Defensive Security Project
by: Andrew Boschini

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

You are a Security Operations Center (SOC) Analyst at Virtual Space Industries (VSI), a tech firm specializing in virtual-reality solutions for businesses.

Intelligence suggests that rival company **JobeCorp** may attempt to sabotage VSI's infrastructure via cyberattacks.

Your mission: **Monitor VSI's systems for threats** using Splunk.

You were provided logs from two key assets:

- A **Windows server** hosting sensitive IP related to next-gen VR technology.
- An **Apache web server** running VSI's public website and administrative tools.

Following a system outage, you received **attack-period logs** to analyze, compare with baselines, and detect malicious activity.

Your objective: Create actionable dashboards, alerts, and reports — and present your findings to executive leadership.

Splunk - Apache Web Server App

Splunk - Apache Web Server App

The *Web Server Add-On* enables Splunk to properly ingest and parse Apache access logs using the `access_combined` sourcetype. It extracts key HTTP fields such as `clientip`, `uri_path`, `method`, `status`, and `useragent`, allowing for enhanced visibility into web server activity. This add-on transforms raw log data into searchable fields to drive actionable insights and support security monitoring.

Splunk - Apache Web Server App

After deploying the Web Server Add-On, VSI’s SOC team noticed an unusually high number of HTTP POST requests from foreign IP addresses. Using the parsed method, status, and clientip fields, they correlated traffic spikes with failed authentication attempts. This led to the discovery of a brute-force attack targeting exposed web forms. Without the add-on, these fields would have remained buried in raw log strings, delaying incident response.

Splunk - Apache Web Server App

New Search
Save As ▾
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (4,497)
Visualization
Show: 20 Per Page ▾
Format ▾
Preview: On
‹ Prev
1
2
3
4
5
6
7
8
...
Next ›

```
sourcetype="access_combined"
| table _time clientip method uri_path status useragent
| sort _time
```

✓ 4,497 events (before 5/13/25 2:29:27.000 AM)

_time	clientip	method	uri_path	status	useragent
2020-03-25 00:05:00	130.237.218.86	GET	/presentations/logstash-provops/images/logstash.png	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
2020-03-25 00:05:00	130.237.218.86	GET	/presentations/logstash-provops/lib/css/zenburn.css	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
2020-03-25 00:05:00	130.237.218.86	GET	/presentations/unix-basics/	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
2020-03-25 00:05:00	82.80.14.189	GET	/presentations/logstash-monitorama-2013/images/apache-icon.gif	200	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2020-03-25 00:05:01	130.237.218.86	GET	/presentations/unix-basics/images/metacity-gnome.png	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
2020-03-25 00:05:01	82.80.14.189	GET	/presentations/logstash-monitorama-2013/images/Dreamhost_logo.svg	200	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2020-03-25 00:05:01	106.78.19.160	GET	/presentations/mpi	301	LAVA.KKT35+.FARSIGHTED60D_CN_11B_HW (MAUI/KKT35_S116_20130820;BDATE/2013/08/20 14:41;LCD/240320;CHIP/MT6260;KEY/Normal;TOUCH/0;CAMERA/1;SENSOR/0;DEV/FARSIGHTED60D_CN_11B_HW;WAP Browser/MAUI (HTTPS)) LAVA_KKT35_S116_20130820 Release/2013.08.20 WAP Browser/MAUI (HTTPS) Profile/ Q03C1-2.40 en-US
2020-03-25 00:05:02	82.80.14.189	GET	/presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js	200	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2020-03-25 00:05:03	82.80.14.189	GET	/presentations/logstash-monitorama-2013/lib/js/head.min.js	200	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2020-03-25 00:05:04	130.237.218.86	GET	/presentations/logstash-provops/js/jquery.min.js	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36

Logs Analyzed

1 Windows Logs

These logs contain event data from the Windows operating system running VSI's critical backend services. The logs include:

- **Security events**: Successful and failed logon attempts, privilege escalations
- **System alerts**: Service failures, restart events
- **Audit trails**: Access to sensitive files and registry changes
  These logs helped identify unauthorized access attempts and suspicious behavior on core systems.

2 Apache Logs

Apache web server logs track all web traffic to and from VSI's public-facing portal. They include:

- **HTTP method activity**: GET, POST, OPTIONS, HEAD requests
- **Status codes**: Success (200), client errors (404), server errors (500), and more
- **IP geolocation**: Client IP addresses mapped to countries and cities
- **URI access patterns**: Repeated hits on specific endpoints like `/VSI_Account_logon.php`
  These logs helped detect suspicious POST floods and foreign-origin traffic spikes.

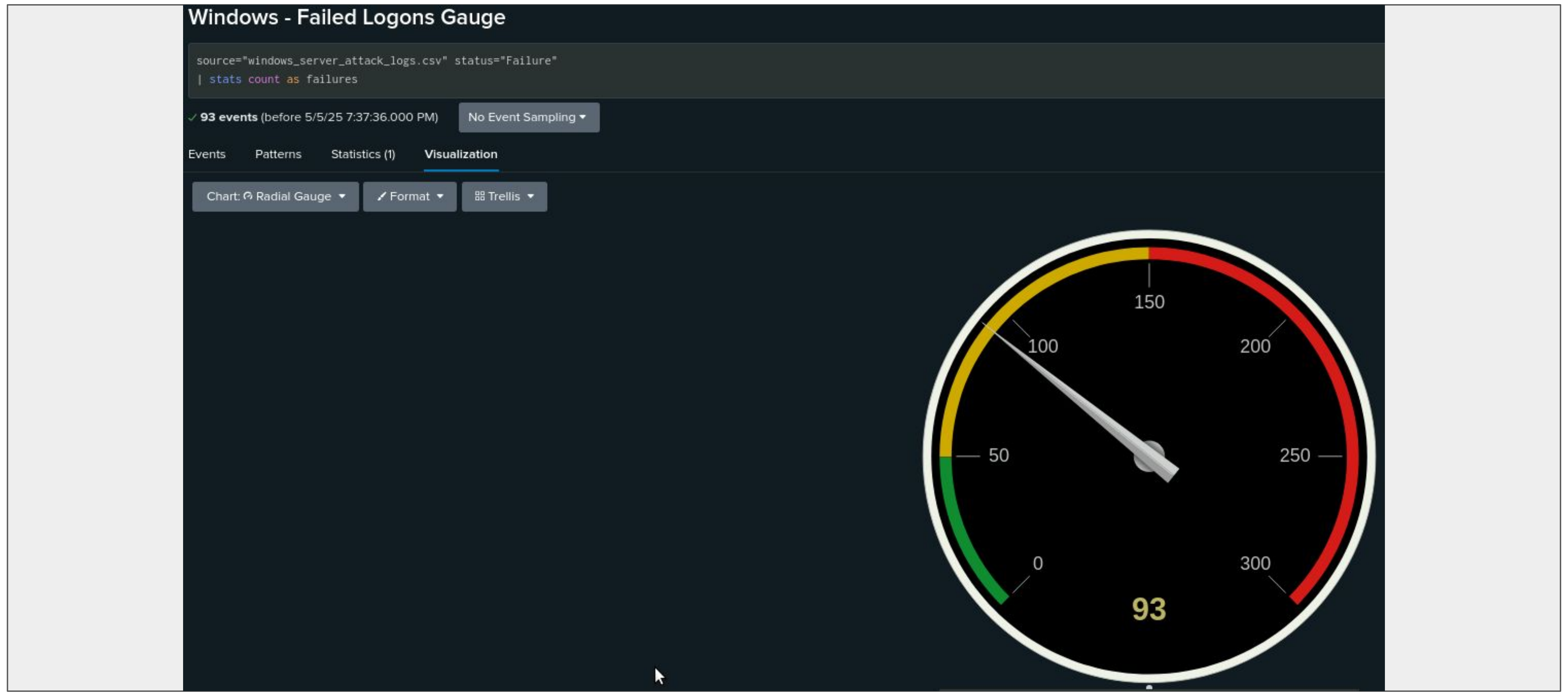
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Windows - Failed Logons Gauge	Visual indicator showing spikes in failed login attempts, helping detect brute-force activity.
Windows - Severity Breakdown Report	Categorizes events by severity level to quickly identify critical threats.
Windows - Signature Trends Over Time	Tracks the frequency of event signatures, revealing abnormal patterns or attack trends.
Windows - User Activity Over Time	Displays user login behavior across time to highlight anomalies in account usage.

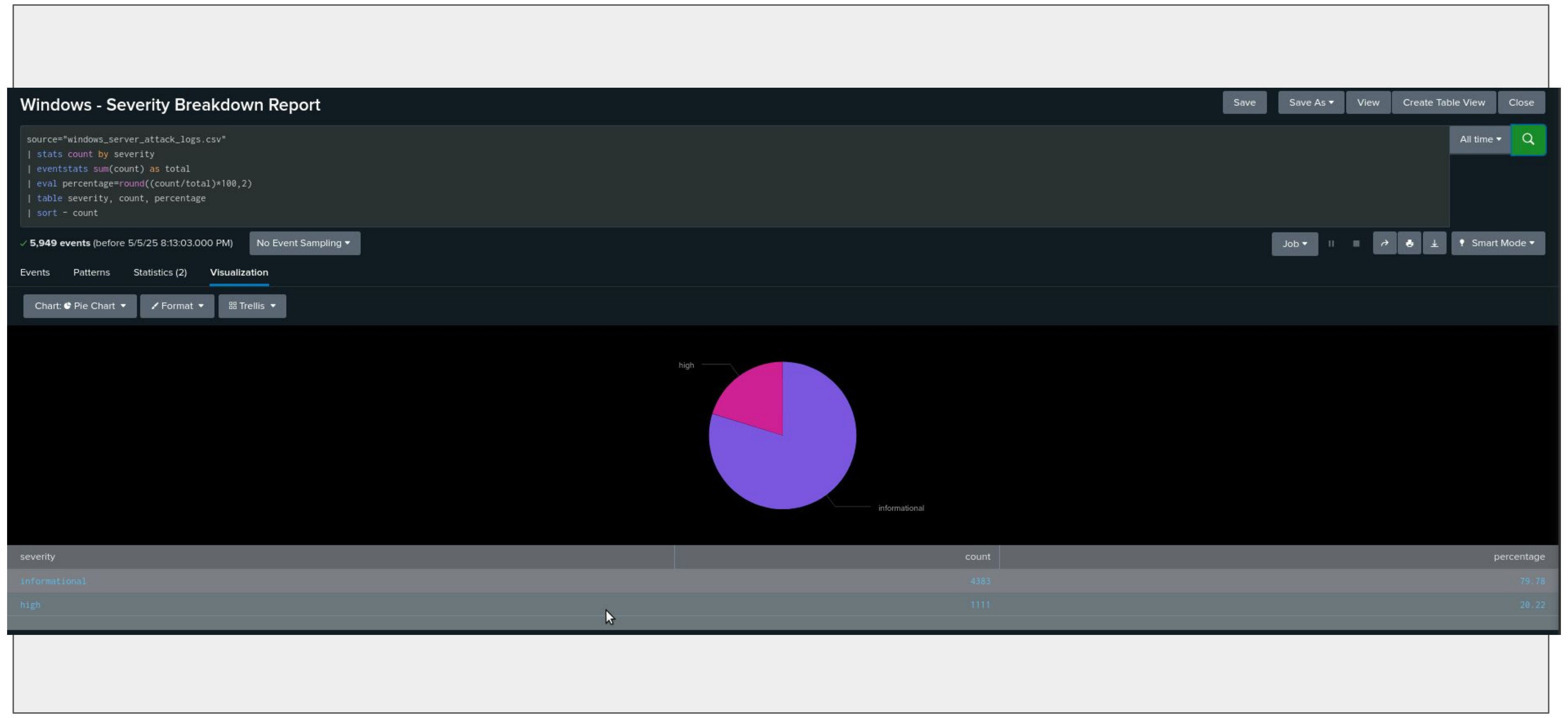
Images of Reports—Windows



Windows - Failed Logons Gauge

```
source="windows_server_attack_logs.csv" status="Failure"
| stats count as failures
```

