Defensive Security Project
by: Team CyberCAT

Chirag Aaron & Tom

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Deployed Splunk Enterprise 9.0.4 on Ubuntu Linux 18.0.4.3
- Determined normal baseline of activity
- Created reports and alerts
- Designed real time monitoring dashboard for SOC team to analyze
- Deployed website monitoring app
- SOC team discovered several attacks in progress

Website Monitoring App

Website Monitoring

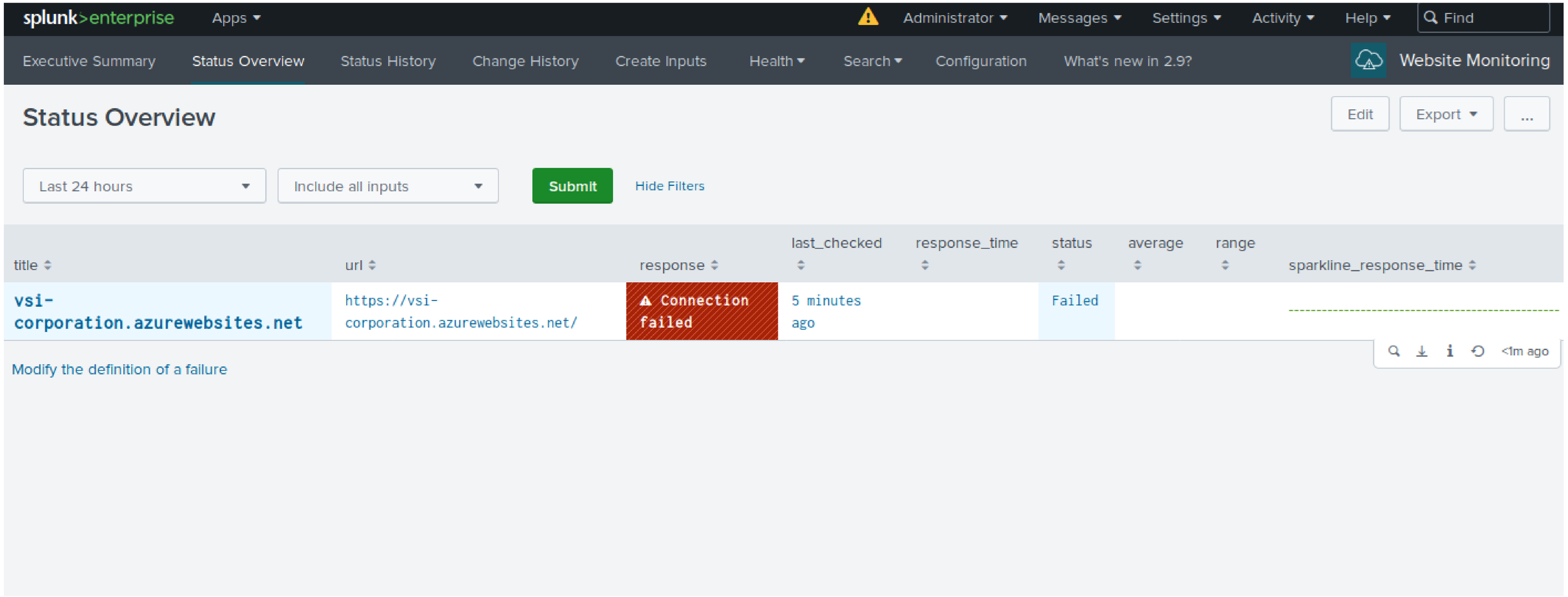
- Monitoring- Monitors websites to detect downtime and performance problems.
- Uptime Calculations - Provides information about past failures and calculates website uptime percentage.
- Status Monitoring Dashboard - Provides response time and historical analysis of the monitored website.
- Outage Alerting - Sends an email alert when the monitored website is down.
- Change History Dashboard - Provides information regarding when the monitored pages change.

Website Monitoring

This website monitoring app will alert when our websites performance starts to degrade, allowing us immediate lead time to determine if there is an issue that needs addressing.

It also allows us to quickly change the parameters in case when marketing campaigns are executed that can drive up traffic outside normal conditions.

Website Monitoring



Logs Analyzed

1 Windows Logs

- Failed logins
- Signatures
- Usernames
- Deleted accounts
- Severity Levels

2 Apache Logs

- HTTP methods
- Referring domains
- HTTP response codes
- Geolocation
- URI data

