Defensive Security Project
by: Stefhanus, Dylan, Gryphon

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- In this project, we have undertaken the task of developing a custom security monitoring environment for an organisation using Splunk. The primary objective is to demonstrate proficiency in defensive security practices and the effective use of Splunk as a security monitoring tool.
- VSI - A virtual-reality program design company with concerns about cyber threats from competing company JobeCorp
- Tasked with designing a security monitoring solution for VSI using Splunk
- Aim to monitor an Administrative Webpage, an Apache Web Server, and a Windows OS
- Provided with historical logs for a baseline to create reports, alerts, and dashboard
- Generate baselines from the logs provided to protect against any attacks from JobeCorp
- A simulated cyber attack will follow to evaluate the effectiveness of the measures taken
- Assess the defensive measures whilst taking note of places of success, and places of improvement

Website Monitoring App

Website Monitoring App

The Website Monitoring add-on app for Splunk is a valuable tool that enables users to monitor websites, detect downtime, and identify performance issues.

This app offers a modular input that can be set up quickly, in just 5 minutes or less. It comes with several key features, including uptime calculation, a status monitoring dashboard, email outage alerting, and a change history dashboard.

These features provide users with a comprehensive solution for website monitoring and analysis, making it easier to ensure website reliability and responsiveness

The Add-On App Website Monitoring was chosen to supplement the Splunk Environment to:

- Monitor customer experience (lag times, speed)

- Gain better insights into common attack paths (denial of service, brute force)

- Determine additional hardware/software needs (more traffic = more servers)

Website Monitoring

Website Monitoring provides constant monitoring of website responsiveness and availability.

In the event of a Denial of Service (DoS) attack, the Website Monitoring system will provide analysts with immediate alerts about a drop in website responsiveness

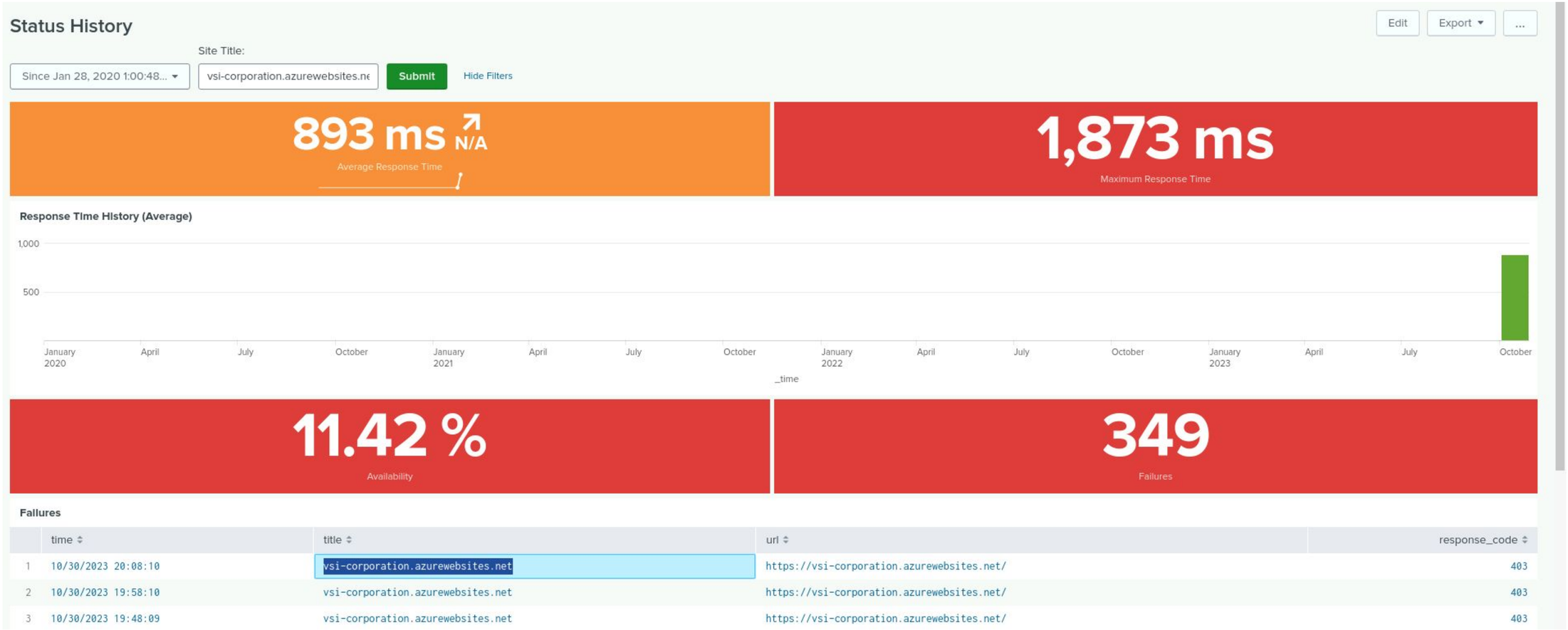
This allows security analysts to identify and respond to any potential Denial of Service (DoS) attacks in real-time

On a daily basis, Website Monitoring helps assess whether additional hosting machines or servers are required to accommodate higher user traffic. This is completed through the tracking of response times which can aid in resource allocation.

This helps to provide a seamless user experience even in the event of a high-traffic spike

Through the optimisation of resource allocation and being able to swiftly address any DoS attacks, the Website Monitoring add-on will help to maintain customer trust and business continuity, whilst safeguarding against threats.

Website Monitoring



Logs Analyzed

1 Windows Logs

The Windows servers run VSI’s back-end systems. The logs represent the normal business operations. These logs contain valuable user-related data, including details such as account creations and deletions, both failed and successful login attempts, and other relevant information pertaining to the status of Windows users. These historical logs provided represent a baseline of normal activity on the windows servers.

2 Apache Logs

The Apache web servers host VSI’s web application. These logs provided contain information related to websites, including HTTP methods, details about the requesting and receiving websites, and HTTP status codes. The historical logs on the Apache web servers represented standard business operations. These were used to develop a baseline for activity within the server.

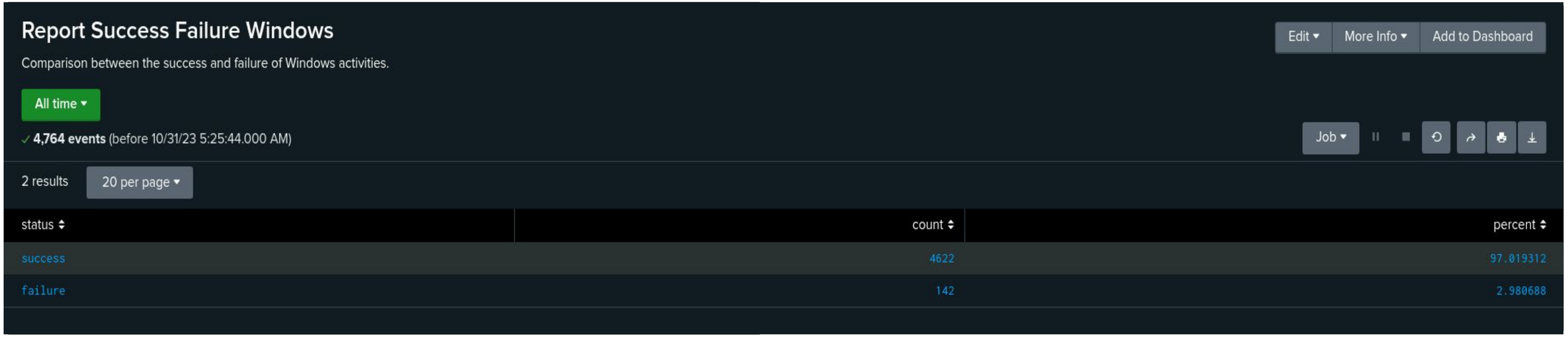
Windows Logs

Reports—Windows

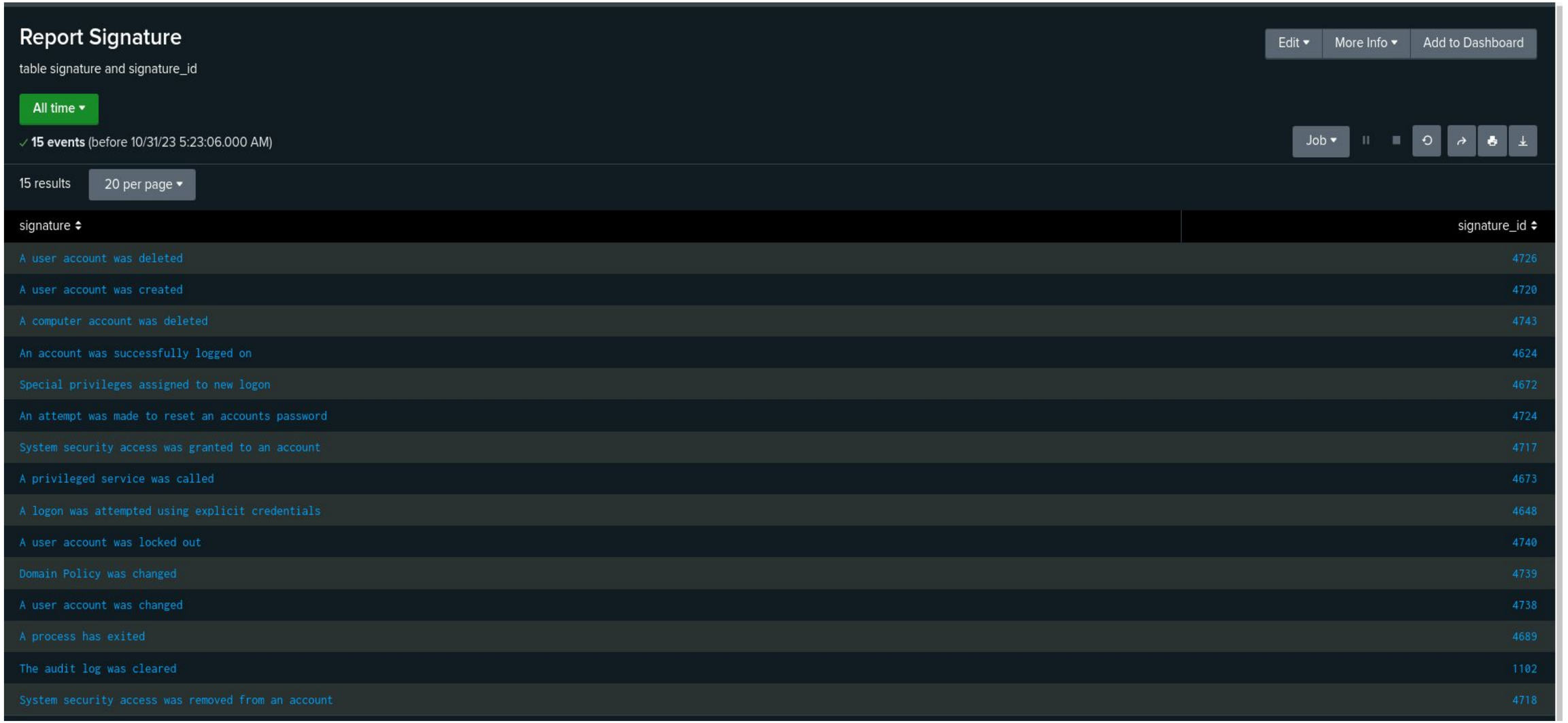
Designed the following reports:

Report Name	Report Description
Severity	This report shows the different severity levels and how many of each were present.
Signatures	A report showing signatures and the corresponding signature ID.
Windows Activities	A report detailing the successes and failures of windows activities.

Images of Reports—Windows



Images of Reports—Windows



Report Signature

table signature and signature_id

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **15 events** (before 10/31/23 5:23:06.000 AM)

Job ▾

15 results | 20 per page ▾

signature	signature_id
A user account was deleted	4726
A user account was created	4720
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724
System security access was granted to an account	4717
A privileged service was called	4673
A logon was attempted using explicit credentials	4648
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A process has exited	4689
The audit log was cleared	1102
System security access was removed from an account	4718

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed_Windows_Activity	Alerts SOC if failed Windows activity for an hour are over the threshold.	10	13

JUSTIFICATION: Our baseline is set to 10 as the normal activity number of failed Windows activity per hour, and the threshold of 13 is considered enough to be a potential attack.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful_Log_On	Alerts SOC if successful log on for an hour are over the threshold.	21	24

JUSTIFICATION: Our baseline is set to 21 as the normal activity number of successful log on per hour, and the threshold of 24 is considered enough to be a potential attack.

