Project 3:

Building a Secure Monitoring Environment

By: TaSheria Walls, Gertrise Thomas, Patrick Schultz, Shantel Varner, Katie Prude-Turner & Leondra Rascoe

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

Our analyst team has been tasked with monitoring potential cyber threat against Virtual Space Industries' (VSI) due to recent intel that a competitor, JobeCorp, may attempt to launch cyberattacks to disrupt VSI’s operations.

To mitigate these risks, we are utilizing Splunk to actively monitor and analyze security events across two key systems:

- Apache Web Server – Hosts VSI’s administrative webpage, a critical access point for system management.
- Windows Operating System – Supports essential back-end operations vital to VSI’s business continuity.

We have been provided with historical log data to help establish security baselines, identify anomalies, and develop reports, alerts, and dashboards.

This initiative aims to strengthen VSI’s cybersecurity posture and safeguard its digital assets against emerging threats.

Splunk Security Essentials

Splunk Security Essentials

Splunk Security Essentials (SSE) is a free add-on that enhances security operations by providing prebuilt detection rules, best practices, and detailed use case guidance. SSE integrates seamlessly with Splunk's analytics engine, delivering out-of-the-box security content mapped to industry frameworks such as **MITRE ATT&CK®**, **NIST**, and **CIS**. It acts as a force multiplier for security teams, enabling quick deployment of detection strategies, improving threat visibility, and supporting data-driven security workflows.

Key Features:

- **Prebuilt Security Content:** Access over **600+** detection and response use cases, mapped to security frameworks for efficient threat identification.
- **Guided Implementation:** Follow **step-by-step** walkthroughs to deploy security detections, complete with **sample data** and **validation tools**.
- **MITRE ATT&CK® Integration:** Visualize security detections within the **ATT&CK framework**, providing a structured and strategic approach to threat detection.
- **Anomaly Detection & Risk-Based Alerting:** Detect deviations from normal behavior and **prioritize alerts** using **risk scoring** to focus on the most critical threats.
- **Cost-Effective Solution:** Available as a **free app** on **Splunkbase**, offering powerful security enhancements **without additional licensing costs**.

Splunk Security Essentials Scenario

Scenario: Protecting VSI from Competitor Cyberattacks with Splunk Security Essentials

Company:

- **Virtual Space Industries (VSI)** is a leader in **virtual-reality program design**.
- Received intelligence that competitor **JobeCorp** may attempt **cyberattacks** to disrupt operations.
- Leadership is concerned about **espionage**, **DDoS attacks**, and **insider threats**, but lacks visibility into potential threats.

Solution:

VSI’s **Security Operations Center (SOC)** deploys **Splunk Security Essentials (SSE)** to enhance security defenses.

1. **Prebuilt Threat Detections:**
   - Utilize **ready-to-use security detections** for:
     - **DDoS attack monitoring**
     - **Unusual login attempts**
     - **Unauthorized data access tracking**
2. **MITRE ATT&CK® Mapping:**
   - Identify and address **security gaps** by mapping them to **JobeCorp’s suspected attack techniques**.
   - Implement **enhanced intrusion detection rules** to counter potential threats.
3. **Risk-Based Alerting:**
   - Automatically trigger alerts for **anomalous employee activity**, such as:
     - **Unauthorized access** to **proprietary VR design files**
     - **Suspicious login patterns**
4. **Security Posture Dashboard:**
   - Monitor **ongoing threats** and **track security improvements**.
   - Maintain **proactive defenses** against **corporate espionage**.

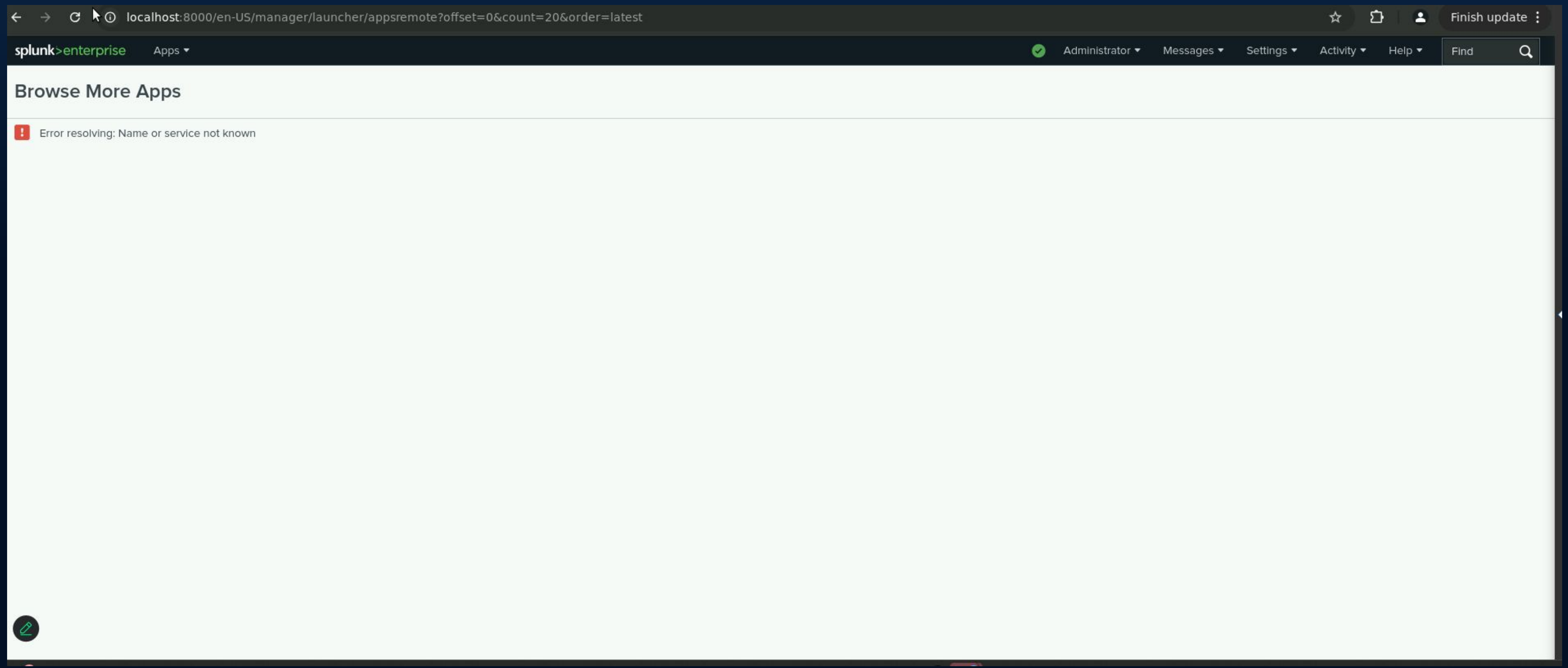
Splunk Security Essentials Scenario, Cont.

Outcome:

- **Prevented Data Theft:** VSI detects and **stops an unauthorized access attempt** before critical VR designs are stolen.
- **Improved Threat Detection:** VSI gains **full visibility** into **DDoS attempts and login anomalies**, blocking attacks before they escalate.
- **Strengthened Competitive Security:** By leveraging **Splunk Security Essentials**, VSI **stays ahead of JobeCorp's cyber threats**, ensuring business continuity.

Using **Splunk Security Essentials**, VSI proactively defends against cyber threats, prevents business disruption and protects its intellectual property—all at no extra cost.

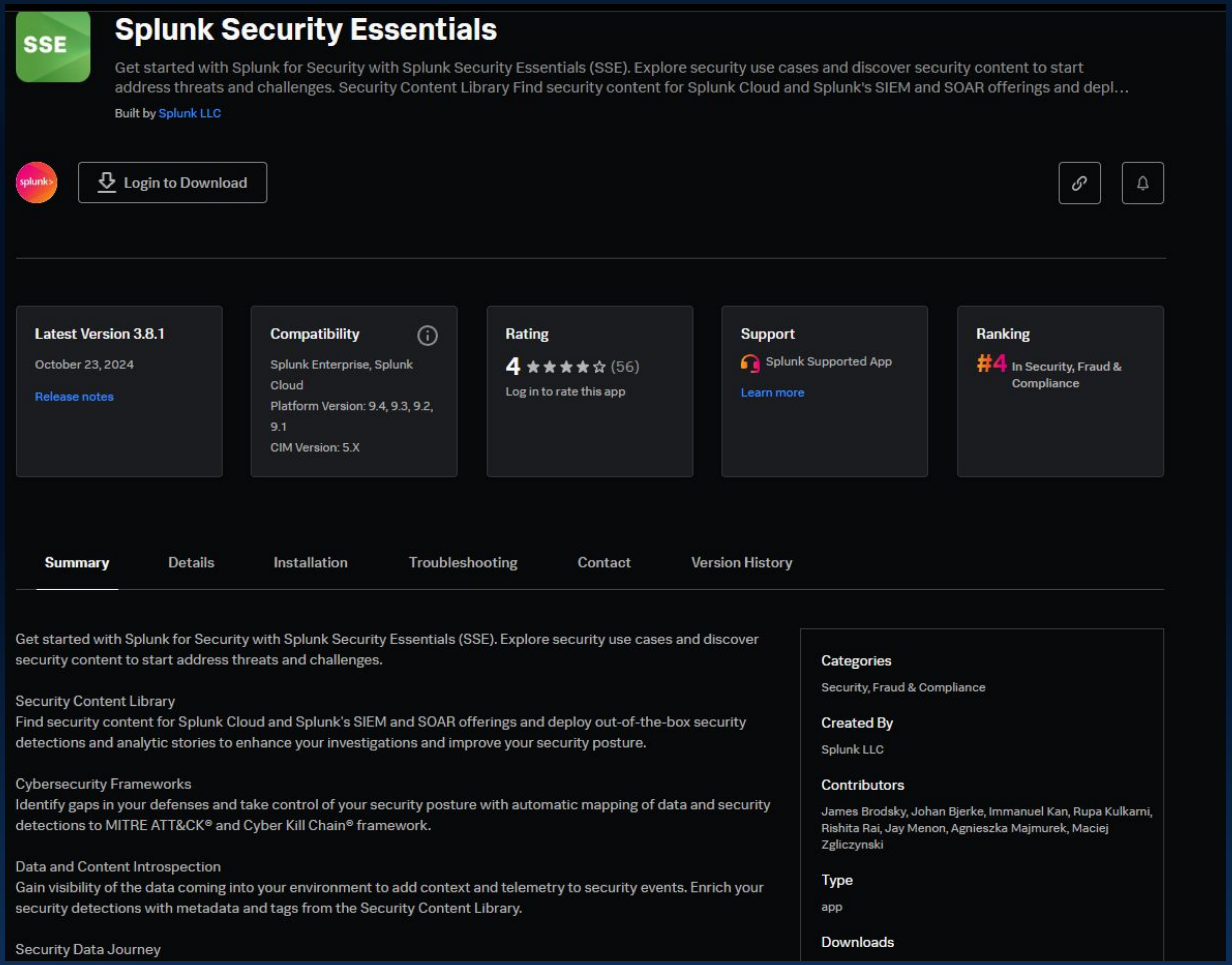
Splunk Security Essentials



localhost:8000/en-US/manager/launcher/appsremote?offset=0&count=20&order=latest

Browse More Apps

Error resolving: Name or service not known



Splunk Security Essentials

Get started with Splunk for Security with Splunk Security Essentials (SSE). Explore security use cases and discover security content to start address threats and challenges. Security Content Library Find security content for Splunk Cloud and Splunk's SIEM and SOAR offerings and depl...

Built by Splunk LLC

Latest Version 3.8.1
October 23, 2024
Release notes

Compatibility
Splunk Enterprise, Splunk Cloud
Platform Version: 9.4, 9.3, 9.2, 9.1
CIM Version: 5.X

Rating
4 ★★★★☆ (56)
Log in to rate this app

Support
Splunk Supported App
Learn more

Ranking
#4 In Security, Fraud & Compliance

Get started with Splunk for Security with Splunk Security Essentials (SSE). Explore security use cases and discover security content to start address threats and challenges.

Security Content Library
Find security content for Splunk Cloud and Splunk's SIEM and SOAR offerings and deploy out-of-the-box security detections and analytic stories to enhance your investigations and improve your security posture.