Windows Logs

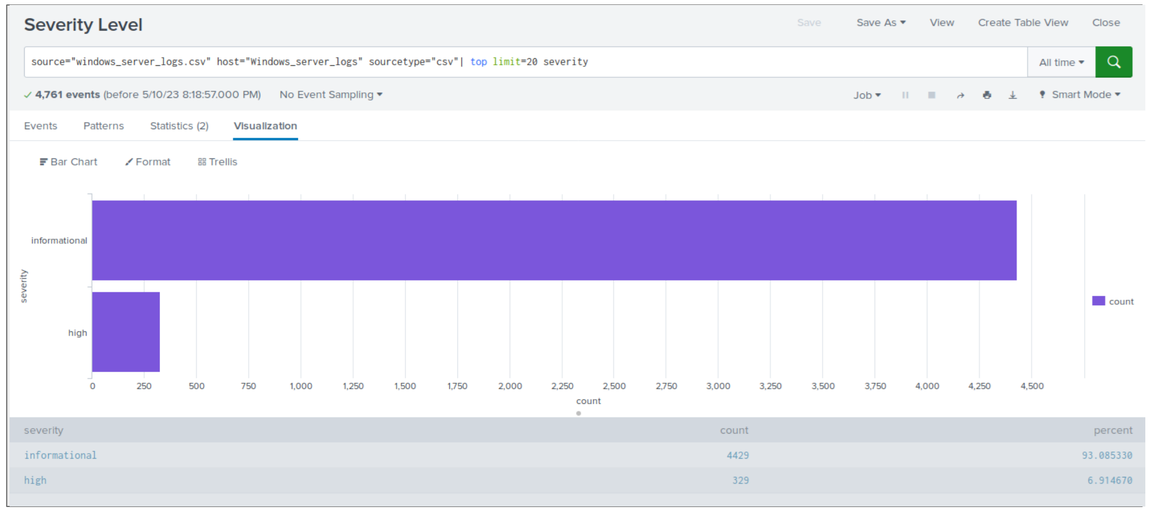
Reports—Windows

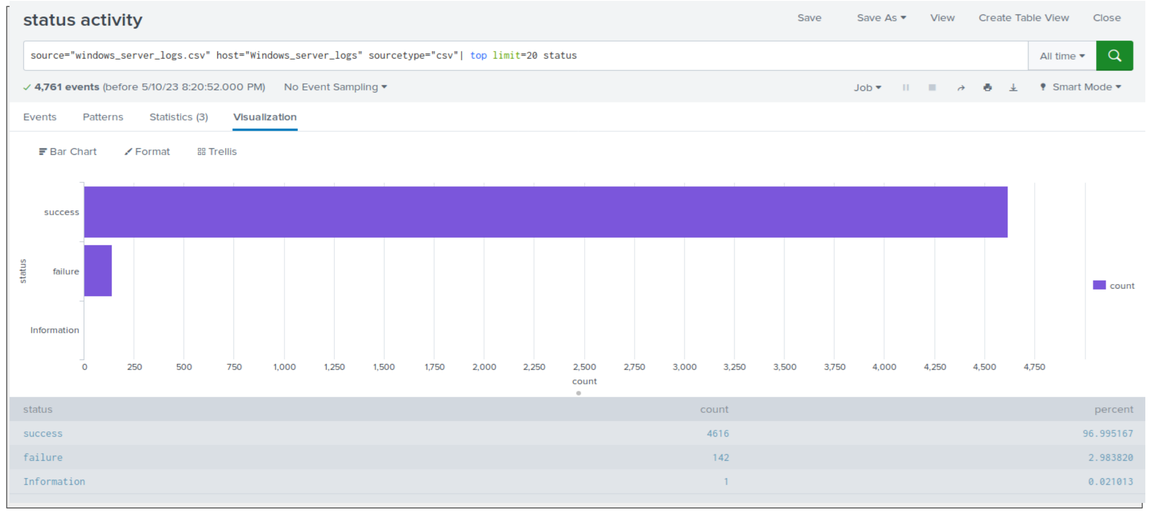
Designed the following reports:

Report Name	Report Description
Signature Report	Shows the Signatures with Associated IDs
Severity Level Report	Describes attempts to change domain policy
Status Activity Report	Describes attempts to change user account policies

