Cybersecurity Attack on VSI
by: Brian Rajaram

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- VSI has recently suffered a slew of cybersecurity attacks, which took down several of it’s systems.
- JobeCorp, one of its competitors, is considered a likely culprit.
- Both Windows and Apache servers were targeted.
- Attack logs have been uploaded to Splunk for analysis.

Logs Analyzed

1 Windows Logs

- Windows_Server_Logs (contains information - such as signature codes and users - about the Windows environment **before** the attack.)
- Windows_Server_Attack_Logs (contains information - such as signature codes and users - about the Windows environment **after** the attack.)

2 Apache Logs

- Apache_Server_Logs (contains information - such as signature codes and users - about the Apache environment **before** the attack.)
- Apache_Server_Attack_Logs (contains information - such as signature codes and users - about the Apache environment **after** the attack.)

Windows Logs

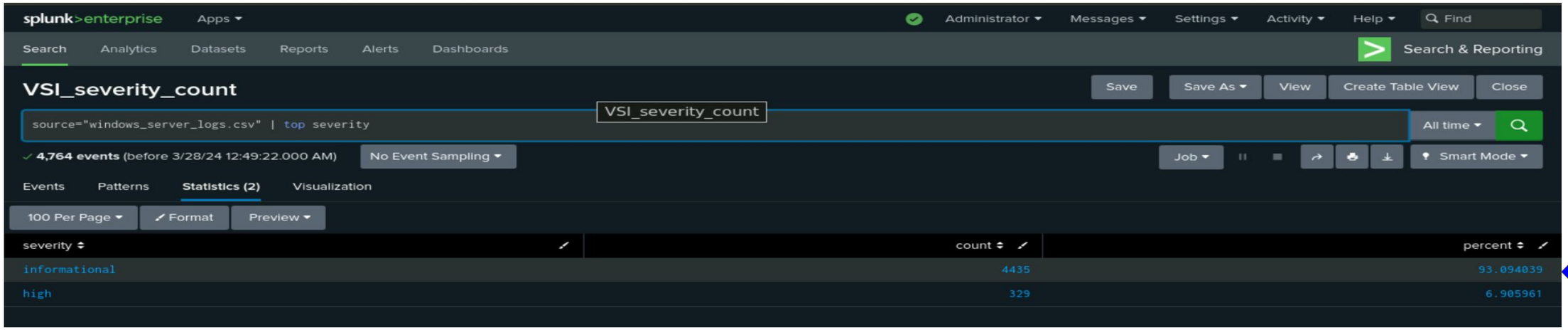
Reports—Windows

Designed the following reports:

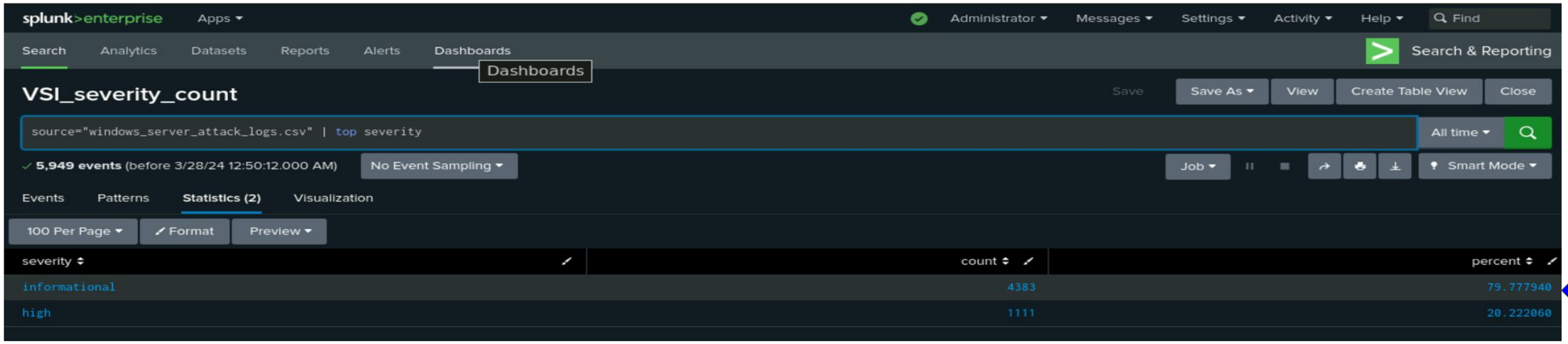
Report Name	Report Description
VSI_signature_codes	A report with a table of signatures and associated signature IDs.
VSI_severity_count	A report that displays the severity levels, and the count and percentage of each.
VSI_status	A report that provides a comparison between the success and failure of Windows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

