Defensive Security Project
by: Room 5

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- The Virtual Space Industries (VSI) suspects their competitor JobeCorp of launching cyber attacks to disrupt their business.
- Our SOC team has been hired to monitor against any potential attacks.
- The main areas of concern are the administrative webpage, the Apache server, and the Windows OS.
- VSI has provided past logs to help create a baseline of activity.
- Our team is tasked with using Splunk to create reports, alerts, and dashboards to help protect VSI from any cyberattacks.

Windows Security Operations Center

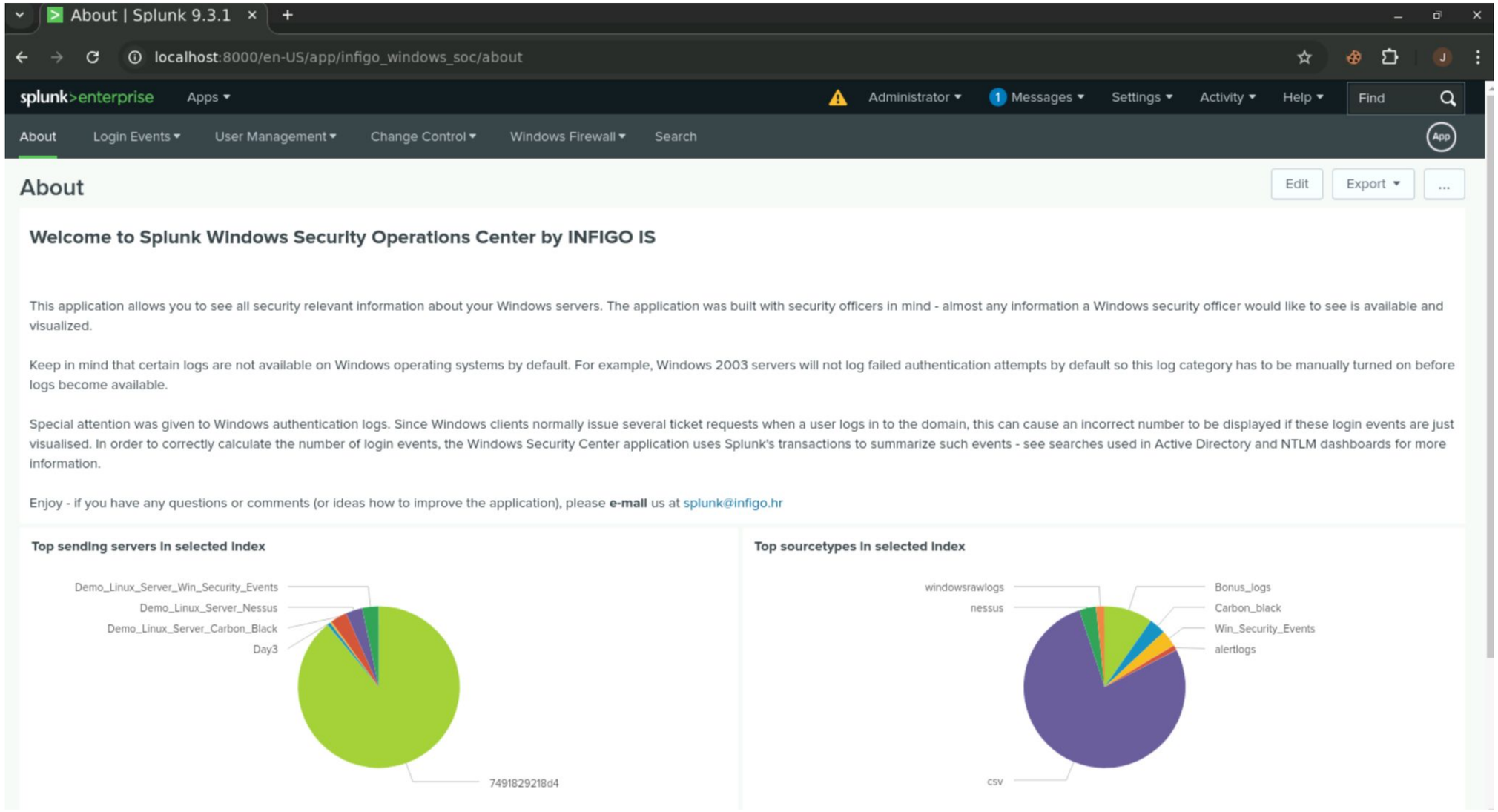
Windows Security Operations Center

- This applications summarizes and visualizes all security relevant information in Windows environments.
- The application offers monitoring of successful and failed Windows AD and NTLM authentications as well as RDP and console services.
- Tracks software installations and Directory Services access and modifications.
- This Add on was provided by INFIGO. Built by Bojan Zdrnja.

Windows Security Operations Center

- It easily helps with the windows server analysis
- Provides great illustrative Dashboards.
- The App monitors all different types of Windows Server Authentication (Windows Active Directory and NTLM).
- The App also monitors RDP authentions.
- Dashboards show Windows host based firewall activities as well.

Windows Security Operations Center



Logs Analyzed

1 Windows Logs

The data in these logs focuses on the backend components for VSI.

- Account Management
- Event codes
- Successful and Unsuccessful logins
- Domain Policy

2 Apache Logs

The data in the logs focuses on the webpage.

- Client IP
- User agents
- HTTP methods

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signatures	Table shows signatures and associated IDs
Severity	Table shows severity levels with count and percentage for each
