Defensive Security Project

by:

Daniel Mazepa

Carrie Hobbs

George Humphrey

Jaibrien Brooks

Gee Bascomb

Wallace Martin

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

Role:

- Position: SOC Analyst at Virtual Space Industries (VSI).
- Objective: Protect VSI’s systems from potential cyberattacks, specifically from the competitor JobeCorp.

Purpose:

- Monitoring Setup:
  - Systems Monitored: Apache web server (public-facing website) and Windows operating system (backend operations).
  - Tools Used: Splunk for log analysis, report generation, alert creation, and dashboard setup.
- Defensive Measures:
  - Baselining: Establish normal activity levels to identify anomalies.
  - Reports and Alerts: Generate reports and set up alerts to detect suspicious activity in real-time.
  - Dashboards: Create visual dashboards for ongoing monitoring and quick incident response.

Outcome:

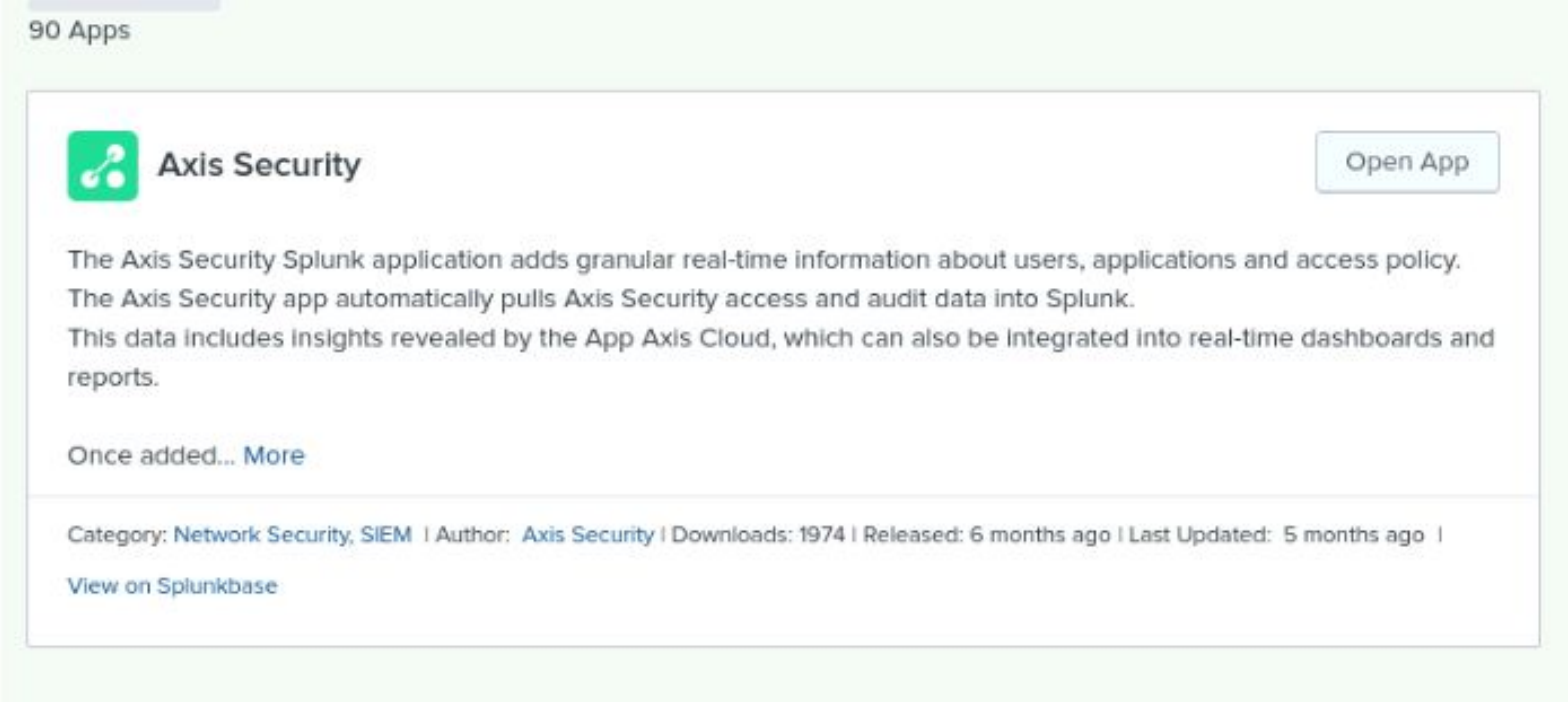
- Initial Setup: Loaded and analyzed historical logs, set baselines, and created monitoring tools.
- Incident Response: Analyzed attack logs, evaluated the effectiveness of monitoring solutions, and provided insights for improvements.
- Presentation: Summarized findings and monitoring effectiveness for senior management.

Conclusion:

- Goal: Ensure the security and integrity of VSI’s critical systems by proactively identifying and responding to cyber threats.

“Add-On” App - Axis Security App for Splunk

Add-On App - Axis Security App for Splunk



90 Apps

Axis Security

The Axis Security Splunk application adds granular real-time information about users, applications and access policy.
The Axis Security app automatically pulls Axis Security access and audit data into Splunk.
This data includes insights revealed by the App Axis Cloud, which can also be integrated into real-time dashboards and reports.

Once added... More

Category: Network Security, SIEM | Author: Axis Security | Downloads: 1974 | Released: 6 months ago | Last Updated: 5 months ago |

View on Splunkbase

Add-On App - Axis Security App for Splunk

Background:

Virtual Space Industries (VSI) operates in a highly competitive industry, relying heavily on secure access to sensitive applications and data. Given the potential cyber threats from competitors like JobeCorp, VSI requires a robust solution to monitor and protect their application access and user activities. The Axis Security app for Splunk is integrated to enhance VSI's security operations.

Implementation:

Using the Axis Security app for Splunk, VSI can collect and analyze granular, real-time information about user activities, application usage, and access policies. This data is critical for creating comprehensive monitoring solutions, including dashboards, reports, and alerts, as well as supporting Zero Trust security principles.

Benefits:

1. Granular Real-Time Information:
   - User Activities and Application Usage: The app provides detailed insights into who is accessing what applications, when, and how often. This allows VSI to monitor user behavior and application usage patterns.
   - Access Policies: Security teams gain visibility into access policies, ensuring they are enforced consistently across the organization.
2. Incident Detection and Investigation:
   - Security Incidents: By integrating with the Axis Security Application Access Cloud, the app helps detect and investigate potential security incidents more effectively. Leveraging Splunk's powerful analytics, VSI can identify security threats and anomalies quickly.
   - Detailed Insights: The app provides detailed insights into potential security threats, allowing for rapid investigation and response.

Add-On App - Axis Security App for Splunk

3. Zero Trust Network Access (ZTNA):
    - Adaptive Access Controls: Supports Zero Trust principles by ensuring that only authenticated and authorized users can access specific applications. Continuous monitoring and adaptive access controls based on user behavior and device posture enhance security.
    - Authenticated and Authorized Access: Ensures that access to applications is granted based on strict authentication and authorization protocols.

4. Integration with CrowdStrike:
    - Endpoint Security: Integration with the CrowdStrike Falcon platform ensures that only secure devices can access sensitive internal resources. This provides an additional layer of protection by enhancing endpoint security.
    - Enhanced Protection: The integration adds another layer of security, ensuring that devices accessing VSI's resources are secure.

5. Ease of Deployment:
    - Business Logic Cloud Overlay: The app operates as a business logic cloud overlay at the application layer, simplifying the process of securing access to applications without requiring significant changes to the network infrastructure.
    - Simplified Security: Easy deployment and operation make it a practical solution for enhancing security without disrupting existing infrastructure.

Conclusion:
By implementing the Axis Security app for Splunk, VSI can significantly enhance its security operations. The app provides detailed visibility into user activities and application usage, improves incident response capabilities, and supports a Zero Trust security model. This ensures that VSI's critical assets are protected against potential threats posed by JobeCorp or other malicious actors, maintaining the security and integrity of its operations.

