Project 3
Defensive Security
By: Leo, Michele, Akiel, Preen

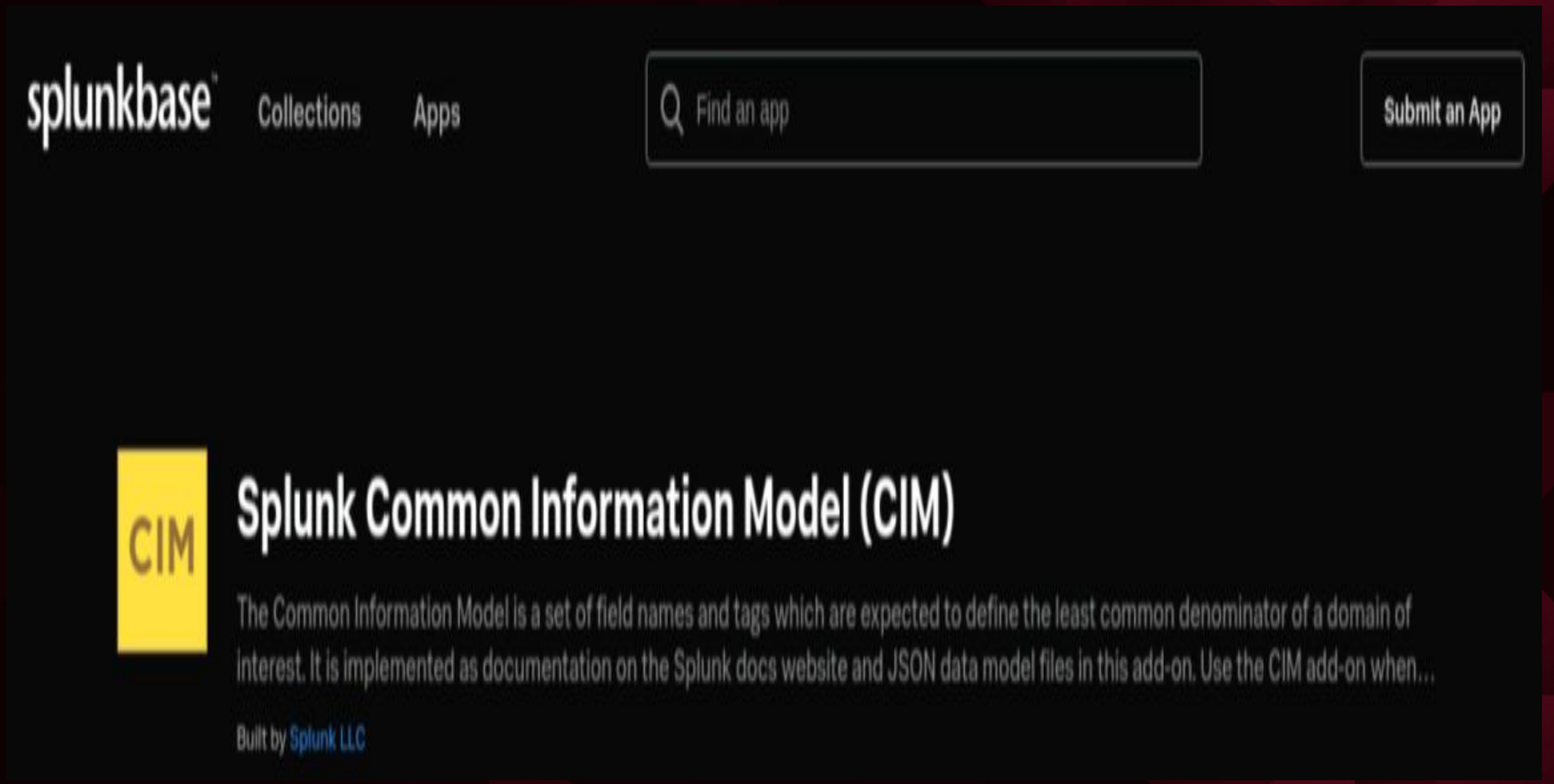
Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- We are a team of SOC analysts working for VSI (Virtual Space Industries)
- VSI hired us because of rumors that a competitor may have launches cybersecurity attacks towards VSI with the intention to disrupt business
- Using Splunk, we monitor VSI against these potential attacks by examining the following:
  - We compare VSI's Windows Server Logs to the attack logs
  - We look at the Apache web server and compare those to their attack logs


splunkbase
Collections
Apps
Find an app
Submit an App
CIM
Splunk Common Information Model (CIM)
The Common Information Model is a set of field names and tags which are expected to define the least common denominator of a domain of interest. It is implemented as documentation on the Splunk docs website and JSON data model files in this add-on. Use the CIM add-on when...
Built by Splunk LLC

Common Information Model (CIM)

Purpose

- **Normalization:** Maps raw data fields to CIM data models using field aliases, calculated fields, lookups, and tags.
- **Compatibility:** Ensures data from diverse sources can be used with Splunk apps (e.g., Splunk Enterprise Security, IT Service Intelligence).
- **Simplification:** Reduces the effort needed to search and analyze data from varied sources.

Common Information Model (CIM)

Key Components

Data Models

- Predefined data schemas for different domains, like authentication, network traffic, and malware.
- Provides a standardized format for categorizing and structuring data.

Field Aliases and Field Extractions

- Maps raw data fields to CIM-compliant field names.
- Makes querying data from different sources easier with consistent field naming.

Tags

- Applied to events to classify them for use in CIM models (e.g., authentication, malware, etc.).

Macros and Lookups

- Macros: Simplify complex queries.
- Lookups: Enhance data enrichment and correlation by adding external or calculated data.

Common Information Model (CIM)

Best Practices

Map Data to CIM Early: Use the add-on during ingestion to minimize manual effort later.

Review CIM Compliance: Regularly check data mappings and field extractions for accuracy.

Update Regularly: The CIM add-on gets frequent updates to include new data models and improve compatibility.

Validate Data Models: Use tools like the **Splunk CIM Validator** to test your data mappings.

Common Information Model (CIM)

How it Works

Install the Splunk Add-on for CIM in your Splunk environment.

Enable and configure the appropriate data models.

Map your data sources to the CIM schema using field aliases, calculated fields, and tags.

Validate the mappings to ensure compatibility with Splunk apps or dashboards.

