

Defensive Security Project
by: Tatia Sherozia,Dawa
Sherpa,Mohammed Rashied, Jason
Acosta,Afful Desmond,
Phillip Hale-christofi, Mubarak Abass Illa

Table of Contents

This document contains the following resources:

01

**Monitoring
Environment**

02

Attack Analysis

03

**Project Summary
& Future
Mitigations**

Monitoring Environment

Scenario

We played the role of a 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. As an SOC analysts, we were tasked with using Splunk to monitor against potential attacks on your systems and applications.

The VSI products that we have been tasked with monitoring include:

- An administrative webpage : <https://vsi-corporation.azurewebsites.net/>
- An Apache web server, which hosts this webpage
- A windows operating system, which runs many of VSI's back-end operations

The background is a complex geometric pattern composed of numerous triangles in various shades of dark red and black, creating a mosaic-like effect.

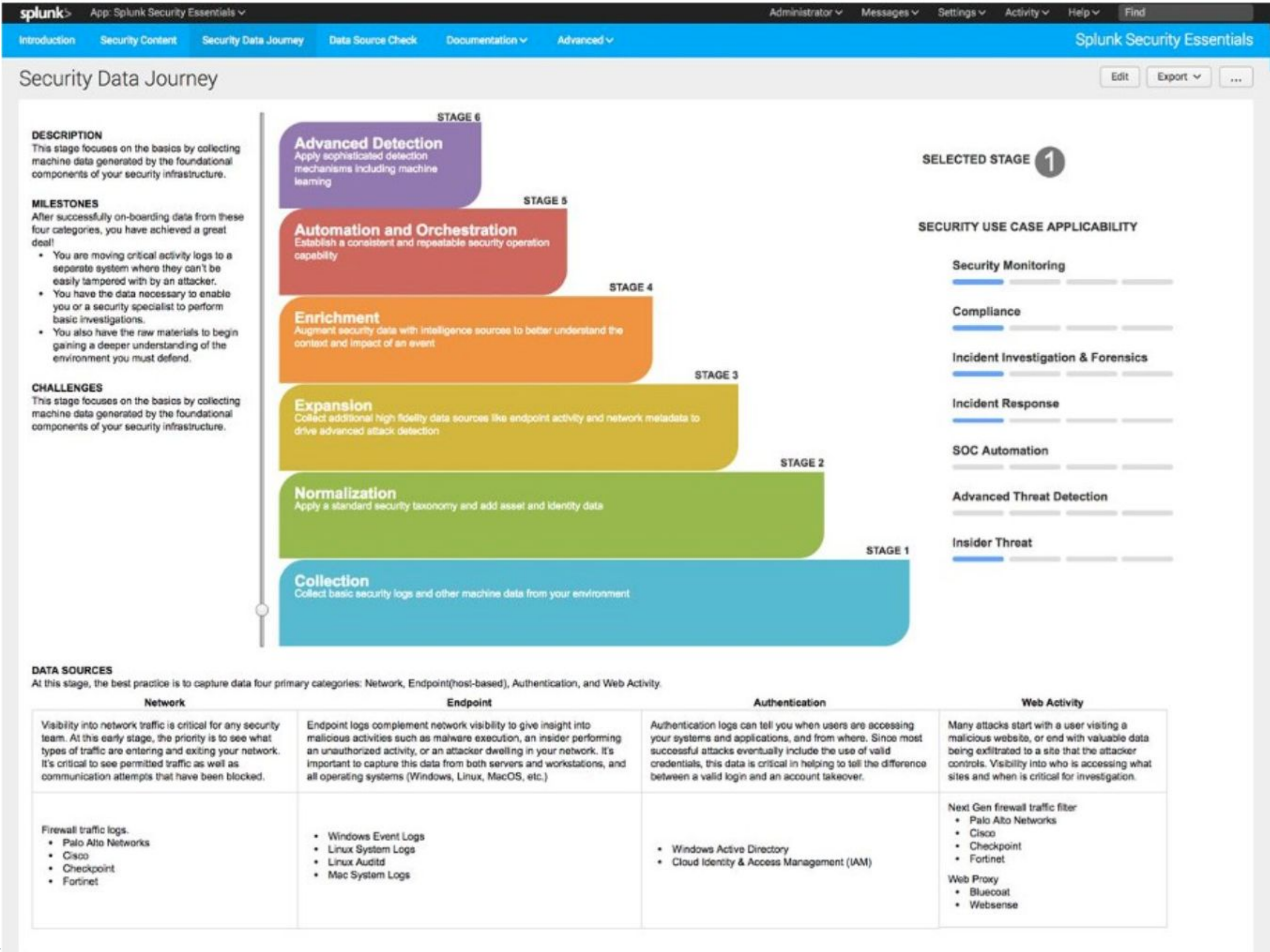
Splunk add-on

Splunk Security Essential (SSE)

SSE aims to provide organizations with a starting point for implementing effective security monitoring and detection practices using Splunk.