Status	Table shows comparison of the success and failure of Windows activities

Images of Reports—Windows

Signatures

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Signatures and Signature ID's

✓ **4,764 events** (before 11/28/24 4:18:16.000 AM)

Job ▾

15 results | 20 per page ▾

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
System security access was removed from an account	4718
A user account was changed	4738
Special privileges assigned to new logon	4672

Severity

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Severity, count and percentage

All time ▾

✓ **4,764 events** (before 11/28/24 4:18:53.000 AM)

Job ▾

2 results | 20 per page ▾

severity	count	percent
informational	4435	93.094039
high	329	6.905961

Status

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Success/Failure rates

All time ▾

✓ **4,764 events** (before 11/28/24 3:45:57.000 AM)

Job ▾

2 results | 20 per page ▾

status	count	percent
success	4622	97.019312
failure	142	2.980688

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Failures	Hourly level of failed Windows Activity	Avg. 6/hr (max 10)	12 per hour

JUSTIFICATION: Since the normal average is about **6** failures in a single hour and the maximum recorded in the normal logs provided was **10**, we determined **12** to be a good threshold to minimize false positives while not missing any unusually high amounts of Windows activity failures that might warrant further investigation.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins	Hourly count of “An account was successfully logged on”	Avg. 13/hr (max 21)	23 per hour

JUSTIFICATION: Since the normal average is about **13** successful logins in a single hour and the maximum recorded in the normal logs provided was **21**, we determined **23** to be a good threshold to minimize false positives while not missing any unusually high amounts of successful logins that might warrant further investigation.