✓ **93 events** (before 5/5/25 7:37:36.000 PM)

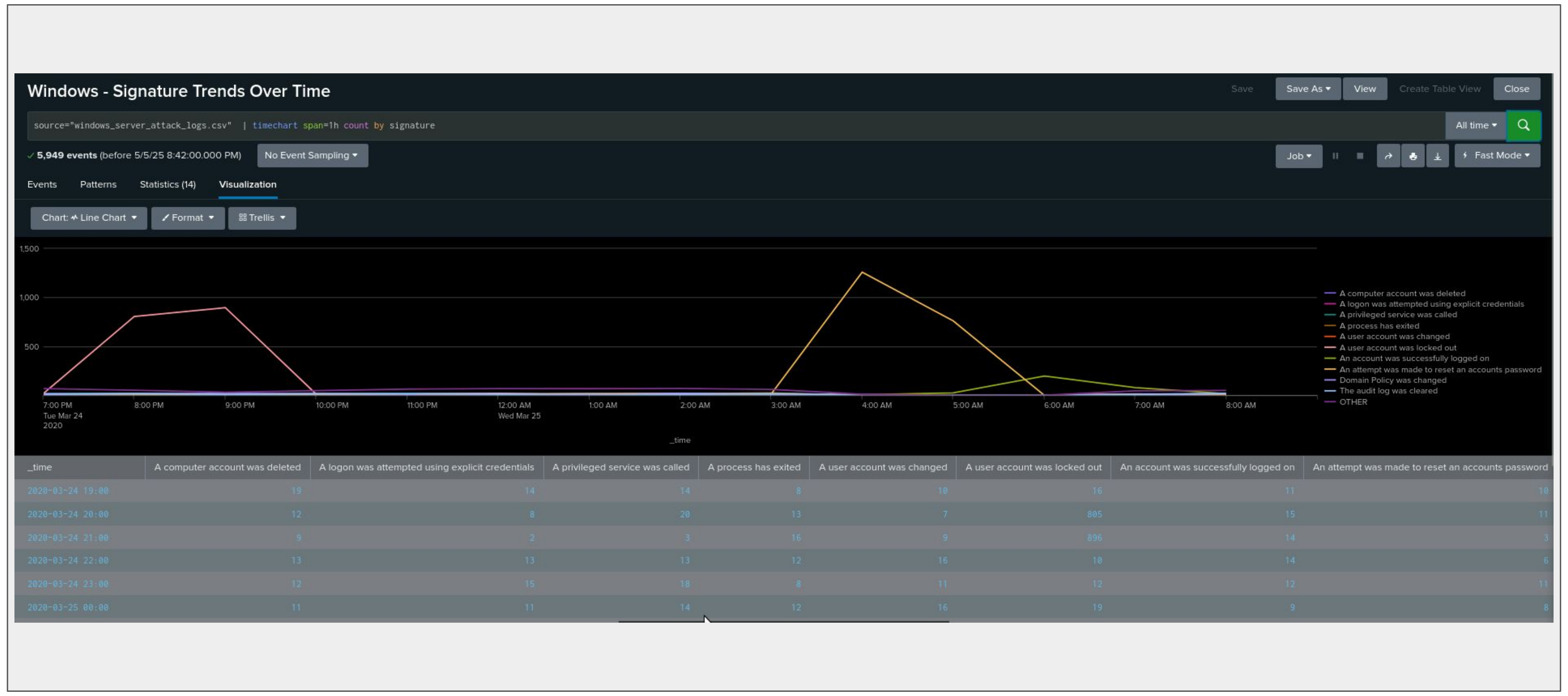


Windows - Severity Breakdown Report

```
source="windows_server_attack_logs.csv"
| stats count by severity
| eventstats sum(count) as total
| eval percentage=round((count/total)*100,2)
| table severity, count, percentage
| sort - count
```

✓ **5,949 events** (before 5/5/25 8:13:03.000 PM)

severity	count	percentage
informational	4383	79.78
high	1111	20.22

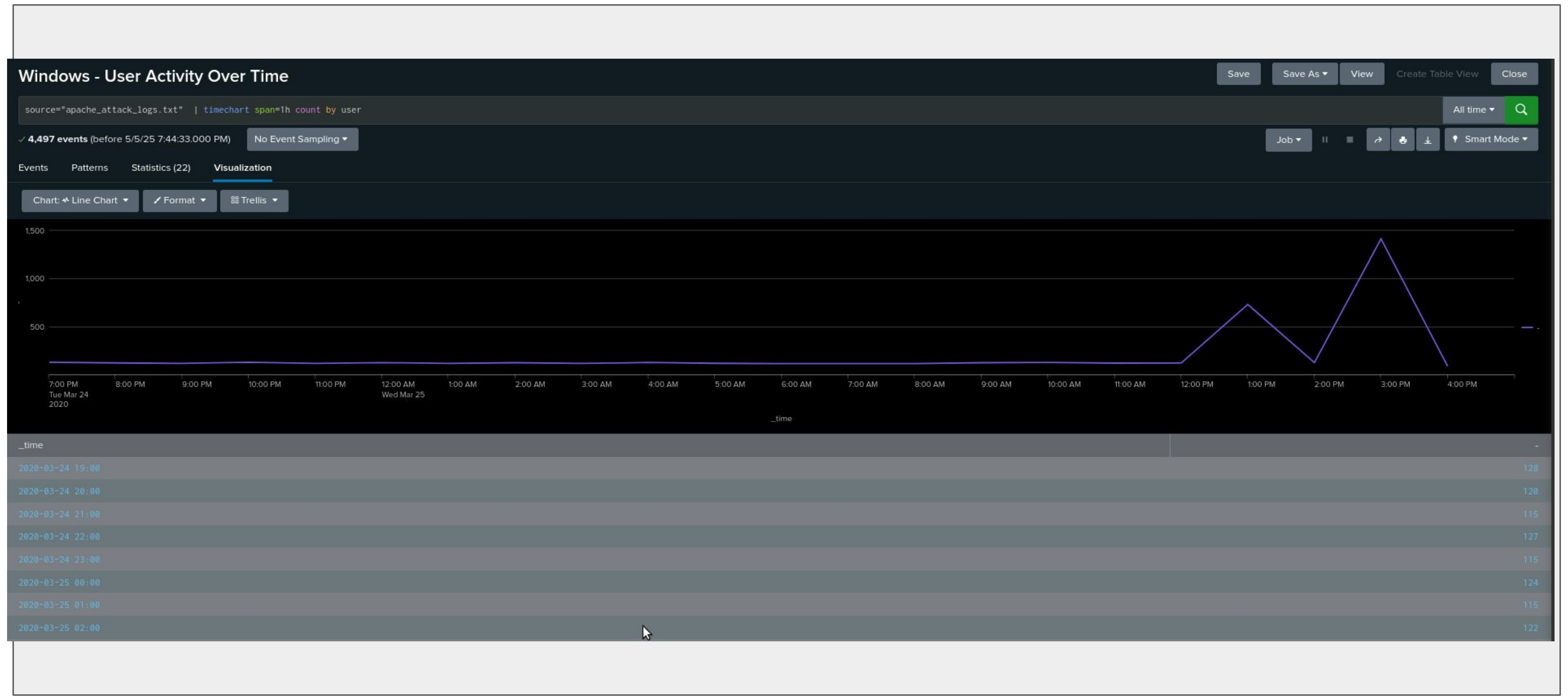


Windows - Signature Trends Over Time

```
source="windows_server_attack_logs.csv"  | timechart span=1h count by signature
```

✓ **5,949 events** (before 5/5/25 8:42:00.000 PM)

_time	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 locked out	An account was successfully logged on	An attempt was made to reset an accounts password
2020-03-24 19:00	19	14	14	8	10	16	11	10
2020-03-24 20:00	12	8	20	13	7	805	15	11
2020-03-24 21:00	9	2	3	16	9	896	14	3
2020-03-24 22:00	13	13	13	12	16	10	14	6
2020-03-24 23:00	12	15	18	8	11	12	12	11
2020-03-25 00:00	11	11	14	12	16	19	9	8



Windows - User Activity Over Time

```
source="apache_attack_logs.txt"  | timechart span=1h count by user
```

✓ **4,497 events** (before 5/5/25 7:44:33.000 PM)

_time	-
2020-03-24 19:00	128
2020-03-24 20:00	120
2020-03-24 21:00	115
2020-03-24 22:00	127
2020-03-24 23:00	115
2020-03-25 00:00	124
2020-03-25 01:00	115
2020-03-25 02:00	122

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Logons Spike	Detects spikes in failed login attempts to identify potential brute-force activity.	<10/hr	>20/hr

Baselines were established through historical log analysis. The "Excessive Failures" alert uses a conservative threshold (>10 failures/hour) to reduce noise while still detecting abnormal system behavior. Each alert threshold reflects a deviation from typical system patterns observed during baseline periods, allowing timely detection without generating false positives.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive Successful Logons (4624)	Detects unusually high successful login activity, which may indicate credential abuse.	~20/hr	≥40/hr

Each alert was based on analyzing log trends to determine normal activity levels. An unusually high number of successful logons (Event ID 4624) may suggest a compromised account being used repeatedly. By setting the threshold to ≥40/hr, we aim to detect potential misuse while minimizing false positives from regular login traffic.