Cybersecurity Frameworks
Identify gaps in your defenses and take control of your security posture with automatic mapping of data and security detections to MITRE ATT&CK® and Cyber Kill Chain® framework.

Data and Content Introspection
Gain visibility of the data coming into your environment to add context and telemetry to security events. Enrich your security detections with metadata and tags from the Security Content Library.

Security Data Journey

Categories
Security, Fraud & Compliance

Created By
Splunk LLC

Contributors
James Brodsky, Johan Bjerke, Immanuel Kan, Rupa Kulkarni, Rishita Rai, Jay Menon, Agnieszka Majmurek, Maciej Zgliczynski

Type
app

Downloads

Logs Analyzed

1 Windows Logs

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

- ■Windows Logs
- ■Windows Attack Logs

2 Apache Logs

This server is used for VSI’s main public-facing website, vsi-company.com.

- ■Apache Logs
- ■Apache Attack Logs

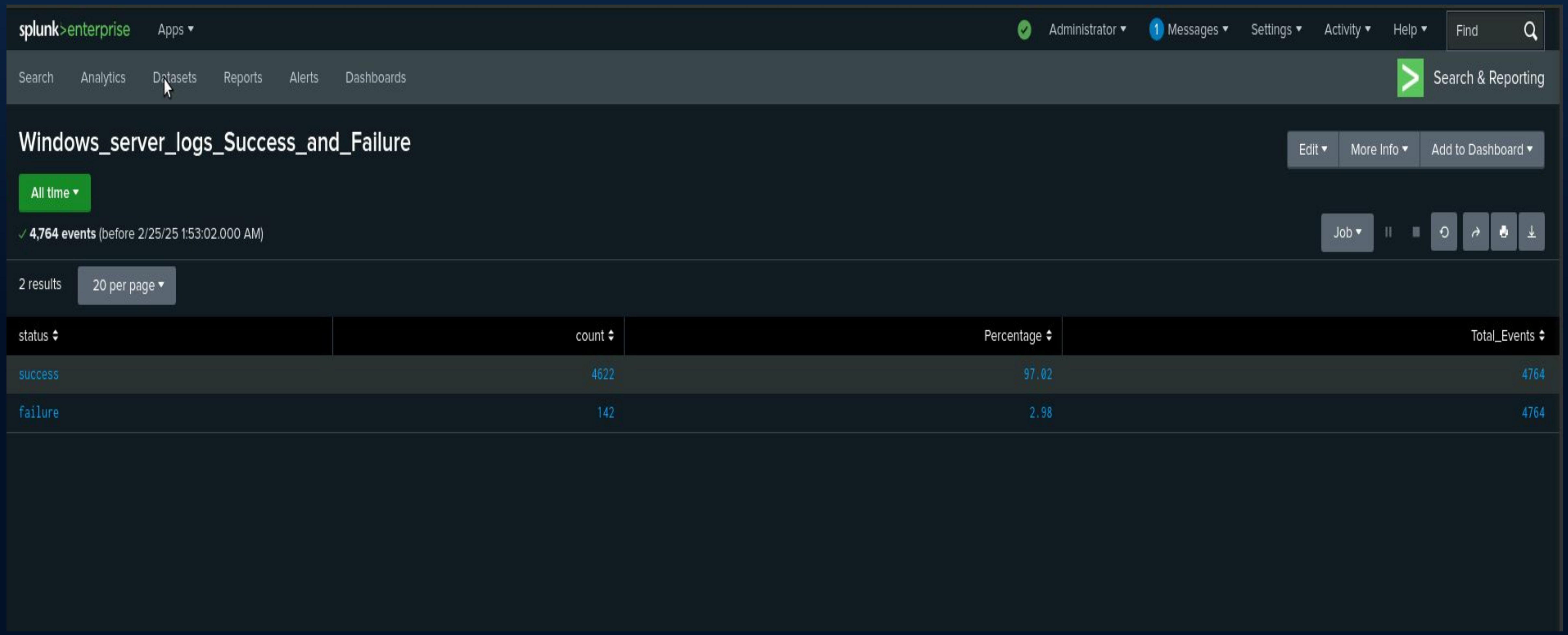
Windows Logs

Reports — Windows

Designed the following reports:

Report Name	Report Description
Windows_Server_logs_Signatures_and Signature IDs	Log showcasing the cumulative count of events executed for each signature ID.
Windows_Server_logs_Severity_levels_counts_and percentages	Log presenting the percentage distribution of events across various severity levels.
Windows_server_logs_Success_and_Failure	Log presenting the total count, percentage distribution, and detailed events of successful and failed account activities.

Images of Reports – Windows

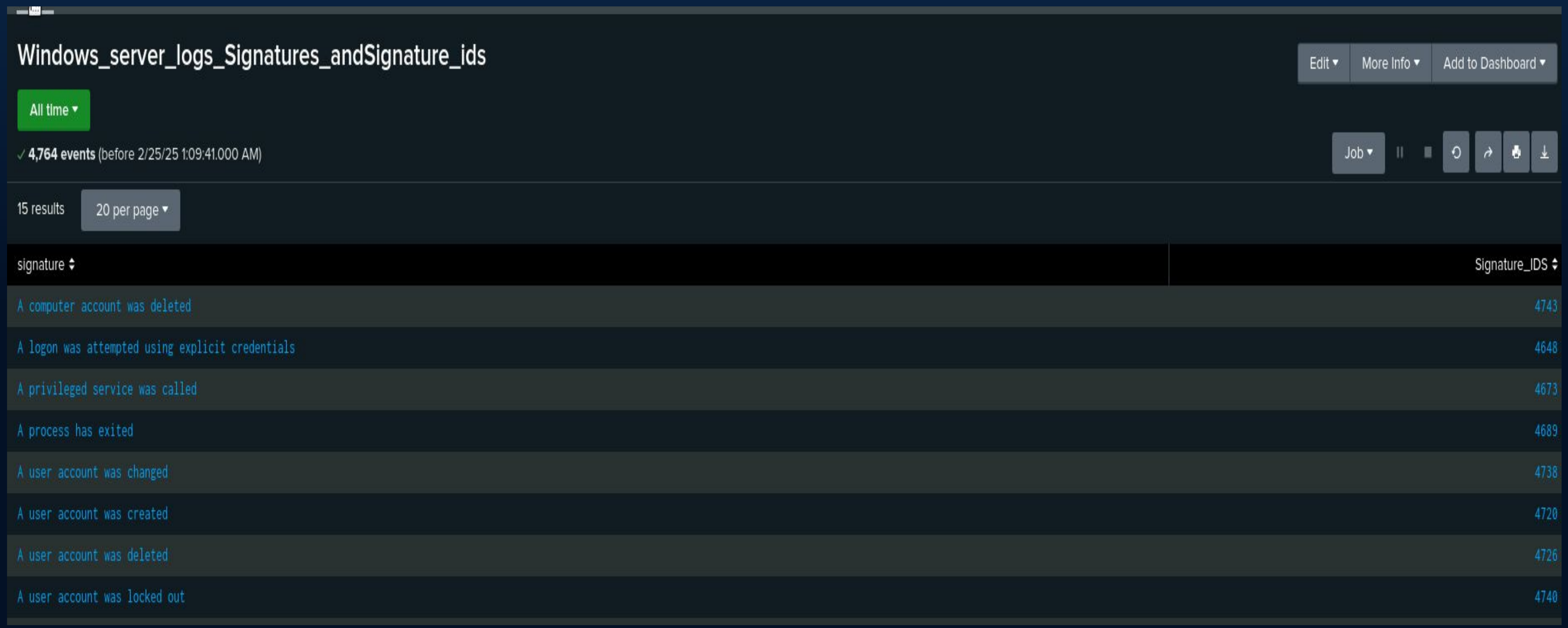


Windows_server_logs_Success_and_Failure

✓ 4,764 events (before 2/25/25 1:53:02.000 AM)

2 results

status	count	Percentage	Total_Events
success	4622	97.02	4764
failure	142	2.98	4764

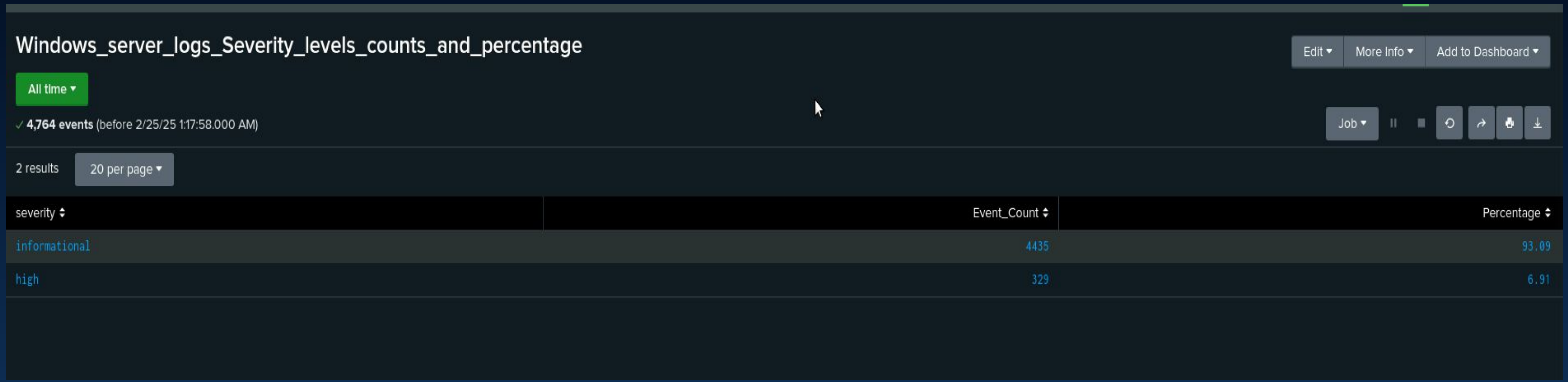


Windows_server_logs_Signatures_andSignature_ids

✓ 4,764 events (before 2/25/25 1:09:41.000 AM)

15 results

signature	Signature_IDS
A computer account was deleted	4743
A logon was attempted using explicit credentials	4648
A privileged service was called	4673
A process has exited	4689
A user account was changed	4738
A user account was created	4720
A user account was deleted	4726
A user account was locked out	4740



Windows_server_logs_Severity_levels_counts_and_percentage

✓ 4,764 events (before 2/25/25 1:17:58.000 AM)

2 results

severity	Event_Count	Percentage
informational	4435	93.09
high	329	6.91

Alerts — Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Server Logs Failed Windows Activity	Alert log capturing and displaying login failure events.	5	7

JUSTIFICATION: We set the baseline at five, as it represents the average number of alerts, with the highest counts reaching 9 and 10. We set the threshold at seven, as it served as a clear indicator of an attack.

Alerts — Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Server Logs-Successful Log On	Alert log capturing and displaying successful login events.	13	15

JUSTIFICATION: We set the baseline at 13, as it represents the average number of alerts for successful login events. Similarly, we chose the alert threshold at 15 as it signifies a potential successful log in attack.