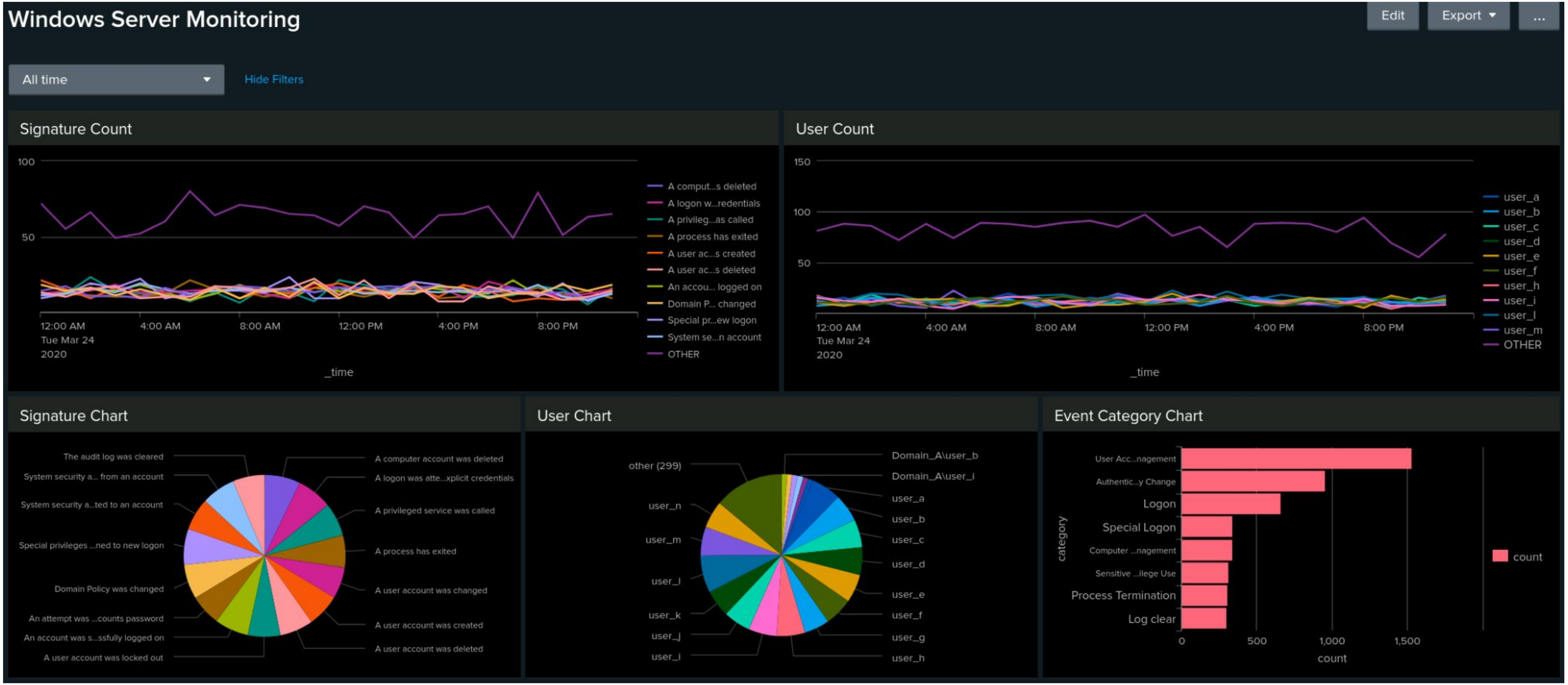
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Accounts Deleted	Hourly count of “A user account was deleted”	Avg. 13/hr (max 22)	23 per hour

JUSTIFICATION: Since the normal average is about **13** deletions in a single hour and the maximum recorded in the normal logs provided was **22**, we determined **23** to be a good threshold to minimize false positives while not missing any unusually high amounts of account deletions that might warrant further investigation.

Dashboards—Windows



Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Table shows the count of the different HTTP methods (GET, POST, HEAD, and OPTIONS)
Domains	Table shows the count and percent of the top 10 referring domains
HTTP Responses	Table shows the count of each HTTP response code

Images of Reports—Apache

Domains Report

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Shows top 10 domain referrers

All time ▾

✓ **10,000 events** (before 11/28/24 4:51:58.000 AM)

Job ▾

10 results | 20 per page ▾

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

HTTP Methods

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Shows different HTTP methods by count

All time ▾

✓ **10,000 events** (before 11/28/24 4:51:51.000 AM)

Job ▾

4 results | 20 per page ▾

method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106

HTTP Responses

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Shows count of HTTP response codes

All time ▾

✓ **10,000 events** (before 11/28/24 4:52:00.000 AM)

Job ▾

8 results | 20 per page ▾

status	count
200	9126
206	45
301	164
304	445
403	2
404	213
416	2
500	3

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
International Activity	Hourly level of activity from any country besides the United States	Avg. 73/hr (max 120)	200

JUSTIFICATION: Since the normal average is about **73** events from international IP addresses in a single hour and the maximum recorded in the normal logs provided was **120**, we determined **200** to be a good threshold to minimize false positives while not missing any unusually high amounts of account deletions that might warrant further investigation.

