March 13th 2025

Defensive Security Project

Presented By:

- Jason Vaz
- Brandi Green
- Dorcas Olawoyin
- Hesam Gohari
- Sean Vanzante
- Bhavinkumar Dabhi

Table of Contents

This document contains the following resources:

Monitoring Environment

Jason Vaz

Scenario

We played a role of an SOC analyst at a small company called Virtual Space Industries (VSI), which designs virtual-reality programs for businesses. VSI has heard rumors that a competitor, JobeCorp, may launch cyberattacks to disrupt VSI's business. Our task as an SOC analyst to monitor potential attacks on VSI’s systems using Splunk.

- The VSI systems we had to analyze those include below:
    - An Apache web server, which hosts the administrative webpage.
    - A Windows operating system, which runs many of VSI’s back-end operations.

Whois XML IP Geolocation API for Splunk

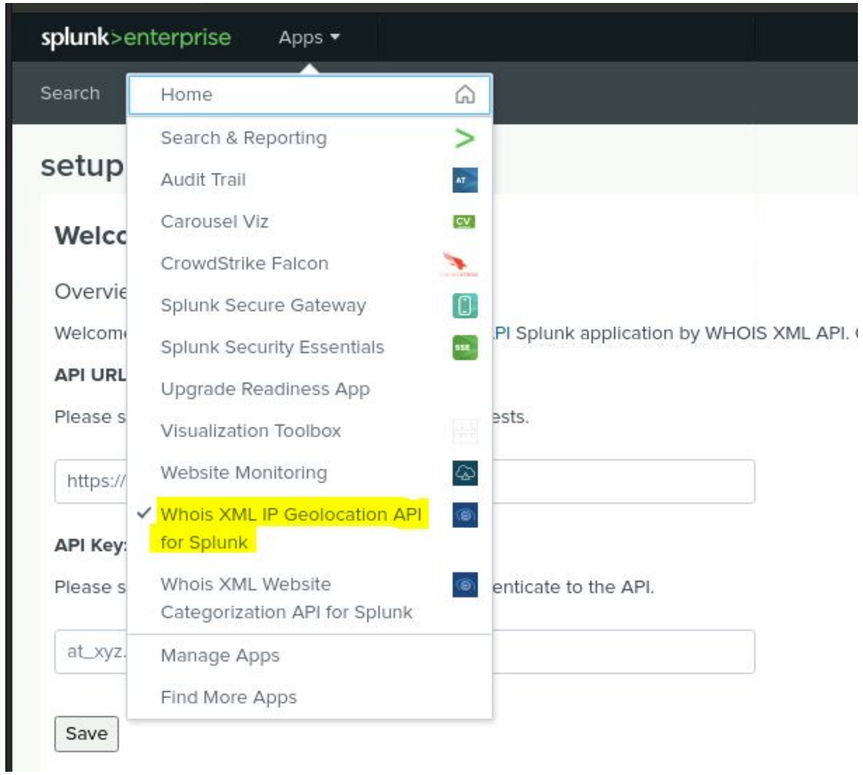
Bhavinkumar Dabhi

Whois XML IP Geolocation API for Splunk

It allows users to enrich IP address data in Splunk with detailed geolocation and WHOIS information. This add-on leverages the Whois XML API to provide insights into IP addresses, including:

1. **Geolocation Data**: It retrieves location information based on the IP address, such as country, city, latitude, longitude, and more.
2. **WHOIS Information**: It provides detailed WHOIS data about the IP address, such as the organization, ISP, domain ownership, and other registration details.
3. **Enrichment**: It enhances Splunk's log data with this additional information, making it easier for analysts to understand the context behind network traffic or security events.
4. **Automation**: It can automatically query the Whois XML API for every IP address in the Splunk events, improving efficiency and insight.

By adding this add-on to Splunk environment, helps in visualizing and analyzing IP-related data with geolocation and registration details, making it useful for threat detection, network monitoring, and investigation purposes.



Whois XML IP Geolocation API for Splunk

How It Works in Splunk

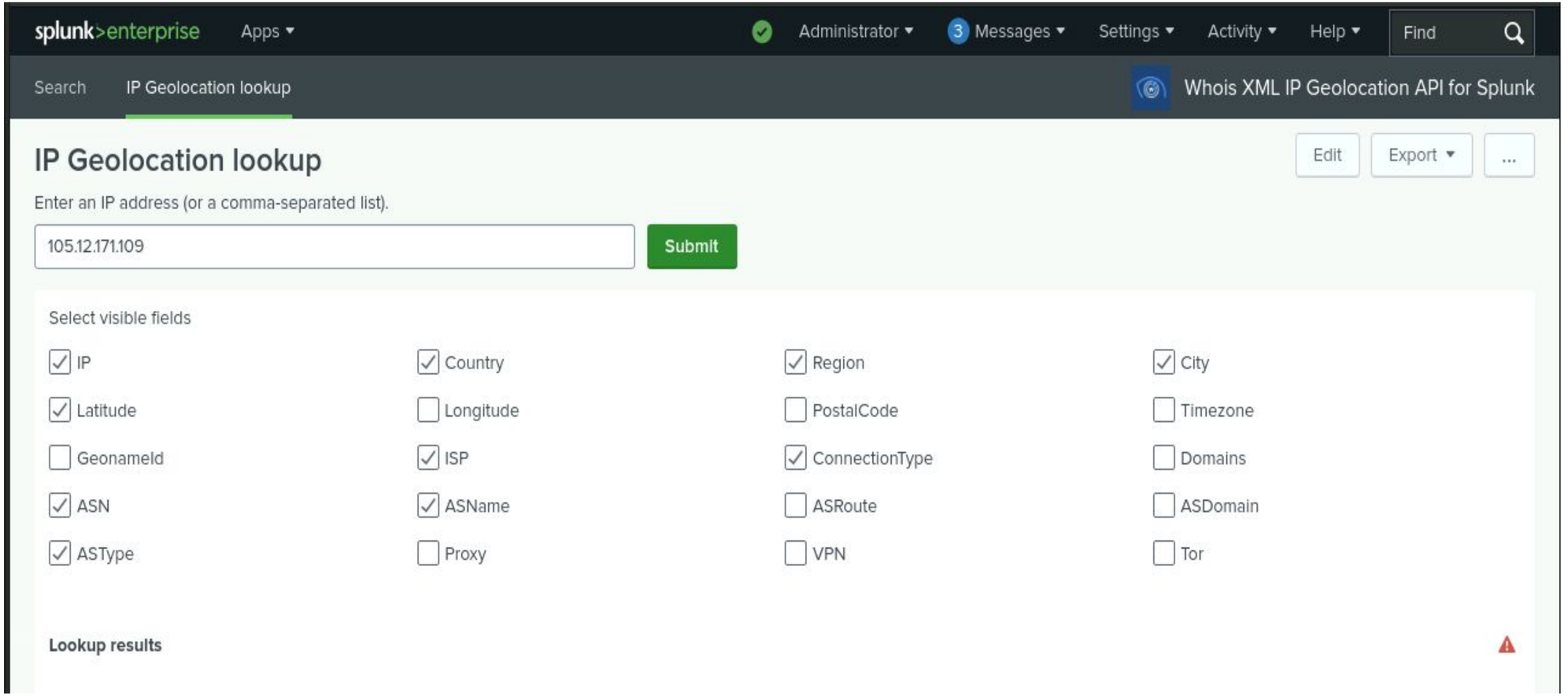
The **Whois XML IP Geolocation API for Splunk Add-on** works in Splunk by enriching IP address data in logs with external geolocation and WHOIS information. Here's a summary of how it works:

1. **Extract IPs**: The add-on automatically identifies and extracts IP addresses from Splunk logs.
2. **API Requests**: It sends these IPs to the Whois XML API to retrieve geolocation (country, city, latitude, longitude) and WHOIS information (ISP, organization, etc.).
3. **Enrich Events**: The add-on enriches the original log events with the retrieved geolocation and WHOIS data.
4. **Search and Analysis**: search, visualize, and analyze the enriched data in Splunk, gaining more context about IP addresses (e.g., identifying suspicious activity based on location or organization).

In summary, the add-on enhances the IP address-related log data with geolocation and WHOIS information, improving network traffic and security analysis in Splunk.

Image Reference - https://www.about-fraud.com/providers/whois-api/

Whois XML IP Geolocation API



Whois XML IP Geolocation API (Website overview)

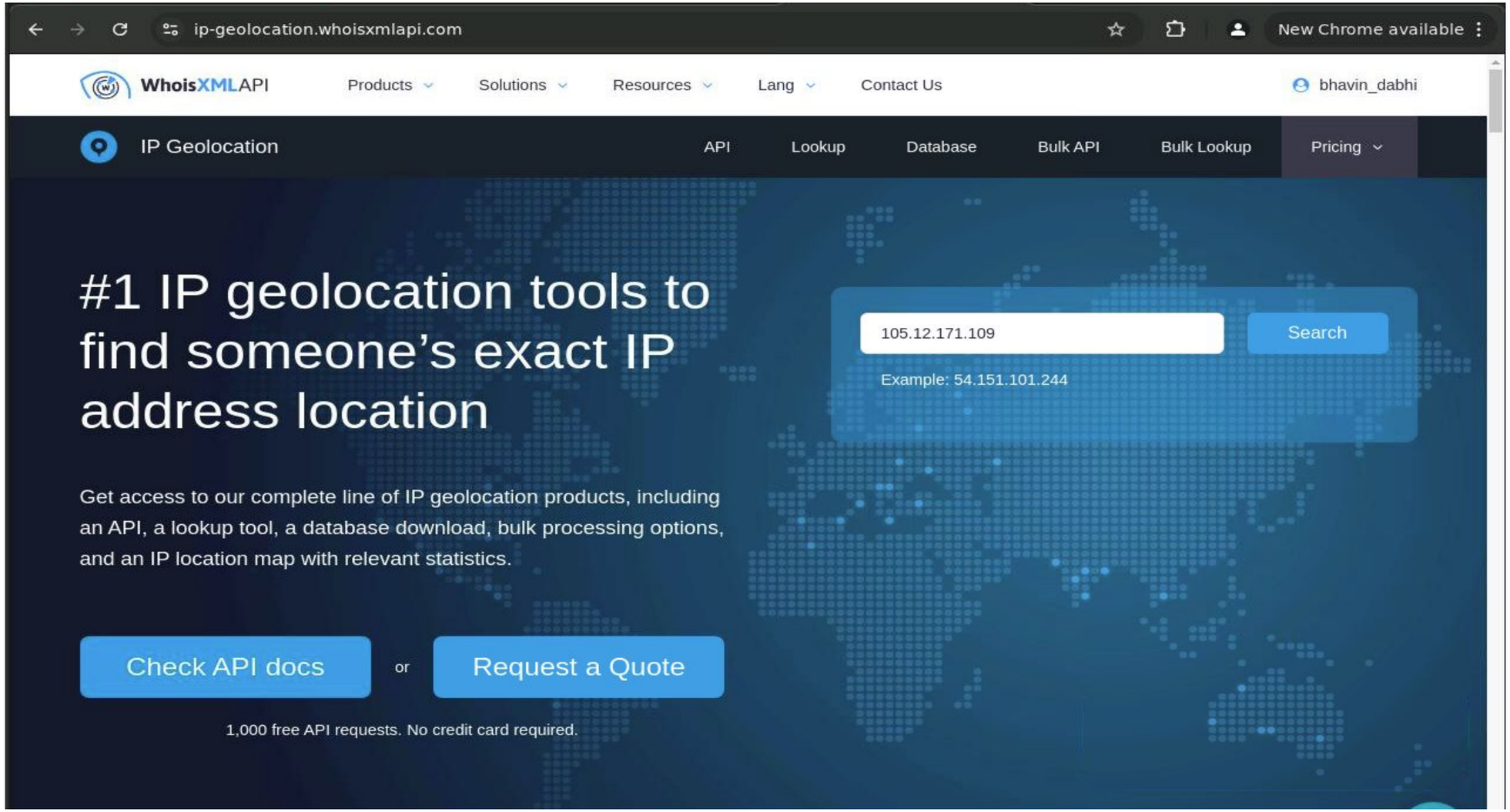


image Reference - https://ip-geolocation.whoisxmlapi.com/

Whois XML IP Geolocation API - (Website Ip Address search result)

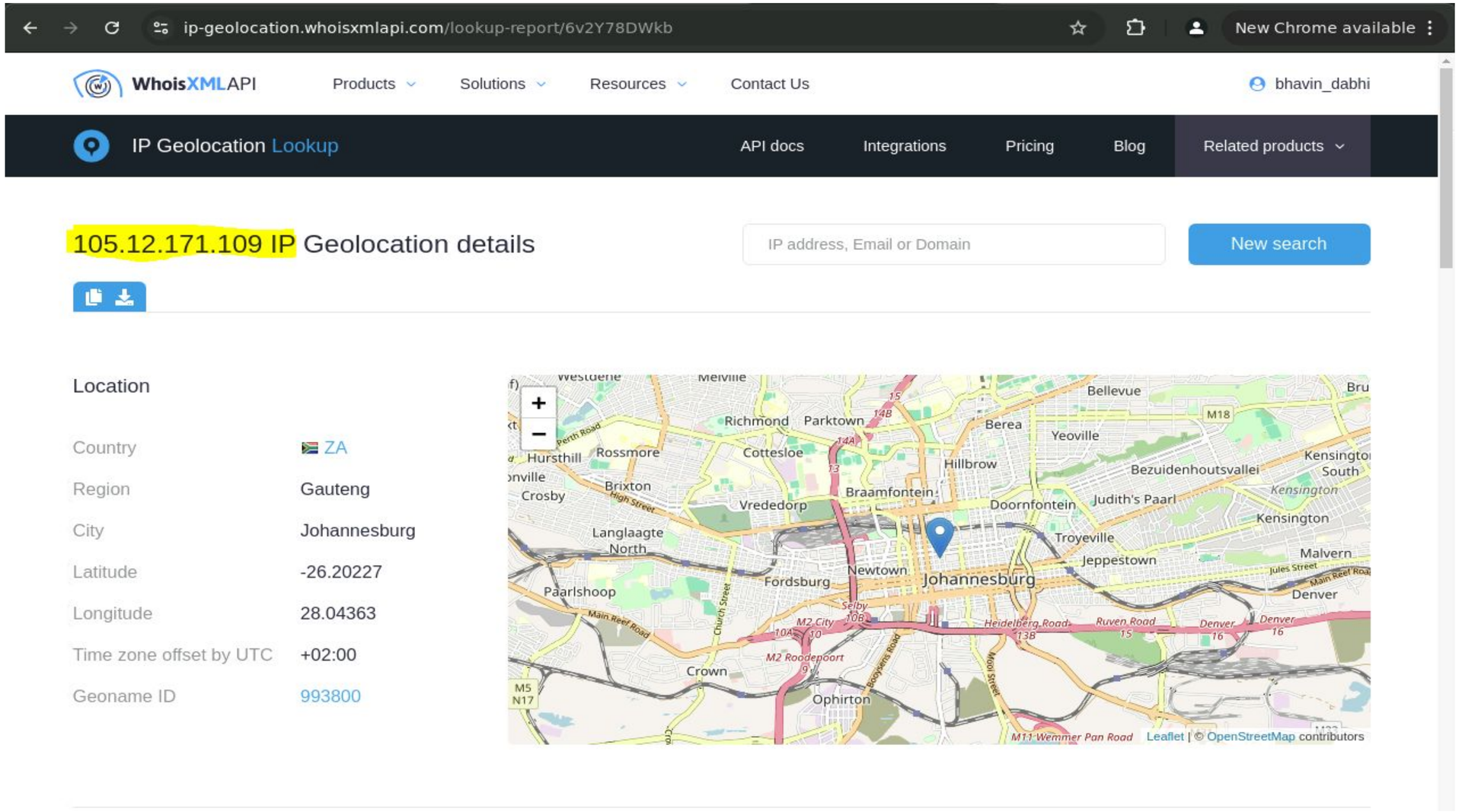


image reference - https://ip-geolocation.whoisxmlapi.com/lookup-report/6v2Y78DWkb

Logs Analyzed

1 Windows Logs

Signature ID: A unique identifier assigned to a specific security event.

Signature: A human-readable description of the logged event.

User: Identifies the account that performed or was affected by the action.

Status: Indicates whether the event was successful or failed.

Severity: Represents the risk level associated with the event.

2 Apache Logs

Method: Specifies the type of action being performed in the request.

Referer Domain: The website or domain that directed the user to the current page.

Status: Identifies errors or anomalies in the request.

Client IP: The IP address of the client making the request.

User Agent: Identifies the browser, operating system, and device used by the client.

Windows Logs

Dorcas Olawoyin

Reports—Windows

Three Windows Reports

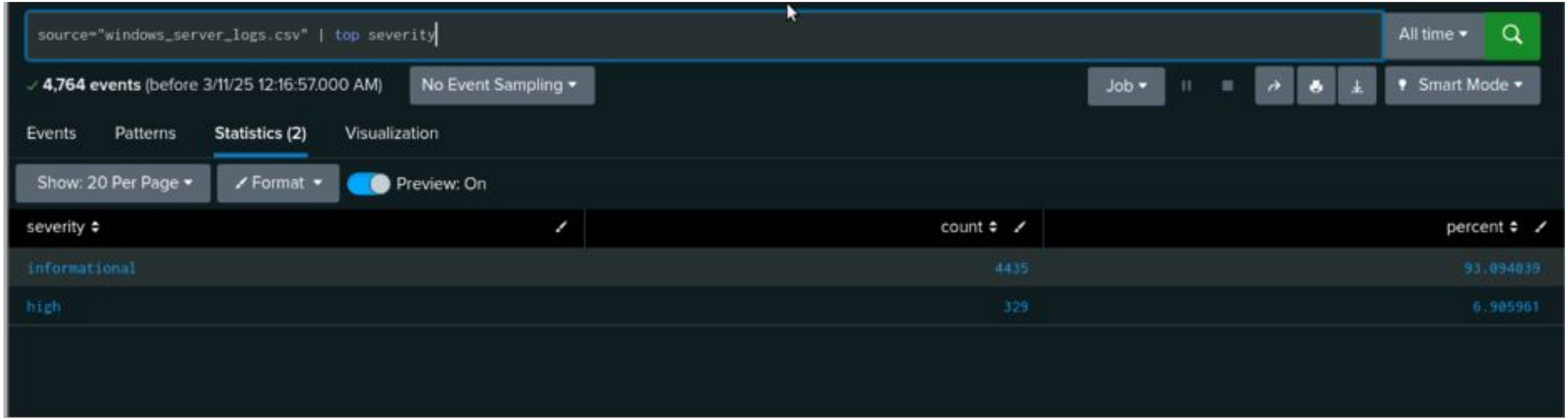
Report Name	Report Description
Windows Signature ID’s	A report with a table of signatures and associated signature IDs
Windows Log Severity Report	Displays the severity levels, and the count and percentage of each.
Windows Success Vs Failure Report	A report that provides a comparison between the success and failure of Windows activities.

Images of Reports—Windows

Windows Signature ID’s

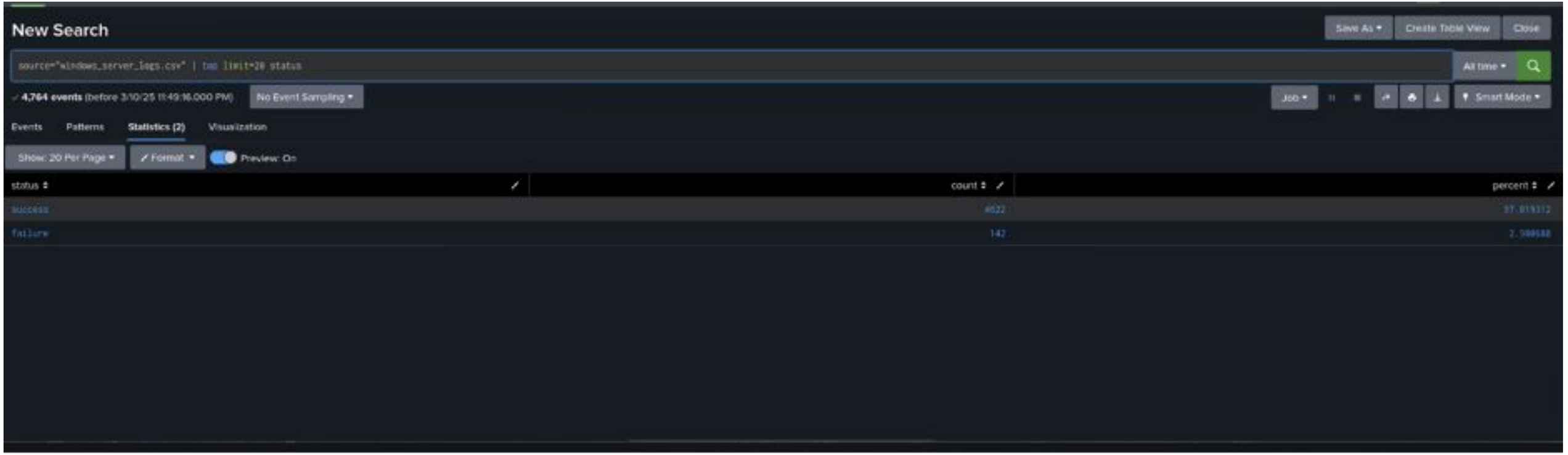
Images of Reports—Windows

Windows Log Severity Report



Images of Reports—Windows

Windows Success Vs Failure Report



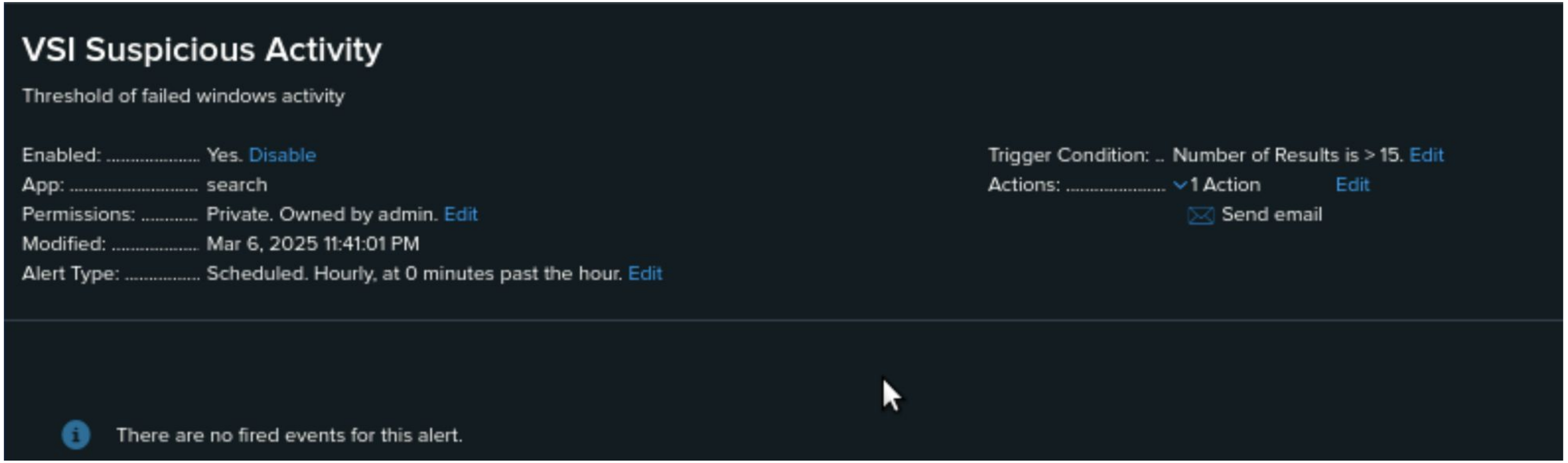
Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Suspicious Activity	Threshold of failed windows activity reached.	Baseline for failed hourly attempts: 6	Threshold for failed hourly attempts: 15

JUSTIFICATION: During regular business hours, VSI records two to five unsuccessful login attempts per user. An automated login attack, credential stuffing, or brute-force attack may be indicated if the failure rate increases by more than 10 to 15 percent per hour.