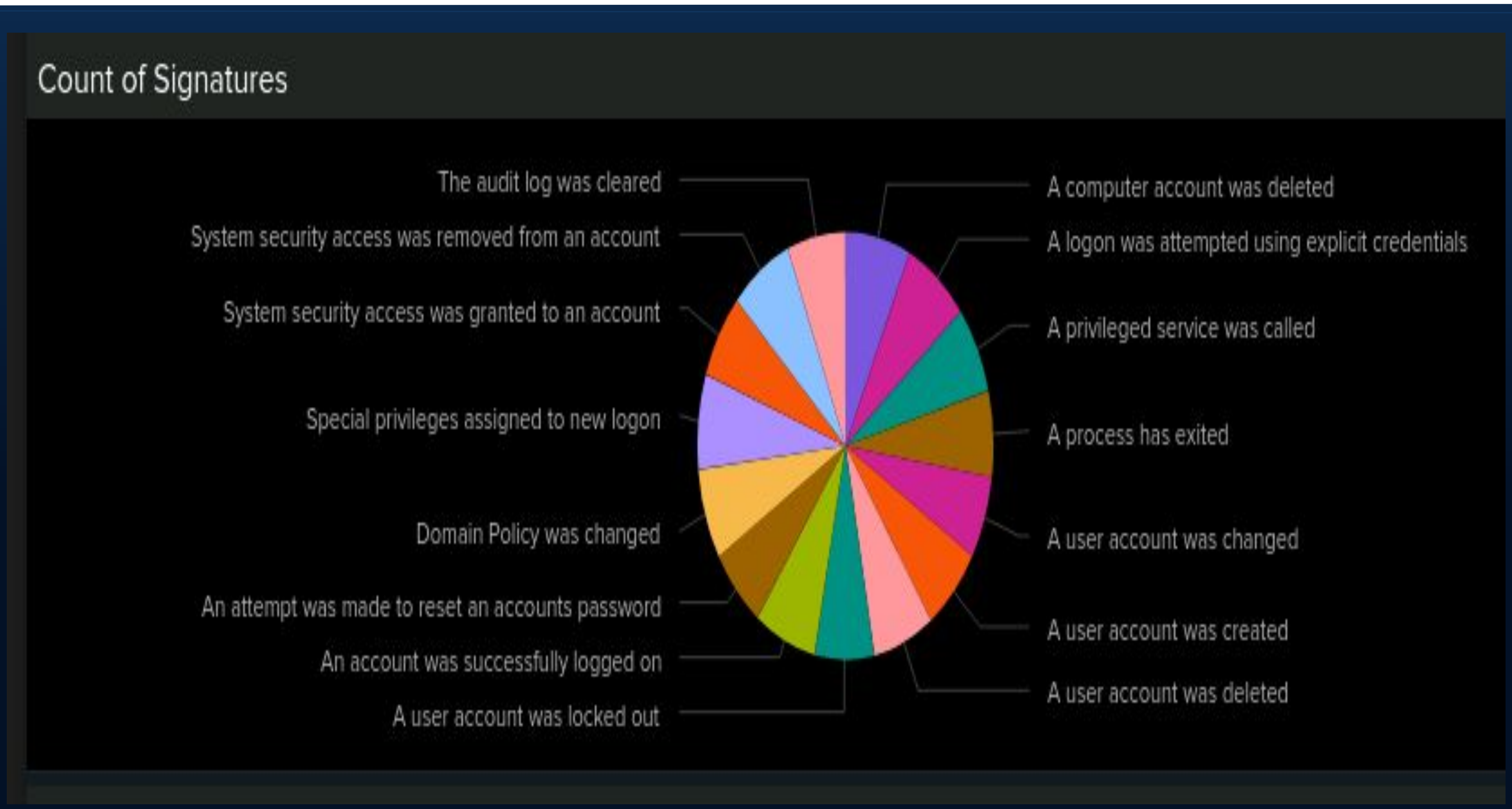
Alerts — Windows

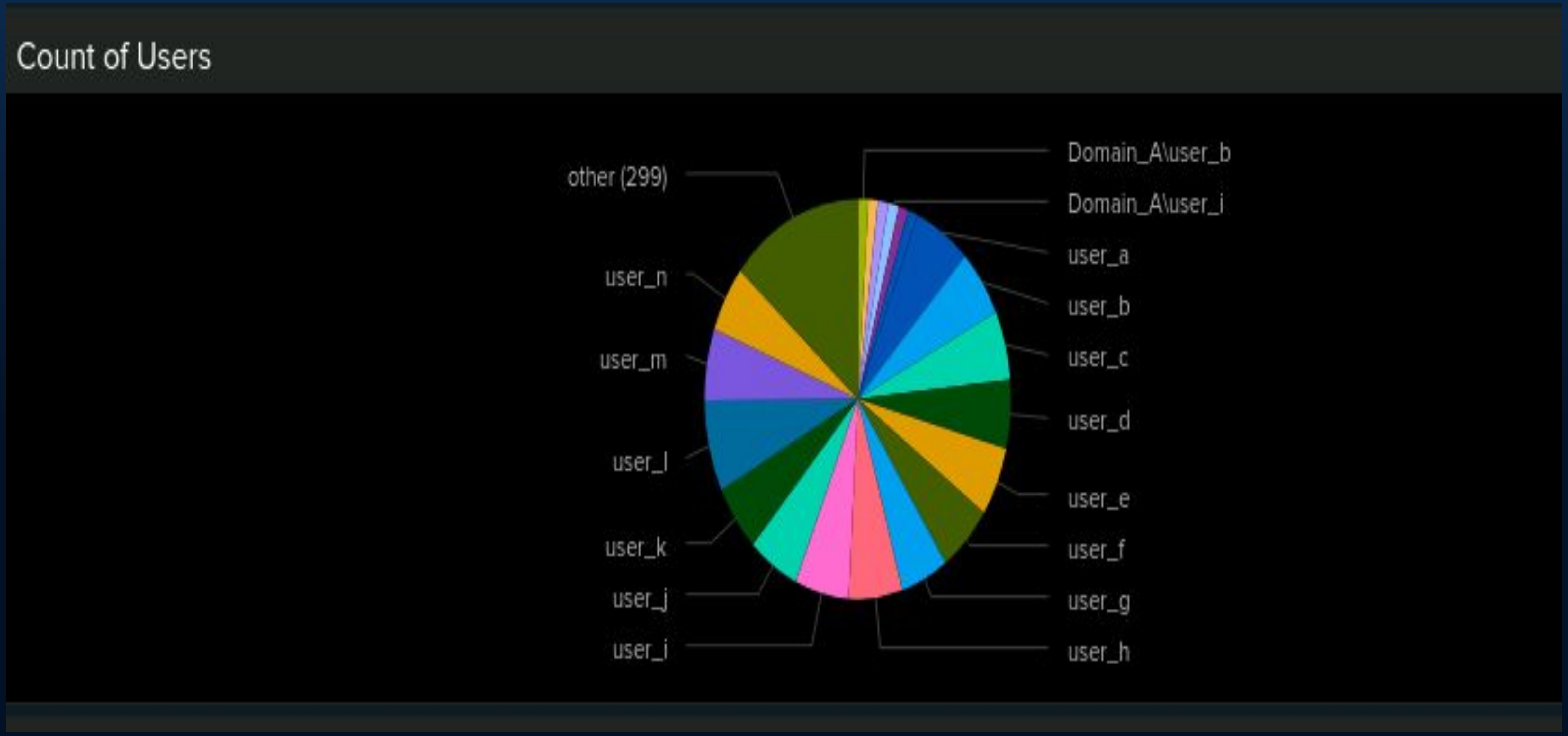
Designed the following alerts:

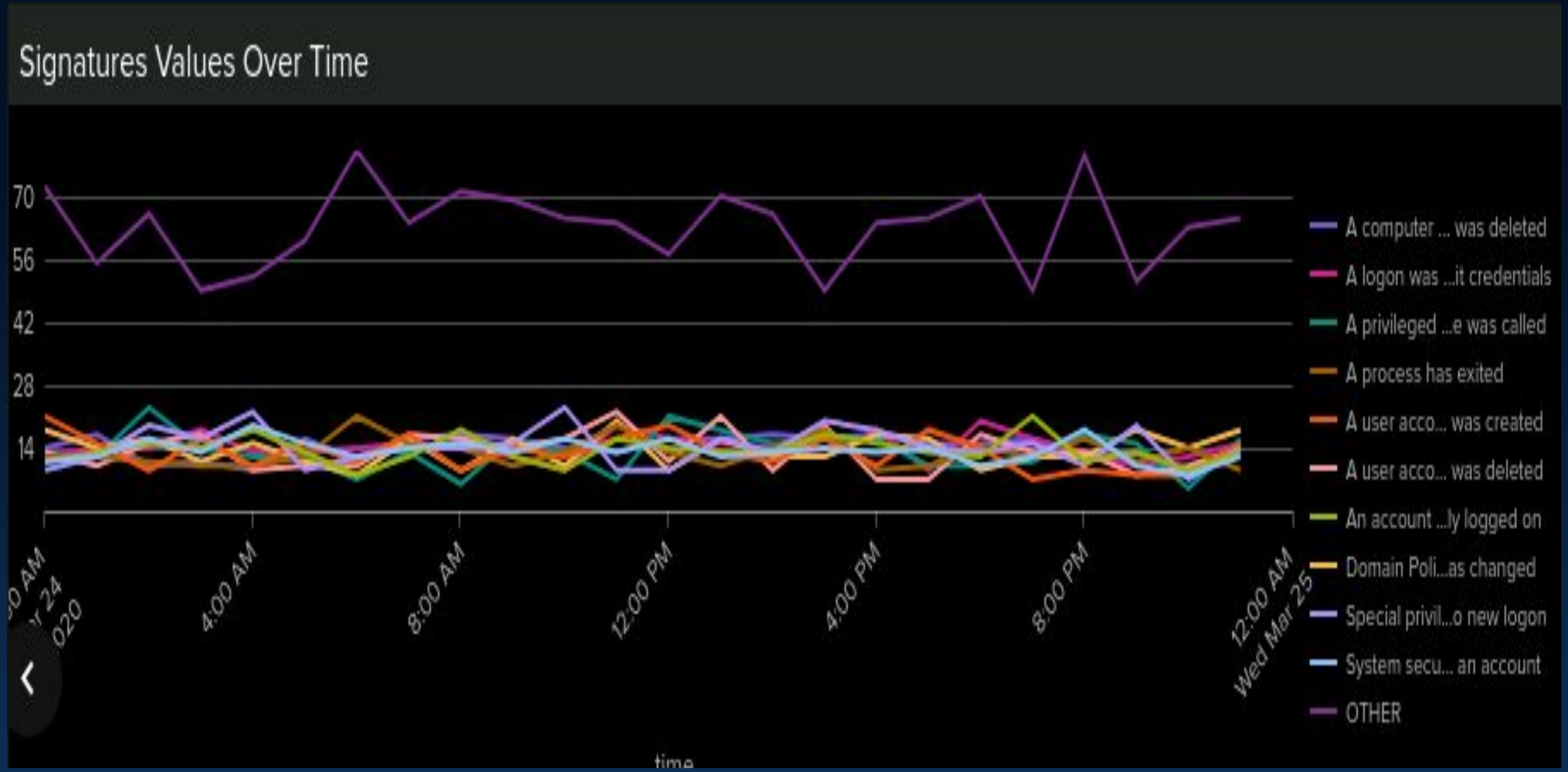
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Servers Logs - Deleted Accounts	Alert log capturing and displaying successful account deletions.	10	13

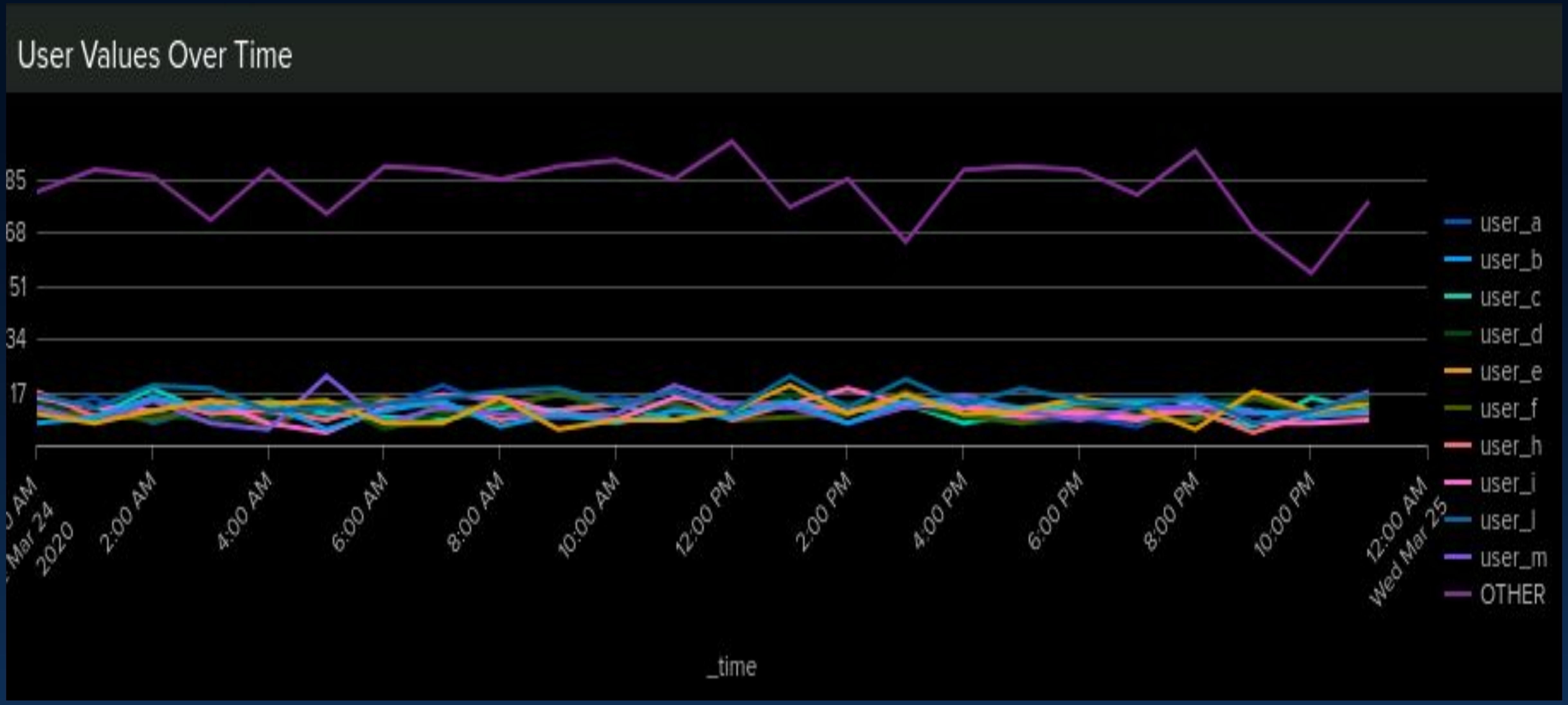
***JUSTIFICATION:** The baseline for deleted accounts was set at 10 as it was the average number of alerts for deleted accounts. Between 9AM and 3PM, account deletions peaked at 22, marking the highest activity during this period.*