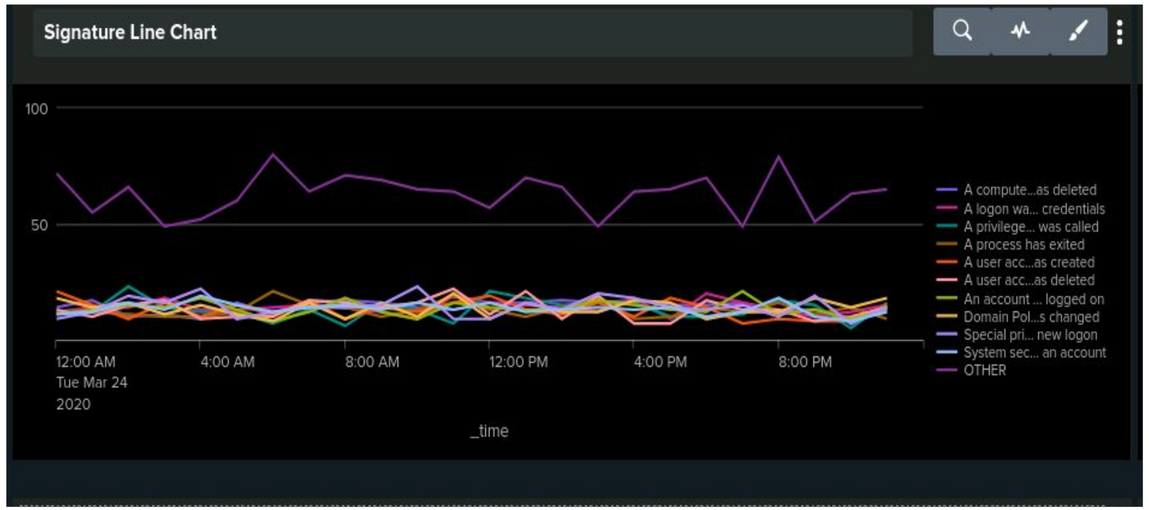
Alerts—Windows

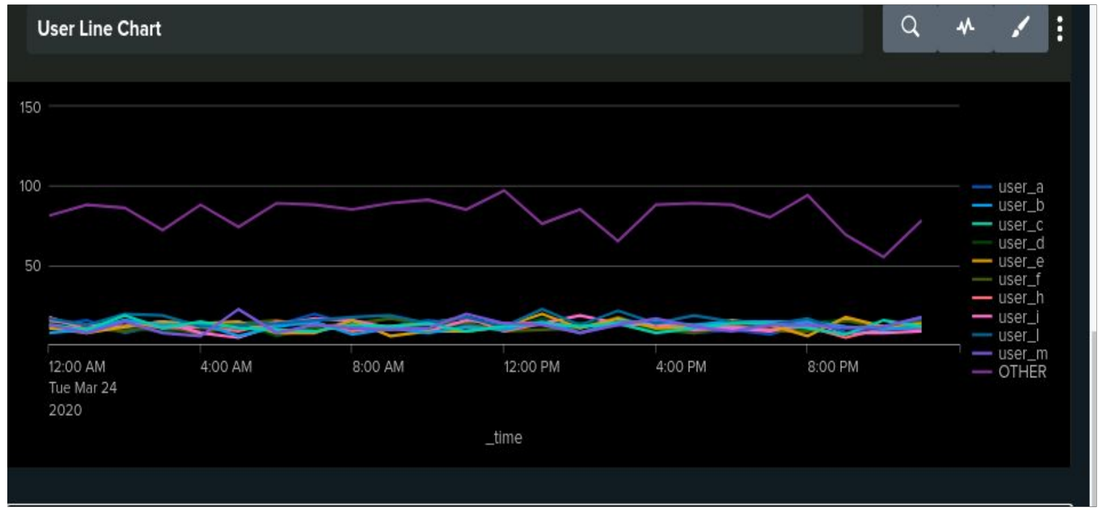
Designed the following alerts:

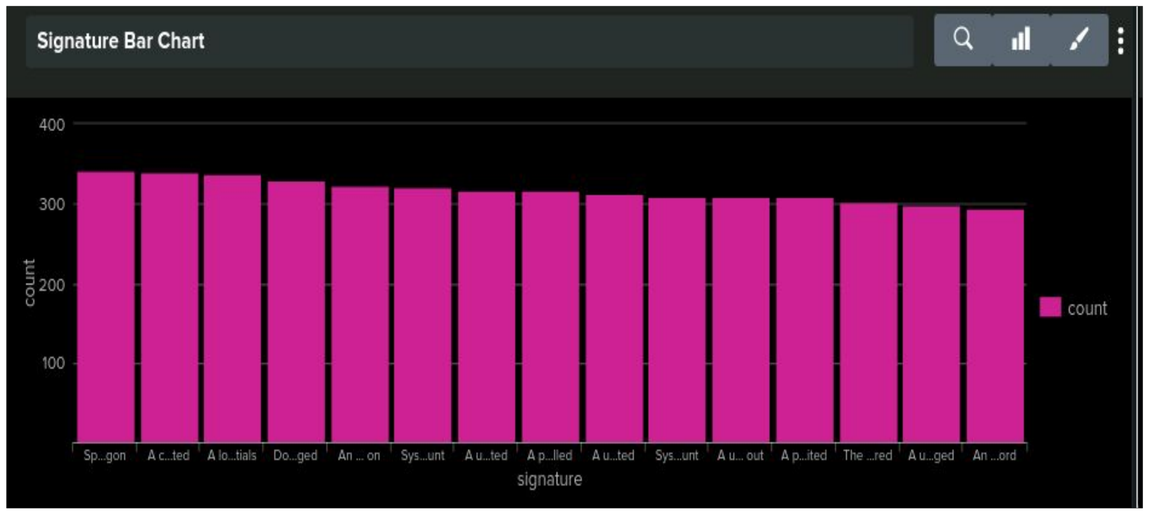
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account_Deleted	Alerts SOC if account deletions for an hour are over the threshold.	22	25

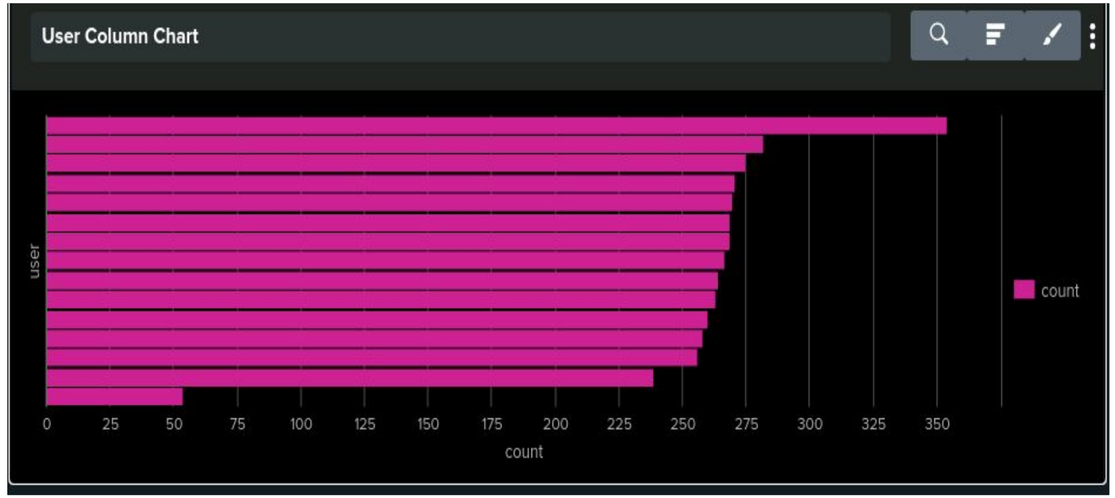
JUSTIFICATION: Our baseline is set to 22 as the normal activity number of successful log on per hour, and the threshold of 25 is considered enough to be a potential attack.

Dashboards—Windows









Dashboards—Windows

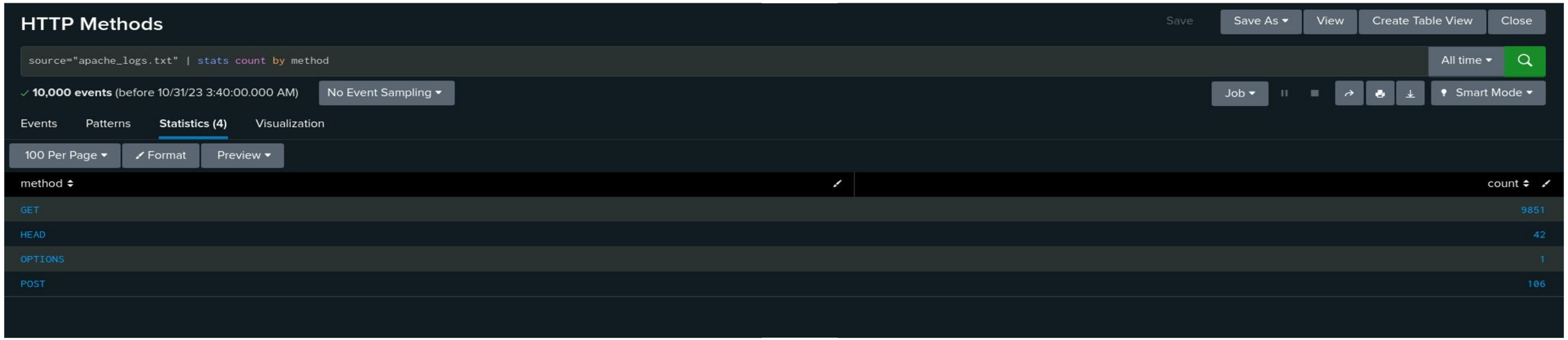
Apache Logs

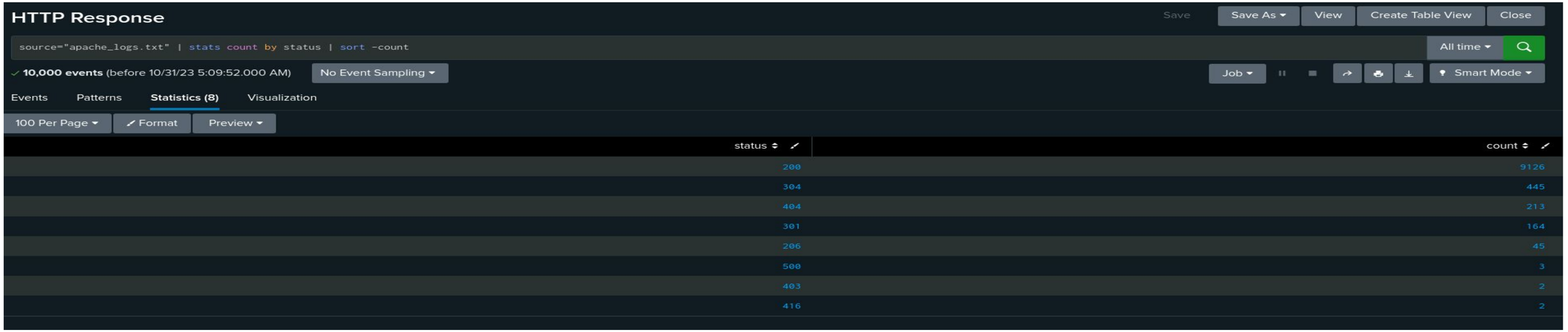
Reports—Apache

Designed the following reports:

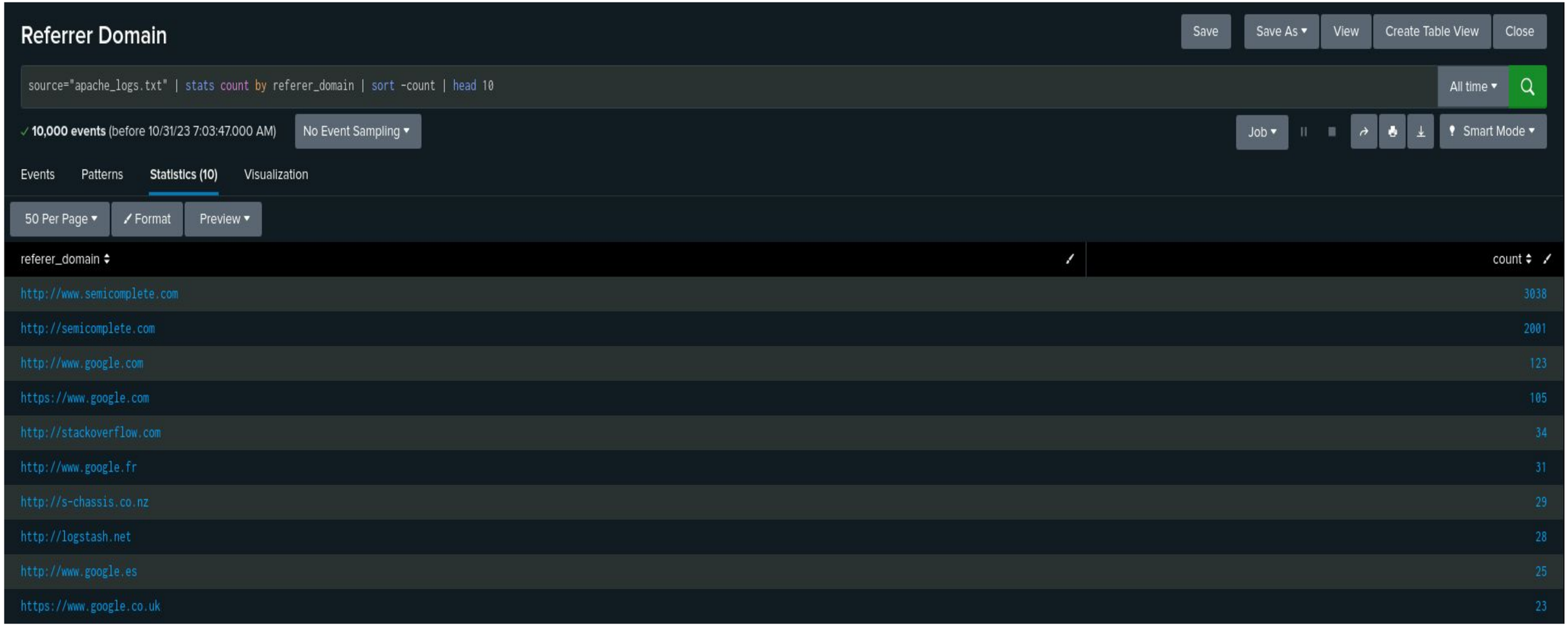
Report Name	Report Description
HTTP Methods	Shows all the HTTP methods given to the Apache server.
Referrer Domains	Shows the top 10 domains refer to the VSI website.
HTTP Response Codes	Shows the different response codes

Images of Reports—Apache





Images of Reports—Apache



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non_US_Traffic	Alerts SOC the non-US IPs identified traffic in 1 hour is over the threshold	75	85

JUSTIFICATION: On average, we see about 75 non-US IPs in one hour. We've set a threshold at 85, which allows normal non-US. clients but also alerts us early if there's suspicious foreign activity.