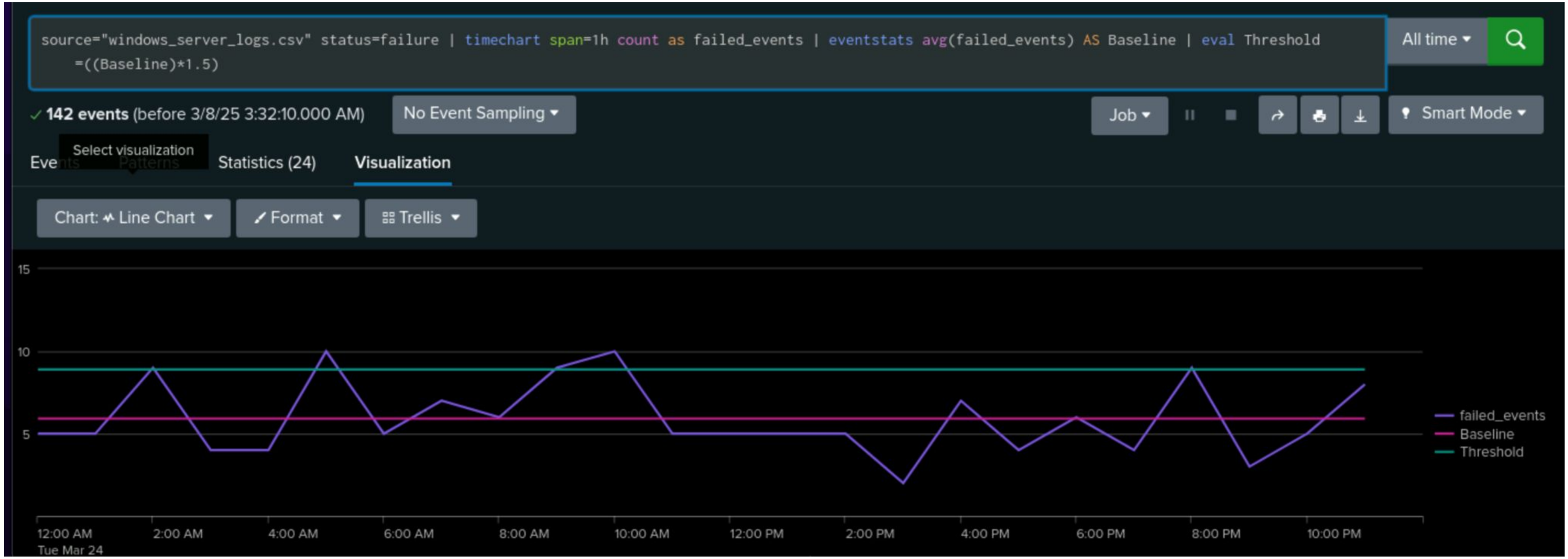
Images of Alerts—Windows

VSI Suspicious Activity



Images of Alerts—Windows

VSI Suspicious Activity



Alerts—Windows

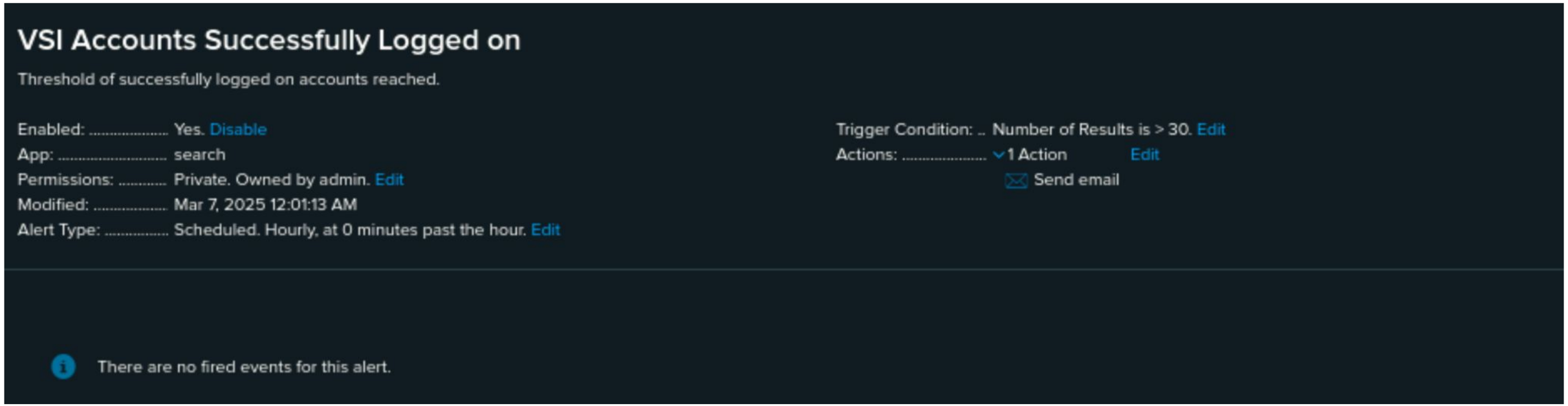
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Volume of Successful Logins	The hourly count of the signature “an account was successfully logged on.”	9	30

JUSTIFICATION: Based on the organizational policies, shift schedules, and login activity. **Login activity that rises sharply over the typical range could be a clue that credentials have been hacked.**

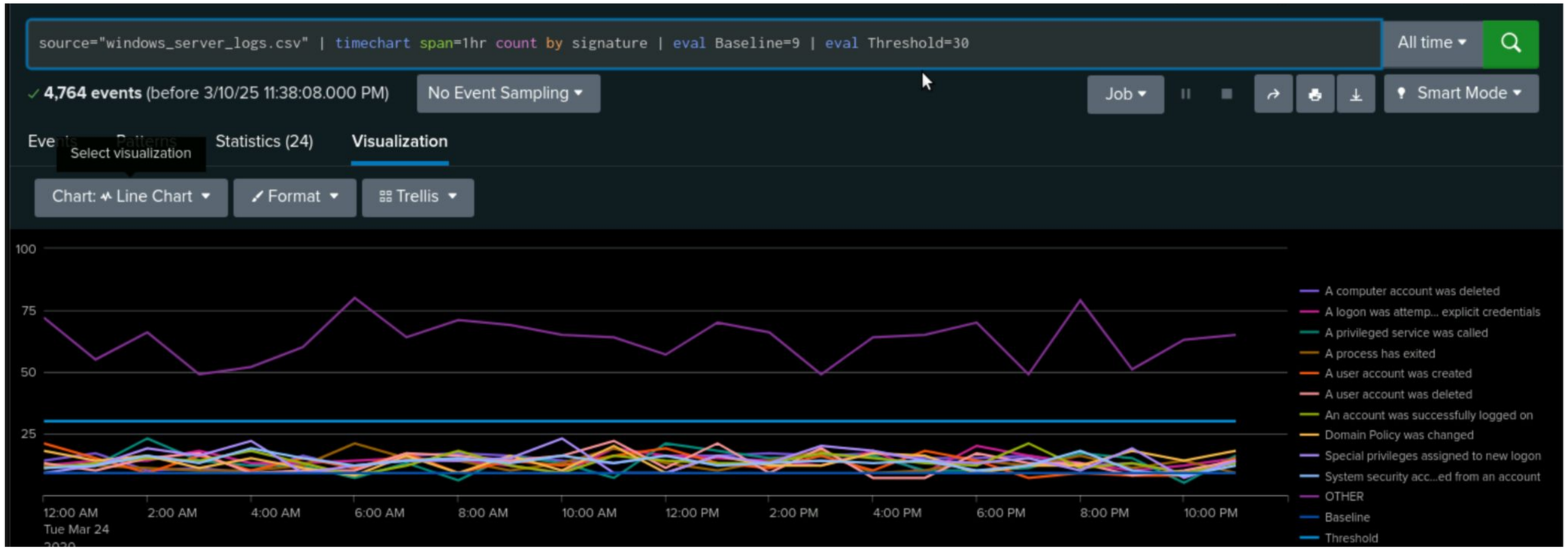
Images of Alerts—Windows

High Volume of Successful Logins



Images of Alerts—Windows

High Volume of Successful Logins



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deletion	The hourly count of the signature “a user account was deleted.”	9	20

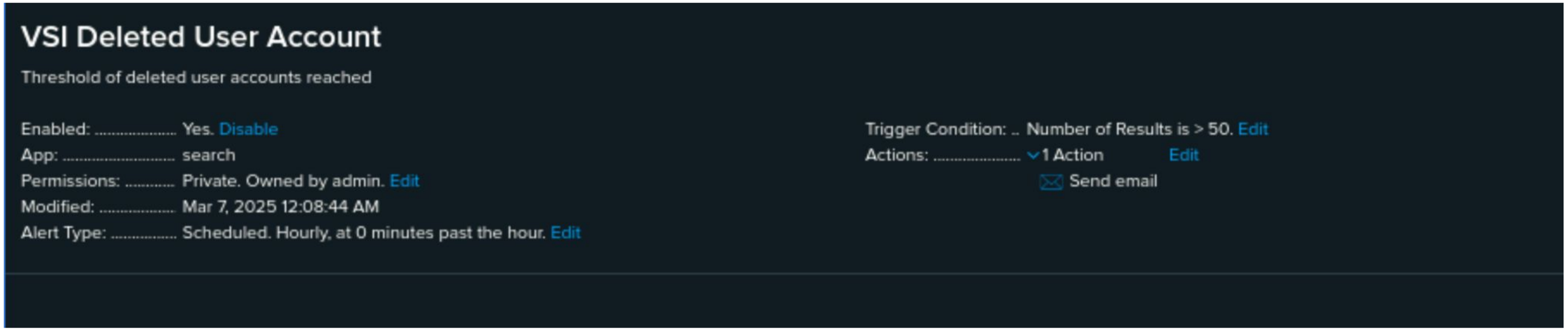
JUSTIFICATION: Deleting of user accounts are uncommon during regular operations. A security breach or insider **threat may be indicated if more than 20 deletions take place in a single hour.**

Images of Alerts—Windows

User Account Deletion

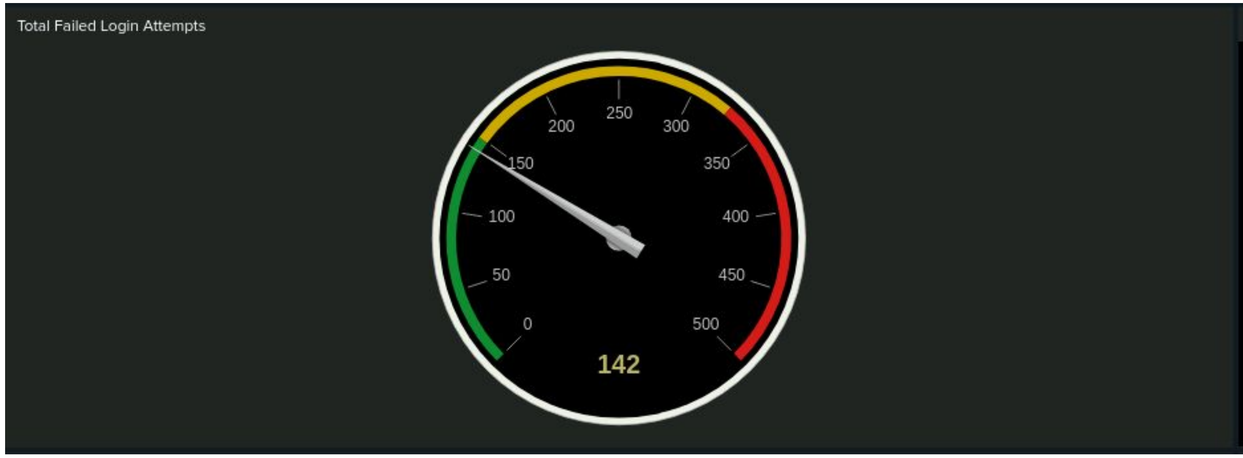
Images of Alerts—Windows

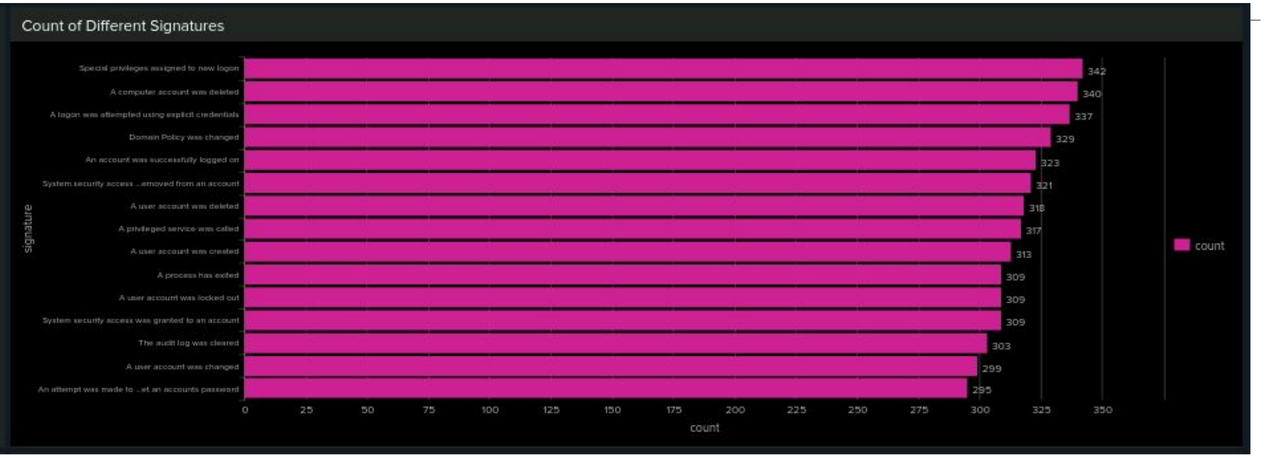
User Account Deletion

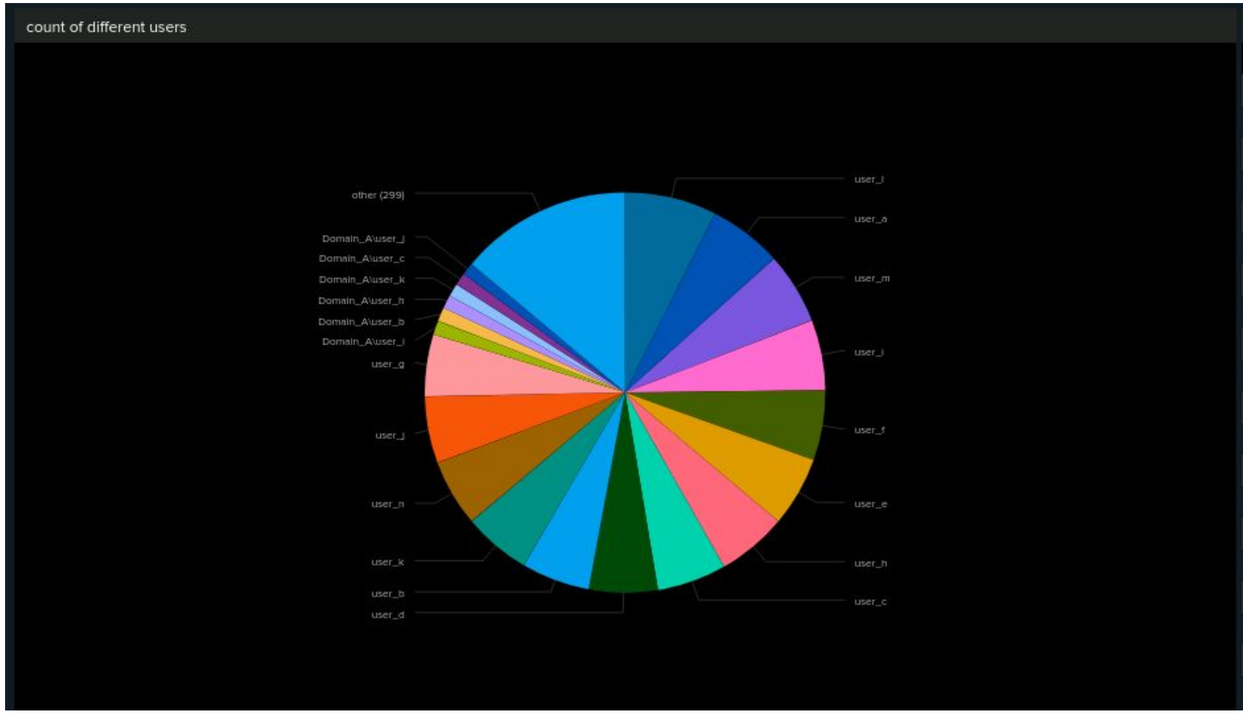


Dashboards—Windows

Dashboards—Windows







count of different users

user	count
user_l	354
user_a	282
user_m	275
user_i	271
user_f	270
user_e	269
user_h	269
user_c	267
user_d	264
user_b	263
user_k	260
user_n	258
user_j	256
user_g	239
Domain_A\user_i	54
Domain_A\user_b	53
Domain_A\user_h	52
Domain_A\user_k	50
Domain_A\user_c	48
Domain_A\user_j	48

Apache Logs

Brandi Green

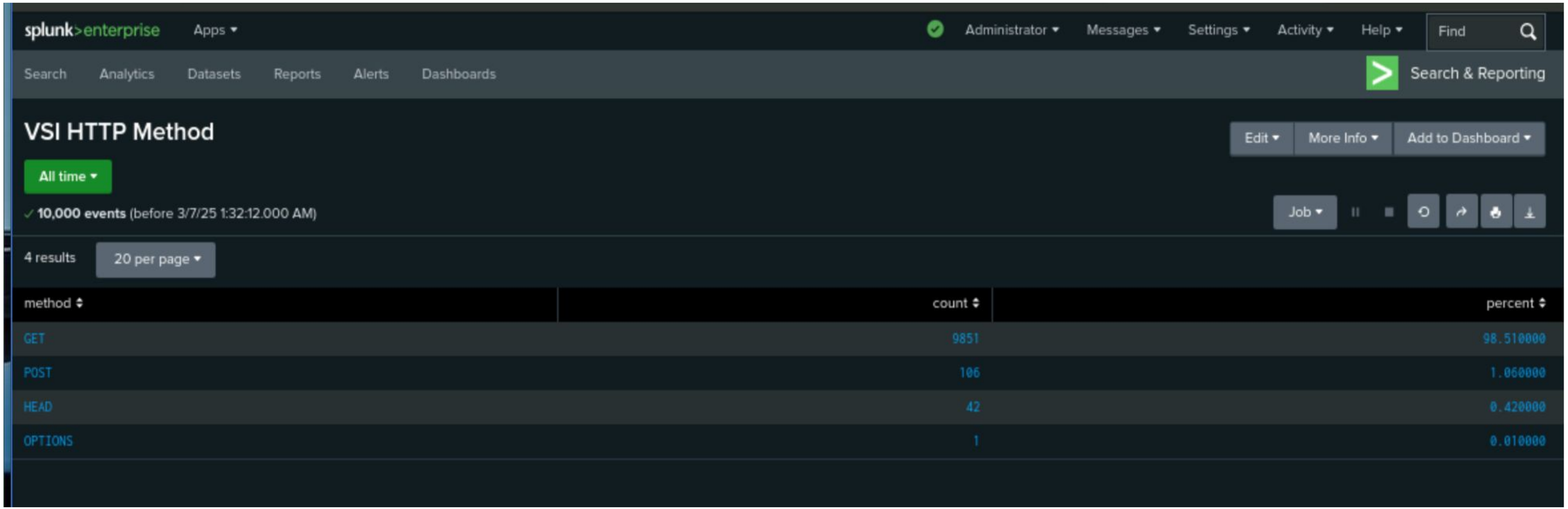
Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Method Activity	Displays information about VSI's web server activities by displaying a table of various HTTP methods.
Top 10 Referring Domains	Determines the top ten domains that provide traffic to VSI's website in order to identify potentially harmful referrers.
HTTP Response Code Analysis	Shows the count of each HTTP response code to highlight any unusual or suspicious activity.