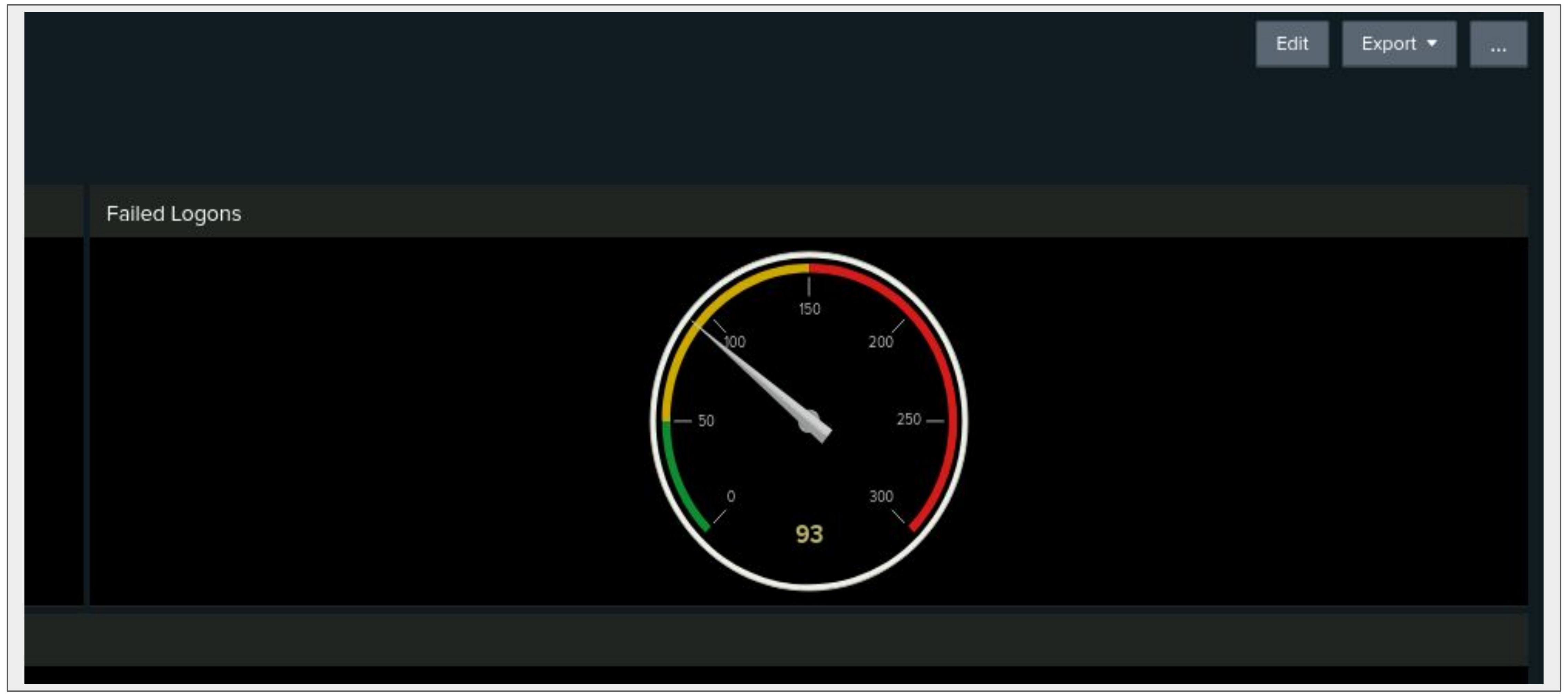
Alerts—Windows

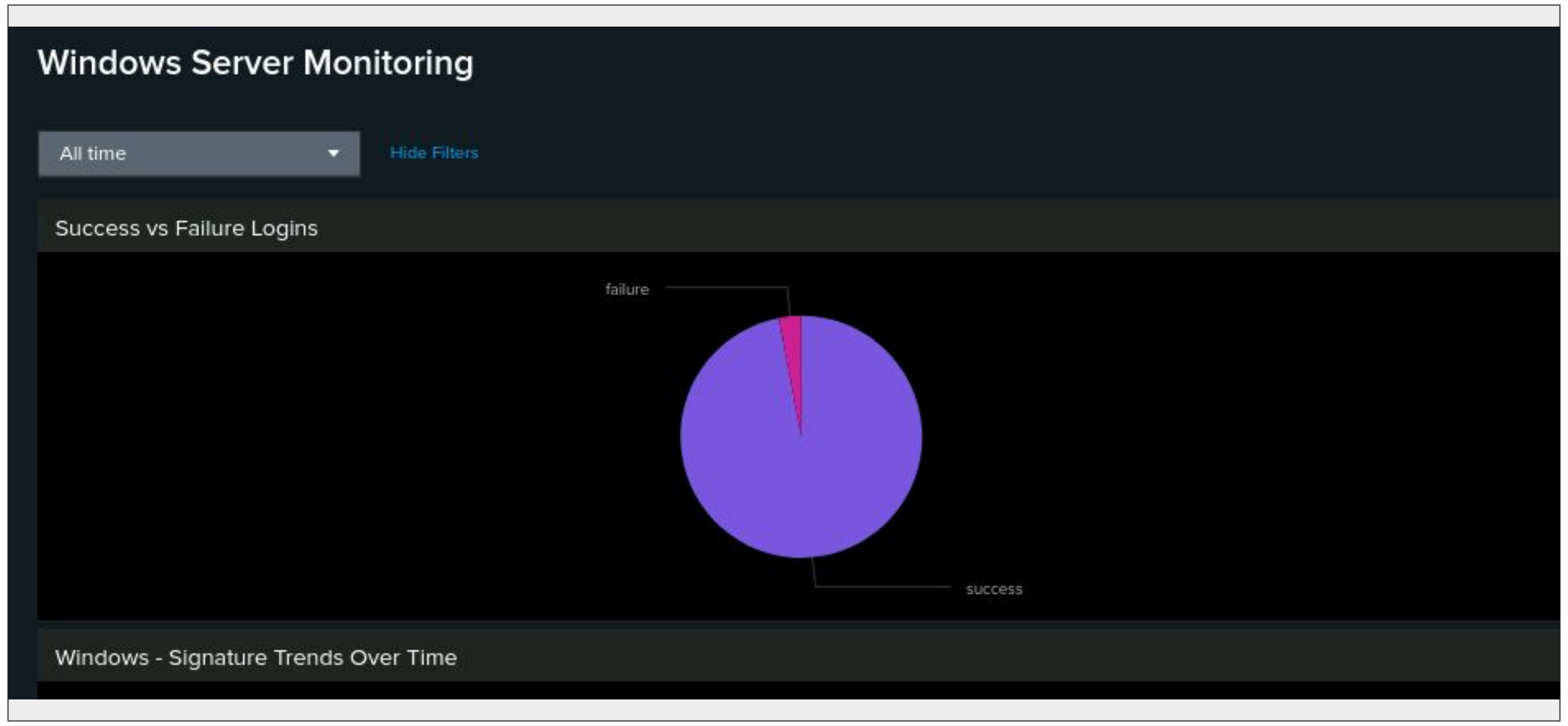
Designed the following alerts:

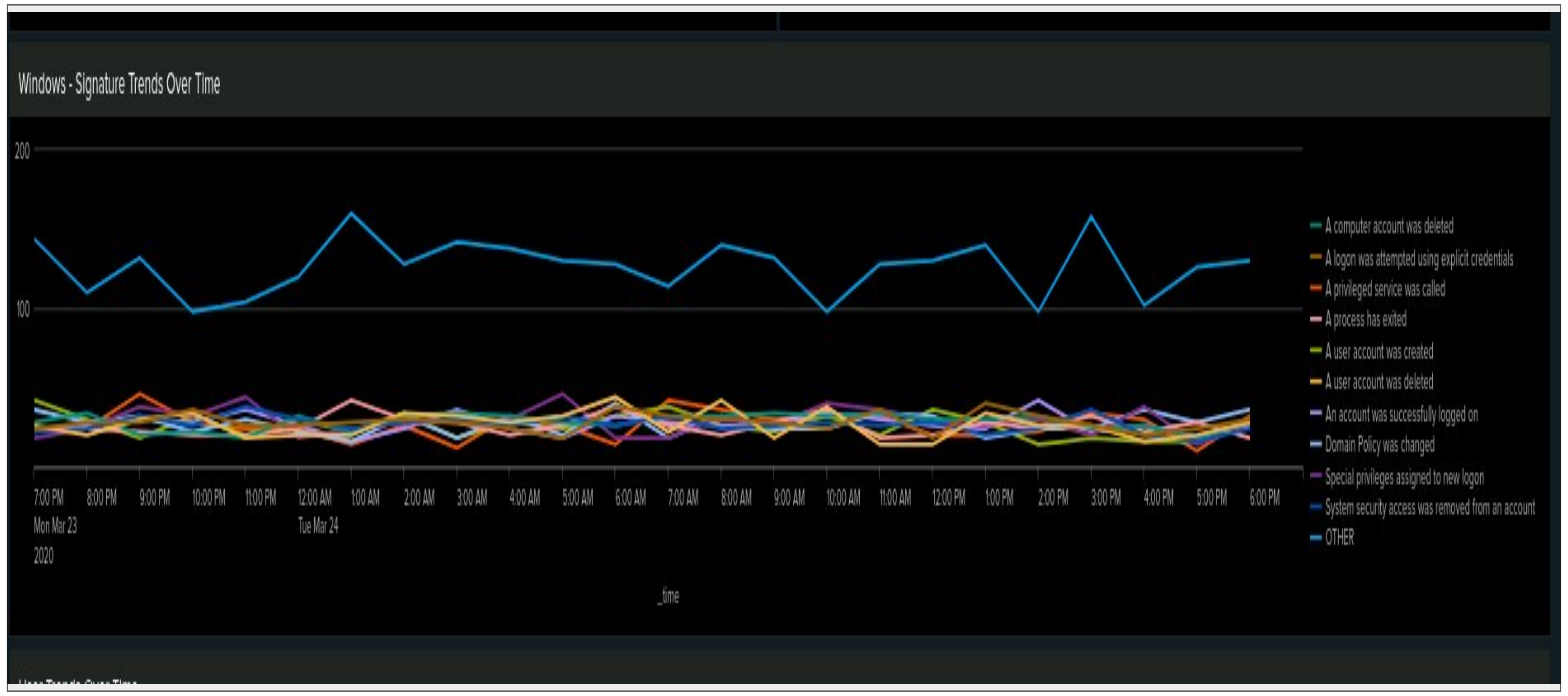
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive User Deletions (4726)	Triggers when there's a sudden increase in user account deletions, suggesting abuse.	0–3/hr	>5/hr