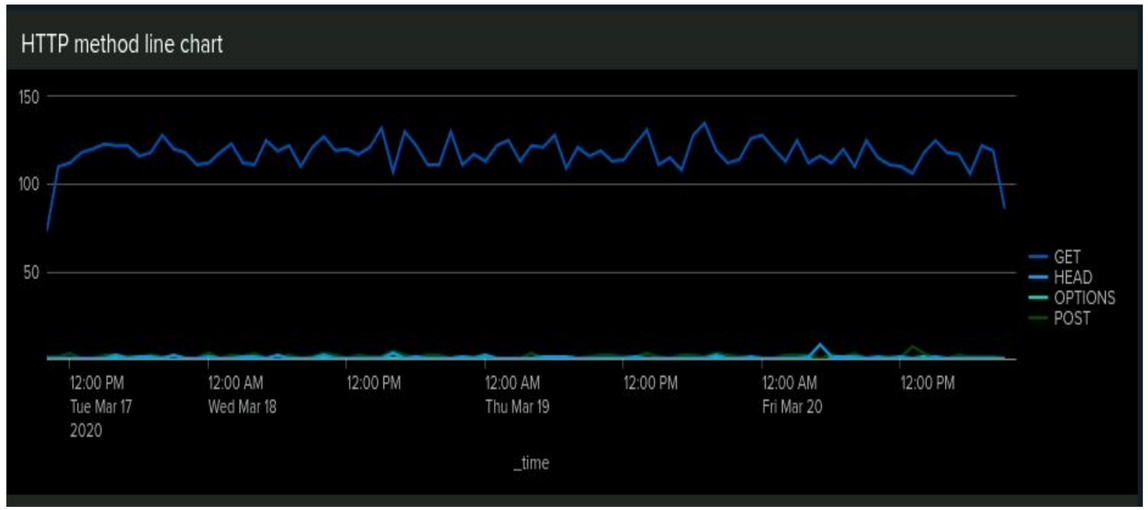
Alerts—Apache

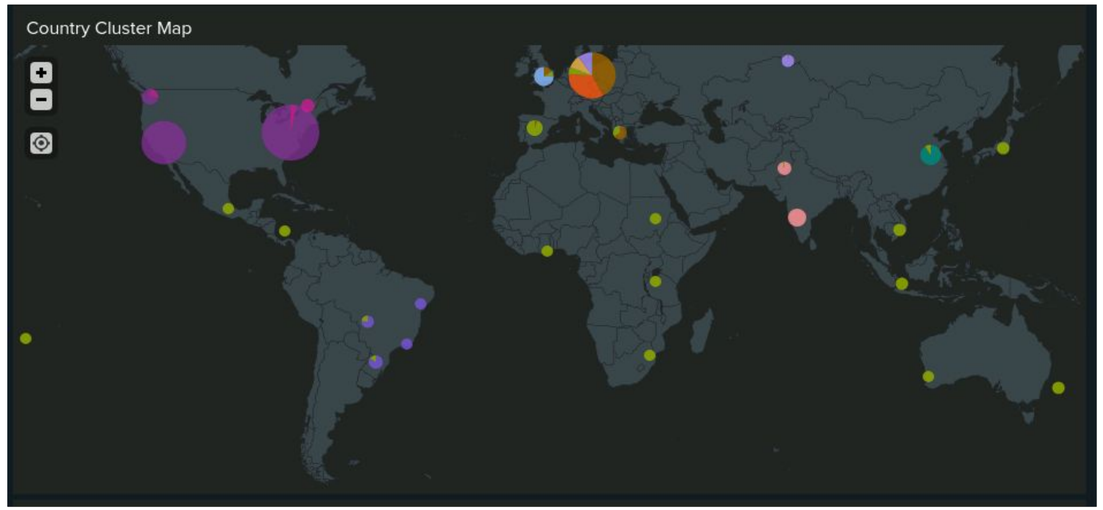
Designed the following alerts:

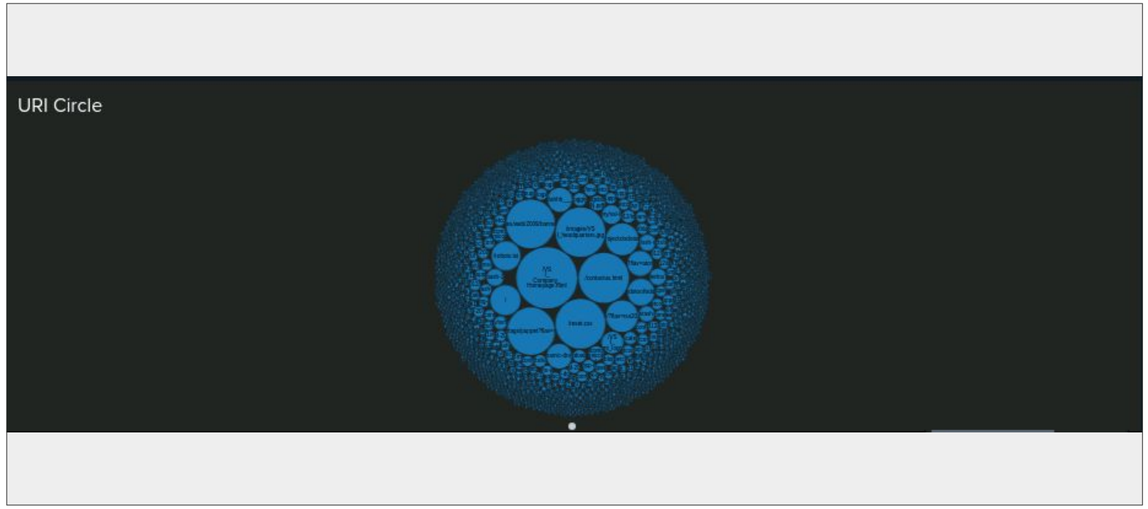
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP_POST	Alerts SOC if the amount of HTTP POST requests made in 1 hour are over the threshold	7	10

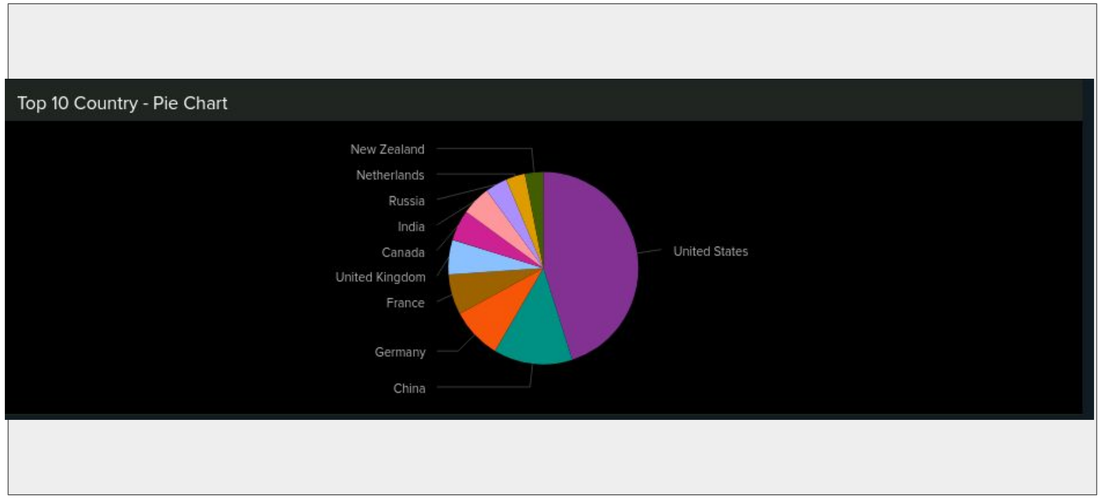
JUSTIFICATION: On average, we see about 7 HTTP POST in one hour. We've set a threshold at 10, which allows normal HTTP POST but also alerts us early if there's suspicious HTTP POST activity.

Dashboards—Apache







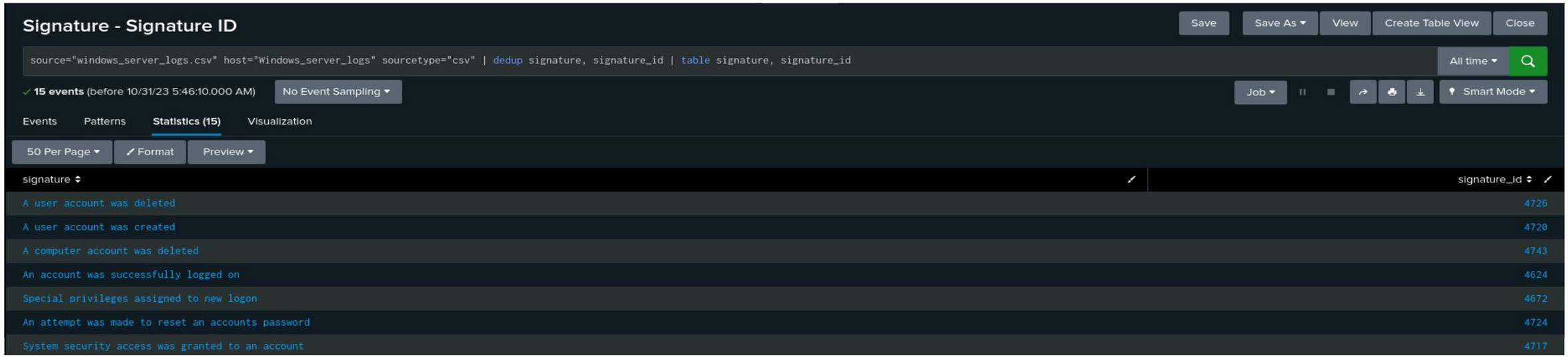


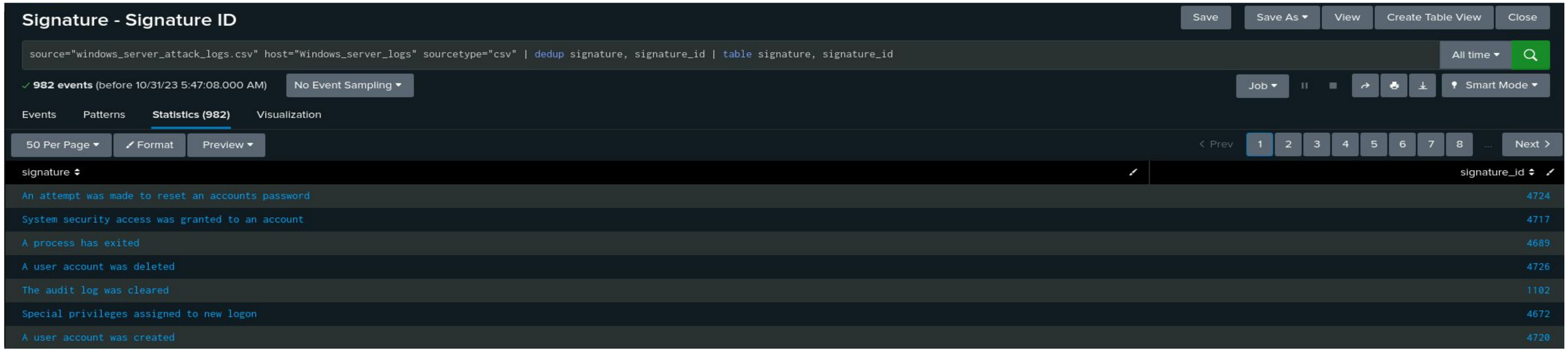
Attack Analysis

Attack Summary—Windows Reports

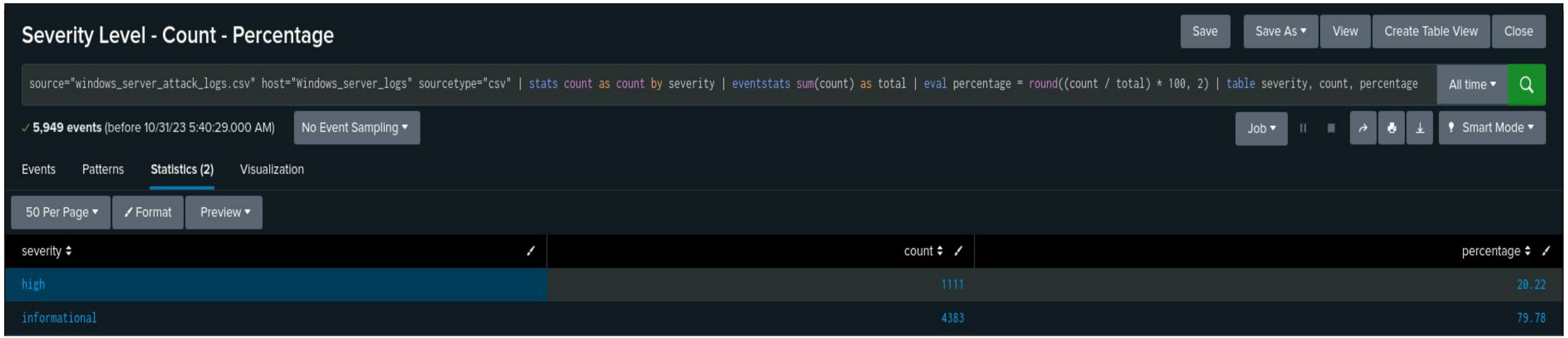
- Windows attack logs indicated a large amount of failed login and password reset which are indicative of a brute-force style attack
- Suspiciously large jump in logs of ‘High’ severity going from 329 to 1111 (6.91% of total - 20.22%)
- Change in signatures names along with corresponding signature_ids affecting results of original report

