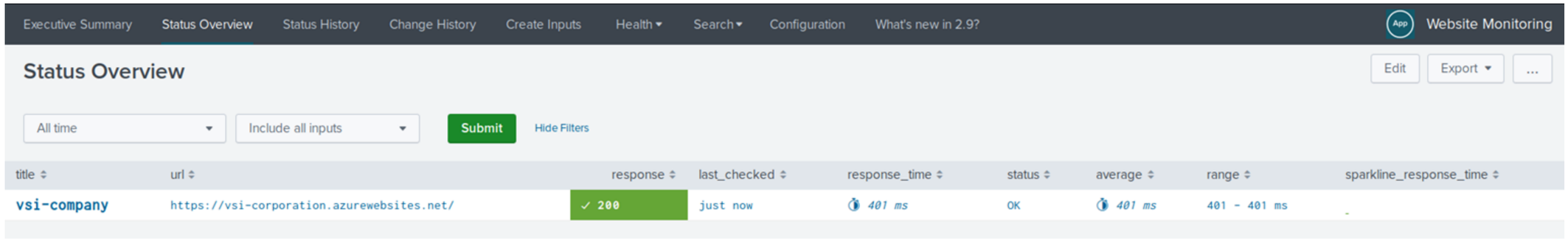
Website Monitoring: App to monitor VSI’s web app

Scenario: JobeCorp, VSI’s adversary, has been known to attack their competitors by launching DDOS attacks to take down their web applications. You will be using this web app to monitor if VSI’s web application is up and functioning.

Website Monitoring: App to monitor VSI's web app







Logs Analyzed

1 Windows Logs

windows_server_logs.csv &
windows_server_attack_logs.csv

Specifically analyzed the following fields:

- signature
- signature_ID
- user
- status
- severity

2 Apache Logs

apache_logs.txt &
apache_attack_logs.txt

Specifically analyzed the following fields:

- method
- referer domain
- status
- clientip
- URI
- useragent

Windows Logs

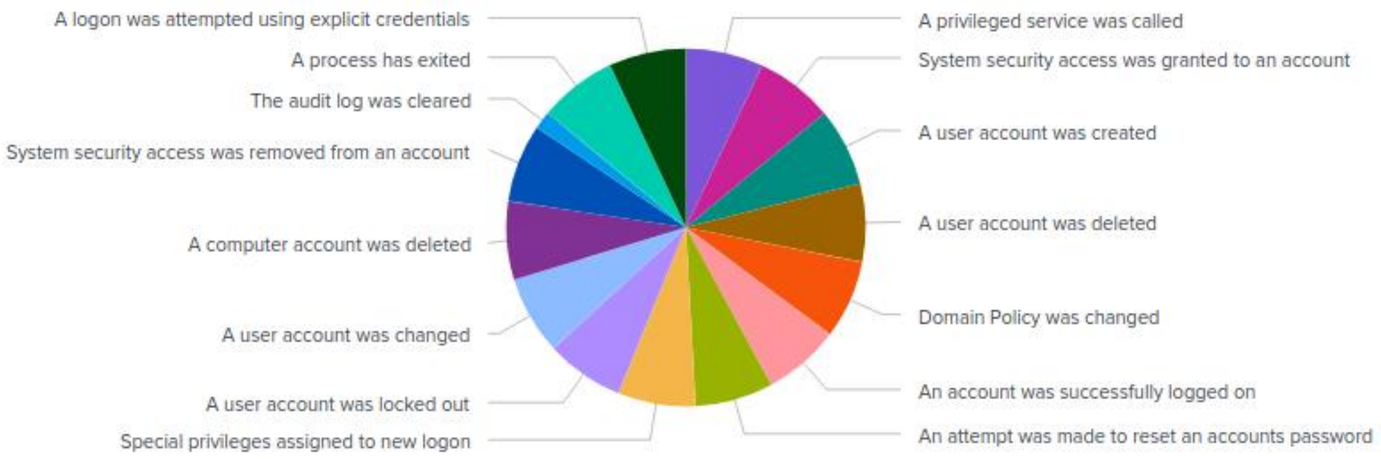
Reports—Windows

Designed the following Reports:

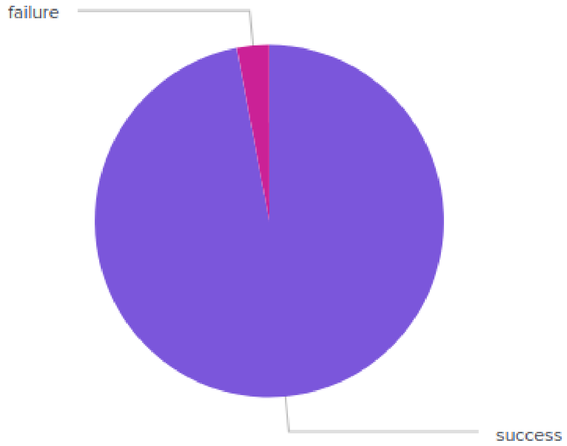
Report Name	Report Description
Signature and Signature ID Report	Table of signatures and corresponding signature IDs present in the logs
Severity Count and Percentage	Count and percentages of severities discovered in logs
Success v Failures Activity	Comparison of success vs failures of windows activities

Images of Reports—Windows

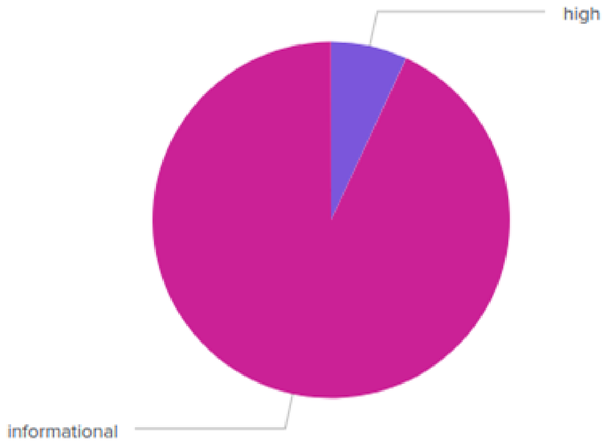
Signature and Signature ID Report



Success v Failures Activity



Severity Count and Percentage



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows_Failed_Activity	Monitors for unusual failed windows activity	6 failed windows activity per hour	8 failed windows activity per hour

JUSTIFICATION: Analyzing normal logs for failed windows activity we discovered that 6 and under is an appropriate baseline while anything over 8 is considered abnormal and is our threshold

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful_Logons	Monitors for abnormal amount of successful logins	13 successful logins per hour	16 successful logins per hour

JUSTIFICATION: Analyzing normal logs for successful windows logins we discovered that 13 and under is an appropriate baseline while anything over 16 is considered abnormal and is our threshold