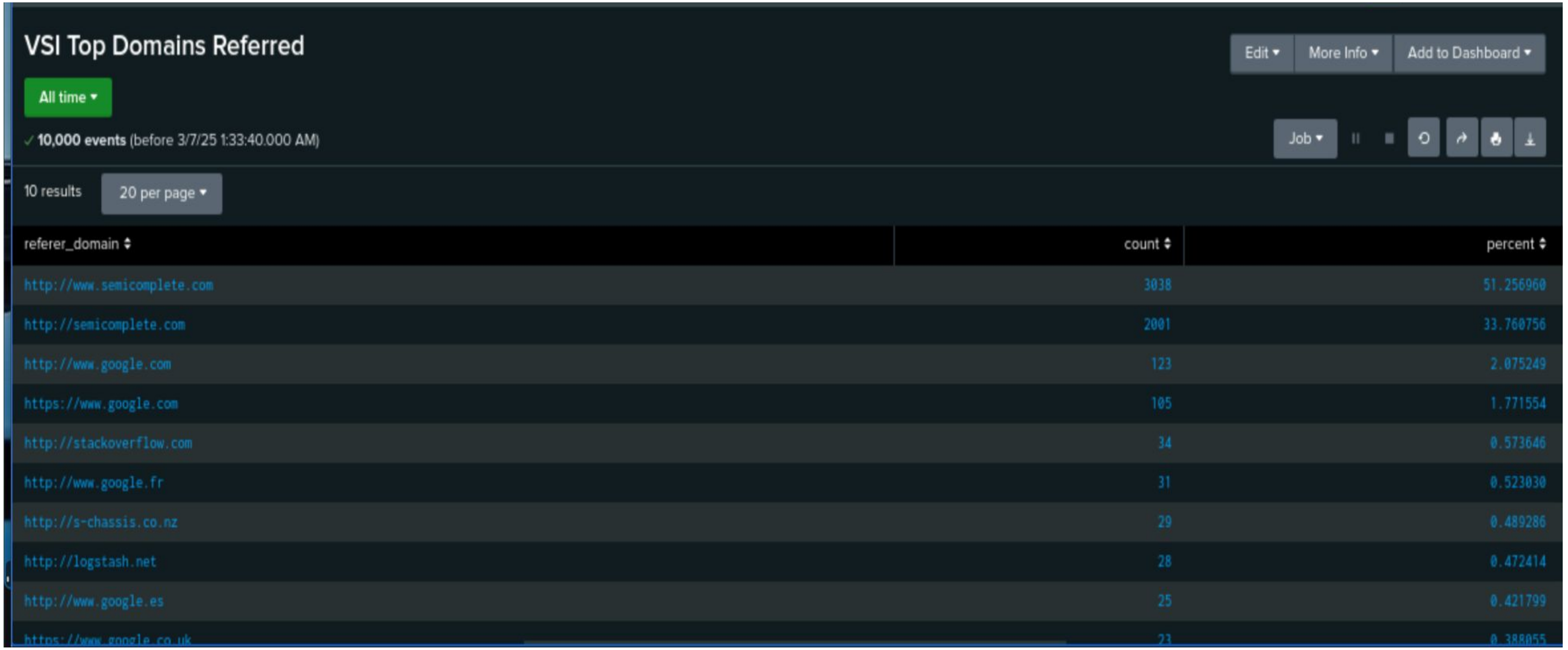
Images of Reports—Apache

HTTP Method Activity



Images of Reports—Apache

Top 10 Referring Domains



VSI Top Domains Referred

Edit ▾ | More Info ▾ | Add to Dashboard ▾

All time ▾

✓ **10,000 events** (before 3/7/25 1:33:40.000 AM)

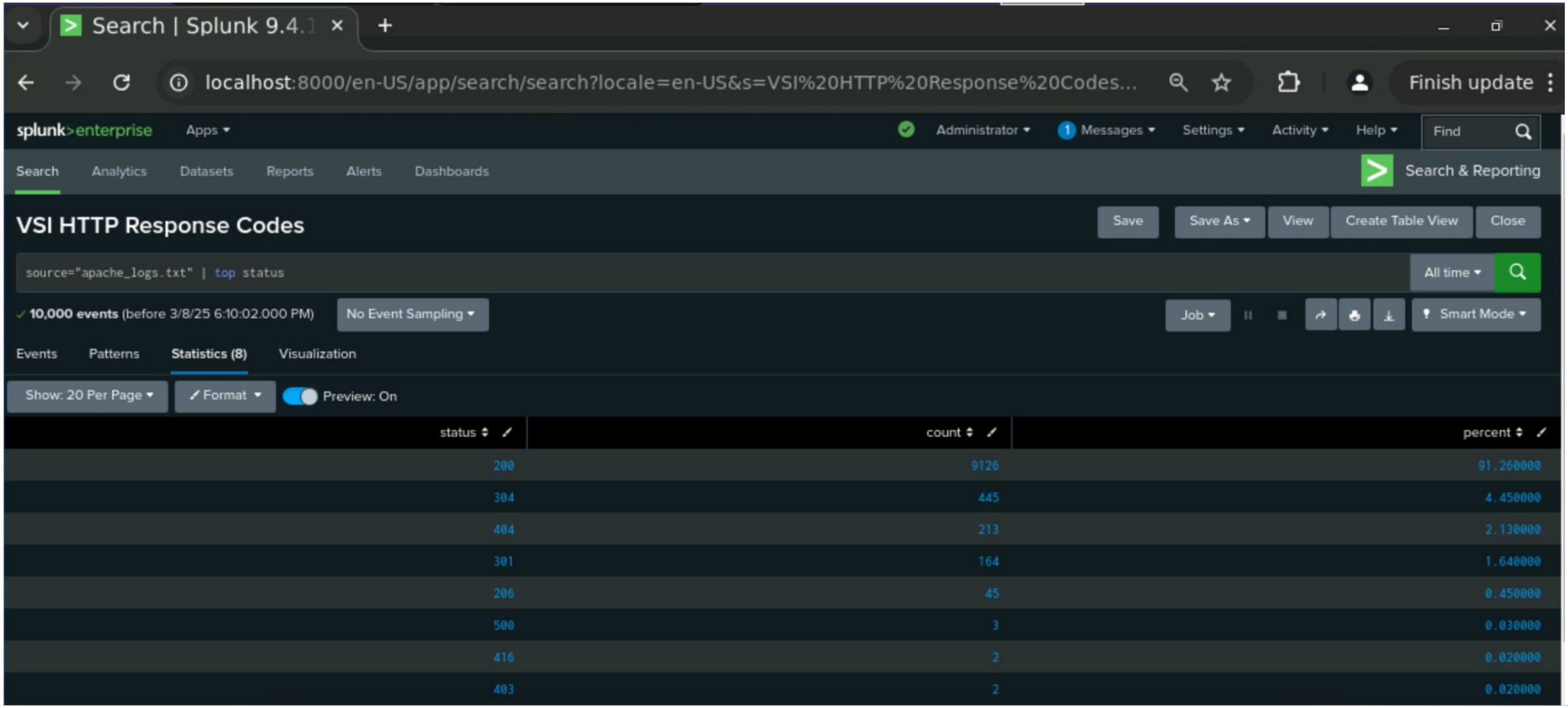
Job ▾

10 results | 20 per page ▾

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

Images of Reports—Apache

HTTP Response Code Analysis



status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-U.S. Traffic Threshold	When hourly activity from any nation outside of the US surpasses the predetermined level, it sets off	80	170

JUSTIFICATION: An average of five non-U.S. queries are sent to VSI every hour. **Requests from non-US countries above 170 per hour may be a sign of possible harmful activity,** including botnet attacks, illegal access attempts, or foreign scouting operations.

Image of Alert—Apache

Non-U.S. Traffic Threshold

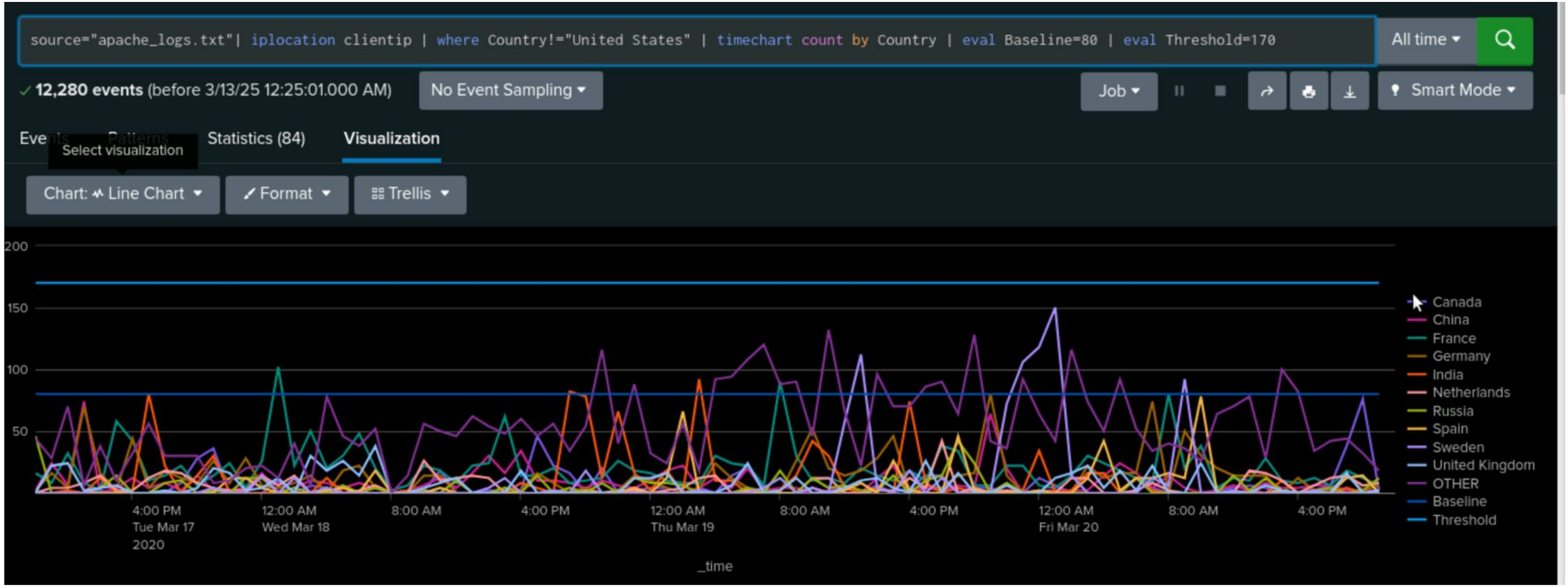
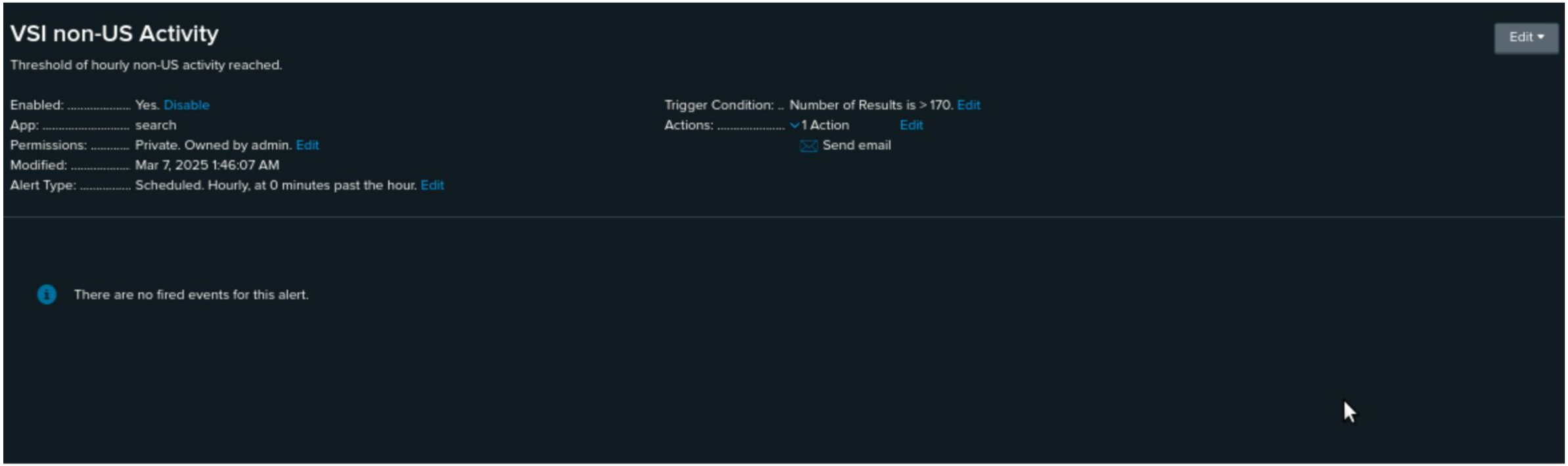


Image of Alert—Apache

Non-U.S. Traffic Threshold

```
source="apache_logs.txt" | iplocation clientip | where Country!="United States
```



Baseline for hourly activity is 80
Threshold for hourly activity is 170

Alerts–Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive HTTP POST Requests	When the hourly total of HTTP POST requests exceeds the predetermined threshold,	2	12

JUSTIFICATION: Typical HTTP POST requests usually fall within a predictable range, such as 50 requests per hour when used regularly. **More than 12 POST requests per hour detected by VSI may be a sign of questionable behavior**, including possible web assaults (such SQL injection), unwanted data submissions, or brute-force login attempts.

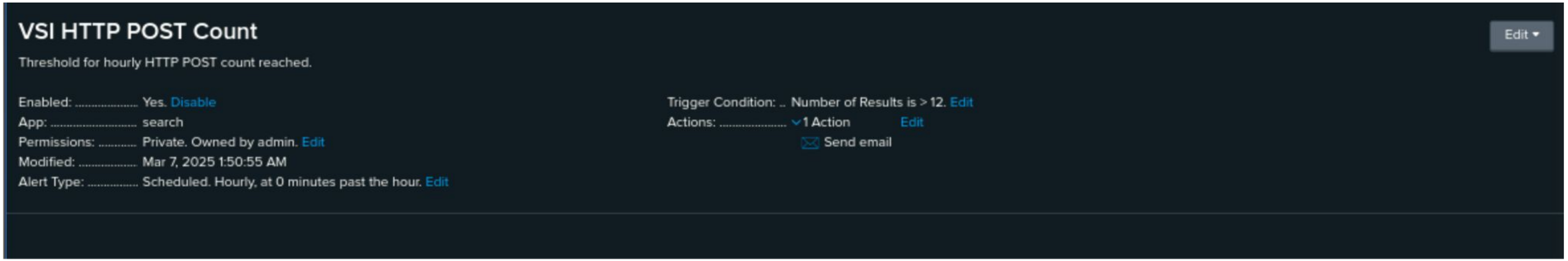
Image of Alert—Apache

Excessive HTTP POST Requests

Image of Alert—Apache

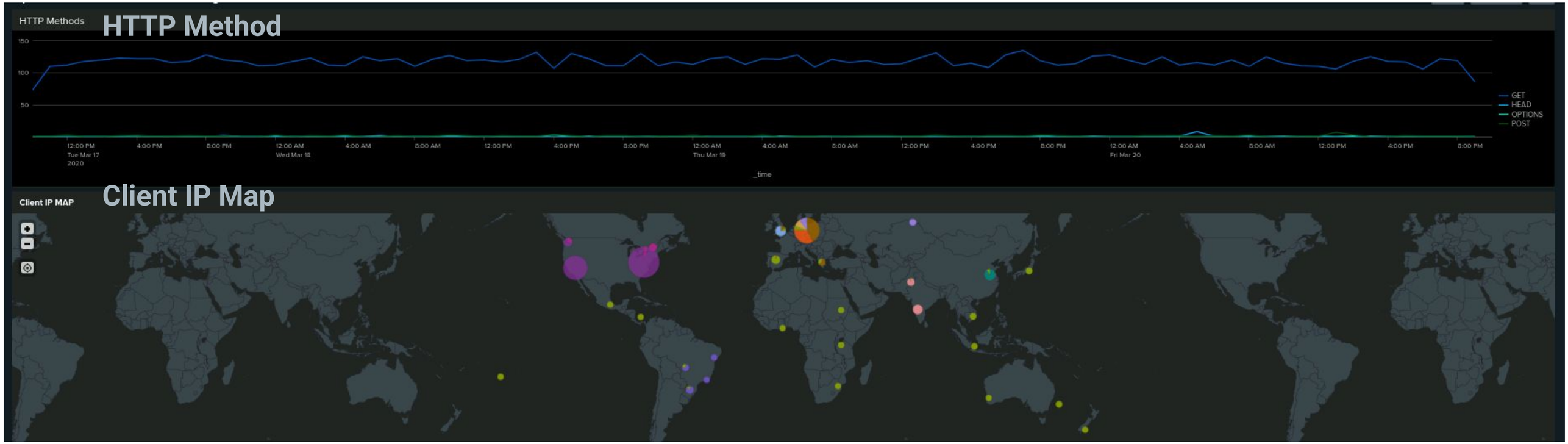
Excessive HTTP POST Requests

```
source="apache_logs.txt" method=POST
```



Baseline for hourly count of HTTP POST method is 2
Threshold for hourly count of HTTP POST method is 12

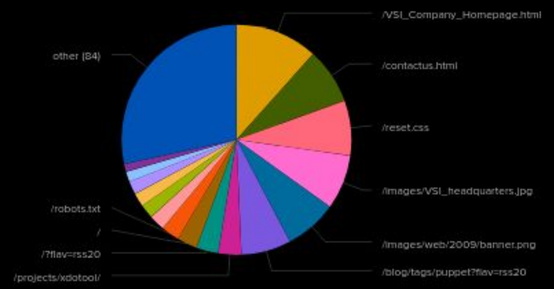
Dashboards—Apache



Dashboards—Apache

top 100 URI

Top 100 URL

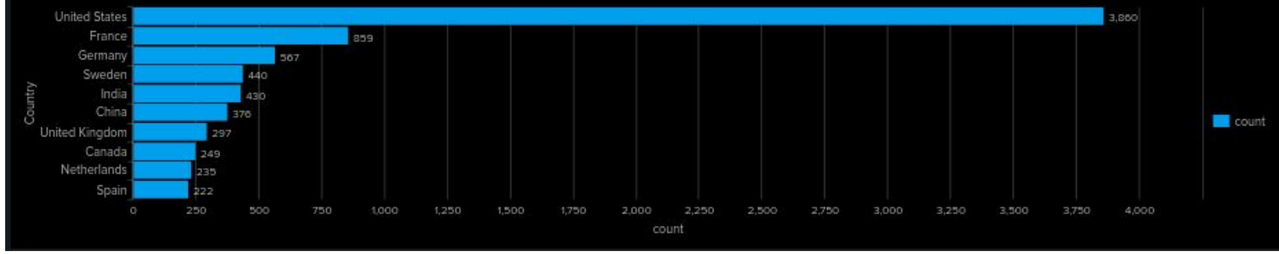


user logins an hour

User Logins An Hour

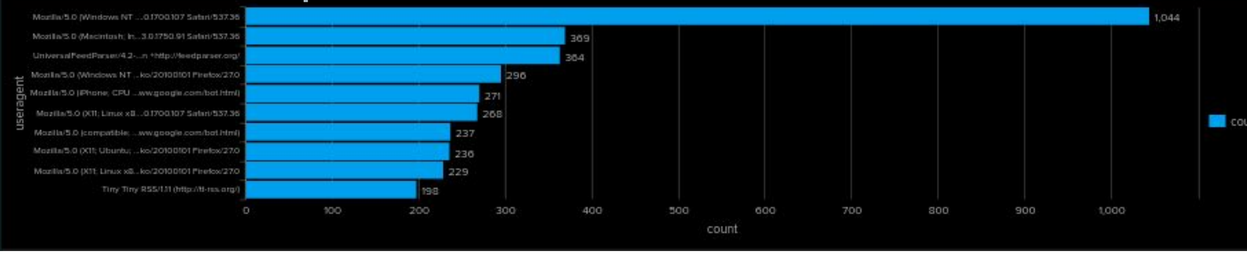
top 10 Countries that appear in log

Top 10 Countries That Appear in Log



top 10 URI's

Top 10 URI's



Attack Analysis

Sean Vanzante
Hesam Gohari

Attack Summary—Windows Reports

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

- Top Severity Report:
  Informational count down from 4435 to 4383 ; down 93% to 80% of total
  High severity count up from 329 to 1111; up 7% to 20% of total
  Results suggest **there are suspicious changes in the high severity count**

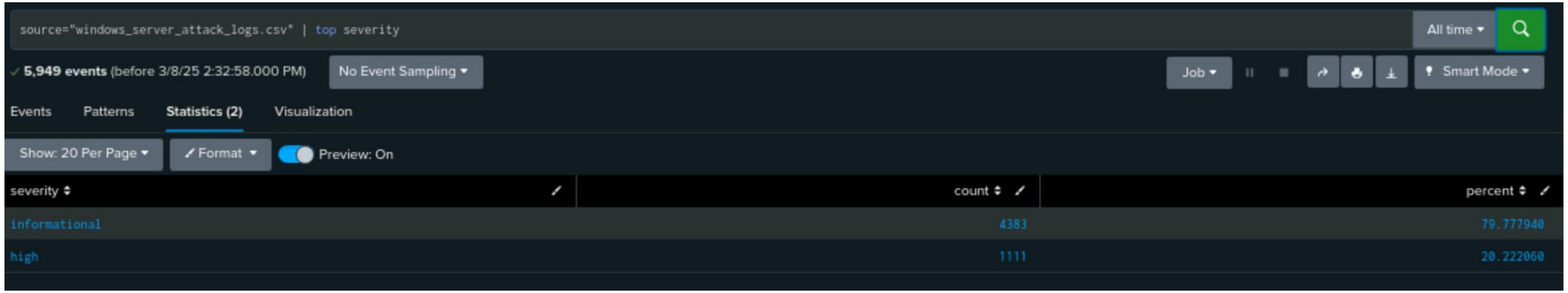
- Failed Activities Report:
  Successful activities: increase of 1%, from 97% to 98%
  Failed activities: decrease of 1%, from 3% to 2%
  Results suggest **no major changes in failed activities**

Attack Summary—Windows Reports

- Top Severity Report:

Pre Attack

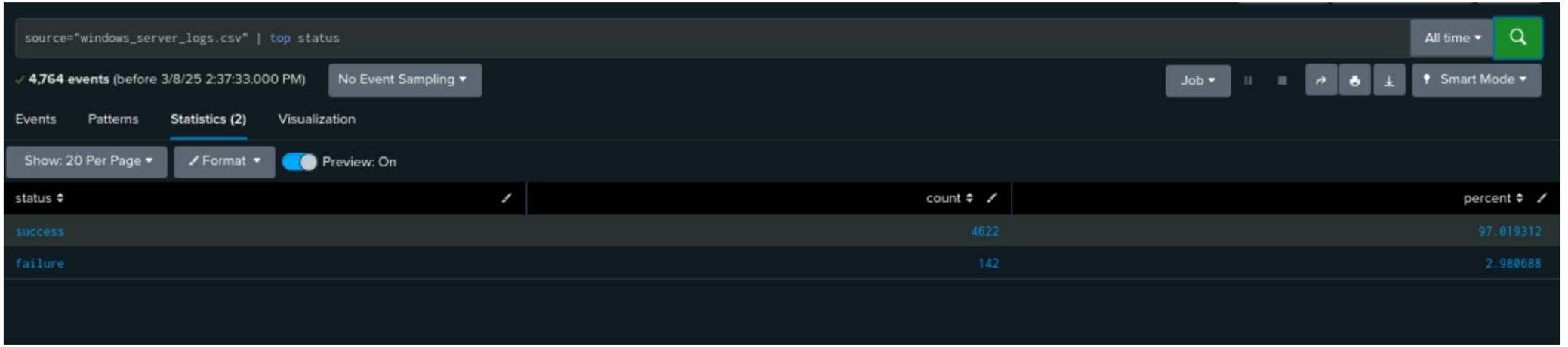
Post Attack



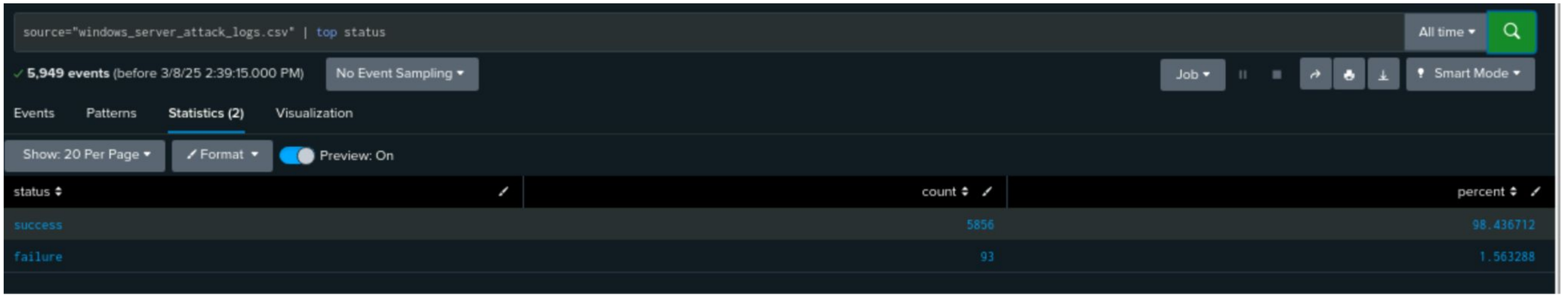
Attack Summary—Windows Reports

- Failed Activities Report:

Pre Attack



Post Attack



Attack Summary—Windows Server Logs Alerts

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

- Failed Windows Activity Alert
  Suspicious volume at 8am on March 25; **35 events** during the hour
  Alert threshold is 15 so alert was successful

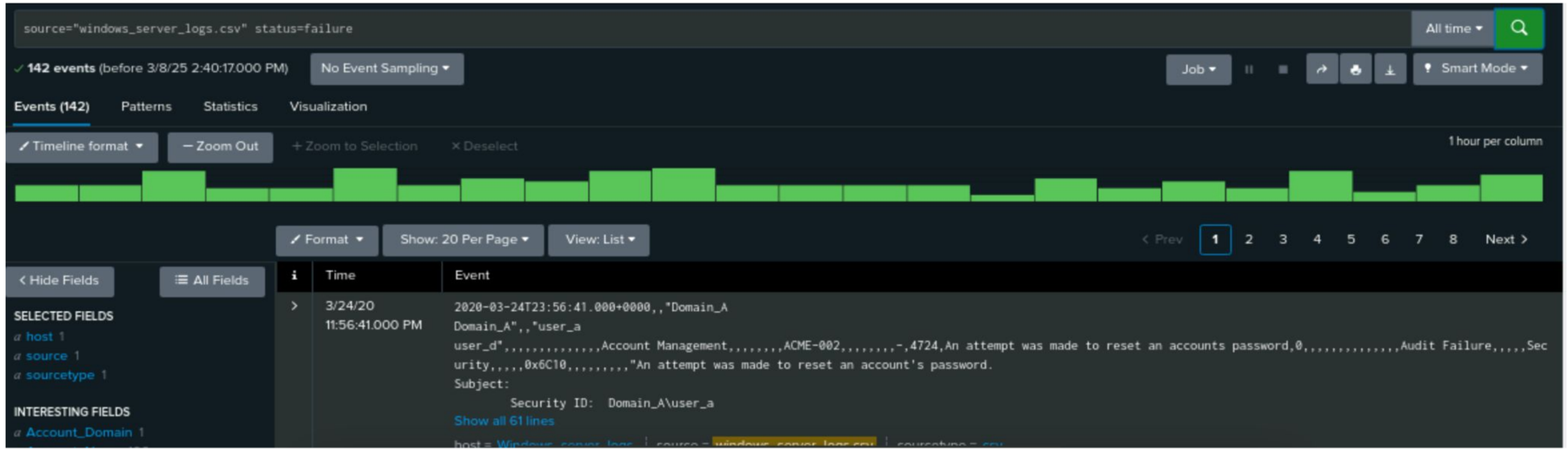
- Successful Logins Alert
  Suspicious activity at 11am and 12 pm on March 25; **196 events** at 11am and 77 events at 12pm; primary user j
  Alert threshold is 30 so alert was successful

- Deleted Accounts Alert
  No suspicious activity; Max deleted accounts was 17 on March 25, 5am
  Alert threshold is 50 so alert was successful

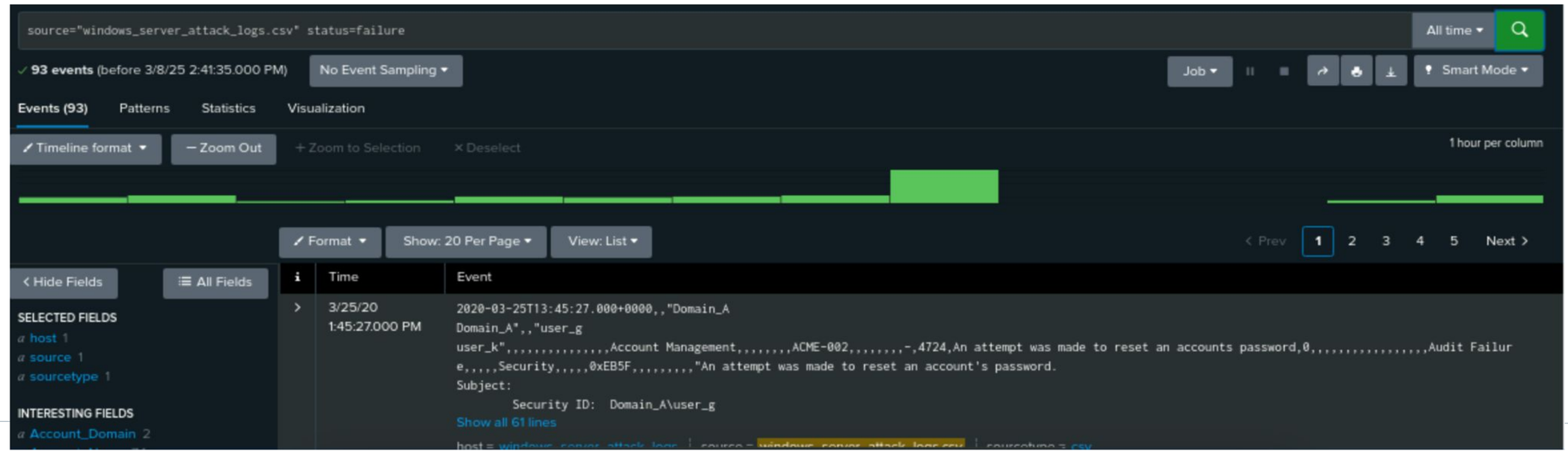
Attack Summary—Windows Server Logs Alerts

ALERT ANALYSIS FOR FAILED WINDOWS ACTIVITY

Pre Attack



Post Attack



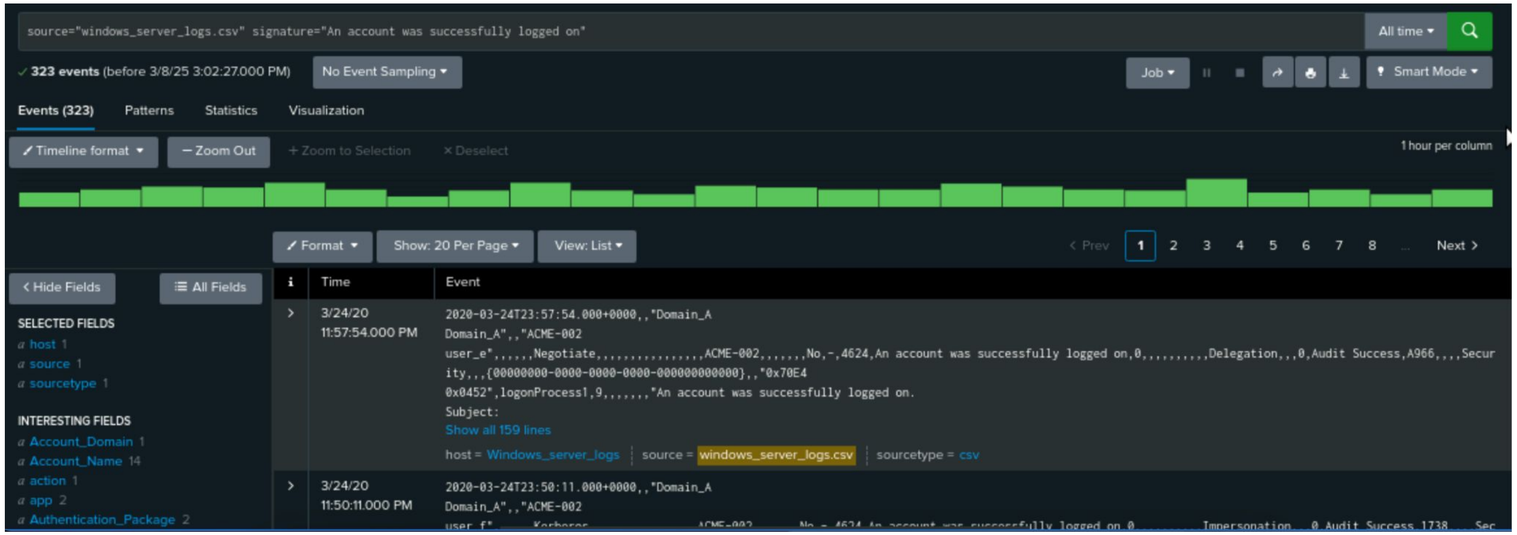
Screenshots of Attack Logs - Windows Server Logs Alerts

ALERT ANALYSIS FOR FAILED WINDOWS ACTIVITY

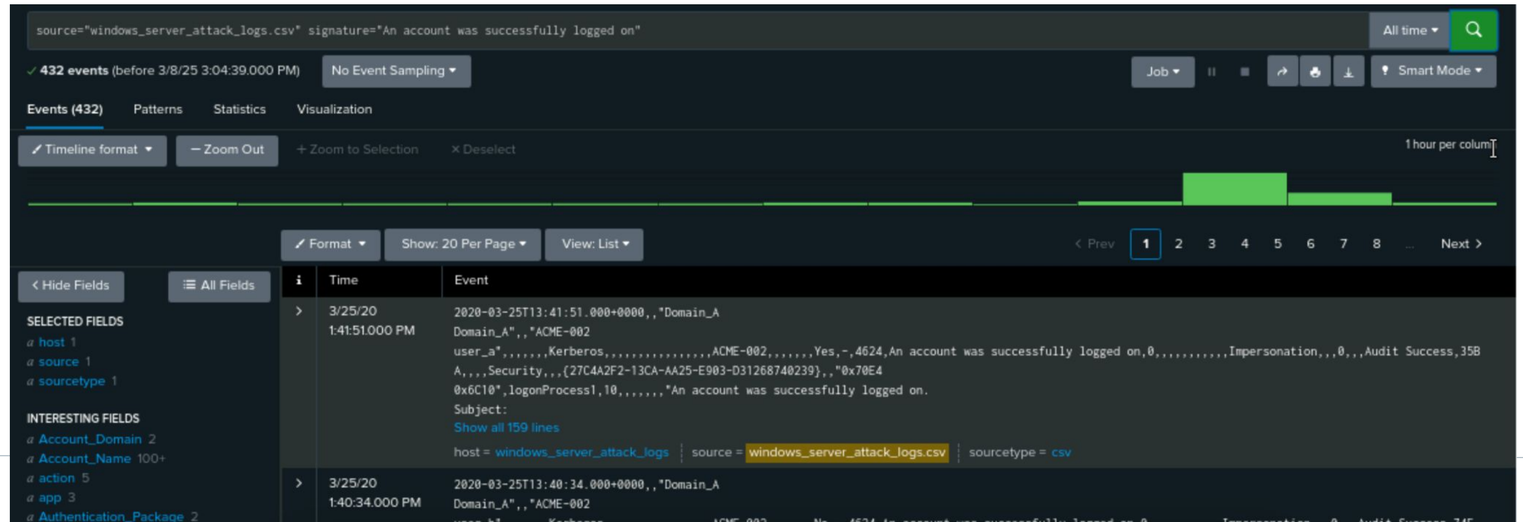
Attack Summary—Windows Server Logs Alerts

ALERT ANALYSIS FOR SUCCESSFUL LOGINS

Pre Attack

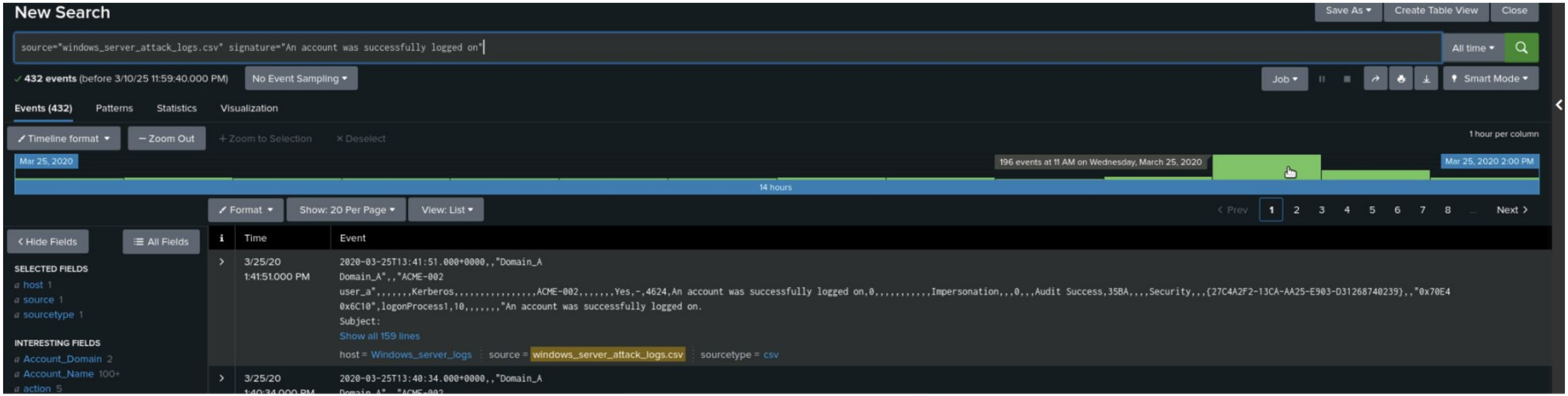


Post Attack



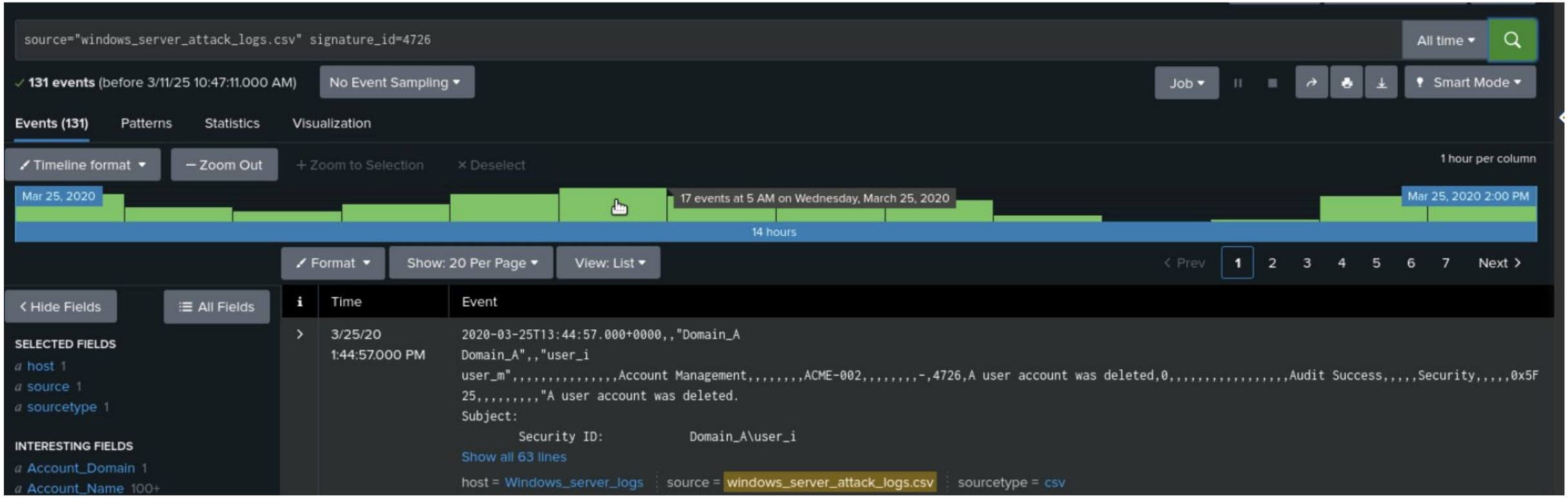
Screenshots of Attack Logs - Windows Server Logs Alerts

ALERT ANALYSIS FOR SUCCESSFUL LOGINS - 196 @ 11AM



Screenshots of Attack Logs - Windows Server Logs Alerts

ALERT ANALYSIS FOR DELETED ACCOUNTS



Attack Summary—Windows Server Logs Dashboard

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

- **Signature Hourly Dashboard Analysis** #1

  Suspicious activity for “**Account locked out**” from 1am to 3am on March 25; Peak count was 896; pre-attack total was 309, post-attack total was 1811

  Suspicious activity for “**Attempt made to reset account password**” from 9am to 11am on March 25; Peak count was 1258; pre-attack total was 295, post-attack total was 2128

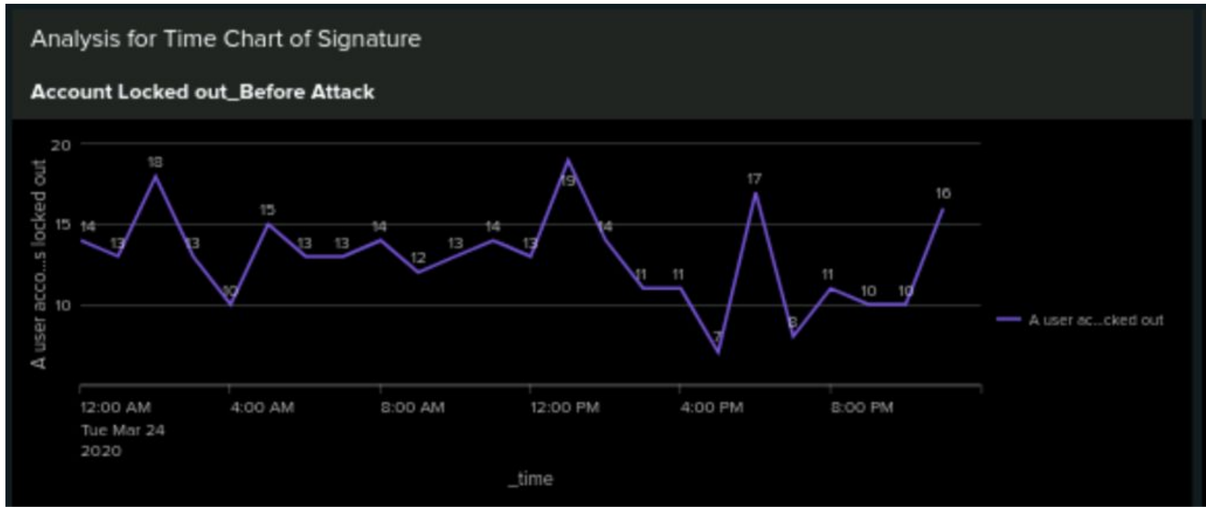
Screenshots of Attack Logs - Windows Server Logs Dashboard

DASHBOARD ANALYSIS FOR TIME CHART SIGNATURE

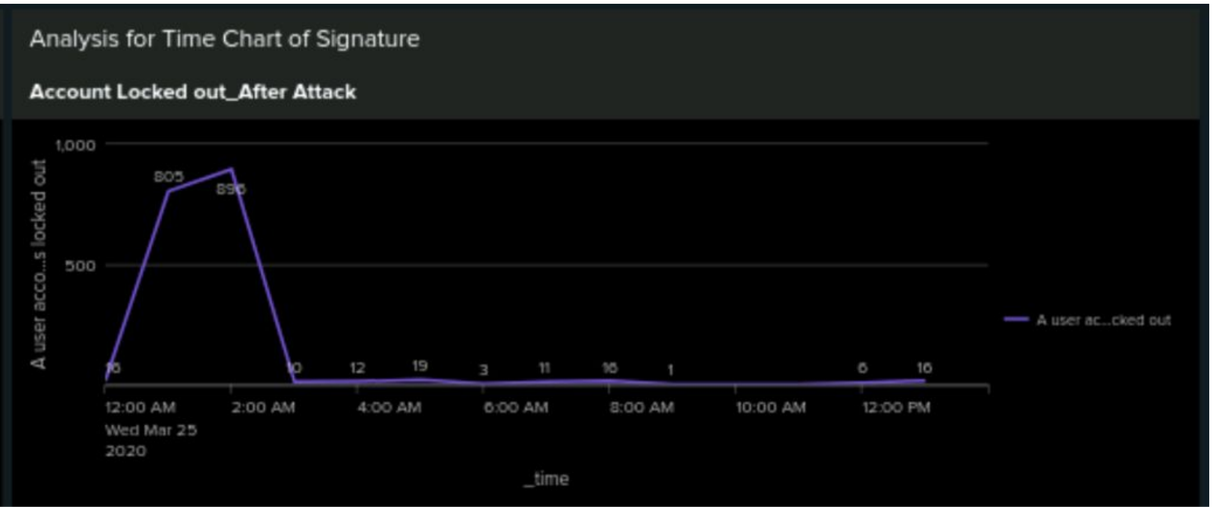
Screenshots of Attack Logs - Windows Server Logs Dashboard

DASHBOARD ANALYSIS FOR TIME CHART SIGNATURE = USER ACCOUNT LOCKED OUT

Pre Attack



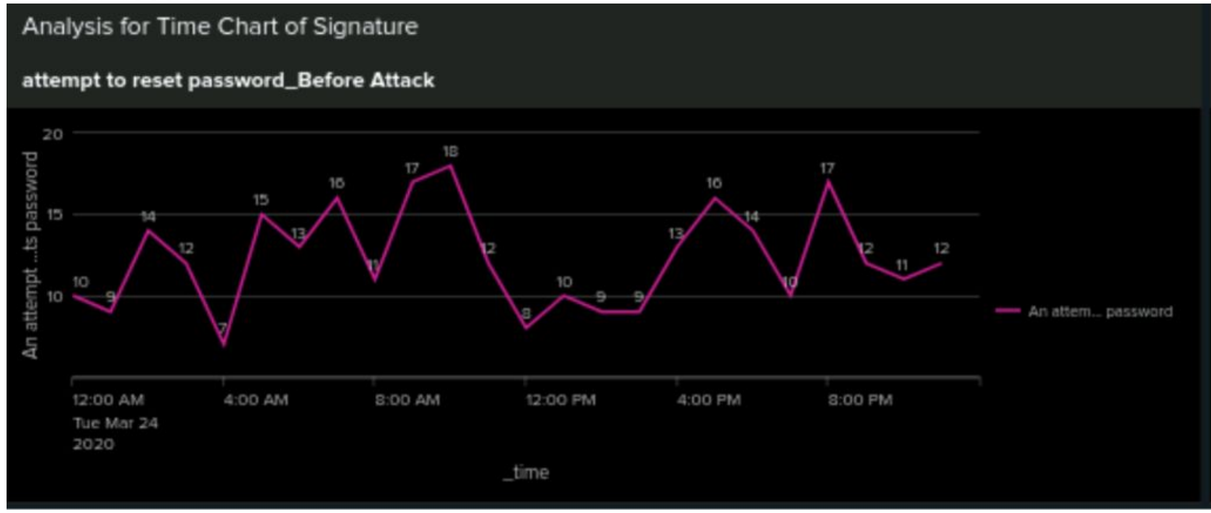
Post Attack



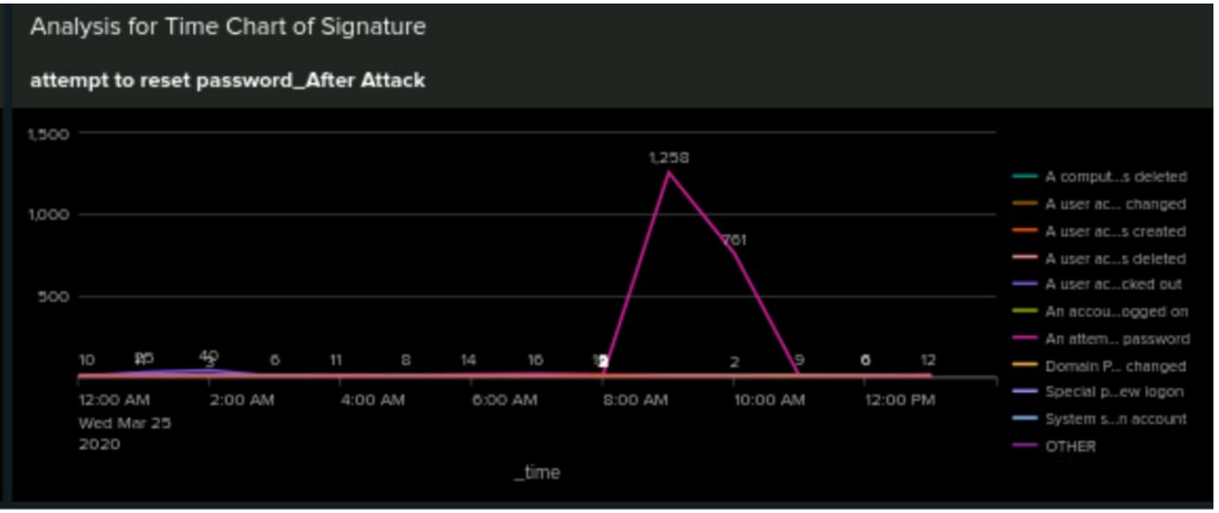
Screenshots of Attack Logs - Windows Server Logs Dashboard

