Defensive Security Project
by: Group 2

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

In the ever-evolving landscape of cybersecurity, our Security Operations Center (SOC) team is essential in safeguarding VSI’s digital assets. We are entrusted with a range of critical responsibilities that ensure the integrity and security of our systems.

Our primary duty is to continuously monitor and analyze logs from various servers, including Windows Server and Apache Web Server. This constant vigilance enables us to detect potential security threats and anomalies that could compromise our systems. We proactively assess user activity, looking for unusual patterns that may indicate unauthorized access or malicious intent.

Another key responsibility is to investigate alerts generated from our monitoring systems. When red flags arise, we delve into the details to understand the context and severity of the situation. This involves collaborating with other teams to address any identified vulnerabilities and implement necessary corrective measures.

We also prioritize user access controls, ensuring that permissions are appropriately assigned and regularly reviewed. By managing who has access to sensitive information, we help mitigate risks associated with unauthorized access.

Additionally, we engage in regular security assessments and vulnerability testing. This proactive approach allows us to identify weaknesses in our infrastructure before they can be exploited.

Our team is dedicated to enhancing our anomaly detection mechanisms, continually refining our processes to minimize alert fatigue while ensuring genuine threats are addressed effectively.

WebSite Monitoring

WebSite Monitoring

Today, I want to talk about the benefits and challenges of implementing Website Monitoring. This is an important consideration for organizations looking to enhance their web performance management.

Pros

1. **Real-Time Monitoring**
   - One of the standout features is real-time visibility into website performance and uptime. This means you can detect issues as they happen, allowing for immediate action.
2. **Uptime Calculation**
   - Website Monitoring tracks your site's uptime and downtime, providing clear insights into reliability. You can easily assess how well your web services are performing.
3. **Detailed Dashboards**
   - The dashboards are comprehensive and visually appealing, showcasing real-time response times and historical data. This makes it easier to analyze trends and identify patterns.
4. **Alerting Features**
   - You receive instant notifications for outages or slow response times. This proactive alerting helps you address issues before they escalate, ultimately enhancing user experience.
5. **Change History Tracking**
   - The tool keeps a record of changes made to monitored pages. This feature is invaluable for understanding how updates impact performance and for troubleshooting purposes.
6. **Integration with Existing Infrastructure**
   - It integrates seamlessly with your existing Splunk setup, allowing you to correlate web performance data with other operational metrics. This holistic view is crucial for effective management.
7. **Scalability**
   - Whether you're monitoring one website or many, this solution is scalable and can handle diverse web assets efficiently.

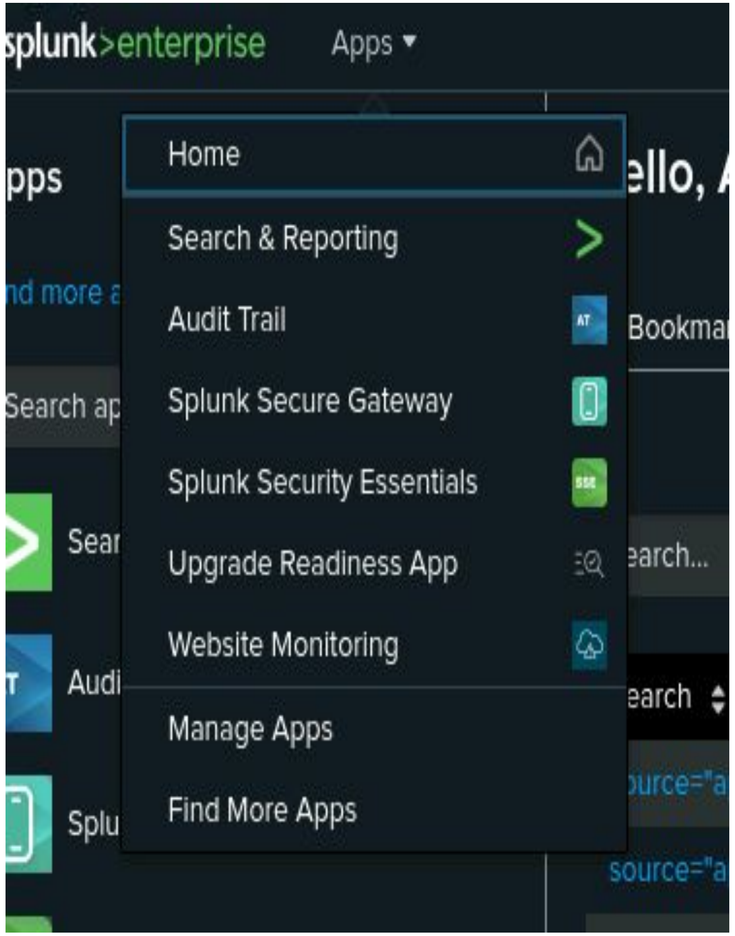
Cons

1. **Complexity**
   - On the flip side, setting up and configuring the monitoring solution can be complex. It may require specialized knowledge of both Splunk and web performance monitoring.
2. **Resource Intensive**
   - Continuous monitoring can be resource-intensive. If not managed properly, it might impact the overall performance of your Splunk environment.
3. **Cost Considerations**
   - Depending on your data volume and monitoring needs, costs can rise. Organizations need to be mindful of potential additional resource or licensing expenses.
4. **False Positives**
   - The alerting mechanisms, while useful, can sometimes generate false positives. This could lead to alert fatigue among teams if they receive too many unnecessary notifications.
5. **Dependency on External Factors**
   - Website performance can be influenced by factors beyond your control, such as third-party services. This complicates monitoring and troubleshooting efforts.
6. **Data Retention Challenges**
   - Keeping historical data for long-term analysis may require additional storage management, which can increase infrastructure costs.
7. **Integration Challenges**
   - Lastly, integrating with existing monitoring tools or workflows might necessitate additional customization, which can be time-consuming and require extra development effort.

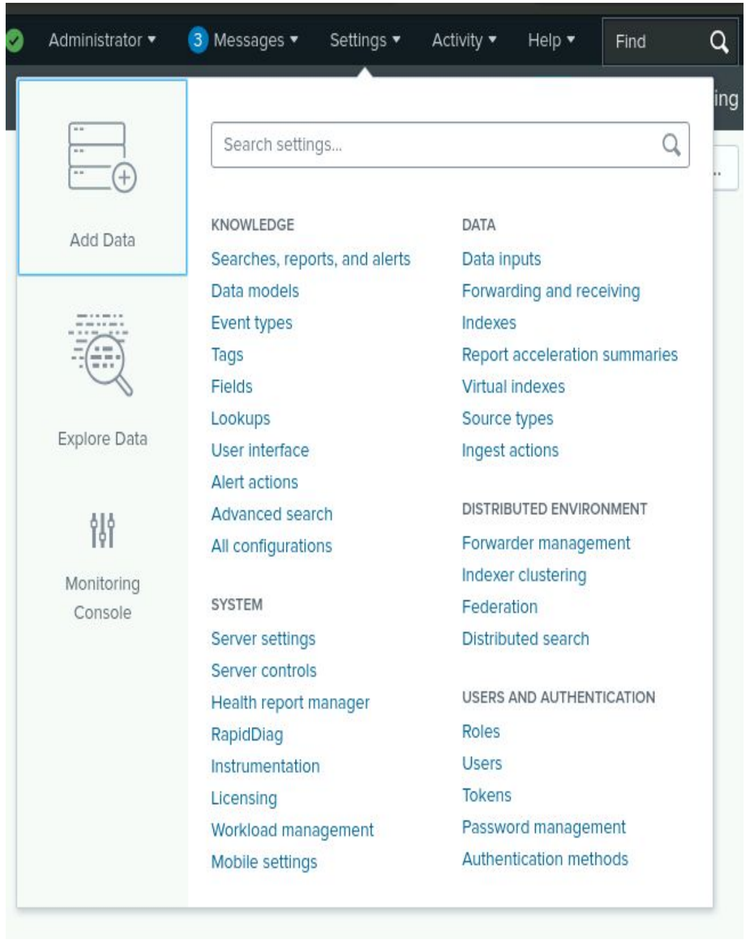
In summary, using Website Monitoring offers significant advantages, particularly in enhancing visibility and proactive incident management. However, it's essential to weigh these benefits against the potential complexities and costs involved. With careful planning and management, organizations can make the most of these tools while minimizing the drawbacks.