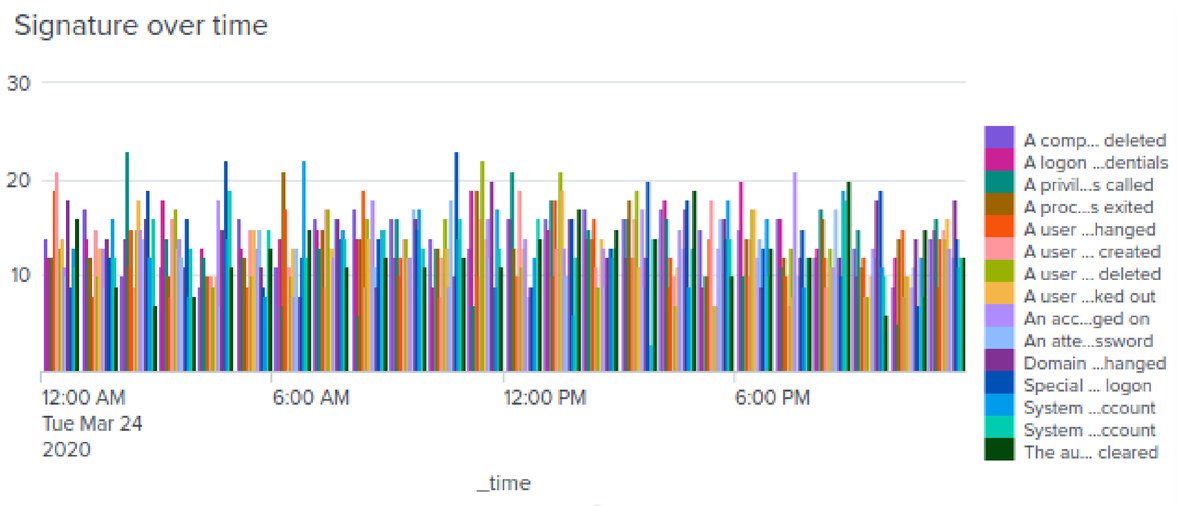
Alerts—Windows

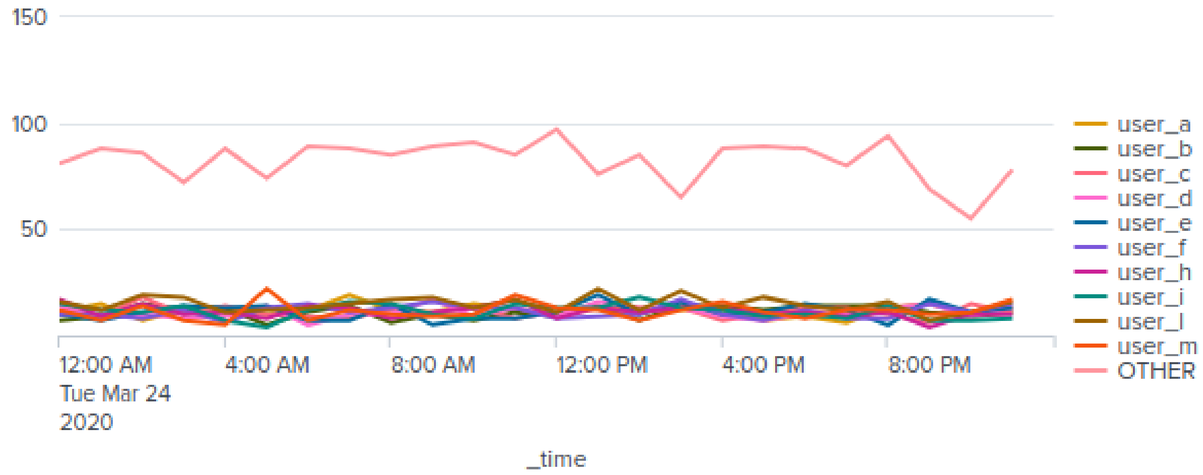
Designed the following alerts:

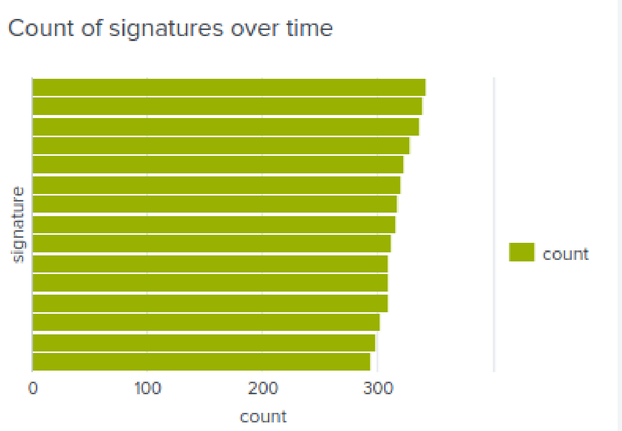
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Deleted_Accounts_Alert	Monitors the amount of deleted accounts in one hour	13 deleted accounts per hour	16 deleted accounts per hour

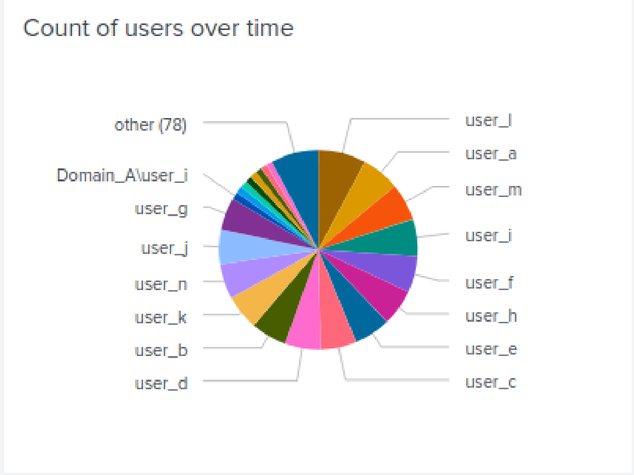
JUSTIFICATION: Analyzing normal logs for deleted user accounts we discovered that 13 and under is an appropriate baseline while anything over 16 is considered abnormal and is our threshold