Images of Reports—Windows

Before Attack: normal breakdown of “informational” vs “high” severity events.



After Attack: significant increase in “high” severity events.



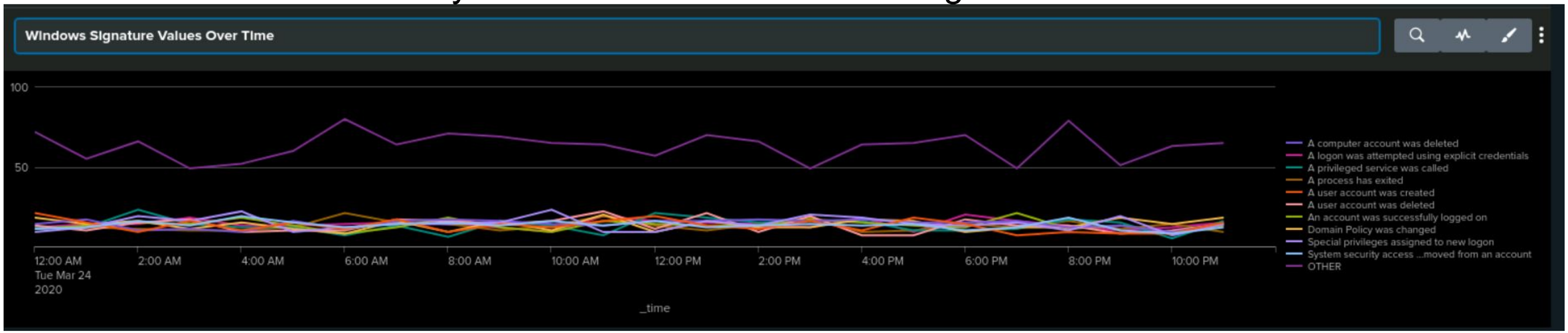
Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
More_than_12_failed	Hourly Level of Failed Activity in Windows System	8	12
VSI_hourly_successful_logins	Number of Hourly Successful Logons for Windows System	15	25
VSI_user_account_deleted	Number of Hourly Account Deletions for Windows System	15	25

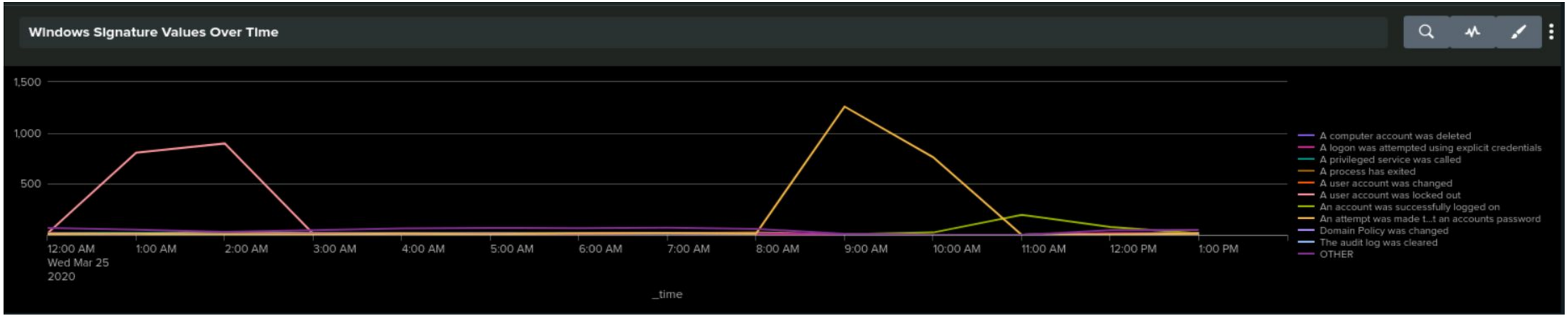
*[Baseline and Threshold based on historical trends in data sets]