DASHBOARD ANALYSIS FOR TIME CHART SIGNATURE = ATTEMPT TO RESET ACCOUNT PASSWORD

Pre Attack



Post Attack



Attack Summary—Windows Server Logs Dashboard

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

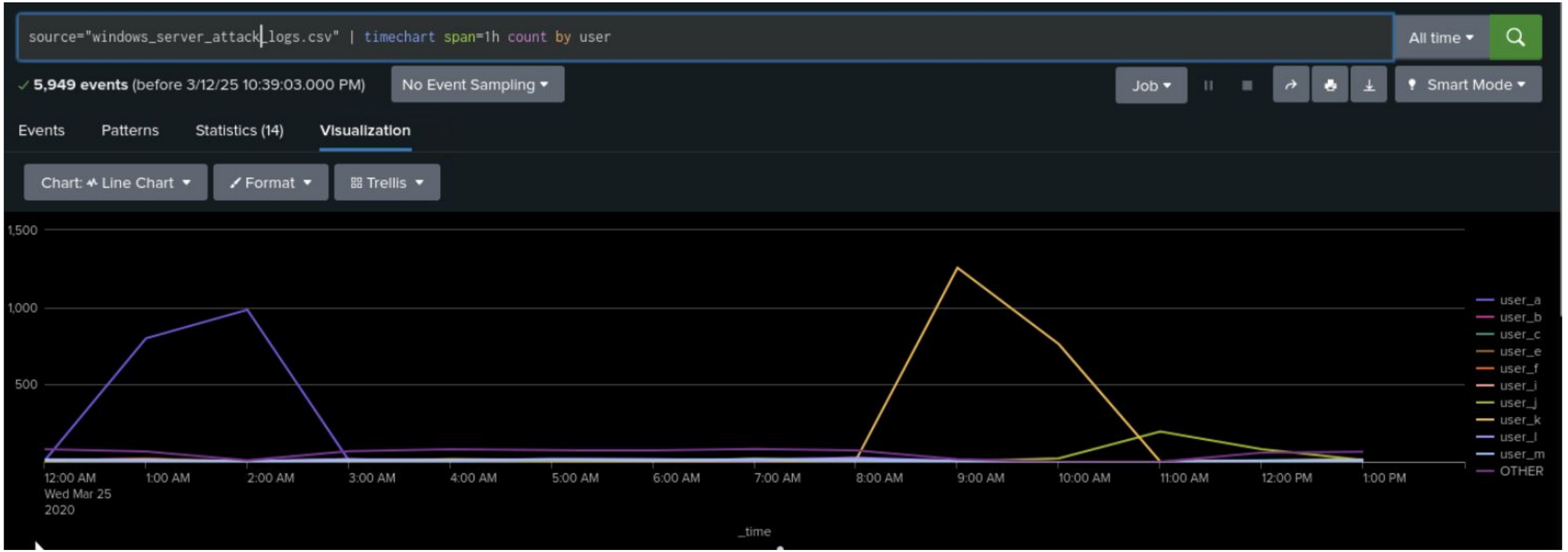
- **User Hourly Dashboard Analysis #2**

  Suspicious activity on March 25 for “**user k**” from 9am to 11am, peak count of 1256; “**user a**” from 1am to 2am, peak count of 984;

  “**user k**”: post-attack count 2118 (36% of total), pre-attack count 260 (5% of total); “**user a**”: post-attack count 1878 (32% of total), pre-attack count of 282 (6% of total)

Screenshots of Attack Logs - Windows Server Logs Dashboard

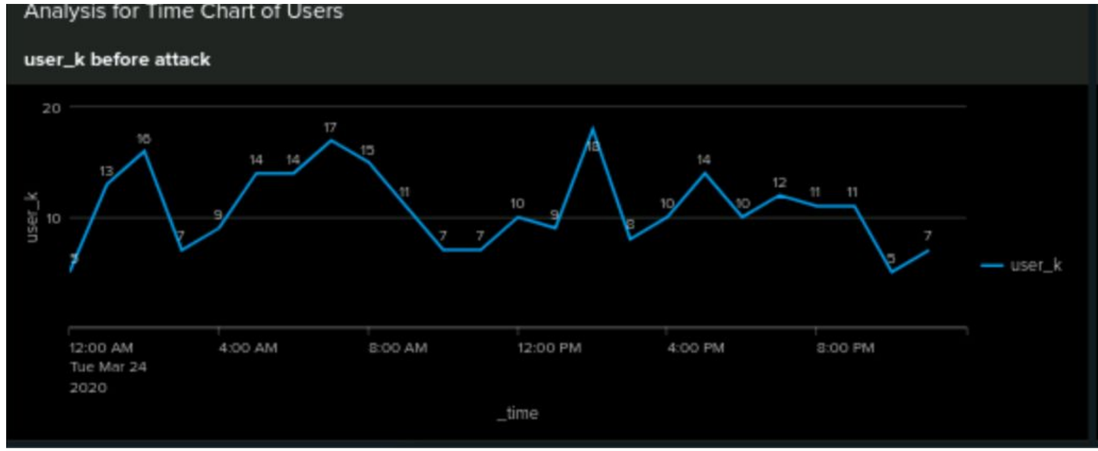
DASHBOARD ANALYSIS FOR USER HOURLY



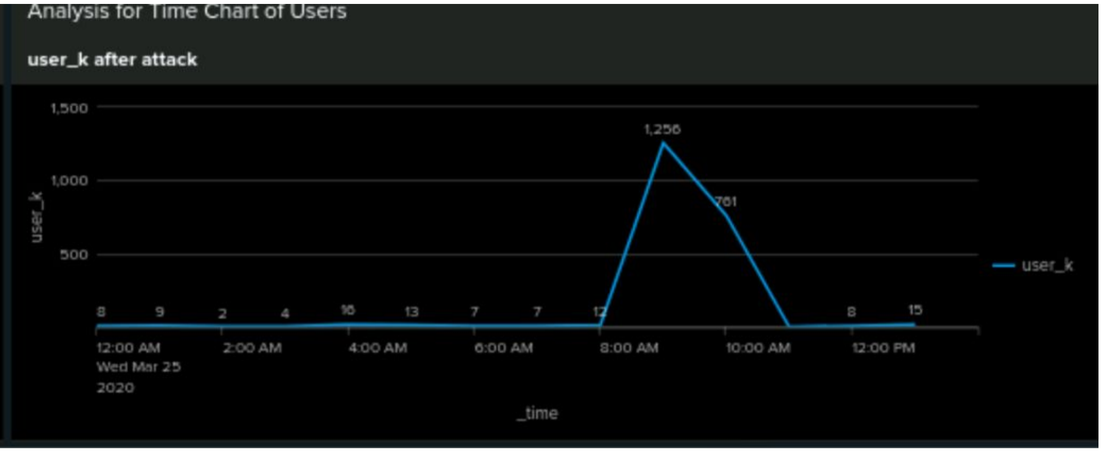
Screenshots of Attack Logs - Windows Server Logs Dashboard

DASHBOARD ANALYSIS FOR USER HOURLY = USER K

Pre Attack



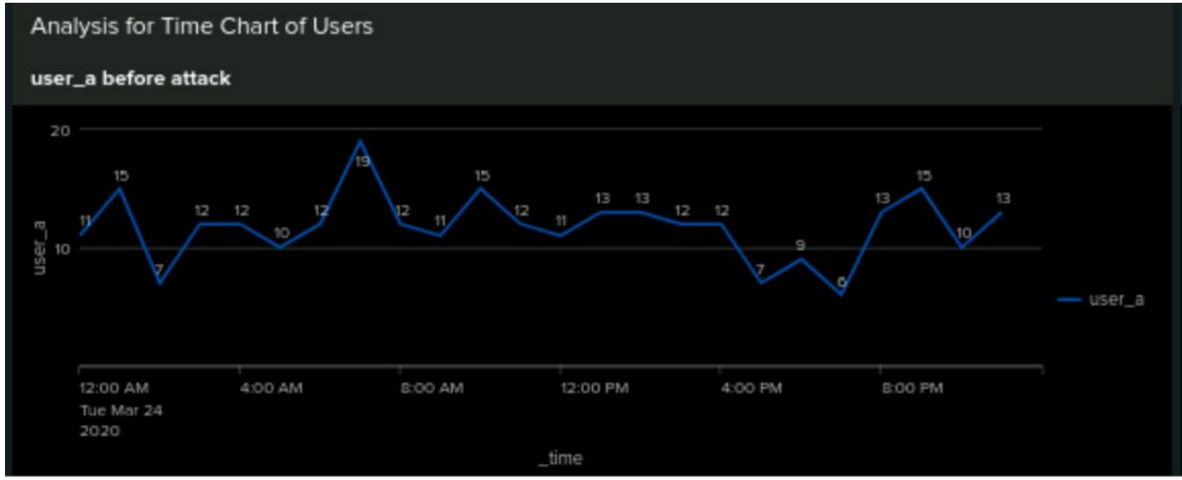
Post Attack



Screenshots of Attack Logs - Windows Server Logs Dashboard

DASHBOARD ANALYSIS FOR USER HOURLY = USER A

Pre Attack



Post Attack

Attack Summary—Windows Server Logs Dashboard

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

- **Signature Count Dashboard Analysis #3**

  Suspicious activity for “**Account locked out**”; pre-attack total was 309, post-attack total was 1811

  Suspicious activity for “**Attempt made to reset account password**”; pre-attack total was 295, post-attack total was 2128

Screenshots of Attack Logs - Windows Server Logs Dashboard

DASHBOARD ANALYSIS FOR SIGNATURE COUNT

Attack Summary—Windows Server Logs Dashboard

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

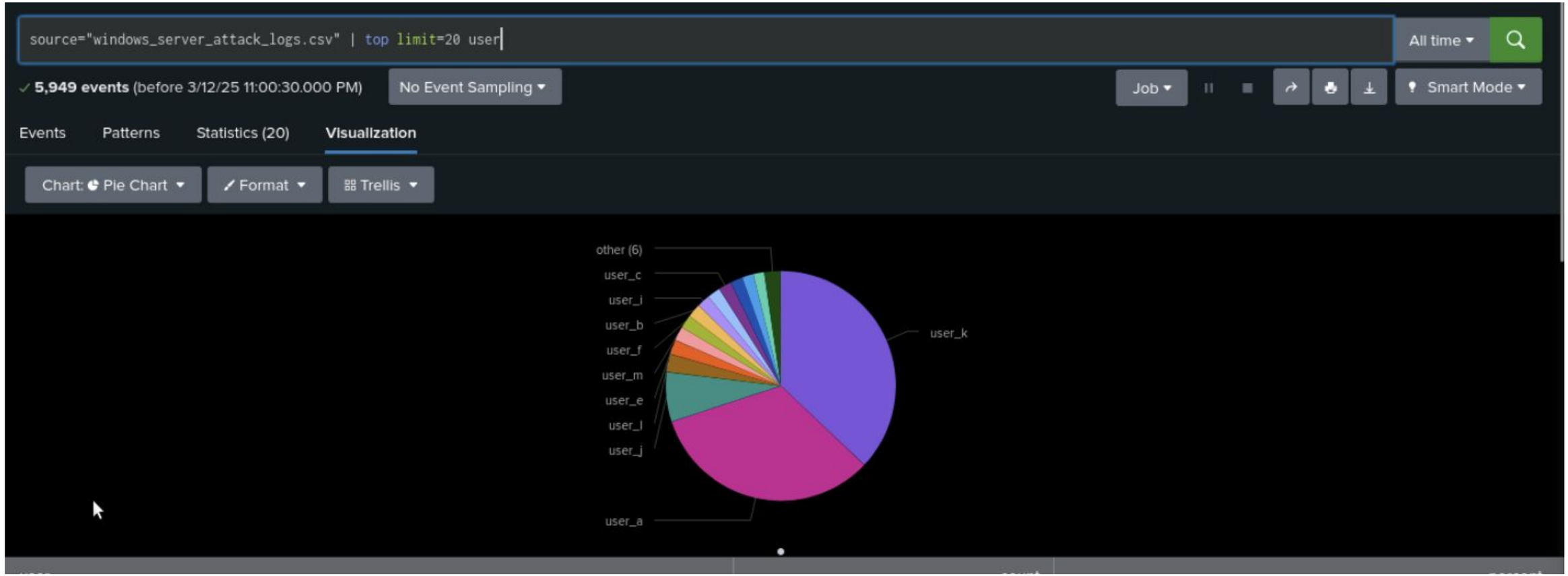
- **User Count Dashboard Analysis #4**

  Suspicious activity for “**user k**”: post-attack count 2118, 36% of total; pre-attack count 260, 5% of total

  Suspicious activity for “**user a**”: post-attack count 1878, 32% of total; pre-attack count of 282, 6% of total

Screenshots of Attack Logs - Windows Server Logs Dashboard

DASHBOARD ANALYSIS FOR USER COUNT



Attack Summary—Windows Server Logs Dashboard

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

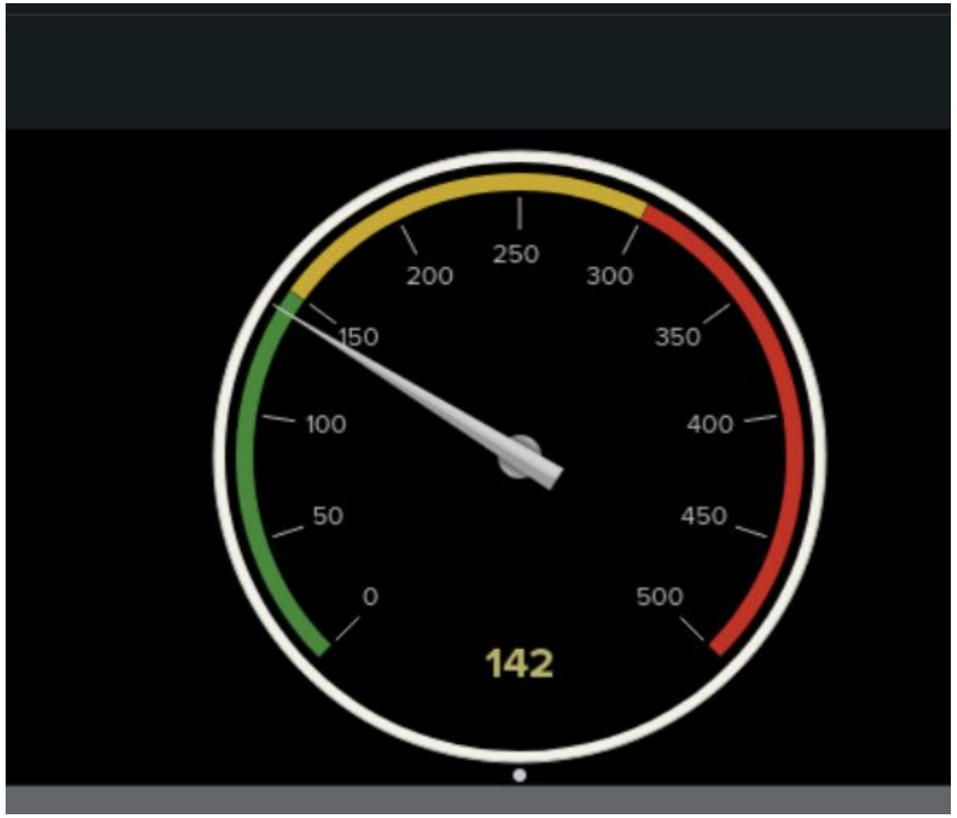
- **Failed Logins #5 - single value visualization**

  Failed logins dropped from 142 pre-attack to 93 post-attack; although this may be an acceptable number of failed logins, it could potentially be interpreted that an attacker has gained access and continues to login successfully

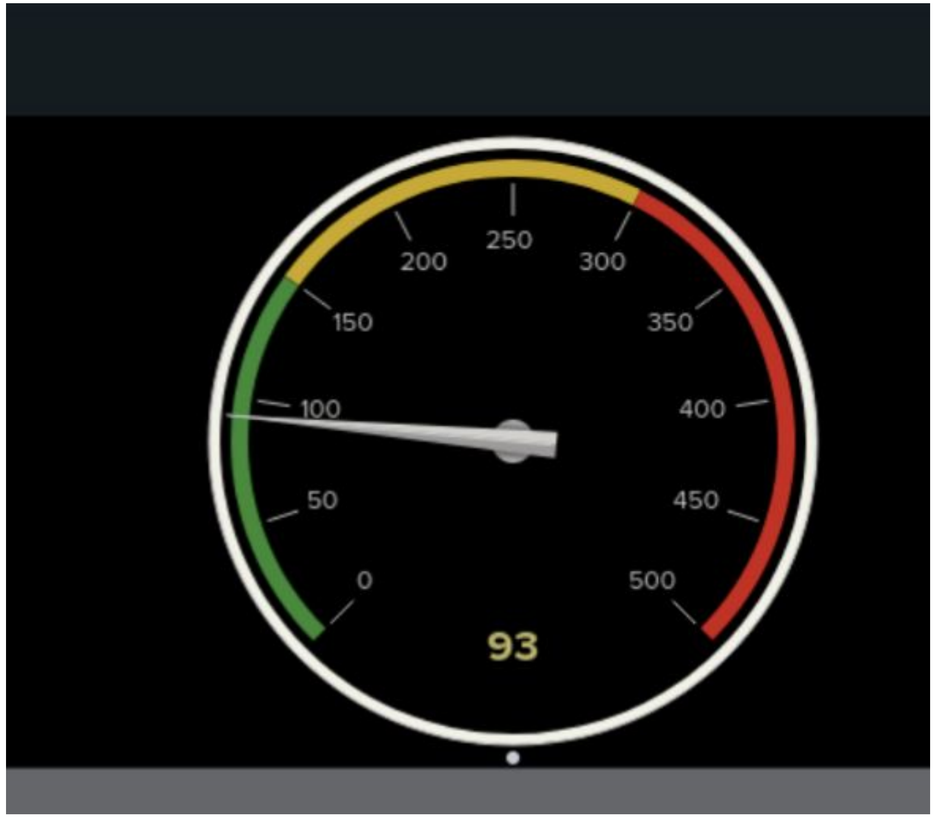
Screenshots of Attack Logs - Windows Server Logs Dashboard

DASHBOARD ANALYSIS FOR FAILED LOGINS

Pre Attack



Post Attack



Screenshots of Attack Logs - Windows Server Logs Dashboard

WINDOWS DASHBOARD PANEL 1 - signature hourly pre vs post attack

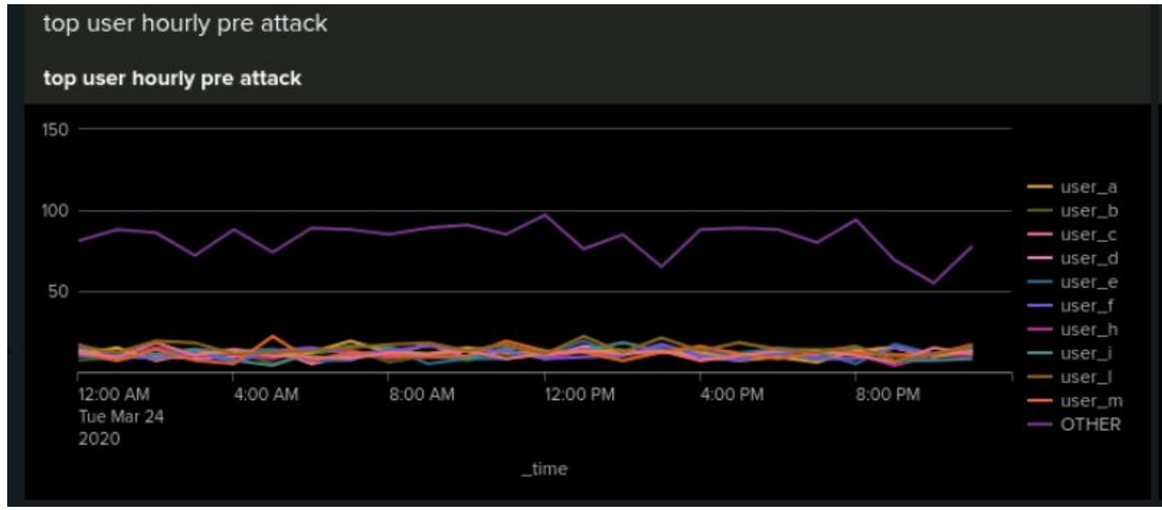
Pre Attack

Post Attack

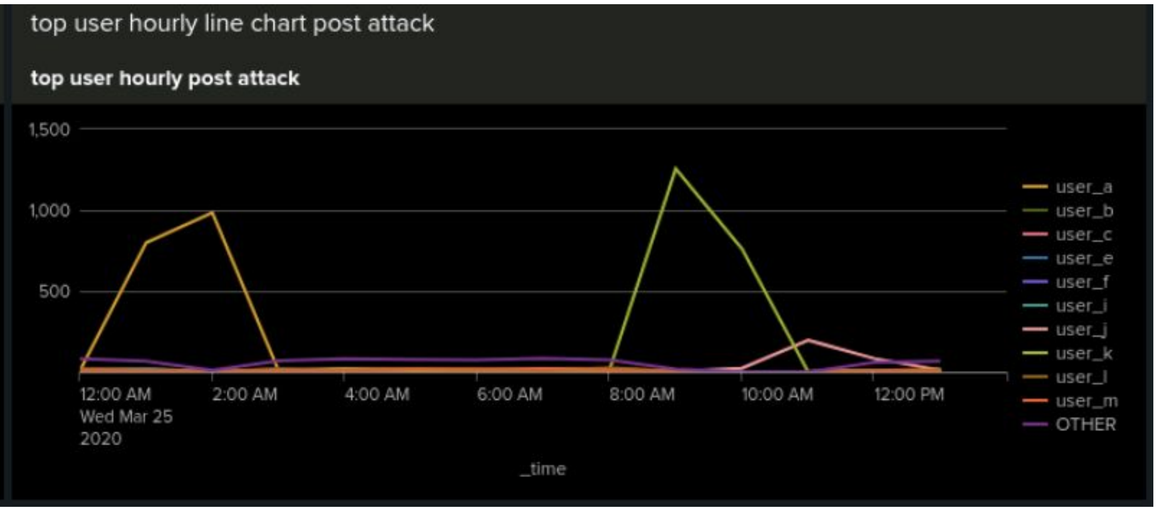
Screenshots of Attack Logs - Windows Server Logs Dashboard