Logs Analyzed

1 Windows Logs

The data contained in these logs include:

- Signature_ID
- Signature
- User
- Status
- Severity

2 Apache Logs

The data contained in these logs include:

- Method
- Referer_domain
- Status
- Clientip
- Useragent

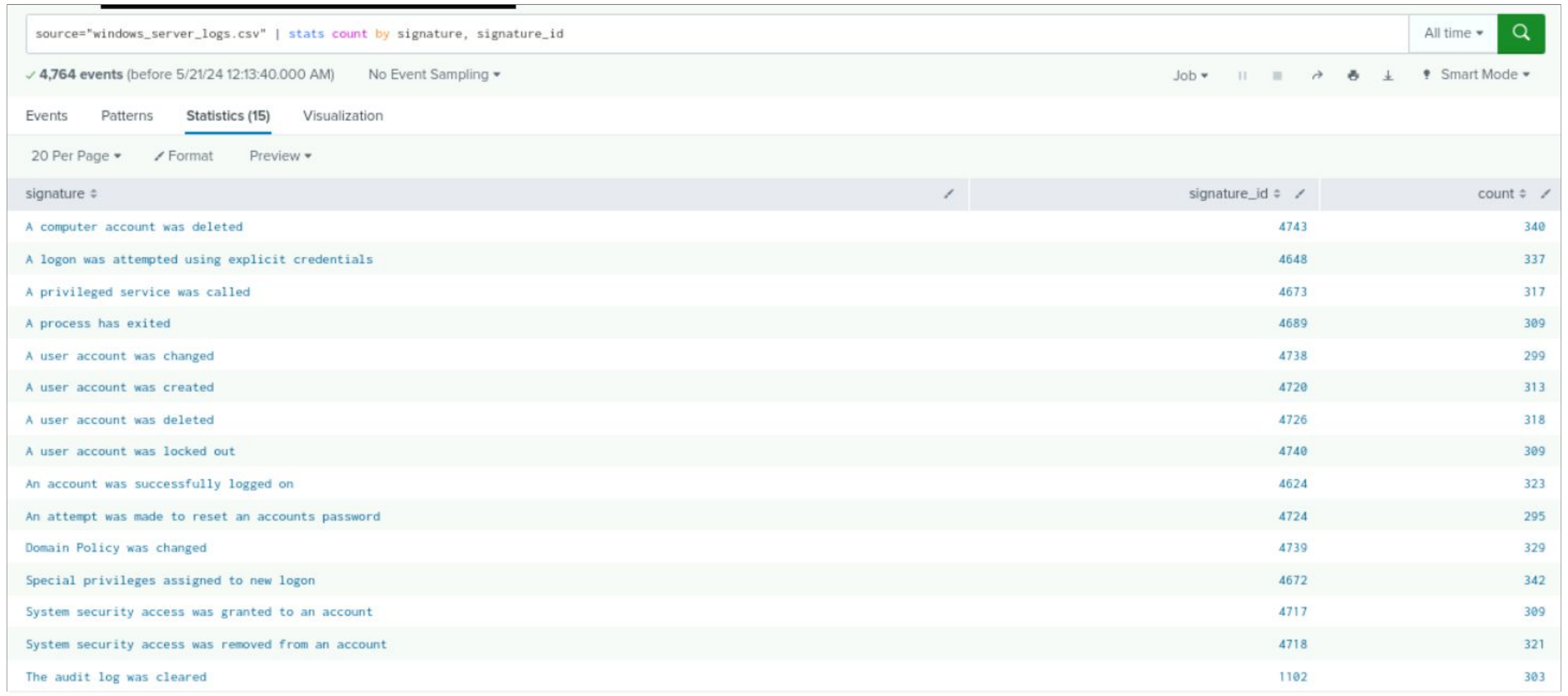
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	**Report Description**
Report_2A_Signatures	Count of activities by signature and signature ID
Report_2B_Severity	Count and percentage of activities by severity
Report_2C_Status	Count and percentage of activities by status (success or failure)

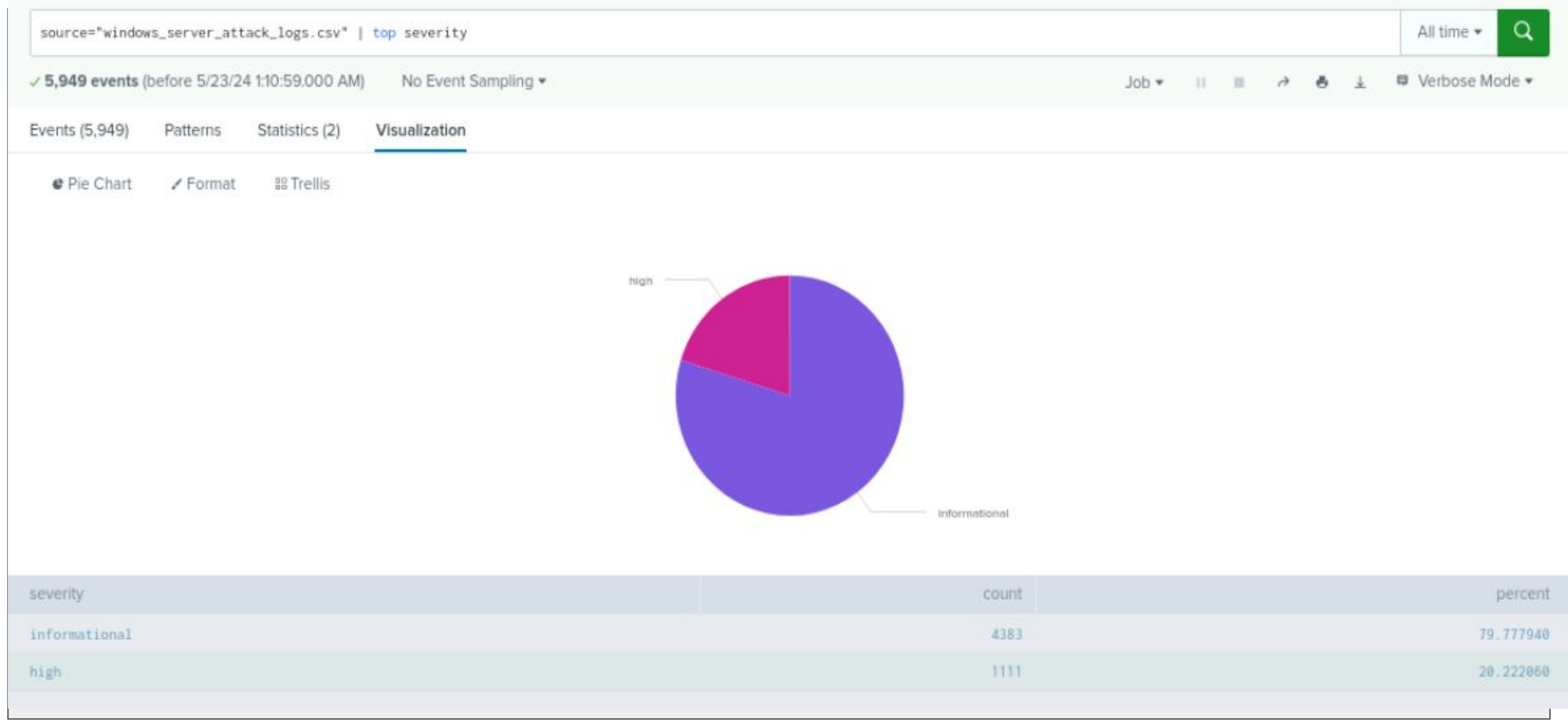
Images of Reports—Windows



```
source="windows_server_logs.csv" | stats count by signature, signature_id
```

