

Defensive Security Project

by: Group 2

Table of Contents

This document contains the following resources:

01

**Monitoring
Environment**

02

Attack Analysis

03

**Project Summary
& Future
Mitigations**

Monitoring Environment

VSI Security: Splunk Analysis of Server Logs

Scenario: Virtual Space Industries is a small tech company that designs virtual-reality programs for their clients. They are concerned that one of their competitors, JobeCorp, may initiate some sort of cyber attack against their servers. As an analyst in their SOC, we have been tasked with analyzing the logs for both their Windows and Apache Servers to determine several baselines for normal activity. Specifically, we baselined the following fields using Splunk on day 1 and then created reports and alerts for each field in question.

Windows Server

- signature_id
- signature
- user
- status
- severity

Apache Server

- method
- referer_domain
- status
- clientip
- useragent

On day 2, we were provided a second set of logs in order to compare them to our baselines and analyze any alerts these logs may have triggered. From there we were to try and establish if any suspicious activity transpired on either server and report our findings.

The background of the slide is a dark red color with a complex geometric pattern. This pattern is composed of numerous triangles of varying sizes, some pointing upwards and some downwards, creating a tessellated effect. The triangles are in different shades of dark red, giving the background a textured, crystalline appearance.

["Add-On" App]

[Splunk Security Essentials]

The add-on provides several useful features such as:

- 1) The “use case library” allows you to reference common security scenarios such as malware detection, insider threats and phishing attacks and quickly implement SPL queries.
- 2) The add-on comes loaded with prebuilt searches and report templates tailored to each security use case.
- 3) Guidelines for best practices when configuring and deploying Splunk.
- 4) Extensive database of training materials.
- 5) Community contributions are encouraged and allow users to share their use cases, searches, reports and dashboards with the Splunk community.
- 6) Dashboards and visualizations.

[Splunk Security Essentials use case Scenario]

Scenario: Your manager needs you to quickly set up Splunk to search for a basic Malware outbreak, a potential insider threat and inactive accounts that have suddenly become active. You are a junior analyst and some of these SPL queries are quite advanced. You can reference the Security Content on Security Essentials and quickly implement these searches by using the use-cases feature.

[Splunk Security Essentials]

Stage 1: Collection

You have the data onboarded, what do you do first?

Access to In-Scope Resources

Visibility into who is accessing in-scope resources is key to your GDPR efforts. Splunk allows easy analysis of that information.

Featured

Searches Included

Access to In-Scope Unencrypted Resources

Unencrypted communications leaves you vulnerable to a data breach -- when users access PII data, ensure that all connections are encrypted.

Featured

Searches Included

Authentication Against a New Domain Controller

A common indicator for lateral movement is when a user starts logging into new domain controllers.

Featured

Searches Included

Remote Services

Basic Brute Force Detection

Uses a simple threshold for Windows Security Logs to alert if there are a large number of failed logins, and at least one successful login from the same source.

Featured

Searches Included

Brute Force

Basic Malware Outbreak

Looks for the same malware occurring on multiple systems in a short period of time.

Featured

Searches Included

User Execution

Exploitation for Privilege Escalation

Greenhouse Attack

Phishing

Basic Scanning

Looks for hosts that reach out to more than 500 hosts, or more than 500 ports in a short period of time, indicating scanning.

Featured

Searches Included

Remote System Discovery

Network Service Discovery

Basic TOR Traffic Detection

The anonymity of TOR makes it the perfect place to hide C&C, exfiltration, or ransomware payment via bitcoin. This example looks for ransomware activity based on FW logs.

Featured

Searches Included

Non-Application Layer Protocol

Credentials In File Detected

Detect known credential patterns inside data indexed in Splunk.

Featured

Searches Included

Exploitation for Credential Access

Unsecured Credentials

Detect Credit Card Numbers using Luhn Algorithm

Detect if any log file in Splunk contains Credit Card numbers.

Featured

Searches Included

Data Staged

Endpoint Uncleaned Malware Detection

Detect a system with a malware detection that was not properly cleaned, as they carry a high risk of damage or disclosure of data.

Featured

Searches Included

User Execution

Spearphishing Link

Phishing

Flight Risk Web Browsing

This search implements several heuristics to look for indications that a user is a flight risk from Web Logs. Detect a user who may be leaving before they do.

Featured

Searches Included

Increase In # of Hosts Logged Into

Find users who log into more hosts than they typically do.

Featured

Searches Included

Remote Services

Increase In Pages Printed

Find users who printed more pages than normal.

Featured

Searches Included

Exfiltration Over Physical Medium

Large Web Upload

Uses a basic threshold to detect a large web upload, which could be exfiltration from malware or a malicious insider.

Featured

Searches Included

Exfiltration Over C2 Channel

Exfiltration Over Alternative Protocol

Multiple Account Deletion by an Administrator

Detect multiple accounts being deleted by an Administrator

Featured

Searches Included

Account Manipulation

Valid Accounts

Multiple Account Disabled by an Administrator

Detect multiple accounts being disabled by an Administrator

Featured

Searches Included

Account Manipulation

Valid Accounts

Multiple Account Passwords changed by an Admin...

Detect multiple account password changes done by an Administrator

Featured

Searches Included

Account Manipulation

Valid Accounts

Multiple Infections on Host

Finds hosts that have logged multiple different infections in a short period of time.

Featured

Searches Included

User Execution

Spearphishing Link

Phishing

Greenhouse Attack

Security Content / Basic Malware Outbreak

Assistant: Simple Search

Export

Description

Looks for the same malware occurring on multiple systems in a short period of time.

Learn how to use this page

Content Mapping

This content is not mapped to any local saved search. Add mapping

Clone This Content Into Custom Content

Use Case

Security Monitoring

Category

Endpoint Compromise

Security Impact

When the same malware occurs on multiple systems, you may be on the brink of a major incident as has been seen frequently with worms, ransomware, and broad phishing campaigns. Find out about these before they become a big deal!

Alert Volume

Low

SPL Difficulty

Basic

Bookmark Status

Not Bookmarked

None

Data Availability

Unavailable

Journey

Stage 1

MITRE ATT&CK Tactics (Click for Detail)

Initial Access

Execution

Privilege Escalation

MITRE ATT&CK Techniques (Click for Detail)

Drive-by Compromise

Phishing

User Execution

Exploitation for Privilege Escalation

Spearphishing Link

Spearphishing Attachment

MITRE Threat Groups (Click for Detail)

Leviathan

Andarjel

PROMETHIUM

APT33

RTM

Cobalt Group

Threat Group-3390

Windigo

Leafminer

Turla

APT38

Whitefly

Lazarus Group

Dragonfly

FIN6

APT19

APT37

Patchwork

BRONZE BUTLER

APT28

Tonto Team

FINB

APT32

Machete

Dragonfly 2.0

Dark Caracal

ZIRCONIUM

Windshift

Elderwood

Transparent Tribe

PLATINUM

GOLD SOUTHFIELD

Darkhotel

Kill Chain Phases

Delivery

Data Sources

Anti-Virus or Anti-Malware

View SPL

index=* sourcetype=symantec:* earliest=-24h

// First we bring in our basic dataset, Symantec Endpoint Protection Risks, over the last 24 hours.

| transaction maxpause=1d Risk_Name

// While there are several approaches to grouping events, and stats is the fastest, we're using transaction because it's the easiest. This will let us group all the events based on the Risk_Name.

| where mvcount(Computer_Name)>3

// Finally, we can look to see if there are more than three different computers that have been affected.

Related Splunk Capabilities

Similar Use Cases

Sometimes Splunk will solve the same problem in multiple ways, based on greater requirements. What we can do with a simple example for one data source at Stage 1 of the Journey, we can do across all datasets at Stage 2, and with more impact at Stage 4. Here are other versions of the same underlying technique.

High Number Of Infected Hosts

Stage 2 ID

Security Monitoring

Endpoint Compromise

Alerts when a high total number of infected hosts is discovered.

Featured

Try Splunk ES

AV Detection

Host With A Recurring Malware Infection

Stage 2 ID

Security Monitoring

Endpoint Compromise

Alerts when a host has an infection that has been re-infected remove multiple times over multiple days.

Featured

Try Splunk ES

AV Detection

Host With Multiple Infections

Stage 2 ID

Security Monitoring

Endpoint Compromise

Alerts when a host with multiple infections is discovered.

Featured

Try Splunk ES

AV Detection

Initial Access

Execution

Related Use Cases

First Time USB Usage

Stage 1 ID

Insider Threat

Data Exfiltration

Find systems the first time they generate Windows Event ID 20001, which for some customers occurs when a USB drive is plugged in.

Searches Included

DLP Violations

Removable Storage File Audit

Outbreak Detected

Stage 2 ID

Security Monitoring

Lateral Movement, Endpoint Compromise

Alerts when a potential outbreak is observed based on newly infected systems all exhibiting the same infection

Featured

Try Splunk ES

8

Logs Analyzed

1

Windows Logs

The pertinent data that we analyzed from the Windows logs were the signatures and signature ID's of the activities being performed and whether or not they were successful as well as the severity level and user activity.

2

Apache Logs

The Apache logs contained information about the type of HTTP activity being performed against the web-app. Specifically, the type of HTTP method being used, the referrer domain, the URI path activity and client IP location.