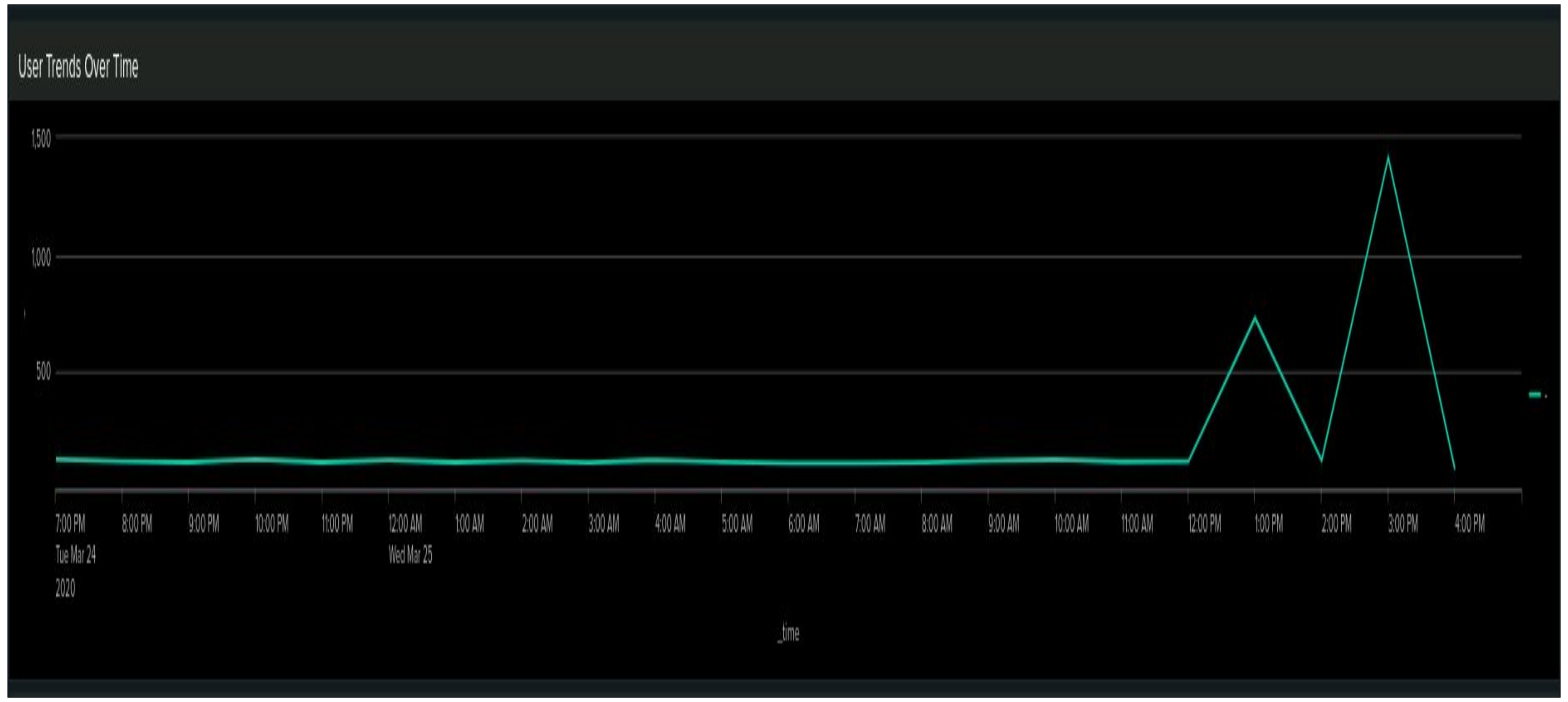
The selected alerts focus on potential signs of credential misuse and insider threats. Event ID 4726 — user deletions — is particularly concerning as it may indicate privilege abuse or attacker clean-up. Thresholds were based on normal server activity patterns with an emphasis on reducing false positives while ensuring we catch abnormal behavior early.

Dashboards—Windows

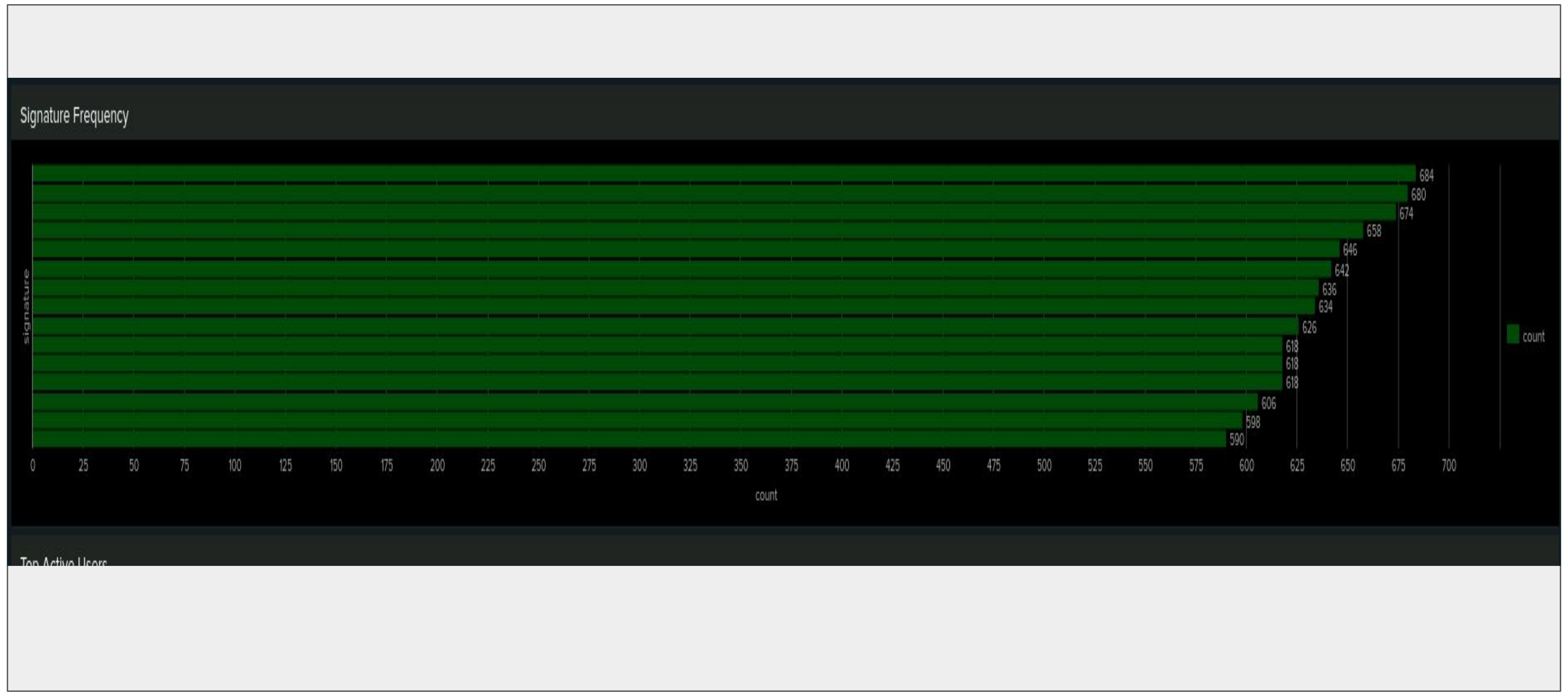


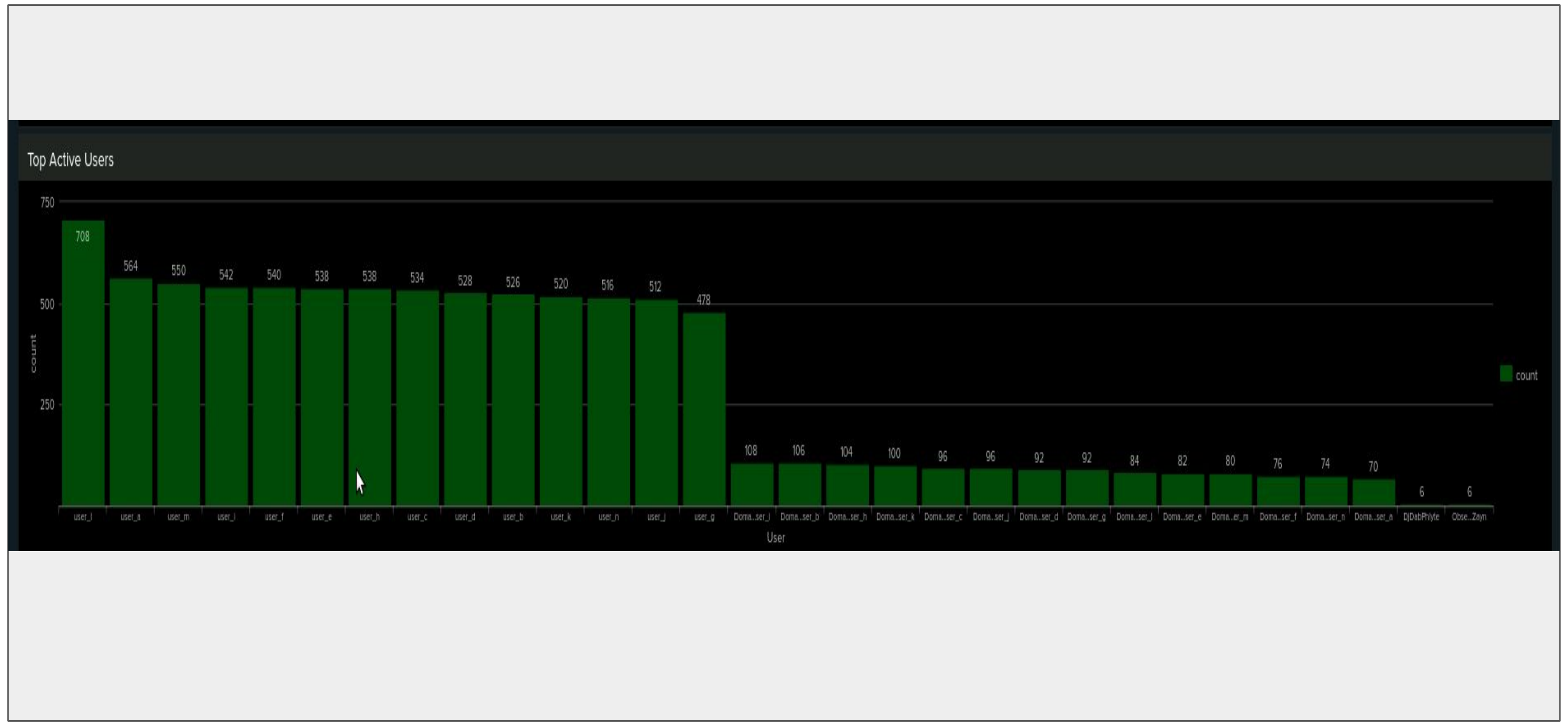

Windows Server Monitoring
All time ▾
Hide Filters
Success vs Failure Logins
failure
success
Windows - Signature Trends Over Time