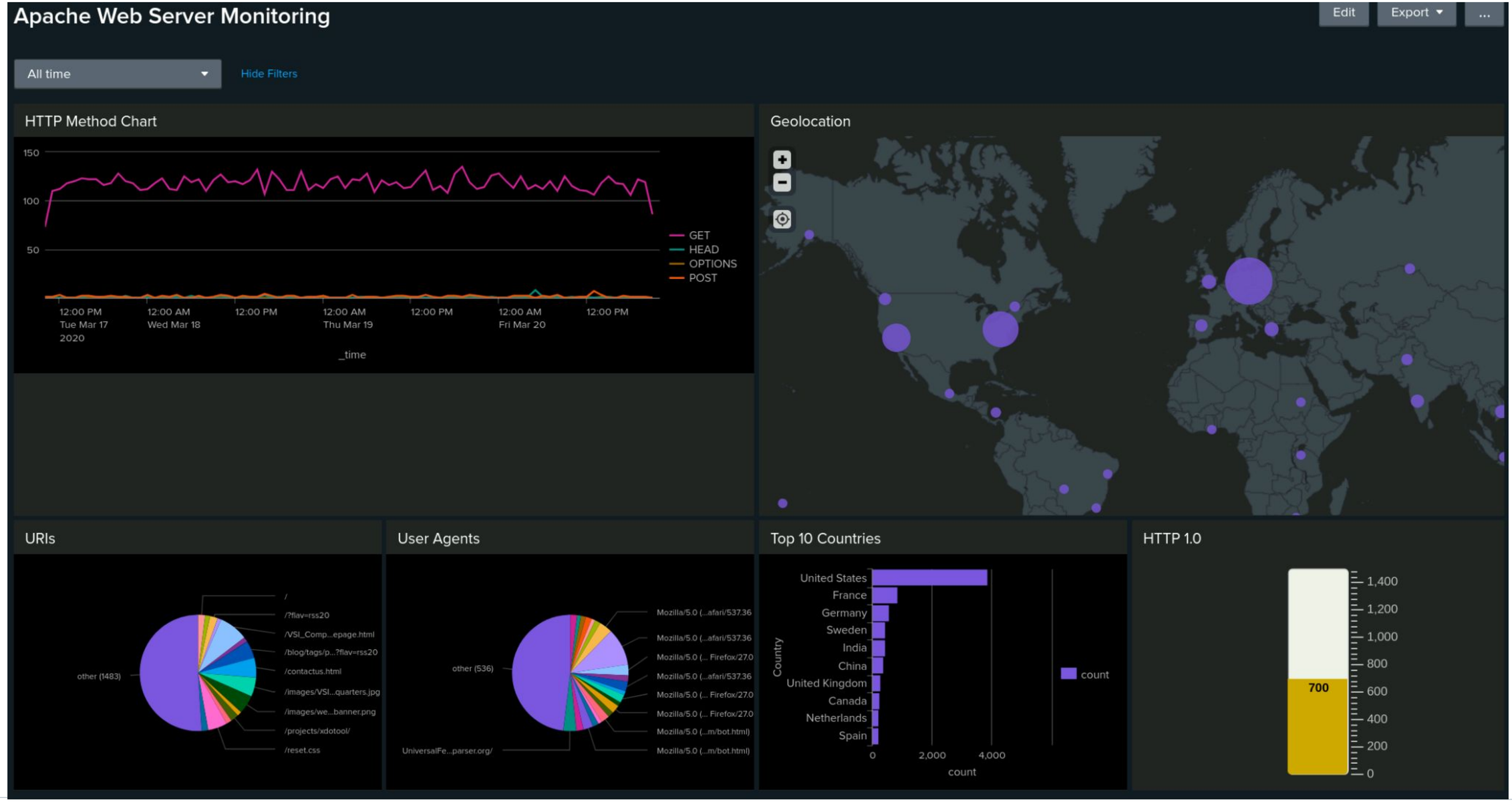
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Methods	Hourly count of the HTTP Post method	Avg. 2/hr (max 7)	10

JUSTIFICATION: Since the normal average is about **2** HTTP POST events in a single hour and the maximum recorded in the normal logs provided was **7**, we determined **10** to be a good threshold to minimize false positives while not missing any unusually high amounts of account deletions that might warrant further investigation.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

Windows attack report summary

- Type of attack identified:
  Brute Force
  - Volume of failed attempts
- Attackers involved
  - User A, User K, User J
- Key Observations
  - Concerted effort
  - Monitoring certain accounts

Attack Summary—Windows

Attack Logins thresholds

- Failed login activity
  - Correct threshold
- Successful login activity
  - Unable to detect
- Account Deletion activity
  - Unable to detect

Attack Summary—Windows

Dashboards attack logs.