Dashboards—Windows

Before Attack: normal activity for various Windows server signatures across time



After Attack: significant uplift in 2 particular signatures the morning of the attack



Apache Logs

Reports—Apache

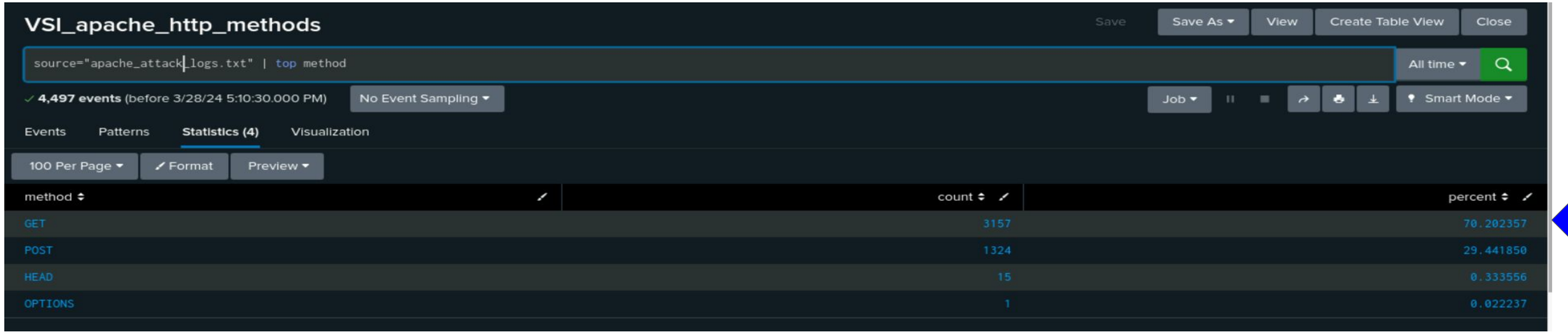
Designed the following reports:

Report Name	Report Description
VSI_apache_http_methods	A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc.).
VSI_apache_top_domainref	A report that shows the top 10 domains that referred to VSI's website.
VSI_apache_count_httpcodes	A report that shows the count of the HTTP response codes.

Images of Reports—Apache

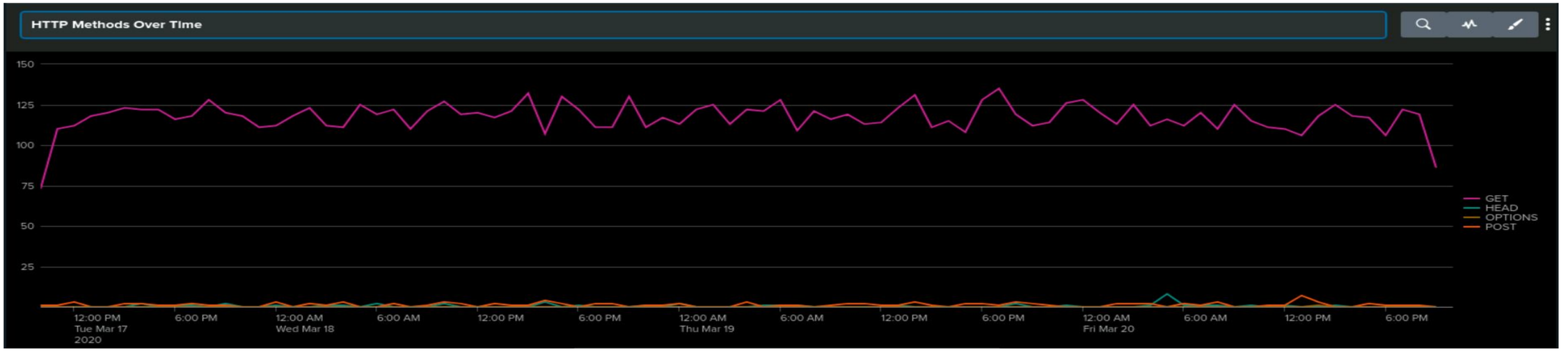
Before Attack:

After Attack:

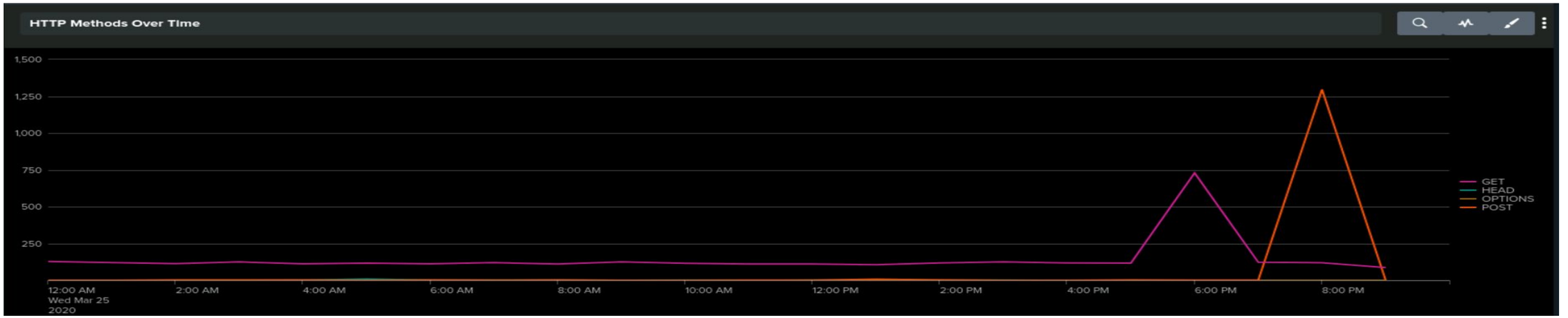


Dashboards—Apache

Before Attack: normal HTTP methods over time.



After Attack: increase in GET and POST methods morning of attack.



Alerts—Apache

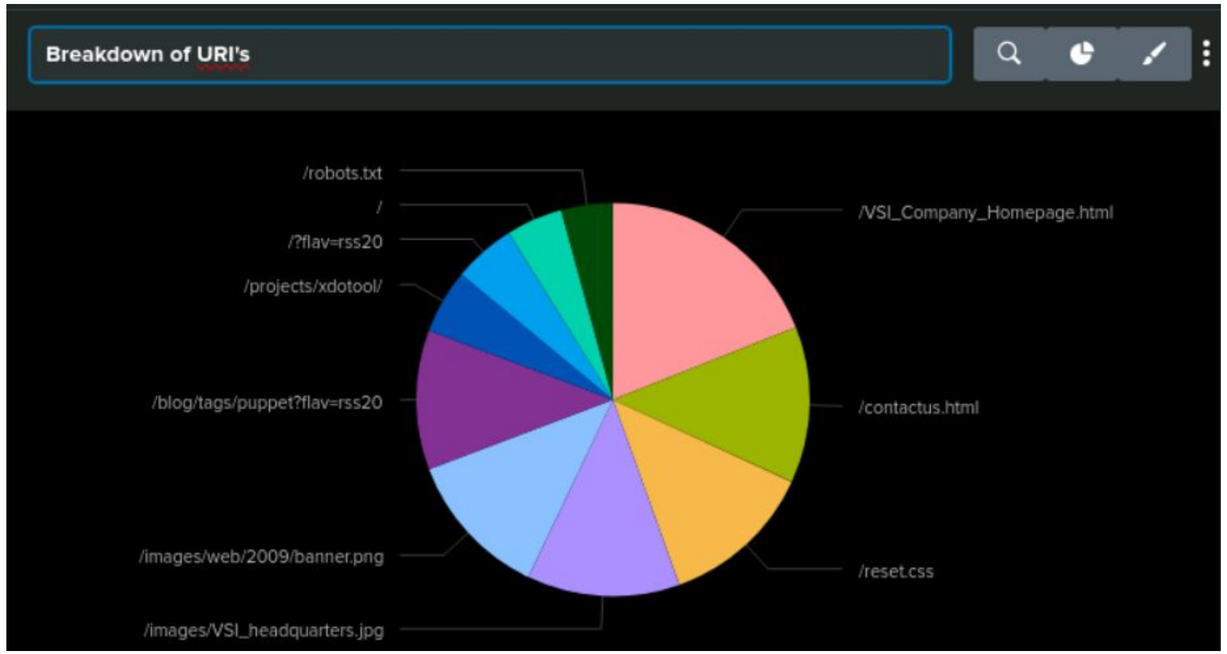
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI_hourly_activity_not_US	Hourly Activity against Apache Server from Countries Outside the US	80	140
VSI_apache_http_post	Hourly Count of HTTP POST method	2	8