WINDOWS DASHBOARD PANEL 2 - user hourly pre vs post attack

Pre Attack



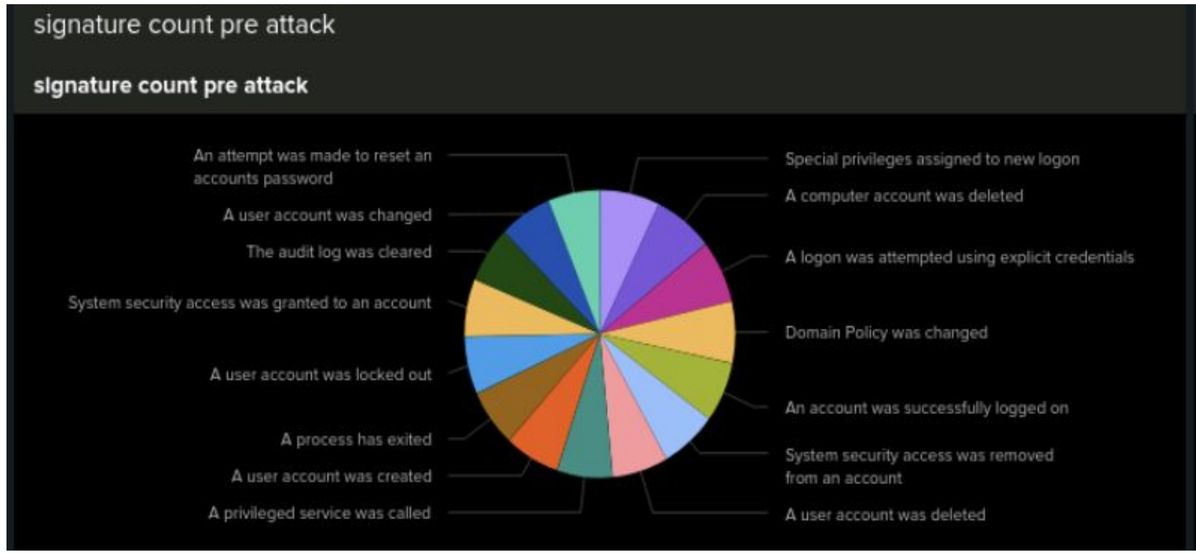
Post Attack



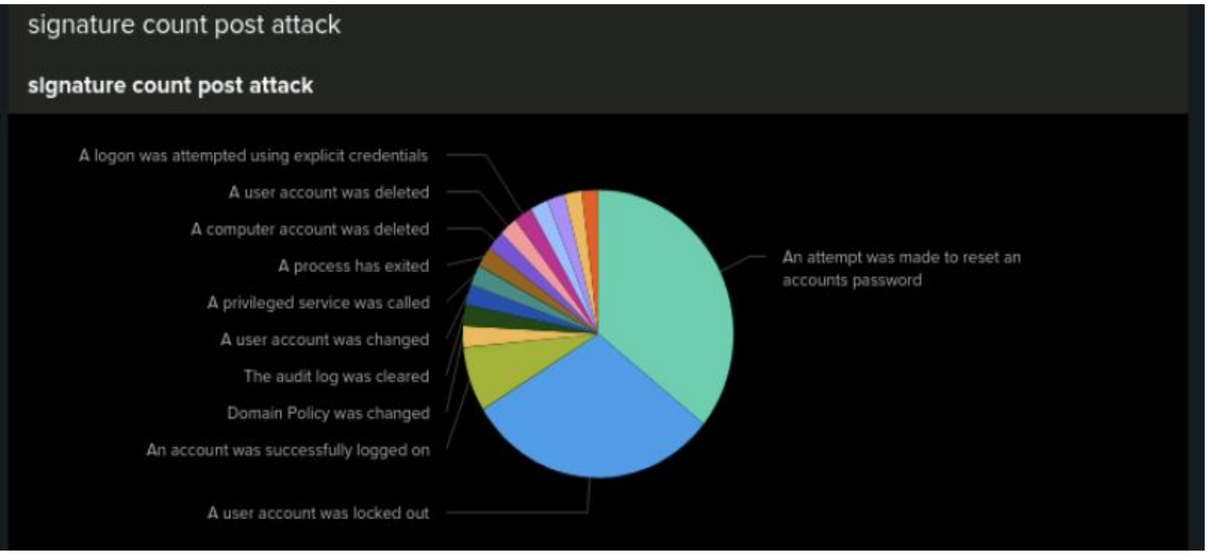
Screenshots of Attack Logs - Windows Server Logs Dashboard

WINDOWS DASHBOARD PANEL 3 - signature count pre vs post attack

Pre Attack



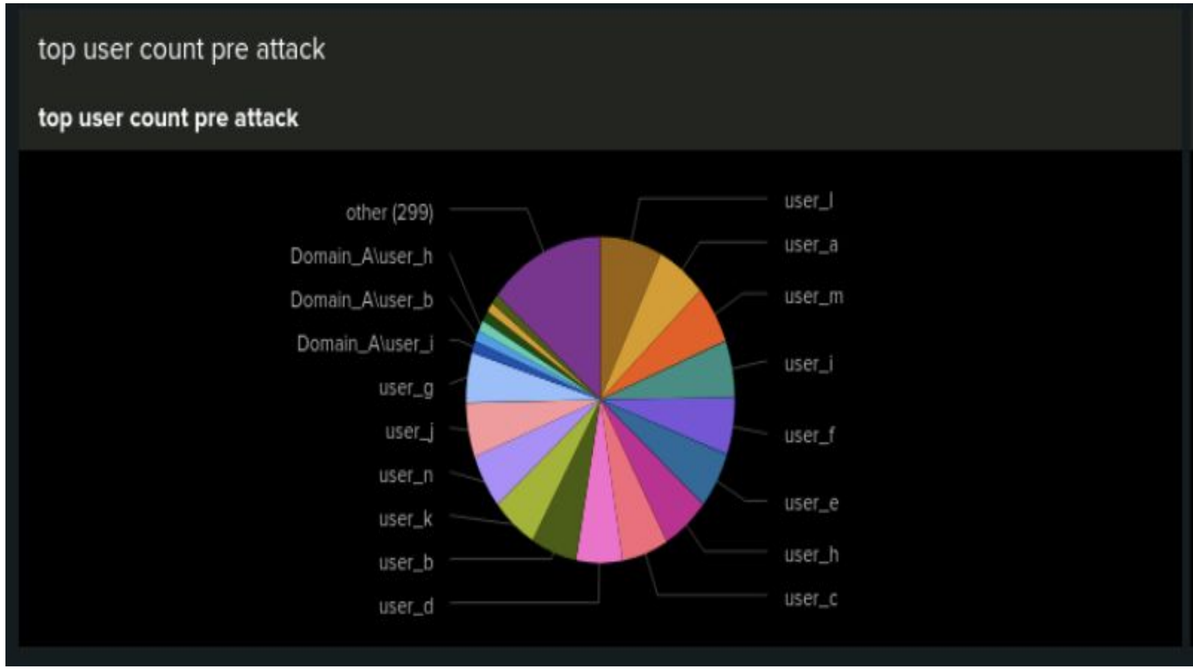
Post Attack



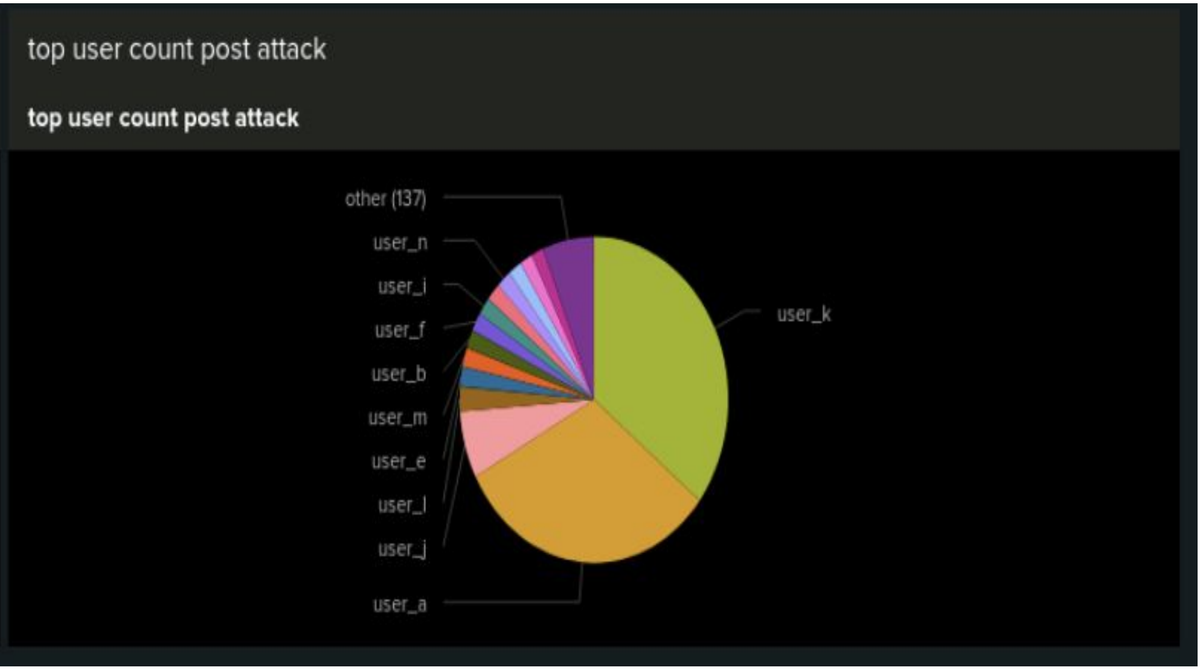
Screenshots of Attack Logs - Windows Server Logs Dashboard

WINDOWS DASHBOARD PANEL 4 - user count pre vs post attack

Pre Attack



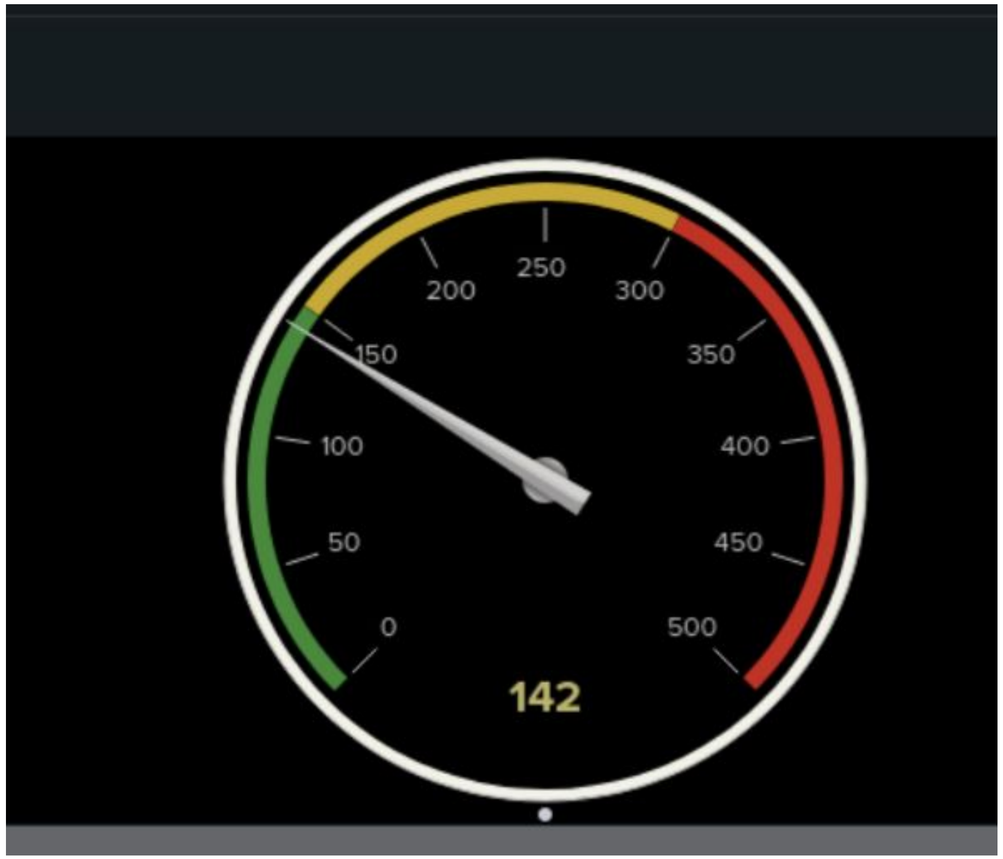
Post Attack



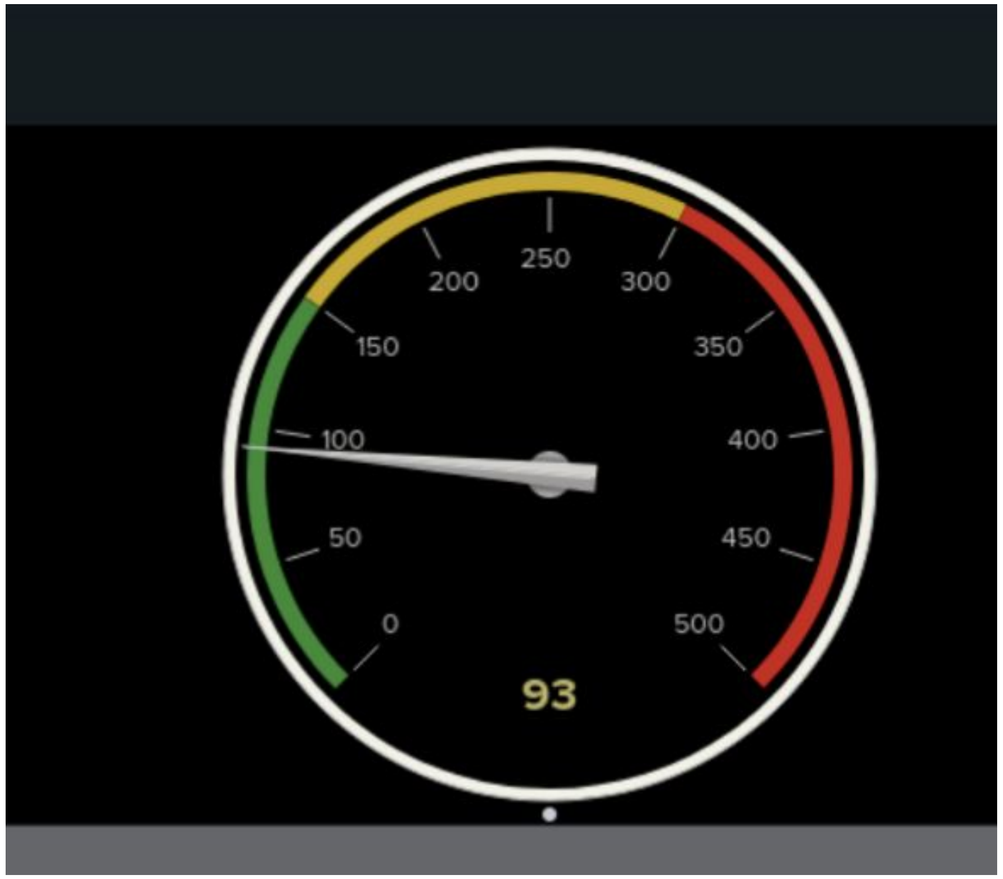
Screenshots of Attack Logs - Windows Server Logs Dashboard

WINDOWS DASHBOARD PANEL 5 - failed logins pre vs post attack

Pre Attack



Post Attack



Attack Summary—Apache Reports

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

- **HTTP Method Report**
  Suspicious decrease in GET by 29% and suspicious increase in POST by 29%
  POST is used to submit or update information to a web server

- **Referrer Domain Report**
  There were no suspicious referrer domains during the attack

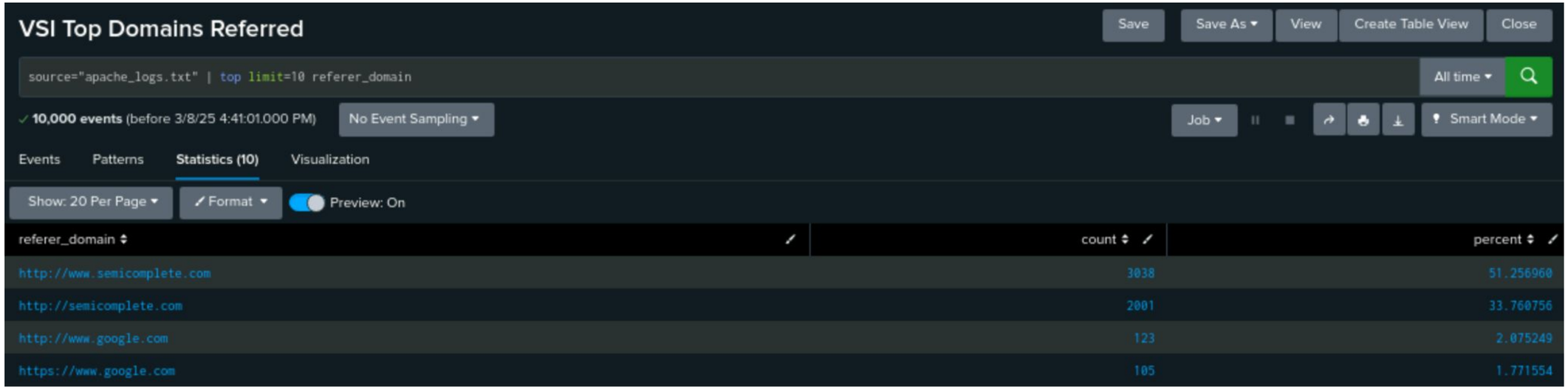
- **HTTP Response Code Report**
  There were several small changes overall, the most suspicious change detected occurred with the 404 response code increasing from 2% to 15%

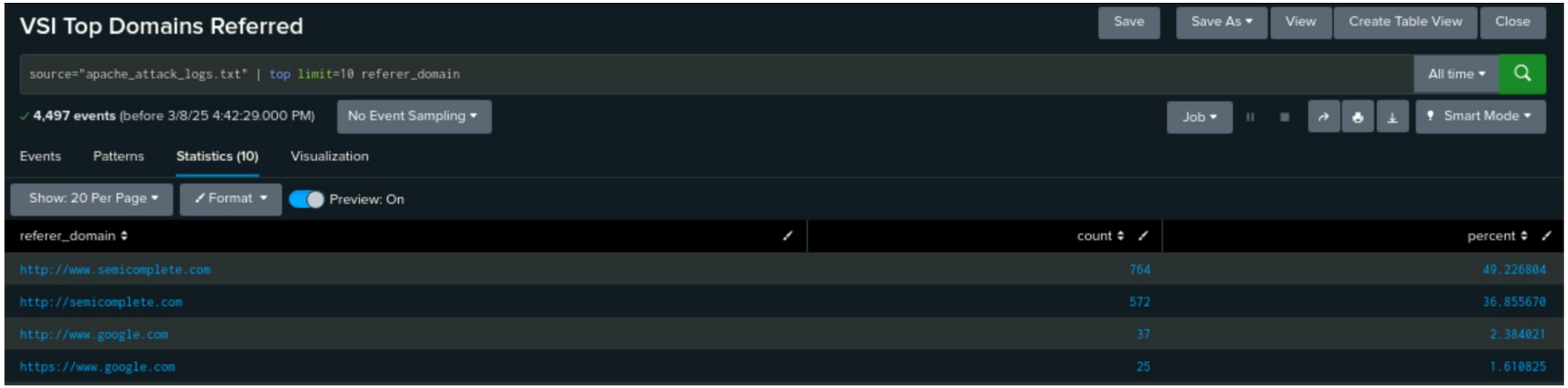
Screenshots of Attack Logs - Apache Reports