- Key attackers Identified
  - Users A, K, and J
- Timing of attacks
  - 3 Hour time frames
- Key insights
  - Lockout and password reset patterns helped reveal attacker behavior

Screenshots of Attack Logs - Reports

Signatures

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Signatures and Signature ID's

✓ **5,949 events** (before 11/28/24 3:45:45.000 AM)

Job ▾

982 results | 20 per page ▾ | ‹ Prev | 1 2 3 4 5 6 7 8 ... | Next ›

signature	signature_id
An account was successfully logged on	4624
A user account was deleted	4726
A user account was changed	4738
A logon was attempted using explicit credentials	4648
Domain Policy was changed	4739
An attempt was made to reset an accounts password	4724
A privileged service was called	4673
System security access was removed from an account	4718
A user account was created	4720
A process has exited	4689
A computer account was deleted	4743
System security access was granted to an account	4717
A user account was locked out	4740
The audit log was cleared	1102
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	5340
An attempt was made to reset an accounts password	5339
An attempt was made to reset an accounts password	5338
An attempt was made to reset an accounts password	5337
An attempt was made to reset an accounts password	5336

Severity

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Severity, count and percentage

All time ▾

✓ **5,949 events** (before 11/28/24 3:45:53.000 AM)

Job ▾

2 results | 20 per page ▾

severity	count	percent
informational	4383	79.777940
high	1111	20.222060

Status

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Success/Failure rates

All time ▾

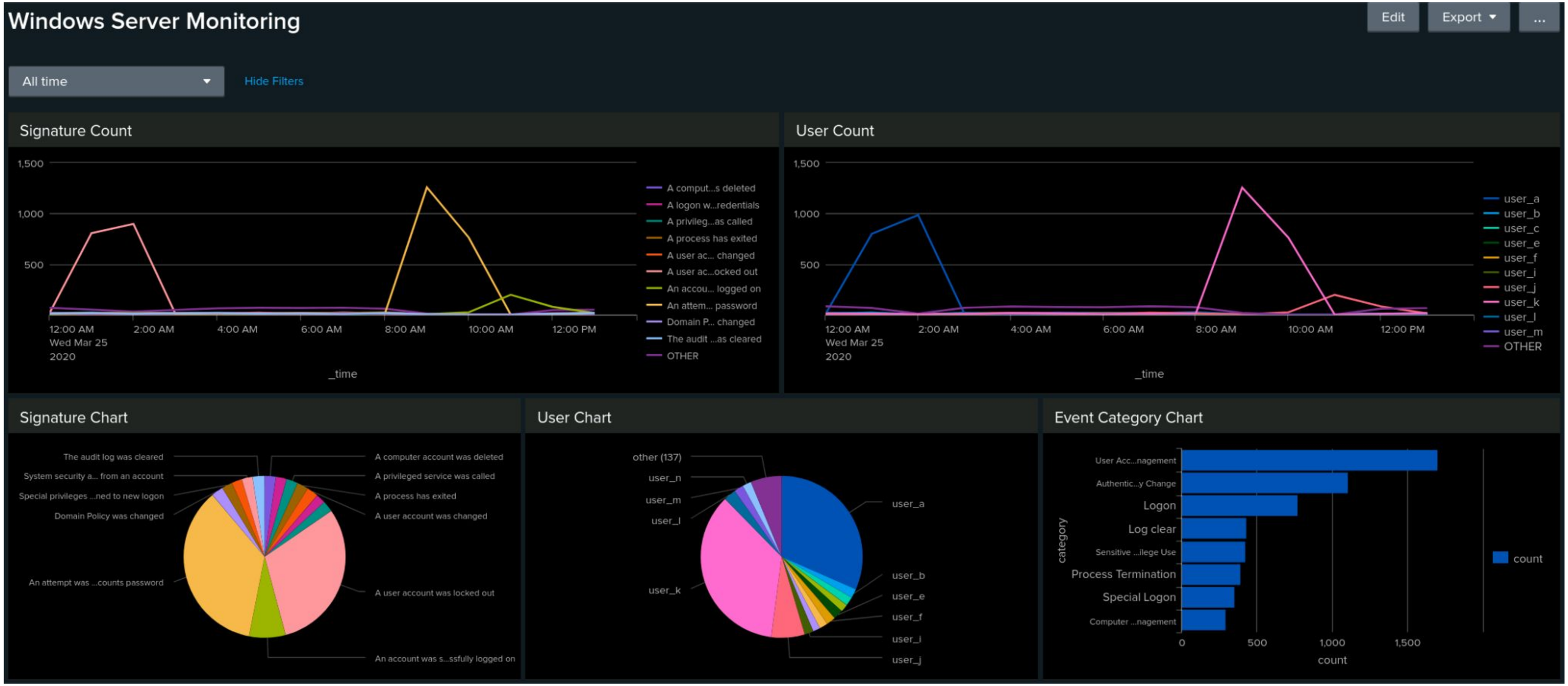
✓ **5,949 events** (before 11/28/24 4:18:36.000 AM)