Dashboards—Windows

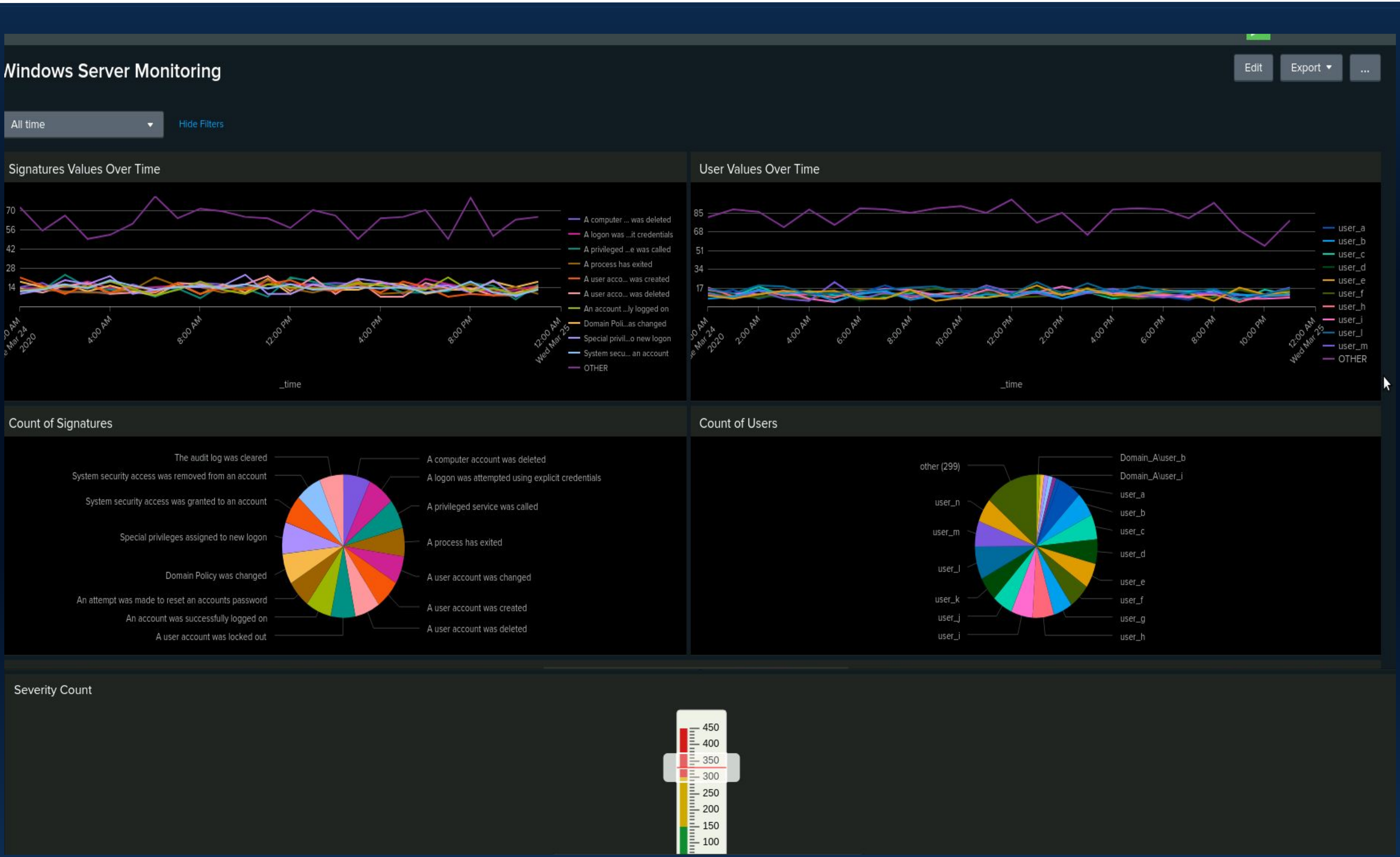

Count of Signatures


Count of Users


Signatures Values Over Time


User Values Over Time

Dashboards – Windows



/indows Server Monitoring

All time

Signatures Values Over Time

User Values Over Time

Count of Signatures

Count of Users

Severity Count

Edit
Export ▾
...
Hide Filters
70
56
42
28
14
0 AM
e Mar 24
2020
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
12:00 AM
Wed Mar 25
_time
A computer ... was deleted
A logon was ...it credentials
A privileged ...e was called
A process has exited
A user acco... was created
A user acco... was deleted
An account ...ly logged on
Domain Poli...as changed
Special privil...o new logon
System secu... an account
OTHER
85
68
51
34
17
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
user_a
user_b
user_c
user_d
user_e
user_f
user_h
user_i
user_l
user_m
OTHER
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
other (299)
user_n
user_m
user_l
user_k
user_j
user_i
Domain_A\user_b
Domain_A\user_i
user_a
user_b
user_c
user_d
user_e
user_f
user_g
user_h
450
400
350
300
250
200
150
100

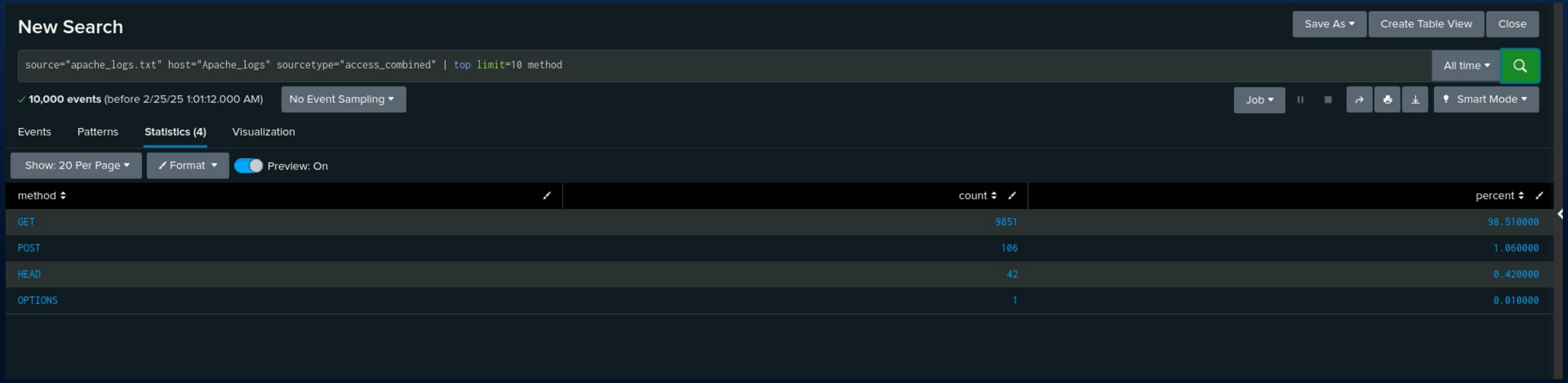
Apache Logs

Reports — Apache

Designed the following reports:

Report Name	Report Description
VSI TOP HTTP Methods	HTTP activity being requested against VSI’s web server
VSI Top Domains	Analyzes the different referrer domains.
VSI HTTP Response Codes	Provides insight into any suspicious levels of HTTP responses

Images of Reports — Apache

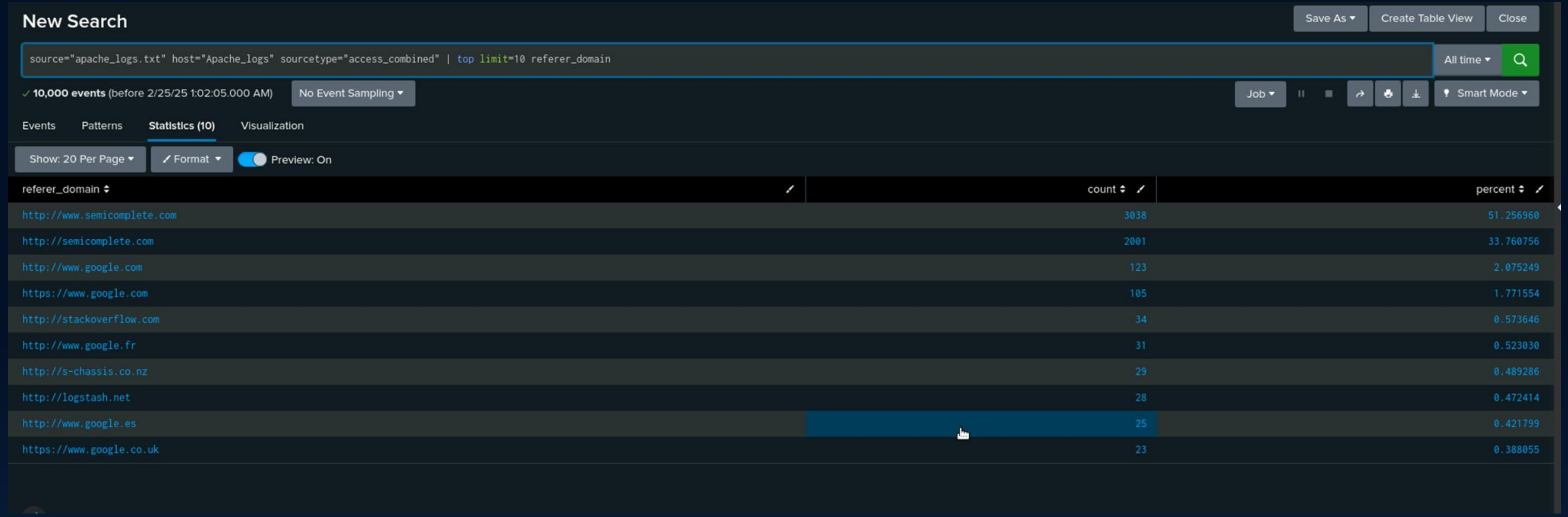


```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | top limit=10 method
```