REPORT ANALYSIS FOR METHODS

Screenshots of Attack Logs - Apache Reports

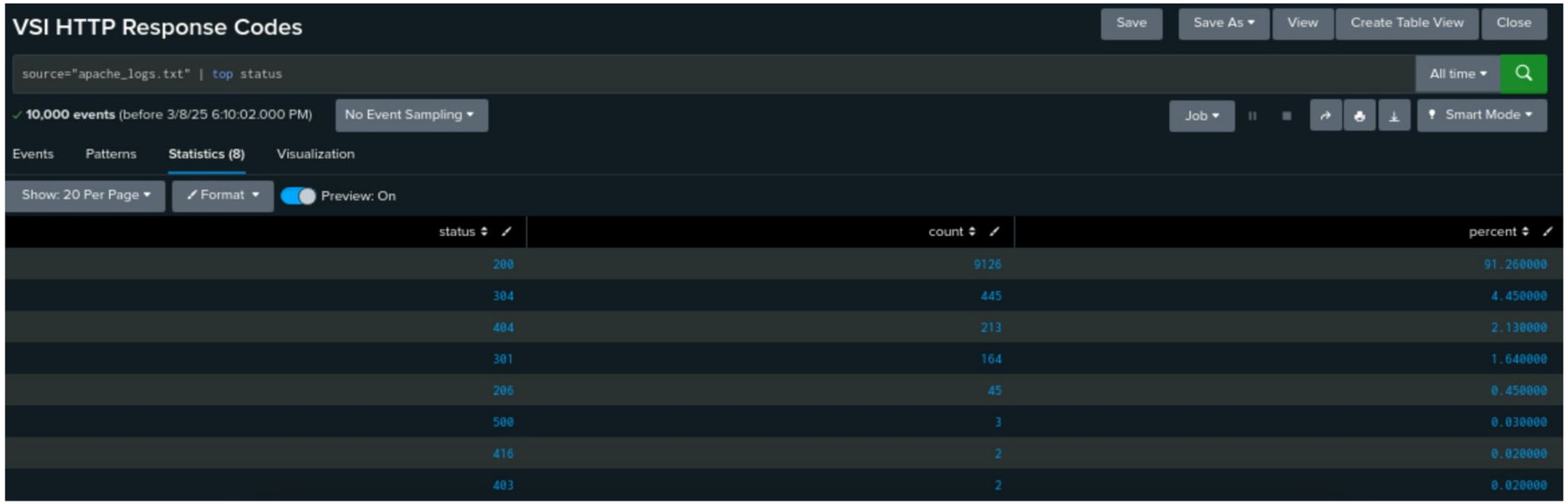
REPORT ANALYSIS FOR Top Domain Referred



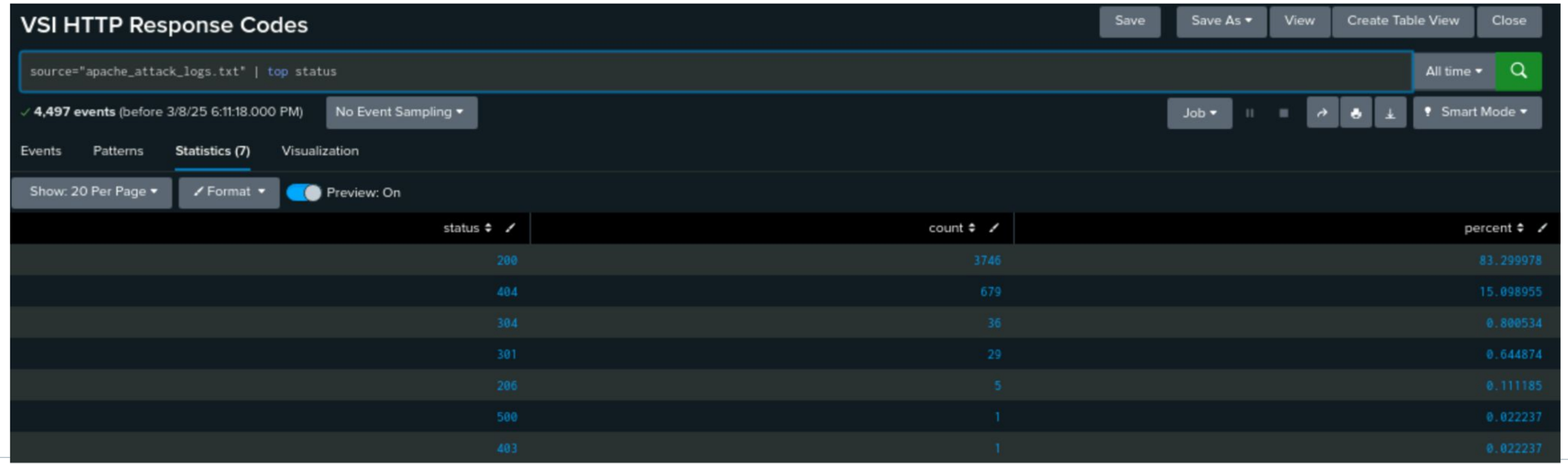


Screenshots of Attack Logs - Apache Reports

REPORT ANALYSIS FOR HTTP RESPONSE CODES



status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000



status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Attack Summary— Apache Alerts

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

- **International Country Activity Alert (Non-US)**

  Suspicious activity in the **Ukraine** at 8pm on March 25, total count of **937** events during the attack

  Alert threshold is 170 so alert was successful

- **HTTP Post Activity Alert**

  Suspicious increase in **POST method** activities, total count of **1296** events on March 25 at 8pm

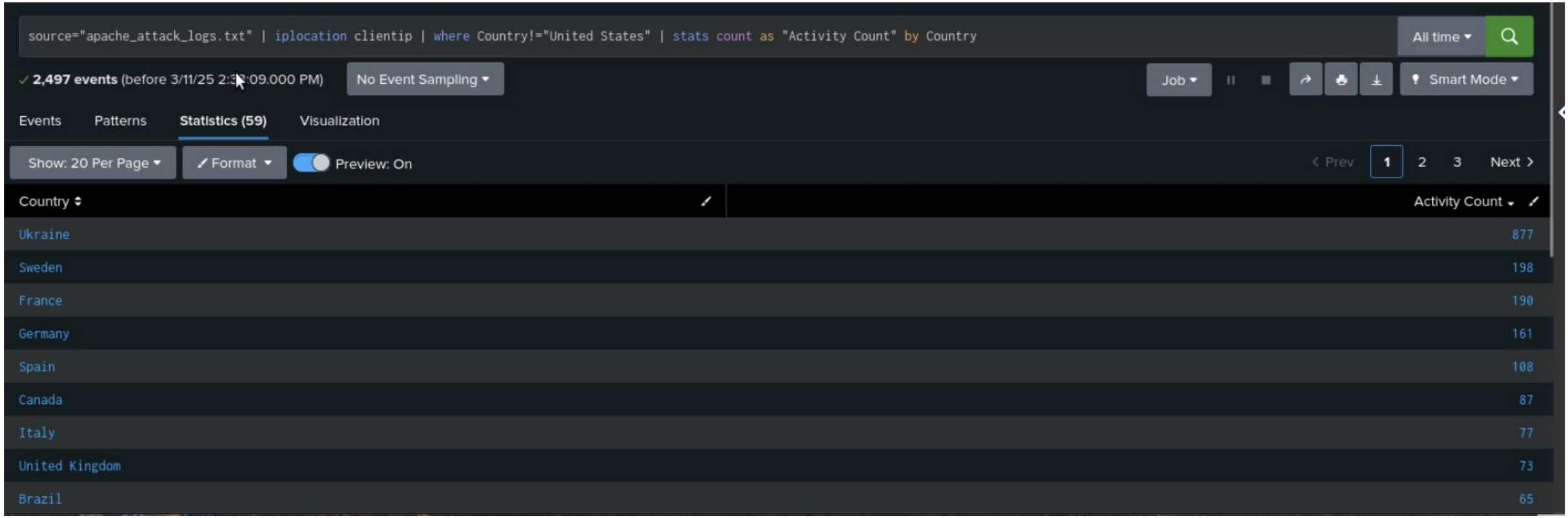
  Alert threshold is 12 so alert was successful

Screenshots of Attack Logs - Apache Alerts

ALERT ANALYSIS FOR INTERNATIONAL ACTIVITY

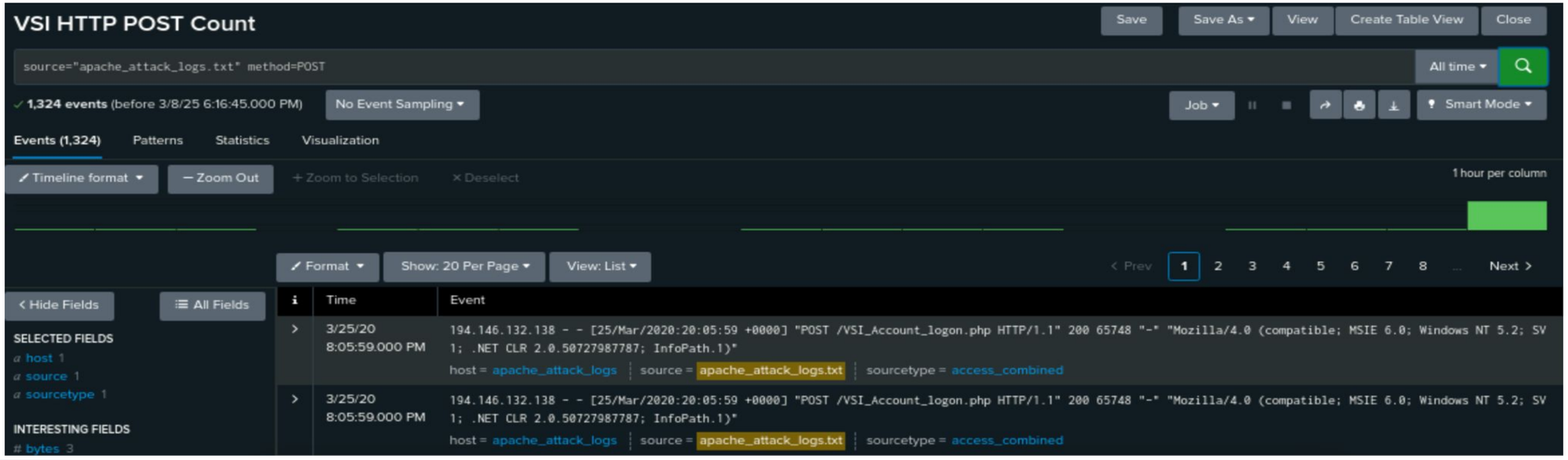
Screenshots of Attack Logs - Apache Alerts

ALERT ANALYSIS FOR INTERNATIONAL COUNTRY ACTIVITY = UKRAINE



Screenshots of Attack Logs - Apache Alerts

ALERT ANALYSIS FOR HTTP POST ACTIVITY



Attack Summary—Apache Dashboard

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

- **HTTP Method Time Chart Dashboard Analysis**

  Suspicious activity with the **GET method** at 6pm on March 25, **peak count was 729**; activity occurred between 5pm and 7pm;

  Suspicious activity with the **POST method** at 8pm on March 25, **peak count was 1296**; activity occurred between 7pm and 9pm;

  both methods seem to be used in the attack

- **Cluster Map Dashboard Analysis**

  Suspicious activity from **Ukraine**, specifically in the cities of **Kiev** and **Kharkiv** which both had a high volume of activity;

  Kiev total count of 438, Kharkiv total count of 432

- **URI Data Dashboard Analysis**

  Suspicious activity on March 25 with the **URI** “/files/logstash/logstash-1.3.2-monolithic.jar” from 5pm to 7pm and with the URI “/VSI_Account_logon.php” from 7pm to 9pm

  URI “/VSI_Account_logon.php” was hit the most with **1323 events** indicating the attacker may be attempting to brute force the VSI logon page

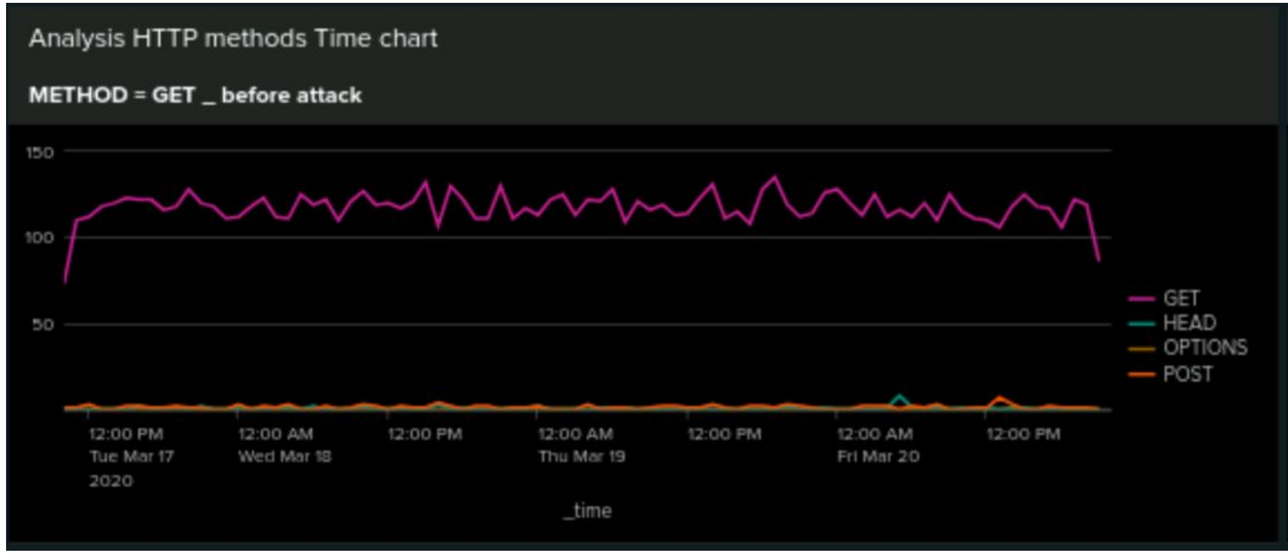
Screenshots of Attack Logs - Apache Dashboard

DASHBOARD ANALYSIS FOR TIME CHART HTTP METHOD

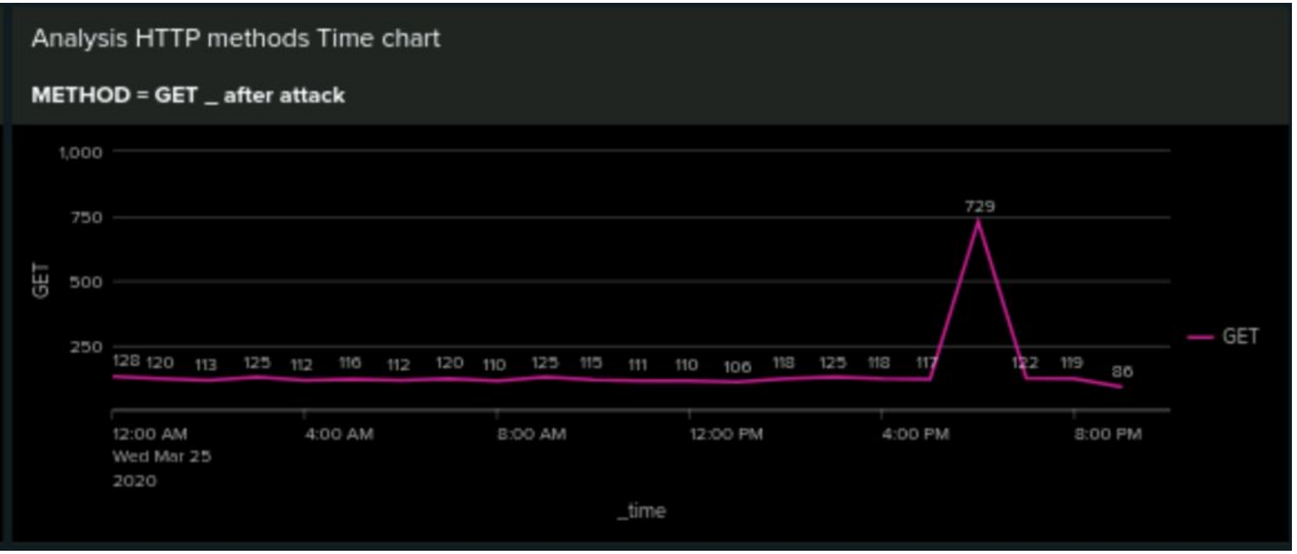
Screenshots of Attack Logs - Apache Dashboard

DASHBOARD ANALYSIS FOR TIME CHART HTTP METHOD = GET

Pre Attack



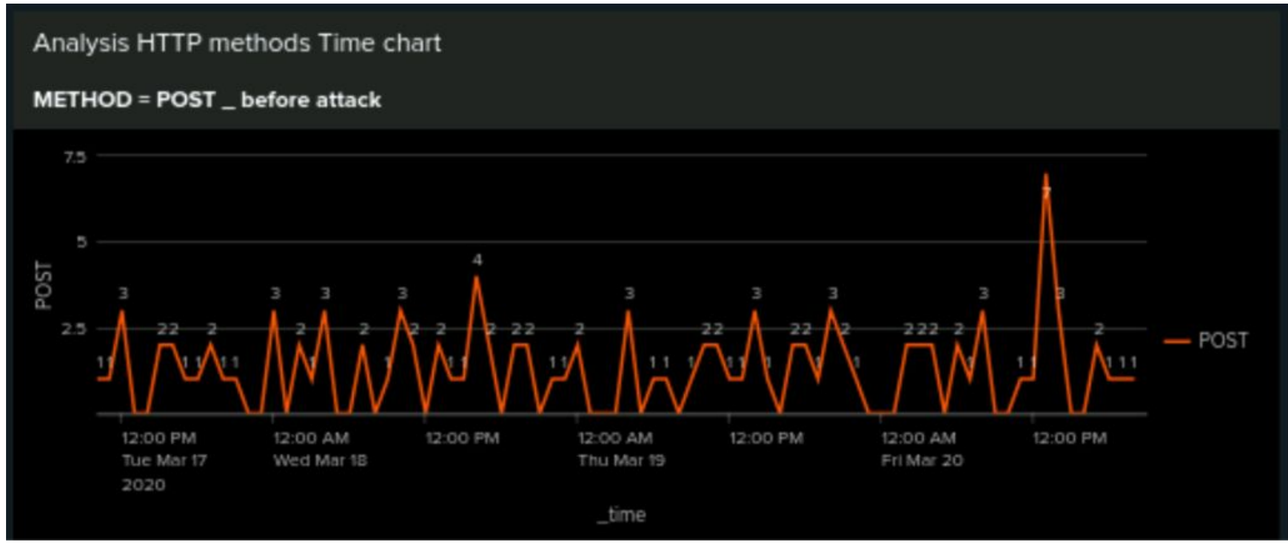
Post Attack



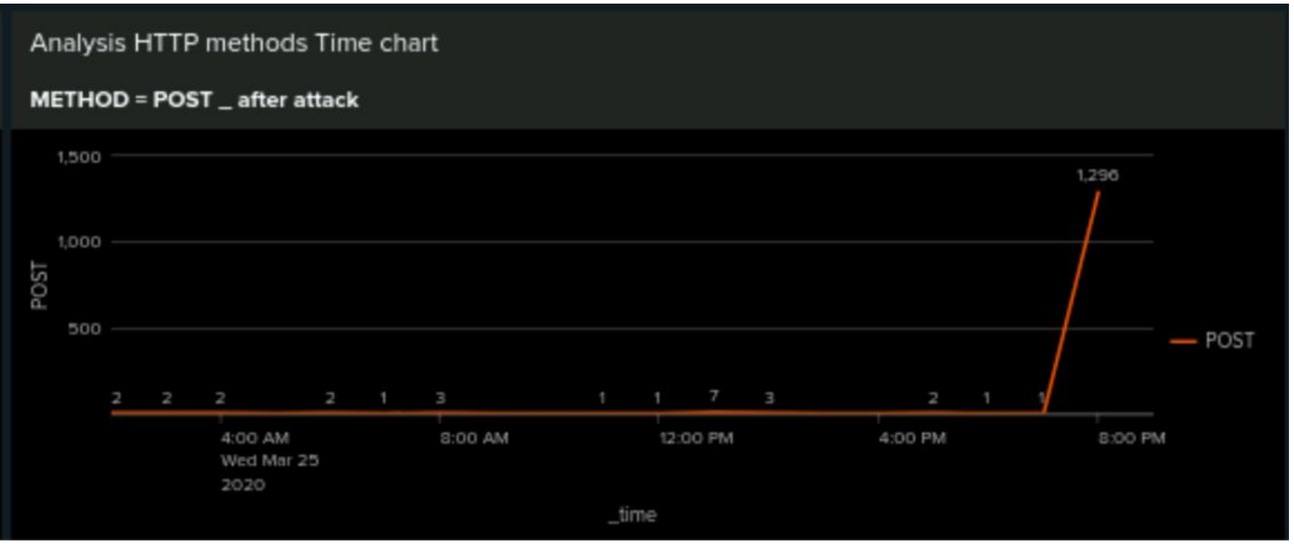
Screenshots of Attack Logs - Apache Dashboard

DASHBOARD ANALYSIS FOR TIME CHART HTTP METHOD = POST

Pre Attack

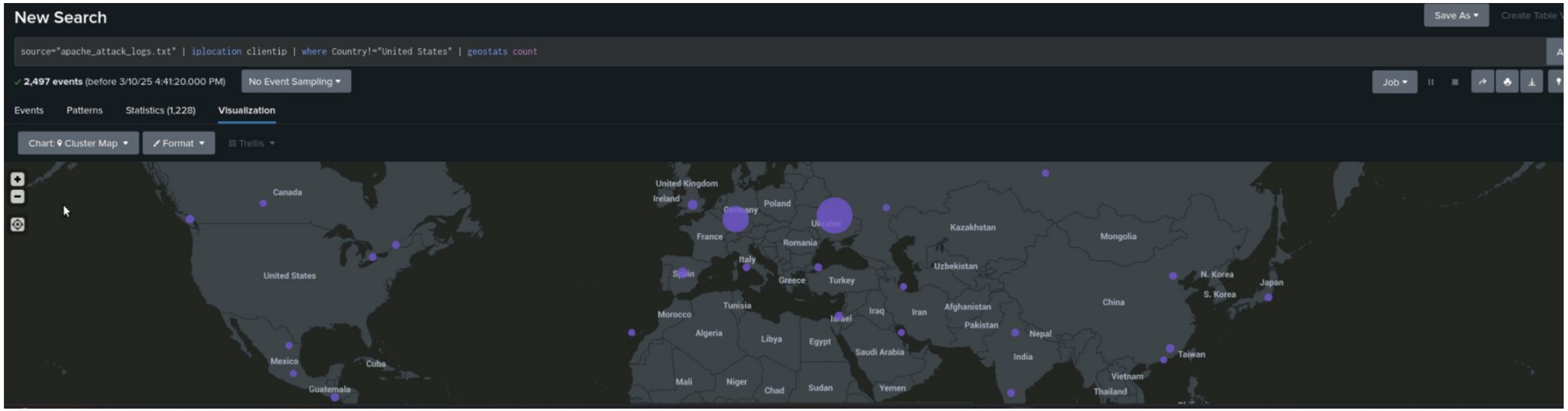


Post Attack

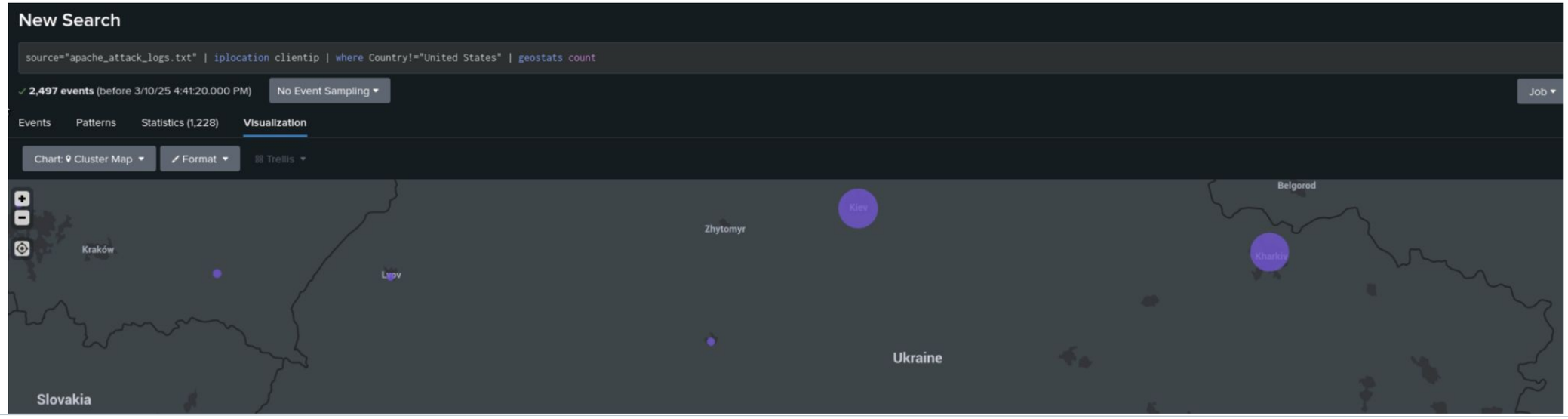


Screenshots of Attack Logs - Apache Dashboard

DASHBOARD ANALYSIS FOR CLUSTER MAP = COUNTRY (Pre Attack)