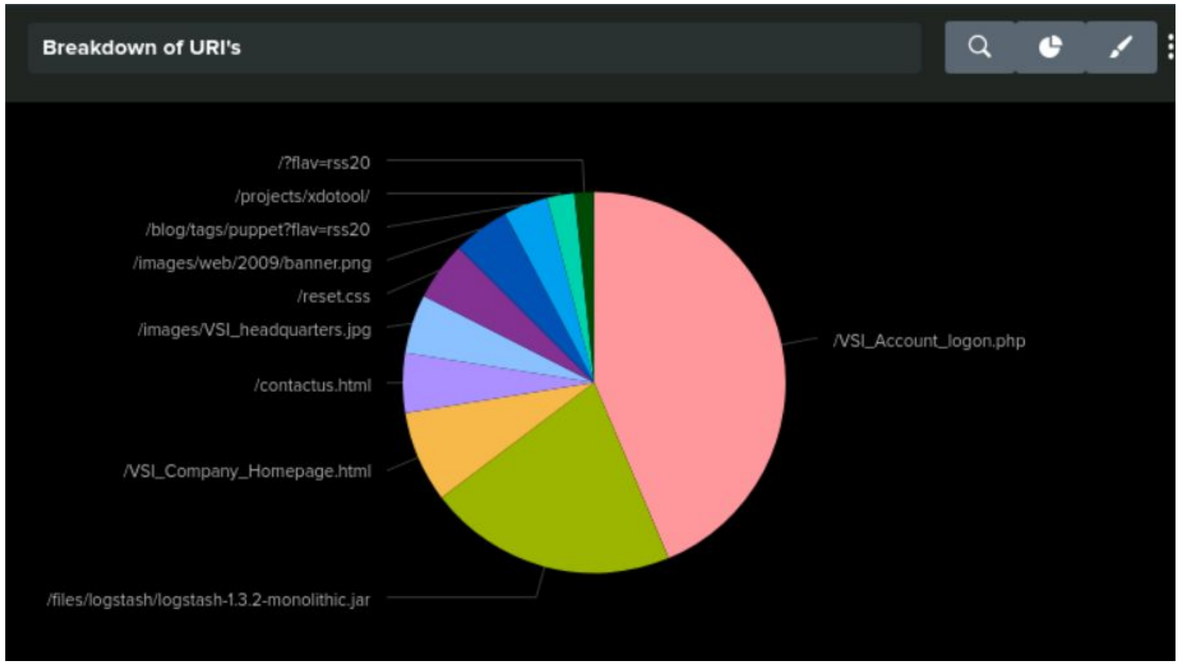
*[Baseline and Threshold based on historical trends in data sets]

Dashboards—Apache

Before Attack: normal HTTP methods over time.



After Attack: Sharp rise in Account.logon.



Attack Analysis

Attack Summary—Windows

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

- Attacks occurred the morning of March 25, 2020.
- High severity events jumped from 6% to 20%.
- Unusually high number of “Failed Activities”.
- Very high number of “An attempt was made to reset an accounts password” (1258) and “An account was locked out” (896).
- Thresholds proved effective at picking up these anomalies.