✓ **10,000 events** (before 2/25/25 1:01:12.000 AM) No Event Sampling

method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

VSI Top HTTP Method



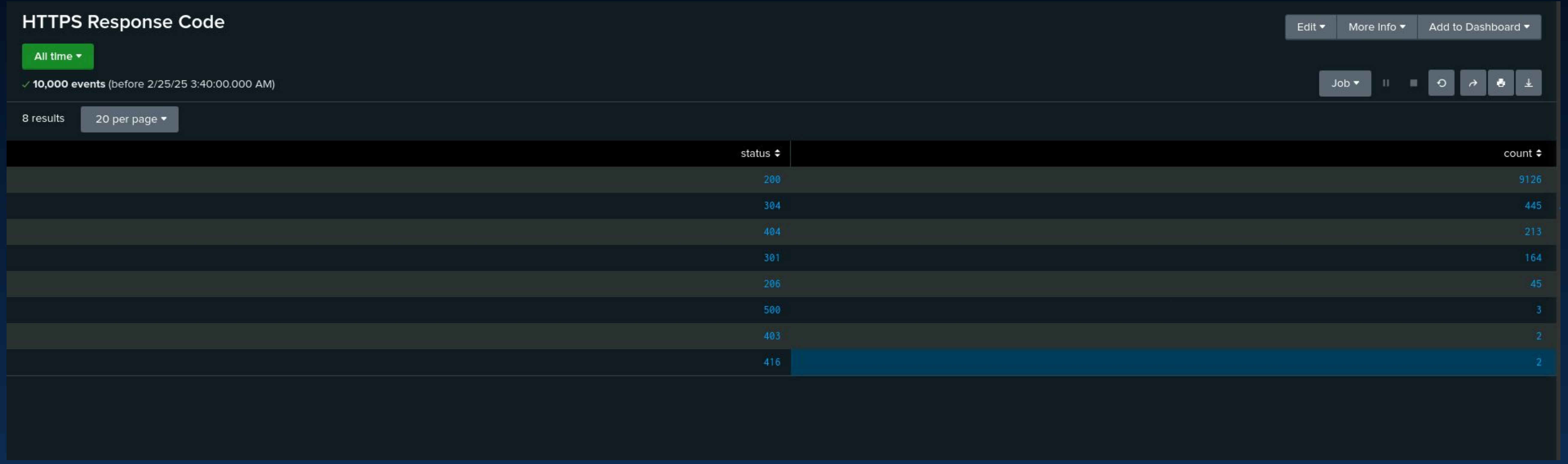
```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | top limit=10 referer_domain
```

✓ **10,000 events** (before 2/25/25 1:02:05.000 AM) No Event Sampling

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

Top 10 Domains

HTTP Response Code



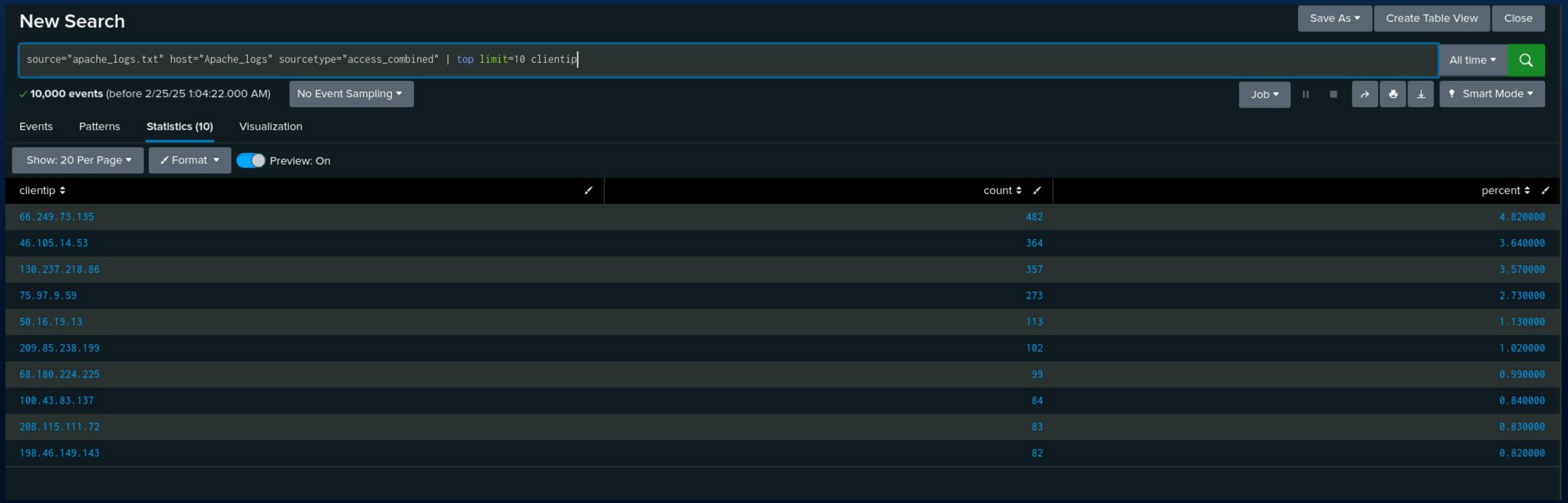
✓ **10,000 events** (before 2/25/25 3:40:00.000 AM)

8 results

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

Images of Reports – Apache

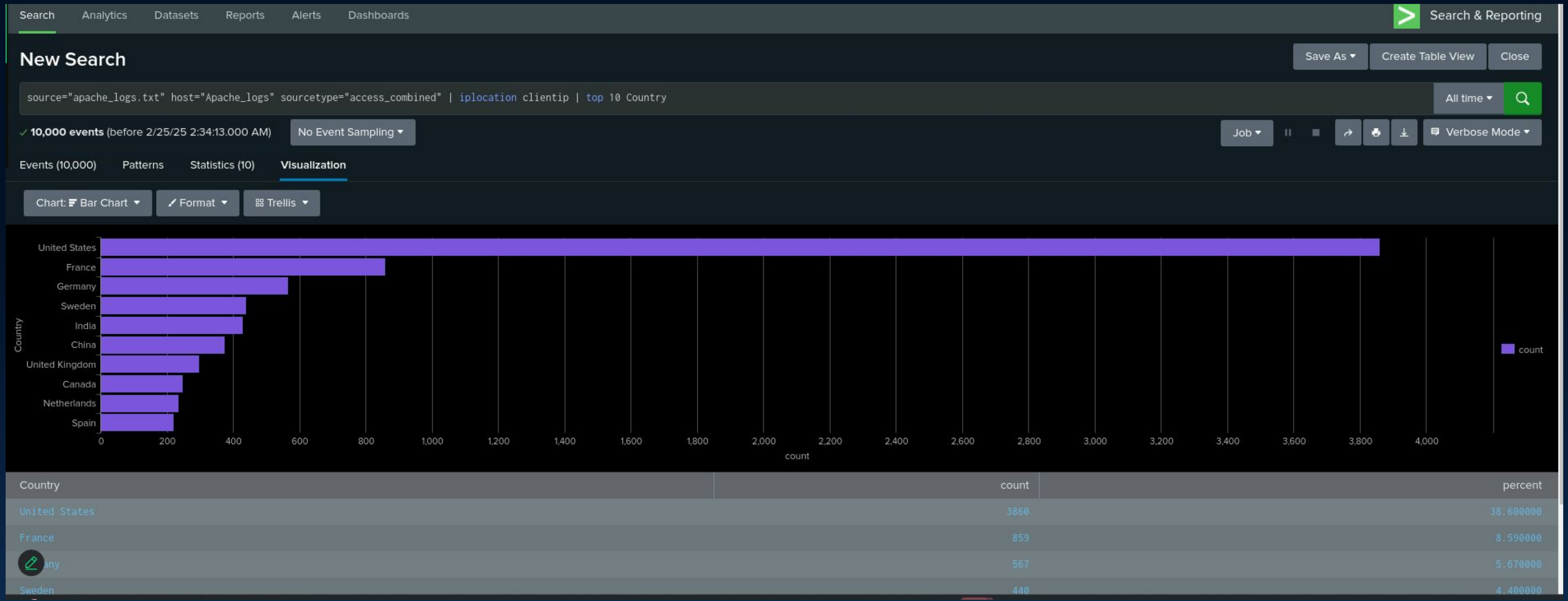
Top 10 Client IP



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | top limit=10 clientip
```

✓ 10,000 events (before 2/25/25 1:04:22.000 AM) No Event Sampling

clientip	count	percent
66.249.73.135	482	4.820000
46.105.14.53	364	3.640000
130.237.218.86	357	3.570000
75.97.9.59	273	2.730000
50.16.19.13	113	1.130000
209.85.238.199	102	1.020000
68.180.224.225	99	0.990000
100.43.83.137	84	0.840000
208.115.111.72	83	0.830000
198.46.149.143	82	0.820000



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | top 10 Country
```

✓ 10,000 events (before 2/25/25 2:34:13.000 AM) No Event Sampling

Country	count	percent
United States	3860	38.600000
France	859	8.590000
Germany	567	5.670000
Sweden	440	4.400000

Top 10 Country AWSM Dashboard

Alerts — Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI IP Outside of US	Activity from any country besides the United States; alert should trigger an email to SOC@VSI-company.com when the threshold has been reached	120	125

"The 'VSI IP Outside of US' alert is based on analyzing past log data to find the normal amount of access requests from non-U.S. IP addresses. The baseline is set at 120, representing the ***usual*** *activity level. The alert threshold is slightly higher at 125 to handle occasional traffic spikes. This balance helps reduce false positives while ensuring that only truly unusual or suspicious activity triggers the alert."*

Alerts — Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI HTTP POST Count	Hourly count of the HTTP POST method The alert should trigger an email to SOC@VSI-company.com when the threshold has been reached	7	12

"The 'VSI HTTP POST Count' alert is based on analyzing historical data to find the typical hourly number of HTTP POST requests, with an average of 7. The threshold is set at 12, allowing a buffer for normal traffic increases. This approach helps reduce false positives while ensuring that any significant deviations are flagged for review, helping to detect potentially malicious activities."

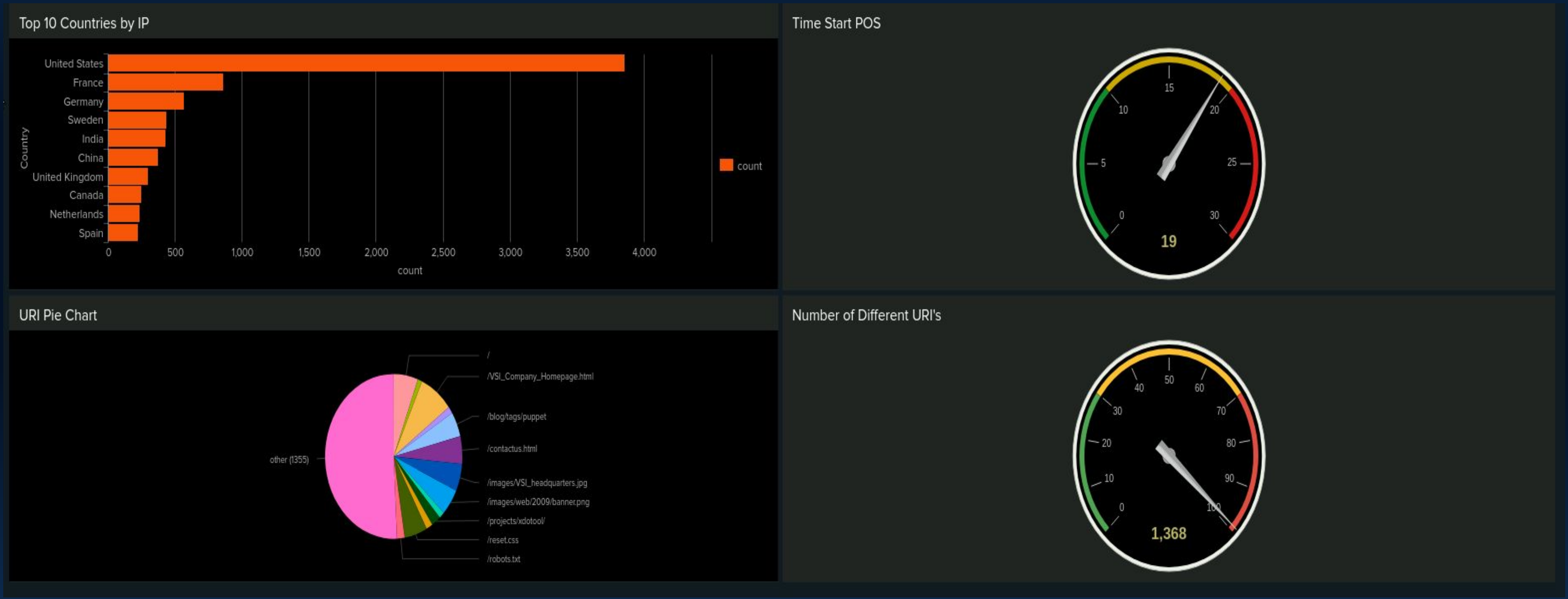
Dashboard — Apache Web Server Monitoring

Apache Web Server Monitoring Dashboard

Last 24 hours

Edit
Export ▾
...
Hide Filters
HTTP Methods Line Chart
150
100
50
12:00 PM Tue Mar 17 2020
12:00 AM Wed Mar 18
12:00 PM
12:00 AM Thu Mar 19
12:00 PM
12:00 AM Fri Mar 20
12:00 PM
_time
GET
HEAD
OPTIONS
POST
Geo Map Clientip
+
−
0 - 800
800 - 1,600
1,600 - 2,400
2,400 - 3,200
3,200 - 4,000
Top 10 Countries by IP
United States
France
Germany
Sweden
India
China
Country
count
Time Start POS
5
10
15
20
25

Dashboard — Apache Cont.