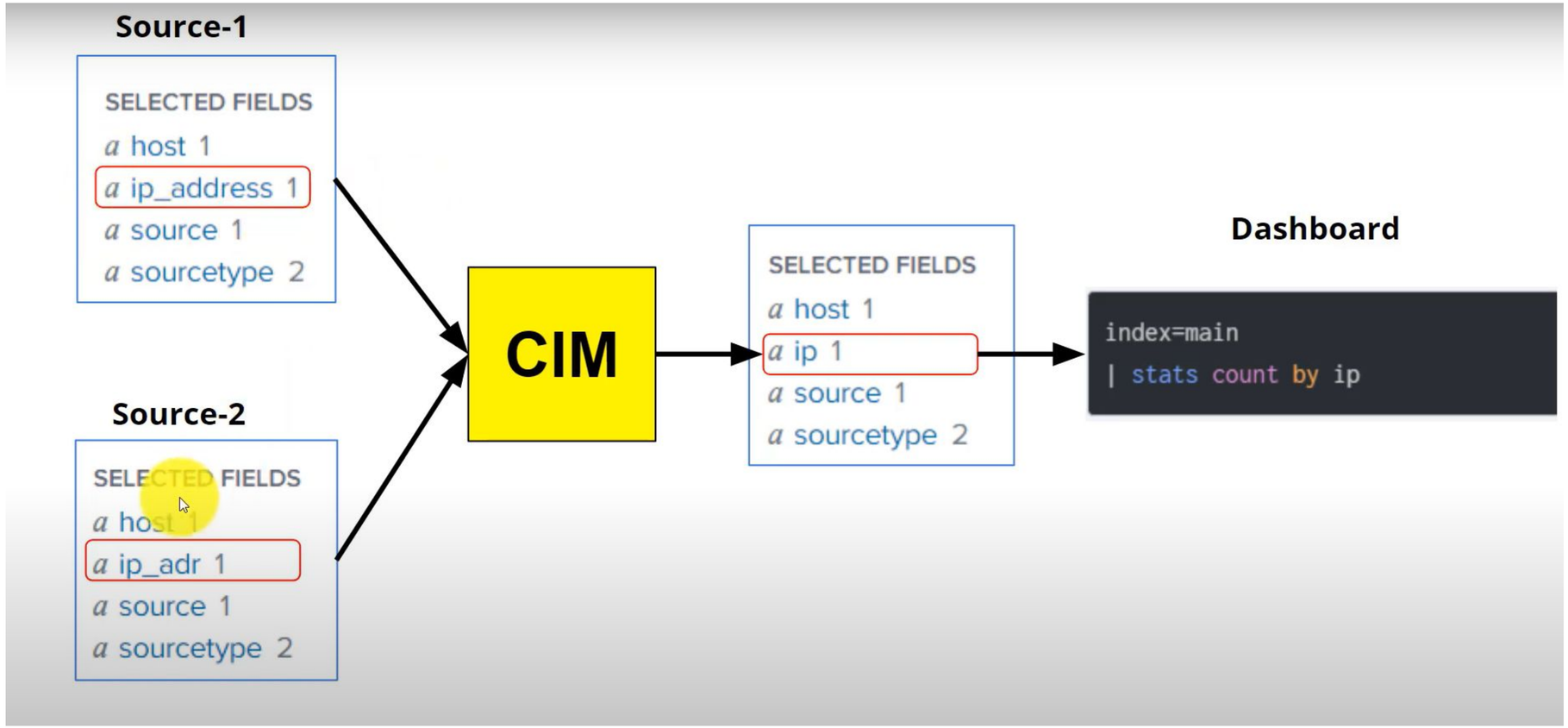
Common Information Model (CIM)

Simple Scenario: Data Normalization with CIM

Imagine a company collects log data from two different systems, **Source-1** and **Source-2**, but the fields for IP addresses are labeled differently: one uses ip_address, while the other uses ip_adr. To standardize reporting across both sources, they use the **Common Information Model (CIM)**. CIM normalizes these fields into a common field called ip.

Once normalized, analysts can write a single query, such as stats count by ip, to generate a unified dashboard showing the frequency of IPs across both sources, regardless of their original field names. This ensures consistent and centralized data analysis.

Common Information Model (CIM)



Logs Analyzed

1

Windows Logs

This server contains intellectual property of VSI's next-generation virtual-reality programs

2

Apache Logs

Logs for VSI's main website, vsi-company.com

Windows Logs

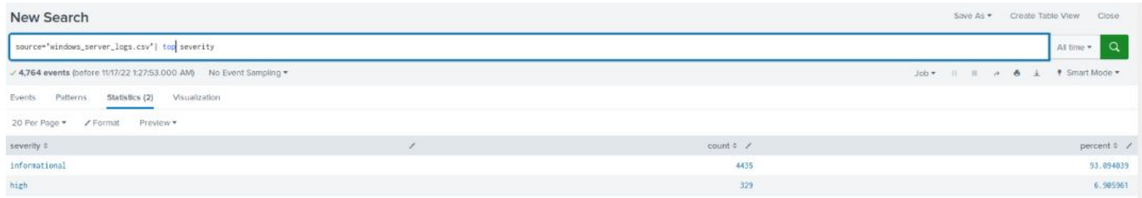
Reports—Windows

Designed the following reports:

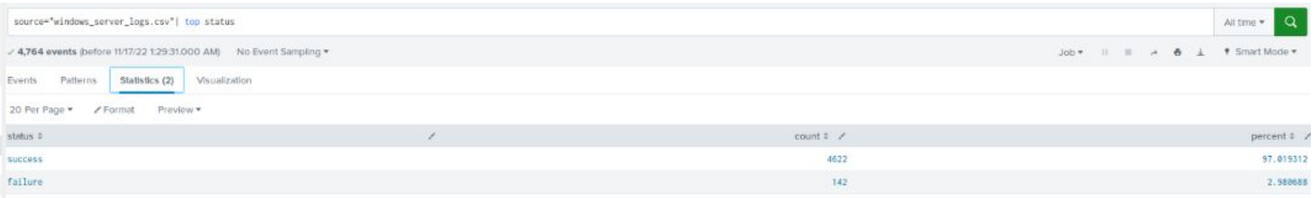
Report Name	Report Description
ID Number Associated with Specific Signature	A report that shows the ID number associated with the specific signature for Windows activity.
Windows Logs Severity	A report to quickly understand the severity levels of the Windows logs being viewed.
Success and Failure - Windows	A report that will show if there is a suspicious level of failed activities on their server.