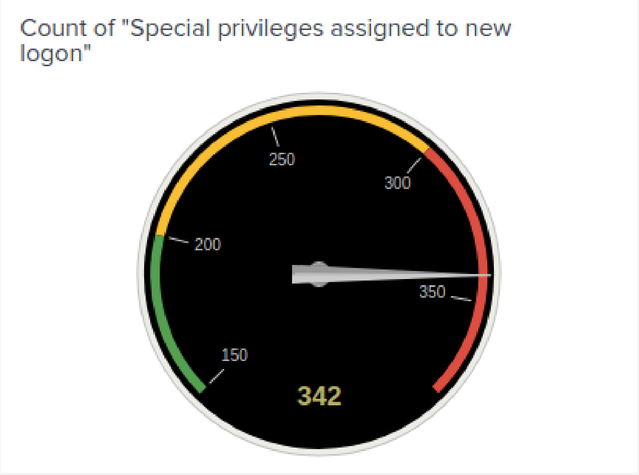
Dashboards—Windows



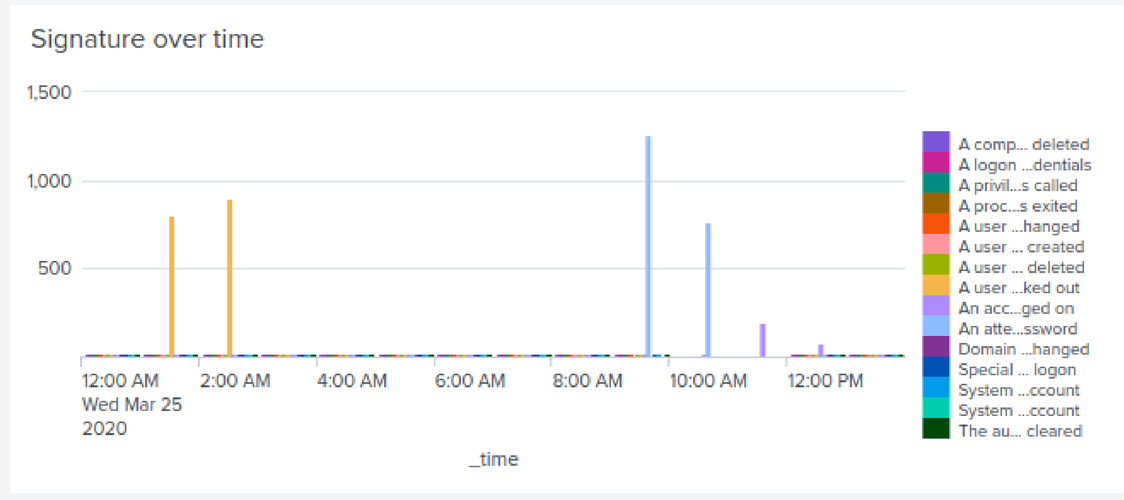


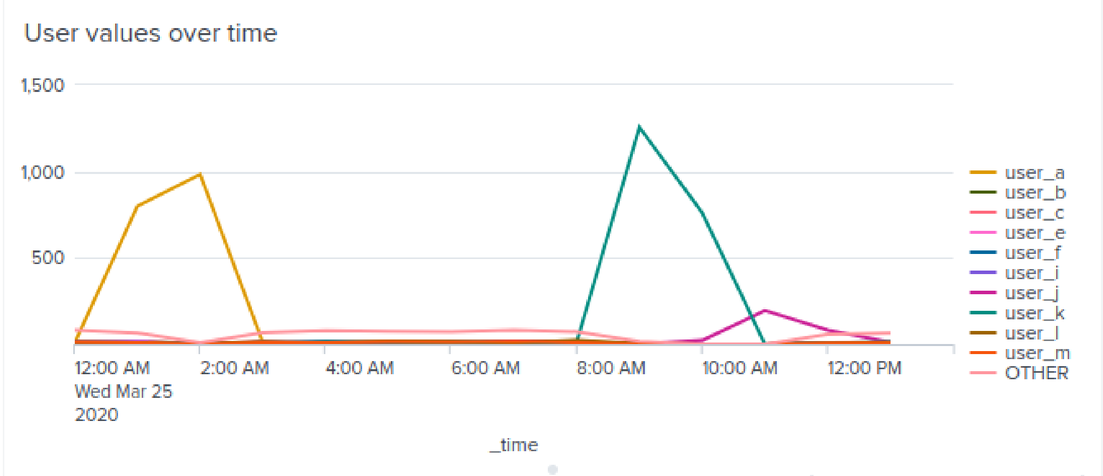


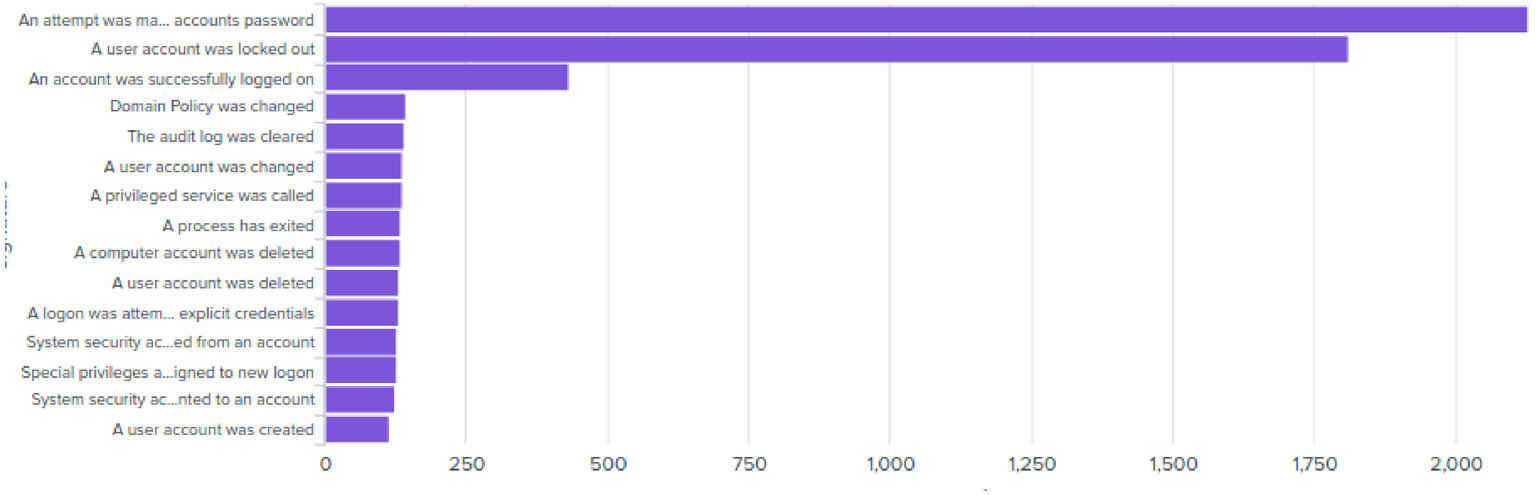


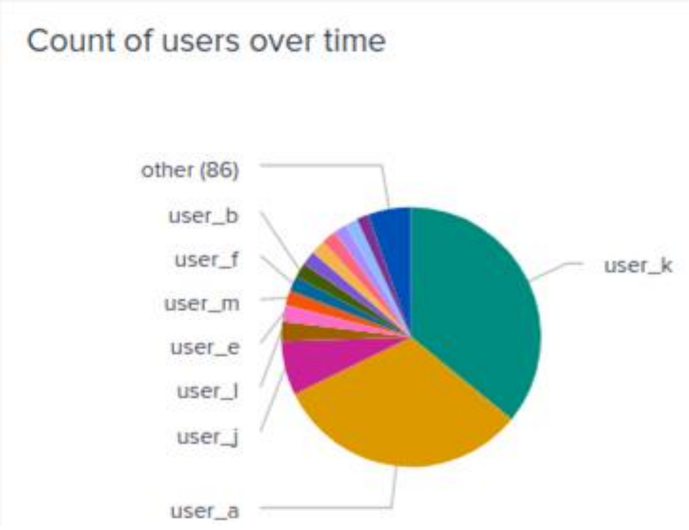


Dashboards—Windows (Attack Log)









Apache Logs

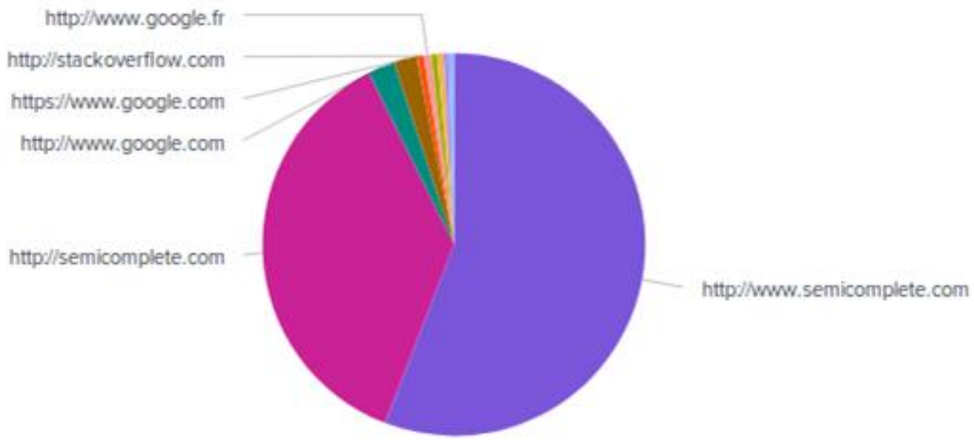
Reports—Apache

Designed the following reports:

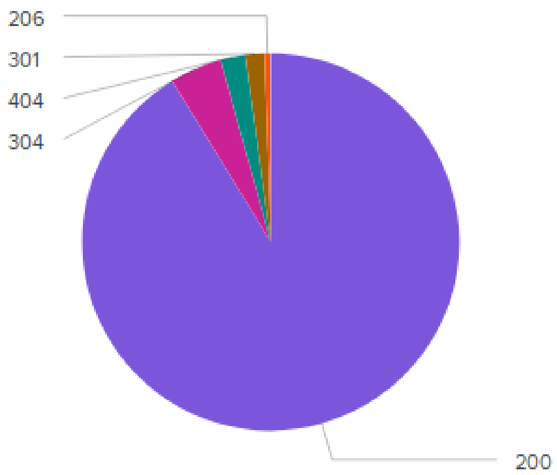
Report Name	Report Description
HTTP Methods	Table of different HTTP methods and their count
Top 10 Domains	Top 10 domains that refer to VSI’s website
HTTP Responses	Count of each HTTP response code

Images of Reports—Apache

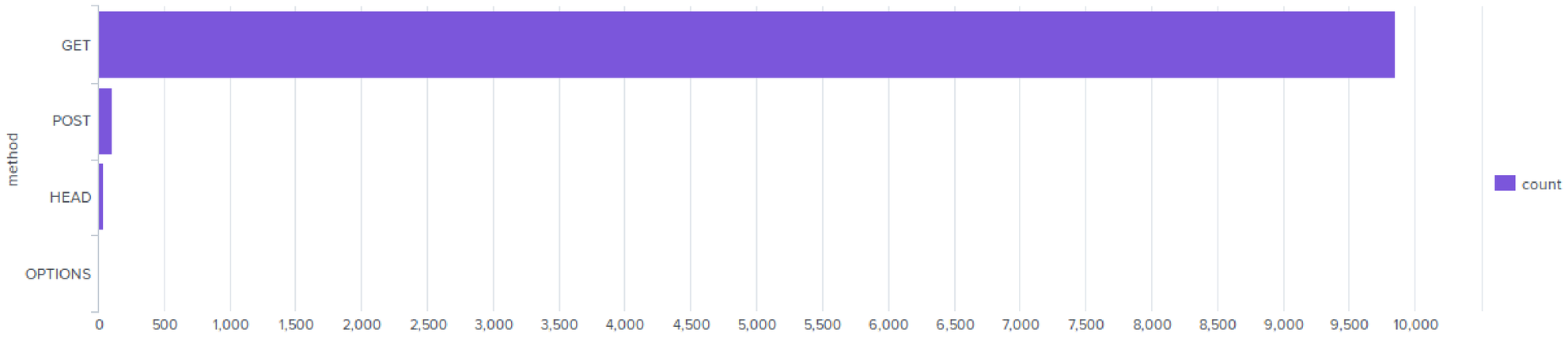
Top 10 Domains



HTTP Responses



HTTP Methods



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Foreign_Activity	Monitors activity sourced outside of U.S.	15 events of activity each hour	23 events of activity each hour

JUSTIFICATION: Analyzing normal log activity, we determined that 15 events of foreign activity is appropriate, and therefore our baseline, while 23 events of foreign activity is abnormal, and therefore our threshold.