✓ **4,764 events** (before 5/21/24 12:13:40.000 AM) No Event Sampling

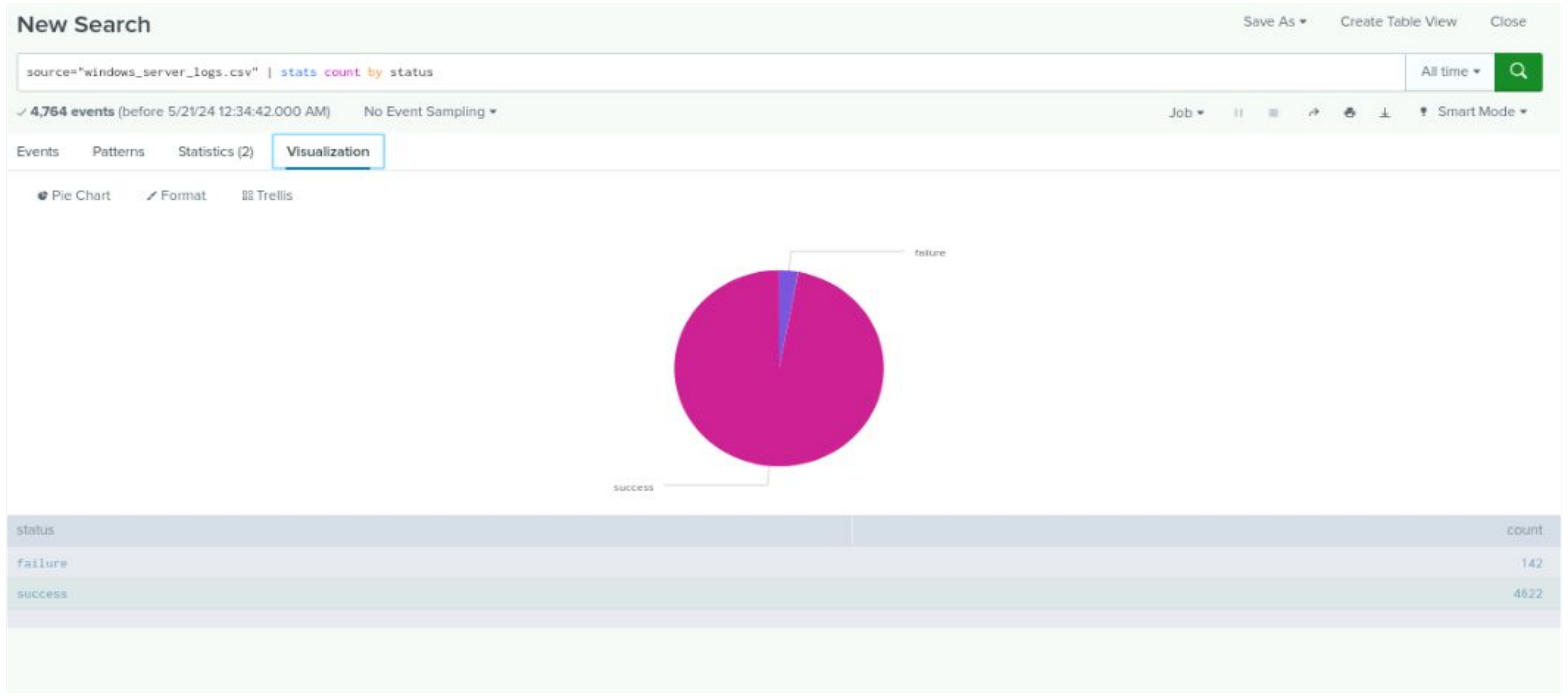
signature	signature_id	count
A computer account was deleted	4743	340
A logon was attempted using explicit credentials	4648	337
A privileged service was called	4673	317
A process has exited	4689	309
A user account was changed	4738	299
A user account was created	4720	313
A user account was deleted	4726	318
A user account was locked out	4740	309
An account was successfully logged on	4624	323
An attempt was made to reset an accounts password	4724	295
Domain Policy was changed	4739	329
Special privileges assigned to new logon	4672	342
System security access was granted to an account	4717	309
System security access was removed from an account	4718	321
The audit log was cleared	1102	303



```
source="windows_server_attack_logs.csv" | top severity
```

✓ **5,949 events** (before 5/23/24 1:10:59.000 AM) No Event Sampling

severity	count	percent
informational	4383	79.777940
high	1111	20.222060



```
source="windows_server_logs.csv" | stats count by status
```

✓ **4,764 events** (before 5/21/24 12:34:42.000 AM) No Event Sampling

status	count
failure	142
success	4622

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert_2A_Hourly_ Failures	Hourly level of failed activity	5	11

JUSTIFICATION: The hourly number of failures observed during normal activities ranged from 2 to 10 with a median of 5, which we chose as our baseline.

The maximum observed during normal activity was 10, so we chose 11 as our threshold.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert_2B_Successful_Logins	Hourly level of successful logins	13	22

JUSTIFICATION: The hourly number of failures observed during normal activities ranged from 8 to 21, with a median of 13, which we chose as our baseline.

The maximum observed during normal activity was 21, so we chose 22 as our threshold.

Alerts—Windows

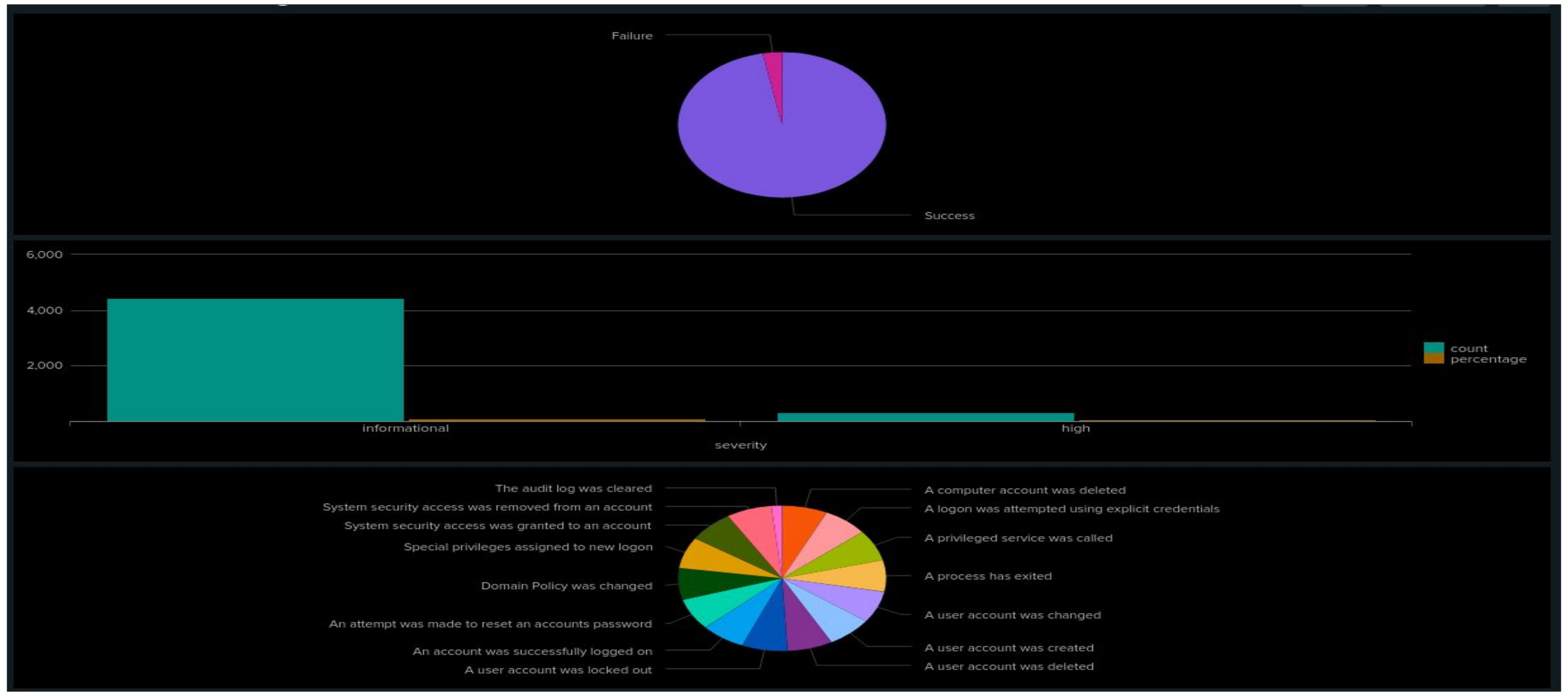
Designed the following alerts:

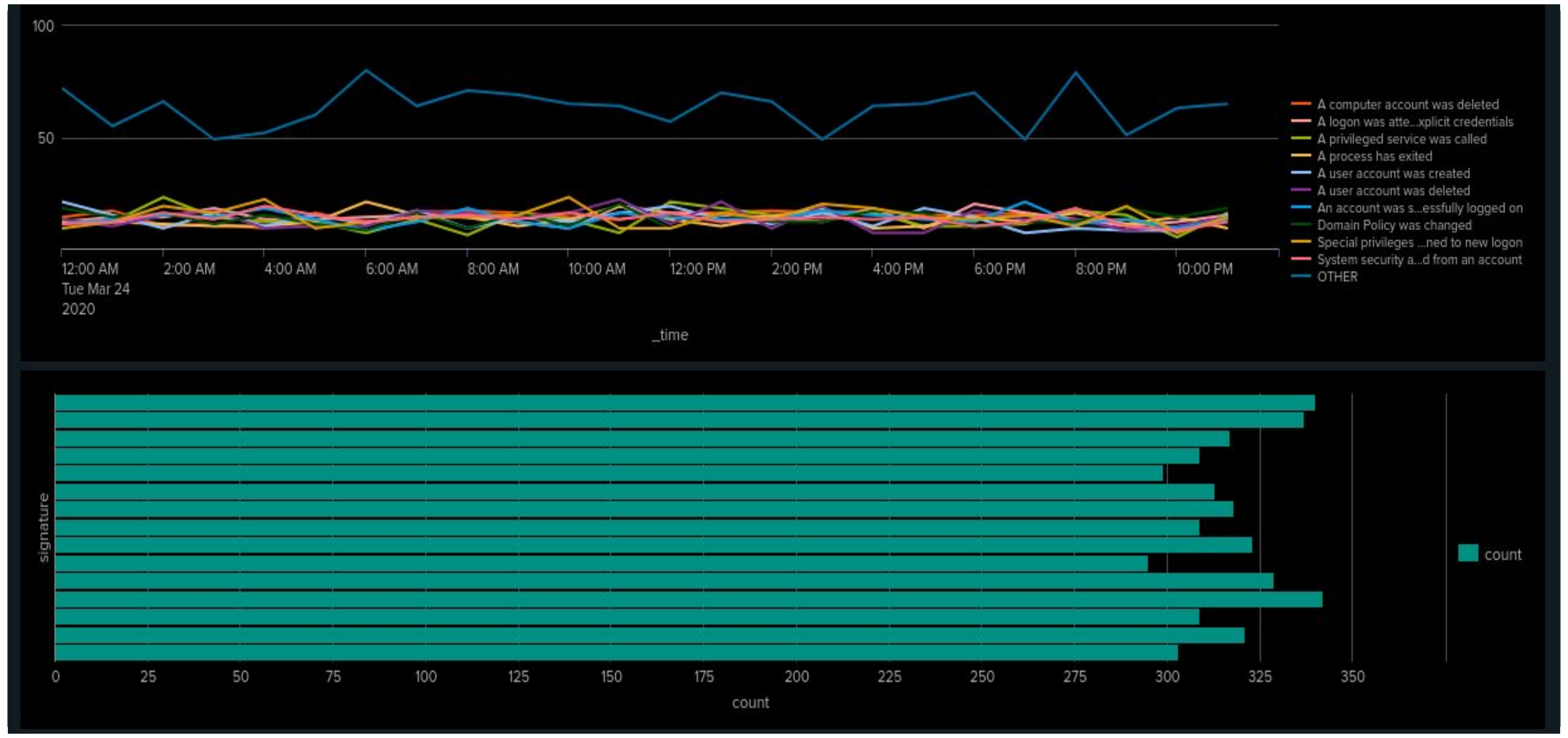
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert_2C_Account_ Deleted	Hourly level of account deletions	13	23

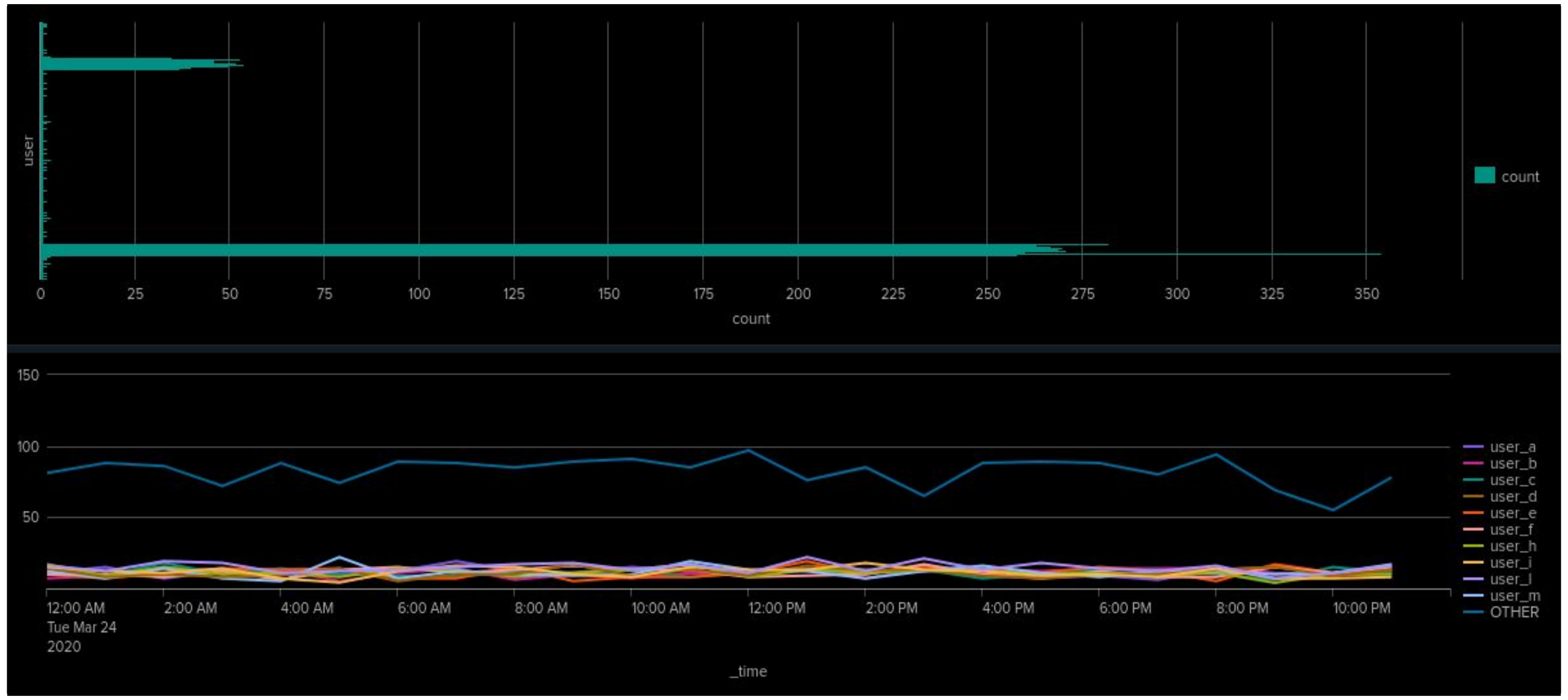
JUSTIFICATION: The hourly number of account deletions observed during normal activities ranged from 7 to 22, with a median of 13, which we chose as our baseline.

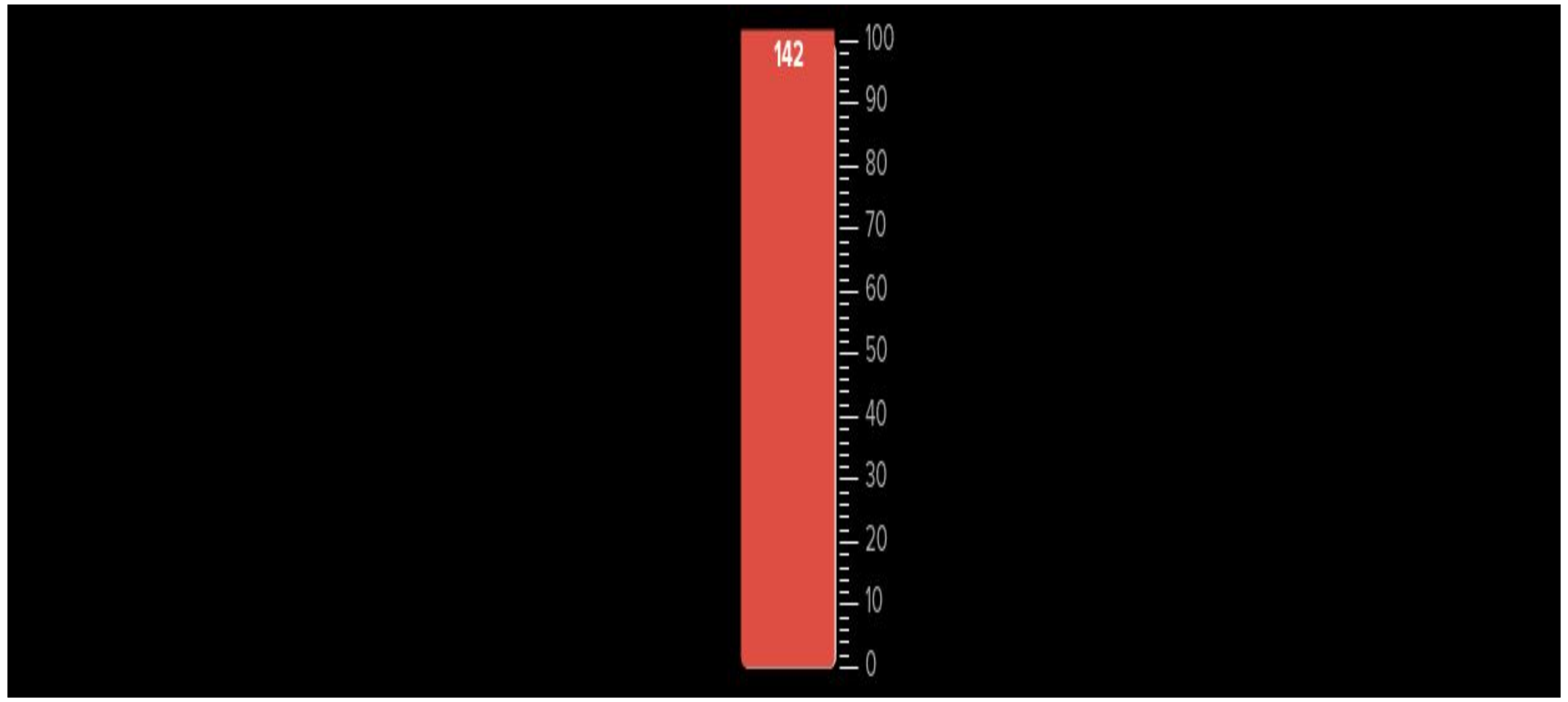
The maximum observed during normal activity was 22, so we chose 23 as our threshold.