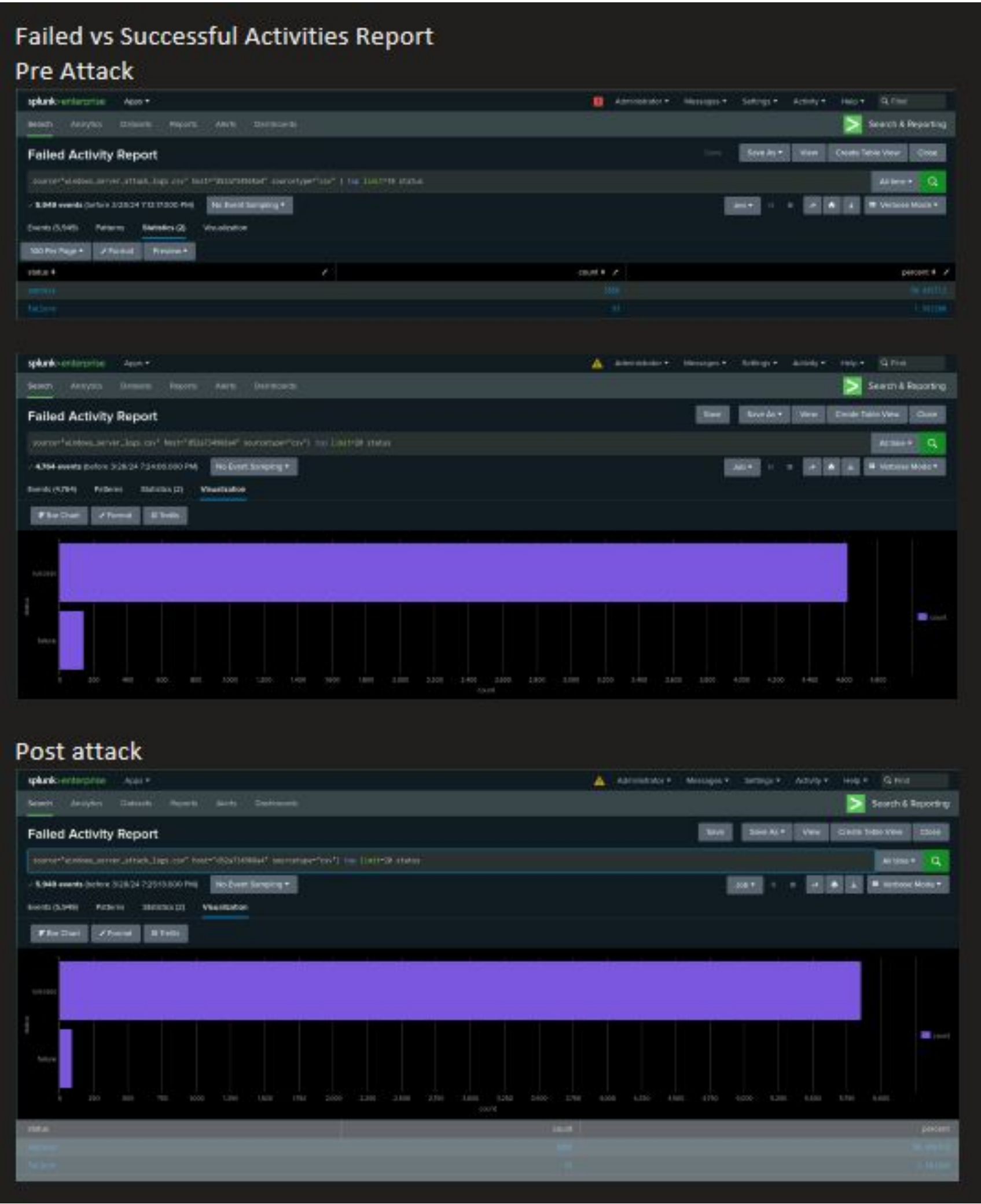
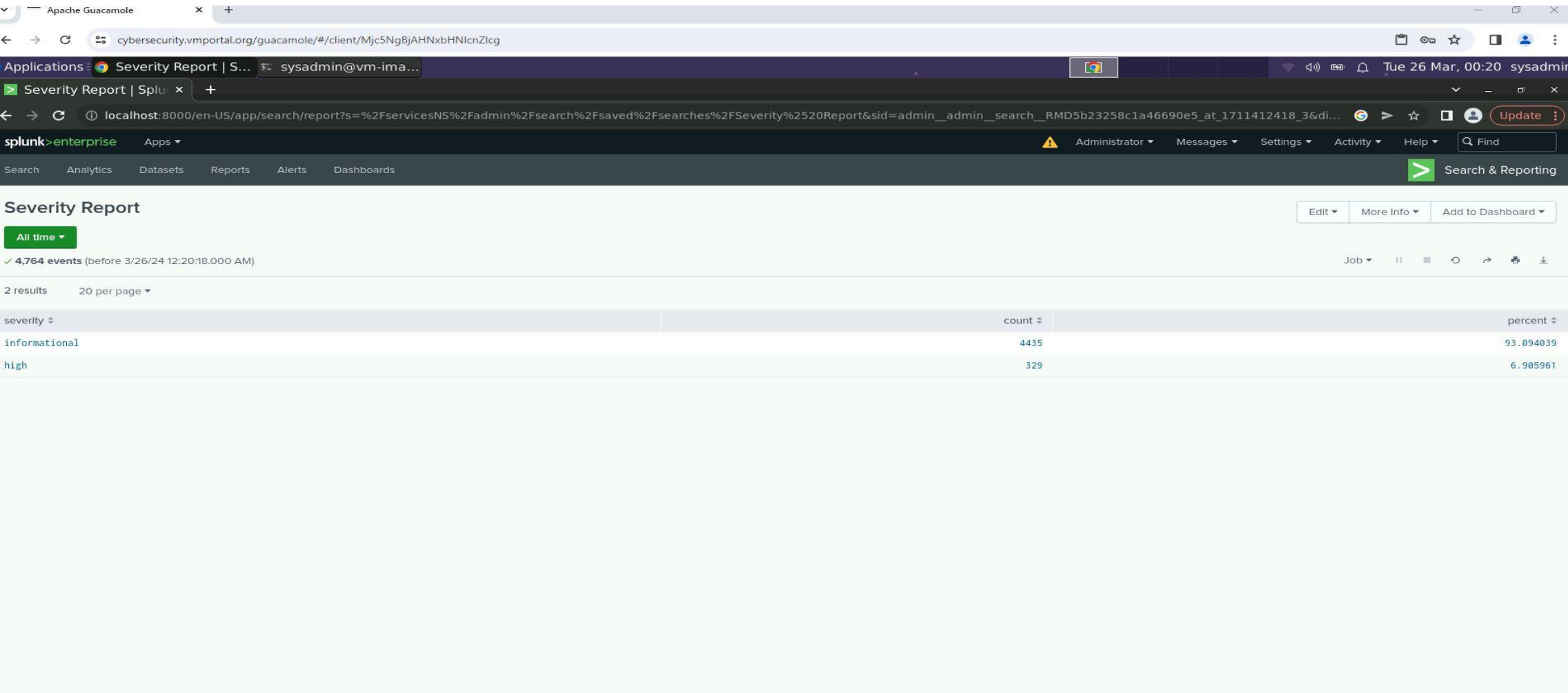
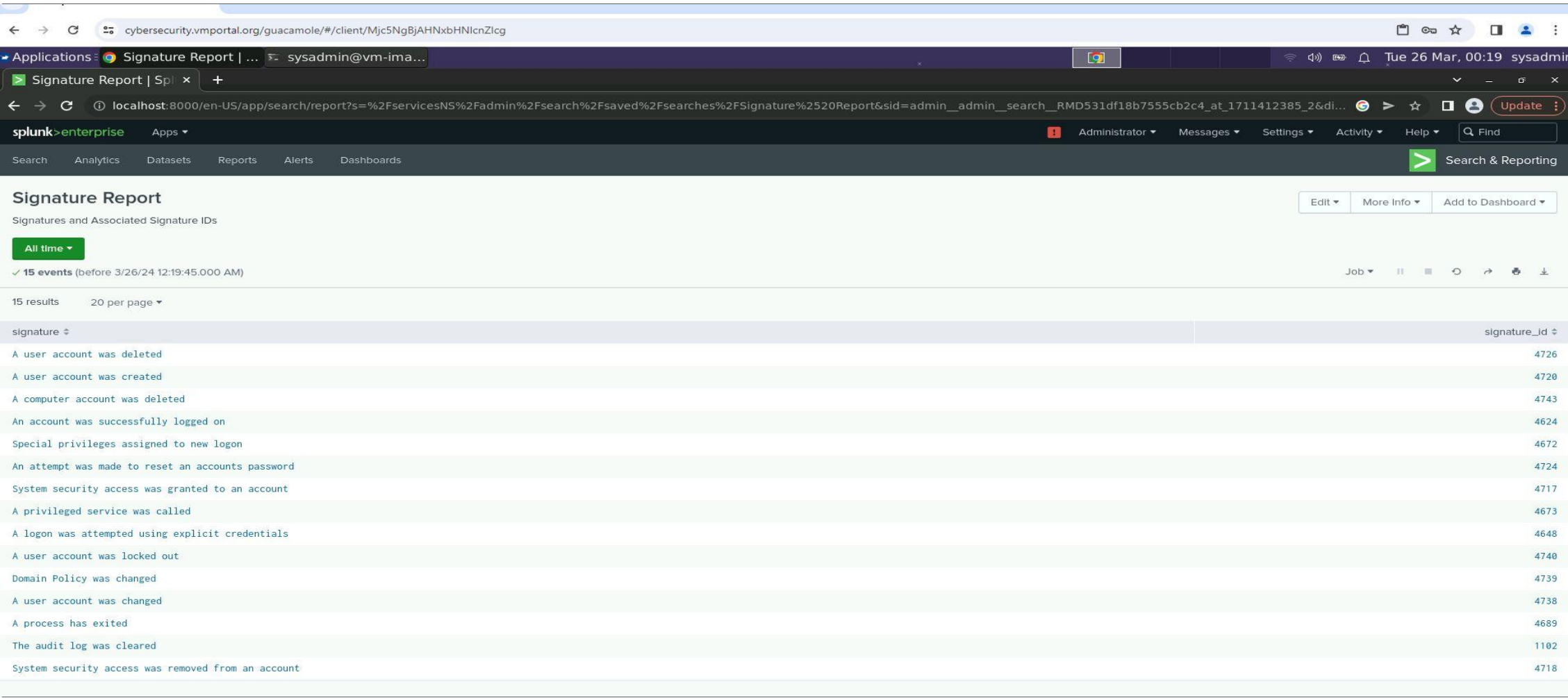
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signatures Report	A count of how many times a specific signature was logged.
Severity Report	A log of how relevant incidents are to the security of the system.
Comparison Report	A report that compares the amount of successful versus unsuccessful events.