Images of Reports—Windows Normal vs Attack Logs

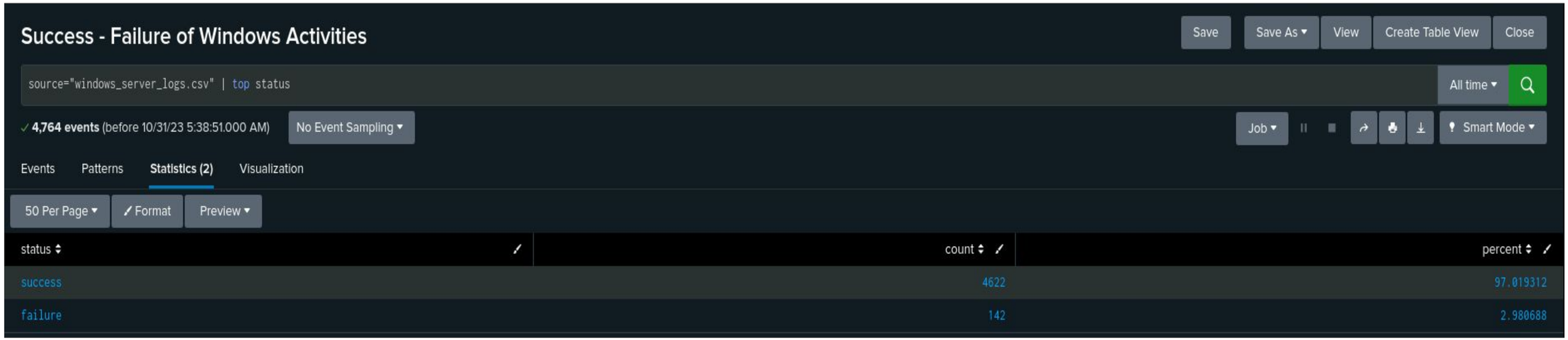


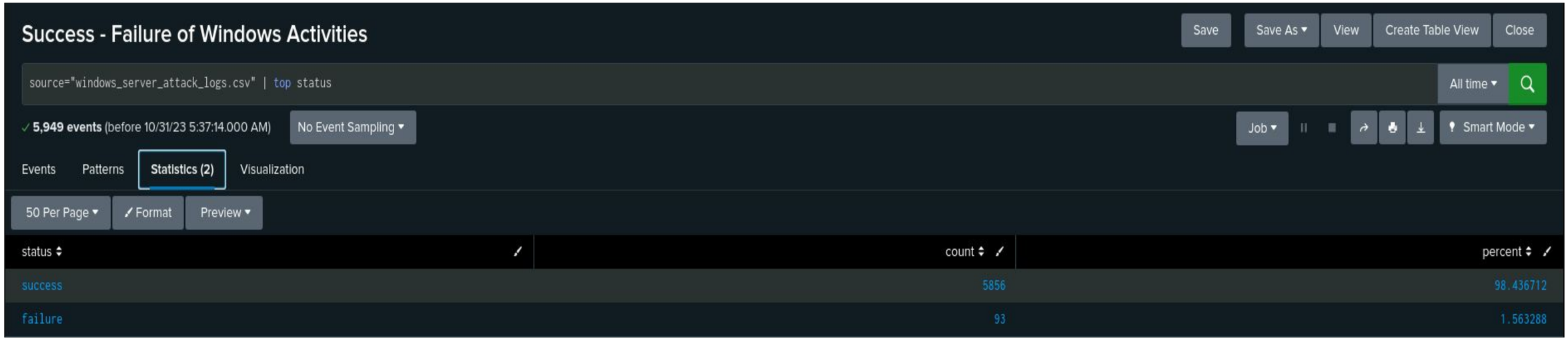


Images of Reports—Windows Normal vs Attack Logs



Images of Reports —Windows Normal vs Attack Logs

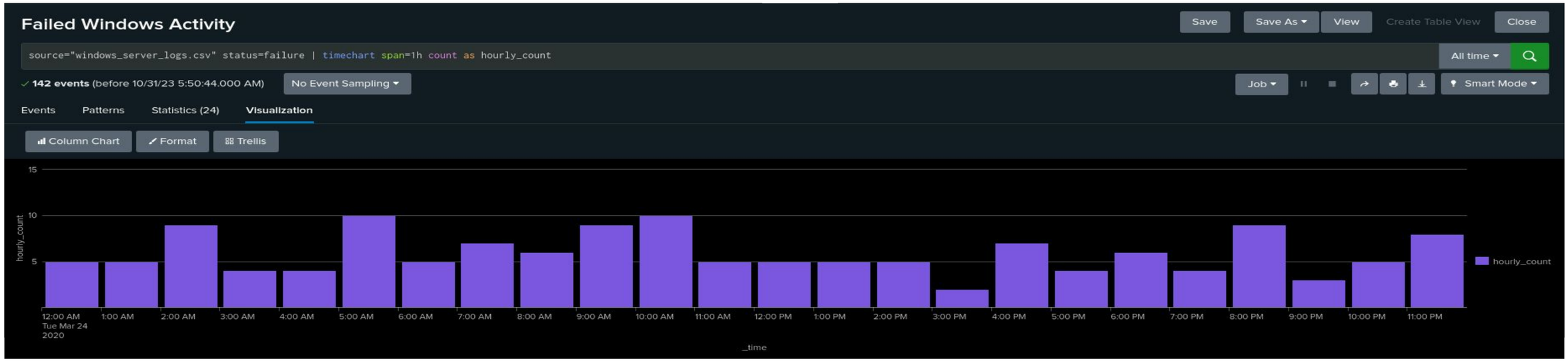


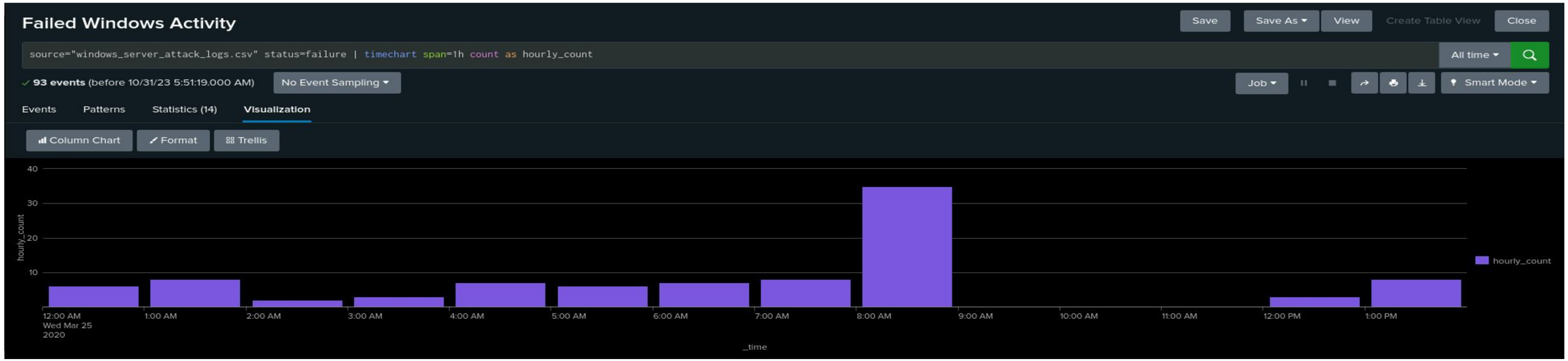


Attack Summary—Windows Alerts

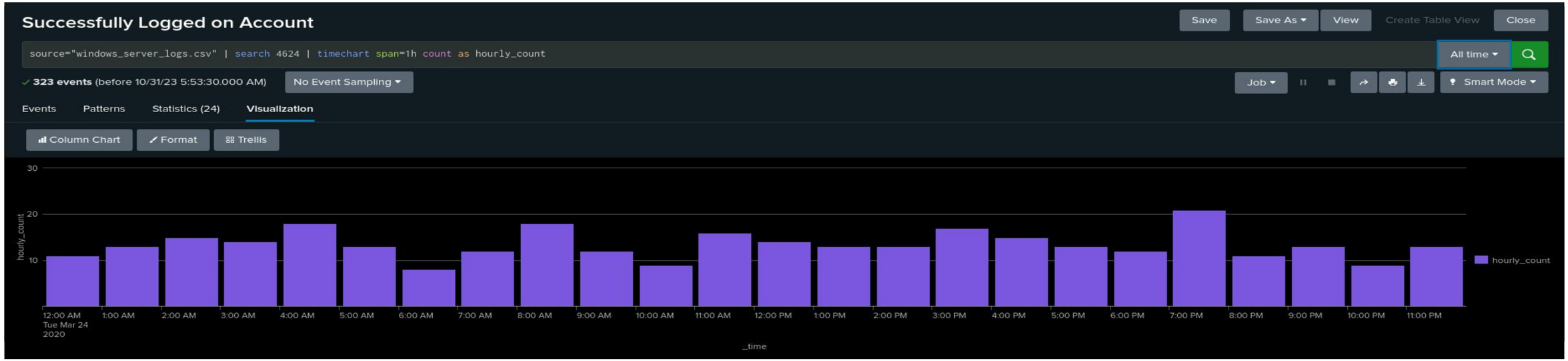
- The alert thresholds for all created alerts were met
- No false positives
- Major jumps of activity in monitored log sections
- Normal range is somewhat consistent in hourly activity throughout the day vs the clustered behaviour of the attack logs indicating suspicious activity
- The changed signature and signature_ids resulted in missing information on the extent of the attack
- The peak number of events on a single user peaked during the attack was 1,256 login attempts throughout the attack

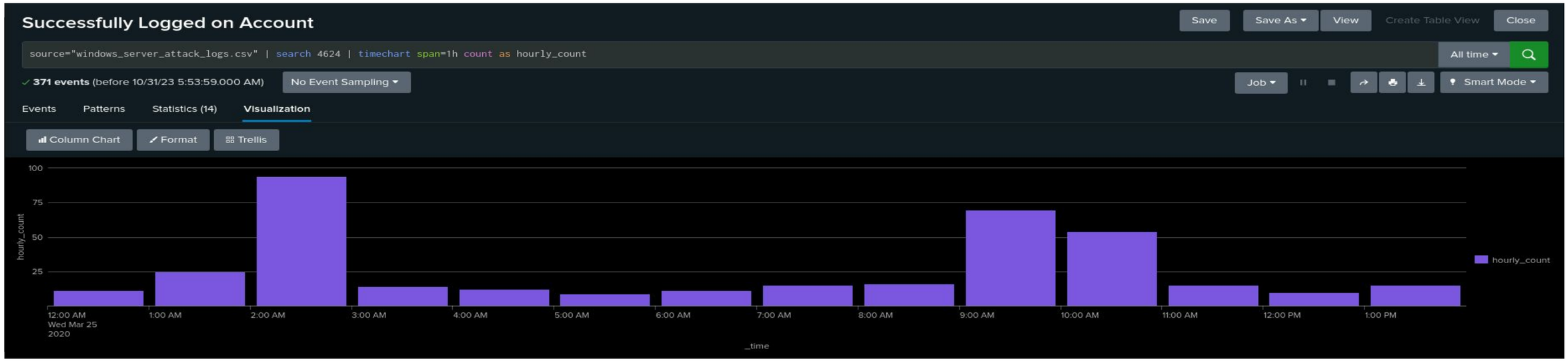
Images of Alerts —Windows Normal vs Attack Logs



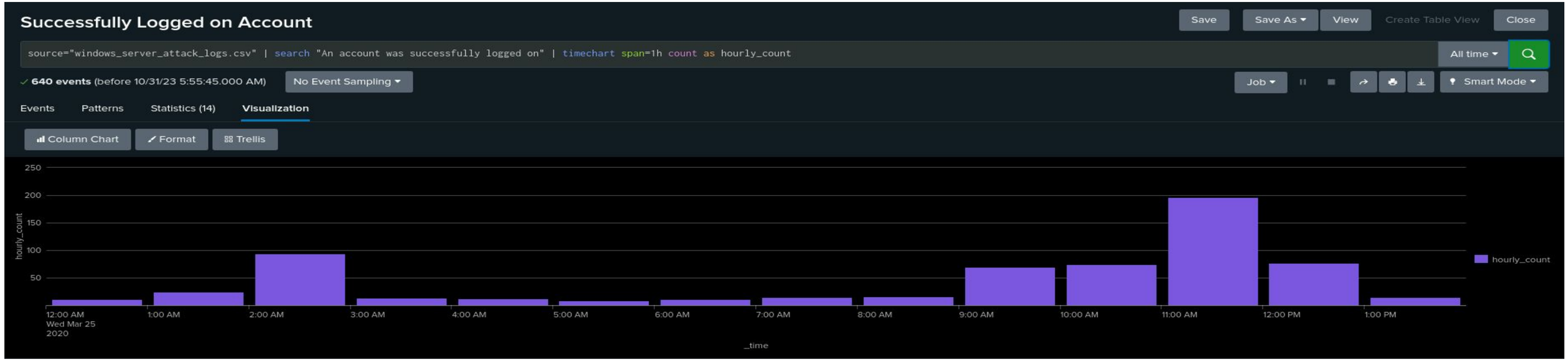


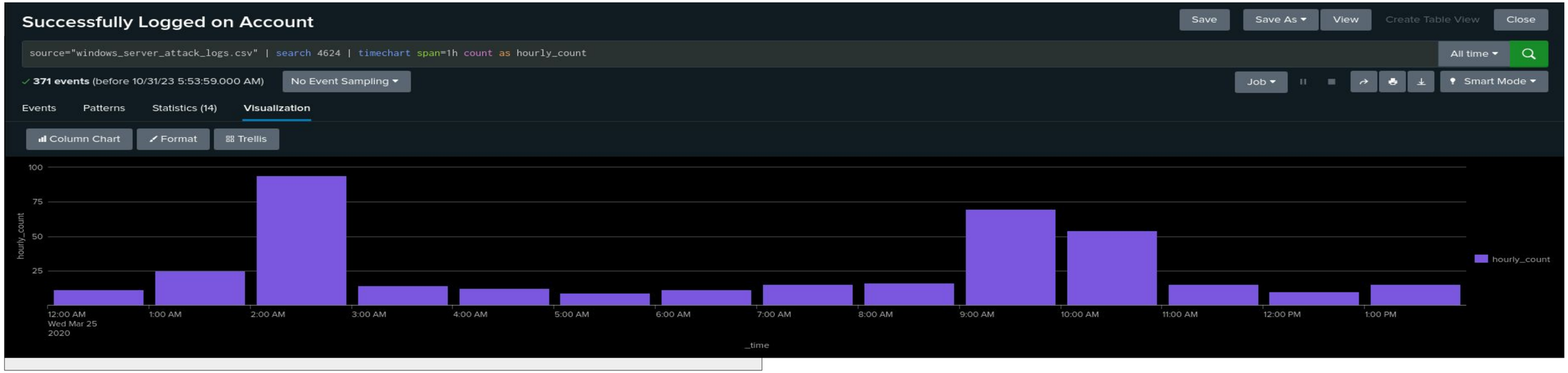
Images of Alerts —Windows Normal vs Attack Logs