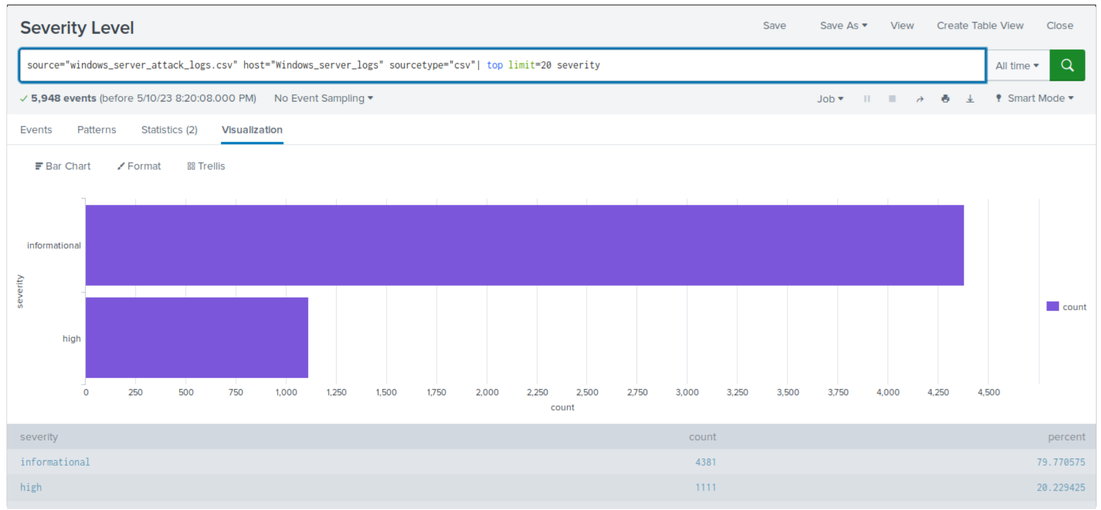
Images of Reports—Windows

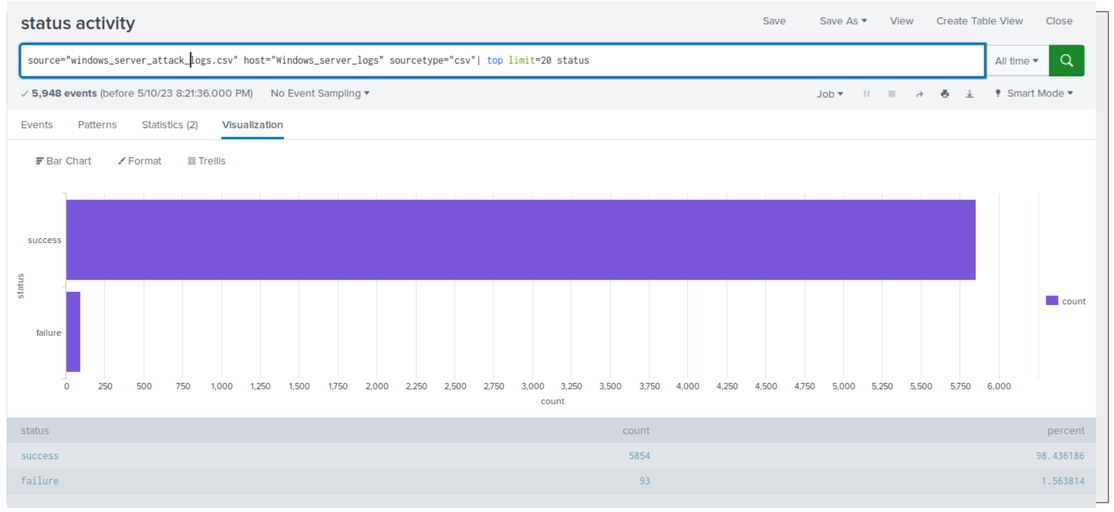
Baseline





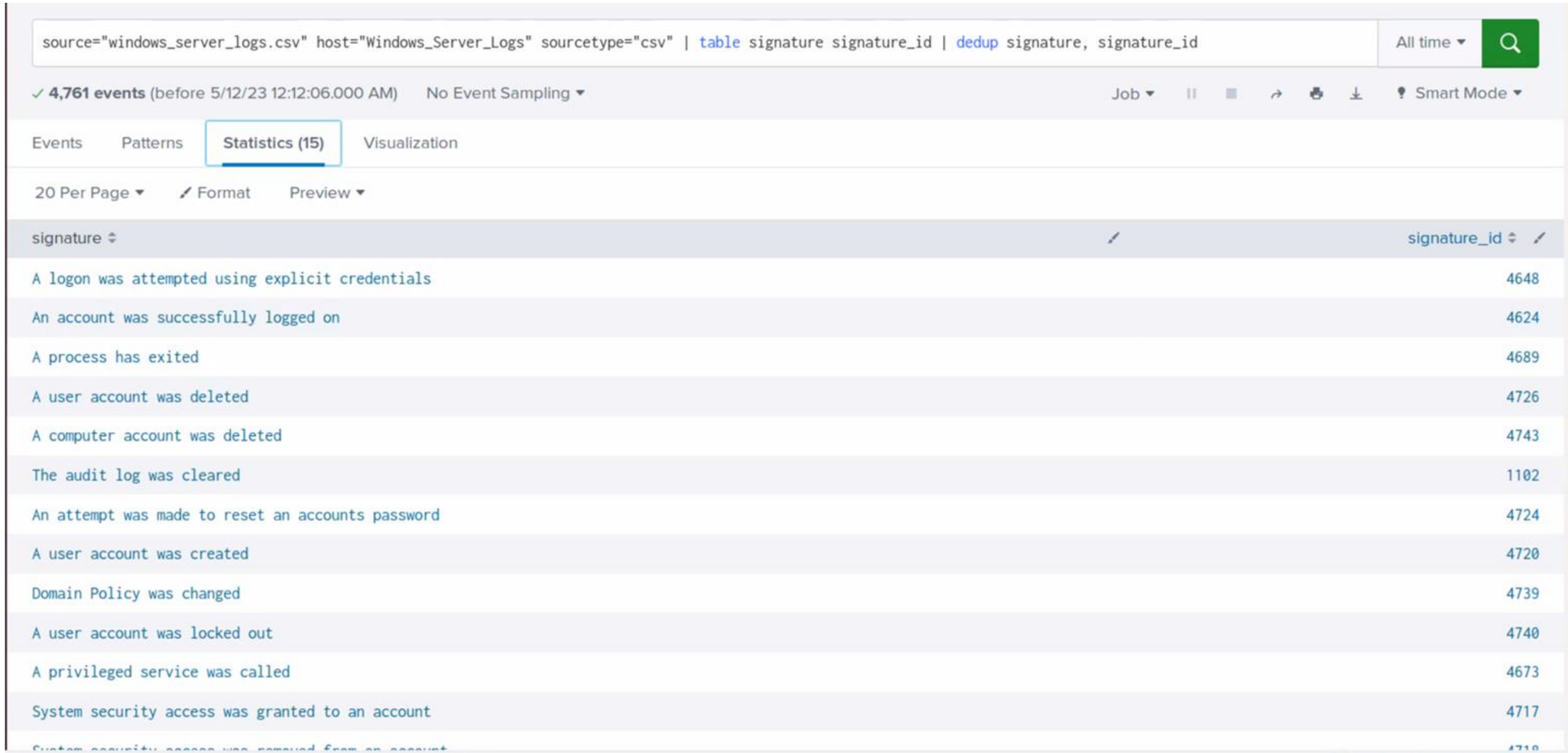
Attack





Images of Reports—Windows

Signatures and associated signature IDs



signature	signature_id
A logon was attempted using explicit credentials	4648
An account was successfully logged on	4624
A process has exited	4689
A user account was deleted	4726
A computer account was deleted	4743
The audit log was cleared	1102
An attempt was made to reset an accounts password	4724
A user account was created	4720
Domain Policy was changed	4739
A user account was locked out	4740
A privileged service was called	4673
System security access was granted to an account	4717

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Account Password Reset Failure	Alerts when an excessive amount of password resets have occured	8	12

JUSTIFICATION: Baseline of 8 password reset failures per hour was determined to be the average threshold of normal activity. The high activity was determined to be 10 in any given hourly period. Threshold of 12 allows for anomalies while then alerting us to look into activity after 12 so that it minimized false positives.