Images of Reports—Windows

Windows Log Severity



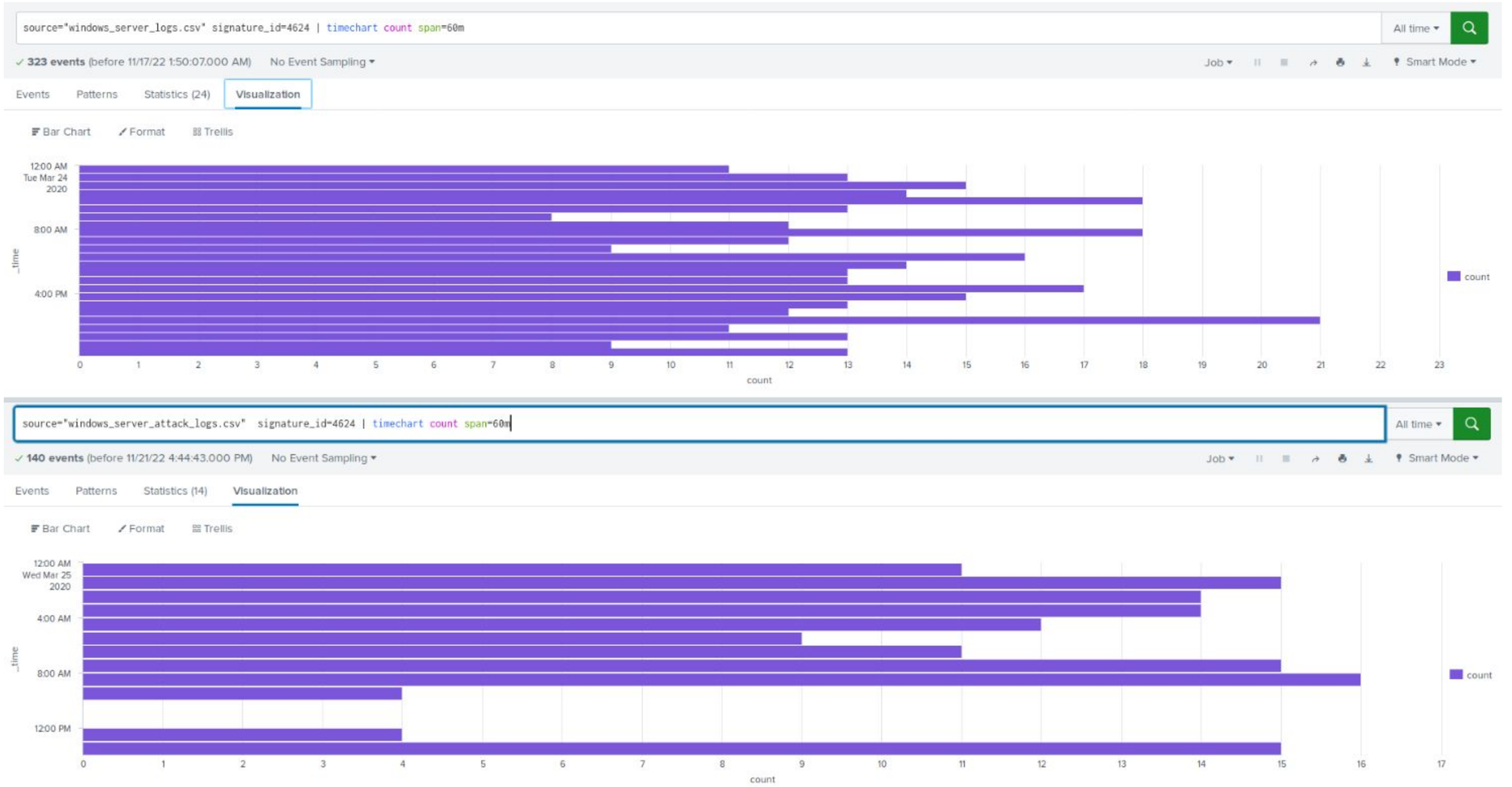
Success and Failure - Windows



ID Number Associated with Specific Signature

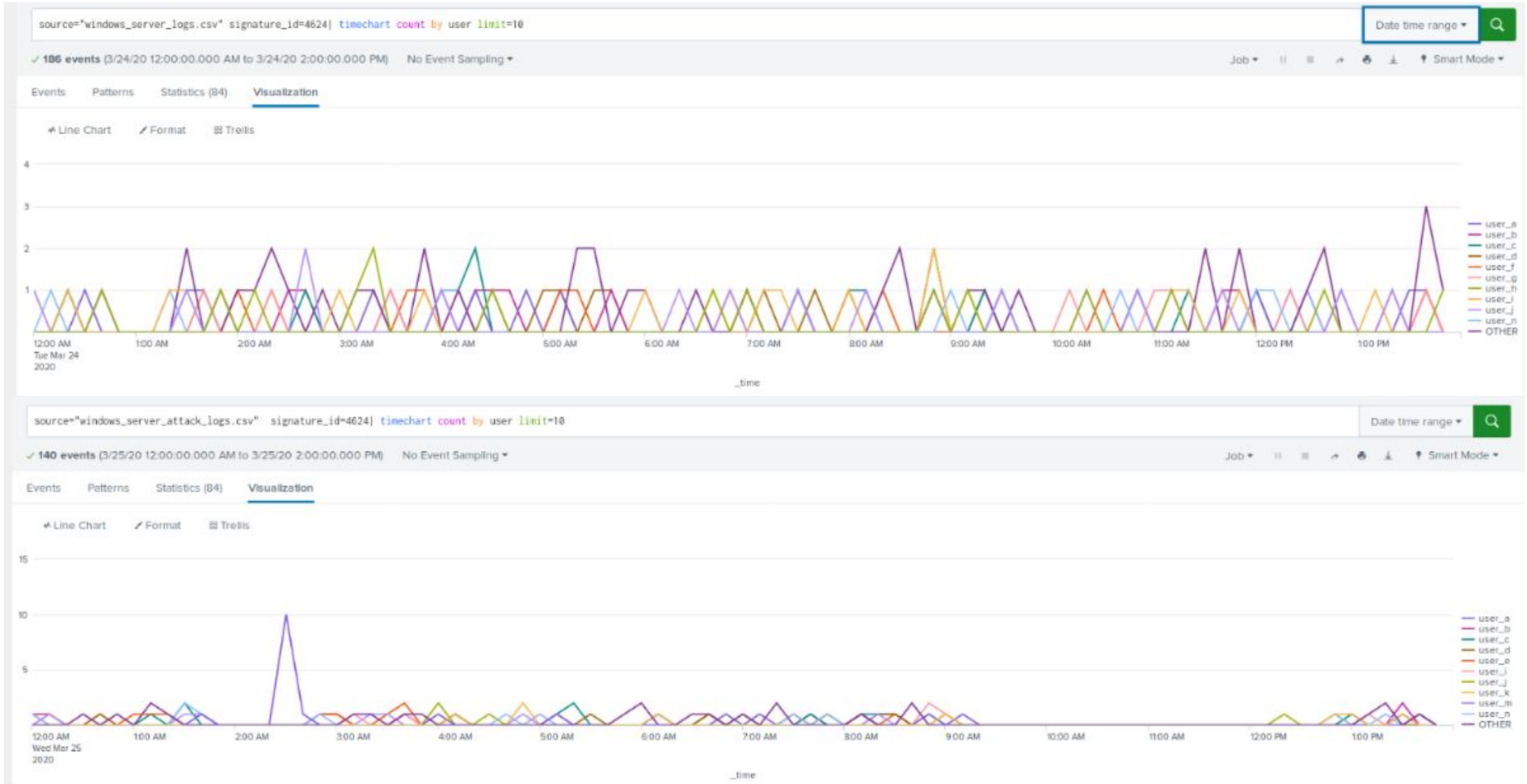
Images of Reports—Windows

Windows Successful Logins



Images of Reports—Windows

Windows Successful Logins by User



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Suspicious Activity VSI	Threshold of failed Windows Activity reached	[6]	[12]

JUSTIFICATION: The average amount of failed Windows activity averaged around 6 to establish our baseline yet never got close to 12. Failures exceeding 12 would certainly indicate suspicious activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins VSI	Threshold of Successful Logged on by Account	[12]	[30]

JUSTIFICATION: The average amount of failed Windows activity averaged around 12 to establish our baseline yet never got close to 30. Failures exceeding 30 would certainly indicate suspicious activity. Lowering it further could cause alert fatigue.