WebSite Monitoring

In Apps Menu, select *Website Monitoring*



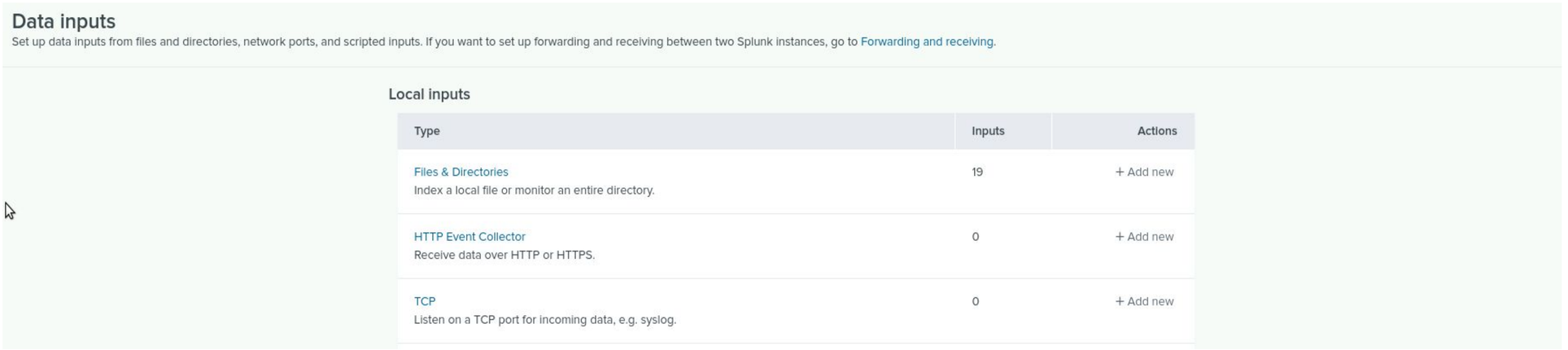
To add Data Source, go to Settings, then Data Inputs



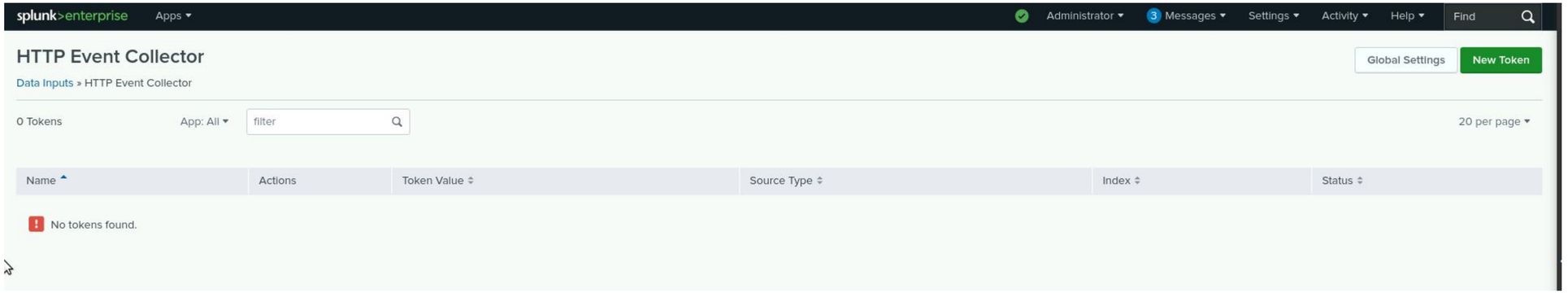
WebSite Monitoring

Data Inputs & Adding New Token

As you'll see in the menu, you can select a varying number of Inputs you'd like to display. For this Input, select *HTTP Event Collector.*



Next, choose *New Token* (A "Token" is a placeholder or variable that is used to represent a dynamic value within a Splunk configuration or search query.)

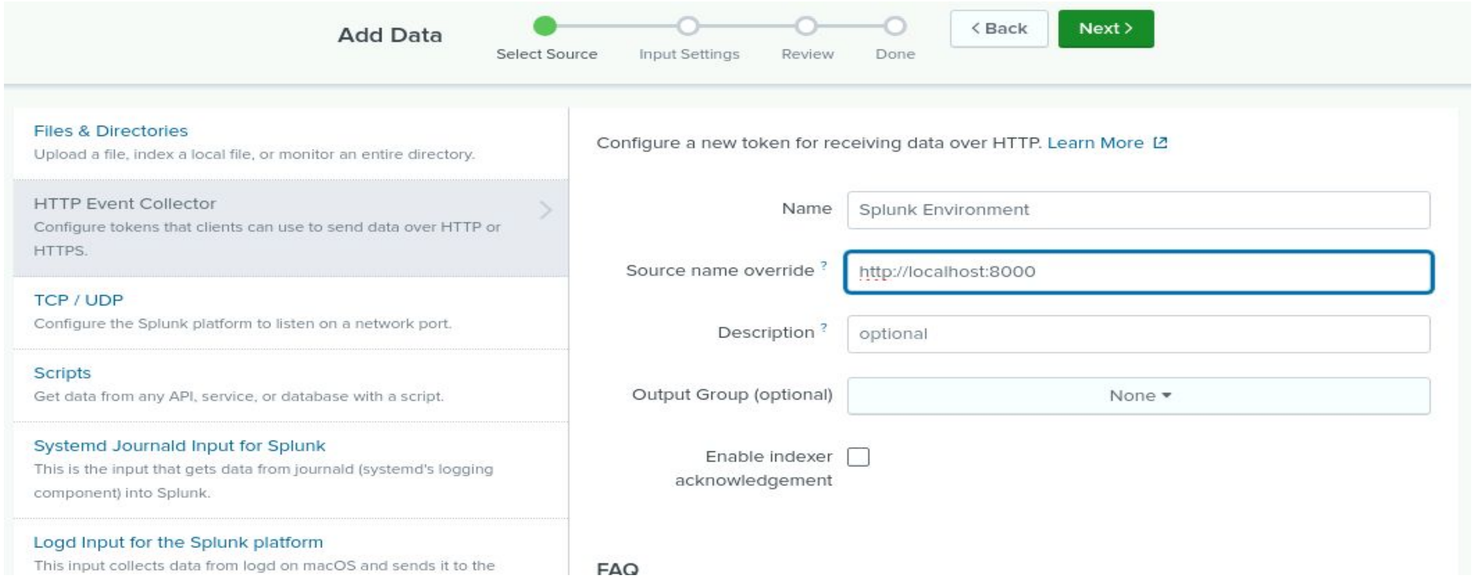


WebSite Monitoring

HEC (HTTP Event Collector)

Enter *Name* to identify Data on Home page at later time. Note the entire URL was entered in *Source Name Override* then hit *Next*