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive Login Attempts	Alerts when an excessive amount of login attempts have occured	20	25

JUSTIFICATION: Baseline of 20 login attempts per hour was determined to be the average threshold of normal activity. The high activity was determined to be 22 in any given hourly period. Threshold of 25 allows for anomalies while then alerting us to look into activity after 25 so that it minimized false positives.

Alerts—Windows

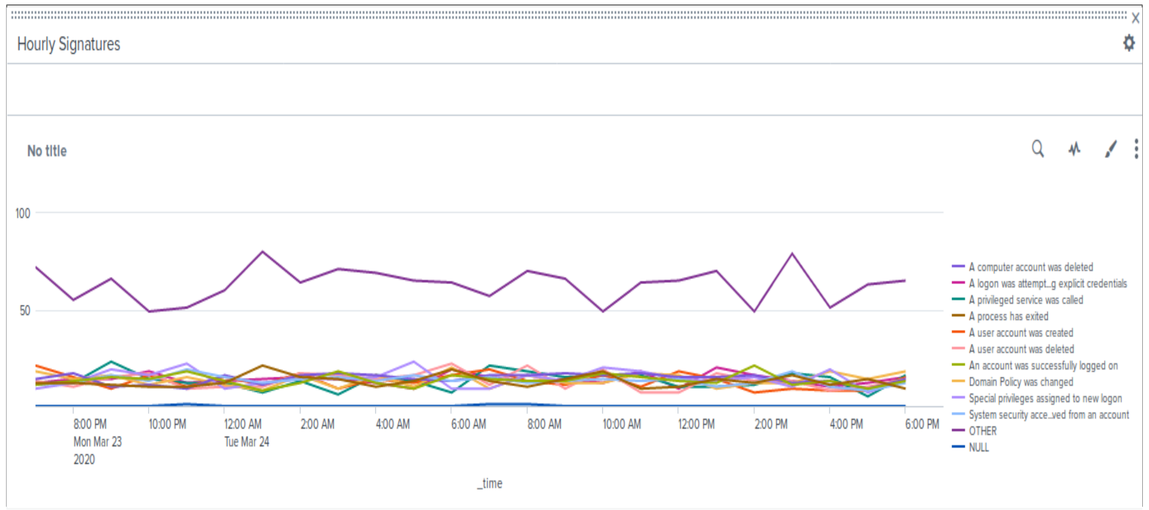
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive Amount of User Accounts Deleted	Alerts when an excessive amount of user accounts have been deleted	20	25

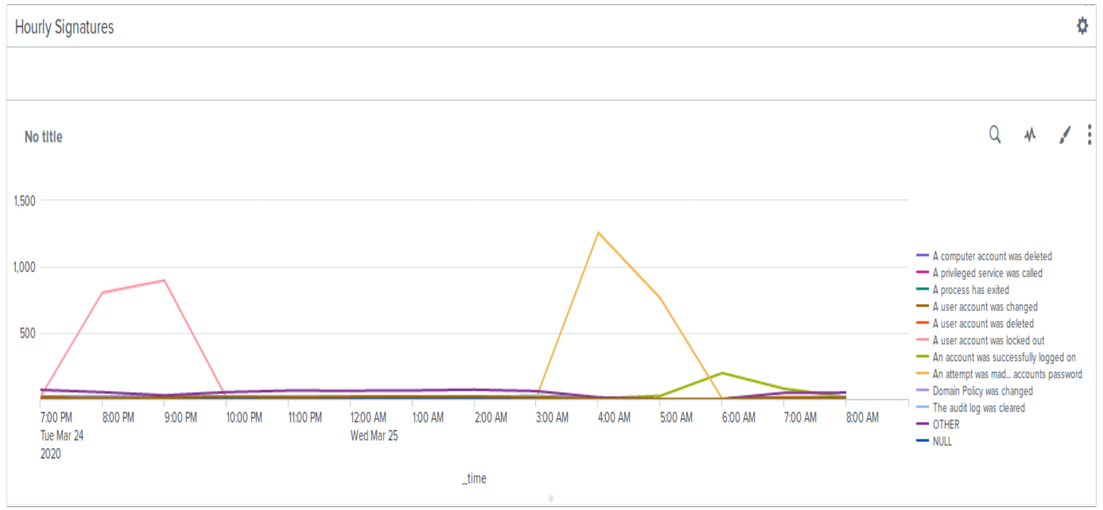
JUSTIFICATION: Baseline of 20 accounts deleted per hour was determined to be the average threshold of normal activity. The high activity was determined to be 22 in any given hourly period. Threshold of 25 allows for anomalies while then alerting us to look into activity after 25 so that it minimized false positives.