Job ▾

2 results | 20 per page ▾

status	count	percent
success	5856	98.436712
failure	93	1.563288

Screenshots of Attack Logs - Dashboard



Attack Summary—Apache

Reports Analysis

- HTTP method:
  - HTTP POST request was suspicious
  - Events rose from 106 to 1324

- Referrer Domain
  - There were no Suspicious activity

- HTTP response code report analysis
  - Response code 404 rose from 213 to 679.

Attack Summary—Apache

Apache Alerts Analysis

- International Activity
  - Correct threshold - threshold was 200 events.
  - Occurred at 8pm
  - Alert was triggered.

- HTTP POST Activity
  - Correct threshold - threshold was 10 events.
  - Occurred at 8pm
  - Alert was triggered

Attack Summary—Apache

Dashboard analysis

- HTTP Method: GET and POST
  - GET occurred at 5pm to 7pm and POST 7pm to 9pm
  - GET count was 729 and POST was 1296

- Cities with suspicious activity
  - Kyiv and Kharkiv

- Most visited URI
  - VSI_Account_Logon.PHP

Screenshots of Attack Logs - Reports

Domains Report

Edit | More Info | Add to Dashboard

Shows top 10 domain referrers

All time

✓ **4,497 events** (before 11/28/24 5:09:58.000 AM)

Job

10 results | 20 per page

referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

HTTP Methods

Edit | More Info | Add to Dashboard

Shows different HTTP methods by count

All time

✓ **4,497 events** (before 11/28/24 5:09:57.000 AM)