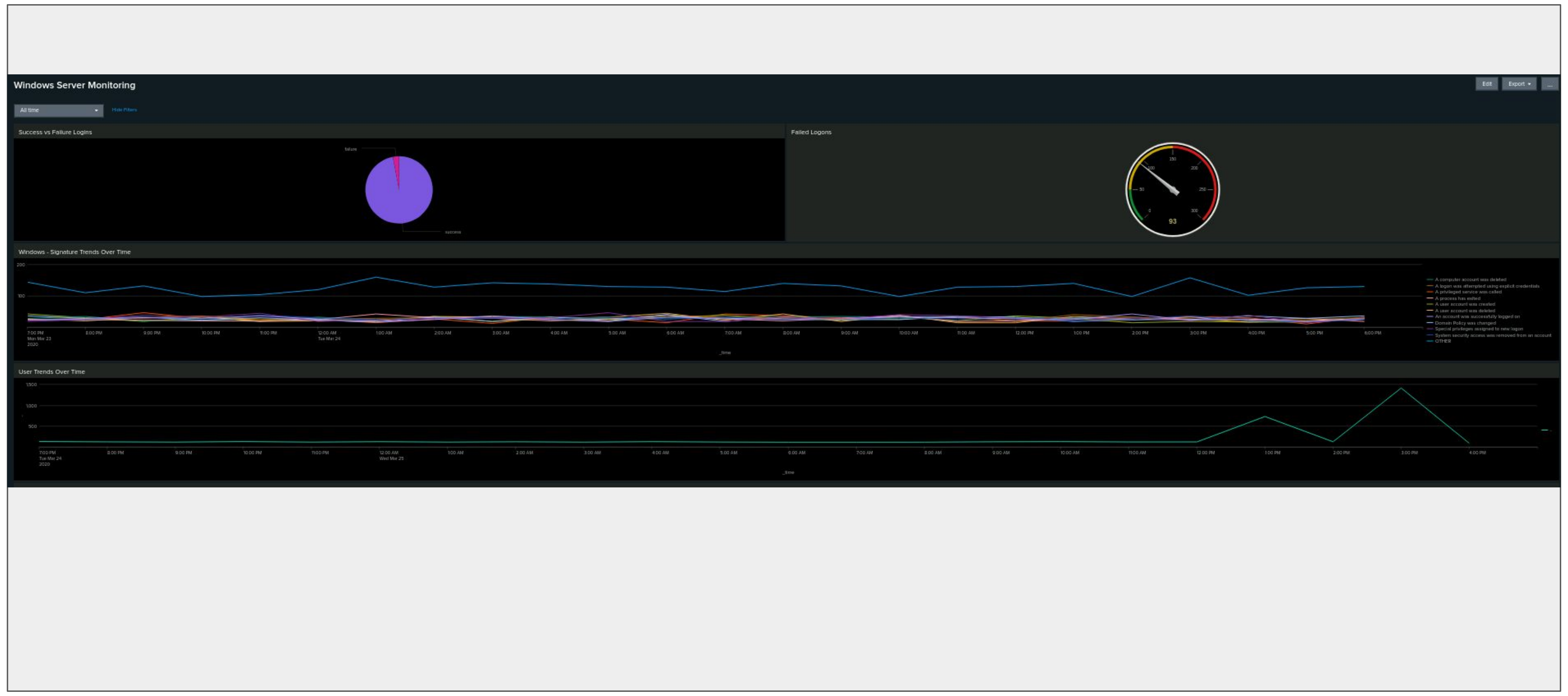

Windows - Signature Trends Over Time
200
100
7:00 PM
Mon Mar 23
2020
8:00 PM
9:00 PM
10:00 PM
11:00 PM
12:00 AM
Tue Mar 24
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
2:00 PM
3:00 PM
4:00 PM
5:00 PM
6:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER
User Trends Over Time

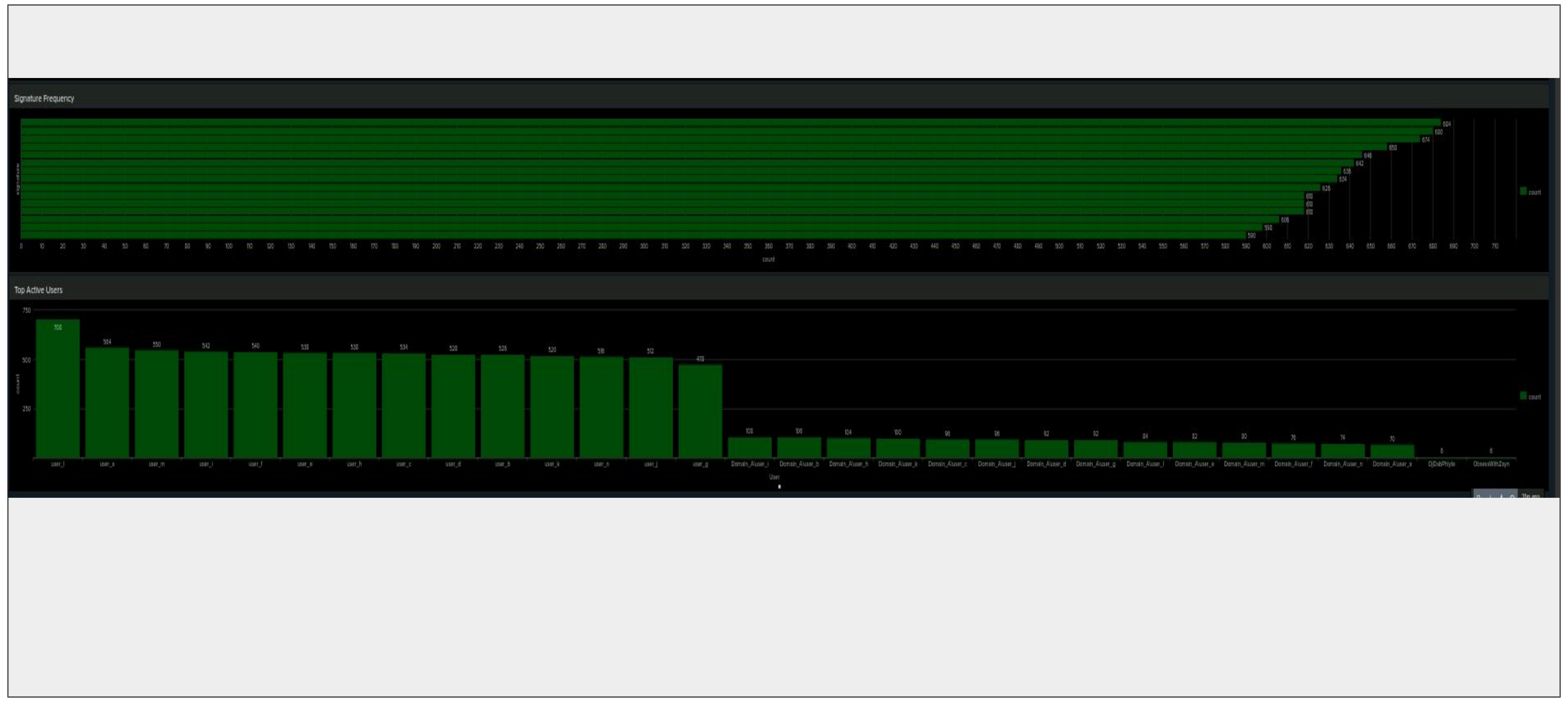


Dashboards—Windows






Windows Server Monitoring
Edit
Export ▾
...
All time
Hide Filters
Success vs Failure Logins
failure
success
Failed Logons
93
Windows - Signature Trends Over Time
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 created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER
_time
User Trends Over Time
1500
1000
500
_time



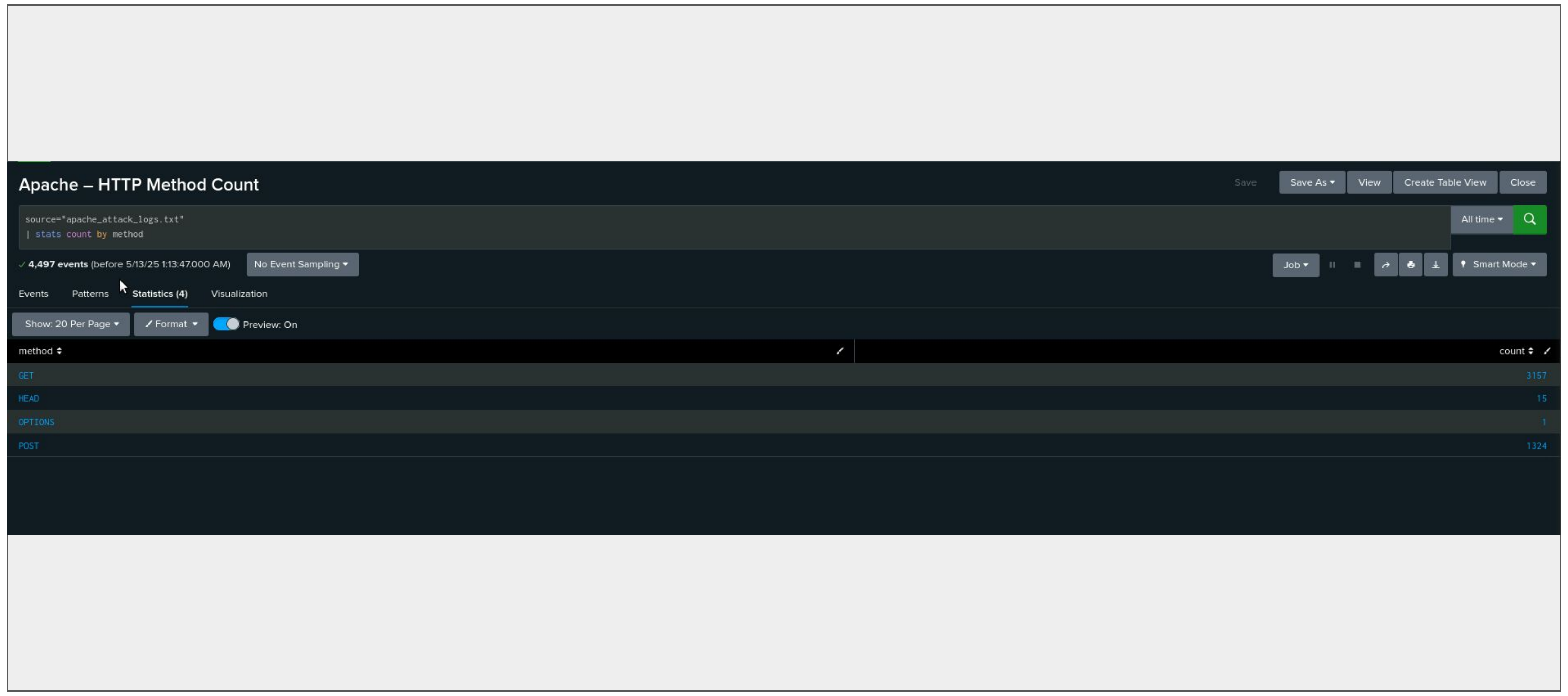
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
Apache – HTTP Method Count	Displays a table of HTTP method types (e.g., GET, POST, HEAD) and their frequency within the Apache attack logs. This report helps identify common and potentially suspicious HTTP activity on VSI's public web server.
Apache – Top 10 Referrer Domains	Identifies the top 10 external domains that directed traffic to VSI's web server. This helps detect unusual or potentially malicious referral patterns that may indicate an ongoing reconnaissance or redirection attack.
Apache – HTTP Response Code Count	Displays the count of HTTP response status codes (e.g., 200, 404, 500) returned by VSI's web server. This report helps identify abnormal levels of failed or error responses, which may indicate attack activity or system misconfiguration.