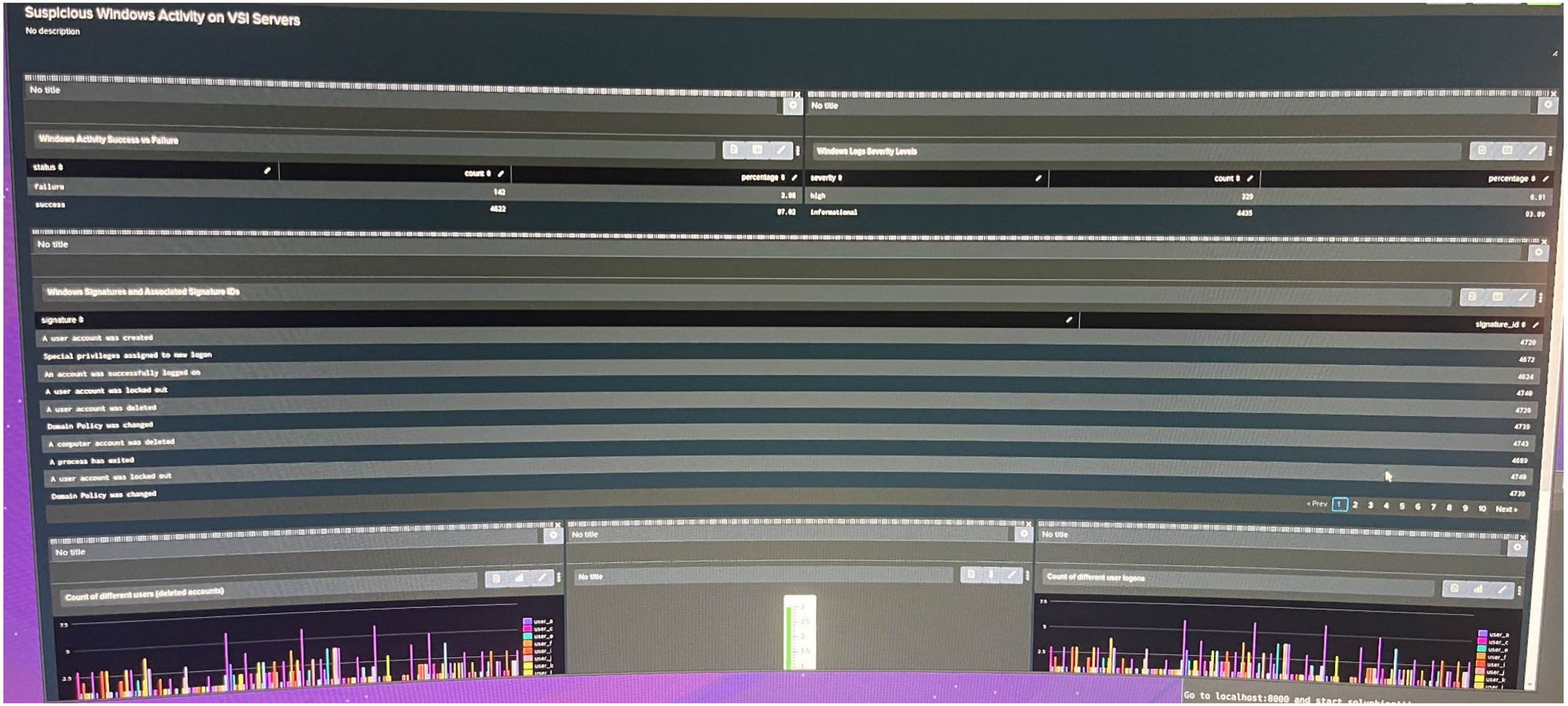
Alerts—Windows

Designed the following alerts:

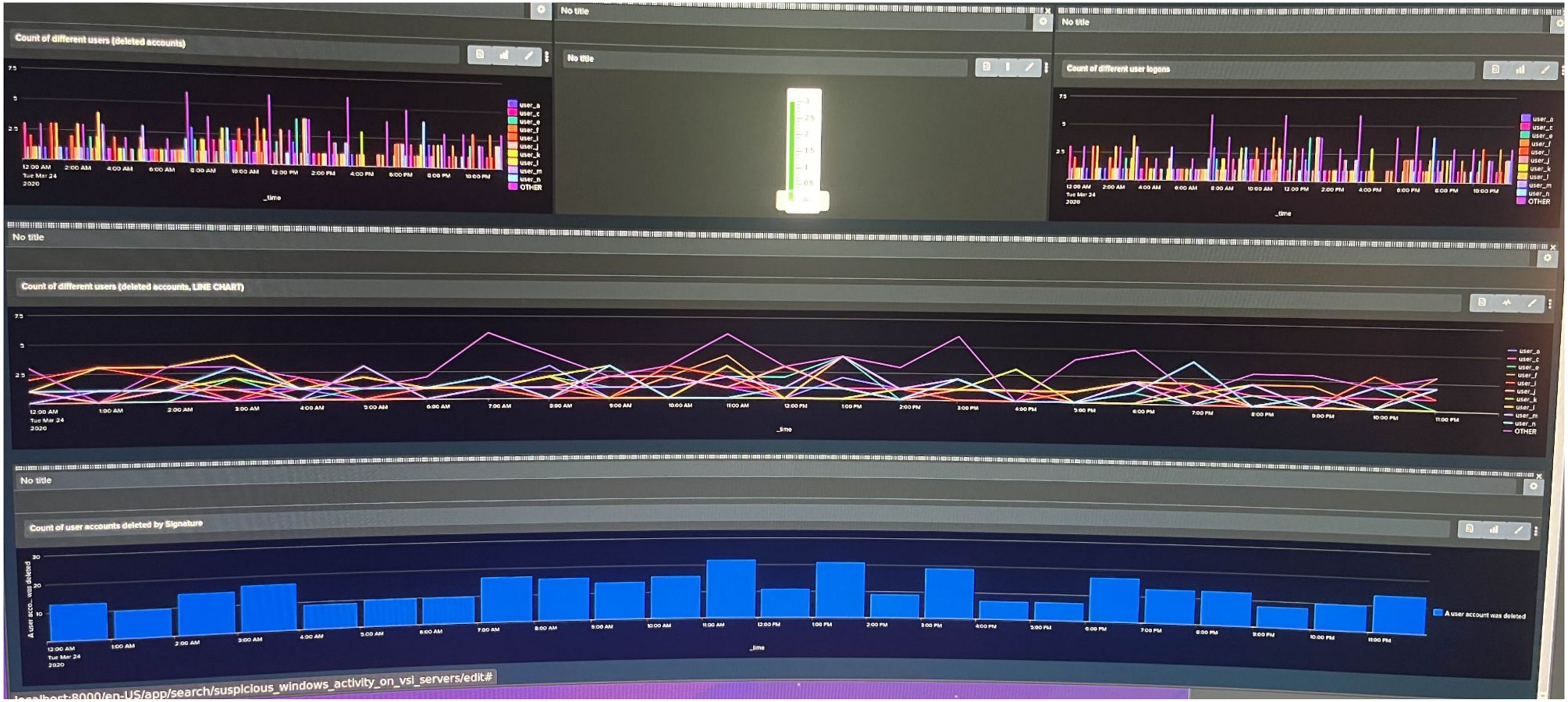
Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Deleted User Accounts	Threshold of Deleted Account Users	[27]	[50]

JUSTIFICATION: A baseline of 27 seemed on par with a "normal" hour. Exceeding 50 would raise suspicion levels and indicate a problem.