Attack Analysis

Attack Summary — Windows

Our findings from analyzing the reports:

- For the Windows Server Logs - Success and Failures:
  - The Status for success
    - Event Count: increased from 4622 to 5856
    - Percentages: increased from 97.02% to 98.44%
  - The status for failure
    - Event Count: decreased from 142 - 93
    - Percentage: decreased from 2.98% to 1.56%
- For the Windows Server Logs - Severity levels counts and percentages:
  - Informational:
    - Event Count: decreased from 4435 - 4383
    - Percentages: decreased from 93.09% to 79.78%
  - High:
    - Event Count: increased from 329 to 1111
    - Percentages increased from 6.91% to 20.22%

Attack Summary — Windows

Our findings from analyzing the alerts:

- While analyzing alerts via the attack logs we identified that there were issues affecting the visibility and effectiveness of security alerts.
    - No alerts were visible on the designated alerts page
    - Adjustments to scheduled alert times and expiration settings did not resolve the issue.
    - Potential alerts were only visible when selecting the “All Time” filter in the search page.
    - All alerts were set in 2020 with no new alerts being generated.

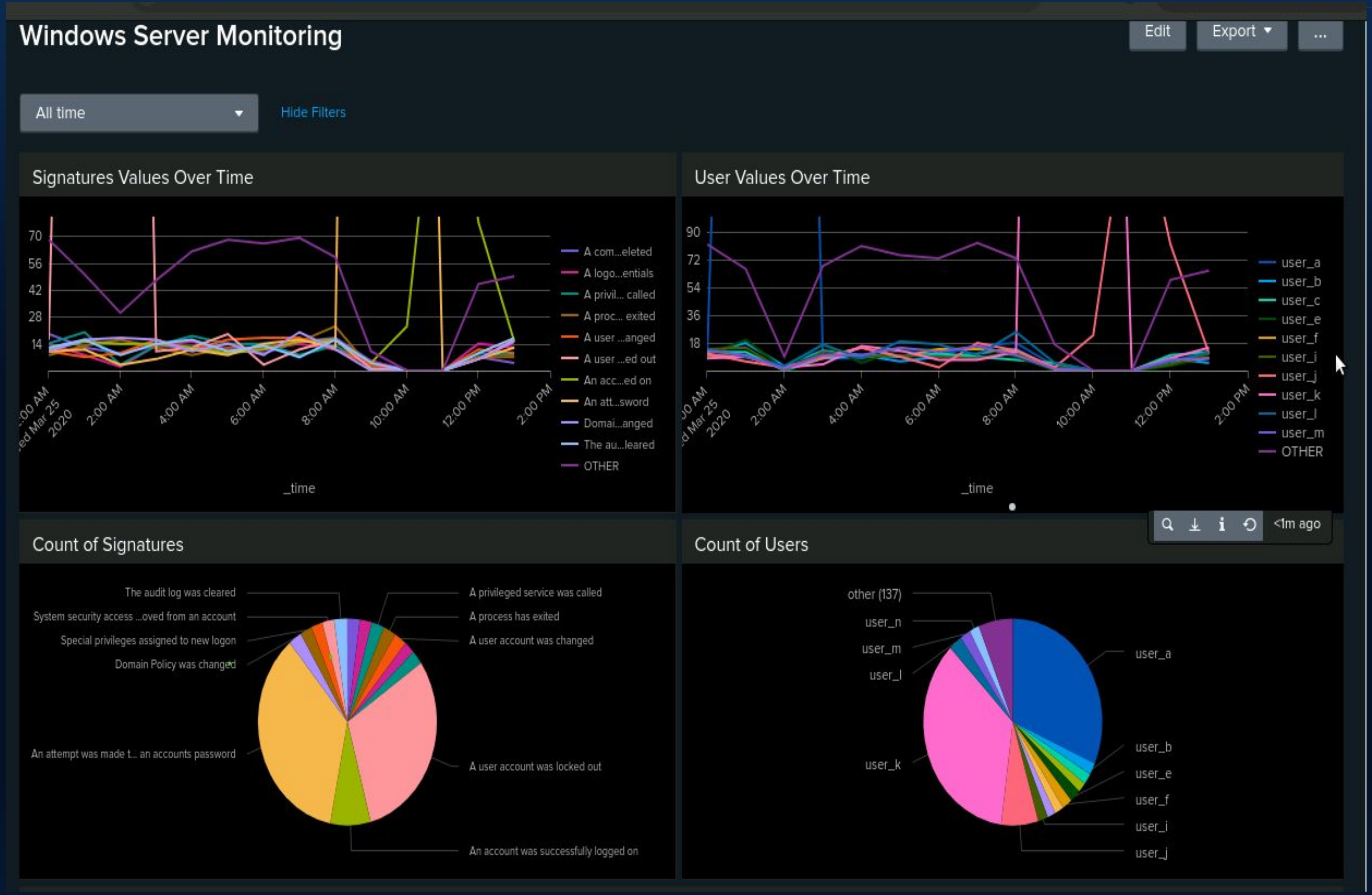
- Due to the lack of properly triggered alerts, we were unable to accurately assess whether existing baselines and threshold configurations were effective.

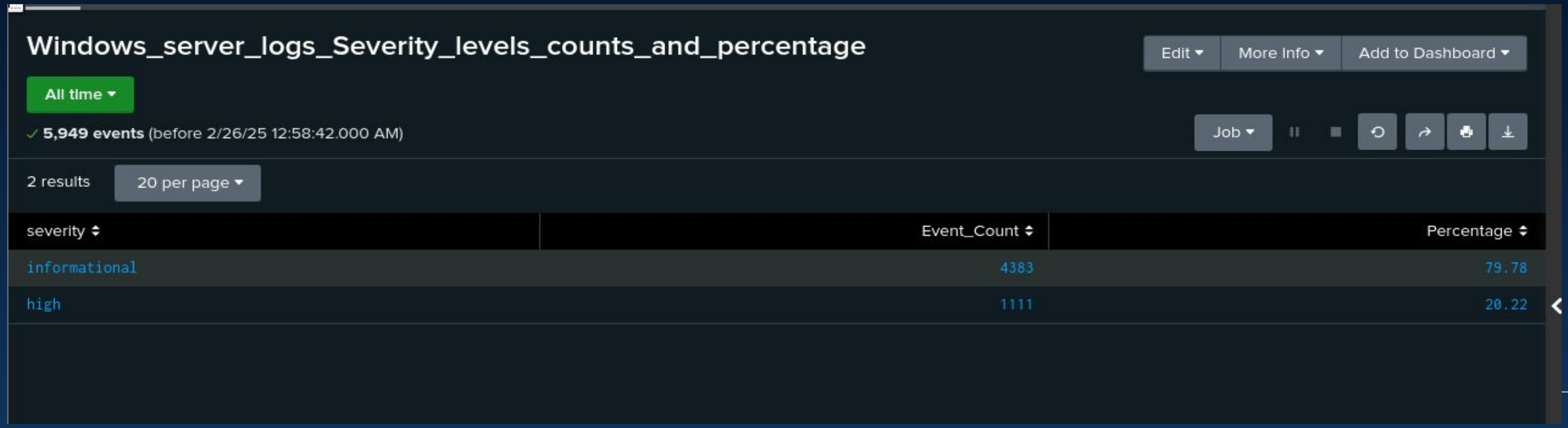
Attack Summary — Windows

Our findings from analyzing the dashboards:

- Analyzing the dashboards via the attack logs, we noticed changes in the percentages and values for our Severity, Signature Values and User Values over time dashboards.
- We observed a striking correlation between the spike in user attack values and the surge in signature detections, both occurring simultaneously. This alignment suggests a potential connection between the two events.
  - Signature Value - an attempt to reset password - coincides with User K
    - from 8AM to 11AM the value for User spiked
  - Signature Value - a user account was locked - coincides with User A
    - from 12AM to 3AM the value for User spiked
  - Signature Value - an account was successfully logged into - coincides with User J
    - from 10AM - 1PM the value for User spiked

Screenshots of Attack Logs



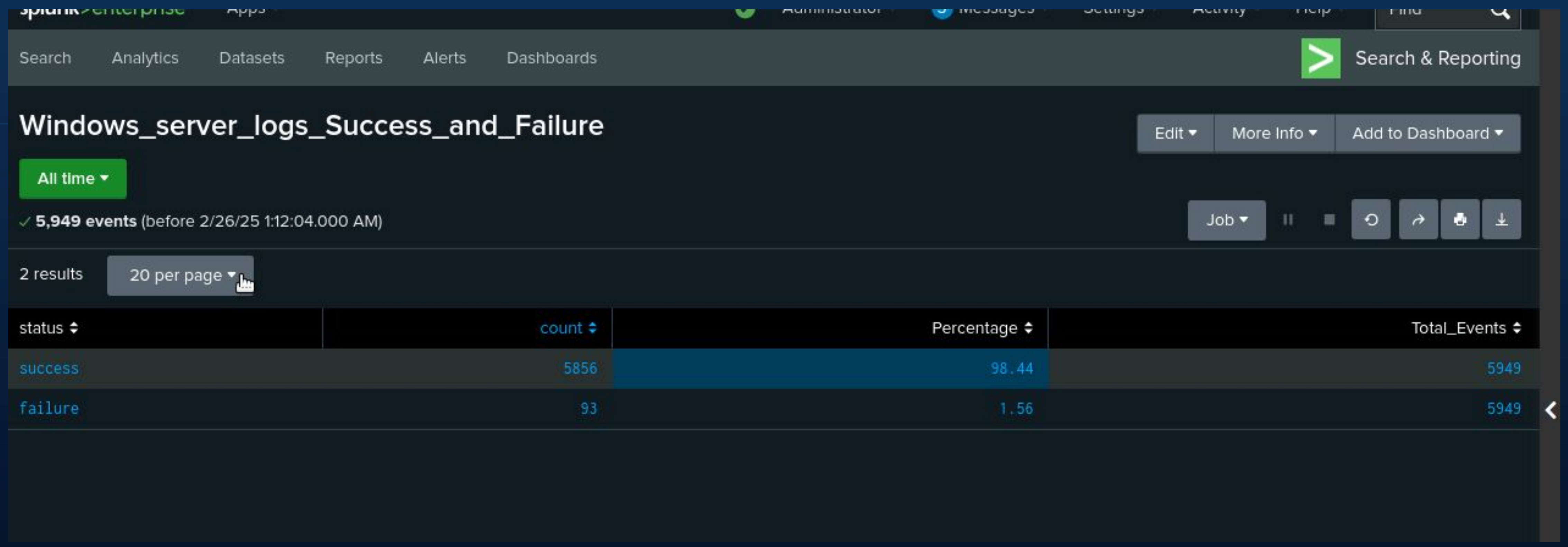


Windows_server_logs_Severity_levels_counts_and_percentage

✓ **5,949 events** (before 2/26/25 12:58:42.000 AM)