Images of Reports—Apache

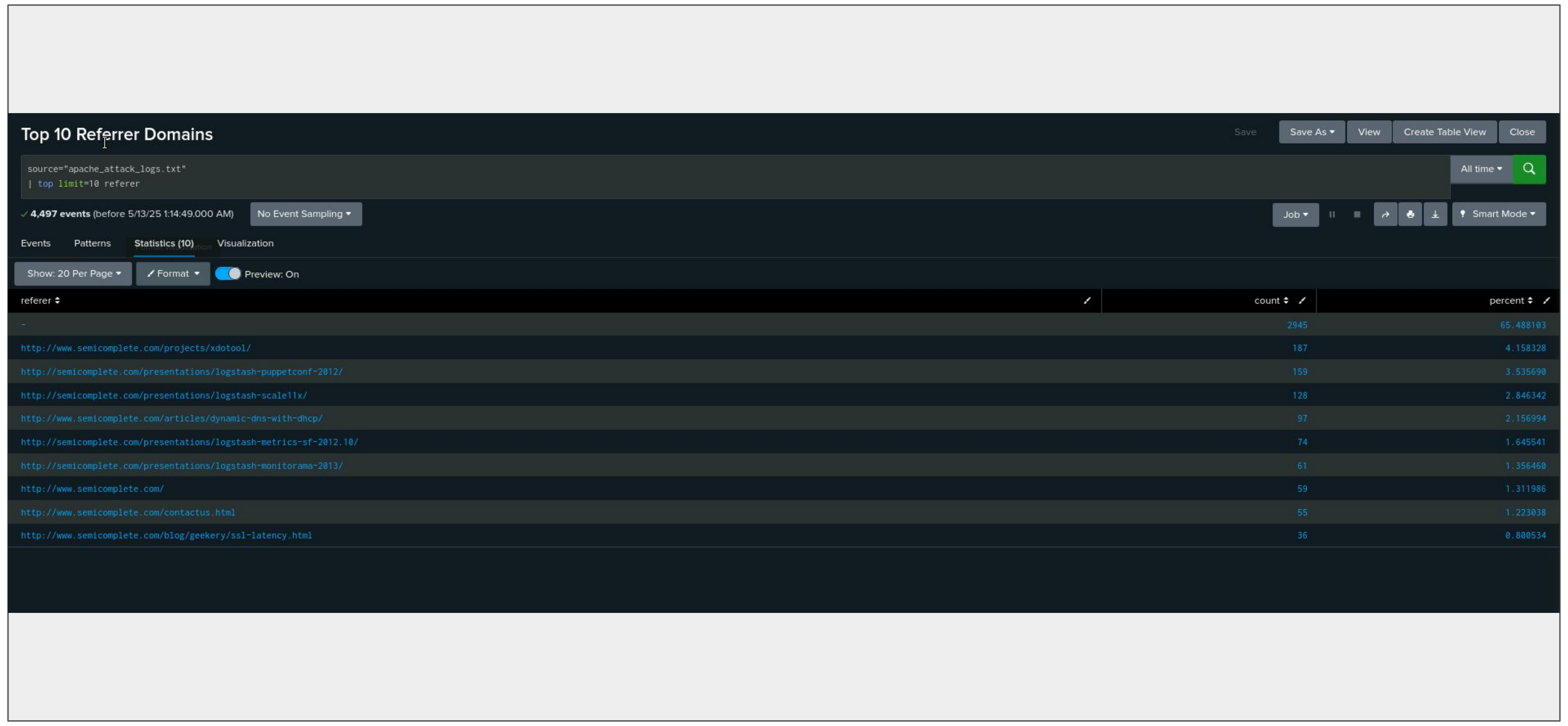


Apache – HTTP Method Count

```
source="apache_attack_logs.txt"
| stats count by method
```

✓ **4,497 events** (before 5/13/25 1:13:47.000 AM)

method	count
GET	3157
HEAD	15
OPTIONS	1
POST	1324

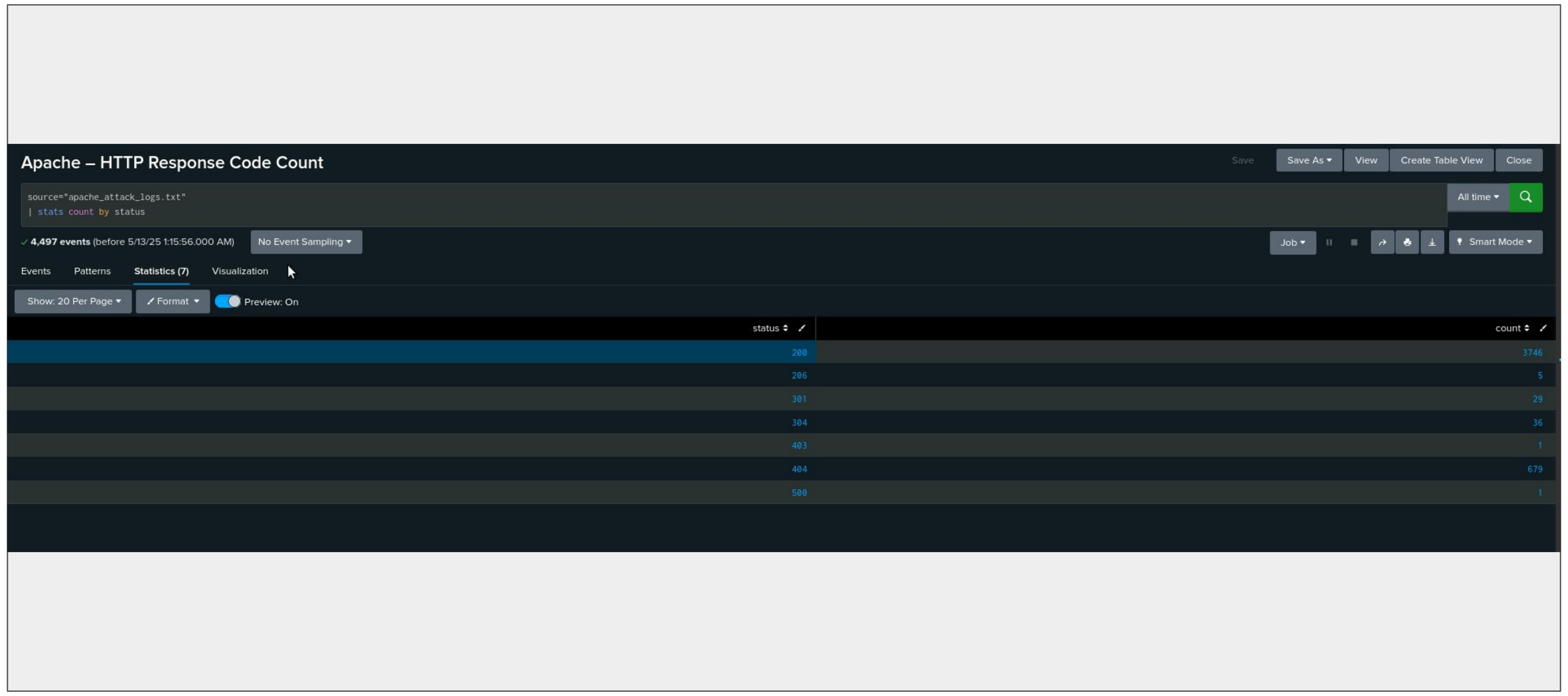


Top 10 Referrer Domains

```
source="apache_attack_logs.txt"
| top limit=10 referer
```

✓ **4,497 events** (before 5/13/25 1:14:49.000 AM)

referer	count	percent
-	2945	65.488103
http://www.semicomplete.com/projects/xdotool/	187	4.158328
http://semicomplete.com/presentations/logstash-puppetconf-2012/	159	3.535690
http://semicomplete.com/presentations/logstash-scale11x/	128	2.846342
http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/	97	2.156994
http://semicomplete.com/presentations/logstash-metrics-sf-2012.10/	74	1.645541
http://semicomplete.com/presentations/logstash-monitorama-2013/	61	1.356460
http://www.semicomplete.com/	59	1.311986
http://www.semicomplete.com/contactus.html	55	1.223038
http://www.semicomplete.com/blog/geekery/ssl-latency.html	36	0.800534



Apache – HTTP Response Code Count

```
source="apache_attack_logs.txt"
| stats count by status
```

✓ **4,497 events** (before 5/13/25 1:15:56.000 AM)

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

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Foreign Traffic Spike	Detects a high volume of traffic from countries other than the U.S. within 1 hour.	80 requests/hour	100 requests/hour

JUSTIFICATION: The baseline of 80 was determined by analyzing 24-hour traffic logs and observing typical hourly volume from non-U.S. countries. The threshold was raised to 100 to allow a margin for normal fluctuations while still detecting meaningful spikes that could represent reconnaissance or a coordinated attack.