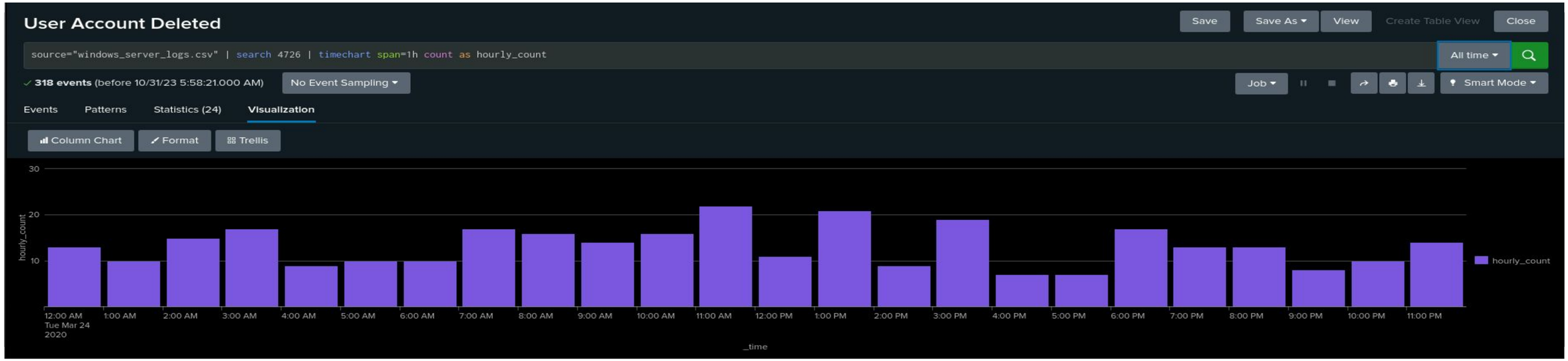


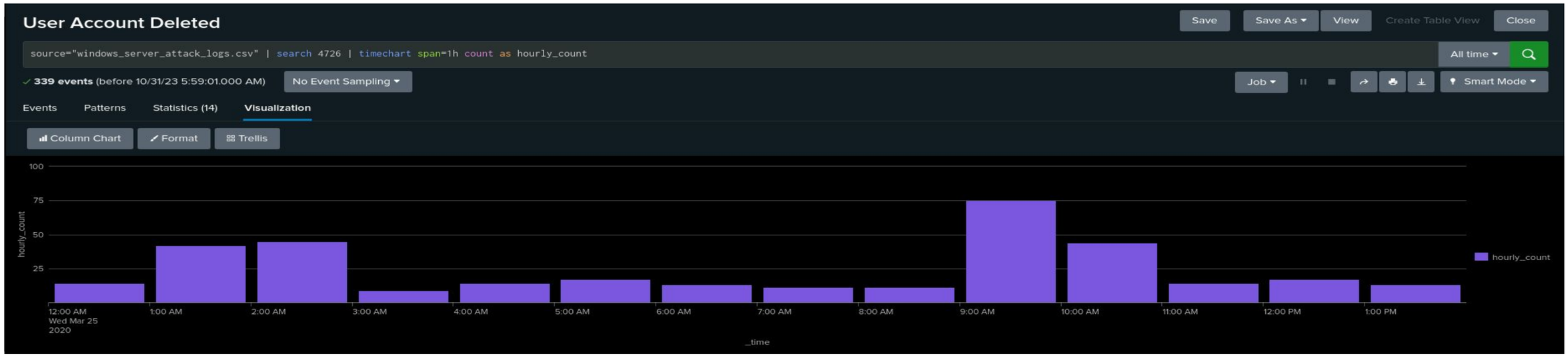
Findings - Differing Results





Images of Alerts —Windows Normal vs Attack Logs

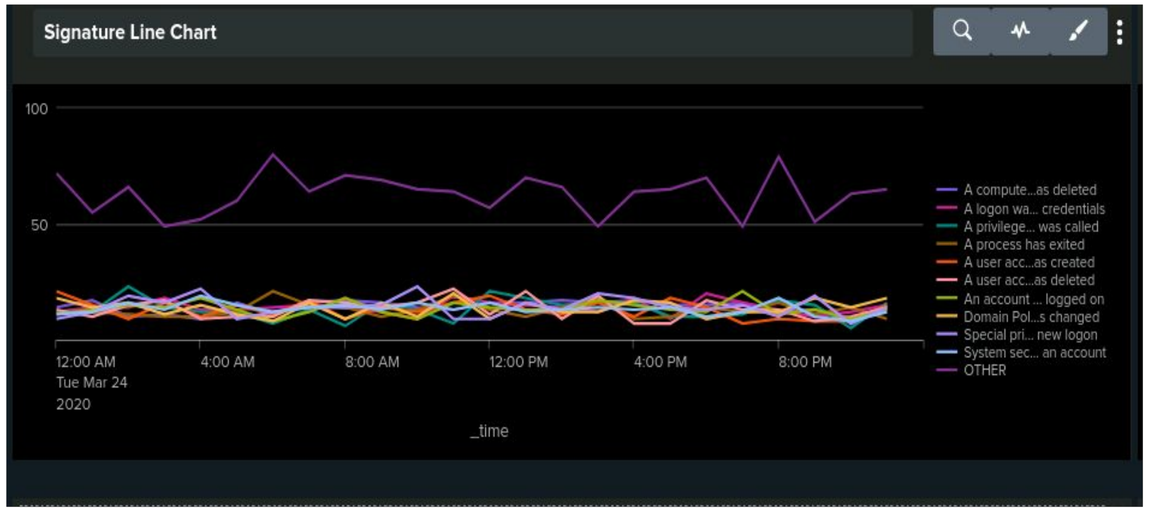


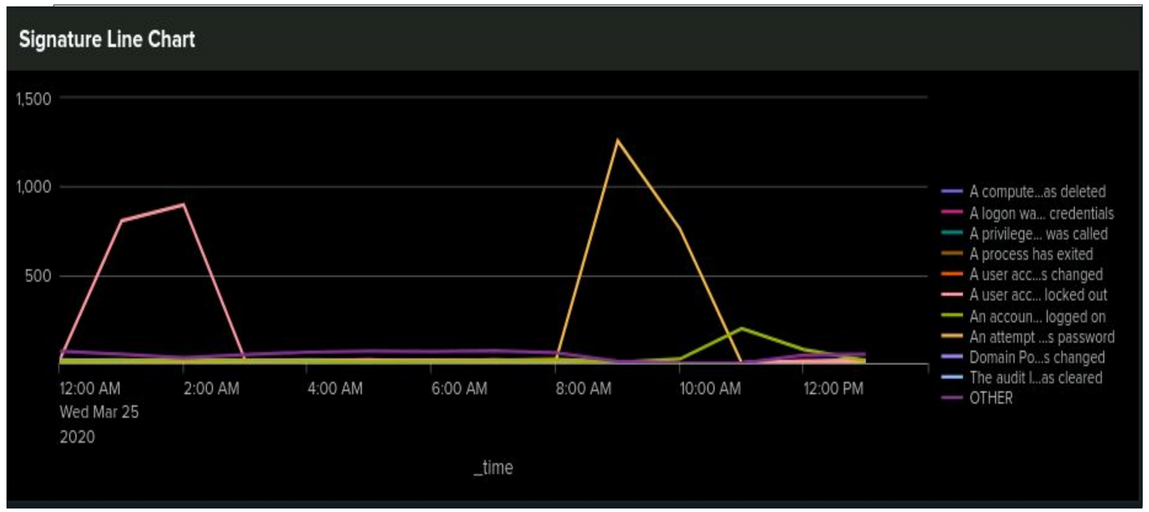


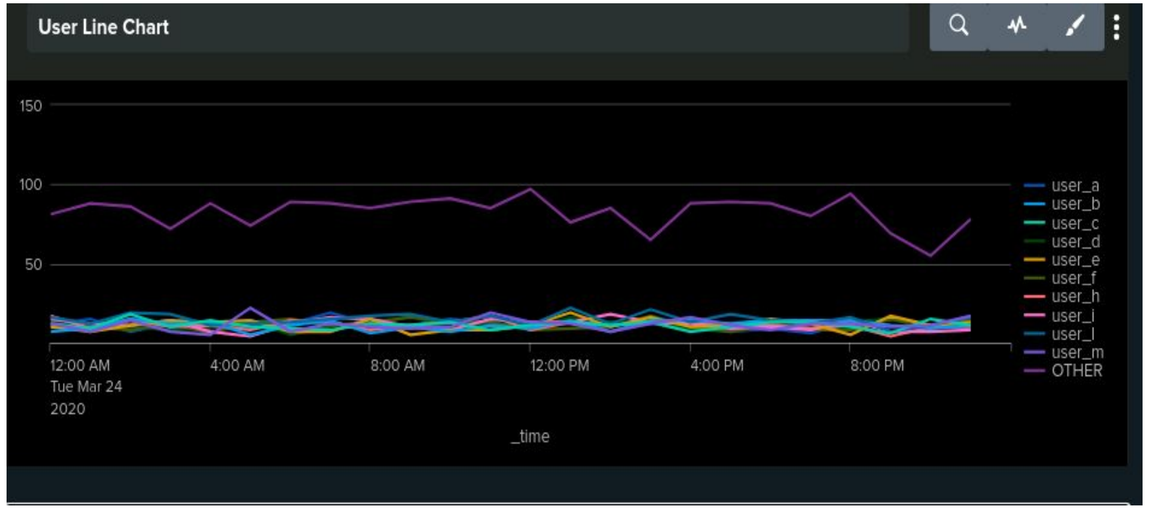
Attack Summary—Windows Dashboards

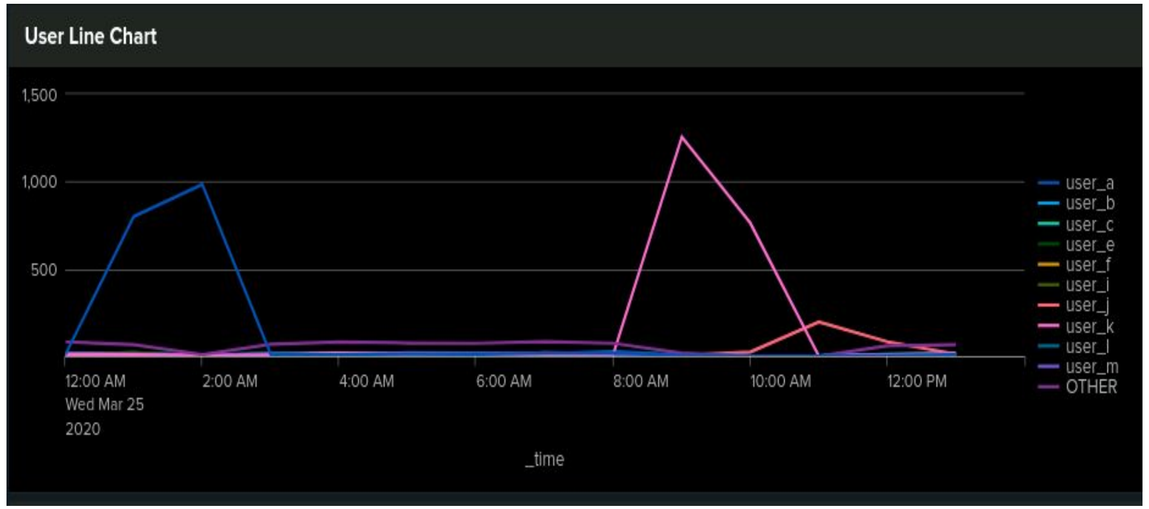
- Shows a significant increase in overall activity compared to the normal levels
- Specific signatures and users experienced major spikes in activity
- Trend connecting the spike of a specific users activity with the specific signature events
- The peak number of events on “A user account was locked out” during the attack is 896 attempts throughout the attack.
- The peak number of events on a “An attempt was made to reset an accounts password” during the attack was 1,258 attempts throughout the attack.
- user_a, user_j, and user_k were responsible for the spike in activity indicating those accounts being compromised