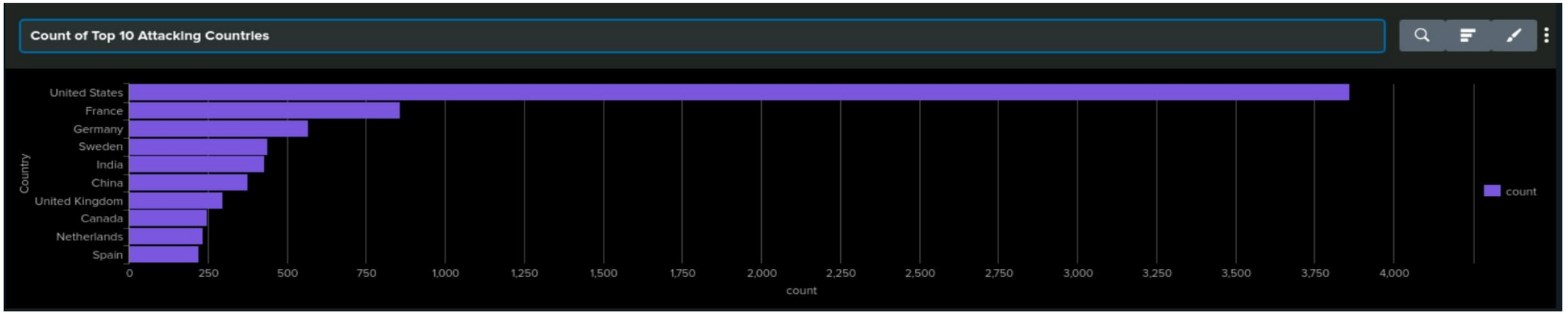
Attack Summary—Apache

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

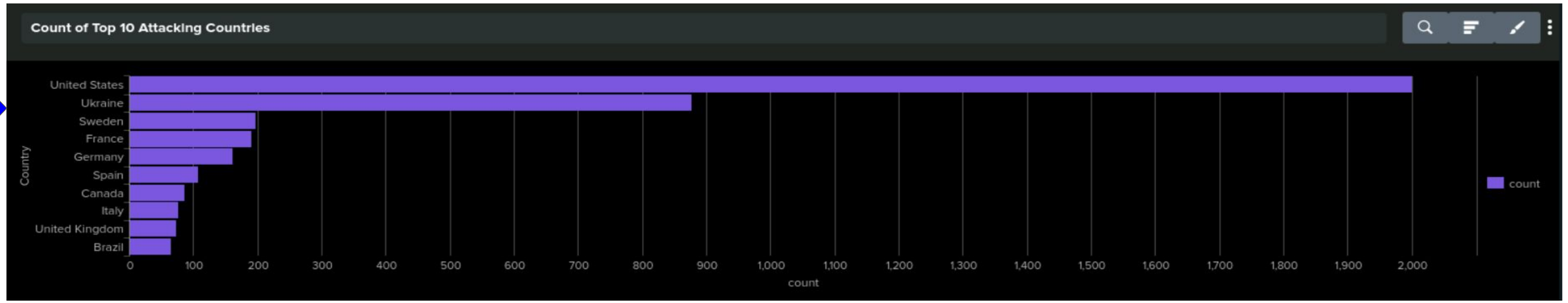
- Attacks occurred in the evening of March 25, 2020.
- Spike in GET requests followed by spike in POST requests (high volume of data was retrieved from the Apache server (GET) and then a high volume of data was later sent (POST)).
- Very high number of login attempts and an increase in 404 errors.
- Suspicious activity from international sources peaked during this time, with a very large increase coming from Ukraine.
- Thresholds proved effective at picking up these anomalies.

Top 10 Attacking Countries

Before Attack: Top 10 Attacking Countries



After Attack: Ukraine Enters Top 10



Summary and Future Mitigations

Project 3 Summary

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

- Windows server attacked the morning of March 25, 2020; Apache server attacked in the evening of the same day.
- High occurences of suspicious activity coming from Ukraine, specifically Kiev and Kharkiv.
- Appears to be a brute force attack on VSI’s login page.

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

- Multi-factor Authentication on Login Page.
  - Would slow down brute force attacks and present another challenge even if credentials were cracked/stolen.