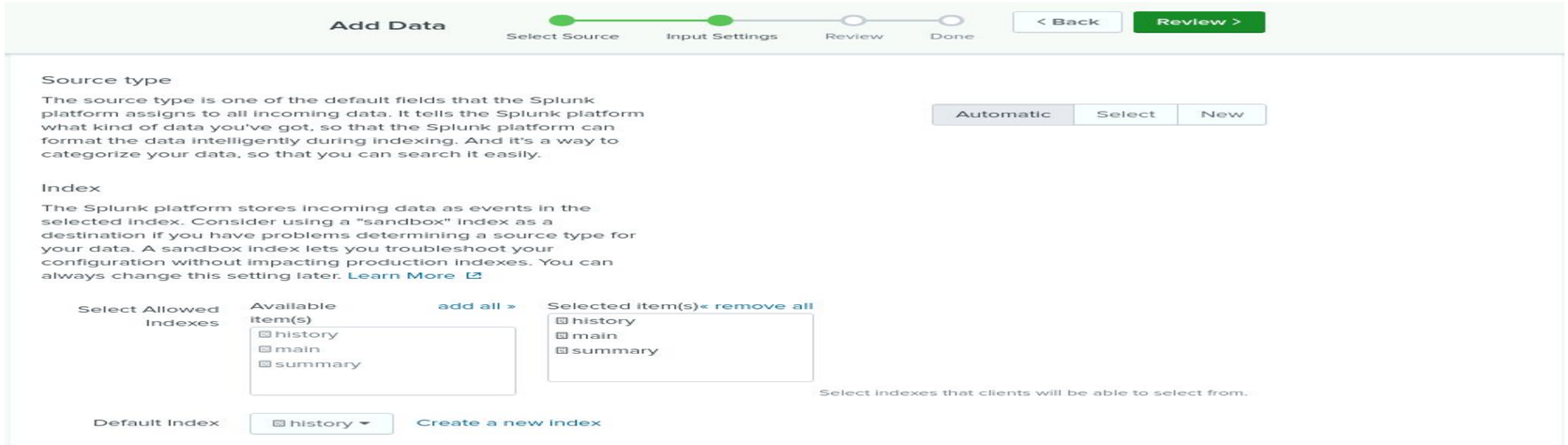
http://localhost:8000/



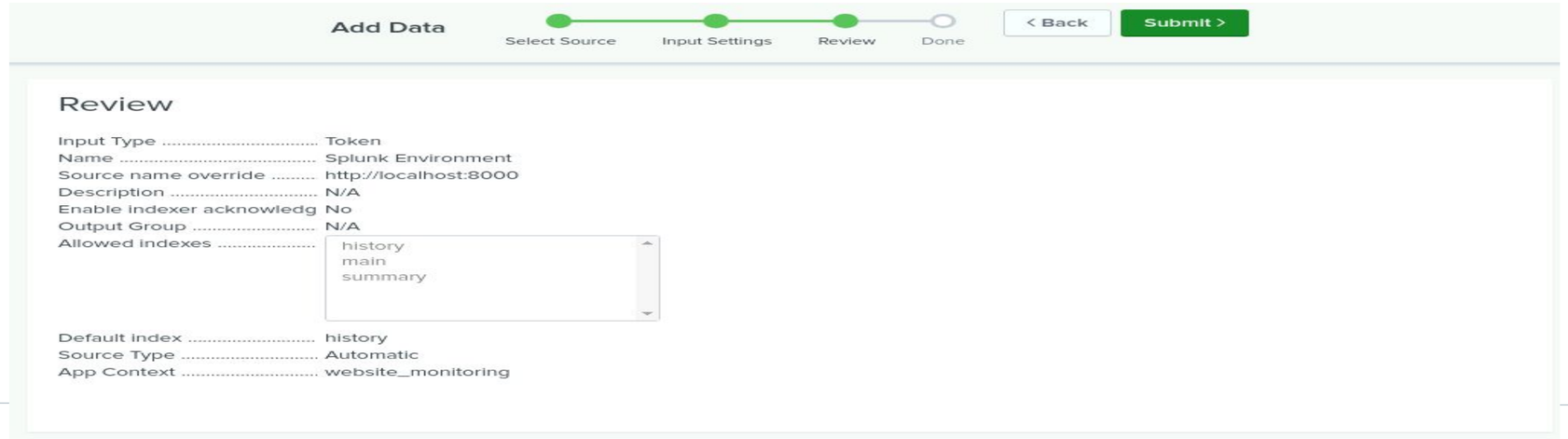
WebSite Monitoring

Review and Add Indexes

You can Add Indexes at bottom left by either clicking on the desired item or clicking *add all>>* then click *Review>*

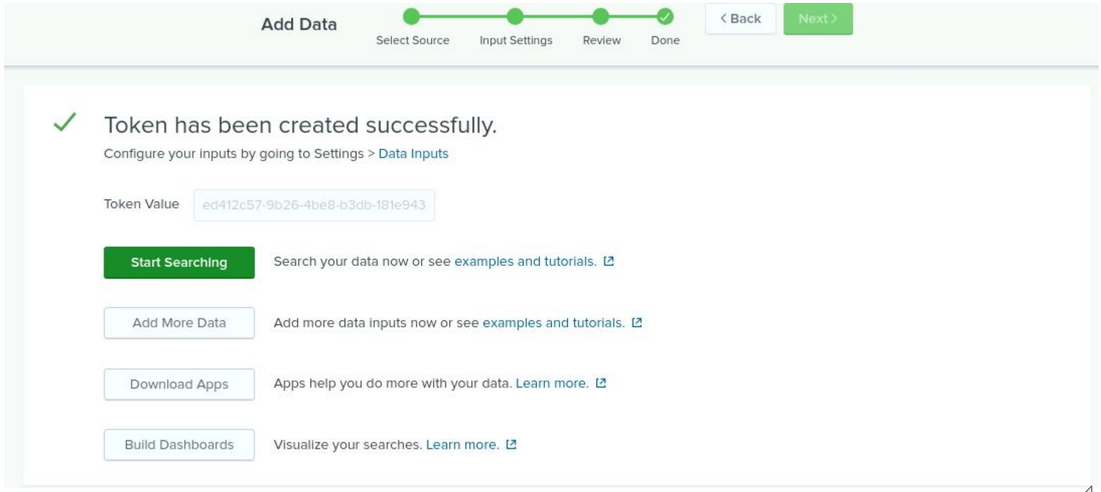


Select *Submit>*



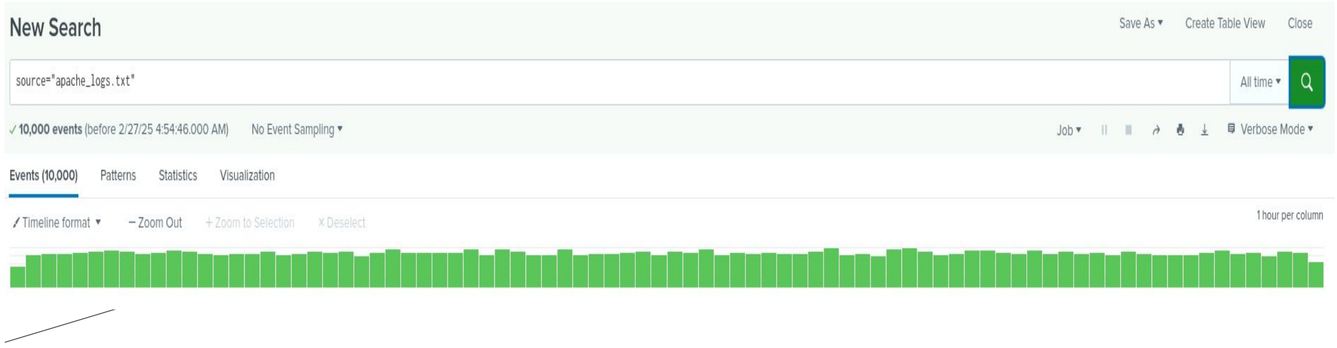
WebSite Monitoring

Token Created! and *Start Searching*



Click

Enter any query as if searching and creating reports in Splunk, then



I encourage you from this point to explore the many options available within this *Website Monitoring Tool.* https://splunkbase.splunk.com/app/1493

Logs Analyzed

1 Windows Logs

The analysis showed that there was a lot going on during the attack, which mig

ht point to security issues.