2 results

severity	Event_Count	Percentage
informational	4383	79.78
high	1111	20.22

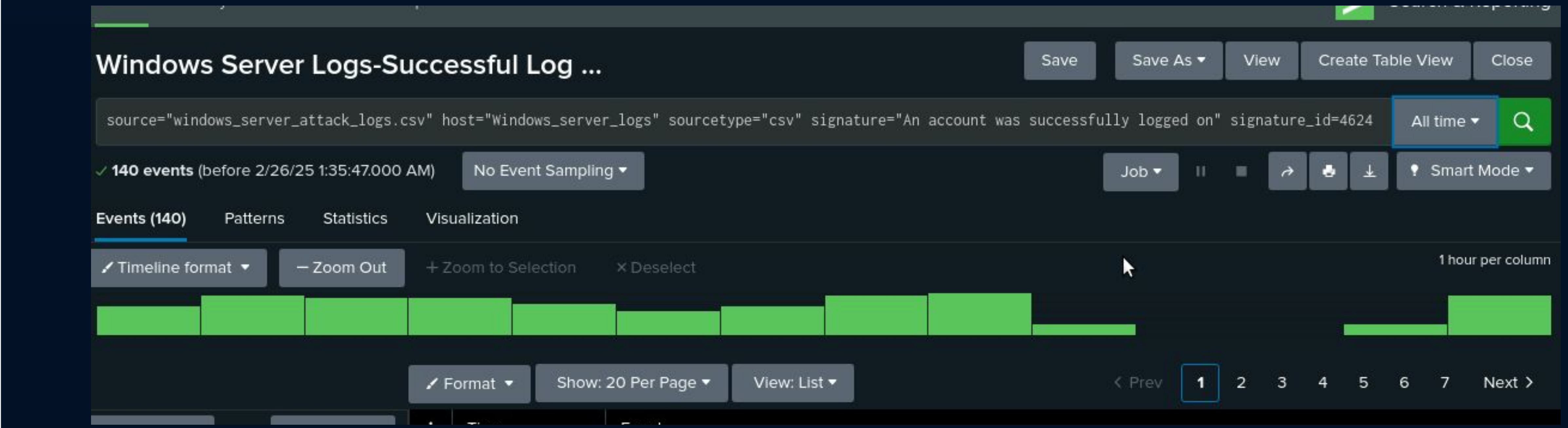


Windows_server_logs_Success_and_Failure

✓ **5,949 events** (before 2/26/25 1:12:04.000 AM)

2 results

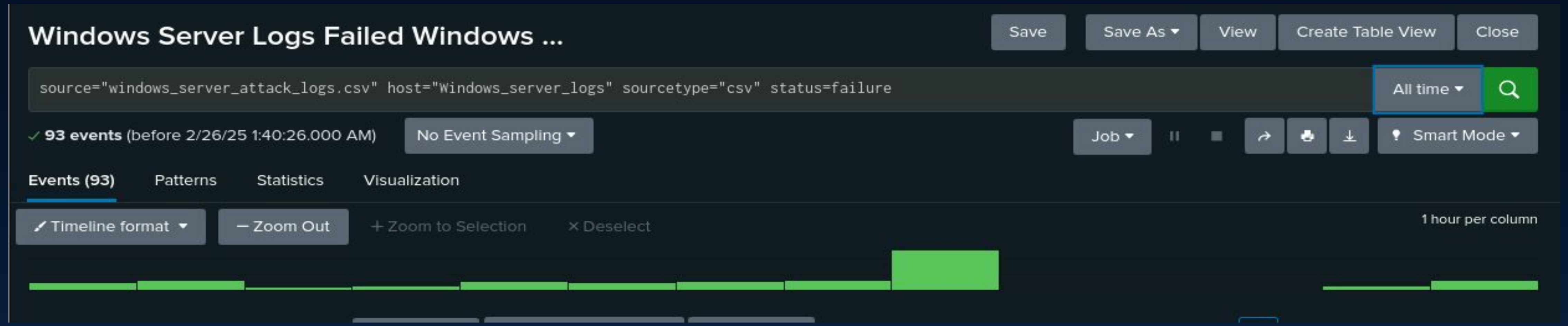
status	count	Percentage	Total_Events
success	5856	98.44	5949
failure	93	1.56	5949



Windows Server Logs-Successful Log ...

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" signature="An account was successfully logged on" signature_id=4624
```

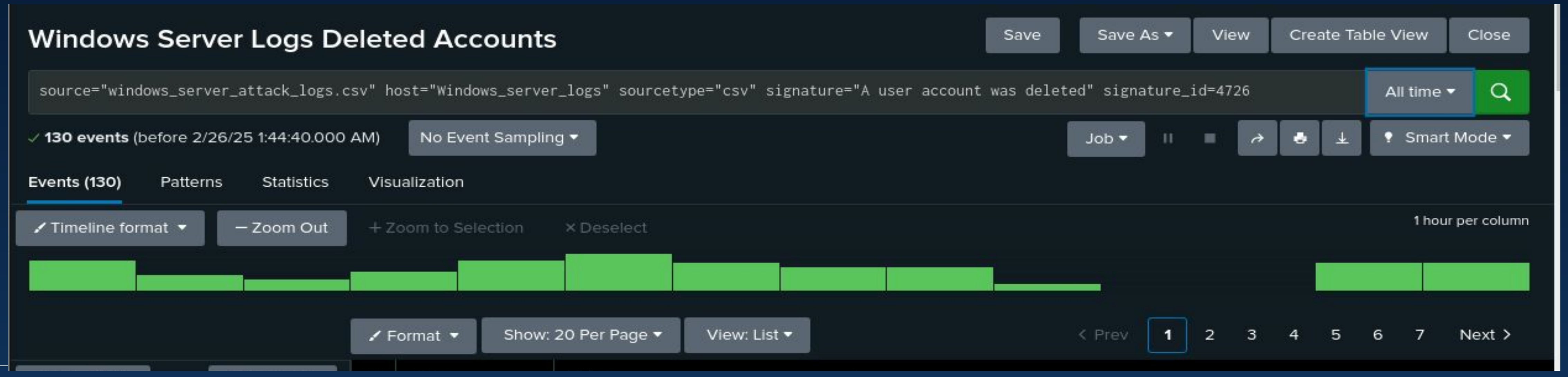
✓ **140 events** (before 2/26/25 1:35:47.000 AM)



Windows Server Logs Failed Windows ...

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" status=failure
```

✓ **93 events** (before 2/26/25 1:40:26.000 AM)



Windows Server Logs Deleted Accounts

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" signature="A user account was deleted" signature_id=4726
```

✓ **130 events** (before 2/26/25 1:44:40.000 AM)

Attack Summary — Apache

- VSI detected suspicious changes in the HTTP method, especially with POST. The POST method is used to transmit data to the server from the HTTP client. POST had an increase of 1218.

- We detected minor changes in the results. The last 5 on the domain list had a decrease in referrer domains. The HTTP response had changes in the response codes 404(Apache_logs:213,Apache_attack_logs:679 and 200(Apache_logs:9126, Apache_attack_logs:3746).

- Code 404 increased to 679 counts, while 200 decreased to 3746 counts.

Attack Summary — Apache

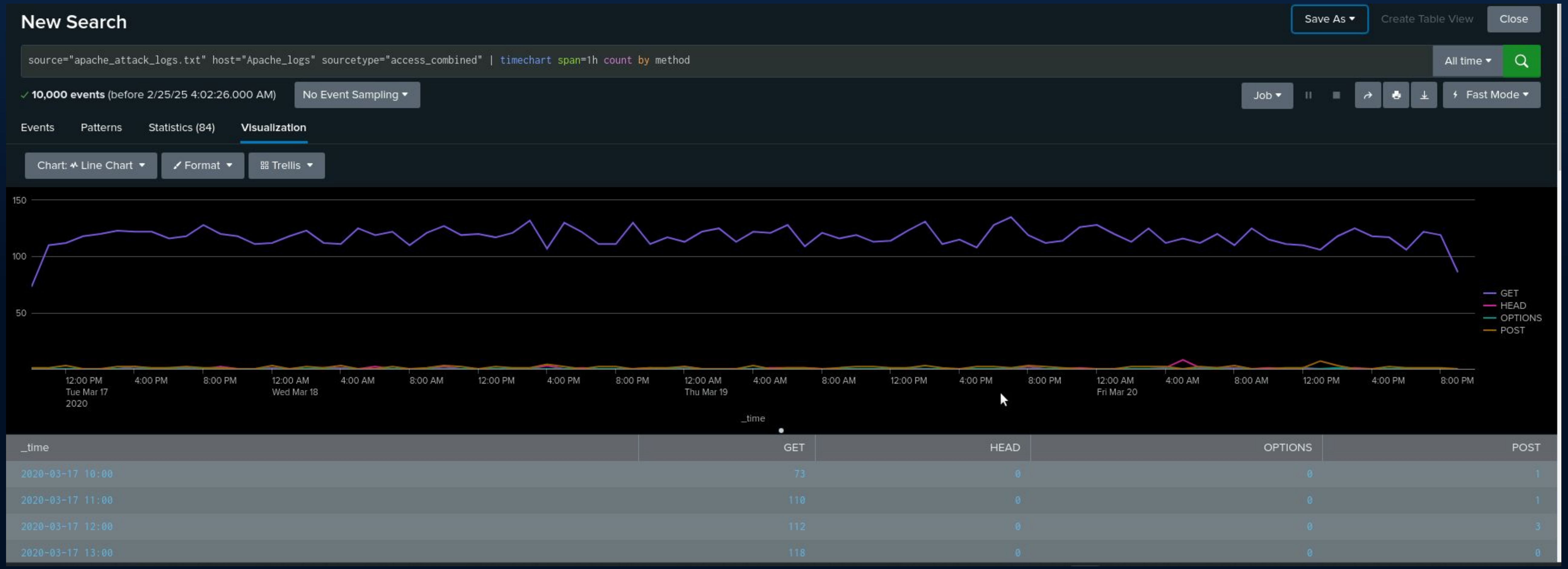
●URL Data-Activity increased on the VSI_Account_login.php. The URL that had the most hits, was /VSI_Accont_login.php, which shows a either a brute force attack or an SQL injections attack.

● HTTP Methods-Post method was used between the dates of 18Mar2020 to 20Mar2020 with a total count of 1324.

● Cluster Map-There was suspicious activity present coming from Kiev (438 counts) and Kharkiv (432 counts).

Screenshots of Attack Logs

HTTP Methods Attack Logs

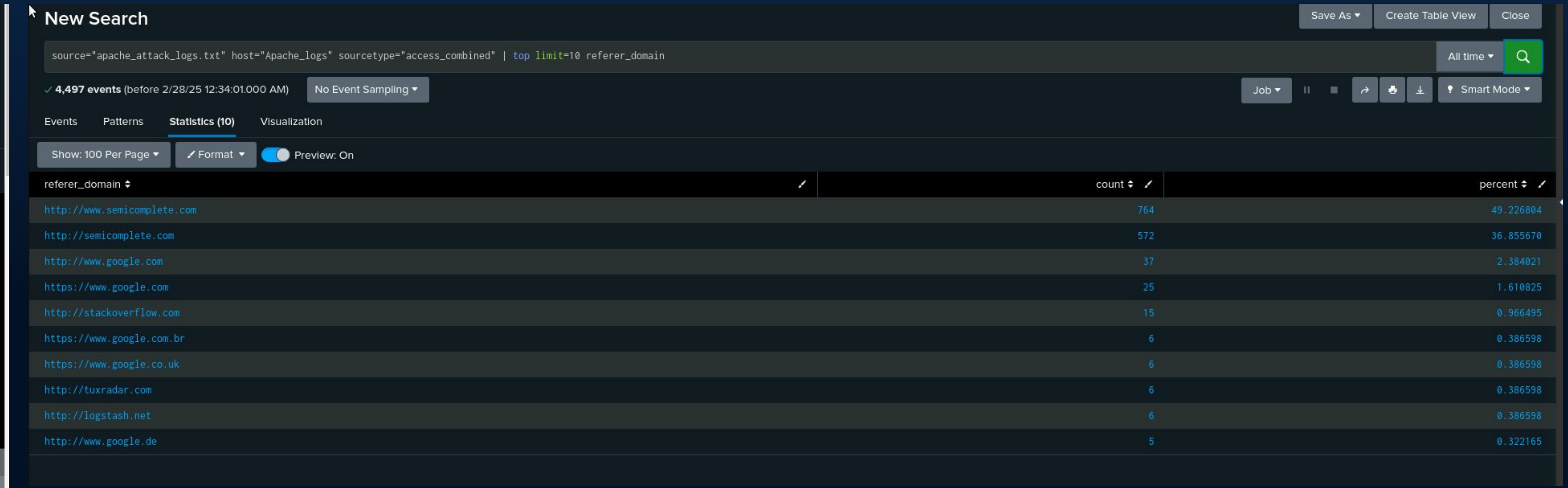