Dashboards—Windows (outdated pics but Ubuntu is down soo)



Dashboards—Windows (outdated pics but Ubuntu is down soo)



Apache Logs

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Count	Alert if the hourly count of the HTTP POST method exceeds the threshold.	3	12

JUSTIFICATION: Most events per hour hovered between 1 and 4 and never surpassed 7. A threshold of 12 seemed like a number that would be out of reach of "normal" hourly events but small enough to catch malicious activity.

Alerts—Apache

Designed the following alerts:

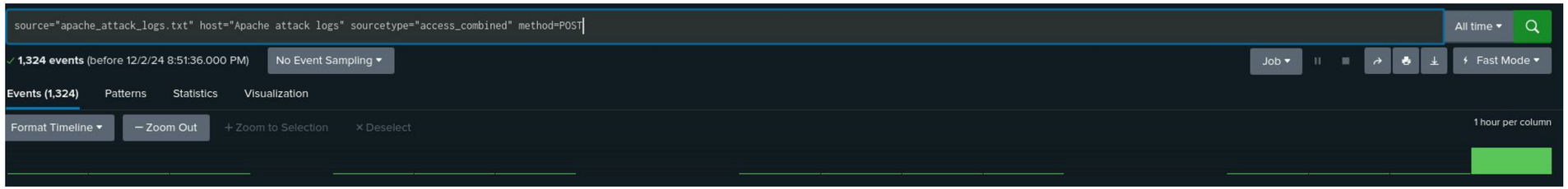
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert International Activity	if the hourly activity from any country besides the United States exceeds the threshold	120	170

JUSTIFICATION: 120 events in a hour seemed standard in the logs, yet exceeding 170 seemed unlikely on a normal day. Seeing any number of events greater than the threshold would indicate issues.

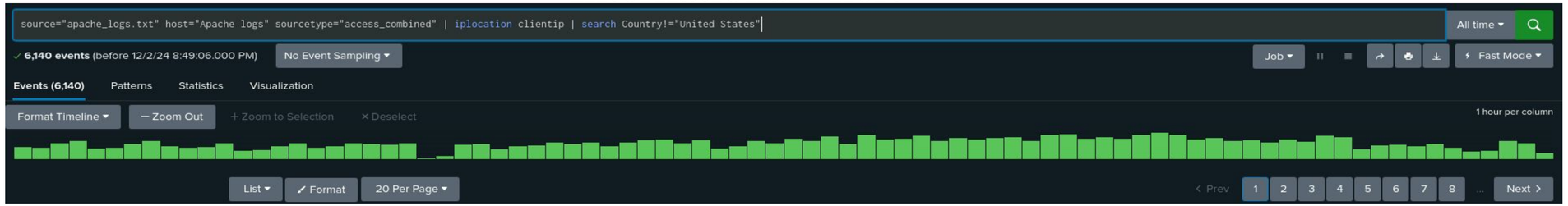
Images of Reports—Apache

HTTP POST Alert

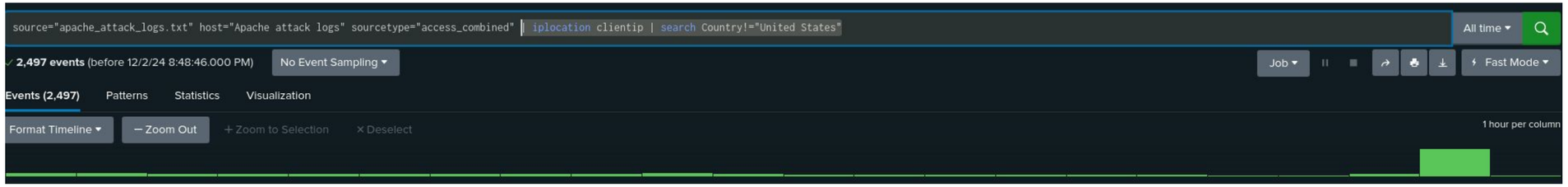
Attack HTTP Alert



International Alert



International Attack Alert



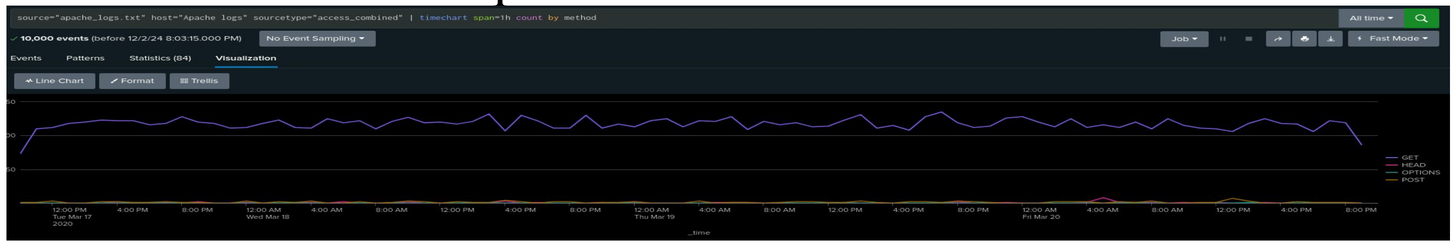
Reports—Apache

Designed the following reports:

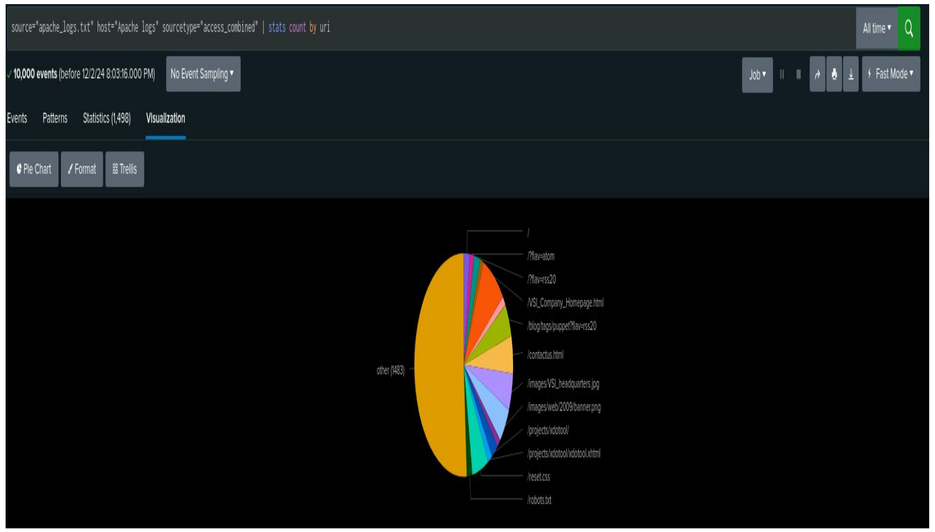
Report Name	Report Description
HTTP methods	A report that will provide insight into the type of HTTP activity being requested against VSI's web server.
Top 10 Domains	A report that shows the top 10 domains that refer to VSI's website
HTTP Errors	A report that shows the count of HTTP connection failures.
Cluster Map	A map of Ip address that shows user counts
URI Data	identify a resource within the network.