Images of Dashboard - Windows Normal vs Attack Logs

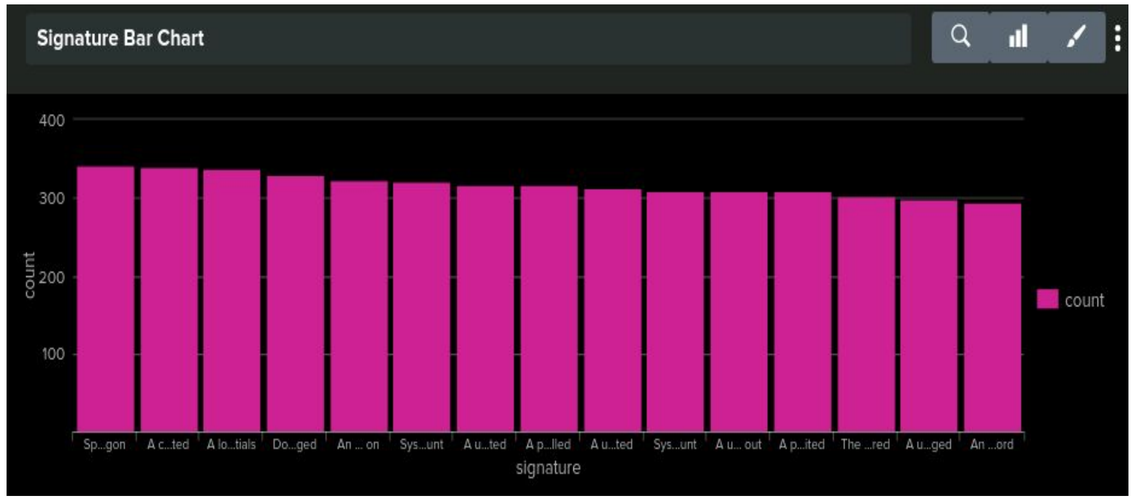


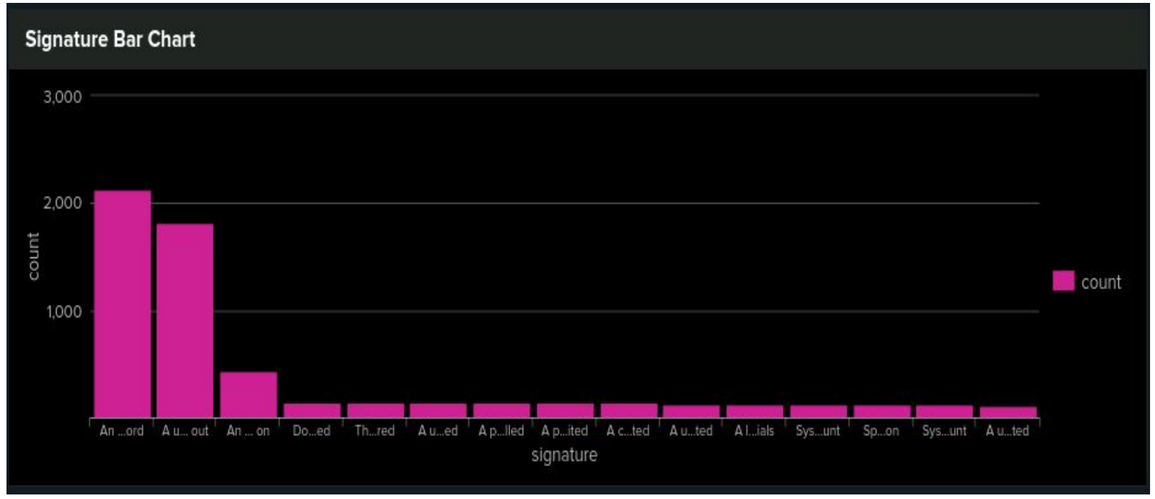


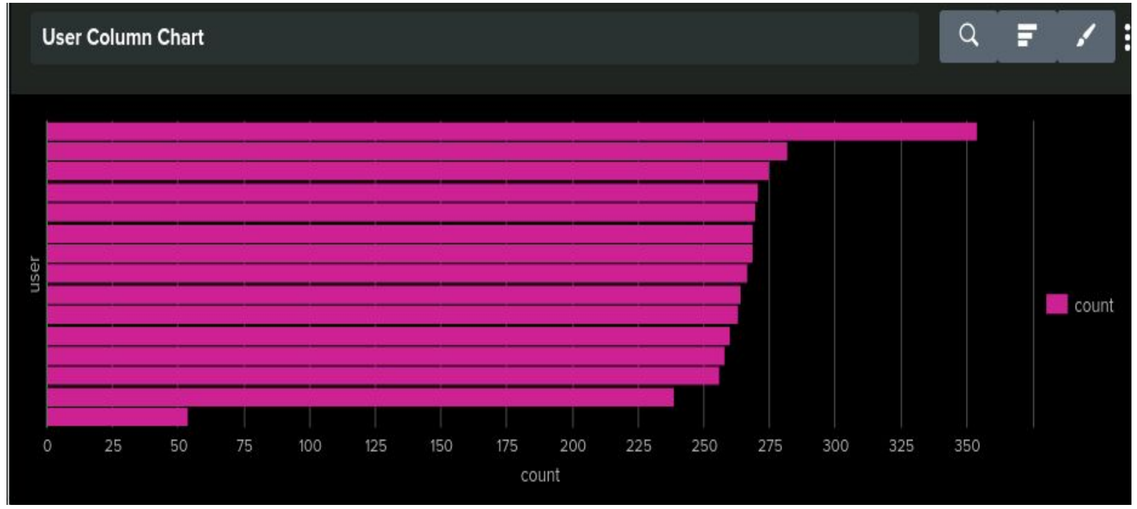


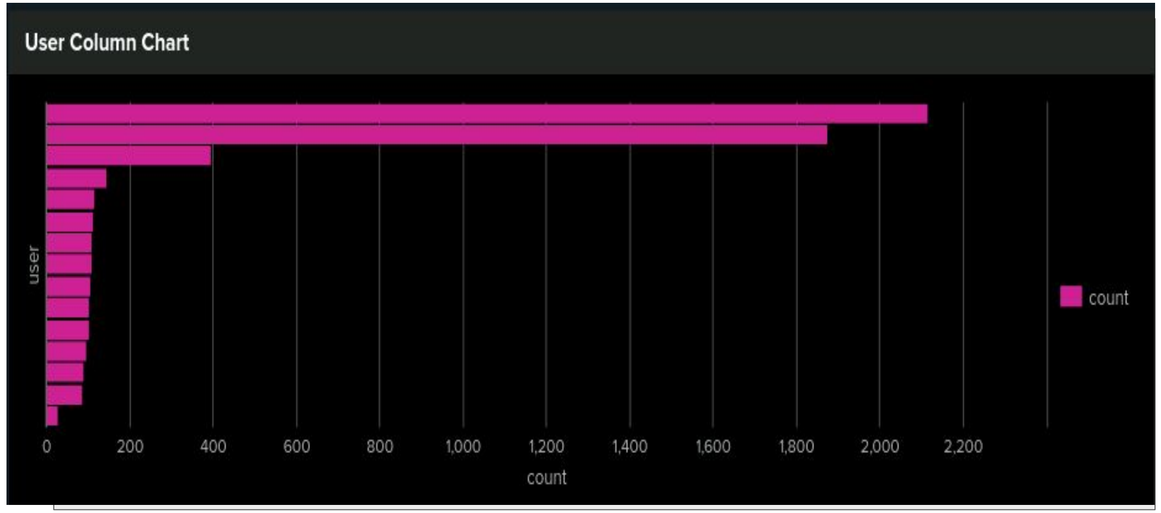


Images of Dashboard - Windows Normal vs Attack Logs





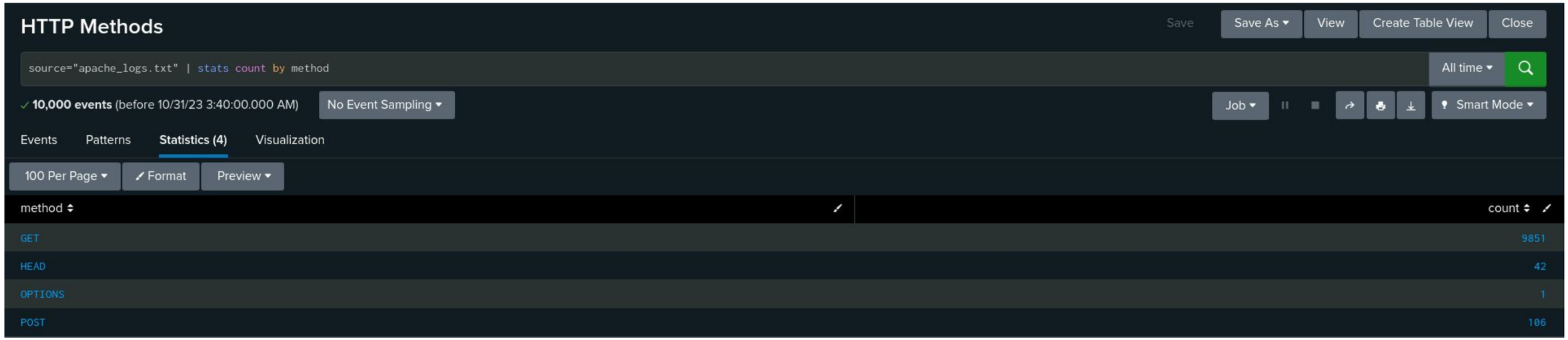


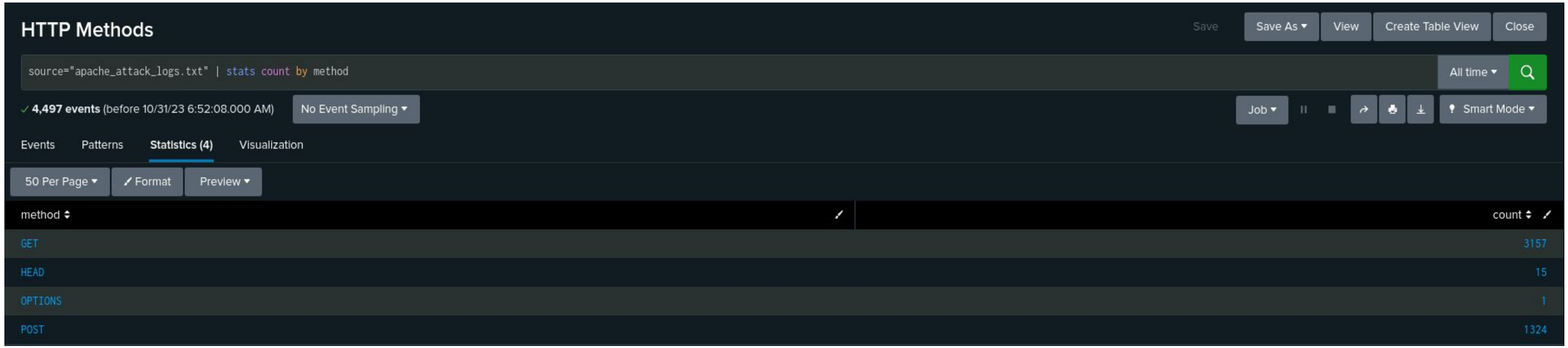


Attack Summary—Apache Reports

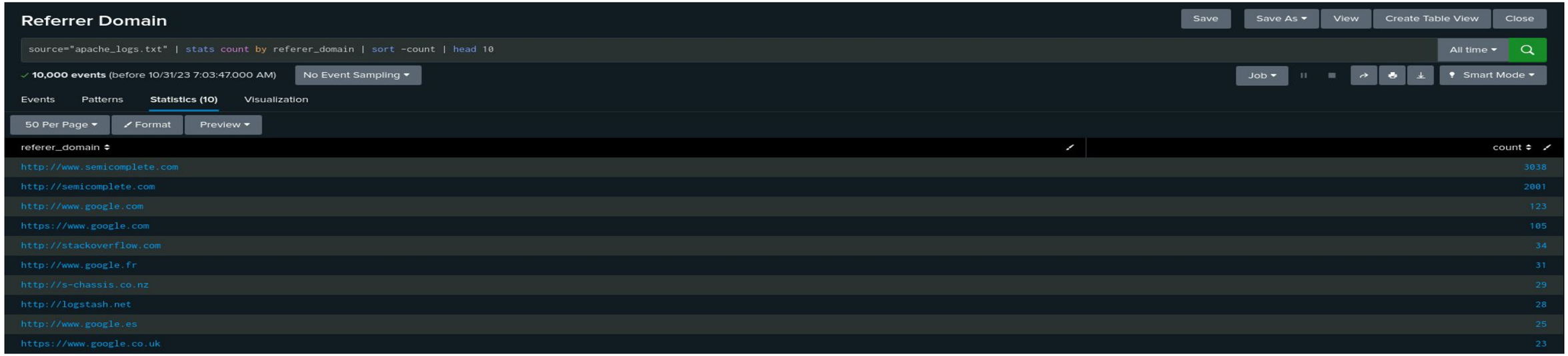
- The attack resulted in a great increase in POST requests as well as a noticeable decrease in GET requests
- During the attack, the total number of HTTP POST requests reached 1,296 compared to the historically normal amount of 106 requests
- Drop in Referrer Domain activity
- Over 3 times the total count of 404 responses with less than half the activity
  - Indicates something affecting the servers ability to find the requested web pages

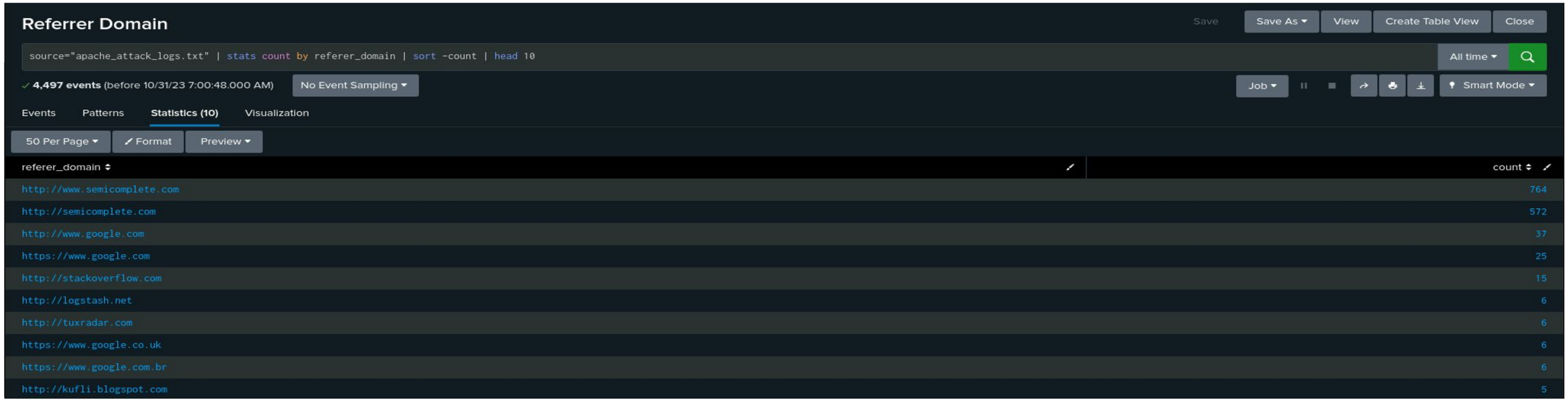
Images of Reports—Apache Normal vs Attack Logs