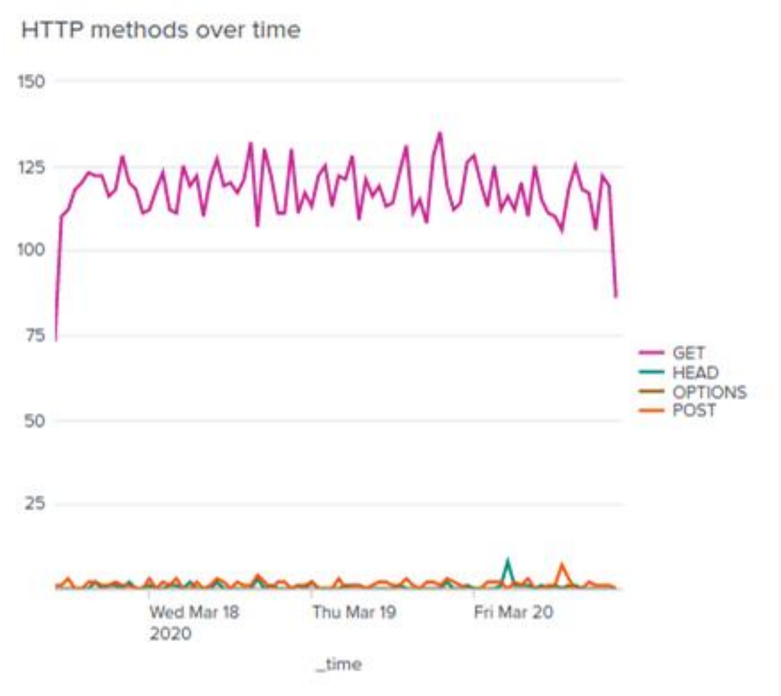
Alerts—Apache

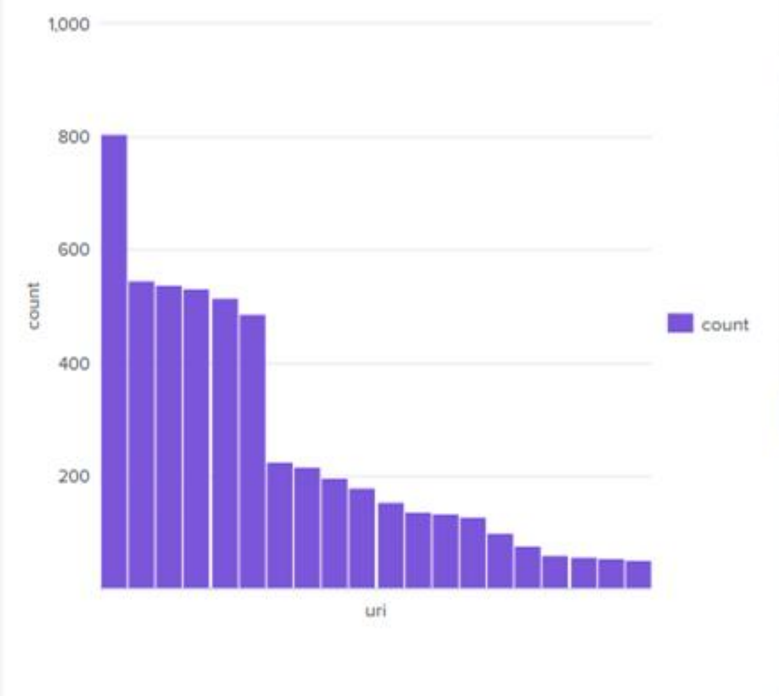
Designed the following alerts:

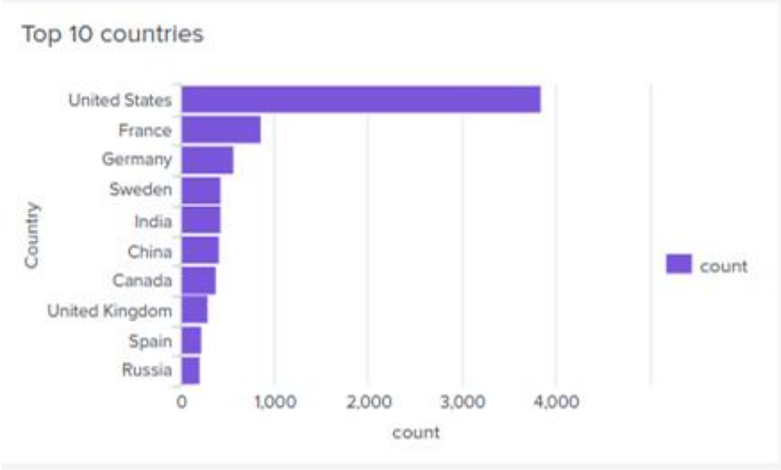
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Post Requests	monitors hourly amount of post requests against apache server	3 post requests per hour	5 posts requests per hour

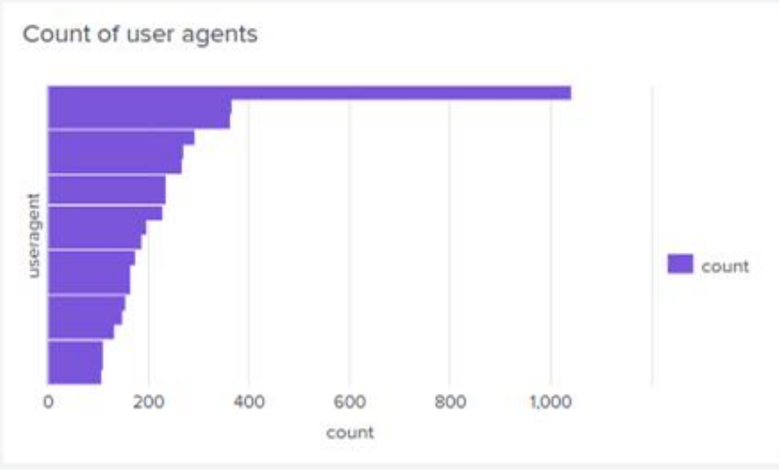
JUSTIFICATION: Analyzing normal log behavior