- There were many serious problems reported.
- There were a lot of failed attempts to use Windows, which set off warnings.
- Fewer people were trying to log in after a certain time.
- One user had strange activity happening early in the morning.
- There was a big jump in password resets and accounts getting locked during two specific times.
- Some unusual online activity was noticed from abroad, especially from Ukraine.
- There was a significant rise in a type of online request called POST requests, which could indicate possible attack methods.

2 Apache Logs

The analysis found important signs that showed there might be security problems during the attack.

- There was a big increase in a specific type of online request called HTTP POST requests.
- More errors were seen when people tried to access pages that didn't exist, while successful access went down.
- There was a lot of foreign online activity, especially from Ukraine, at one point.
- A particular web address received a lot more visitors, which could mean someone was trying to attack it.
- Alerts were set off because of the high number of POST requests, prompting changes to help reduce false alarms.

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Report Analysis for Signatures	Allows VSI to view reports that show the ID number associated with the specific signature for Windows activity.
Report Analysis for Severity	Allows VSI to quickly understand the severity levels of the Windows logs being viewed.
Report Analysis for Failed Activities	Shows VSI if there is a suspicious level of failed activities on their server.

Images of Reports—Windows (Report Analysis for Signatures)

Images of Reports—Windows (Report Analysis for Severity)

Report Analysis for Severity

Edit | More Info | Add to Dashboard

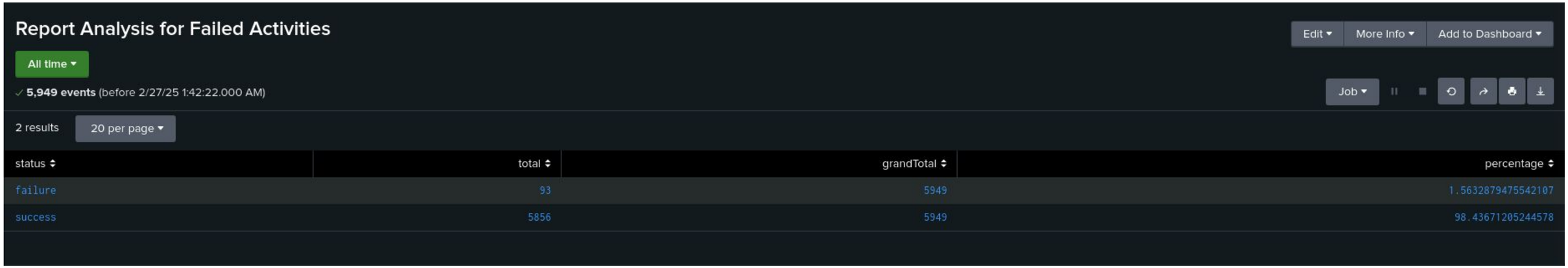
All time

✓ 5,949 events (before 2/27/25 1:40:39.000 AM)

Job

2 results | 20 per page

severity	total	grandTotal	percentage
high	1111	5494	20.22206042955952
informational	4383	5494	79.77793957044048



Report Analysis for Failed Activities

Edit | More Info | Add to Dashboard

All time

✓ 5,949 events (before 2/27/25 1:42:22.000 AM)

Job

2 results | 20 per page

status	total	grandTotal	percentage
failure	93	5949	1.5632879475542107
success	5856	5949	98.43671205244578

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for Failed Windows Activity	An alert that monitors the hourly level of failed Windows activity.	6	15

JUSTIFICATION: The baseline was determined by the average counts per hour which was between 2 and 10 in a 24 hour period. From there we wanted to use 15 because it was high enough to mitigate alert fatigue as well as being low enough to capture an attack.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for Successful Logins	An alert that monitors the hourly count of the signature “an account was successfully logged on.	12	30

JUSTIFICATION: The average amount of successful logins averaged around 12 for the baseline. From there we used the highest amount of counts per hour which was 21 and set a threshold high enough to mitigate triggering alerts for benign metrics.

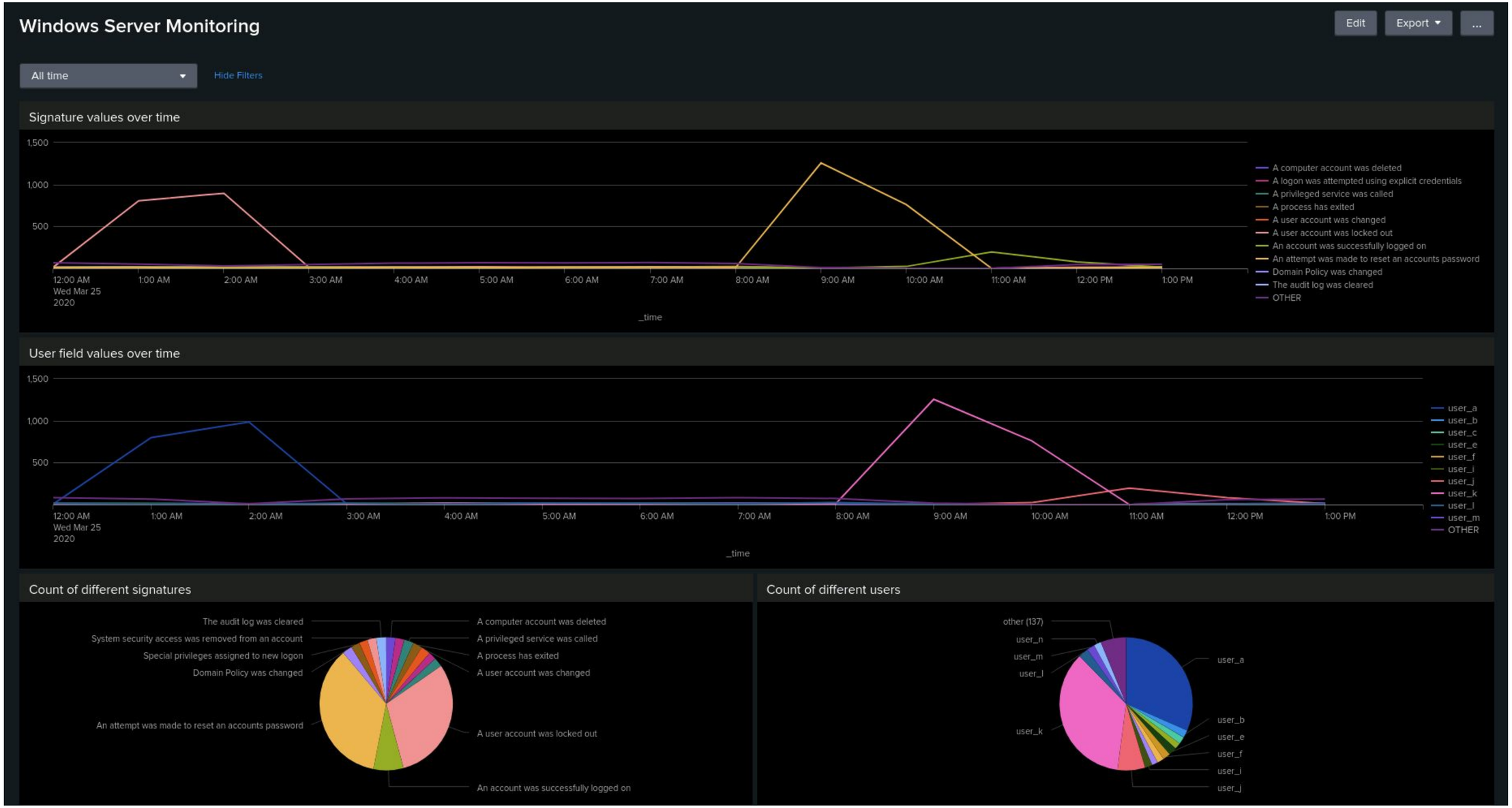
Alerts—Windows

Designed the following alerts:

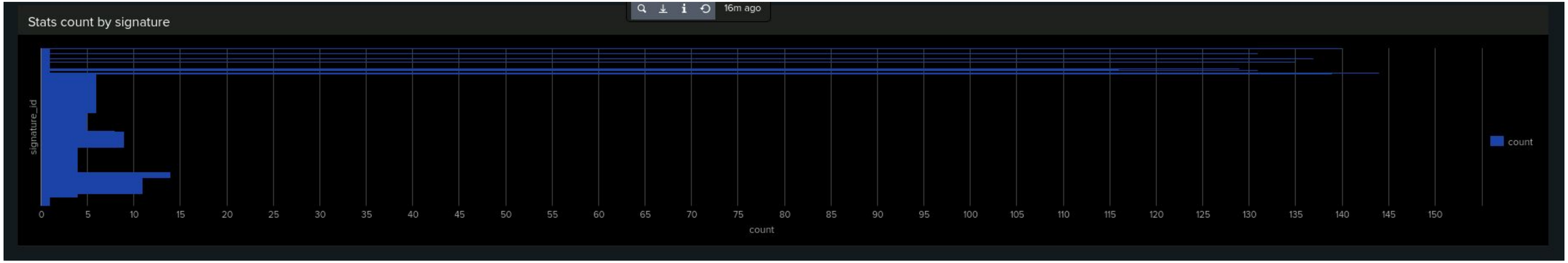
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for Deleted Accounts	An alert that monitors for the hourly count of the signature “a user account was deleted.”	15	30

JUSTIFICATION: A baseline of 15 was determined as the “normal” average for an hour. We then used the highest amount of deleted accounts in 1 hour was 22. From there we set the threshold at 30 to avoid alert fatigue and low enough to capture a real attack.

Dashboards—Windows



Dashboards—Windows (Continued)



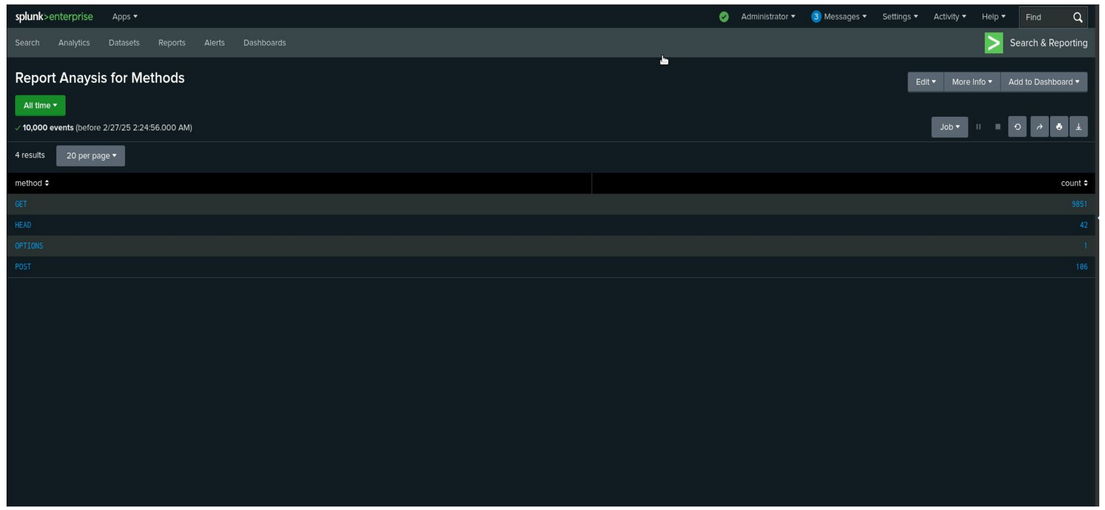
Apache Logs

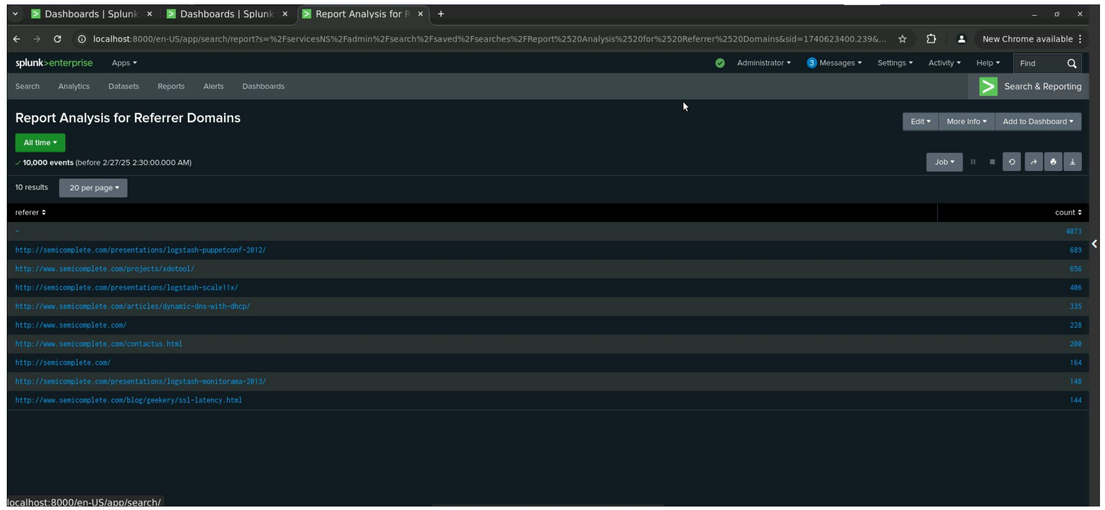
Reports—Apache

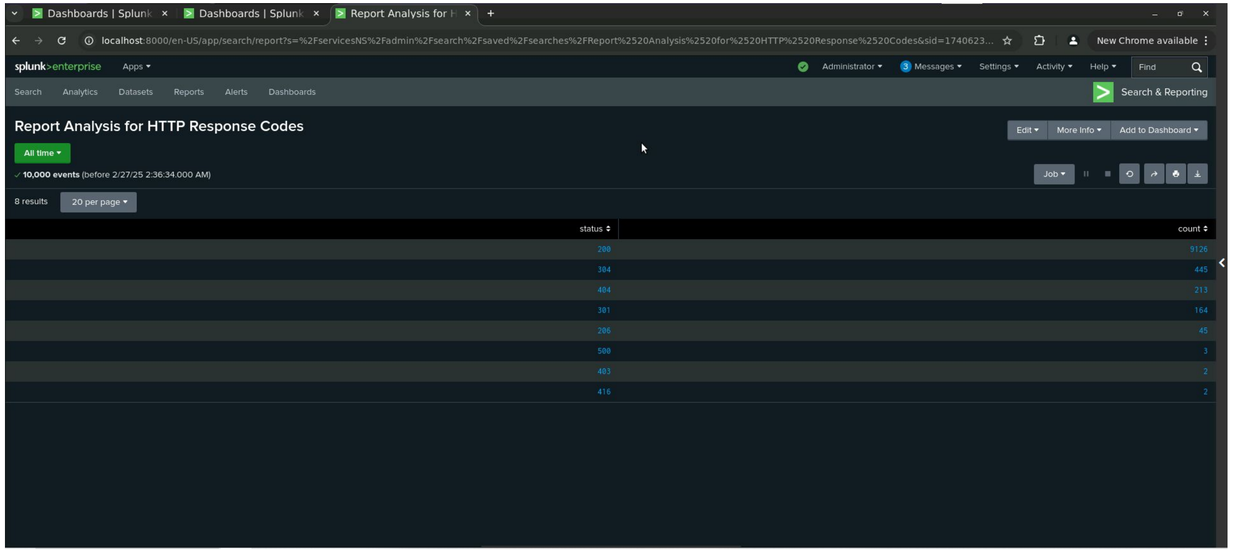
Designed the following reports:

Report Name	Report Description
Report Analysis for Methods	Allows VSI to identify the number of different HTTP methods being requested against VSI's web server.
Report Analysis for Referrer Domains	Assists VSI with identifying suspicious referrers.
Report Analysis for HTTP Response Codes	Provides insight to VSI in identifying any suspicious levels of HTTP responses.