Images of Reports—Windows



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Activity Alert	An alert that triggers and sends an email to SOC email when threshold is breached.	Anywhere from 8-10	15 failed events

JUSTIFICATION: The baseline activity across all hours of the day capped at around 8-10. We felt that a good policy was 1.5x this number to set as a threshold just to account for heavy traffic days. The threshold is just high enough that an accident or two will not trigger the alert.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Login Alert	Once the threshold of successful logins is surpassed, it sends an email to SOC.	10-15	25

JUSTIFICATION: Like our other alerts, we set the alert threshold to approximately one and a half time the maximum range of the baseline. That way anomalies in logins will not trigger the alert.

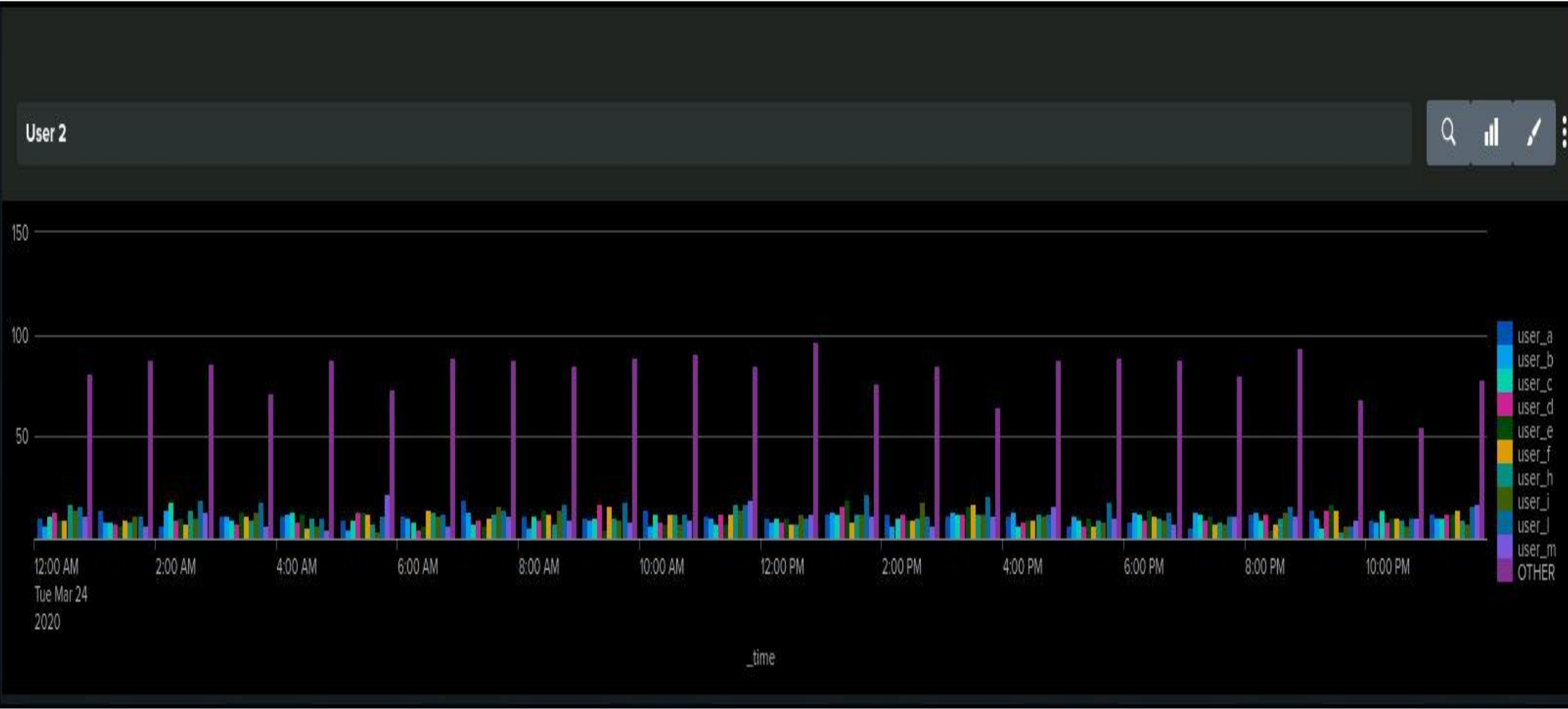
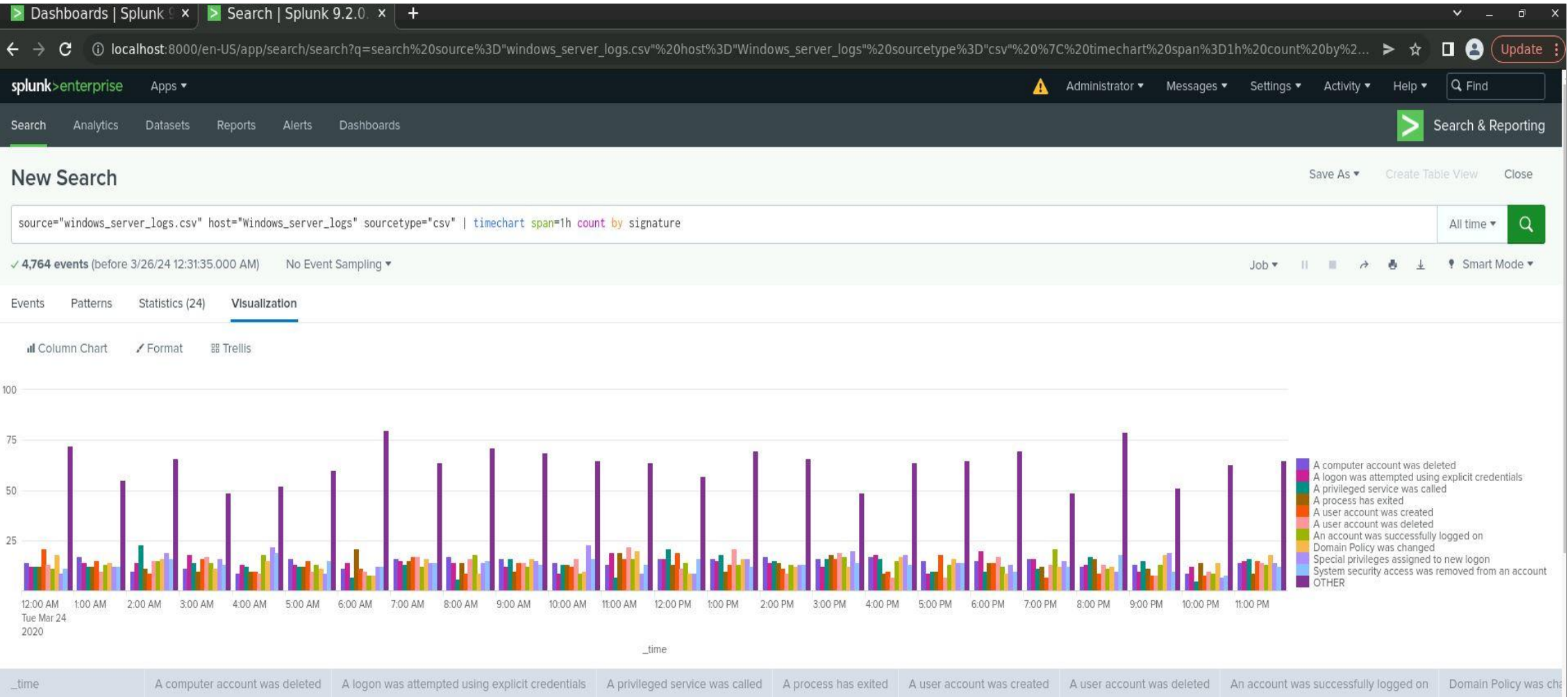
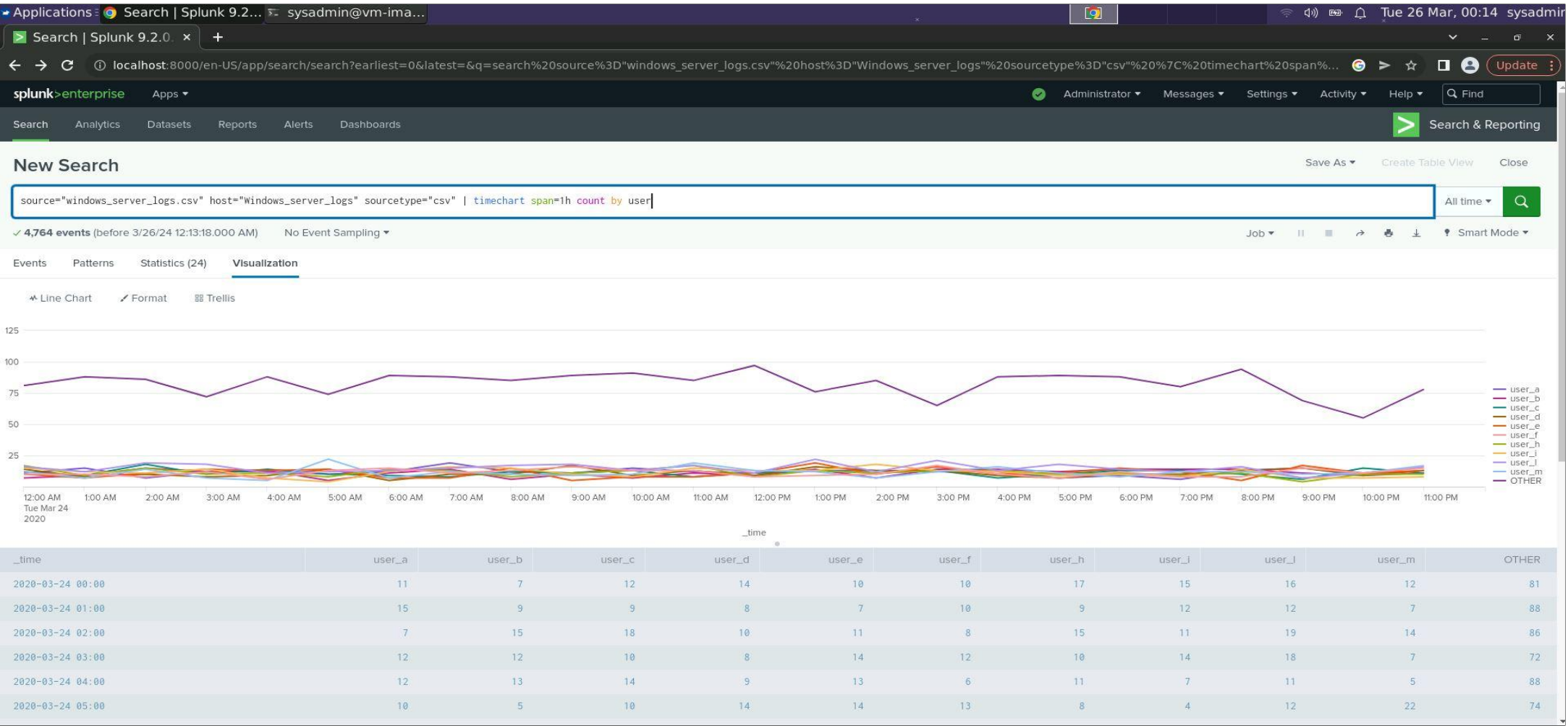
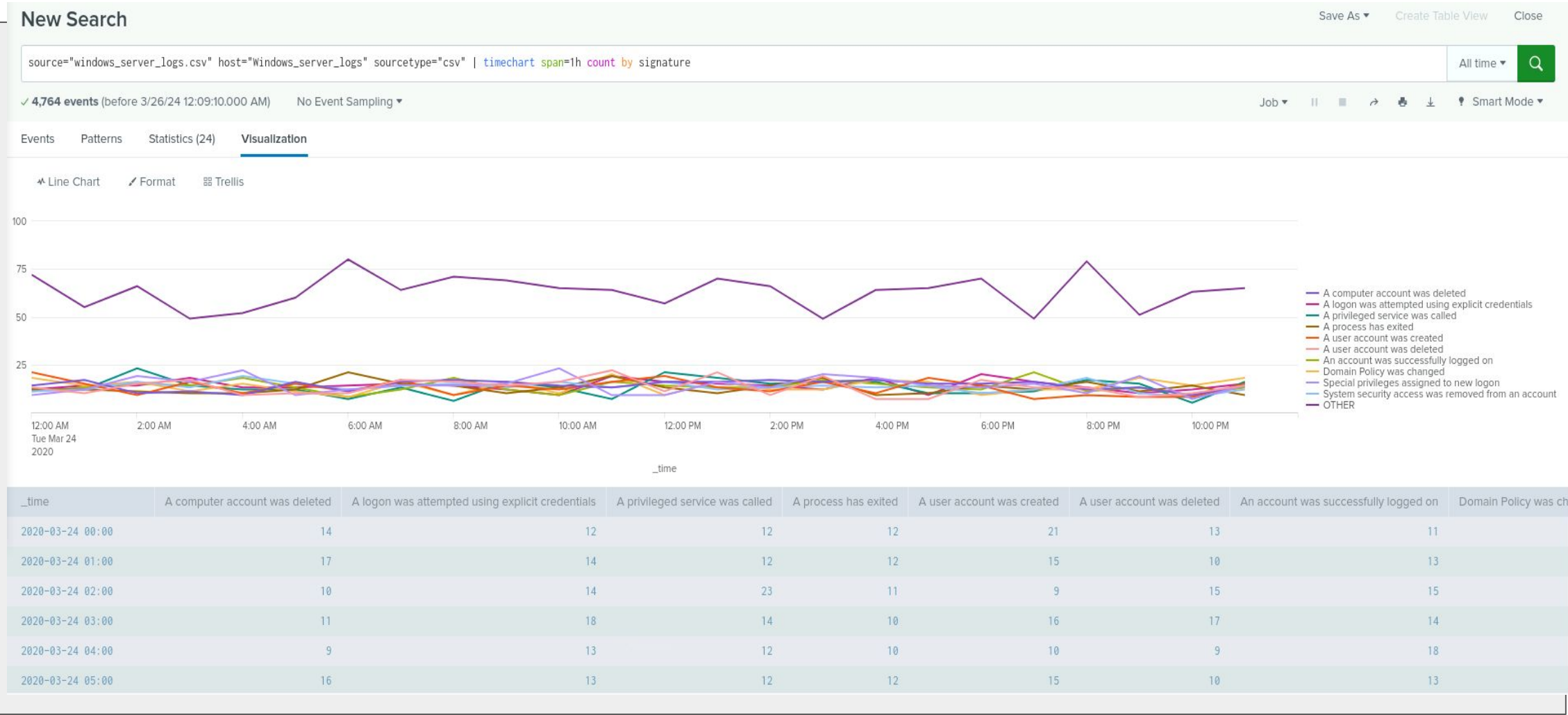
Alerts—Windows