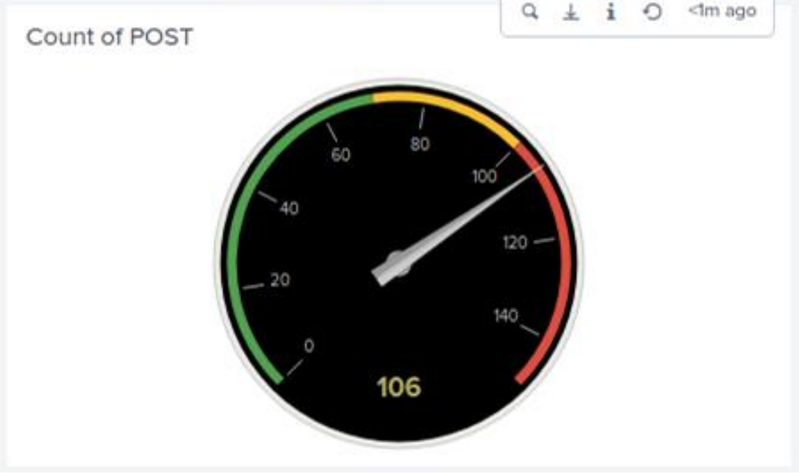
Dashboards—Apache



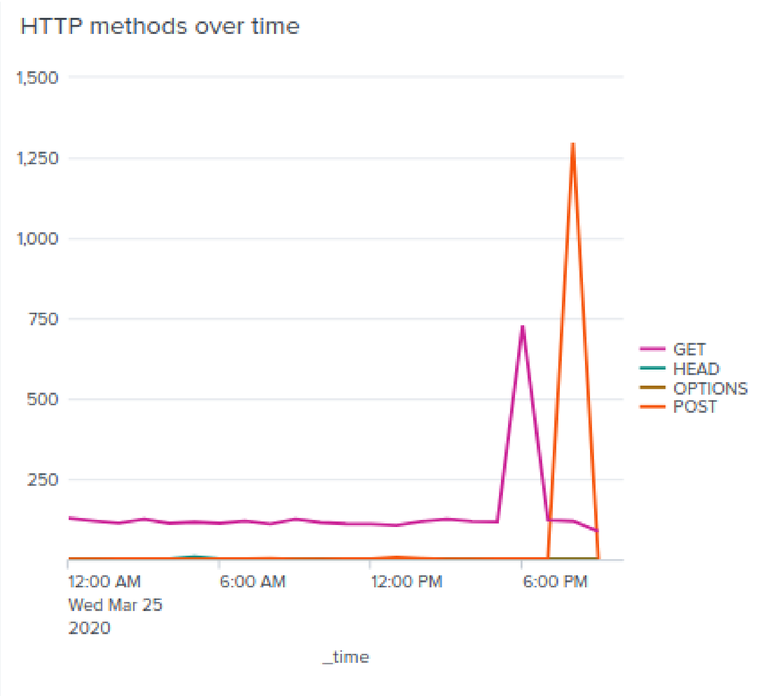


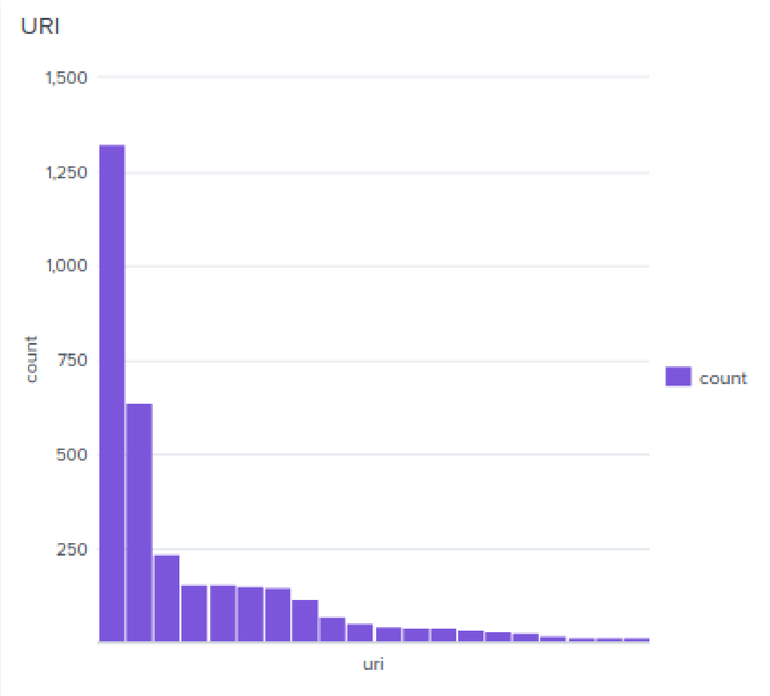


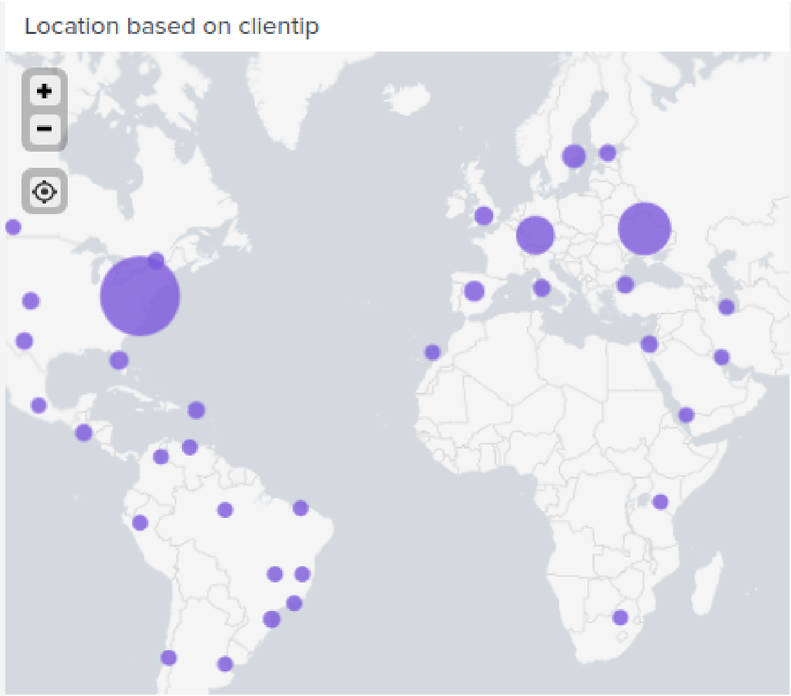


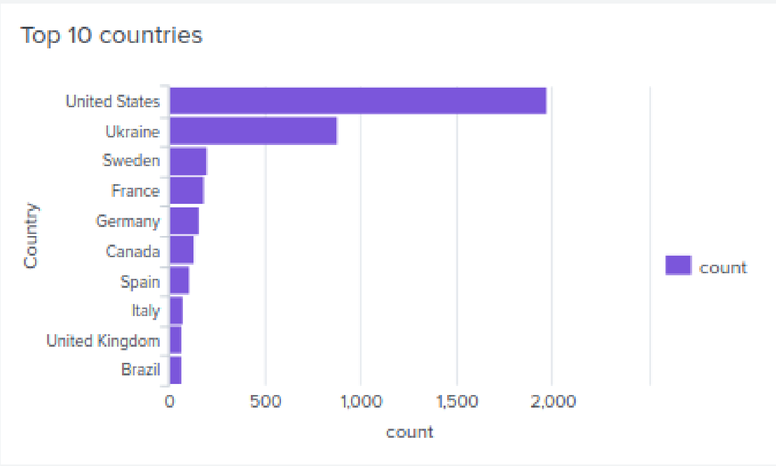


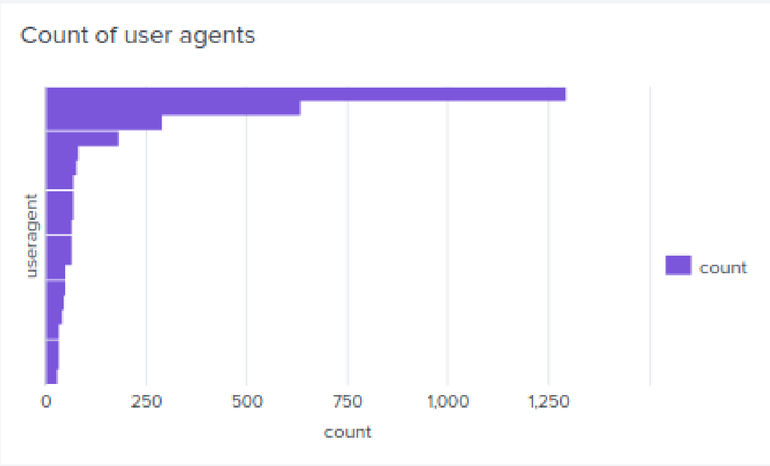
Dashboards—Apache (Attack Log)

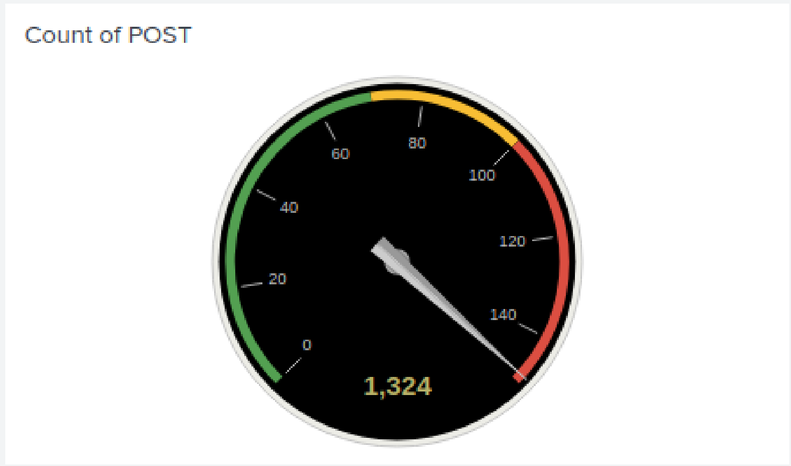










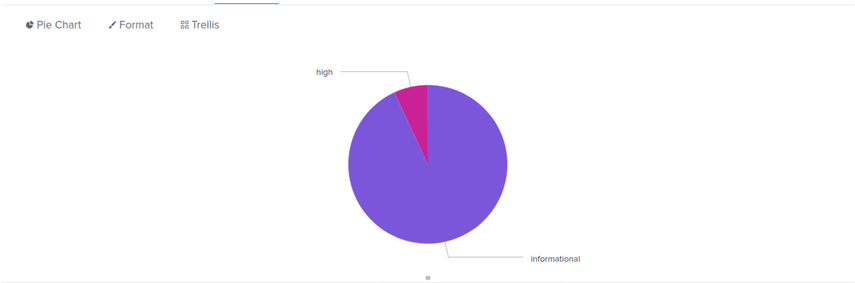


Attack Analysis

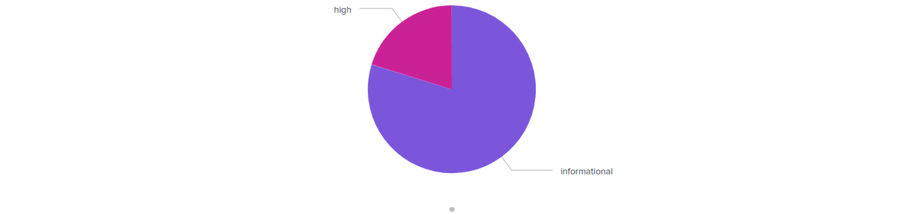
Attack Summary—Windows

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

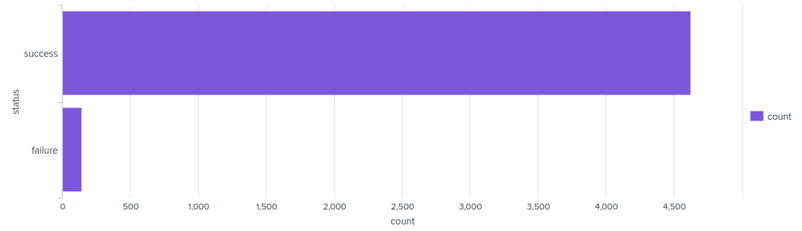
- High severity changed from 329 to 1111 (6.9%-20.2%)
- No significant changes in failed activity. Decreased from (142 to 93)
    - *Note - Total total activity increased by 1185 in the attack logs.