Job

4 results | 20 per page

method	count
GET	3157
HEAD	15
OPTIONS	1
POST	1324

HTTP Responses

Edit | More Info | Add to Dashboard

Shows count of HTTP response codes

All time

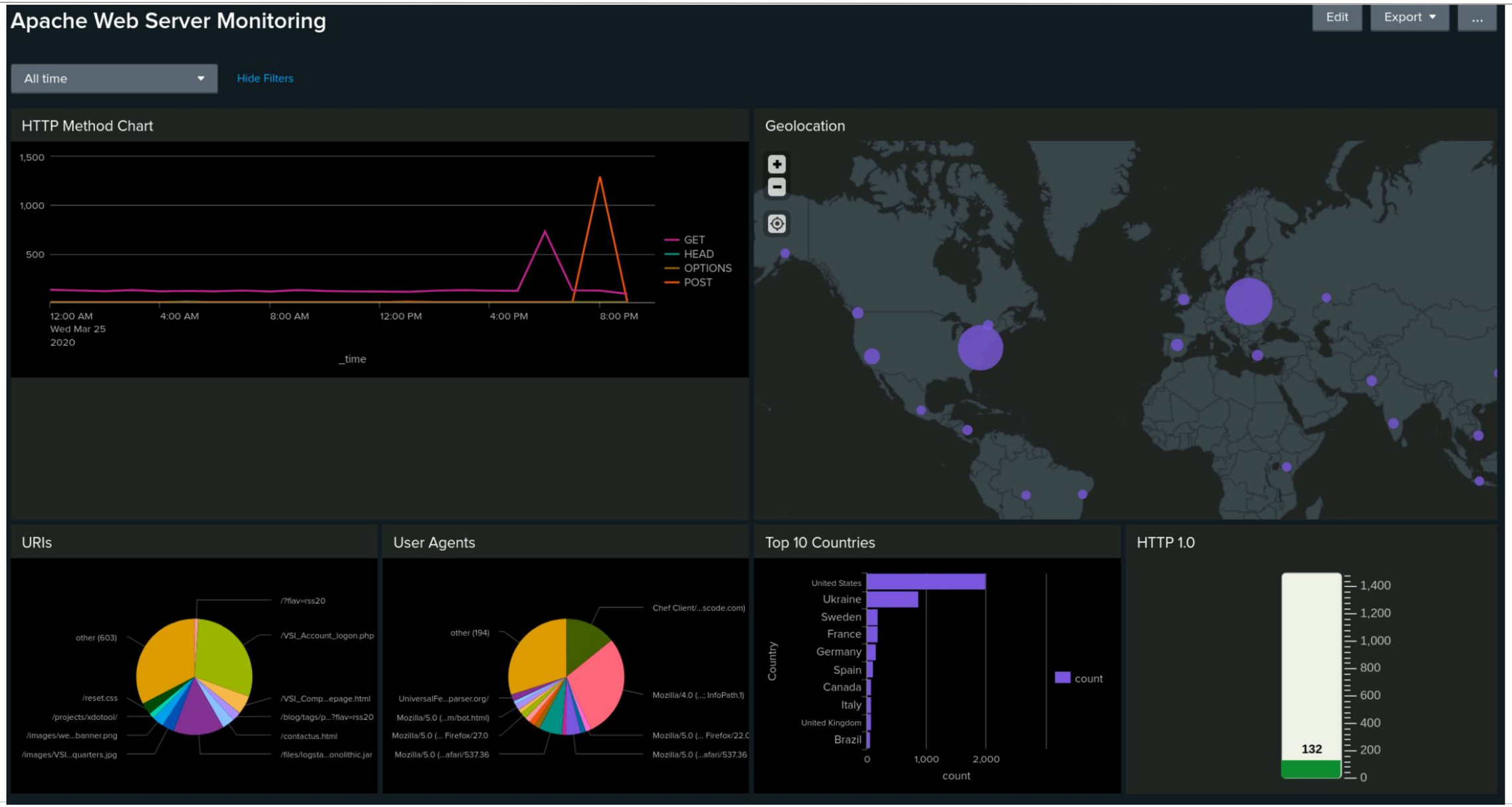
✓ **4,497 events** (before 11/28/24 5:10:00.000 AM)

Job

7 results | 20 per page

status	count
200	3746
206	5
301	29
304	36
403	1
404	679
500	1

Screenshots of Attack Logs - Dashboard



Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
- Windows severity events increased from 329 to 1111 and failures changed from 142 to 93.
- Windows Users A, K, and J had 895 account lockouts, 1258 attempts to reset password, and 196 logins. This would be a credential stuffing attack.
- Apache HTTP requests were 729 GET’s and 1296 POST’s from 5pm-9pm. This could be a DDOS attack. High activity from Kyiv and Kharkiv, Ukraine could indicate coordinated attackers or botnets.
- VSI_Account_logon.php had an attempted brute force attack to access a login page

Summary Mitigations

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

- For Windows, implement MFA, account lockout policies, Email notifications for account changes, password complexity requirements, session management, rate limit login attempts, and IP whitelisting to prevent specific locations for sensitive accounts.

- On Apache, implement rate limiting, strict web application firewalls, IP blacklisting preventing suspicious IP’s, input validation and sanitization, strict access controls and permissions, and use HTTPS.