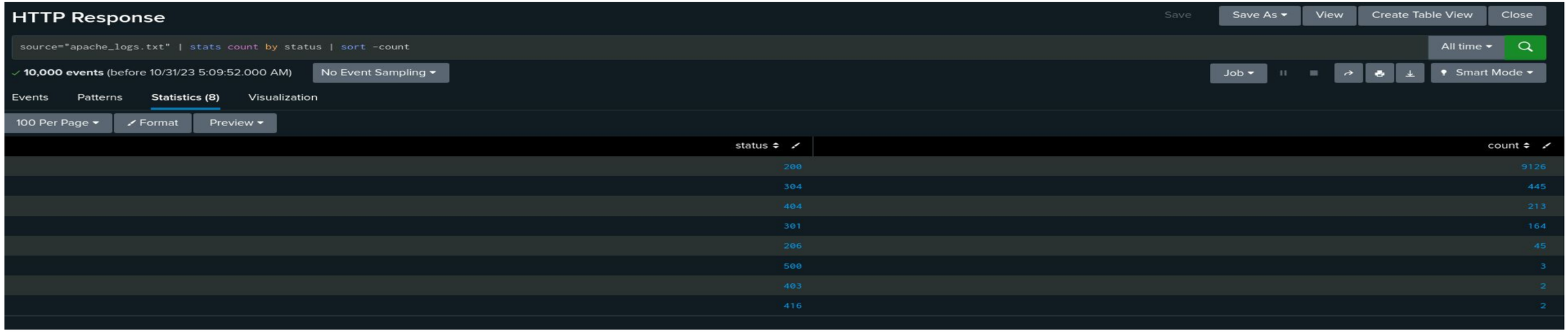


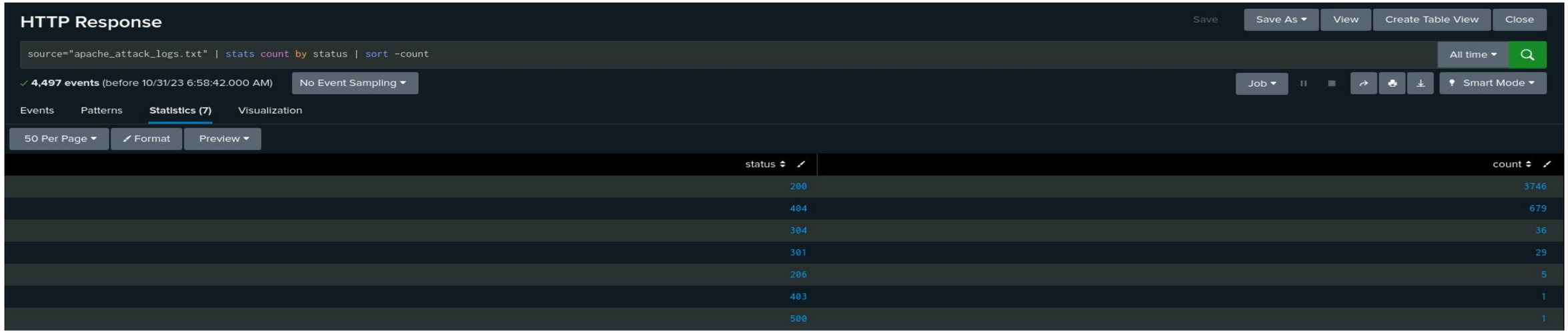
Images of Reports—Apache Normal vs Attack Logs





Images of Reports—Apache Normal vs Attack Logs

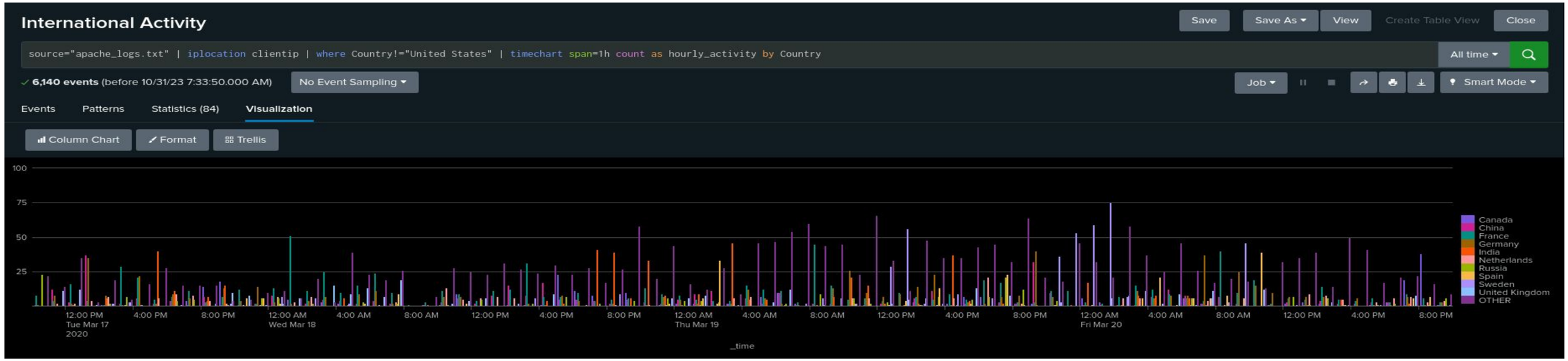


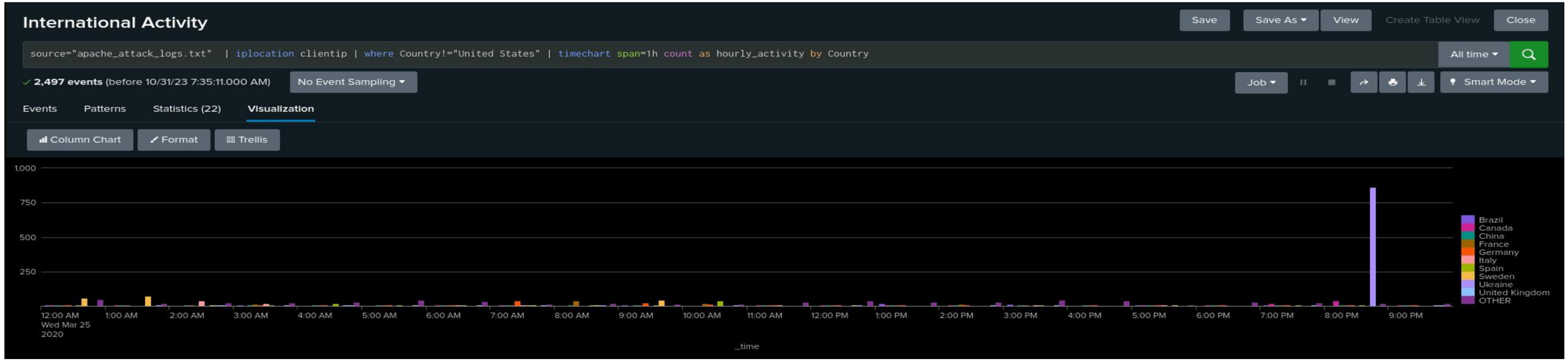


Attack Summary—Apache Alerts

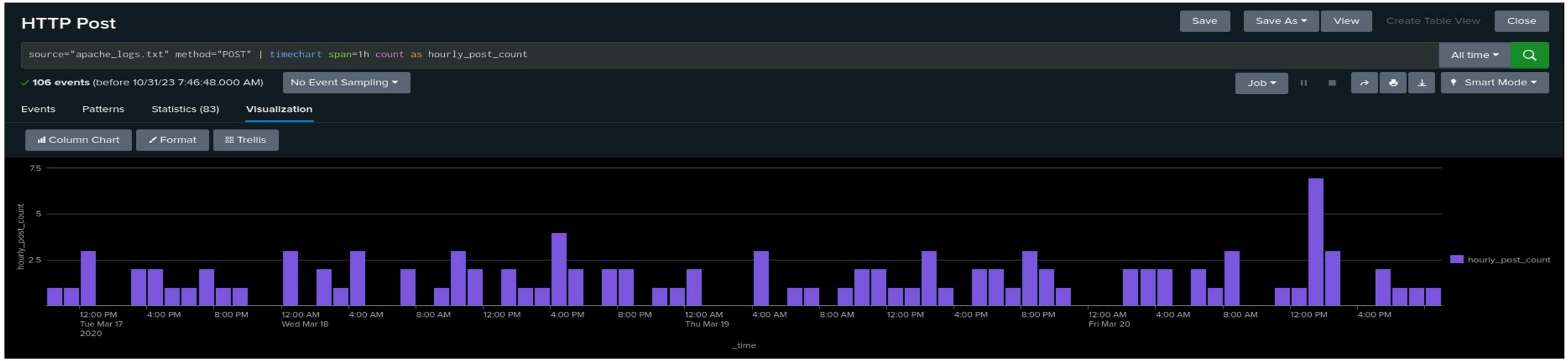
- The alert thresholds for all created alerts were met
- No false positives
- Major jumps of activity in monitored log sections
- Normal range is somewhat consistent in hourly activity throughout the day vs the clustered behaviour of the attack logs indicating suspicious activity
- Shows that the attack was not sustained due to the high activity only occurring in short bursts
- Confirmed the attack to be coming from ukraine and at 8pm with a substantial spike in activity coming from ukraine as well as HTTP POST activity at the same time

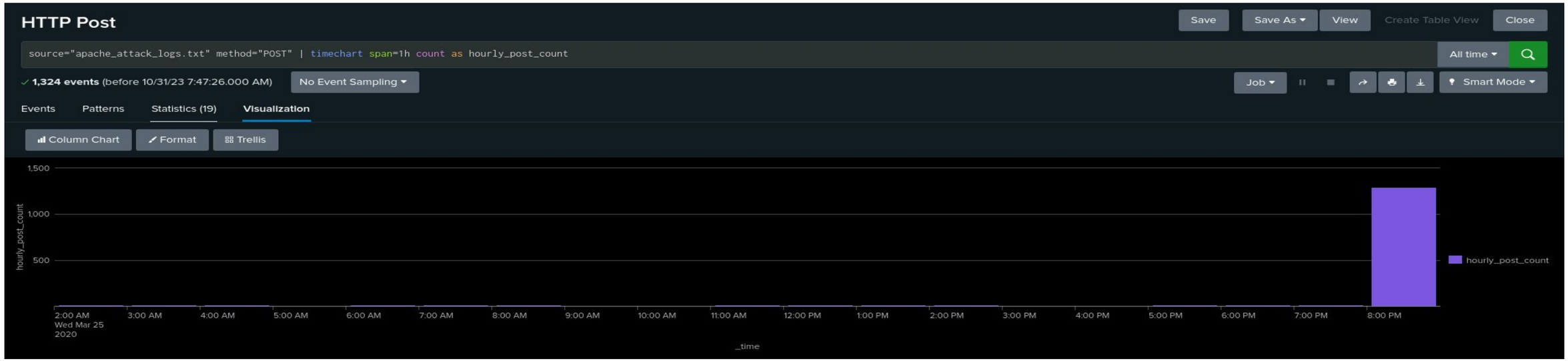
Images of Alerts—Apache Normal vs Attack Logs