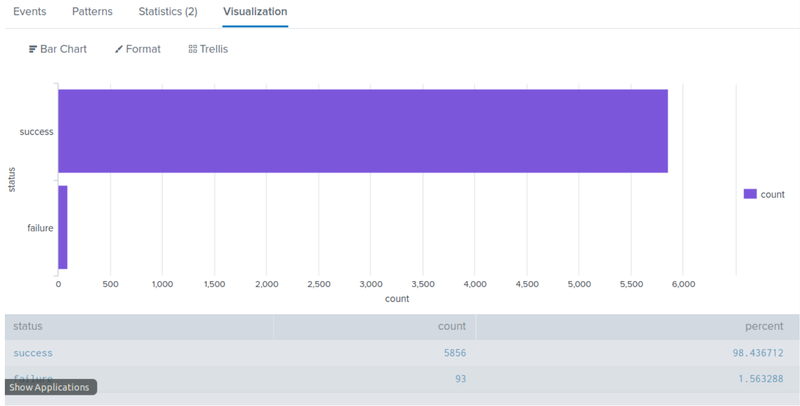
severity	count	percent
informational	4435	93.094039
high	329	6.905961



severity	count	percent
informational	4383	79.777940
high	1111	20.222060



status	count	percent
success	4622	97.019312
failure	142	2.980688

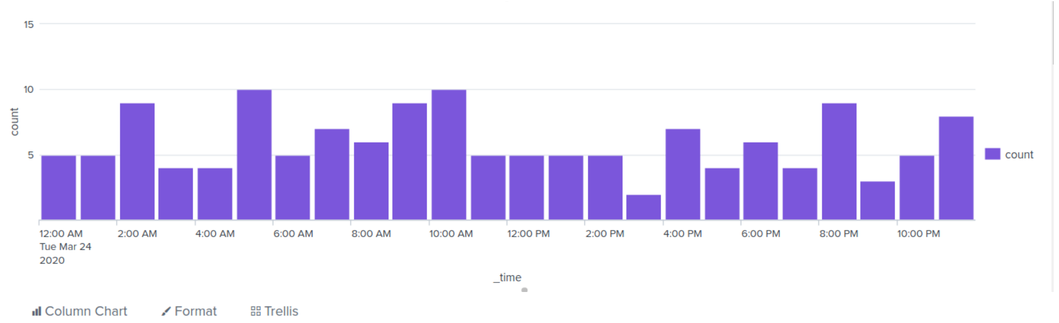


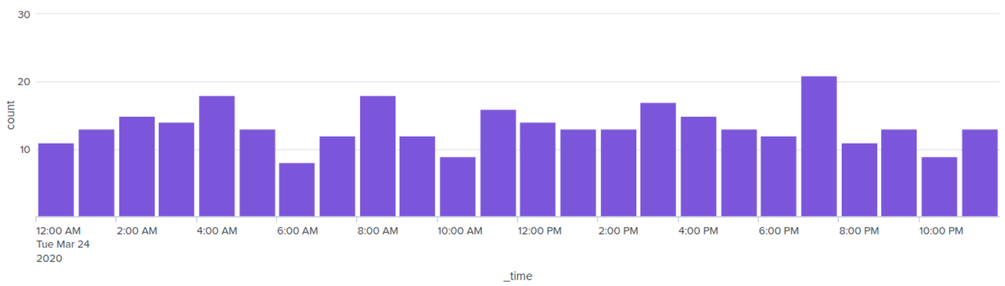
status	count	percent
success	5856	98.436712
failure	93	1.563288

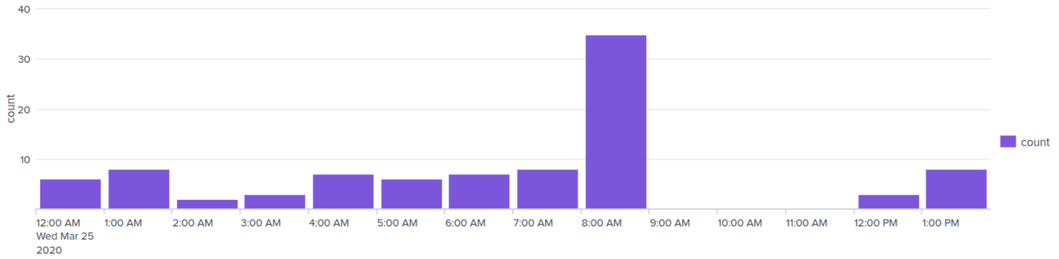
Attack Summary—Windows

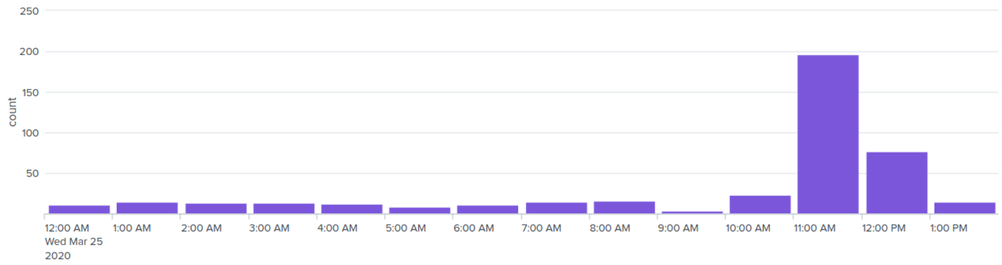
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- Between 8AM - 9AM, failed windows activity spiked to 35.
- Our threshold for the alert was 8, and it would've triggered the alert.
- Between 11am - 1pm, successful logins spiked to 196 and 76 the next hour, then reverted closer to our baselines afterwards.
  - user_j was the primary user logging in at the time of the spike.
- Our threshold for the alert was 16, and it would've triggered the alert.
- There was no suspicious volume of deleted accounts in the attack logs.