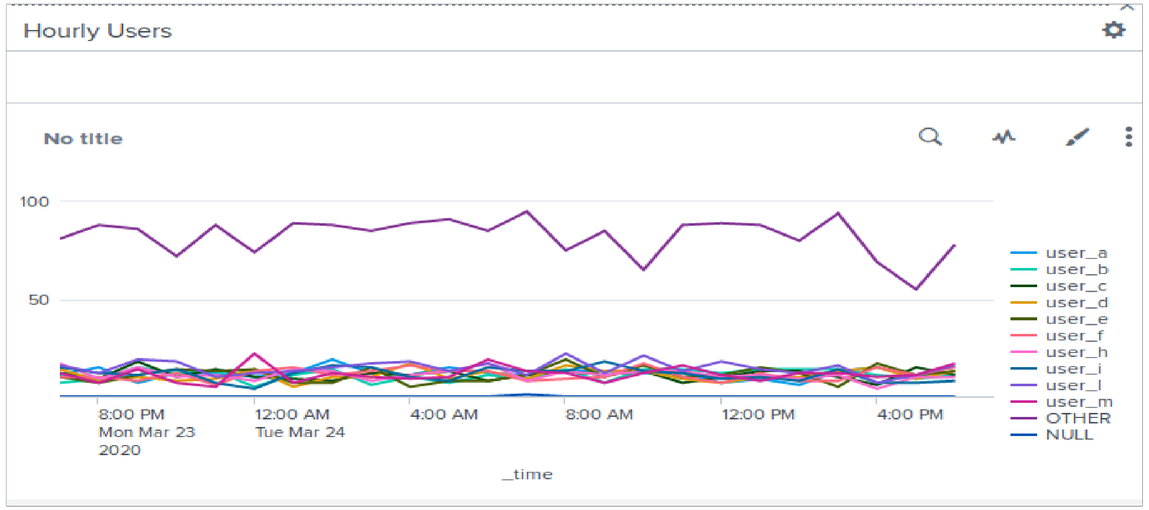
Dashboards—Windows

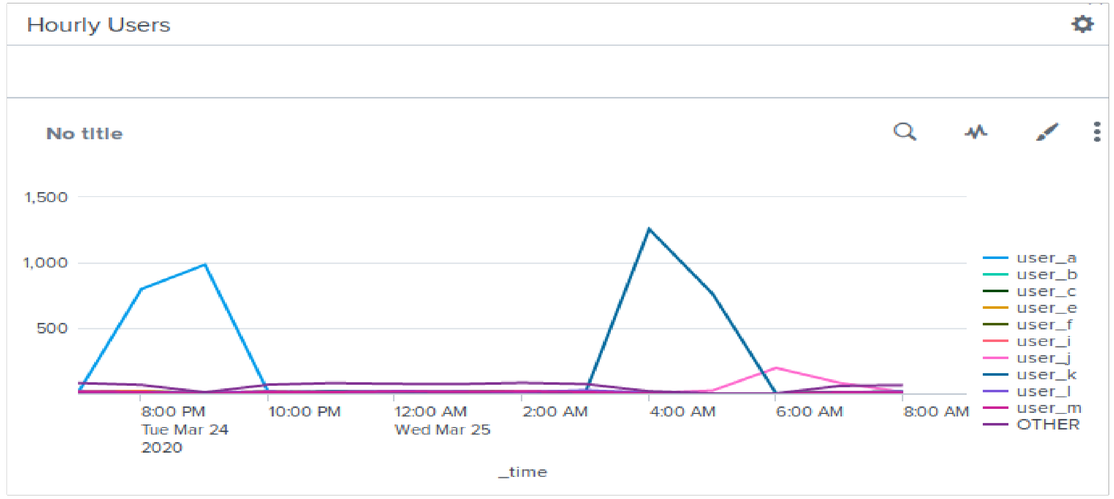
Baseline



Attack

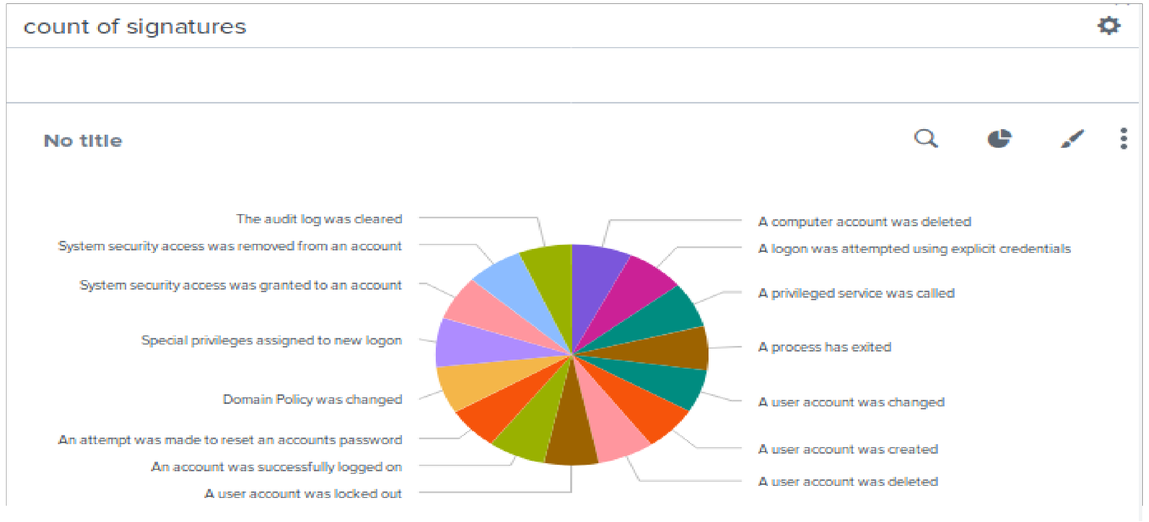


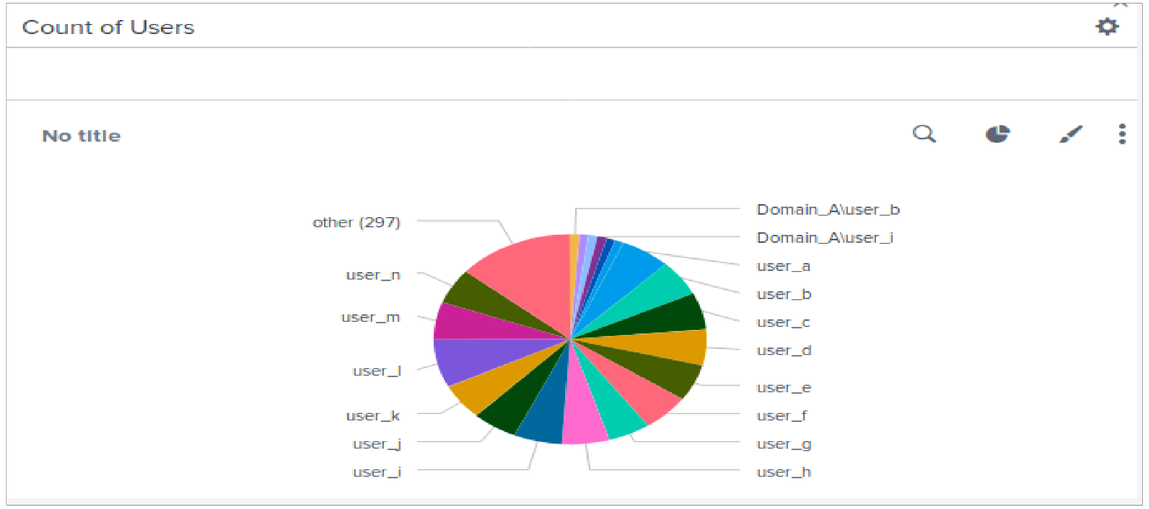




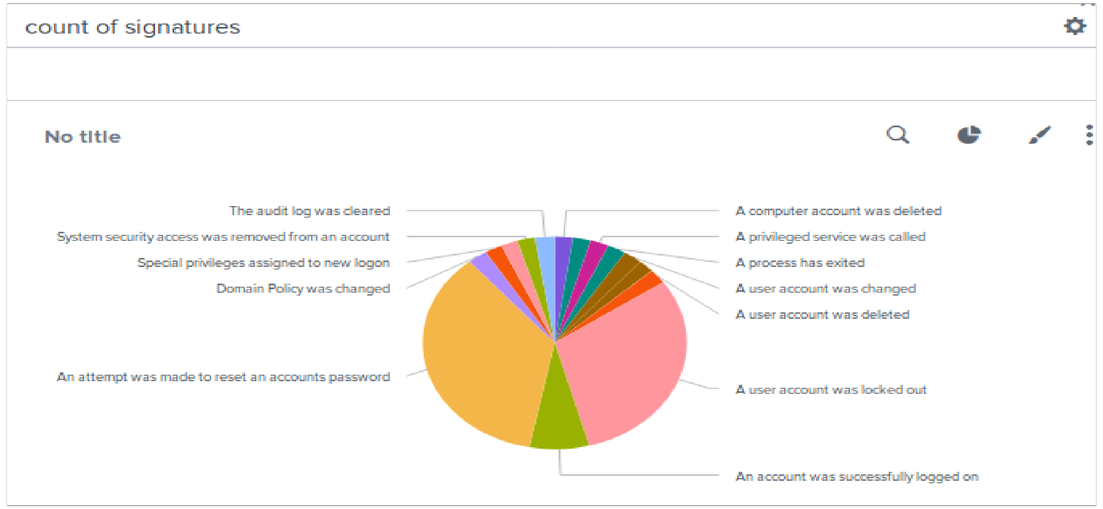
Dashboards—Windows

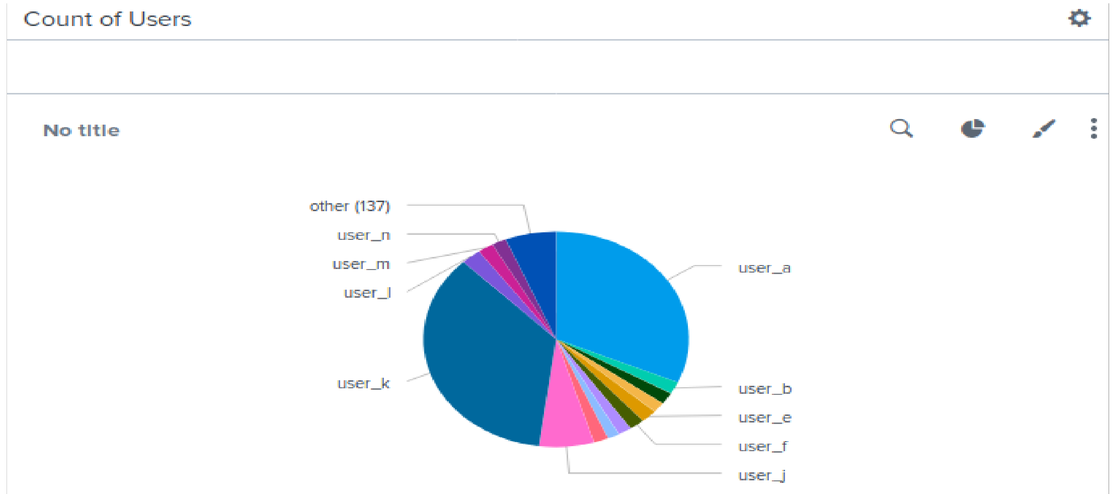
Baseline





Attack





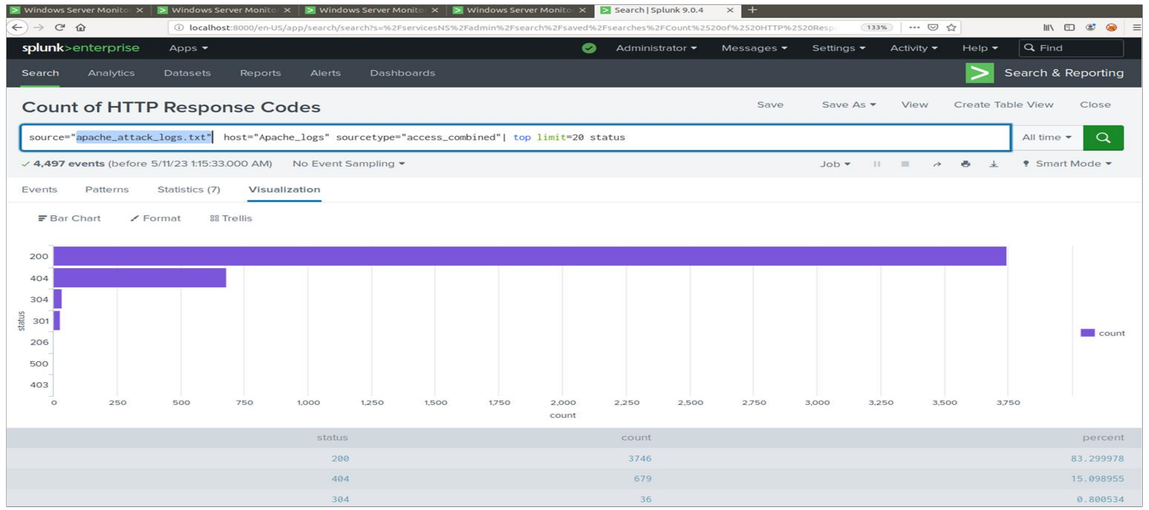
Apache Logs

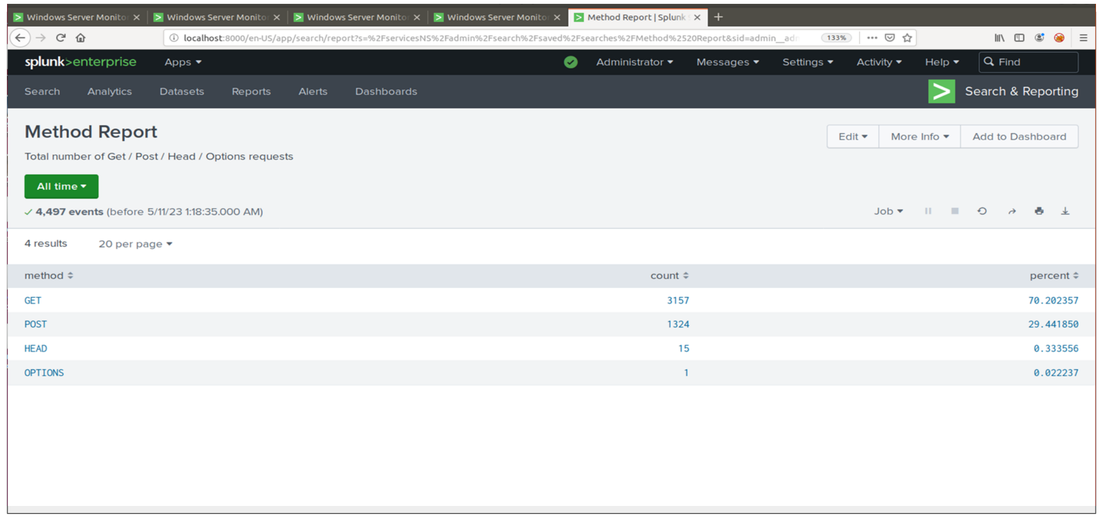
Reports—Apache

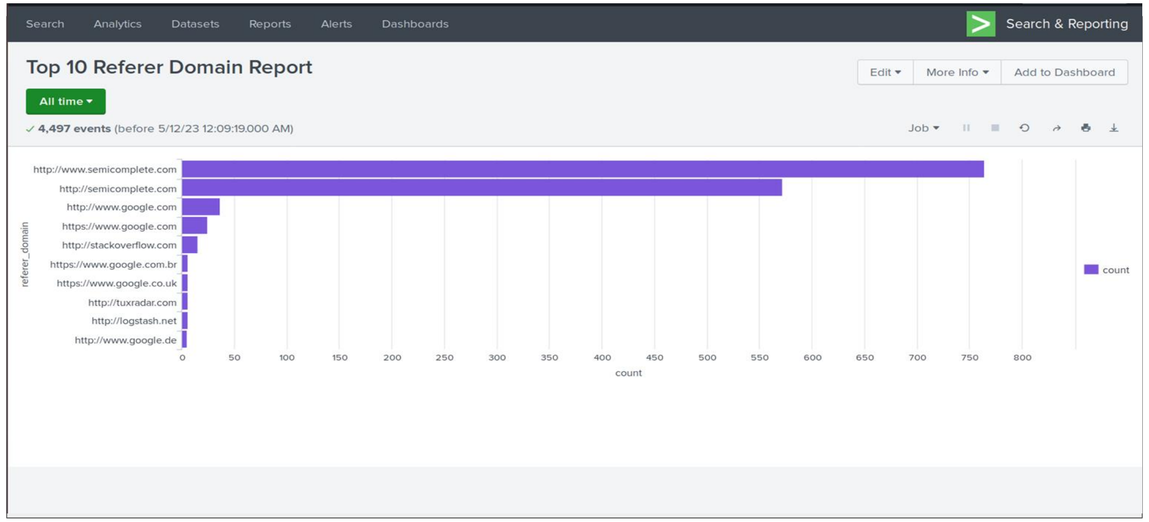
Designed the following reports:

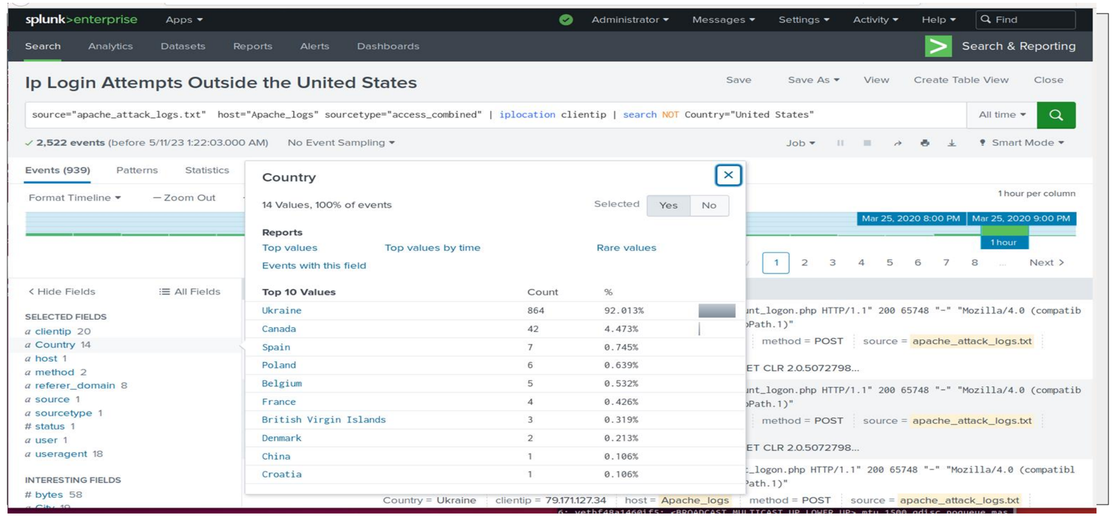
Report Name	Report Description
HTTP Activity	Describes HTTP methods
Top Ten Referred Domains	Lists top 10 domains that referred traffic to website
IP Location by ClientIP	Describes geolocation of traffic to website
Count of HTTP Response Codes	Describes the count of HTTP codes that indicate success or failure on the web server.

Images of Reports—Apache









Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive Post Alert	Alerts by email when the number of posts exceed	3	5

JUSTIFICATION: Baseline of 3 posts per hour was determined to be the average threshold of normal activity. The high activity was determined to be 4 in any given hourly period. Threshold of 5 allows for anomalies while then alerting us to look into activity after 5 so that it minimized false positives.