Dashboards—Windows


Failure
Success
6,000
4,000
2,000
informational
high
severity
count
percentage
The audit log was cleared
System security access was removed from an account
System security access was granted to an account
Special privileges assigned to new logon
Domain Policy was changed
An attempt was made to reset an accounts password
An account was successfully logged on
A user account was locked out
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was changed
A user account was created
A user account was deleted


100
50
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_time
A computer account was deleted
A logon was atte...xplicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was s...essfully logged on
Domain Policy was changed
Special privileges ...ned to new logon
System security a...d from an account
OTHER
signature
0
25
50
75
100
125
150
175
200
225
250
275
300
325
350
count
count





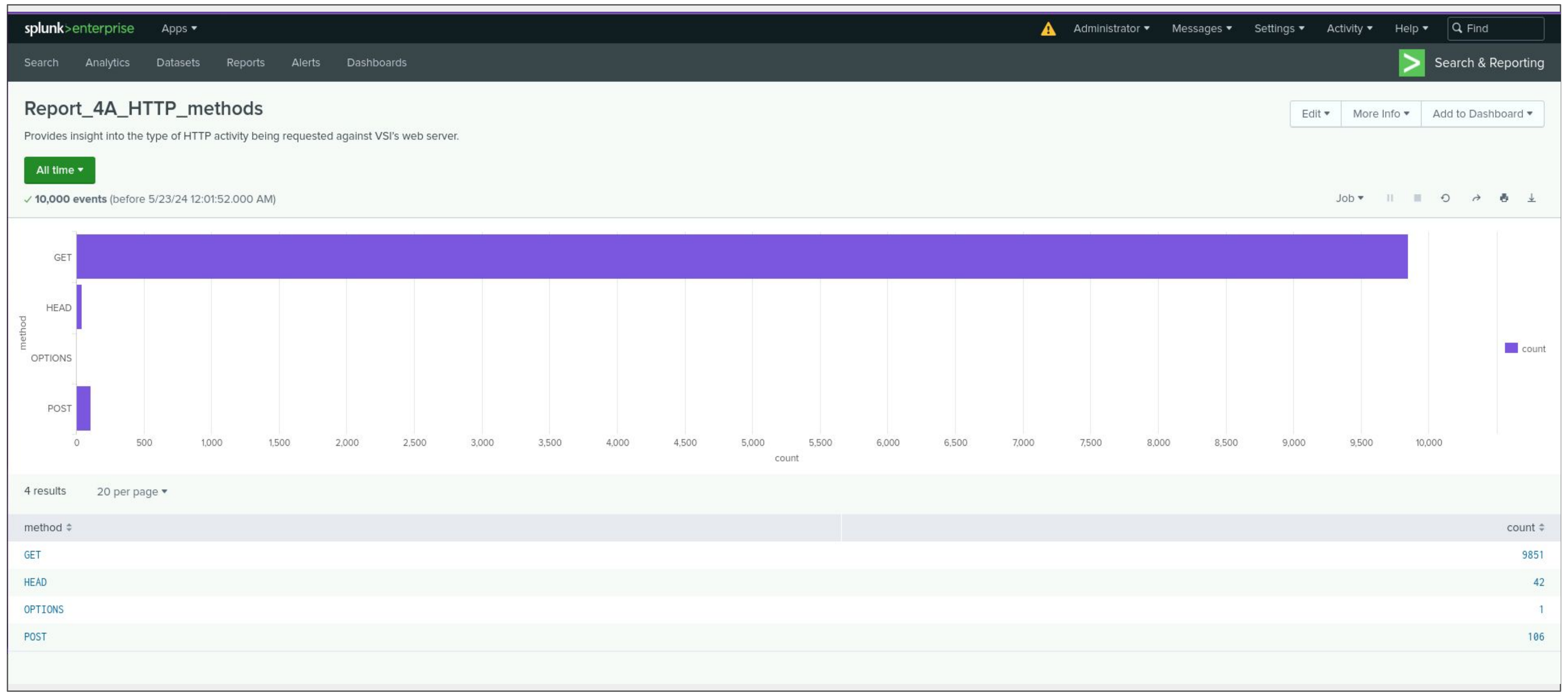
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	**Report Description**
Report_4A_HTTP_Methods	Type of HTTP activity being requested
Report_4B_Top10_Refer_Domains	Top 10 domains that refer to VSI’s website
Report_4C_HTTP_Response_Count	Count of each HTTP response code

Images of Reports—Apache



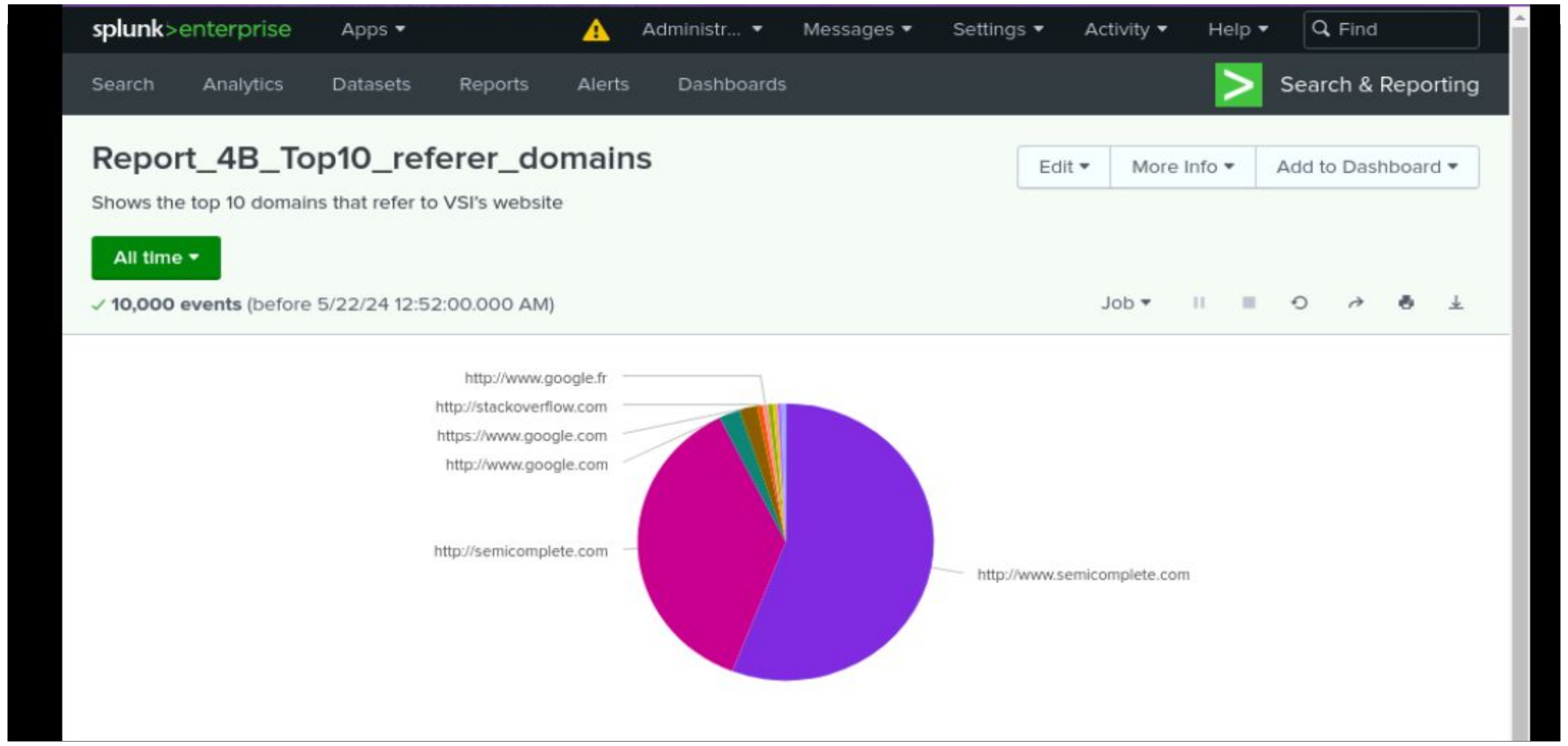
Report_4A_HTTP_methods

Provides insight into the type of HTTP activity being requested against VSI's web server.