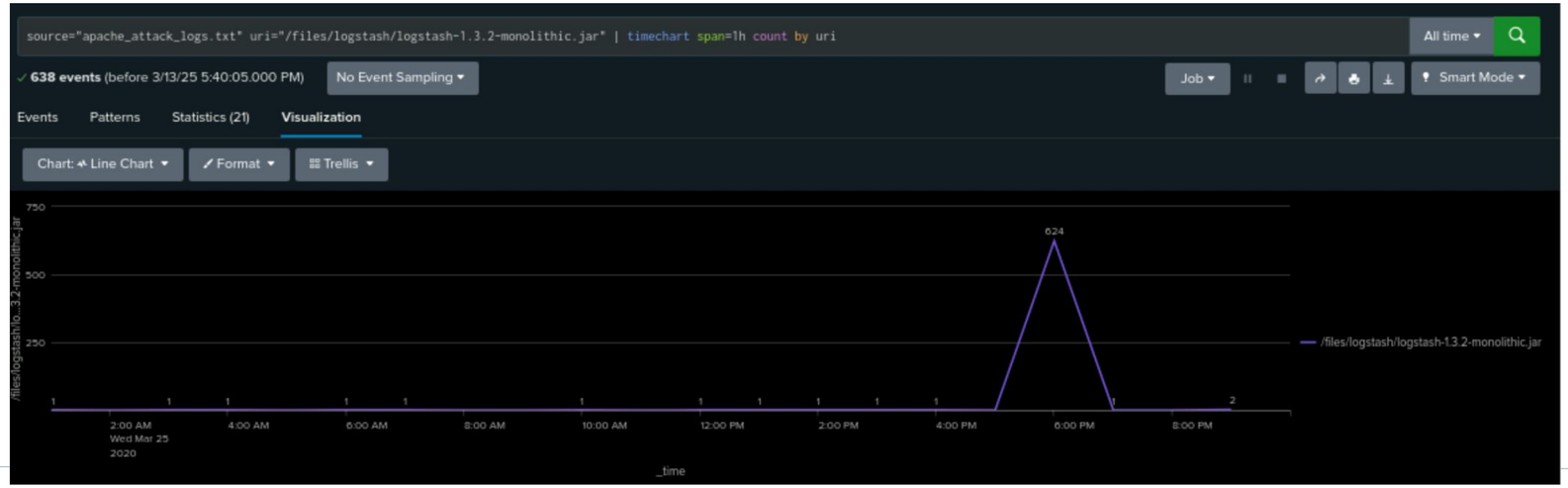
DASHBOARD ANALYSIS FOR CLUSTER MAP = CITIES (Post Attack)



Screenshots of Attack Logs - Apache Dashboard

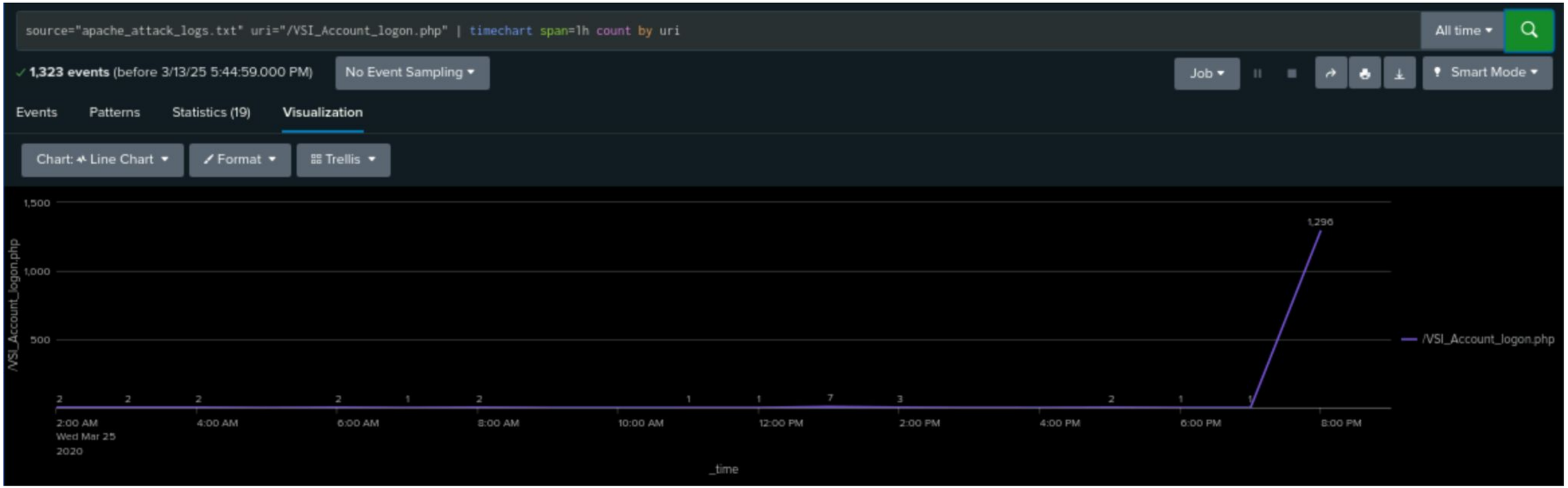
DASHBOARD ANALYSIS FOR URI DATA

DASHBOARD ANALYSIS FOR URI DATA = LOGSTASH



Screenshots of Attack Logs - Apache Dashboard

DASHBOARD ANALYSIS FOR URI DATA = ACCOUNT LOGON

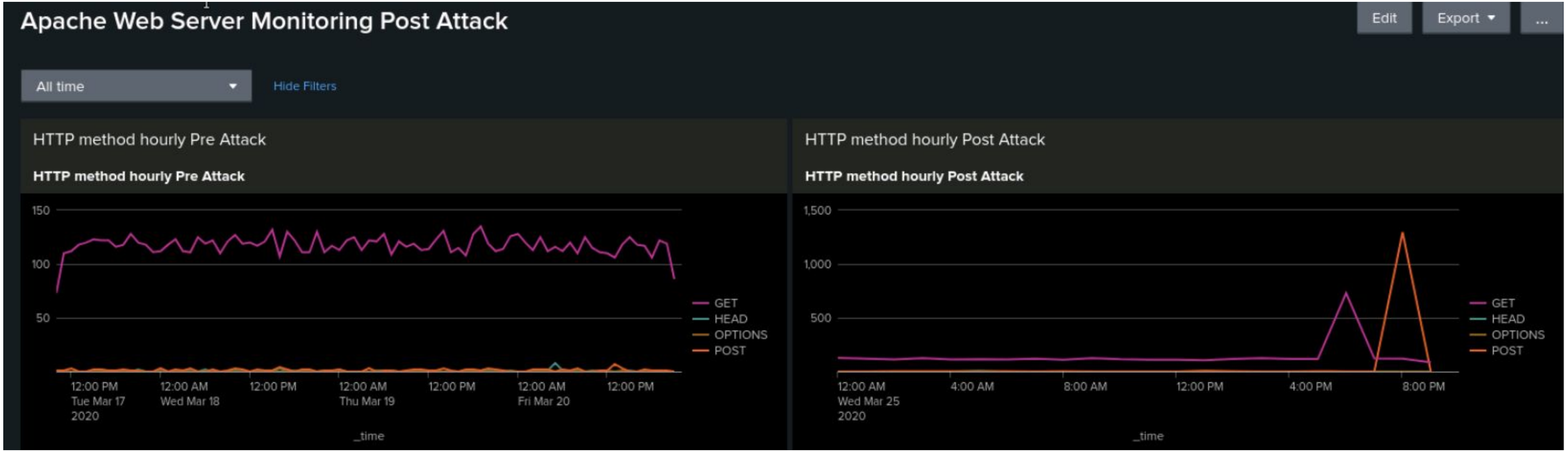


Screenshots of Attack Logs - Apache Dashboard

APACHE DASHBOARD PANEL 1 - HTTP method pre vs post attack

Pre Attack

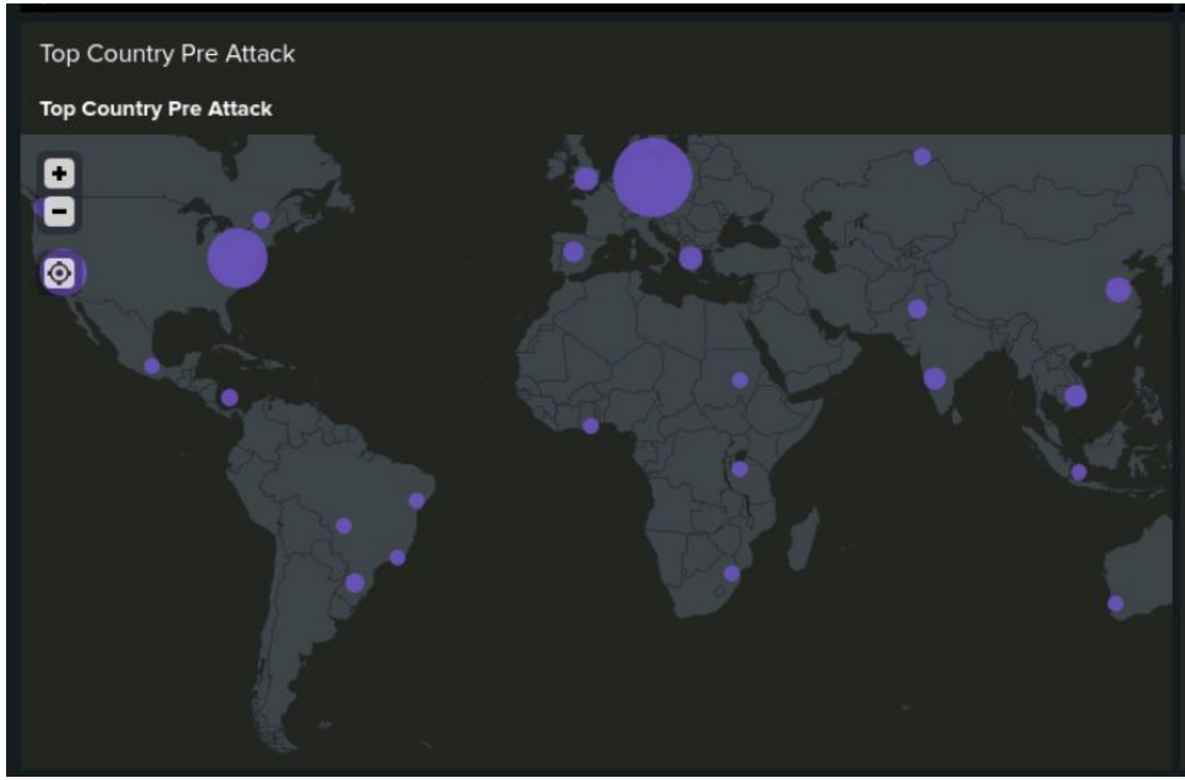
Post Attack



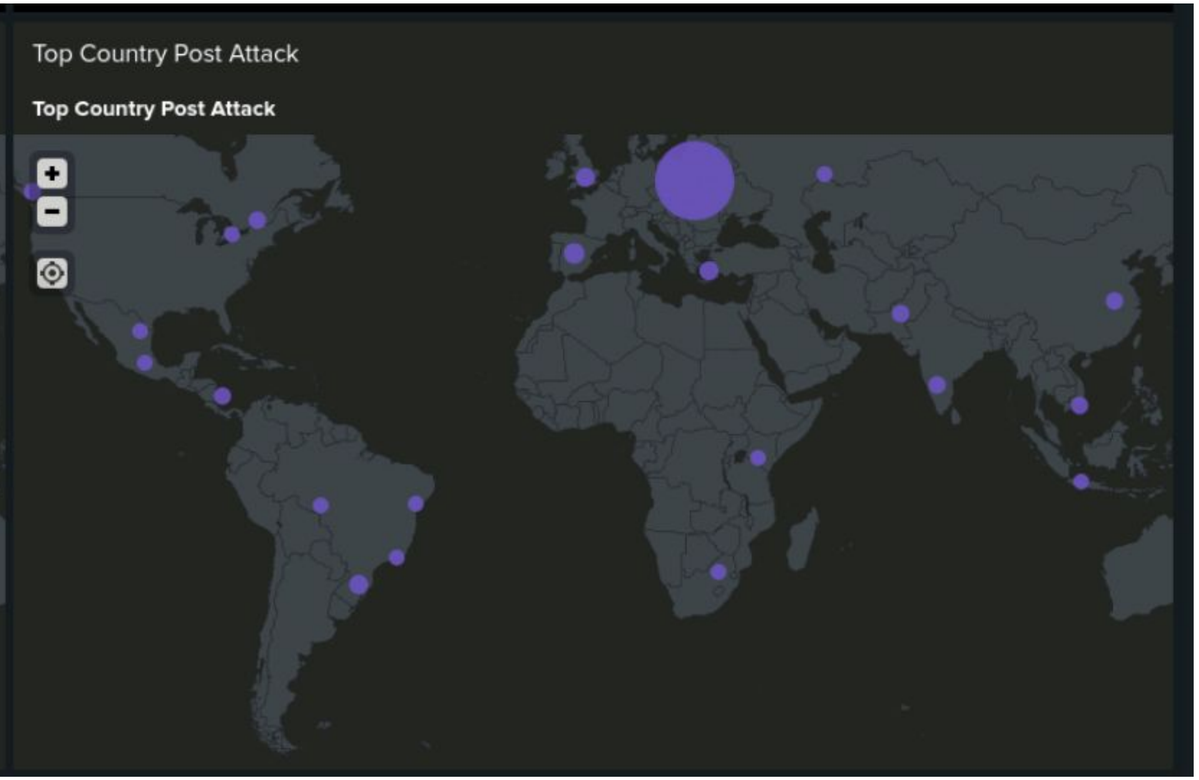
Screenshots of Attack Logs - Apache Dashboard

APACHE DASHBOARD PANEL 2 - Country (non-US) pre vs post attack - Cluster

Pre Attack



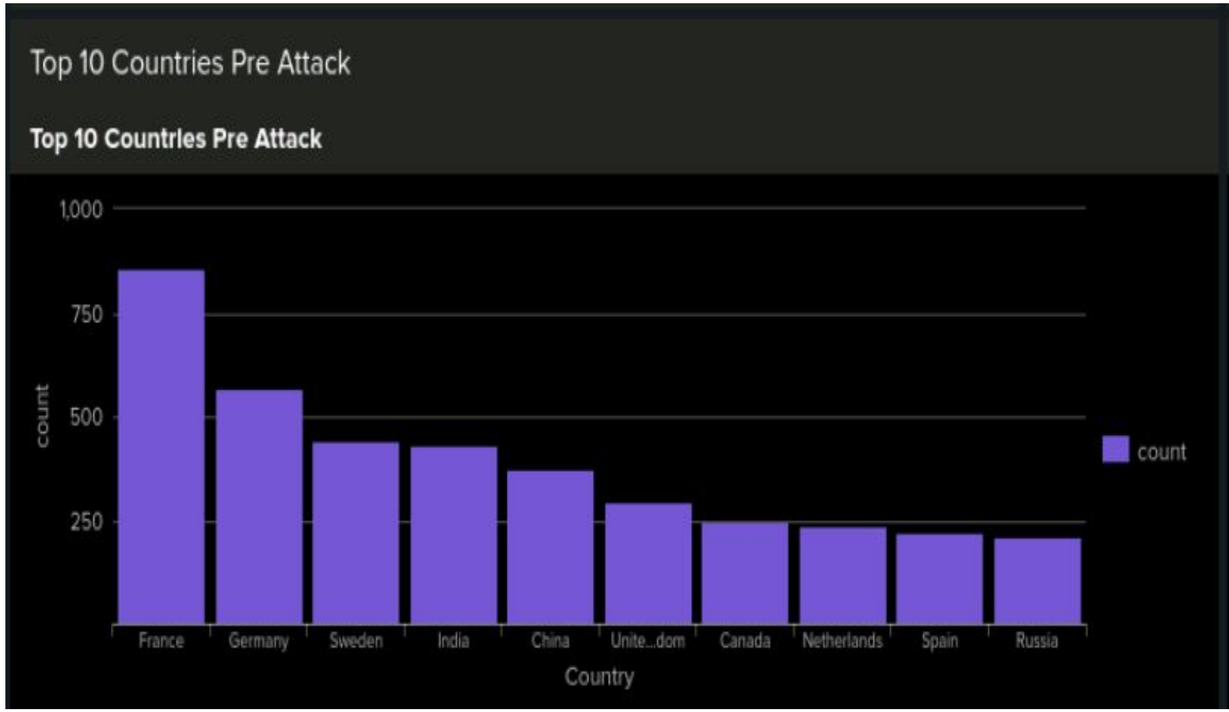
Post Attack



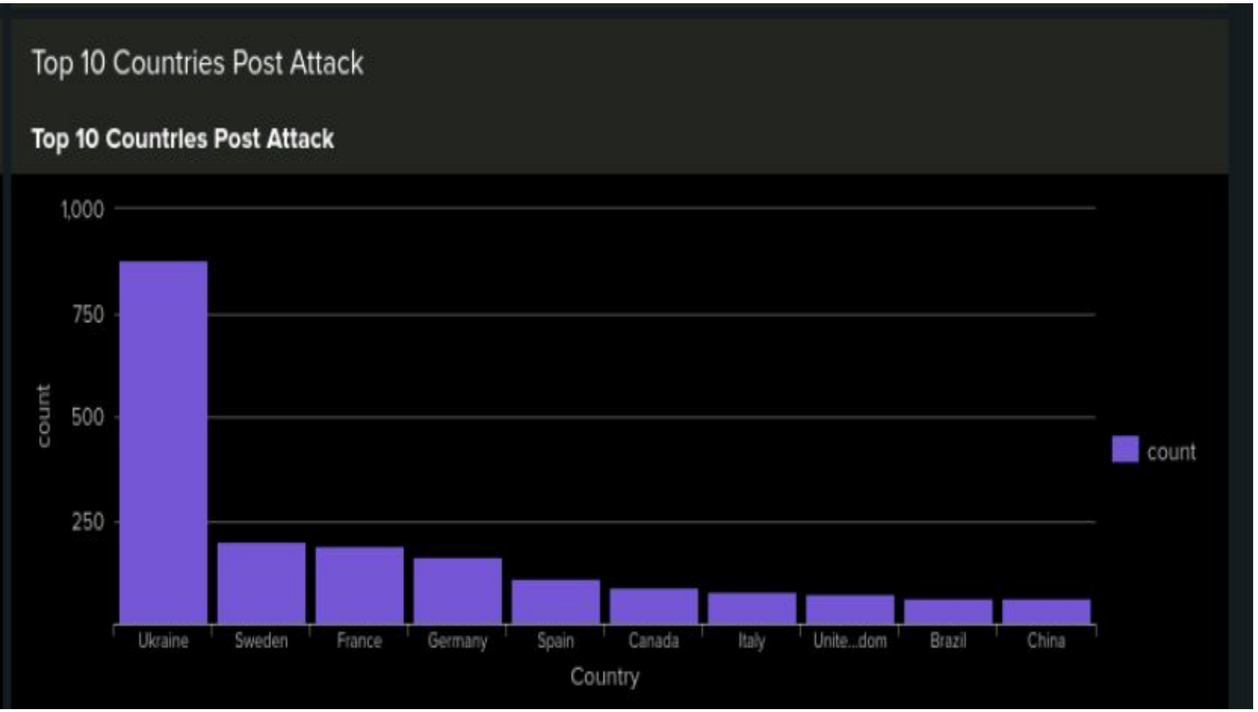
Screenshots of Attack Logs - Apache Dashboard

APACHE DASHBOARD PANEL 3 - Country (non-US) pre vs post attack - Bar

Pre Attack



Post Attack

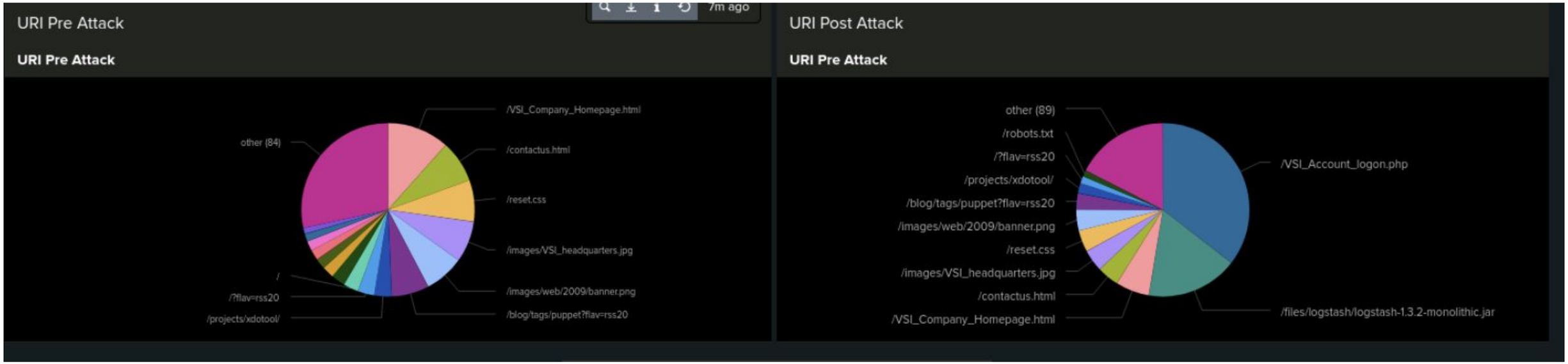


Screenshots of Attack Logs - Apache Dashboard

APACHE DASHBOARD PANEL 4 - URI Data pre vs post attack

Pre Attack

Post Attack



Summary and Future Mitigations

Jason Vaz

Project 3 Summary

Findings from the Attack Analysis:

The attack analysis showed a significant increase in high-severity alerts, rising from 329 to 1,111 (7% to 20% of total alerts). Meanwhile, informational alerts decreased by 93%, indicating that malicious activity intensified. However, failed activities remained stable (only a 1% decrease), suggesting that attackers may have been more successful in their attempts rather than repeatedly failing.

Alert analysis confirmed that thresholds were correctly set, as key alerts successfully detected anomalies:

- **Failed Windows Activity Alert** triggered correctly at 8 AM on March 25, detecting 35 suspicious events.
- **Successful Logins Alert** flagged unusual activity at 11 AM and 12 PM, particularly tied to USER "j" with 196 and 77 login events respectively.
- **Deleted Accounts Alert** remained below the threshold, confirming no suspicious mass deletions.

Project 3 Summary

Recommended Future Mitigations for VSI:

1. **Strengthen Monitoring & Detection:**
   - Lower alert thresholds for high-severity events to detect early-stage attacks sooner.
   - Implement real-time anomaly detection using AI-driven behavior analytics.
2. **Enhance Authentication Security:**
   - Implement multi-factor authentication (MFA) to prevent unauthorized logins.
   - Investigate USER "j" for potential compromise or misuse.
3. **Improve Access Controls & Account Protections:**
   - Enforce least privilege access to limit exposure.
   - Implement automatic account lockout after multiple failed login attempts.
4. **Incident Response Enhancements:**
   - Establish automated response actions for high-severity alerts (e.g., isolating a machine, forcing password resets).
   - Conduct post-incident forensic analysis on affected systems.

Thank you