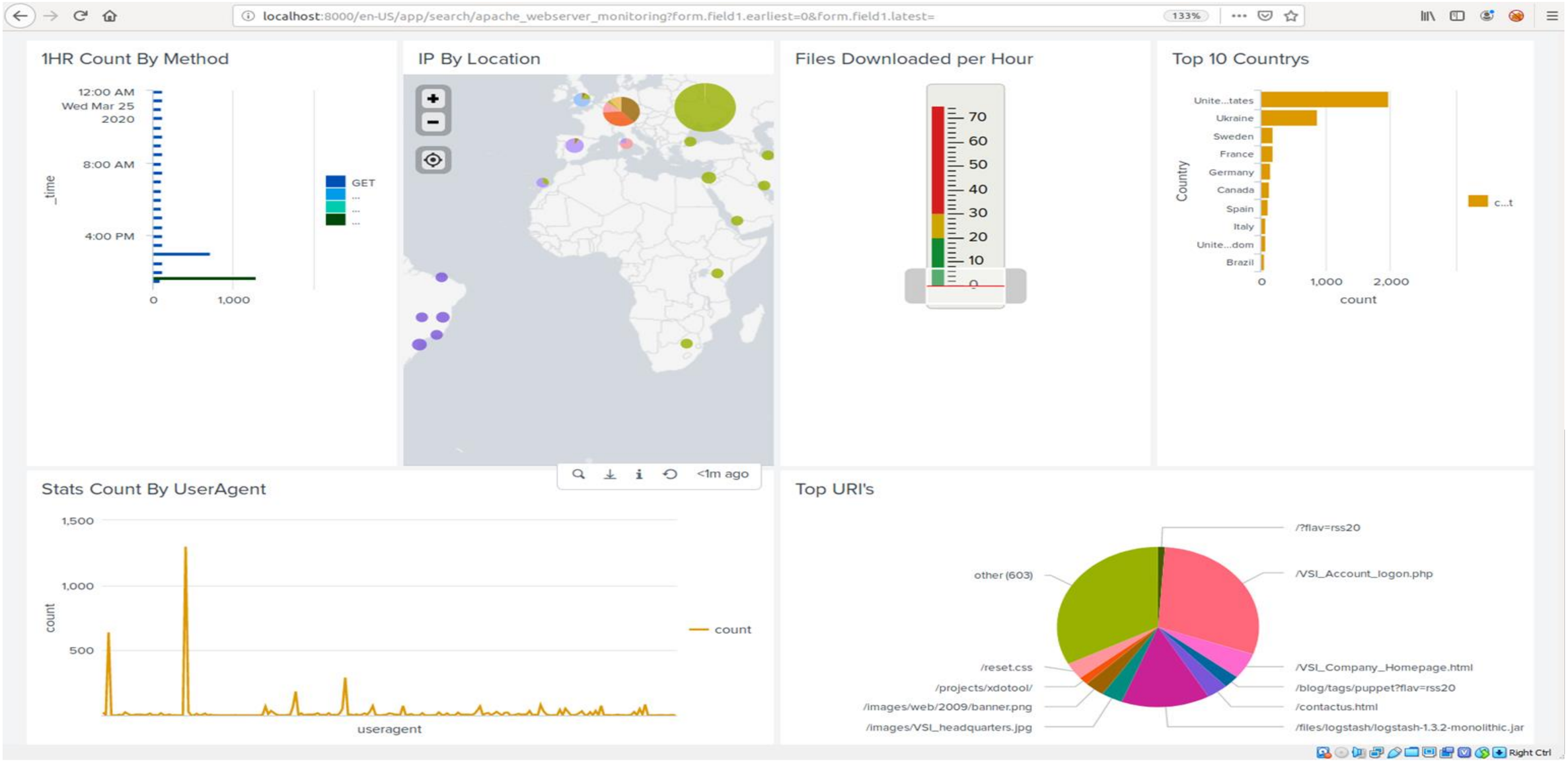
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Ip Login Attempts Outside the United States	Alerts when there are more than 125 login attempts from outside the US	107	125

JUSTIFICATION: Baseline of 85 logins per hour was determined to be the average threshold of normal activity. The high activity was determined to be 107 in any given hourly period. Threshold of 125 allows for anomalies while then alerting us to look into activity after 125 so that it minimized false positives.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

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

- Beginning at 1am on 3/25/23 a spike in success activity occurred exceeding baseline thresholds of normal activity
- Attackers attempted to reset account passwords 2064 times in a 2 hour period, and 1810 lockouts occurred. Normal activity is expected around ~170 an hour
- Severity level reports spiked from around 230 expected events to over 1100 during the attack with attempts to reset user passwords 610 times.
- The signature report indicated “A logon was attempted using explicit credentials” as the top signature ID during the attack period.

Attack Summary—Windows

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

- *A user account was locked out* thresholds were correct.
- *An attempt was made to reset an accounts password* thresholds were correct.
- *An account was successfully logged on* thresholds were correct.

With the thresholds we defined for the above we successfully were alerted with suspicious activity.