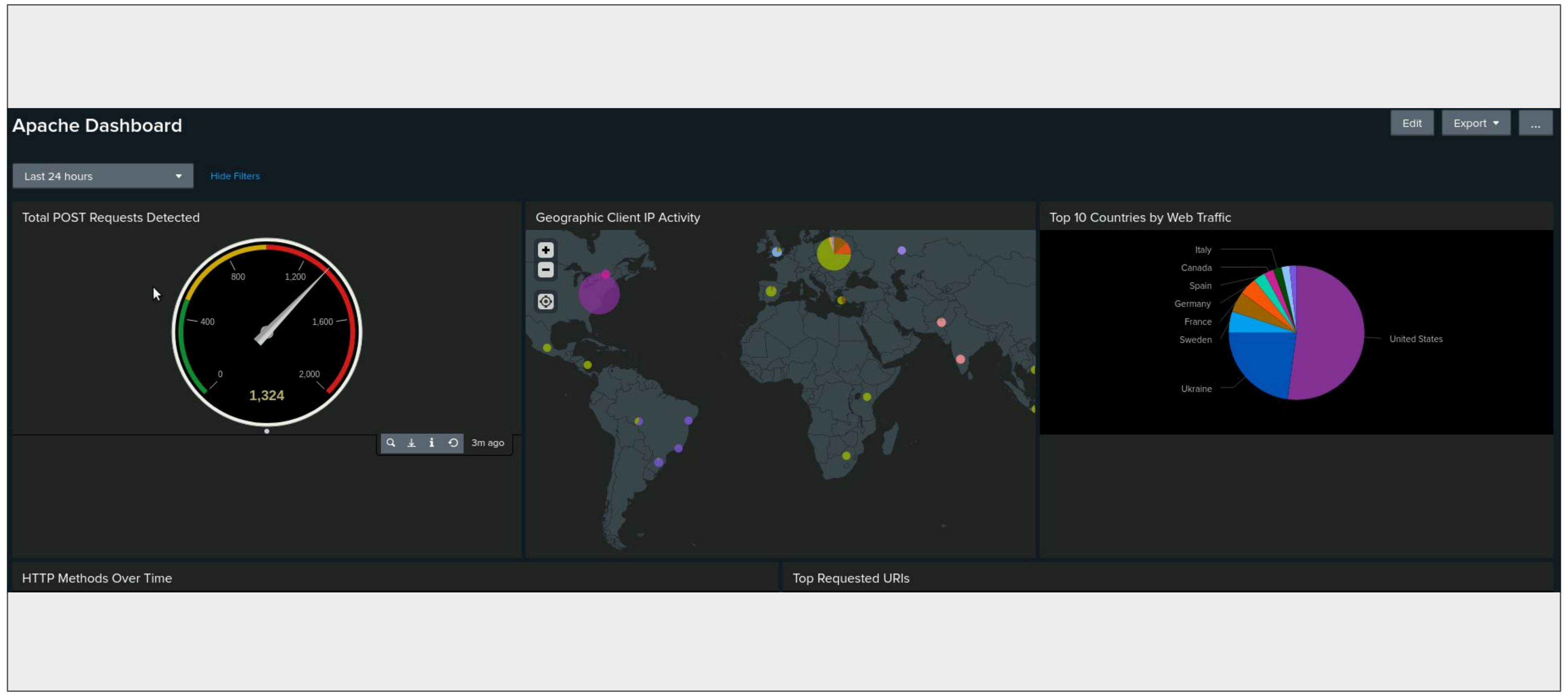
Alerts—Apache

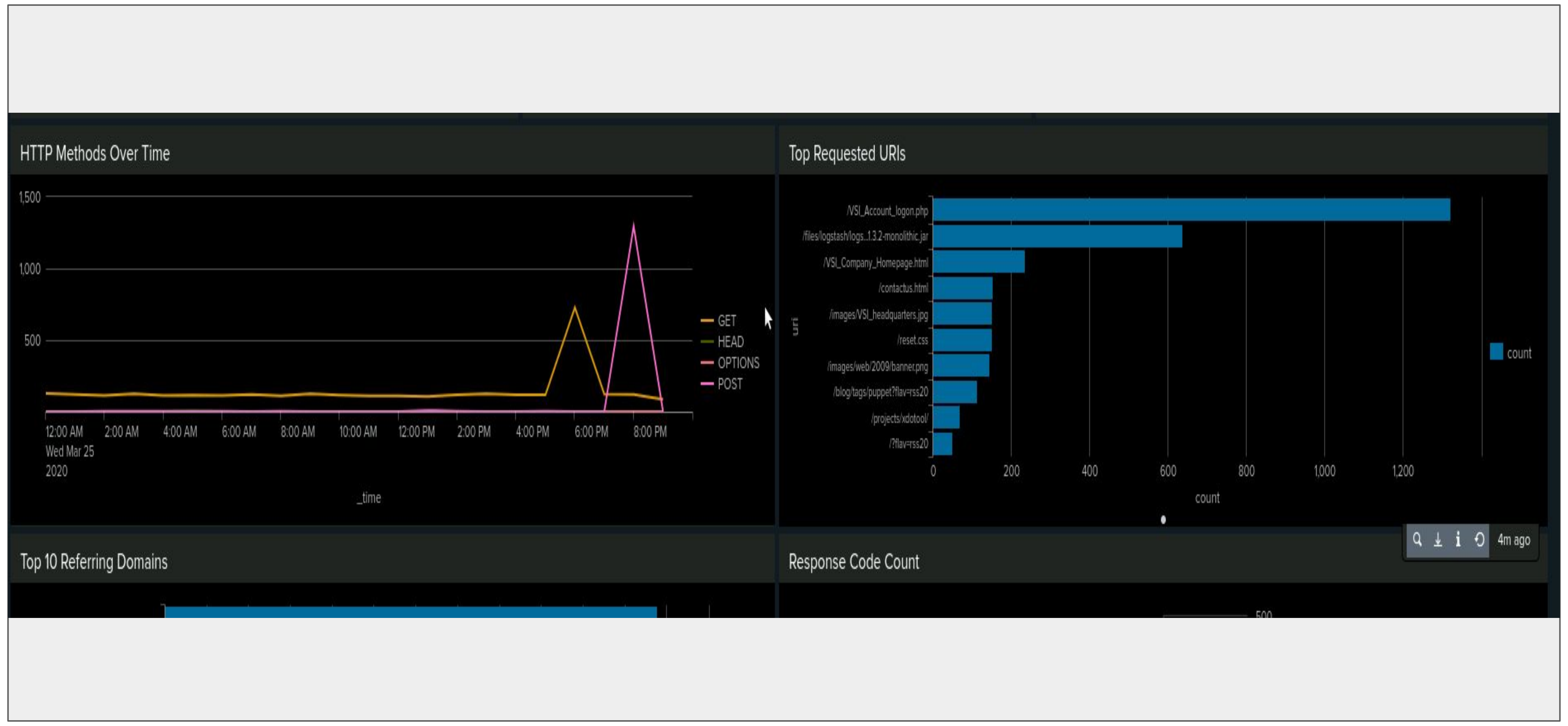
Designed the following alerts:

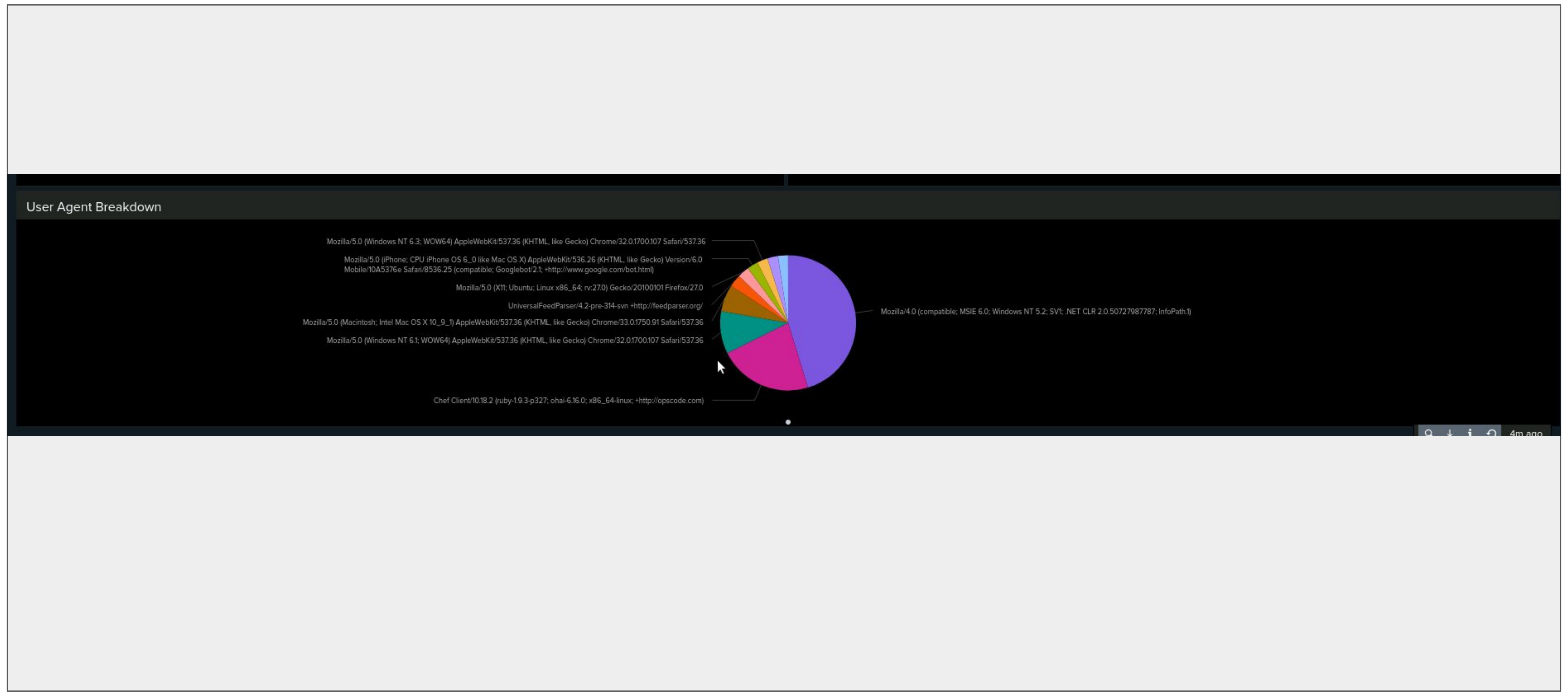
Alert Name	Alert Description	Alert Baseline	Alert Threshold
POST Method Spike	Detects an excessive number of HTTP POST requests within a 1-hour window.	30 requests/hour	50 requests/hour