Designed the following alerts:

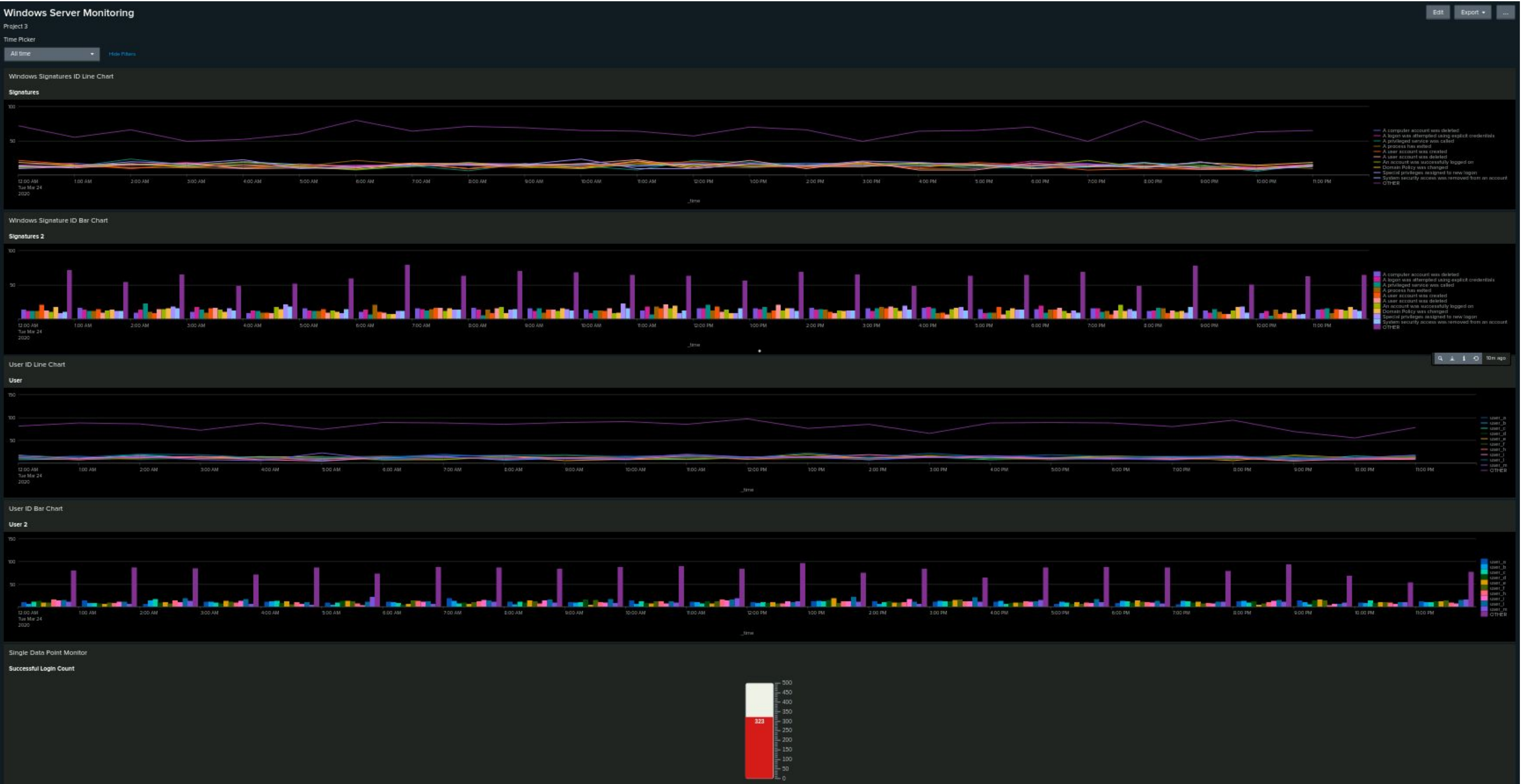
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account Deletion Alert	An alert that when the threshold of account deletions is triggered sends an email to SOC.	10-15/hr	25/hr