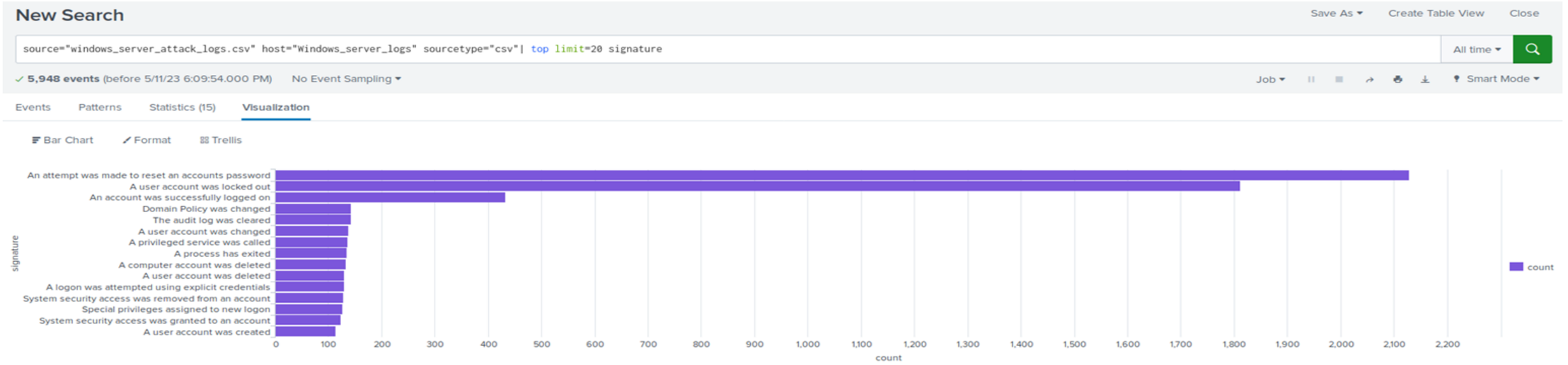
Attack Summary—Windows

Based on the attack logs and the visualizations on the dashboard,

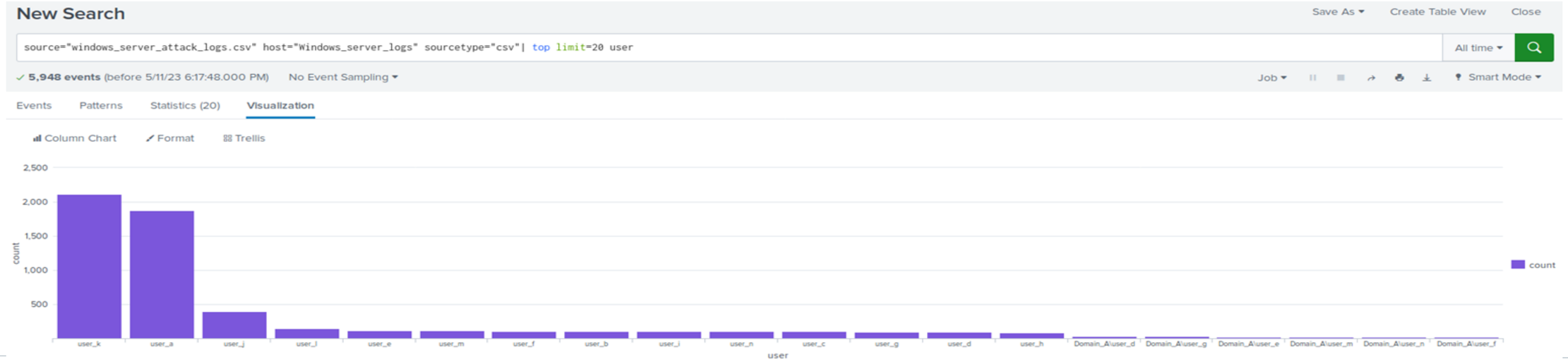
- High volume of user account lock outs occurred between 8:00PM and 9:00PM on March 24, 2020 when user_a attempted to login
- Massive spike in the number of attempts to reset an account password between 4:00AM and 5:00AM on March 25, 2020 by user_k
- User counts for user_k and user_a went from an average of 6% to over 30%

Screenshots of Attack Logs

Signatures showing spike in attempts to reset account password and accounts locked out



Spike in user counts for user_k and user_a



Attack Summary—Apache

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

- HTTP POSTs went from a baseline of approximately 100 to over 1300 at 3:00PM on March 25, 2020
- HTTP GET activity spiked at 1:00PM on March 25, 2020
- Referer Domains dropped by 50%
- Geographic source location shows abnormally heavy use from Ukraine

Attack Summary—Apache

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

- *HTTP Method* thresholds were correct.
- *HTTP Response Code* thresholds were correct.
- *URI Data* thresholds were correct.
- *Geolocation of source traffic* thresholds were correct.

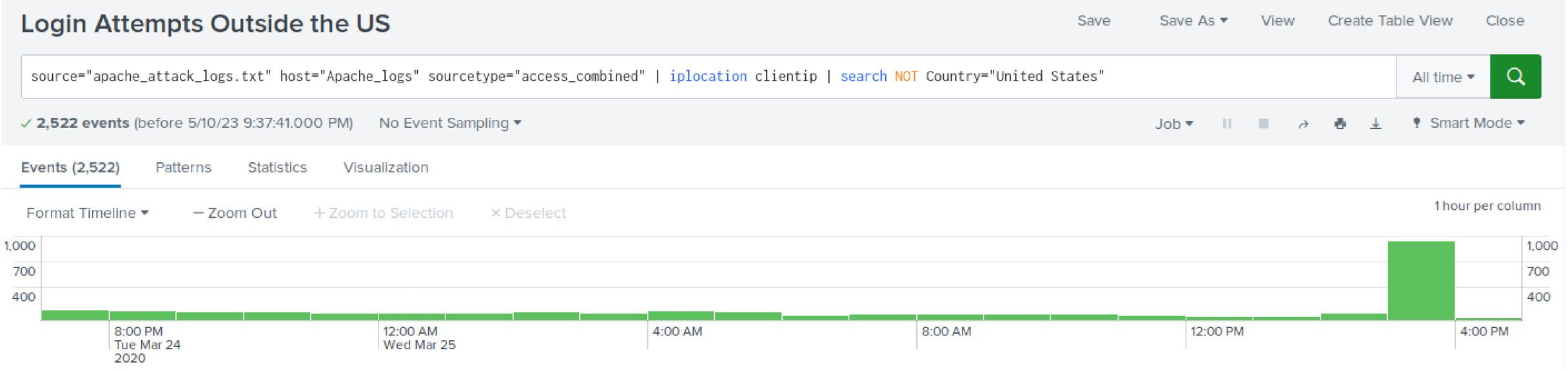
With the thresholds we defined for the above we successfully were alerted with suspicious activity. We would continue to monitor this on an ongoing basis to make any necessary adjustments to minimize false positives. We would continue to monitor this on an ongoing basis to make any necessary adjustments to minimize false positives.

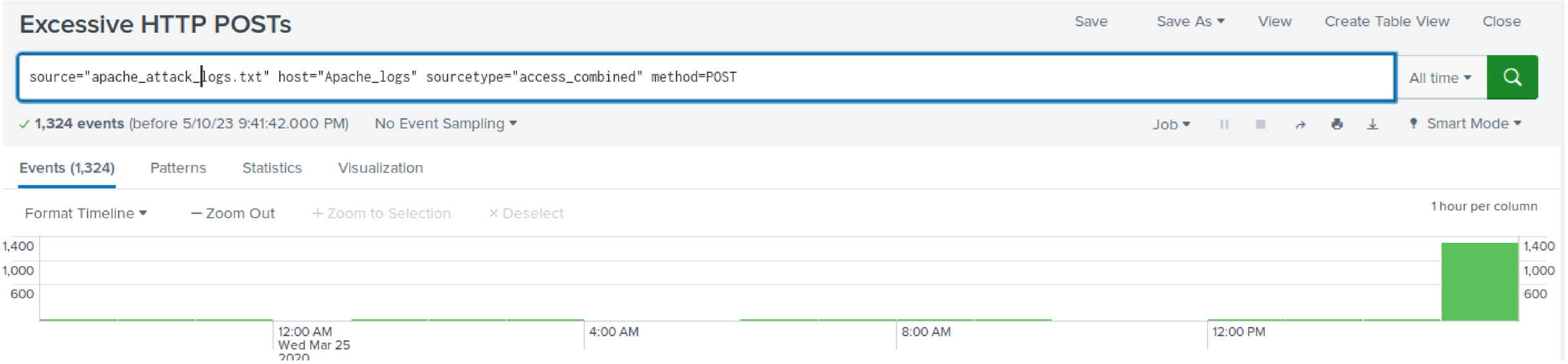
Attack Summary—Apache

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

- Normal activity for GET method is approximately 120 per hour, around 6pm on 3/25/20 GET activity spiked to 729 in one hour. POST activity is rarely an occurrence and spiked at 1296 at 8pm.
- A 877 OTHER requests originated from the country of Ukraine with normal activity expected to be ~40 outside the US. Ukraine was uncharacteristically in the top 10 countries
- Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com was an unexpected client that spiked in usage with 638 requests. Not a common web client. Mozilla 4.0 spiked at 1296 attempts.
- The VSI_Account_logon.php page was uncharacteristically called upon 1323 times while “OTHER” was called upon 603 teams.

Screenshots of Attack Logs





Summary and Future Mitigations

Project 3 Summary

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

  Our findings determined VSI was the victim of a brute force attempt which then pivoted to an escalation of privileges attempt in the windows environment. We also discovered there also a brute force attack on VSI's webserver.

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

  Implement Lockouts after 10 invalid sign-in attempts on the Active Directory Server. Implement a Network Intrusion System that automatically blocks suspicious ip addresses. Also setup thresholds by countries or regions to improve our alerting.