Images of Reports—Apache







Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for International Activity	An alert that monitors the hourly activity from any country besides the United States.	85	180

JUSTIFICATION: The baseline was determined by omitting any outliers and then calculating the average of the levels of activity which was determined to be 85. The threshold was set at 180 to prevent false positives .

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for HTTP POST Activity	An alert that monitors the hourly count of the HTTP POST method	5	10

The baseline was determined by calculating the average of the hourly count of the HTTP POST method being utilized. The alert threshold was set to 10 as the highest count shown throughout regular activity was slightly lower.

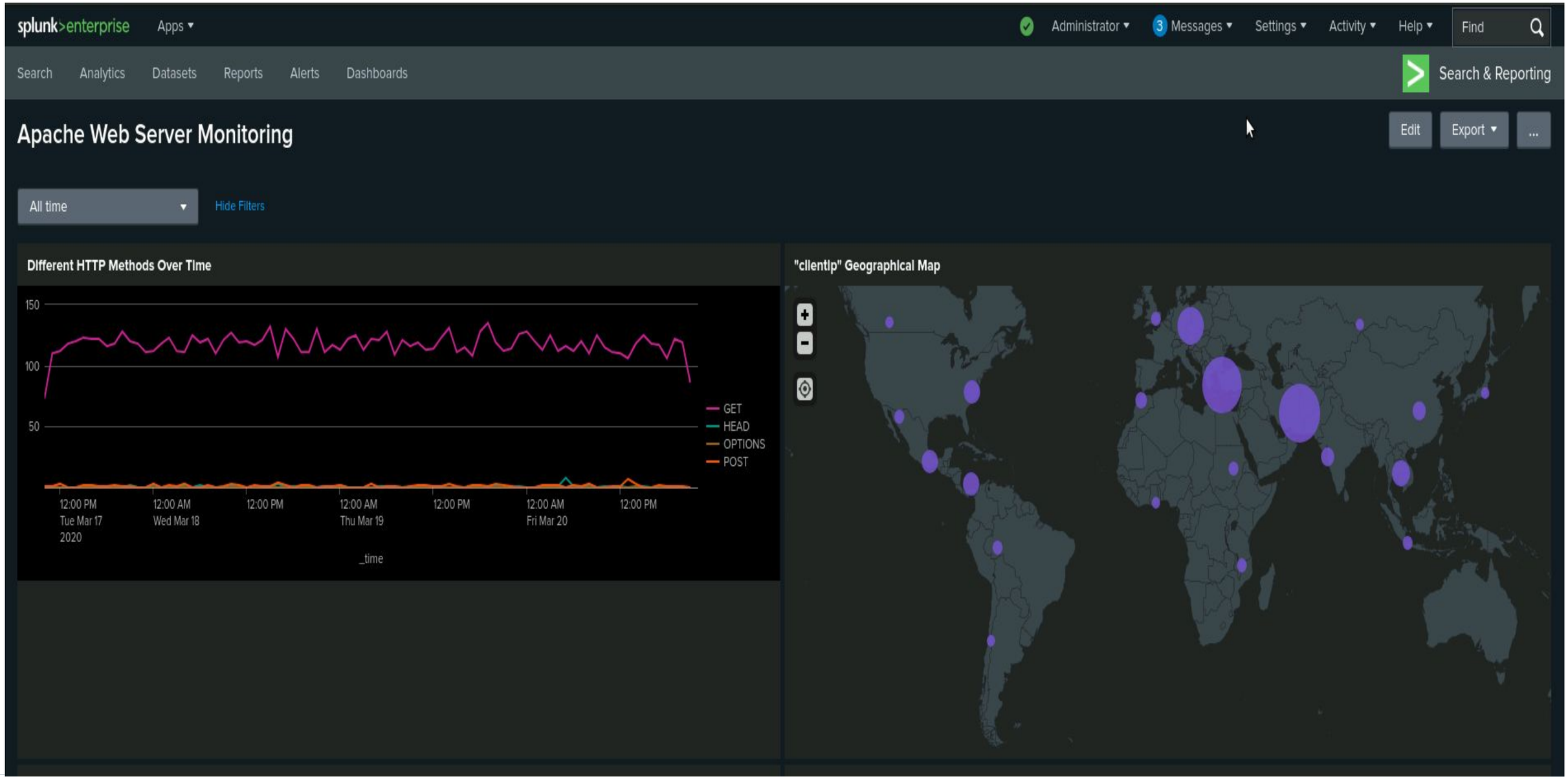
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for Deleted Accounts	An alert that monitors for the hourly count of the signature “a user account was deleted.”	15	30

JUSTIFICATION: A baseline of 15 was determined as the “normal” average for an hour. We then used the highest amount of deleted accounts in 1 hour was 22. From there we set the threshold at 30 to avoid alert fatigue and low enough to capture a real attack.

Dashboards—Apache



Dashboards—Apache (Continued)

Attack Summary—Windows

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

Our alerts successfully identified key anomalies in the attack logs, including failed logins, suspicious user activity, and account related events.

Deleted Accounts: An alert monitors hourly counts of the signature "a user account was deleted." We established a baseline of 15, with a threshold set at 30 to minimize alert fatigue while still detecting real attacks.

Successful Logins: We track the hourly count for "an account was successfully logged on," with a baseline of 12. The threshold is set at 30 to avoid triggering alerts for normal activity, ensuring we focus on significant anomalies. The events dropped significantly, from 16 at 8:00 AM to 0 by 10:00 AM causing for, unfortunately our alert threshold of 30 did not trigger an alert.

Failed Windows Activity: An alert monitors hourly counts of failed Windows activity, with a baseline of 6 and a threshold of 15. This balance helps reduce alert fatigue while still capturing potential security threats.

Threshold Evaluation:

The alert thresholds were set correctly and effectively detected malicious activity without excessive false positives.

Attack Analysis

Attack Summary—Windows

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

Our investigation uncovered clear indicators of suspicious activity, including spikes in failed logins, unusual user behavior, and account-related events. These patterns suggest a coordinated attack attempting to gain access through multiple methods.