✓ **10,000 events** (before 5/23/24 12:01:52.000 AM)

4 results   20 per page ▾

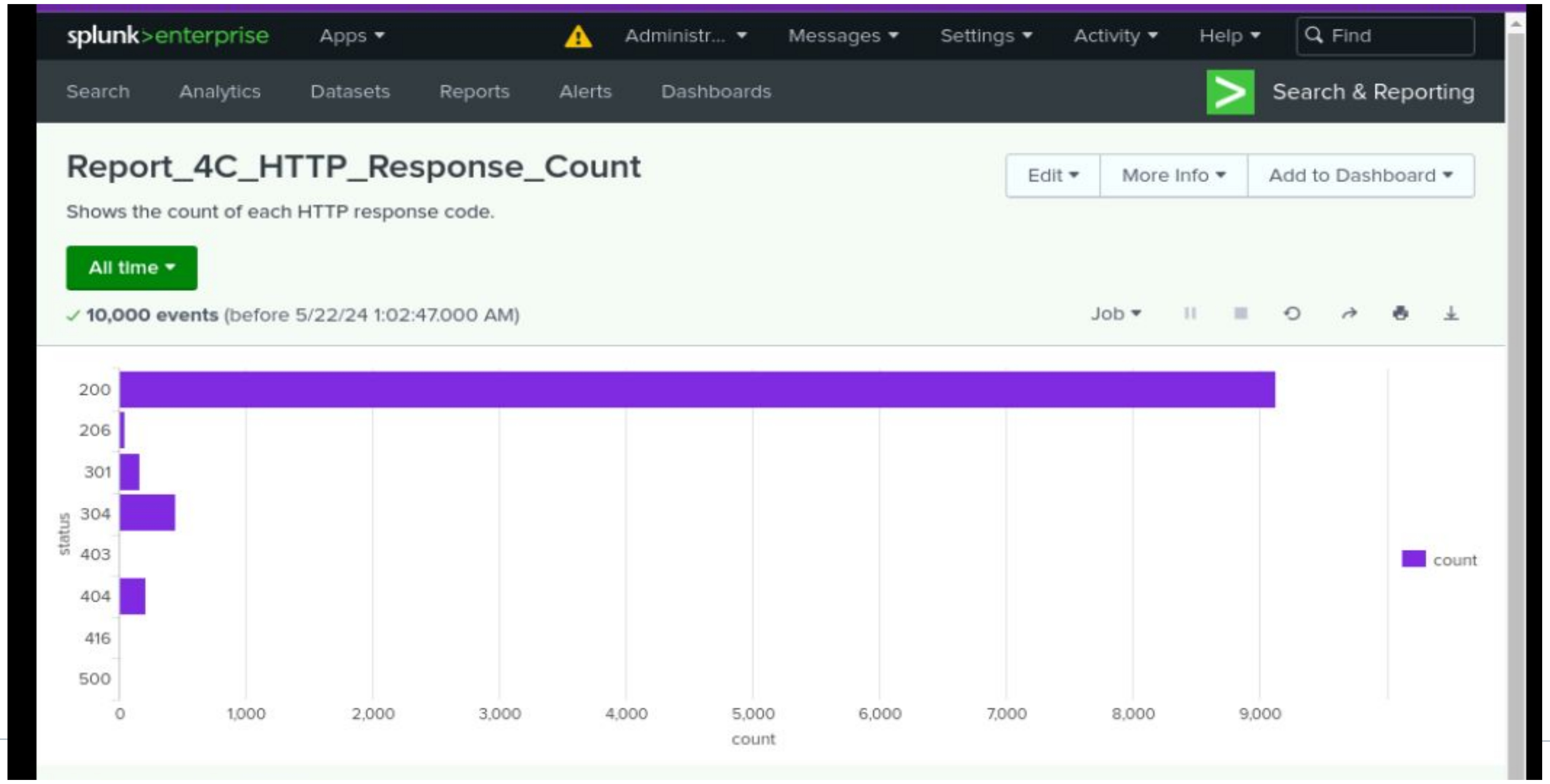
method ⇕	count ⇕
GET	9851
HEAD	42
OPTIONS	1
POST	106



Report_4B_Top10_referer_domains

Shows the top 10 domains that refer to VSI's website

✓ **10,000 events** (before 5/22/24 12:52:00.000 AM)



Report_4C_HTTP_Response_Count

Shows the count of each HTTP response code.

✓ **10,000 events** (before 5/22/24 1:02:47.000 AM)

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
China Activity by Hour Alert	Hourly activity from IP addresses located in China.	35	>40

JUSTIFICATION: The apache_logs used to establish a baseline indicated an hourly activity rate of as low as 1 event per hour and as high as 37. We had no knowledge of past suspicious activity levels, so a threshold was established to avoid false positives.

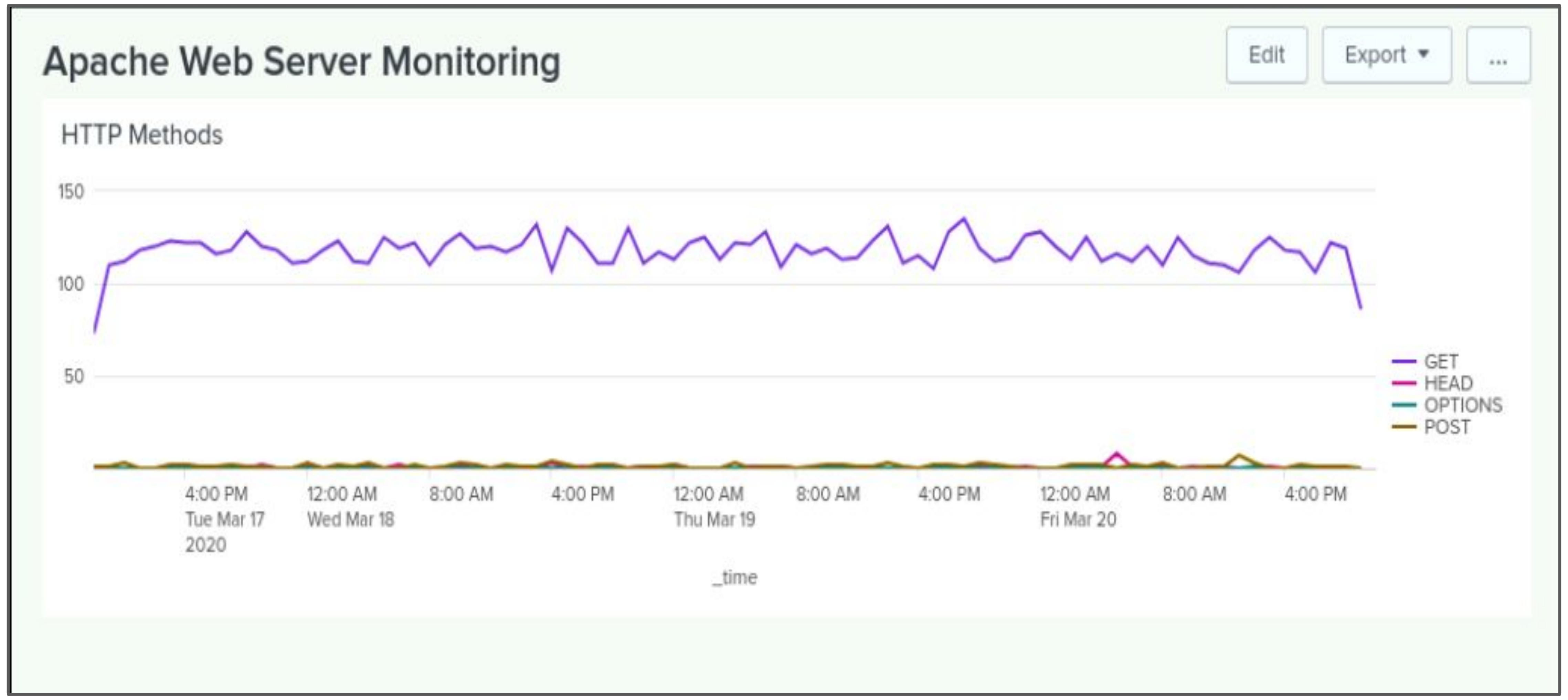
Alerts—Apache

Designed the following alerts:

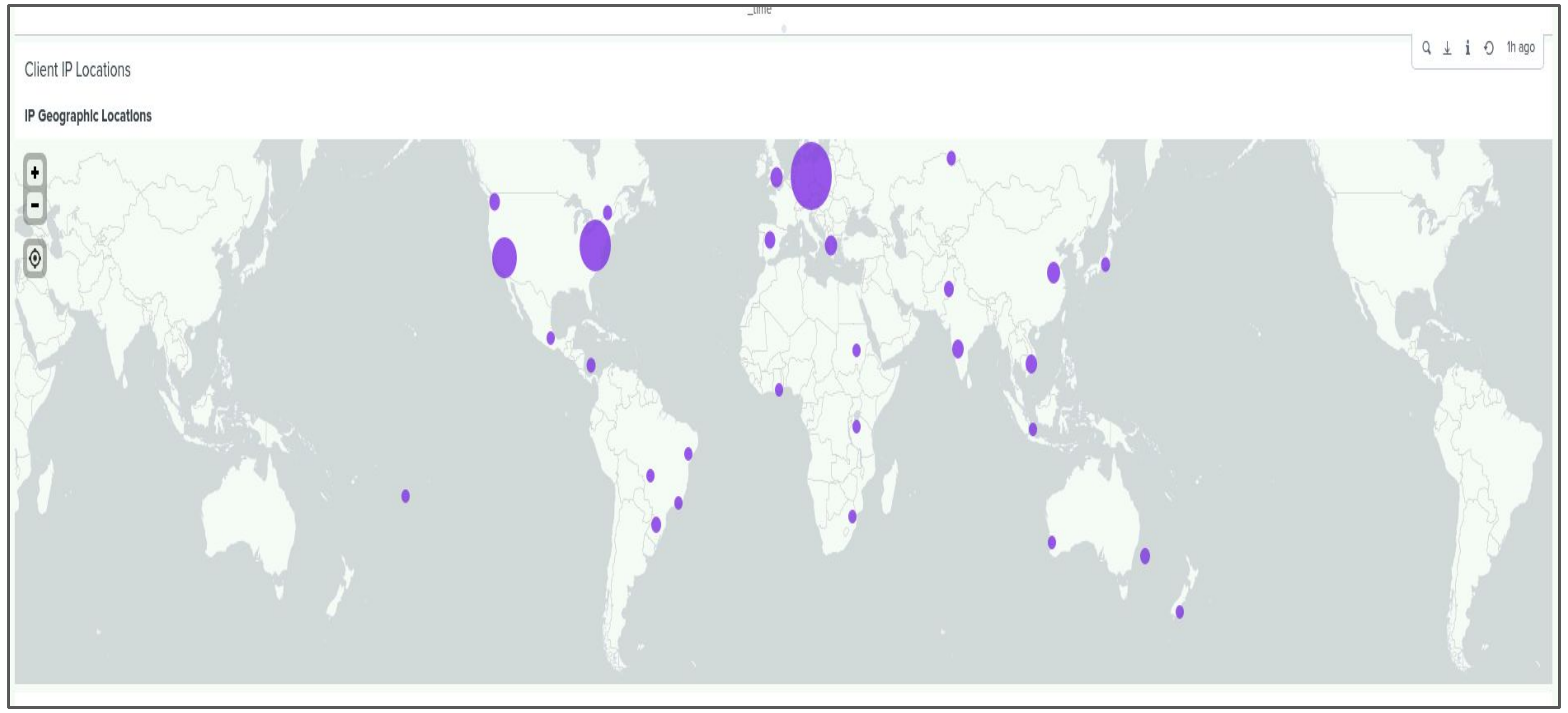
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Count	Hourly Count of the HTTP POST Method.	2	9

JUSTIFICATION: 2 seemed to be a good baseline for the apache_logs since most of the events did not deviate too far from that amount. A threshold of 9 was put in place since that’s uncommon territory for events per hour. During the initial search, the highest amount of events per hour was 7.