JUSTIFICATION: Our baseline was the average of the activity that was saw during the day, and we set our threshold to one and a half times that just to make sure there is wiggle room for days where there is an above average amount of legitimate events.

Dashboards—Windows



Dashboards—Windows



Apache Logs

Reports—Apache

HTTP Method Report

Report Description: This monitors the GET, POST, HEAD, and OPTIONS requests made to the server, this offers insight into the variety of actions performed by clients interacting with the server.

MethodTable

All time

✓ 20,000 events (before 3/26/24 12:57:13.000 AM)

Edit

More Info

Add to Dashboard

Job

||

4 results

20 per page

method	count	percent
GET	19702	98.510000
POST	212	1.060000
HEAD	84	0.420000
OPTIONS	2	0.010000

Reports—Apache

Top 10 Referrer Domain Report

Report Description: Monitors and helps us understand where the traffic to the VSI website is coming from.

source="apache_logs.txt" host="3e72404c940f" sourcetype="access_combined" | top limit=10 referer_domain

All time

✓ 70,000 events (before 3/27/24 11:09:45.000 PM) No Event Sampling ▾

Job ▾ || ▢ ↶ ↷ ⬇ ⬆ ⬇ ⬆ Smart Mode ▾

Events Patterns **Statistics (10)** Visualization

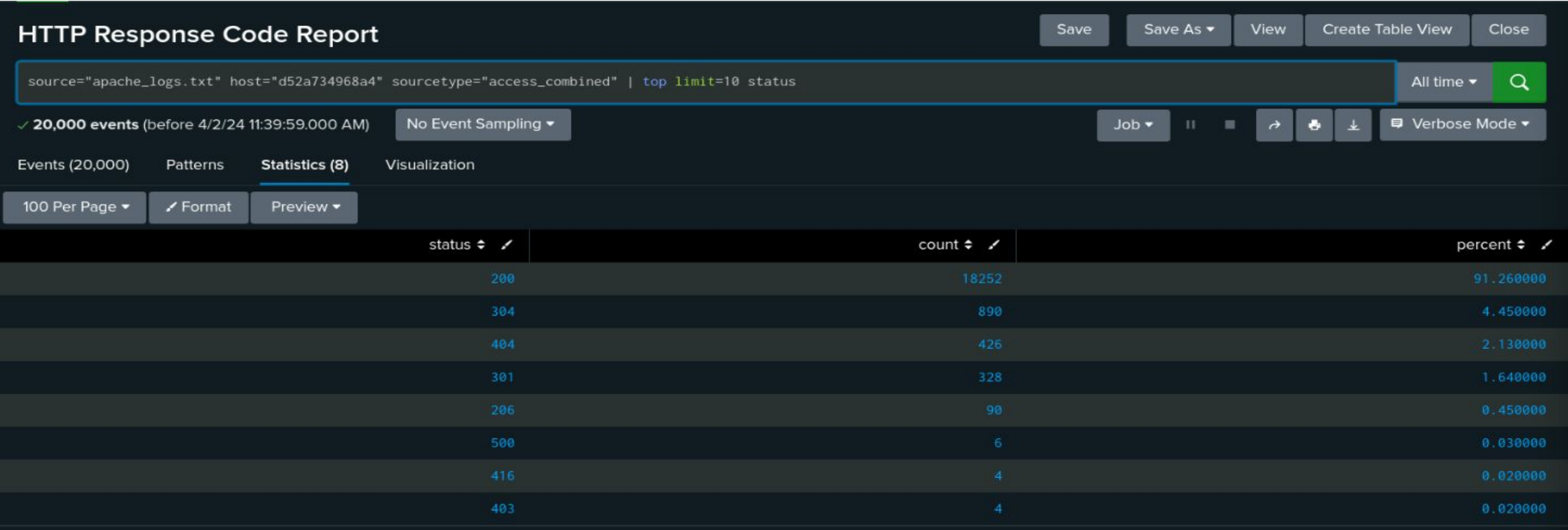
20 Per Page ▾ ↗ Format Preview ▾

referer_domain ⚙	count ⚙	percent ⚙
http://www.semicomplete.com	21266	51.256960
http://semicomplete.com	14007	33.760756
http://www.google.com	861	2.075249
https://www.google.com	735	1.771554
http://stackoverflow.com	238	0.573646
http://www.google.fr	217	0.523030
http://s-chassis.co.nz	203	0.489286
http://logstash.net	196	0.472414
http://www.google.es	175	0.421799
https://www.google.co.uk	161	0.388055

Reports—Apache

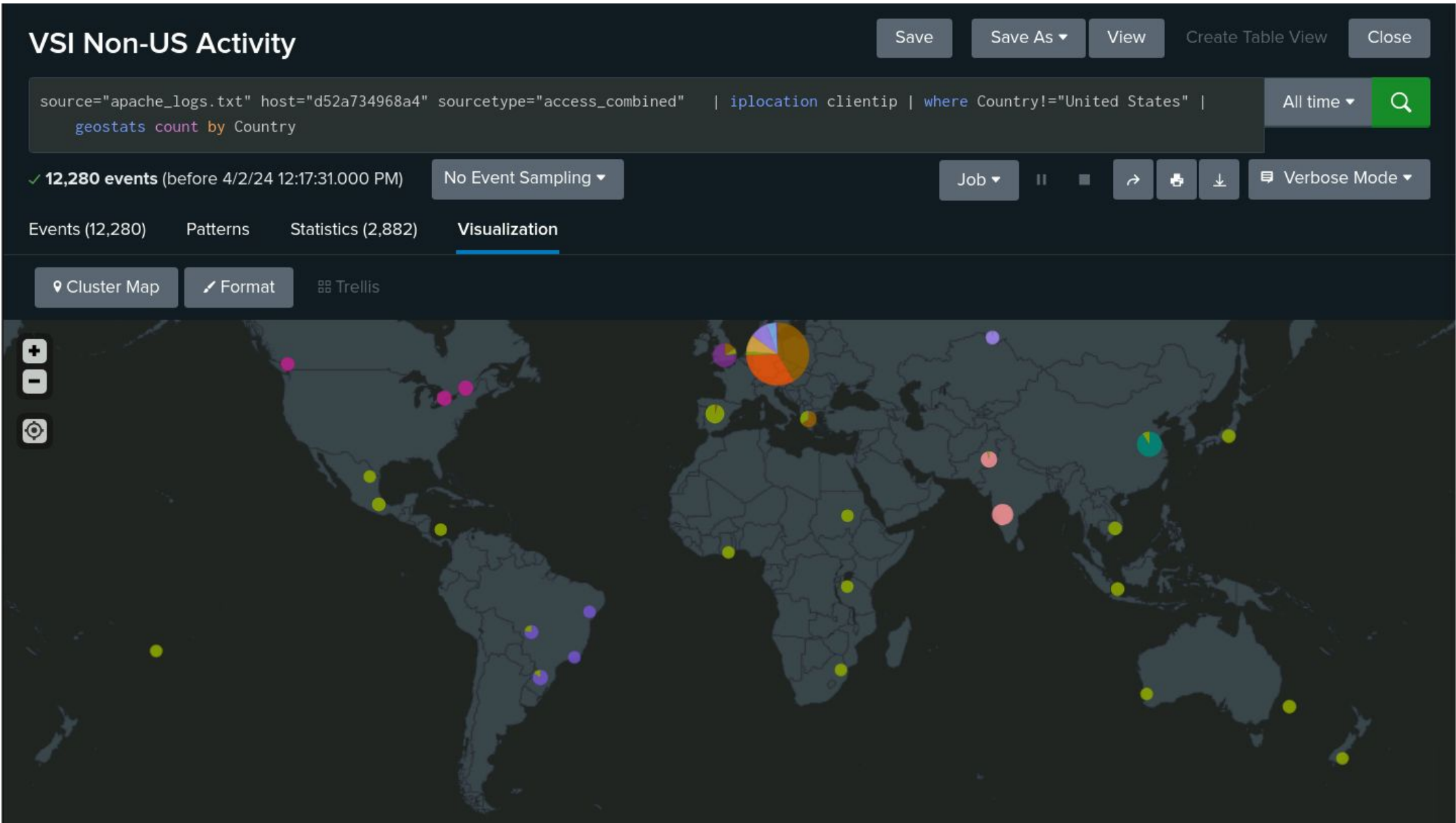
HTTP Response Code Report

Report Description: Monitors response codes and helps track the performance of the VSI web server. Low rates of 200 status codes and high rates of error responses may indicate server-side issues affecting user experience.



Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Non-US Activity	Detects an influx of IP addresses coming from countries outside the US.	146/hr	230



VSI Non-US Activity

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Mar 27, 2024 12:40:35 AM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 230. [Edit](#)

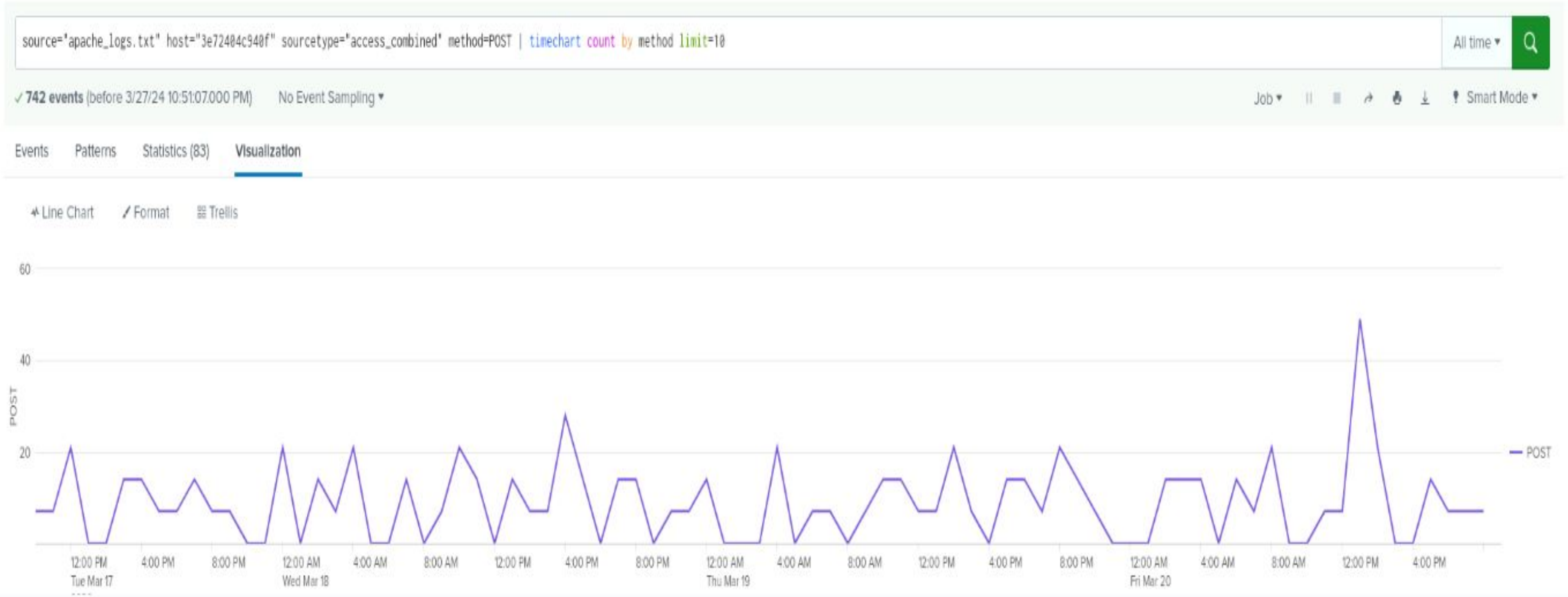
Actions: [1 Action](#) [Edit](#)

[Send email](#)

JUSTIFICATION: The baseline was set determined to be 146 events/hr with a high of 240. Threshold was set to 230 to limit false positives but also considers normal highs.

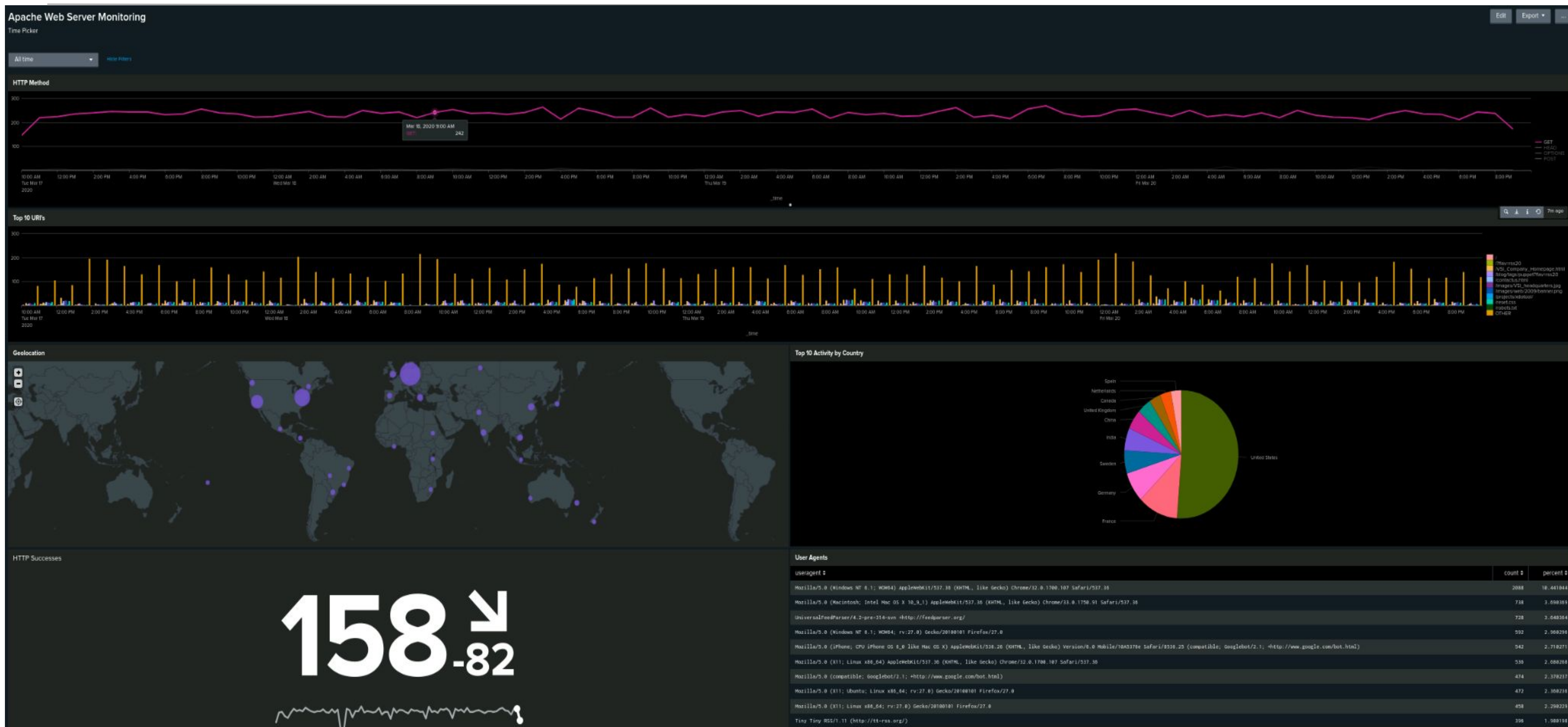
Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI HTTP POST ALERT	Detects an influx of incoming HTTP POST requests	~3/hr with a max of 14	12/hr



Justification:
We established a baseline of roughly 3 POST activities/hour with a max of 14. The threshold was set to 12/hr to consider that although 14 POSTs/hr could be normal, it generally isn't. Our alert may give some false positives, but this is necessary in order to not miss an actual attack.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

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

- When comparing severity reports from the attack logs and normal logs, the severity events in the attack logs saw a sharp increase. The high severity events nearly tripled in the attack logs.
- When comparing Failed Activity events from attack logs to normal logs, the failed activities saw an increase as well. Not as sharp an increase as the severity logs, but enough to cause concern.