Key Findings:

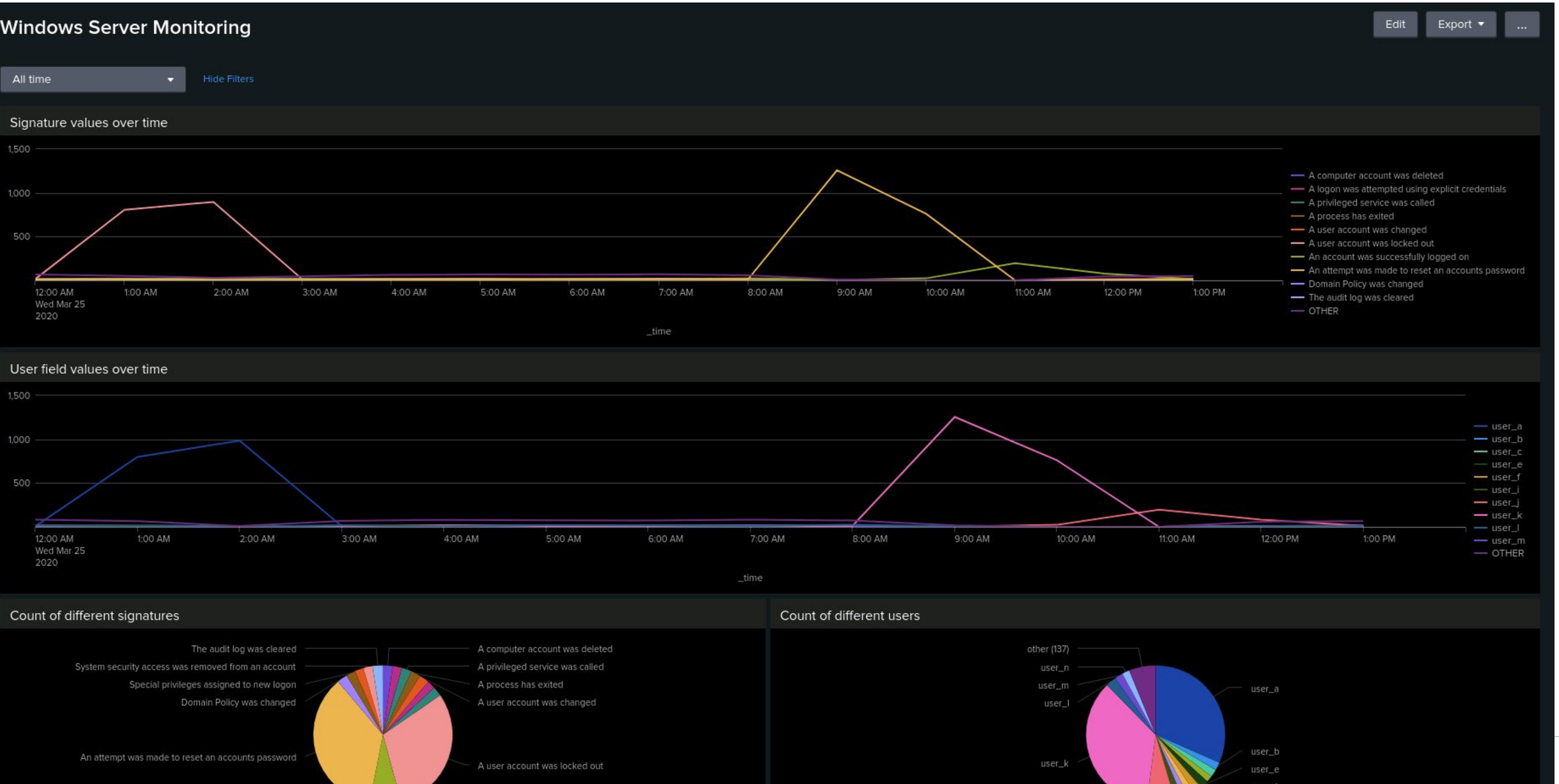
- Severity events increased significantly, rising from 7% to 20% during the attack window.
- Failed Windows logins peaked at 35 at 8:00 AM, exceeding our alert threshold of 15, confirming suspicious login attempts.
- Successful logins dropped unexpectedly, decreasing from 16 at 8:00 AM to 0 by 10:00 AM, indicating a potential disruption in normal access.
- User activity anomalies:
- User_a saw a login spike at 2:00 AM, potentially marking the start of the attack.
- User_k showed heightened activity from 9:00 AM to 10:00 AM, aligning with password reset attempts.
- Unusual account-related events:
- 1:00 – 2:00 AM: 896 instances of “User account locked out.”
- 9:00 – 10:00 AM: 1,258 password reset attempts, suggesting an attempt to regain control of locked accounts.

Attack Summary—Windows

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

All information from dashboards aligned with our reports and verified where our alerts were set. During the attack time frame, severity events increased significantly. Failed login attempts peaked at 35 at 8:00 AM, exceeding the alert threshold. Successful logins dropped from 16 at 8:00 AM to zero by 10:00 AM, indicating disruption in access. User activity anomalies were notable, with User_a logging in at 2:00 AM, likely marking the start of the attack, while User_k exhibited heightened activity from 9:00 AM to 10:00 AM, aligning with password reset attempts. Additionally, there were 896 account lockouts recorded between 1:00 AM and 2:00 AM, along with 1,258 password reset attempts from 9:00 AM to 10:00 AM, suggesting efforts to regain access to locked accounts. This summary underscores critical security events and user behaviors that require further investigation within the Splunk environment.

Screenshots of Windows Attack Logs Dashboard



Attack Summary—Apache

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

The attack logs revealed a significant increase in POST requests, with a spike from 106 to 1,324, suggesting a potential SQL injection or brute-force attack targeting /VSI_Account_logon.php. At 8:00 PM on March 25, 2020, HTTP POST activity peaked at 1,296. There was also an uptick in 404 errors, indicating failed access attempts. International activity, especially from Kiev and Kharkiv in Ukraine, showed a combined total of 877 events, pointing to potential attack origins. Additionally, there was a decrease in 200 OK responses and a rise in 404s. The alert threshold for international activity was triggered, but future adjustments may be necessary to avoid false positives.