Images of Dashboard—Apache

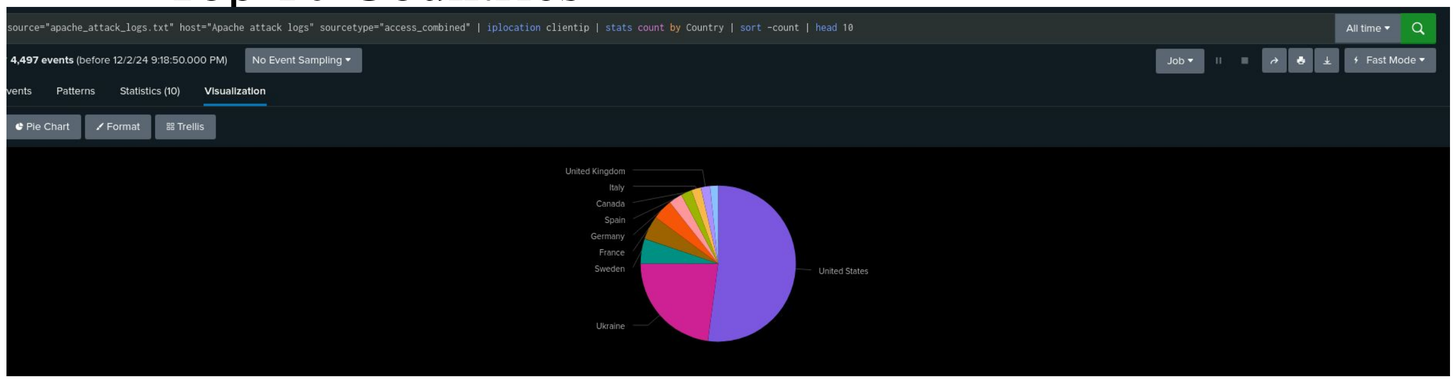
HTTP Methods Graph



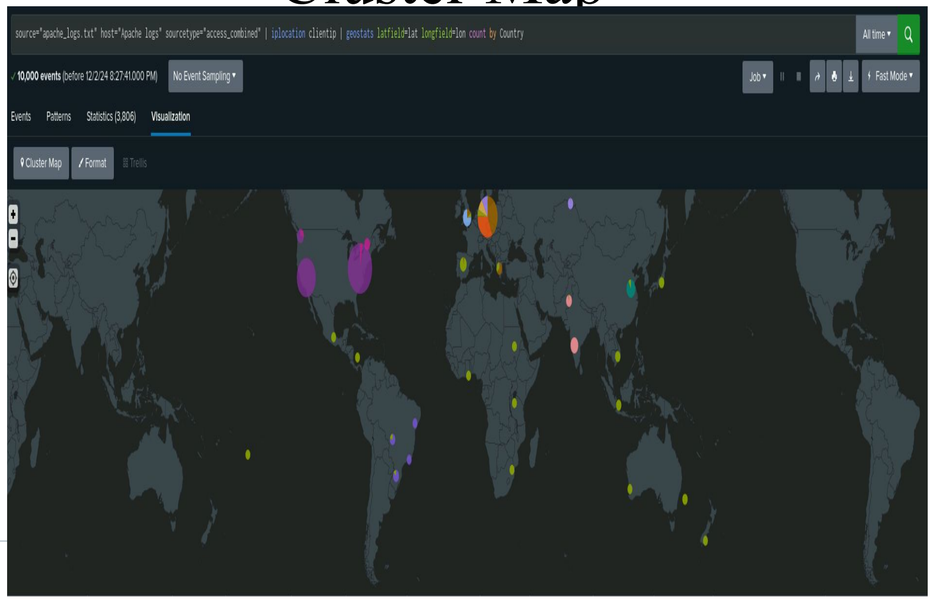
URI Data



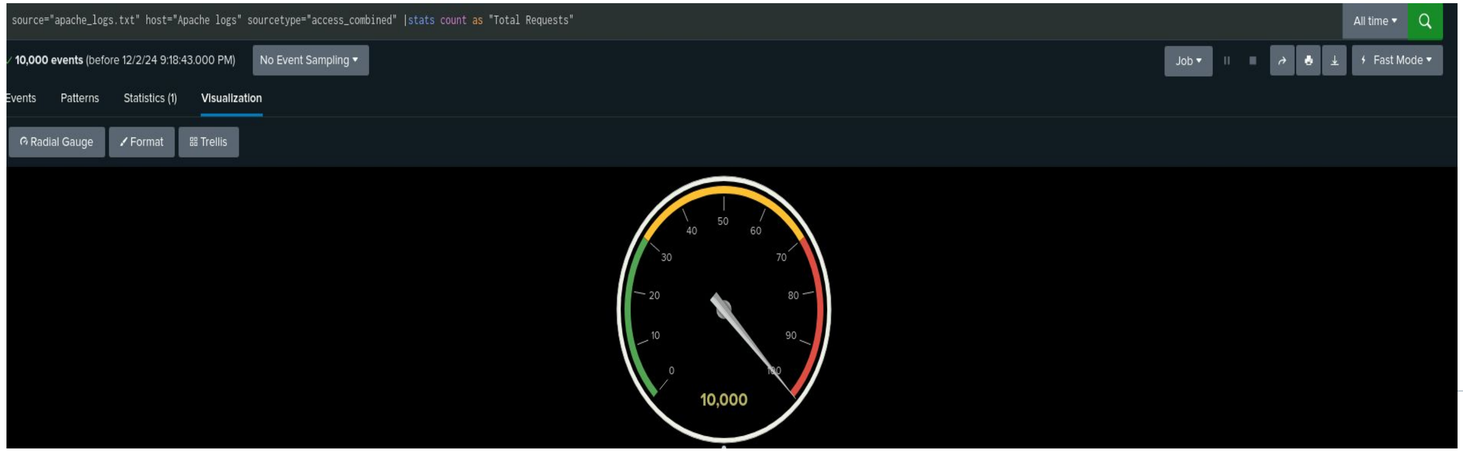
Top 10 Countries



Cluster Map



HTTP Errors

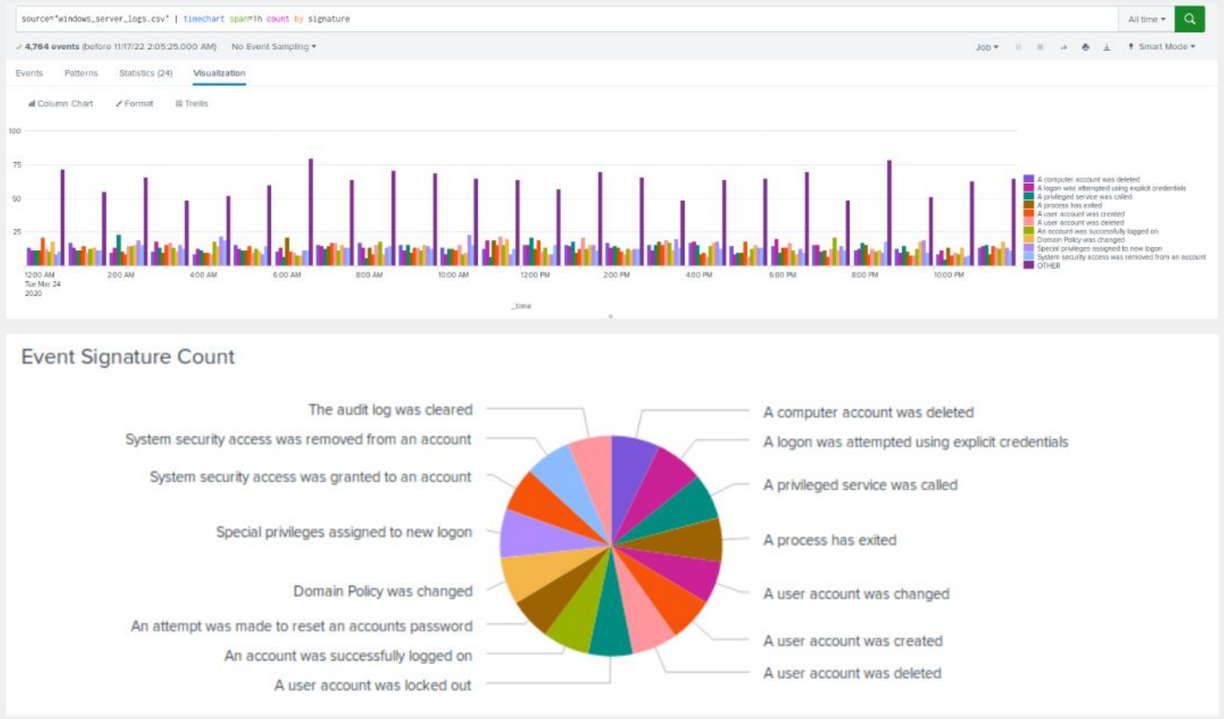


Attack Analysis

Attack Summary—Windows

"An attempt was made to reset an account password" and "A user account was locked out" increased in the attack logs compared to the regular Windows server logs

Normal Logs:

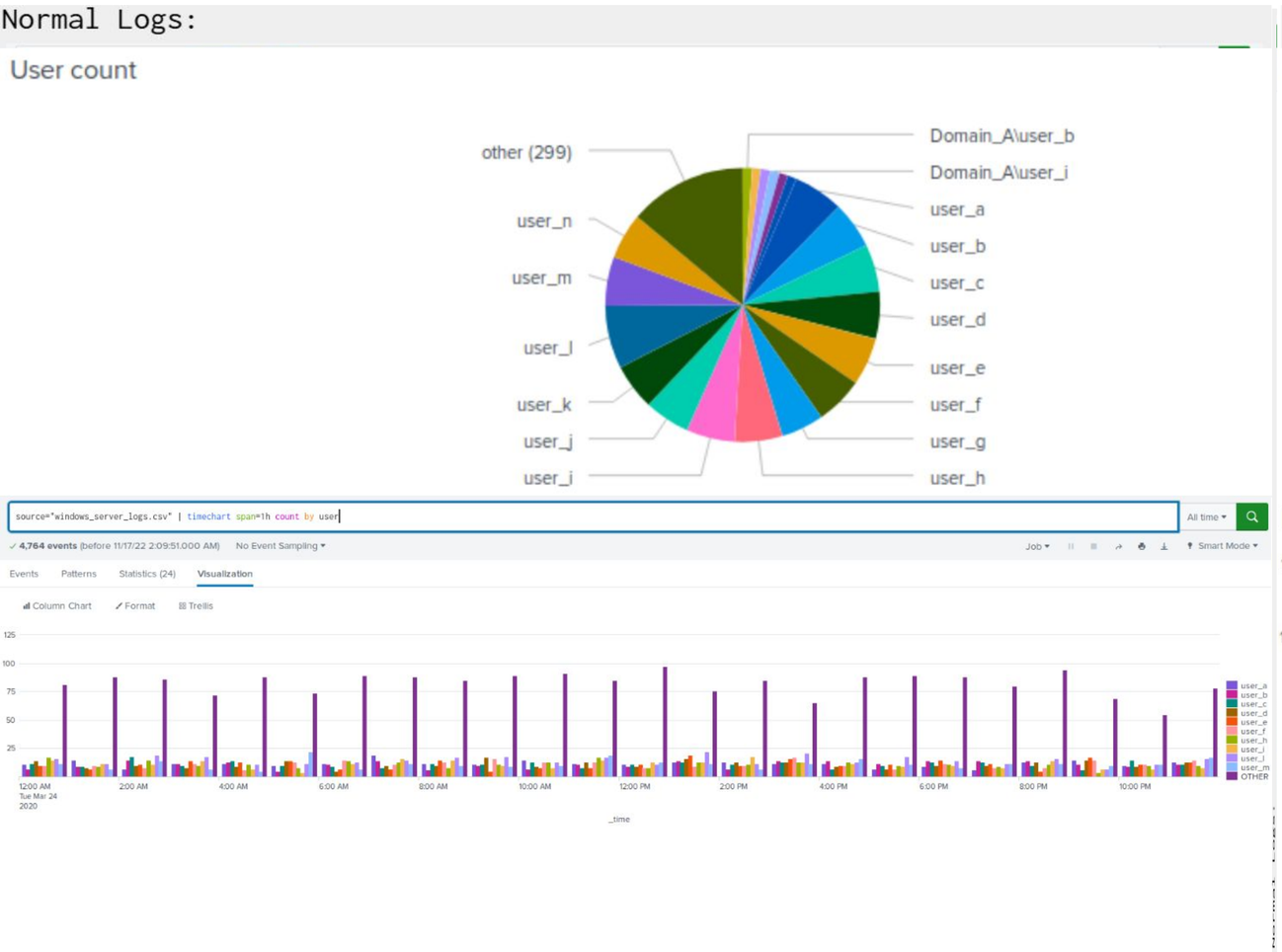


Attack Logs:

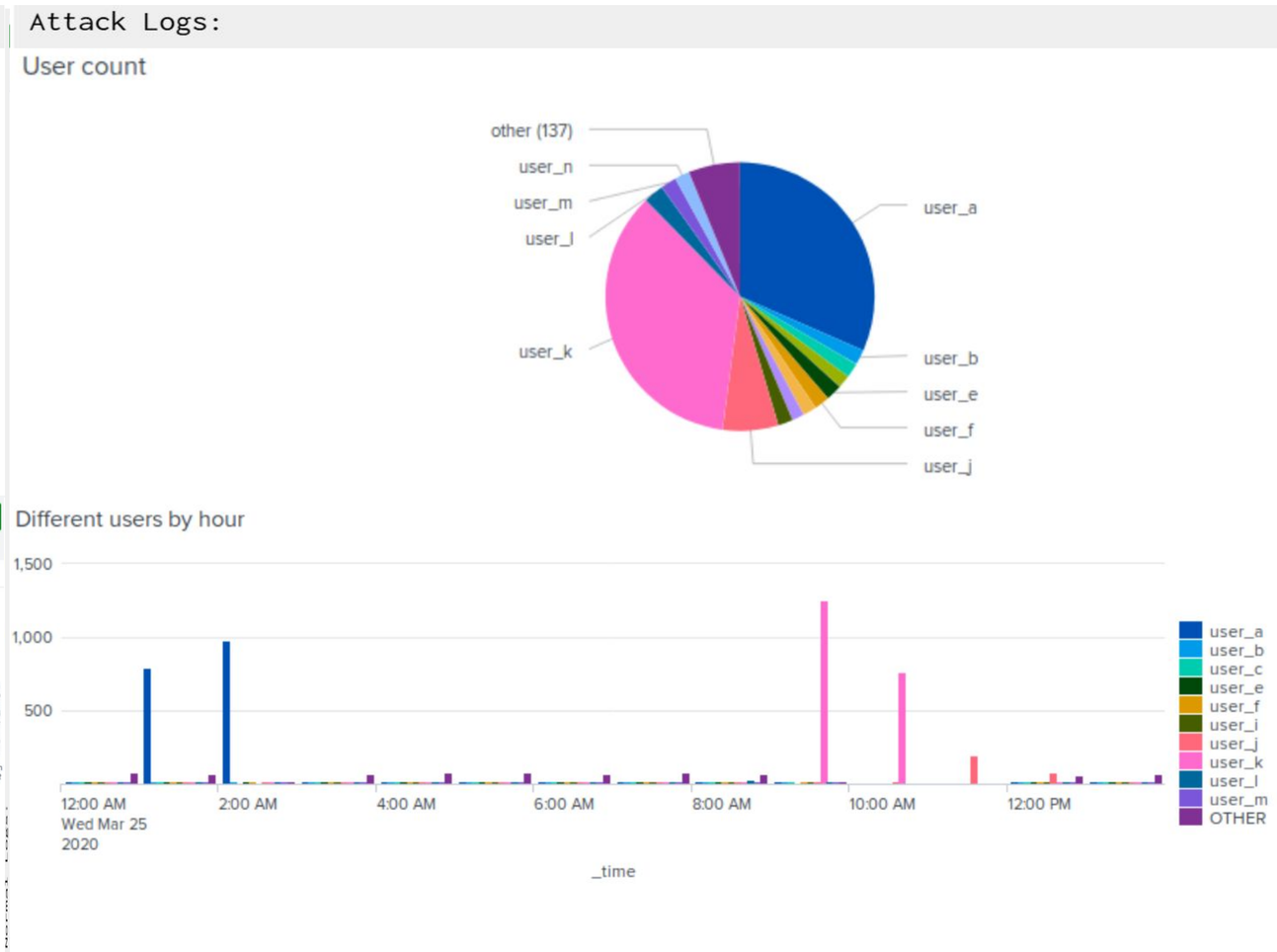
Attack Summary—Windows

Users user_a and user_k had suspiciously high and long activity in the attack logs analyzed when compared to the avg. user in the Windows server logs

Normal Logs:



Attack Logs:



Attack Summary—Windows

Executive Windows Summary pt.1

- Windows attack system had more severity levels in the "high" category than almost 95% "informational" before the attack. Alert analysis indicated suspicious volume of failed activity

- Failed logins: Threshold was met, flags indicated, no significant changes are recommended

- Successful logins: Suspicious volumes of successful logins detected by user_a and user_k – thresholds adjusted accordingly to avoid alert fatigue

- Suspiciously high levels of failed activity (“A user account was locked out” & “An attempt was made to reset an account password”) – diagnosed user_a and user_k of being the culprit accounts to this Brute Force attempt

Attack Summary—Windows

Executive Windows Summary pt.2

Suspicious login activity detected:

- User_a has an increase in their amount of activity time during the attack logs between 01:00-02:00AM. User_k had an increase in their activity from 09:00-10:00AM
- During this time, user_a peaked at 984 and user_k peaked at 1256

Suspicious signature increases detected:

- “An attempt was made to reset account password” & “A user account was locked out” increased significantly during the attack between 09:00-10:00AM and 01:00-02:30AM, respectively
- During this time, Account locked out peaked at 896 and Reset password attempts peaked at 1268

The login attempts of user_a and user_k exceeding thresholds during the same time as these signature increases leads our SOC team to believe these two users are responsible for attempting to hinder VSI business functionality via Brute Force attacks through the Windows Server.

Attack Summary—Apache

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

We detected a suspicious volume of international activity between

8pm and 9pm

Our threshold was correct and our alert would have been triggered.

We detected a suspicious volume of HTTP POST activity between

8pm and 9pm on March 25th peaking at 1,296.

Our threshold was correct and our alert would have triggered.

Attack Summary—Apache

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

Our Time Chart of HTTP methods revealed suspicious volumes of GET

and POST methods.

The GET attack went from 5pm to 7pm and peaked with a count of 729.

The POST attack went from 7pm to 9pm and peaked with a count of 1,296.

Our Cluster Map revealed suspicious activity from a couple cities.

Kiev (439), Kharkiv (433), D.C. (714), and NYC(549) all had high volumes of activity.

Our URI Data flagged "/VSI_Account_logon.php" as having suspiciously high volume.

Attack Summary—Apache

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

There was a significant increase in POST, HTTP methods.

We did not detect any suspicious activity in referrer domains.

It is possible our reports did not catch it. More analysis is needed.

The HTTP Response Codes report showed that "404" jumped from 2% to 15%.

Summary and Future Mitigations

Project 3 Summary

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

On March 25, 2020 VSI had multiple attacks on there Windows and Apache servers. These attacks mainly consisted of Bruteforce Password spamming, from different regions and countries across the glob.

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

  Two-factor authentication

Lock users out after a certain number of login attempts