```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | timechart span=1h count by method
```

✓ **10,000 events** (before 2/25/25 4:02:26.000 AM)

_time	GET	HEAD	OPTIONS	POST
2020-03-17 10:00	73	0	0	1
2020-03-17 11:00	110	0	0	1
2020-03-17 12:00	112	0	0	3
2020-03-17 13:00	118	0	0	0

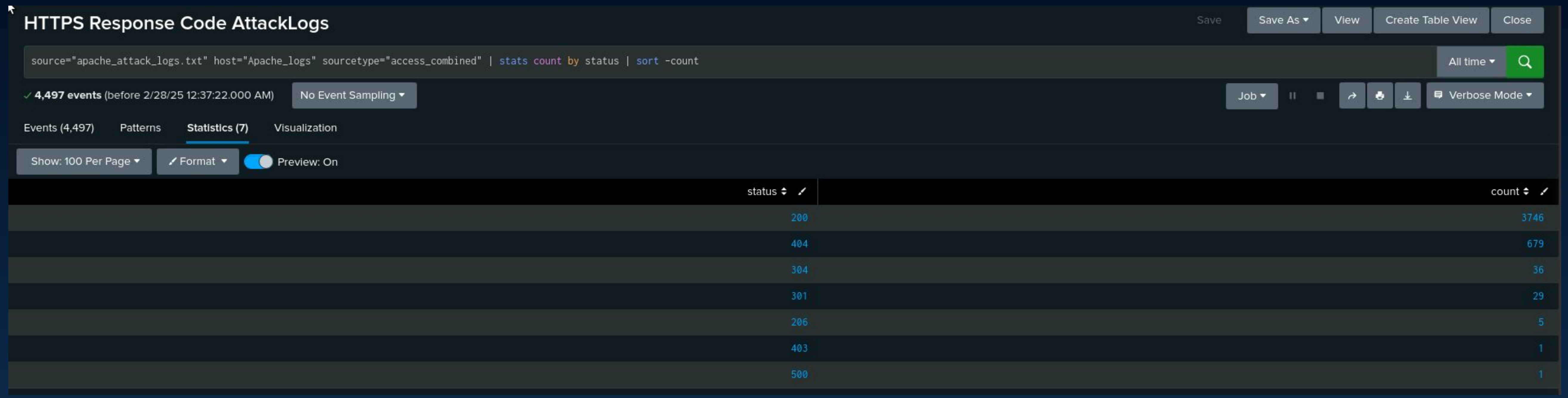
Referrer Domains Attack Logs



```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | top limit=10 referer_domain
```

✓ **4,497 events** (before 2/28/25 12:34:01.000 AM)

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

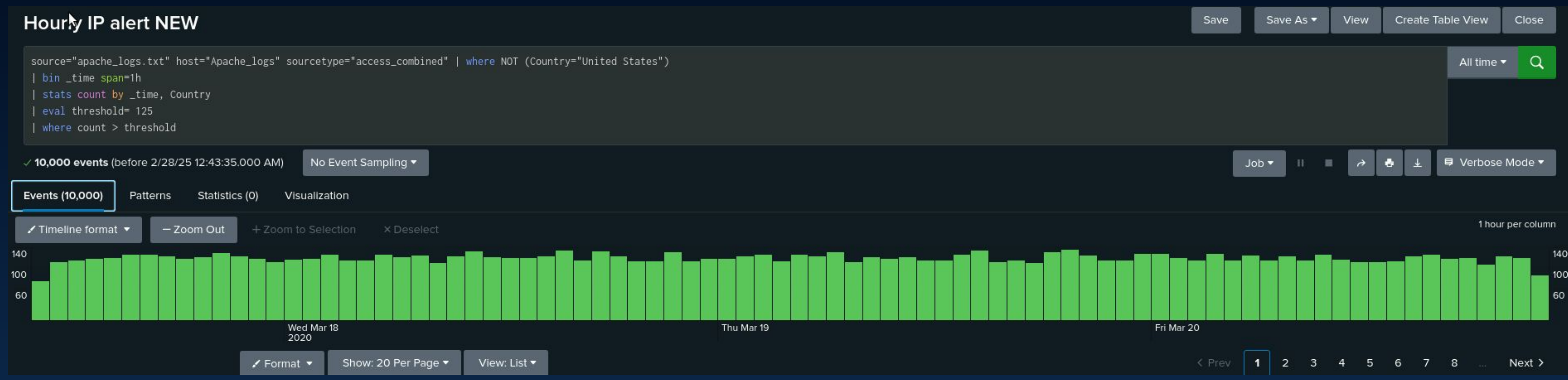


```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | stats count by status | sort -count
```

✓ **4,497 events** (before 2/28/25 12:37:22.000 AM)

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

HTTP Response Code Attack Logs



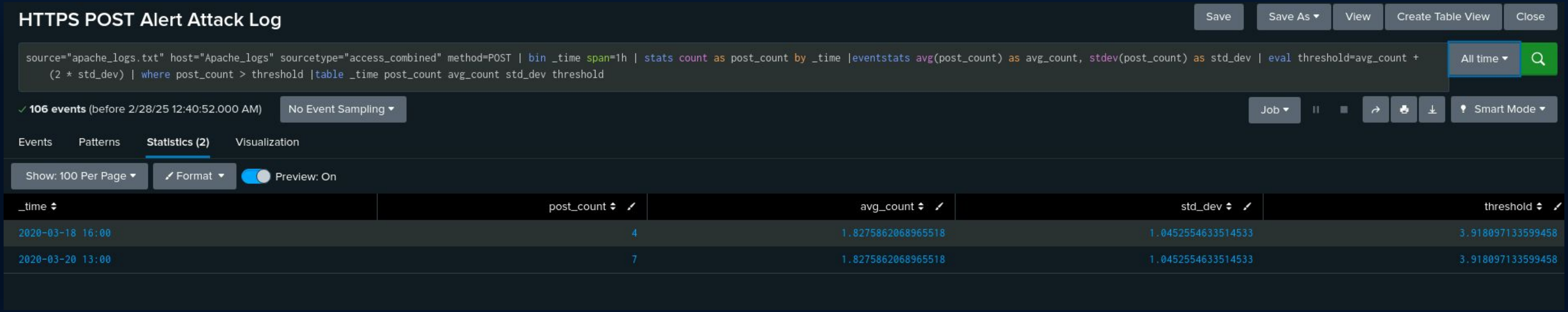
```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | where NOT (Country="United States")
| bin _time span=1h
| stats count by _time, Country
| eval threshold= 125
| where count > threshold
```

✓ **10,000 events** (before 2/28/25 12:43:35.000 AM)

International IP Attack Alert Log

Screenshots of Attack Logs Cont.

HTTP POST Attack Alert Log



HTTPS POST Alert Attack Log

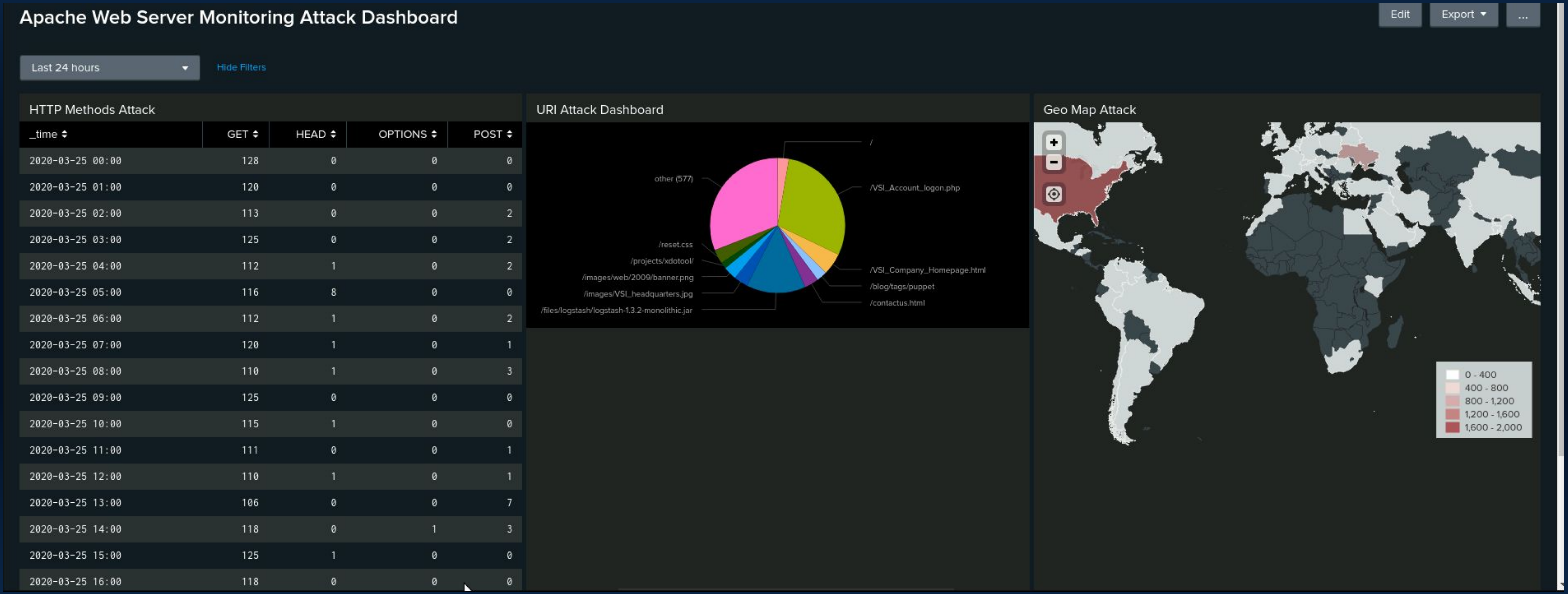
```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" method=POST | bin _time span=1h | stats count as post_count by _time |eventstats avg(post_count) as avg_count, stdev(post_count) as std_dev | eval threshold=avg_count +
    (2 * std_dev) | where post_count > threshold |table _time post_count avg_count std_dev threshold
```

✓ **106 events** (before 2/28/25 12:40:52.000 AM)

Statistics (2)

_time	post_count	avg_count	std_dev	threshold
2020-03-18 16:00	4	1.8275862068965518	1.0452554633514533	3.918097133599458
2020-03-20 13:00	7	1.8275862068965518	1.0452554633514533	3.918097133599458

Apache Attack Dashboard



Apache Web Server Monitoring Attack Dashboard

HTTP Methods Attack

_time ⬍	GET ⬍	HEAD ⬍	OPTIONS ⬍	POST ⬍
2020-03-25 00:00	128	0	0	0
2020-03-25 01:00	120	0	0	0
2020-03-25 02:00	113	0	0	2
2020-03-25 03:00	125	0	0	2
2020-03-25 04:00	112	1	0	2
2020-03-25 05:00	116	8	0	0
2020-03-25 06:00	112	1	0	2
2020-03-25 07:00	120	1	0	1
2020-03-25 08:00	110	1	0	3
2020-03-25 09:00	125	0	0	0
2020-03-25 10:00	115	1	0	0
2020-03-25 11:00	111	0	0	1
2020-03-25 12:00	110	1	0	1
2020-03-25 13:00	106	0	0	7
2020-03-25 14:00	118	0	1	3
2020-03-25 15:00	125	1	0	0
2020-03-25 16:00	118	0	0	0

URI Attack Dashboard

/
other (577)
/VSI_Account_logon.php
/reset.css
/projects/xdotool/
/images/web/2009/banner.png
/images/VSI_headquarters.jpg
/files/logstash/logstash-1.3.2-monolithic.jar
/VSI_Company_Homepage.html
/blog/tags/puppet
/contactus.html

Geo Map Attack

Summary and Future Mitigations

Project 3 Summary

Following our analysis of VSI's security logs, our team identified multiple cyberattacks targeting both the Windows operating system and Apache web server. The primary attack vector was brute-force password attempts from various regions and countries.

Proposed Mitigation Measures:

To enhance VSI's security posture and prevent future attacks, we recommend implementing the following measures:

- Account Lockout Policy – Automatically lock user accounts after three consecutive failed login attempts to prevent automated brute-force attacks.
- Two-Factor Authentication (2FA) – Enforce 2FA across all critical systems to add an additional layer of security beyond traditional passwords.

By implementing these measures, VSI can significantly reduce the risk of unauthorized access and strengthen authentication security.