Images of Alerts—Apache Normal vs Attack Logs

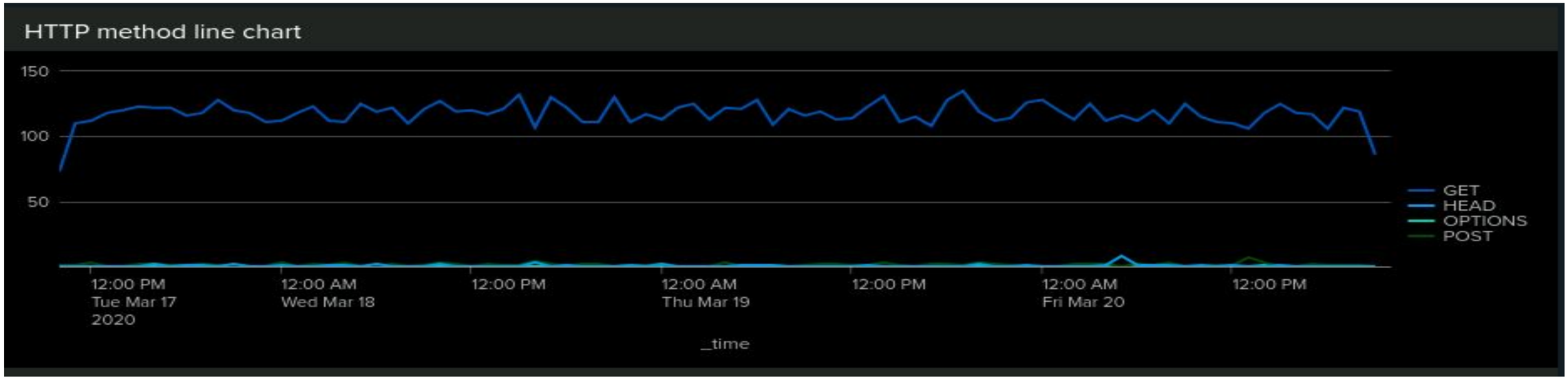


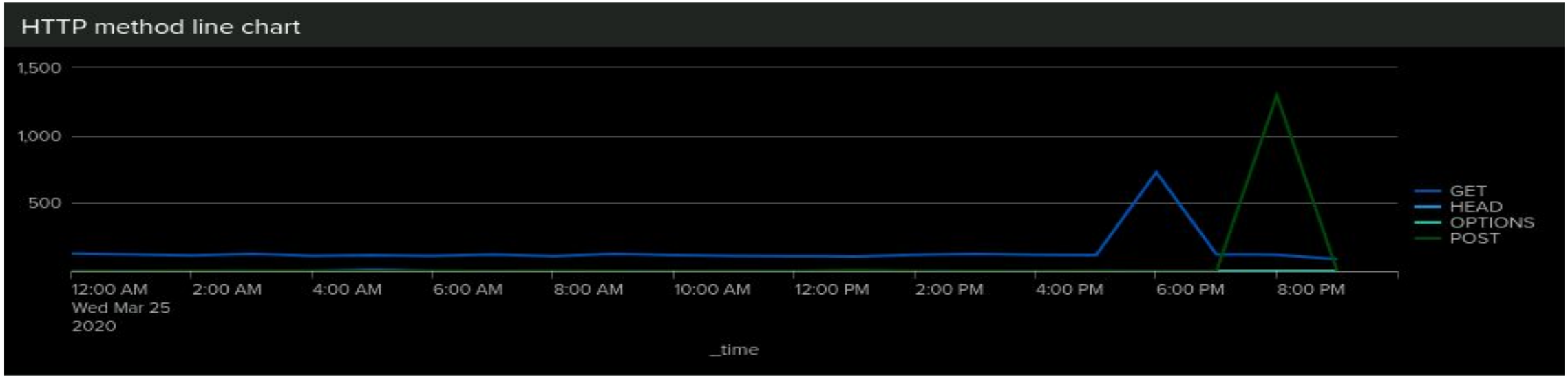


Attack Summary—Apache Dashboards

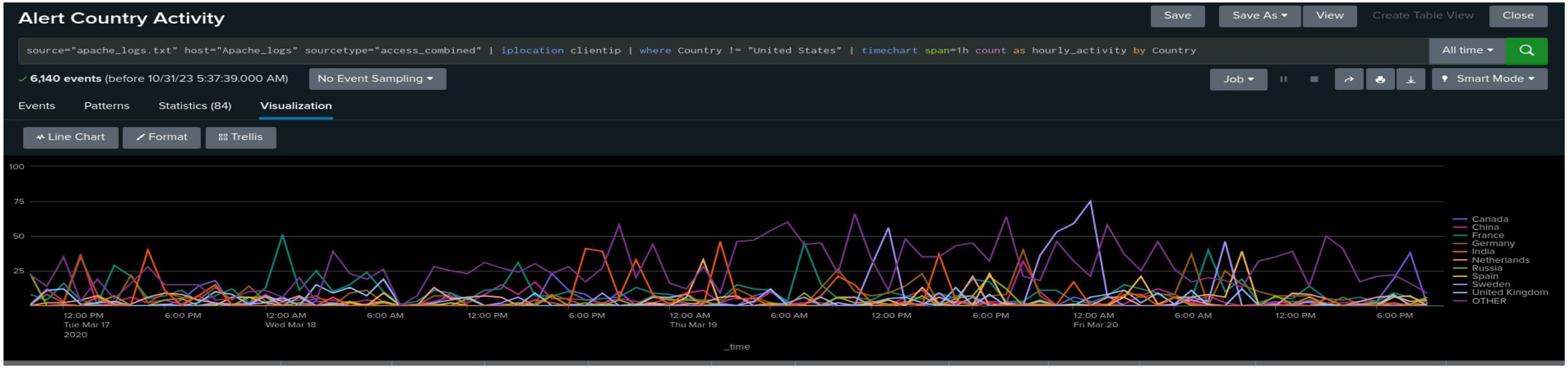
- Apache attack logs showed a large number of increase in HTTP POST requests from foreign sources, which indicate a Denial of Service style attack.
- The dashboard showed information on the time and location of the attack.
- Specific country (Ukraine), specific HTTP Method (GET and POST), and specific URI’s show major differences in activity.

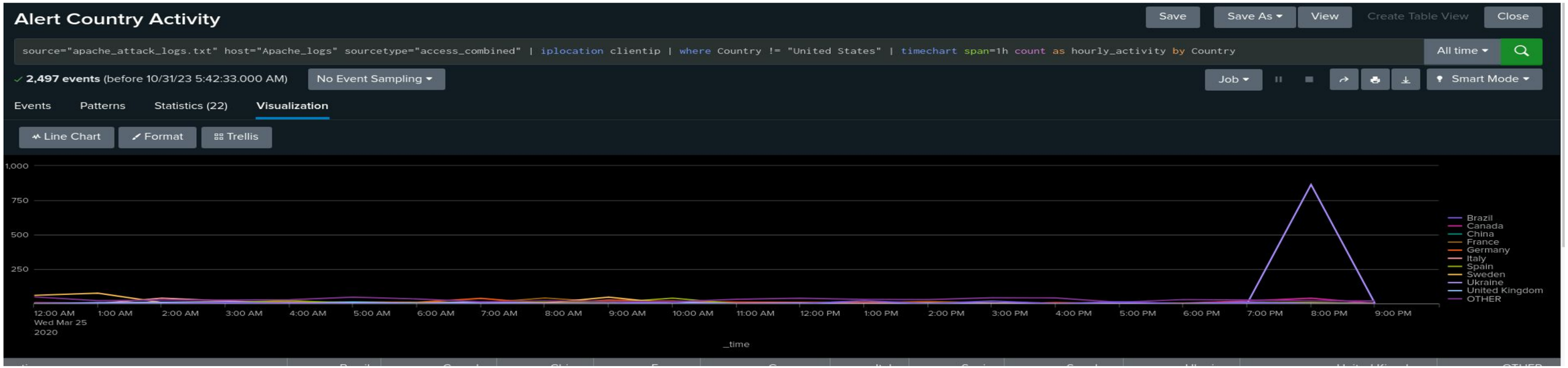
Images of Dashboard—Apache Normal vs Attack Logs



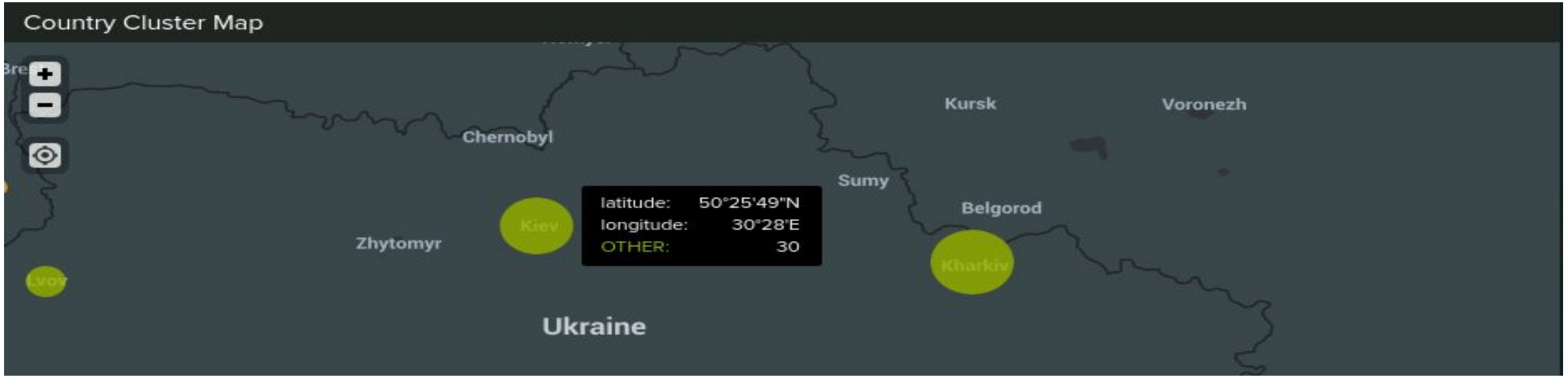


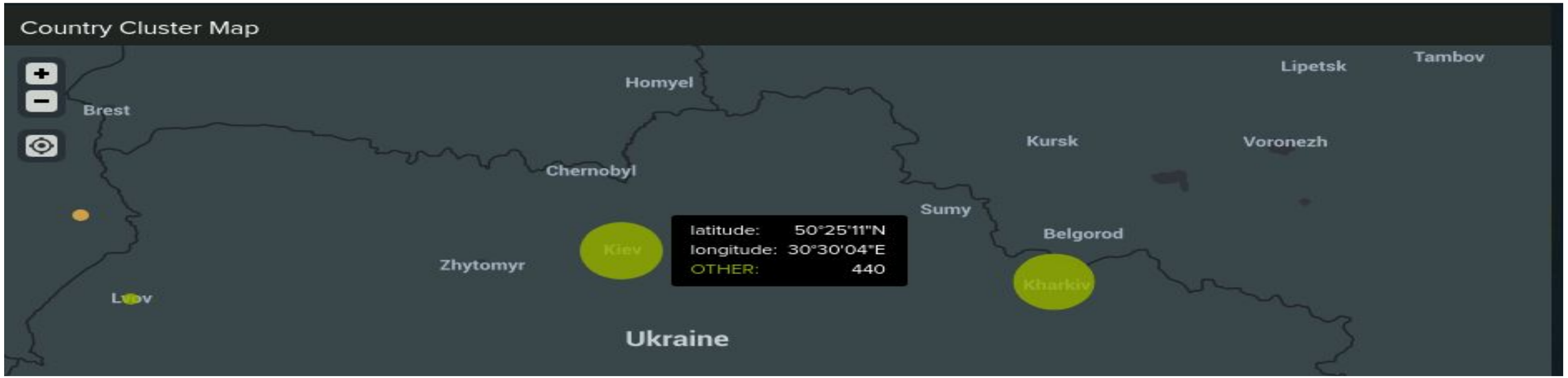
Images of Dashboard—Apache Normal vs Attack Logs



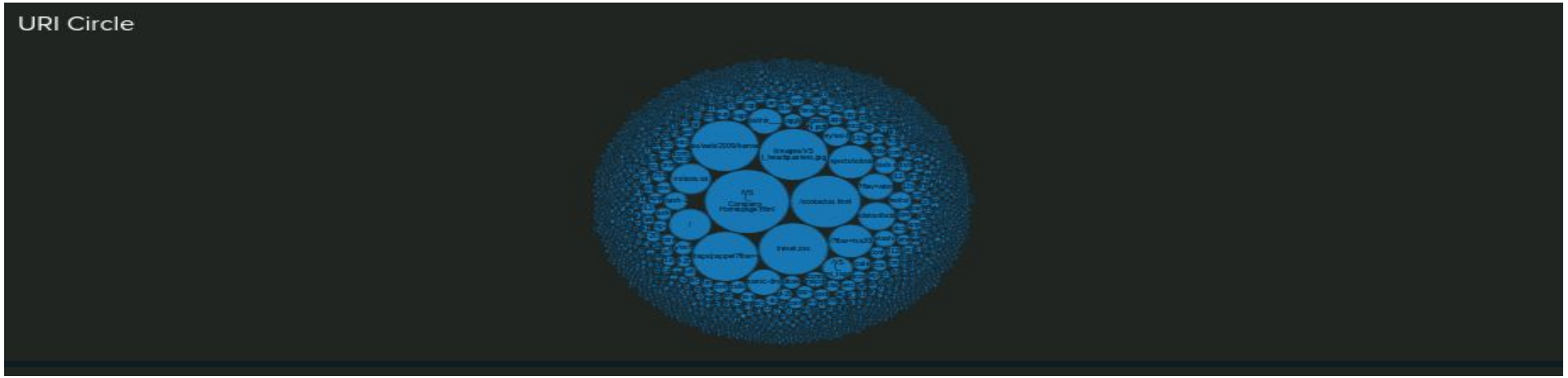


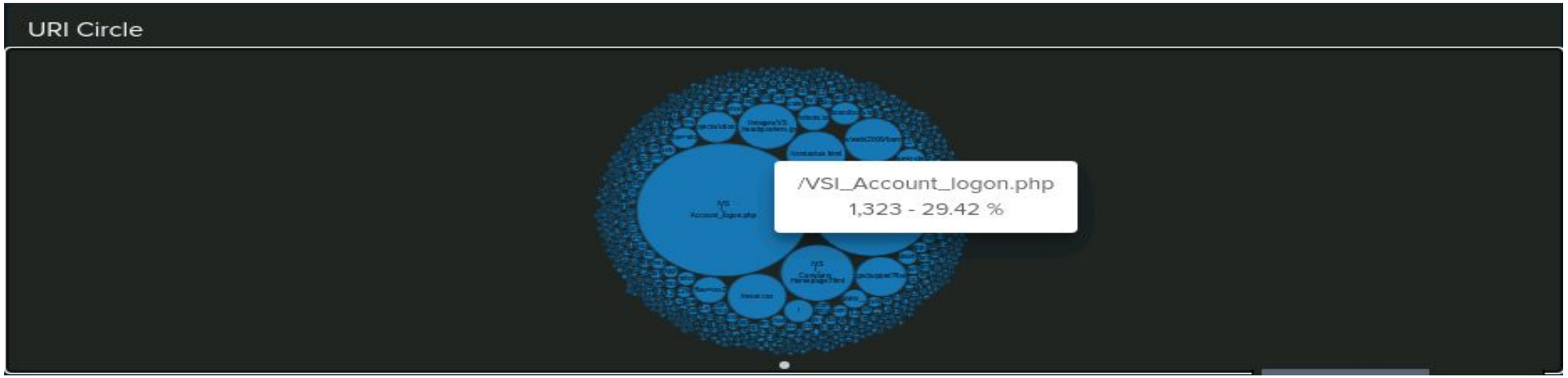
Images of Dashboard—Apache Normal vs Attack Logs





Images of Dashboard—Apache Normal vs Attack Logs





Summary and Future Mitigations

Project 3 Summary

Findings

Foreign state actors from Ukraine carried out a brute force attack also potentially causing a Denial of Service (DoS) condition as a byproduct, on VSI's Apache servers. They flooded the website with HTTP POST requests combined with the spiked activity found within the "/VSI_Account_logon.php" URI.

A brute force attack was also carried out on the windows servers as a means of entry into VSI's back-end servers. This was carried out through accessing multiple vulnerable users. The set thresholds and baselines did detect the attacks and notified VSI's security team accordingly, however to improve the ability to detect these attacks as early as possible, lowering both the baseline and threshold can be deemed beneficial. This follows a method of maximum safety at the sacrifice of some efficiency due to the increased alerts to be analysed. Utilising this method will allow for early detection as well as improving the company's chances of stopping an attack before it even starts.

Project 3 Summary

Mitigation Methods

- Utilise the alerts created to swiftly respond to potential attacks
- Implement multi factor authentication and account lockout policies for brute force attacks
- Include stronger password policies on users to defend against any brute force attacks
- Implement rate limiting to restrict the number of HTTP methods
  - For example GET and POST requests, to prevent DoS attacks
- Constantly analyse traffic and activity to detect any abnormalities
- IP Blocking can defend against specific IP addresses deemed suspicious