Attack Summary—Apache

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

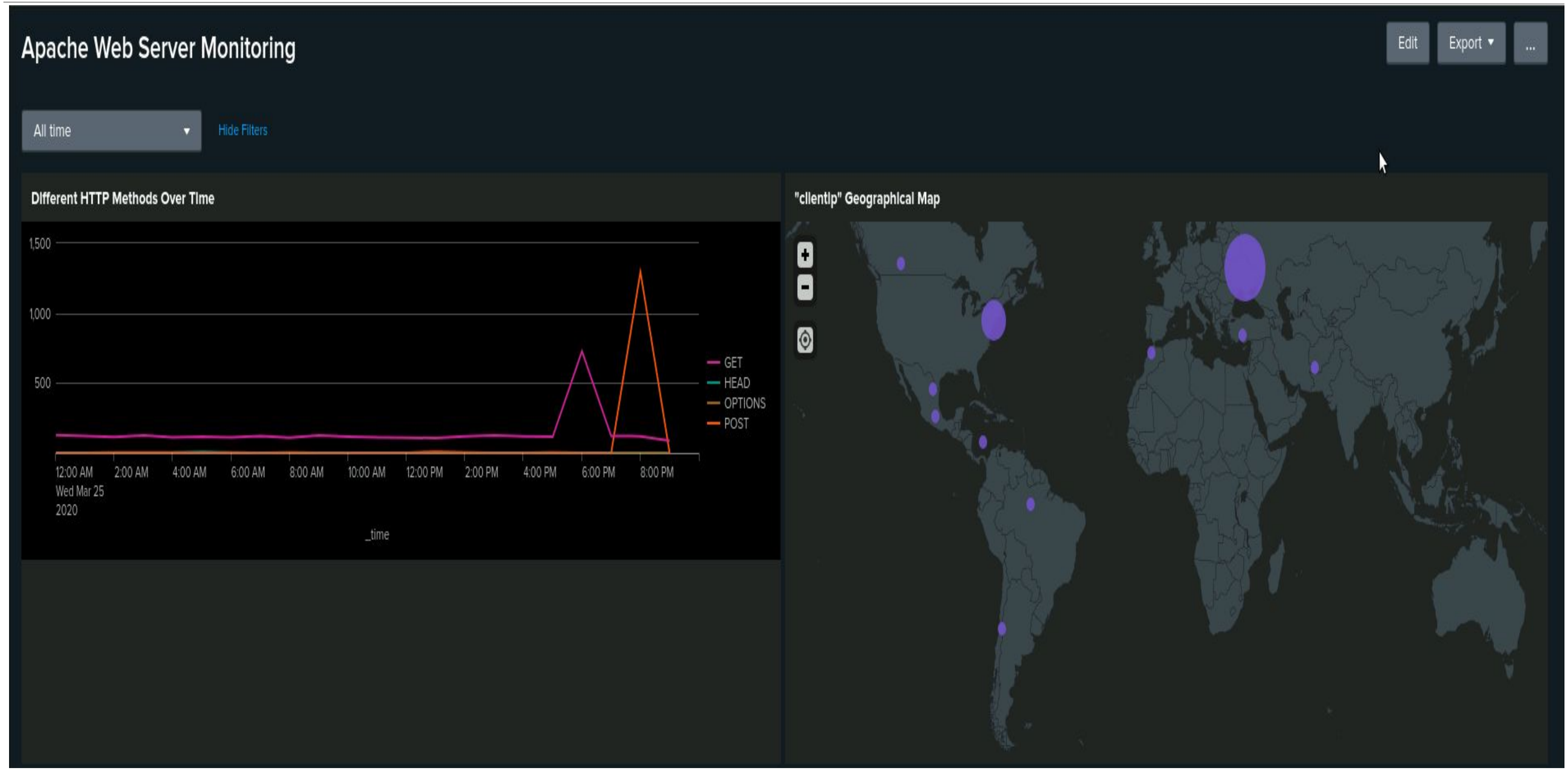
The alerts correctly detected suspicious activity, including 35 failed Windows attempts at 8:00 AM and international activity with 937 events at 8:00 PM. However, the successful login alert didn’t trigger due to a lower threshold. After reviewing, the international activity threshold should be raised to prevent false positives. Overall, the thresholds were mostly accurate but could be fine-tuned.

Attack Summary—Apache

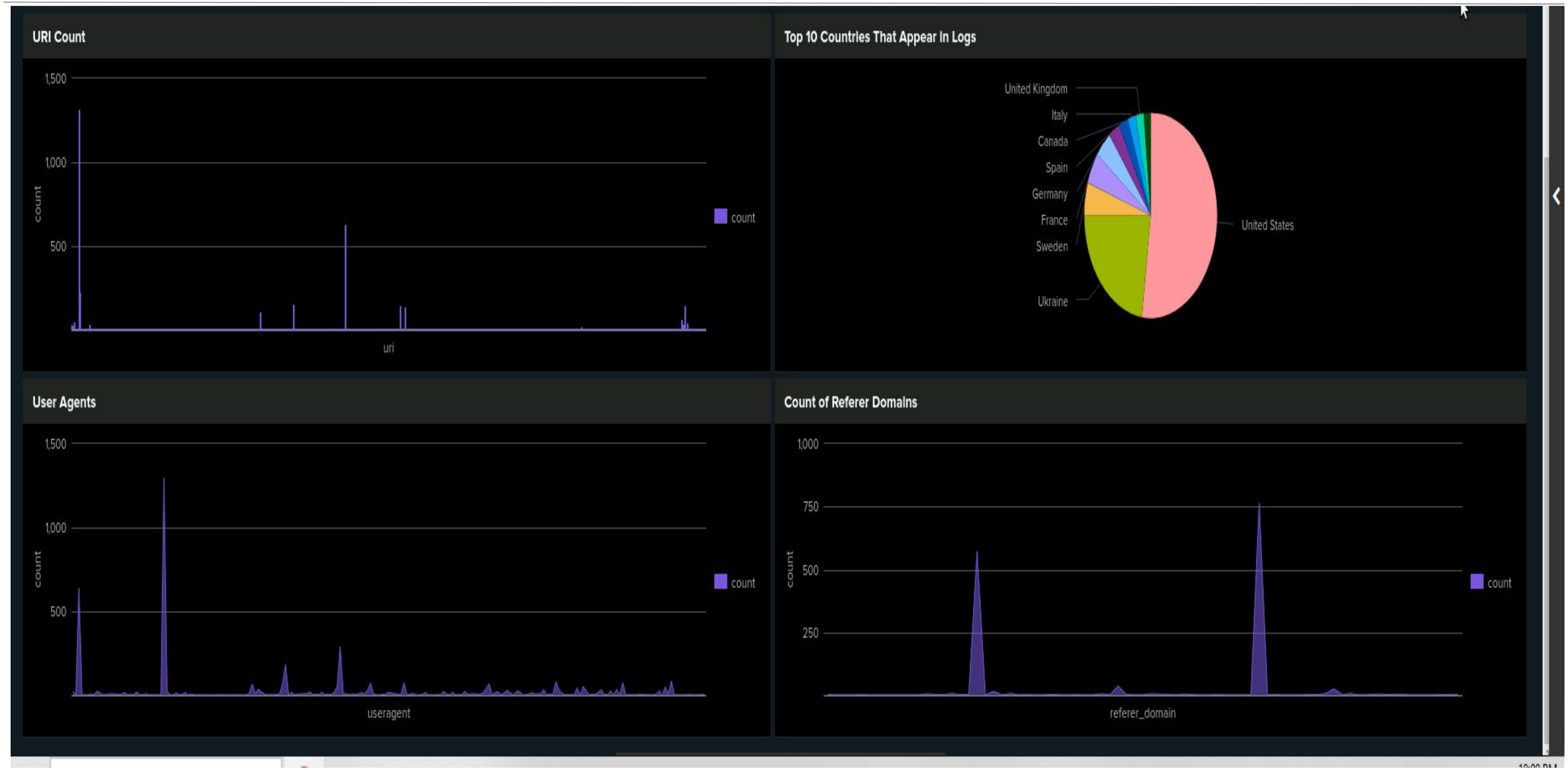
Summarize your findings from your dashboards when analyzing the attack logs.

The dashboards revealed some concerning patterns during the attack. There was a sharp increase in POST requests, particularly targeting the /VSI_Account_logon.php page, which likely indicates an SQL injection or brute-force attack. The activity also spiked in Kiev and Kharkiv, with a total of 877 events coming from Ukraine. At the same time, we saw a rise in 404 errors, meaning there were a lot of failed attempts to access certain pages, while 200 OK responses dropped. The attack seemed to peak around 8:00 PM, with POST activity hitting 1,296. These patterns suggest a focused attack, particularly on login pages, with unusual international traffic and failed access attempts.

Screenshots of Apache Attack Log Dashboard



Screenshots of Apache Attack Log Dashboard



Summary and Future Mitigations

Project 3 Summary

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

The attack showed coordinated intrusion attempts, with spikes in failed logins, account lockouts, and password resets, mainly from user_a, user_k, and Ukraine Kiev, Kharkiv. Apache logs revealed a spike in HTTP POST requests, likely indicating a brute force or SQL injection attack on /VSI_Account_logon.php. A rise in 404 errors suggests probing for vulnerabilities. Strengthening authentication, monitoring, and alert thresholds is key to improving security.

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

To protect VSI from future attacks, I'd recommend setting up multi-factor authentication (MFA), strengthening password policies, and boosting SIEM monitoring to catch any strange activity. You should also consider geo-blocking risky locations and using WAFs to guard against brute-force attacks. Regular security audits and patching will help stay ahead, and adopting a Zero Trust model will reduce the chances of someone moving freely through the network. Finally, giving employees security training will help minimize human errors.