Dashboards—Apache

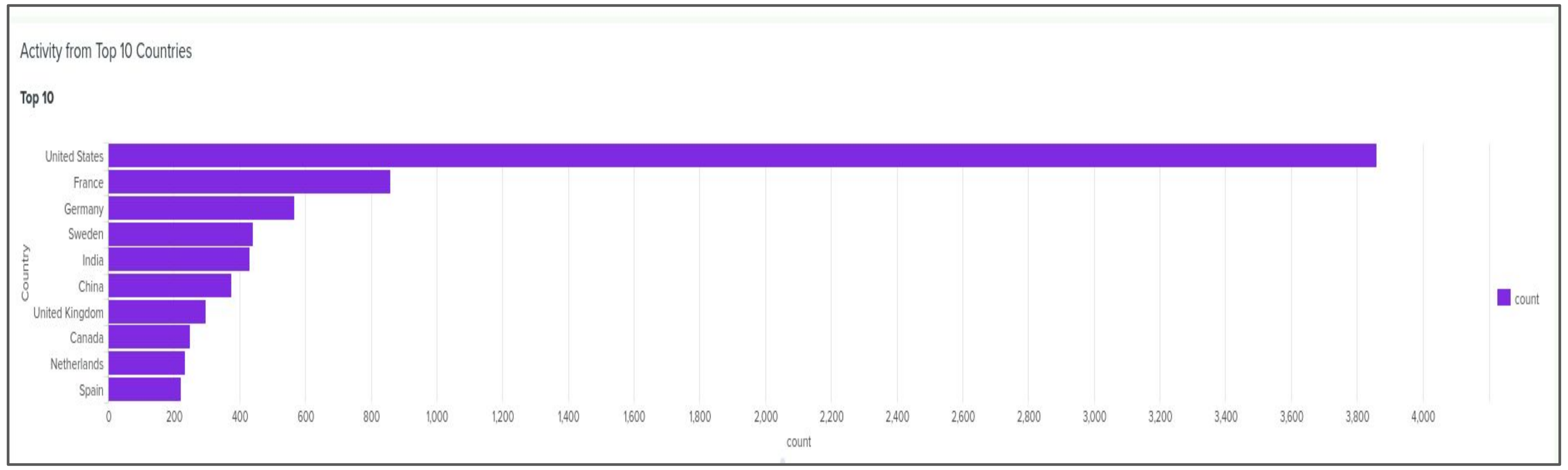


Apache Web Server Monitoring



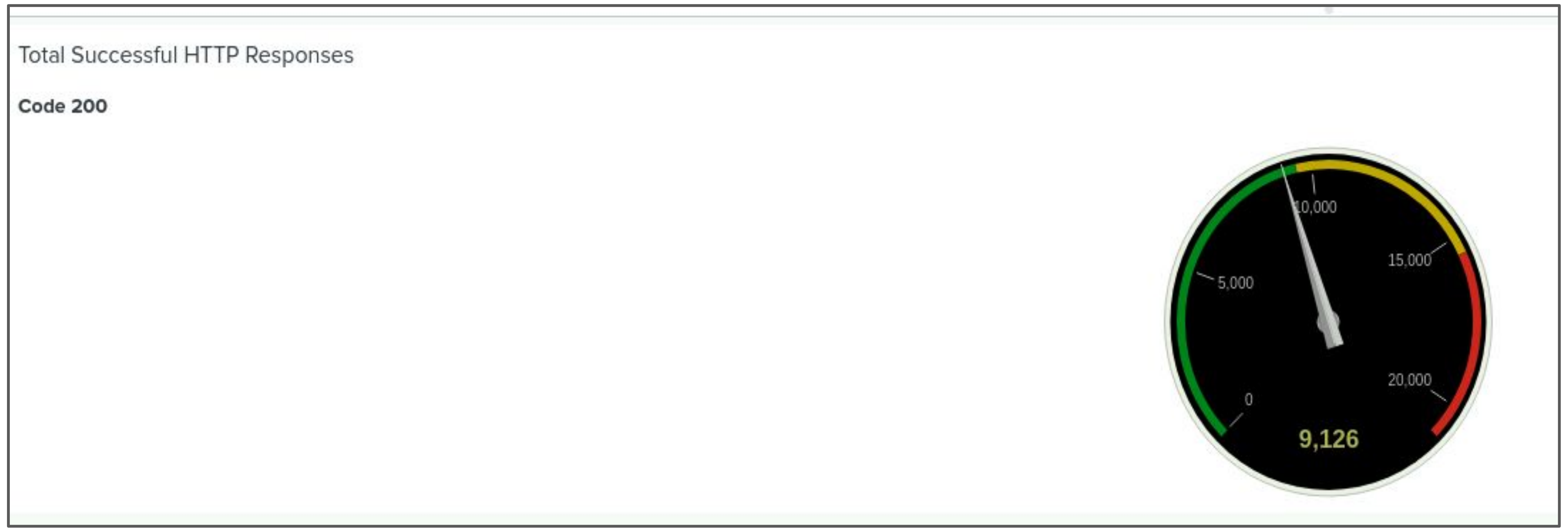
Client IP Locations

IP Geographic Locations



Activity from Top 10 Countries

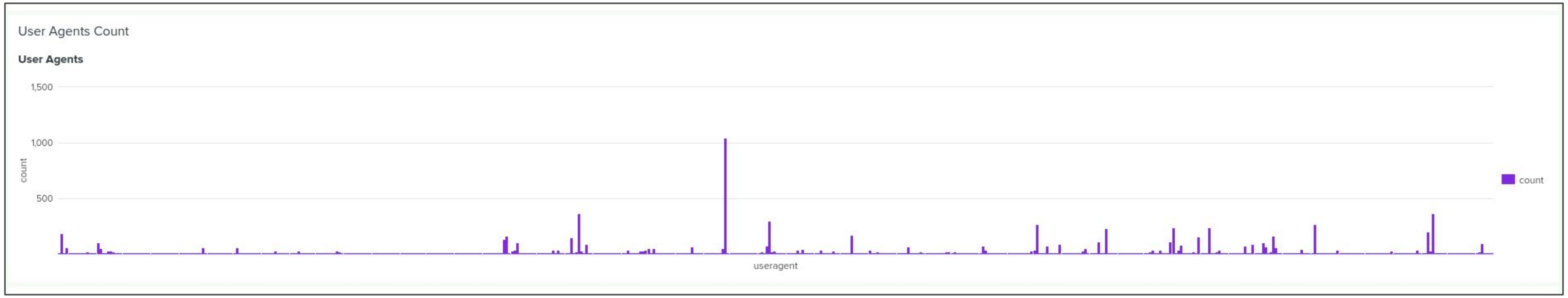
Top 10



Total Successful HTTP Responses

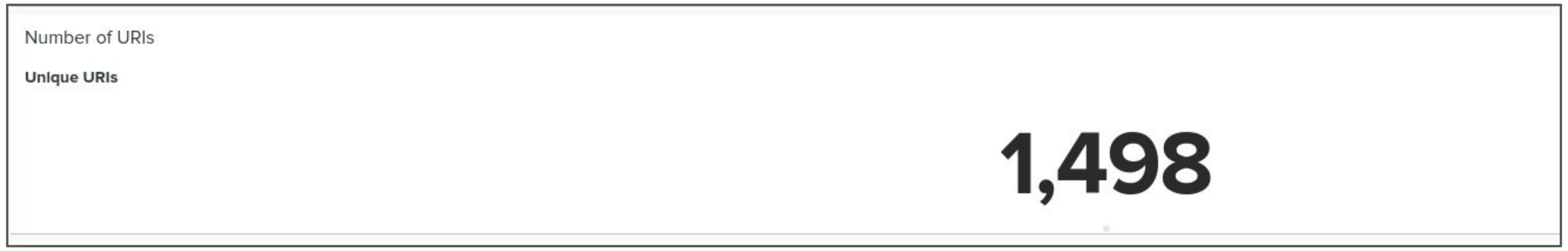
Code 200

Dashboards—Apache



User Agents Count

User Agents



Number of URIs

Unique URIs

1,498

Attack Analysis

Attack Summary—Windows

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

- Our findings from the attack logs indicated the following:
  - Suspicious changes were detected on the report analysis for **severity**.
    - The Ratio of severity went from information severity of 4435/93.09% to 4383/79.78% **(decrease),** and high severity of 329/6.91% to 1111/20.22% **(increase).**
  - Suspicious changes were detected on the report analysis for **failed activities.**
    - The ratio of failed activities to successful activities went from 142/622 failures/success (2.98%/97.02%) to 93/5856 failure/success (1.56%/98.44%).

Attack Summary—Windows

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

- Alert Analysis for **Failed Windows Activity** showed a spike in volume of 35 events in the 8:00AM hour. The threshold of 11 events was correct.
- Alert Analysis for **Successful Logins** showed a spike in volume at 11am with 196 successful logins, followed by 77 successful logins at 12am. The threshold of 22 events was correct.
- Alert Analysis for **Deleted Accounts** did not detect any suspicious volume with the threshold set at 22. The average hourly volume was not out of the norm based on our established baseline of 22.

Attack Summary—Windows

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

- Dashboard Analysis for the **Time Chart of Signatures** showed spikes in user lockouts (896), password resets (1,258), and successful logins (196) at various times throughout the day.
- Dashboard Analysis for the **Time Chart of User Activity** showed corresponding spikes in activity for User K, User A, and User J, respectively.
- Dashboard Analysis of **Total Signature Counts** and **Total User Activity**, supported the first two findings, with significantly above average total counts for the three aforementioned signatures and significantly above average total activity for the aforementioned three users.

Attack Summary—Apache

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

- The **HTTP POST method** under normal conditions is approximately 1% of total web server activity. While under attack it **rose to 29.4%** effectively overwhelming our server and disrupting normal operations.
- The **404** response code (“not found”) **increased from 2% to 15%** and code **200** (OK) **decreased from 91% to 83%**. Due to the poor performance of our server during the attack, client experience was impacted likely leading to user frustration, confusion and an overall poor perception of website quality.
- For the **Domain Referer report**, although there were less total referrations from outside websites on the day of the attack, the **top two remained the same** - www.semicomplete.com and semicomplete.com. These websites contain information and technology on security breaches.

Attack Summary—Apache

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

- Alert Analysis for **International Activity** showed a lower volume of events during the attack than normal baseline activity. The threshold of greater than 40 events from IP addresses in China was correct. We would however recommend adding an alert for Ukraine IP addresses.
- Alert Analysis for **HTTP POST Activity** showed a spike in volume at 8PM with 1,296 POST events. The threshold of 10 events was correct.

Attack Summary—Apache

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

- Dashboard Analysis for **Time Chart of HTTP Methods** showed spikes in GET requests at 6PM (up from 117 events to 729) followed by POST requests at 8:00PM (up from 1 event to 1,296).
- Dashboard Analysis for **Cluster Map** showed increased activity in two major cities in Ukraine - Kiev (increased from 30 during normal conditions to 454) and Kharkiv (increased from 35 during normal conditions to 433).
- Dashboard Analysis for **URI Data** indicates suspicious activity at 6PM from /files/logstash/logstash-1.3.2-monolithic.jar and at 8PM from /VSI_Account_logon.php (with 1296 hits).

Summary and Future Mitigations

Project 3 Summary

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

The attack on March 25, 2020, exhibited suspicious spikes in Windows server log activities, including failed logins, account lockouts, and password reset attempts. Additionally, there was a significant increase in HTTP POST activities and GET requests in the Apache web server logs, particularly targeting the URI /VSI_Account_logon.php, indicating a potential brute force attempt. Unusual activity was also detected from IP addresses in Ukraine.

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

Enhanced Monitoring: Implement continuous monitoring for spikes in failed logins, account lockouts, and password resets, with alerts for unusual activity.

Rate Limiting: Apply rate limiting on critical URIs like /VSI_Account_logon.php to prevent brute force attacks.

Geolocation Blocking: Consider blocking or scrutinizing traffic from regions with unusual activity, such as Ukraine.

Strong Authentication: Enforce multi-factor authentication (MFA) for all user logins.

Regular Audits: Conduct regular security audits and vulnerability assessments on both Windows servers and Apache web servers.

Incident Response Plan: Develop and regularly update an incident response plan to swiftly address potential security breaches.