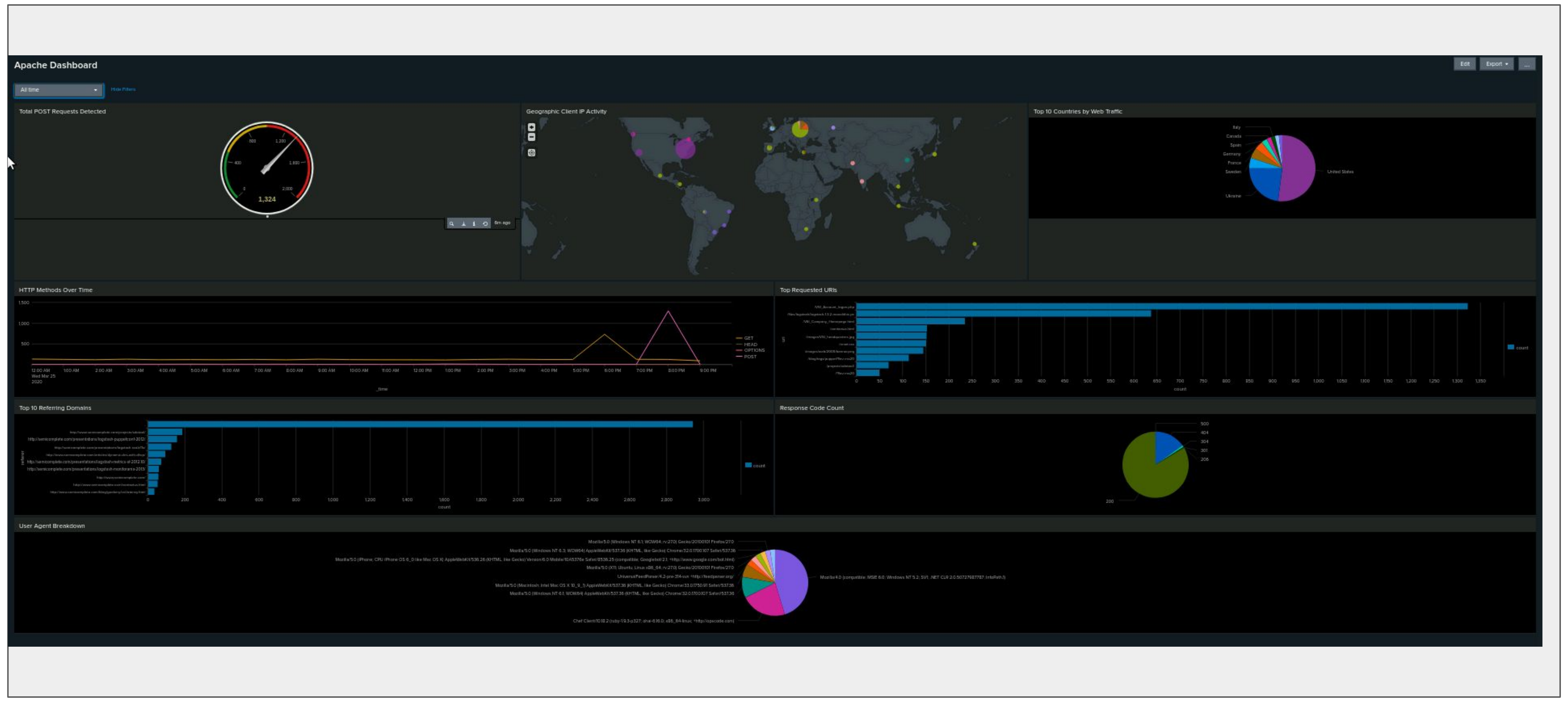
JUSTIFICATION: Normal traffic patterns showed an average of 20–30 POST requests per hour, primarily for standard form submissions. A spike to 50 or more POSTs in a single hour may indicate suspicious activity, such as brute-force login attempts or data exfiltration via form abuse. This threshold provides early warning without triggering false positives from legitimate usage.

Dashboards—Apache






User Agent Breakdown
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)
4m ago



Attack Analysis

Attack Summary—Windows

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

- Analysis of the Windows attack logs revealed unusual behavior indicative of potential compromise. The most frequent signatures included "Special privileges assigned to new logon" and "A computer account was deleted," both of which could signify privilege escalation and lateral movement.

- No excessive logon or deletion activity triggered our thresholds; however, the aggregate volume of sensitive actions, such as account modifications and policy changes, suggests coordinated attacker activity.

- These findings imply that attackers may have gained access to administrative credentials and attempted to manipulate user accounts and system settings to maintain persistence or disrupt operations.

- Continued monitoring is essential, with adjusted thresholds and enhanced alerting around privilege assignment and system policy changes.

Attack Summary—Windows

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

- The configured alerts did trigger during the attack window, signaling unusual activity such as excessive successful logons (event ID 4624) and assignment of special privileges (event ID 4672).
- These alerts indicated potential lateral movement or privilege escalation, both of which align with common post-exploitation behaviors.
- Our thresholds — such as 40+ successful logons and spikes in privileged access events — were effective in detecting the anomalies.
- While they were accurate in this case, continued tuning based on evolving baselines will be necessary to balance sensitivity and false positives.

Attack Summary—Windows

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

- The dashboards revealed notable spikes in activity correlated with the attack timeline. Specifically, a surge in Event ID 4624 (successful logons) and Event ID 4672 (privilege assignments) indicated lateral movement and potential privilege escalation.

- Signature frequency visualizations showed repeated targeting of sensitive operations, such as account creation and deletion.

- HTTP POST request anomalies and login success/failure comparisons further validated suspicious access behavior.

- Overall, the dashboards effectively visualized the attack progression and pinpointed critical indicators of compromise

Screenshots of Attack Logs

All time
Job
Verbose Mode
No Event Sampling
Events (515)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
+ Zoom to Selection
× Deselect
1 hour per column
Format
Show: 50 Per Page
View: Table
‹ Prev
1
2
3
4
5
6
7
8
...
Next ›
‹ Hide Fields
All Fields

```
source="windows_server_attack_logs.csv" signature_id IN ("4624", "4672", "4720", "4726")
```

✓ **515 events** (before 5/5/25 9:19:14.000 PM)

SELECTED FIELDS

a Account_Name	100+
a host	1
a source	1
a sourcetype	1

INTERESTING FIELDS

a Account_Domain	2
a Account_Expires	60
a action	3
a Allowed_To_Delegate_To	3
a app	3
a Authentication_Package	2
a body	100+
a category	5
a CategoryString	1
a change_type	1
a ComputerName	1
a date_hour	13
a date_mday	1
a date_minute	60
a date_month	1
a date_second	60
a date_wday	1
a date_year	1
a date_zone	2

i	_time	host	source	sourcetype	Account_Name
›	3/25/20 8:44:57.000 AM	Windows_server_logs	windows_server_attack_logs.csv	csv	user_i user_m
›	3/25/20 8:44:09.000 AM	Windows_server_logs	windows_server_attack_logs.csv	csv	user_n user_c
›	3/25/20 8:43:15.000 AM	Windows_server_logs	windows_server_attack_logs.csv	csv	user_j
›	3/25/20 8:42:55.000 AM	Windows_server_logs	windows_server_attack_logs.csv	csv	user_h user_k
›	3/25/20 8:41:51.000 AM	Windows_server_logs	windows_server_attack_logs.csv	csv	ACME-002 user_a
›	3/25/20 8:40:34.000 AM	Windows_server_logs	windows_server_attack_logs.csv	csv	ACME-002 user_h
›	3/25/20 8:40:20.000 AM	Windows_server_logs	windows_server_attack_logs.csv	csv	user_e user_i
›	3/25/20	Windows_server_logs	windows_server_attack_logs.csv	csv	ACME-002 user_n

Attack Summary—Apache

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

- After analyzing the Apache attack logs, we detected abnormal HTTP activity indicating potential malicious probing from foreign IP addresses. Spikes in HTTP POST requests and traffic from non-US countries exceeded our baseline thresholds, triggering alerts.

- Several referrer domains appeared suspicious, showing repeated access patterns.

- The HTTP response code analysis showed elevated 404 and 500 errors during attack hours, signaling possible attempts to access non-existent or restricted resources.

- Overall, our monitoring solution successfully identified these anomalies in real time, confirming the value of our alerts and dashboards in detecting and responding to threats from JobeCorp.

Attack Summary—Apache

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

- The alert thresholds for foreign traffic and excessive HTTP `POST` requests were accurate and effective.
- The alert for foreign traffic triggered as expected when non-U.S. IP activity spiked significantly above the baseline.
- The `POST` method alert successfully detected an unusual surge in `POST` traffic—likely indicative of an attempted upload or brute-force form abuse.
- These alerts allowed us to detect potentially malicious behavior in real time and would enable prompt escalation if deployed in production.

Attack Summary—Apache

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

- The Apache Web Server Monitoring dashboard provided real-time visibility into critical server activity.
- The HTTP Methods Over Time visualization clearly highlighted a spike in POST activity—correlating with the observed attack window.
- The geographic map pinpointed high traffic volume originating from Ukraine, supporting the foreign traffic alert.
- The URI analysis identified /VSI_Account_logon.php as the most frequently targeted path, suggesting targeted credential harvesting.
- Overall, the dashboard enabled quick identification of anomalies and provided actionable insights for incident response.

Screenshots of Attack Logs

New Search
Save As ▾
Create Table View
Close
All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (4,497)
Visualization
Show: 20 Per Page ▾
Format ▾
‹ Prev
1
2
3
4
5
6
7
8
...
Next ›
File Manager
Browse the file system

```
source="apache_attack_logs.txt"
| table _time, clientip, method, uri_path, status, useragent, referrer
| sort _time
```

✓ 4,497 events (before 5/13/25 1:48:02.000 AM) No Event Sampling ▾

Preview: On

_time	clientip	method	uri_path	status	useragent	referrer
2020-03-25 00:05:00	130.237.218.86	GET	/presentations/logstash-provops/images/logstash.png	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	
2020-03-25 00:05:00	130.237.218.86	GET	/presentations/logstash-provops/lib/css/zenburn.css	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	
2020-03-25 00:05:00	130.237.218.86	GET	/presentations/unix-basics/	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	
2020-03-25 00:05:00	82.80.14.189	GET	/presentations/logstash-monitorama-2013/images/apache-icon.gif	200	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	
2020-03-25 00:05:01	130.237.218.86	GET	/presentations/unix-basics/images/metacity-gnome.png	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	
2020-03-25 00:05:01	82.80.14.189	GET	/presentations/logstash-monitorama-2013/images/Dreamhost_logo.svg	200	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	
2020-03-25 00:05:01	106.78.19.160	GET	/presentations/mpi	301	LAVA.KKT35+.FARSIGHTED60D_CN_11B_HW (MAUI/KKT35_S116_20130820;BDATE/2013/08/20 14:41;LCD/240320;CHIP/MT6260;KEY/Normal;TOUCH/0;CAMERA/1;SENSOR/0;DEV/FARSIGHTED60D_CN_11B_HW;WAP Browser/MAUI (HTTPS)) LAVA_KKT35_S116_20130820 Release/2013.08.20 WAP Browser/MAUI (HTTPS) Profile/ Q03C1-2.40 en-US	
2020-03-25 00:05:02	82.80.14.189	GET	/presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js	200	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	
2020-03-25 00:05:03	82.80.14.189	GET	/presentations/logstash-monitorama-2013/lib/js/head.min.js	200	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	
2020-03-25 00:05:04	130.237.218.86	GET	/presentations/logstash-provops/js/jquery.min.js	200	M (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	

Summary and Future Mitigations

Project 3 Summary

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

- The attack originated from multiple foreign IP addresses, with a notable spike in POST requests targeting VSI’s login endpoint.
- The logs revealed a coordinated attempt to exploit authentication mechanisms, elevate privileges, and potentially exfiltrate data.
- Apache and Windows logs confirmed anomalies across user logons, account creations, and high-frequency access attempts.

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

- Implement multi-factor authentication (MFA) for all administrative access.
- Geo-fence traffic to block or monitor access from non-business regions.
- Introduce automated alerting for abnormal HTTP method usage and logon behaviors.
- Schedule regular log reviews and ensure dashboards remain active with updated thresholds.
- Harden the Apache server by limiting access to sensitive URIs and applying rate limiting.