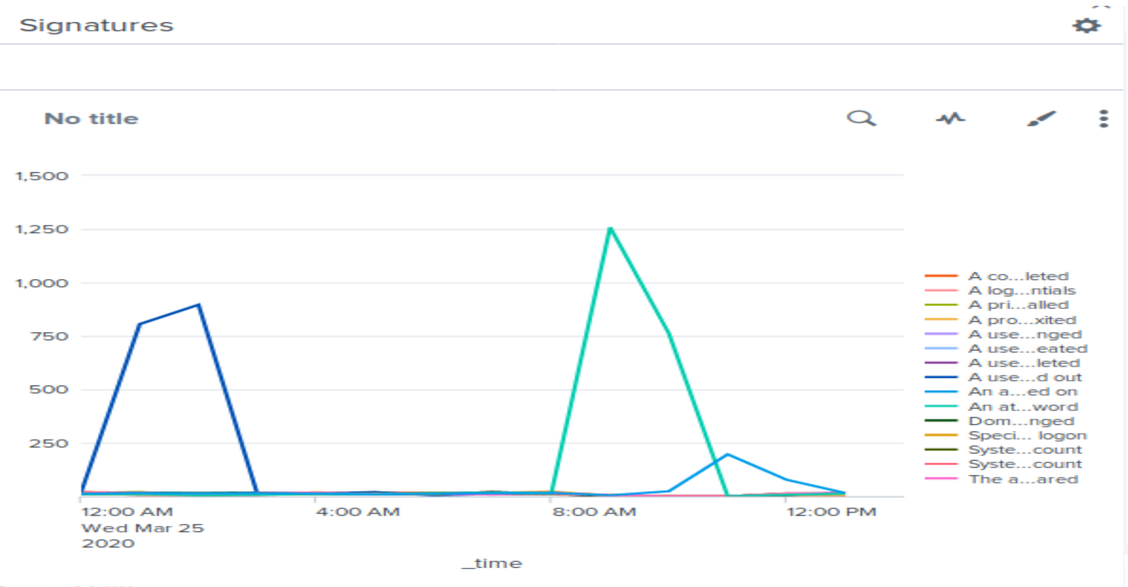


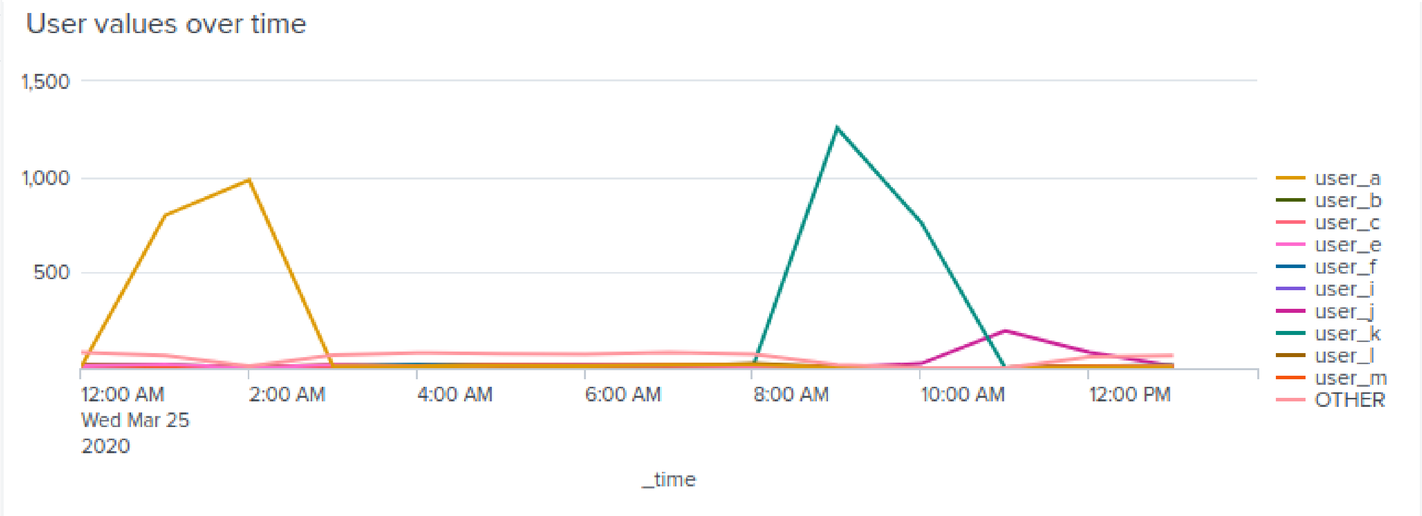
Attack Summary—Windows

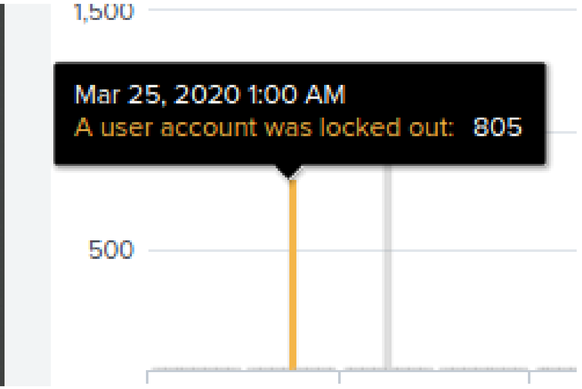
Summarize your findings from your dashboards when analyzing the attack logs.

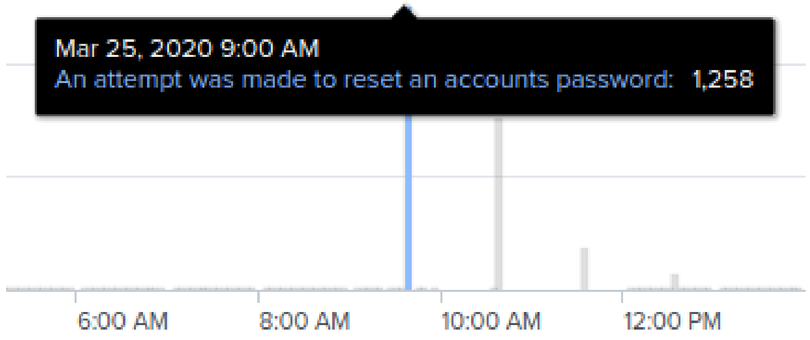
- Between 12 am - 3 am
  - 805
  - events for “A user account was locked out”
  - “user_a” had the most activity during that time period (984)
- Between 9am - 10 am
  - 1258 events for “An attempt was made to reset an accounts password”
  - “user_k” had the most activity during that time period (1256)
- Between 11am -1 pm
  - 196 events for “An account being successfully logged on”
  - “user_j” had the most activity during that time period (196)

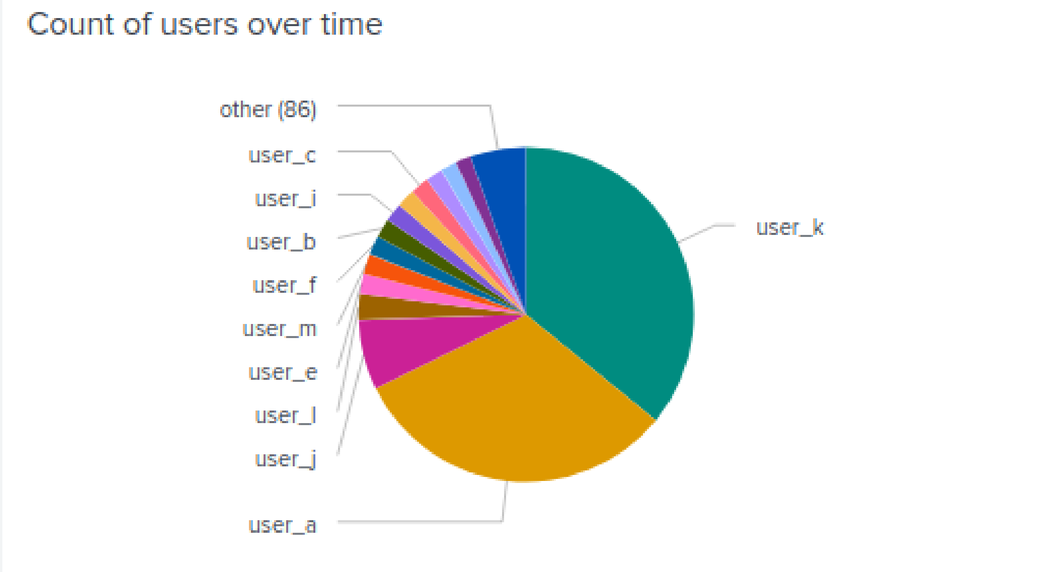
Screenshots of Attack Logs







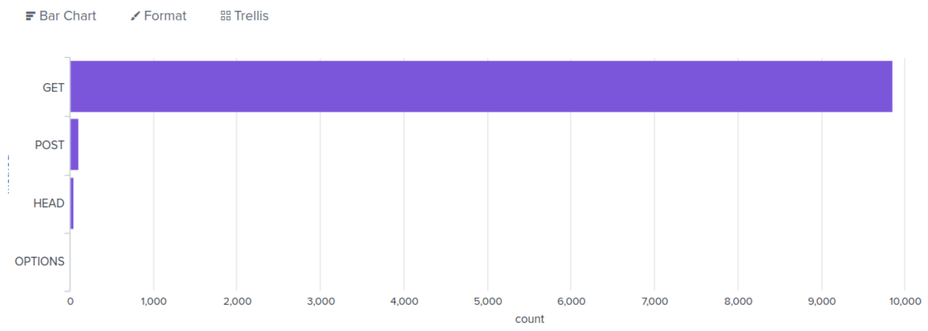


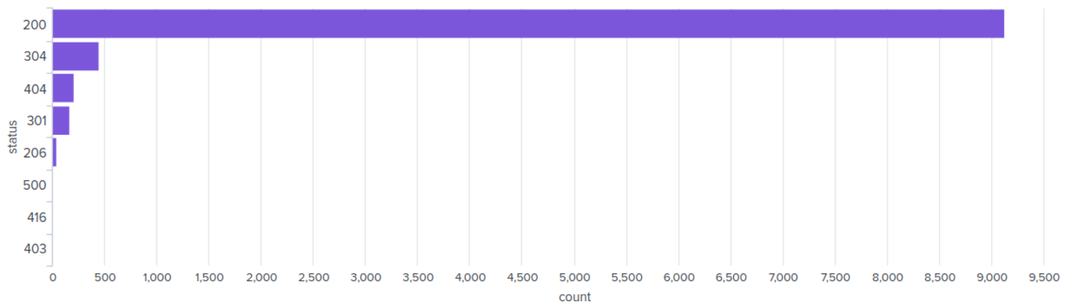


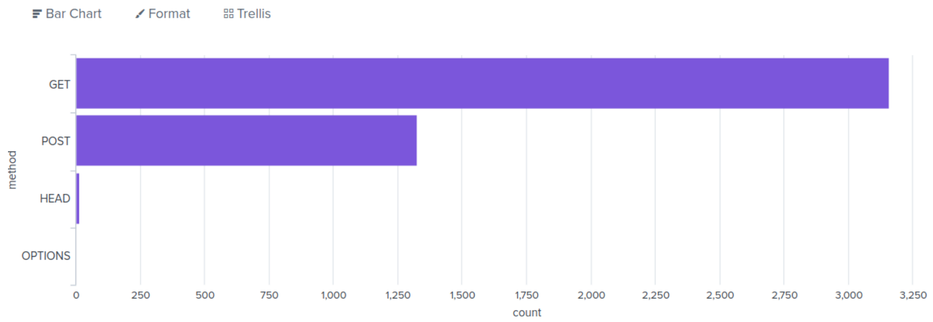
Attack Summary—Apache

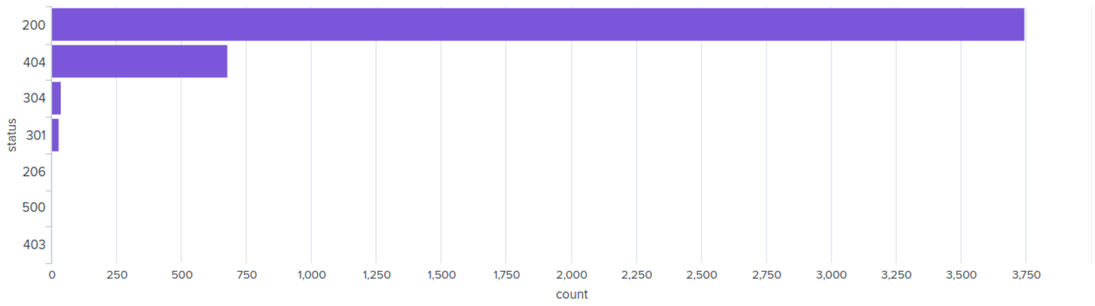
Summarize your findings from your reports when analyzing the attack logs.