Attack Summary—Windows

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

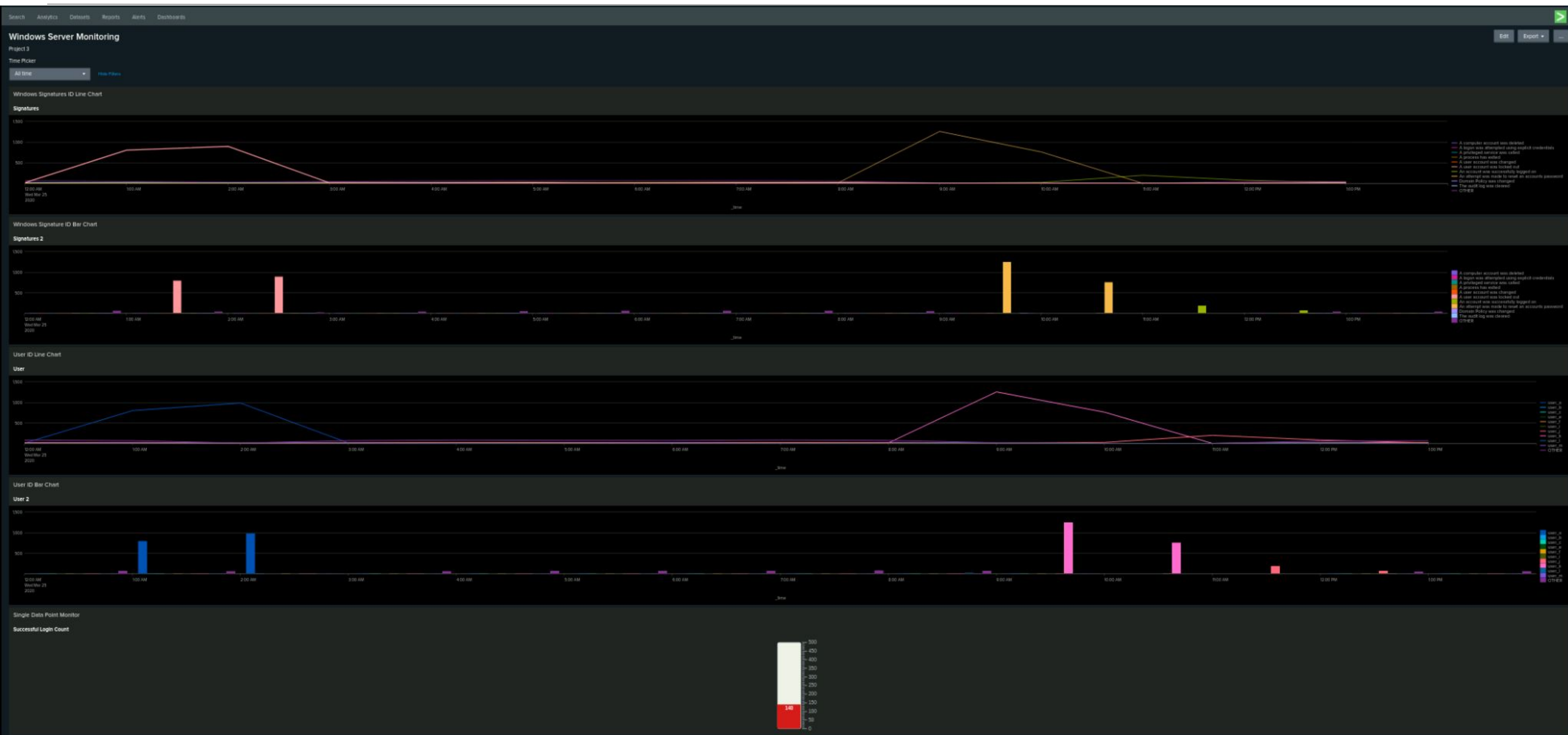
- Suspicious activity would have been caught by almost all of our alerts. The thresholds were exceeded in every case except for successful logins.
- For Failed Windows Activity, the baseline was 9, the threshold was 15, highest we saw was 35.
- For Successful Logins, the baseline was 12, the threshold was 25, peak was 21. However, our alert should have had a minimum set. The suspicious activity is when logins fall to 0. Which occurred between 10:00 a.m. and 11:00 a.m.
- For Deleted Accounts, the volume is one part of the suspicion, the time was a factor as well. As they all happened outside of working hours.

Attack Summary—Windows

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

- The Signature Timechart showed lockout activity between 12:00 a.m. - 3:00 a.m., and attempted password resets between 8:00 a.m. and 11:00 a.m. The latter may be legitimate uses, but they are all from one user, so likely not. Thus, they are suspicious.
- During the above times, the two signatures are exclusively done by two users. user_a for the former, and user_k for the latter.
- The signature timechart and the user timecharts both match up in terms of the time and number of events.
- There is a third suspicious user, user_j, who has a relatively large number of successful logins after the activities of both user_a and user_k.

Attack Dashboard - Windows



Screenshots of Attack Log Reports and Summary

source="apache_attack_logs.txt" host="3e72404c940f" sourcetype="access_combined" | top limit=20 method

All time

Q

✓ 8,994 events (before 3/28/24 7:14:19.000 PM) No Event Sampling ▾

Job ▾ || ■ ↗ 🖨 ⬇ ⚙ Smart Mode ▾

Events Patterns **Statistics (4)** Visualization

20 Per Page ▾ ✎ Format Preview ▾

method ▾ ✎	count ▾ ✎	percent ▾ ✎
GET	6314	70.202357
POST	2648	29.441850
HEAD	30	0.333556
OPTIONS	2	0.022237

source="apache_attack_logs.txt" host="3e72404c940f" sourcetype="access_combined" | top limit=20 referer_domain

All time

Q

✓ 8,994 events (before 3/28/24 7:15:51.000 PM) No Event Sampling ▾

Job ▾ || ■ ↗ 🖨 ⬇ ⚙ Smart Mode ▾

Events Patterns **Statistics (20)** Visualization

20 Per Page ▾ ✎ Format Preview ▾

referer_domain ▾ ✎	count ▾ ✎	percent ▾ ✎
http://www.semicomplete.com	1528	49.226804
http://semicomplete.com	1144	36.855670
http://www.google.com	74	2.384021
https://www.google.com	50	1.610825
http://stackoverflow.com	30	0.966495

source="apache_attack_logs.txt" host="3e72404c940f" sourcetype="access_combined" | top limit=20 status

All time

Q

✓ 8,994 events (before 3/28/24 7:19:12.000 PM) No Event Sampling ▾

Job ▾ || ■ ↗ 🖨 ⬇ ⚙ Smart Mode ▾

Events Patterns **Statistics (7)** Visualization

20 Per Page ▾ ✎ Format Preview ▾

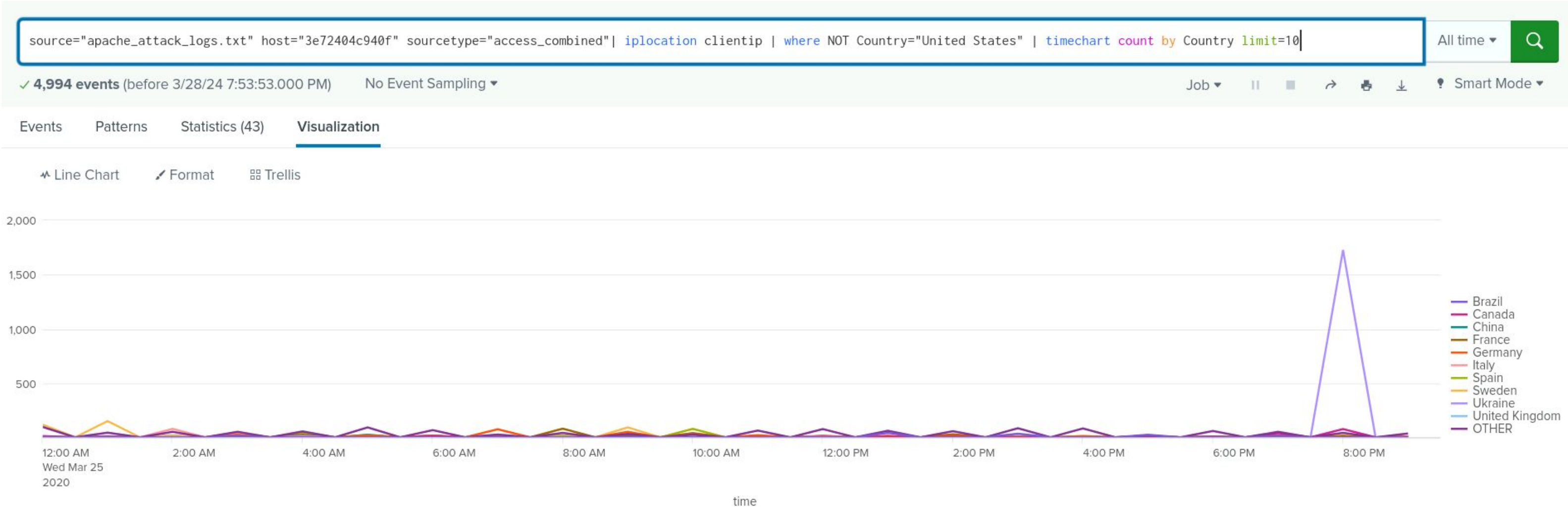
status ▾ ✎	count ▾ ✎	percent ▾ ✎
200	7492	83.299978
404	1358	15.098955
304	72	0.800534
301	58	0.644874
206	10	0.111185
500	2	0.022237
403	2	0.022237

When it comes to the Method requests report we see a decrease in GET Requests and an increase in POST requests.