- Increase in POST requests from 106 to 1324, decrease in GET responses
- Increase in 404 responses.
  - *Note - 404 responses mean the server cannot find the requested resource.
- No suspicious changes in the referrer domains, but less activity in the attack logs.





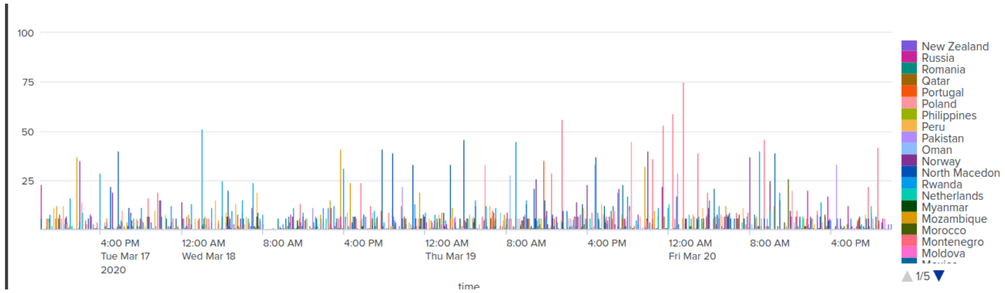


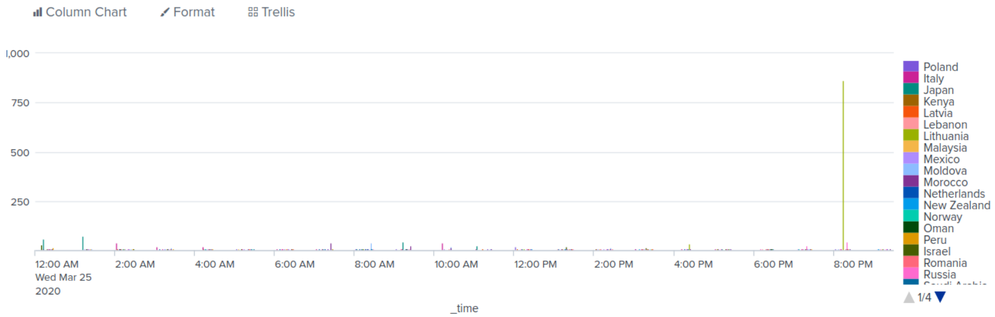


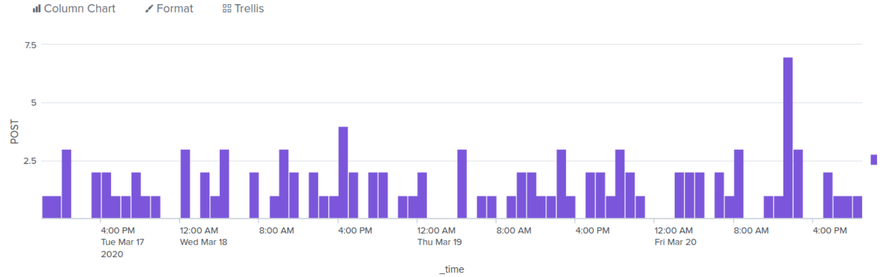
Attack Summary—Apache

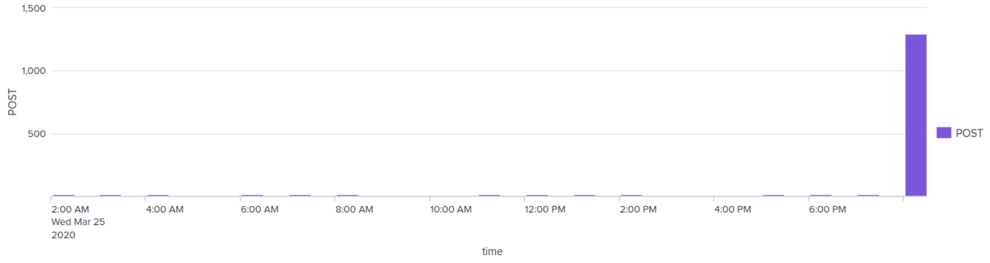
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- There was a spike in international activity at 8PM from Ukraine. 864 event count.
- 23 was our threshold, and it would trigger the alert. We would change the threshold to 45, to prevent any overload in alerts: alert fatigue
- There was also a spike in POST requests at 8 PM.
- 5 was our threshold, and it would trigger the alert.







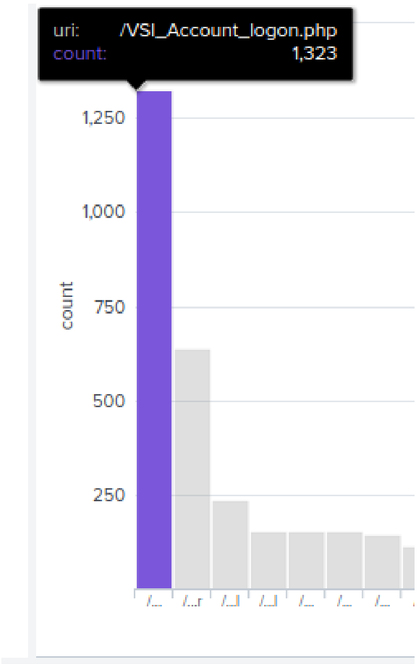


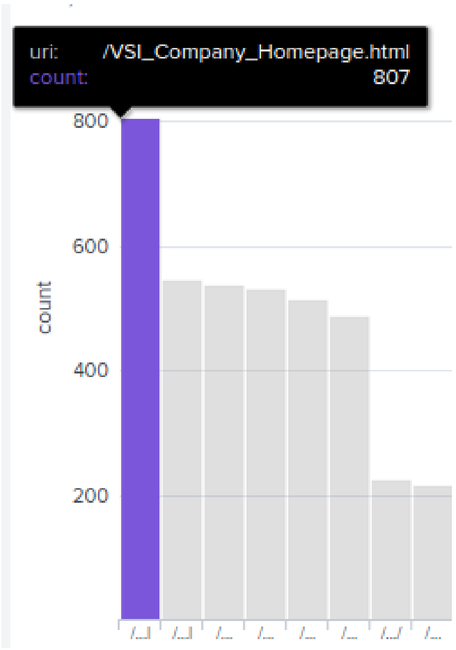
Attack Summary—Apache

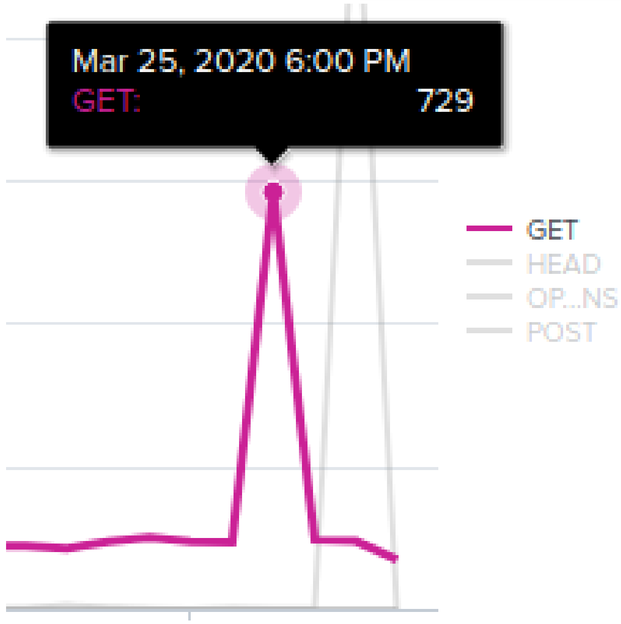
Summarize your findings from your dashboards when analyzing the attack logs.

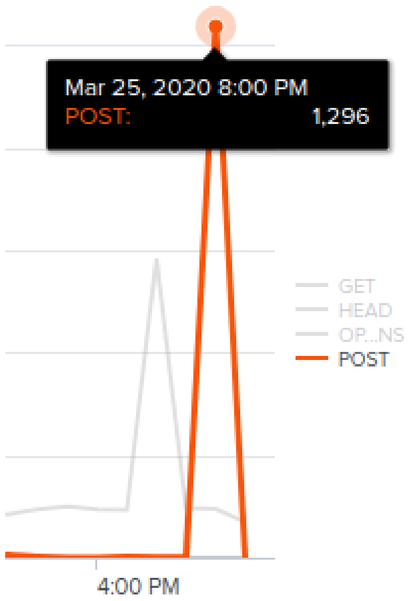
- There is a significant number of GET requests between 6pm and 7pm (729)
- There is a significant number of POST requests between 8pm and 9pm (1296)
- In the cluster map, Ukraine has a high volume of activity
- According to our URI’s, there was an increase of activity in the /VSI_Account_logon.php

Screenshots of Attack Logs









Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
  - ❑It appears to be a brute force attack on Windows Active Domain
  - ❑It appears to be a brute force attack on the web application

- To protect VSI from future attacks, what future mitigations would you recommend?
  - Account lockout
  - Limit login attempts
  - Required stronger password policies
  - Blacklist IPs that have high login attempts