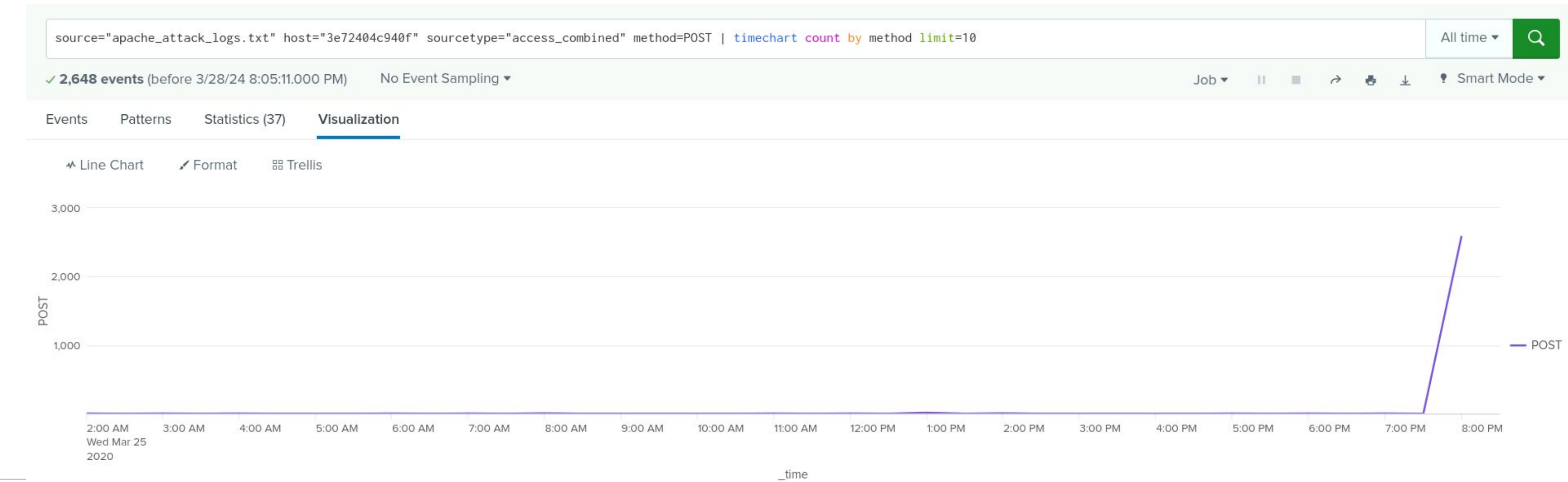
We also see an overall decrease of Referrer domains meaning less traffic is coming from these sites.

Finally we see the same trend of a severe decrease of 200 HTTP response codes and an increase in 404's.

Attack Summary—Apache Alerts



From this line chart we see that there is barely any activity coming from other countries besides Ukraine with 1296 events at 8:00pm. This would trigger our alert because our threshold was set at 230 events for activity outside the US.



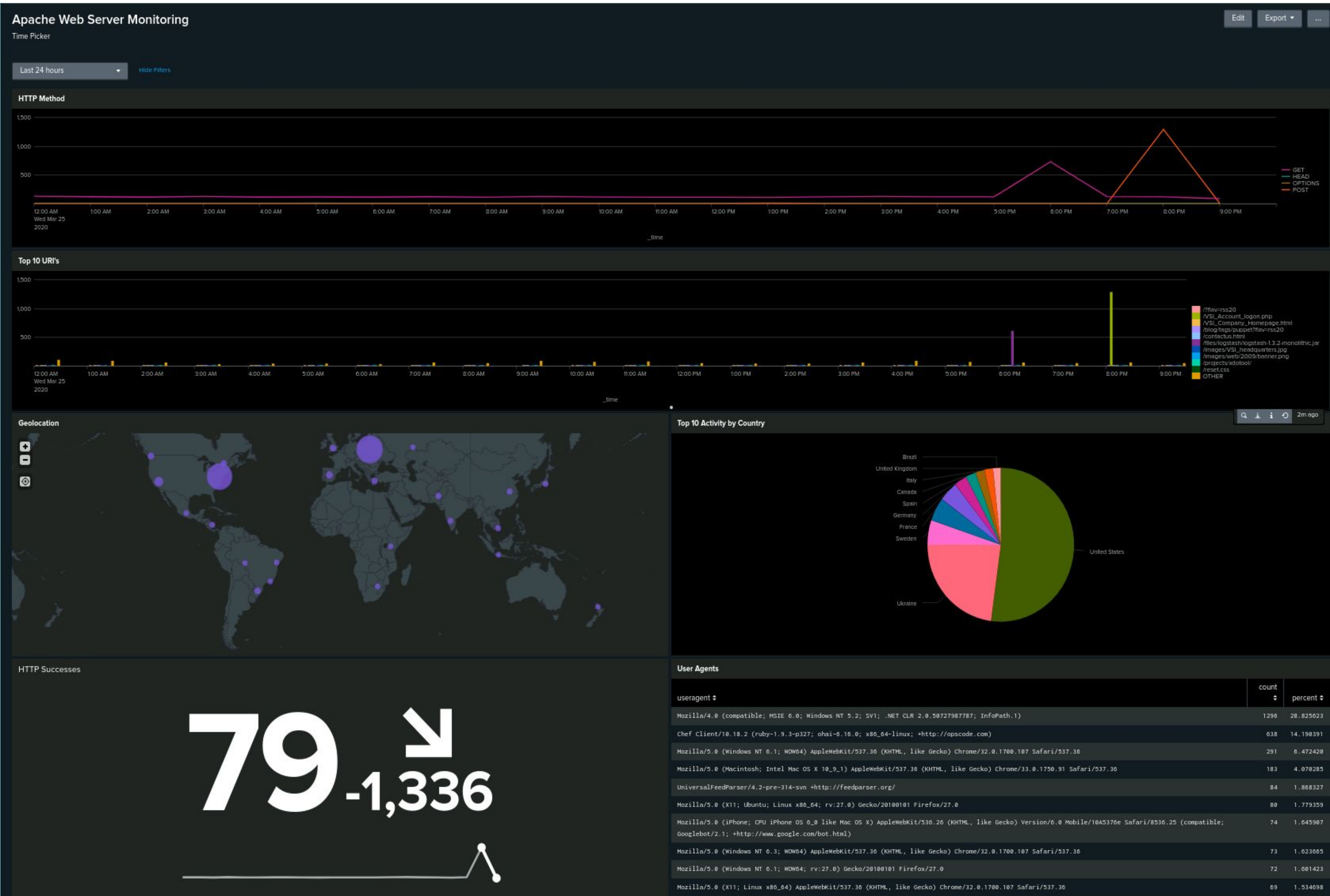
From the information gathered from the method POST requests, we can see that At 8:00pm there were 1296 POST requests that correlate Ukraine's activity. Our alert would trigger because our threshold was set at 12 events/hr.

Attack Summary Dashboard—Apache

Using our dashboard, alerts and reports to evaluate the attack, we were able to determine the following:

Between 5:00 p.m. and 7:00 p.m. we saw a spike in GET requests directed at the files/logstash/logstash-1.3.2-monolithic.jar URI and then from 7:00 p.m. to 9:00 p.m. we saw a spike in POST requests targeting the /VSI_Account_logon.php URI. All coming from the area around Kiev, Ukraine. The attacker was using Mozilla/4.0 on a Windows machine.

The data suggests that the attacker may have exfiltrated data from the logstash and then attempted a Brute Force/DDoS attack on the logon.php URI as we can see which HTTP requests were targeting which URI. We also noted that the rate of 200 HTTP response codes fell during this time, which points to denial of service.



Summary and Future Mitigations

Project 3 Summary

Windows Attack Summary:

1. **Severity Increase:** A sudden large increase in severity events from 329 to 1111 could indicate a significant uptick in security-related incidents, suggesting that the system is experiencing a higher volume of potentially malicious activities.
2. **Account Lockouts:** The occurrence of account lockouts (1701) suggests repeated failed login attempts, possibly indicating an attacker trying to gain unauthorized access to user accounts using various credentials.
3. **Passwords Reset:** A high number of password resets (1258) could indicate attempts by either legitimate users to reset their passwords due to compromise or by attackers attempting to gain control of user accounts.
4. **Zero Successful Logins:** The sudden drop to zero successful logins between 10:00 a.m. and 11:00 a.m. is highly suspicious and could indicate a successful breach or a deliberate disruption of legitimate access, possibly to cover malicious activities.
5. **Increase in Failed Activities:** The overall increase in failed activities, along with account lockouts and password resets, suggests ongoing efforts by attackers to gain unauthorized access to the system or escalate privileges.
6. **Deleted Accounts at Strange Hours:** The deletion of accounts at unusual times could indicate attempts by attackers to cover their tracks or disrupt the system's integrity, possibly by removing traces of compromised accounts or unauthorized access.

Project 3 Summary cont.

Apache:

1. **GET and POST Request Spike:** A sudden spike in both GET and POST requests could indicate an attempt to overwhelm the server with a high volume of traffic. This could be indicative of a Distributed Denial of Service (DDoS) attack, especially if the spike is abnormal and not due to legitimate user activity.
2. **Attacks on Logstash and Login URI:** Targeting Logstash and the login URI suggests that the attacker is specifically aiming to disrupt logging and monitoring systems (Logstash) and potentially gain unauthorized access to the server or sensitive information through the login page. This could indicate a targeted attack focused on compromising the server's security or disrupting its operation.
3. **Source of Attack: Ukraine:** Knowing the source of the attack (in this case, Ukraine) could provide additional context, but it's important to note that the source IP address can be spoofed or routed through compromised systems. Nevertheless, if the attack originates from a specific geographic location, it might suggest a coordinated effort, or the involvement of threat actors based in that region.
4. **HTTP Successes Dropped:** A decrease in HTTP successes indicates a decline in successful requests, which could mean that legitimate users are experiencing difficulties accessing the server or that the server's performance is degraded due to the attack.

Mitigation

Mitigation:

1. Reset passwords for user_a & user_k, but I would recommend doing it for all users on the system as we do not know how many credentials were compromised.
2. Implement a stronger password policy.
3. Reconfigure alerts to look for low login rates.
4. Block all traffic from Ukraine.
5. Implement load balancing to ensure continued uptime for servers.
6. Continue to monitor and update baselines and alerts