The Essentials:







- Pre-built Use Cases
- Dashboards and Visualizations
- Search Queries and Alerts
- Testing Environment
- Continuous Updates
- Community Collaboration



Splunk Security Essential (SSE)

SSE includes a use case specifically designed to detect insider security threats. This use case uses various data sources and detection techniques to single out malicious activities from within the organization.

Using the insider security use case, SSE flagged an abnormal increase in account lockouts. By comparing the number of lockouts against established baselines and user behavior patterns, SSE determines that there were 896 account lockouts within the time frame of 1:50 am to 2:40am.

 <p>Security (continuous) monitoring enables you to analyze a continuous stream of near real-time snapshots of the state of risk to your security data, the network, endpoints, as well as cloud devices, systems and applications.</p>	 <p>An advanced threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. APTs usually targets either private organizations, states or both for business or political motives.</p>
 <p>Insider Threat Insider threats come from current or former employees, contractors, or partners who have access to the corporate network and intentionally or accidentally exfiltrate, misuse or destroy sensitive data. They often have legitimate access to access and download sensitive material, easily evading traditional security products. Nothing to fear, Splunk can also help here.</p>	 <p>Compliance In nearly all environments, there are regulatory requirements of one form or another - when dealing with the likes of GDPR, HIPAA, PCI, SOC, and even the 20 Critical Security Controls, Splunk enables customers to create correlation rules and reports to identify threats to sensitive data or key employees and to automatically demonstrate compliance.</p>
 <p>Application Security Application security is the use of software, hardware, and procedural methods to protect applications from threats. Whether detecting DDoS, SQL Injections, or monitoring for attacks against known or unknown vulnerabilities, Splunk has your critical applications covered.</p>	 <p>SOC Automation With the ever-increasing volume and complexity of security incidents, a constantly evolving technology landscape, and a massive shortage of security analysts, the current model of manual response is falling short. Automation and orchestration of security operations addresses these issues, enabling enterprises to effectively investigate, contain, correct and remediate threats at scale.</p>

Splunk Security Essential (SSE)

Stage 1: Collection [\[i\]](#)
You have the data onboard, what do you do first?

Search Name	Description	Featured	Searches Included	Threat Categories
Flight Risk Web Browsing	This search implements several heuristics to look for indications that a user is a flight risk from Web Logs. Detect a user who may be leaving before they do.	Yes	Searches Included	Exfiltration
Increase in Pages Printed	Find users who printed more pages than normal.	Yes	Searches Included	Exfiltration, Exfiltration Over Physical Medium
Large Web Upload	Uses a basic threshold to detect a large web upload, which could be exfiltration from malware or a malicious insider.	Yes	Searches Included	Exfiltration, Exfiltration Over Alternative
Sources Sending a High Volume of DNS Traffic	A common method of data exfiltration is to send out a huge volume (in bytes) of DNS or ping requests, embedding data into the payload. This is often not logged.	Yes	Searches Included	Exfiltration, Command and Control
User Login with Local Credentials	Categorically, most interactive login should use domain credentials. Detect when a new user logs on with local credentials that bypass most centralized logging and policy systems, but not Splunk!	Yes	Searches Included	Initial Access, Persistence
Detect Many Unauthorized Access Attempts	Most login failures are due to failed passwords. Login failure to sensitive systems where the users simply aren't authorized, though, can indicate malicious intent. Detect that.	Yes	Searches Included	Credential Access, Brute Force
First Time USB Usage	Find systems the first time they generate Windows Event ID 20001, which for some customers occurs when a USB drive is plugged in.	Yes	Searches Included	Initial Access, Lateral Movement, Collection, Exfiltration, Replication Through Removable
Flight Risk Printing	This search implements two heuristics to look for indications that a user is a flight risk. Many people will print off letters, drafts of their resume, or related docs on the work environment (for convenience, or because they don't have a printer at home). Detect when that happens.	Yes	Searches Included	Exfiltration
Potential Day Trading	Detect users who exhibit a large amount of stock trading activity in their proxy logs.	Yes	Searches Included	
Sources Sending Many DNS Requests	A common method for Data Exfiltration is to send out many DNS or Ping requests, embedding data into the payload. This is often not logged.	Yes	Searches Included	Exfiltration, Command and Control, Application Layer Protocol, Exfiltration Over C2 Channel
Web Browsing to Unauthorized Sites	Detect users who are persistently attempting to violate your proxy policy.	Yes	Searches Included	Exfiltration, Command and Control, Exfiltration Over Alternative Protocol, Web Service

By utilizing Splunk security Essentials insider threat security category we successfully detected and reported suspicious numbers of account lockouts within our Splunk analysis. The add-on definitely gave us some needed assistance during the investigation.

Logs Analyzed

1

Windows Logs

- This Server contains properties of VSI's next generation virtual-reality programs.
- Windows Server logs
- Windows Server attack logs

2

Apache Logs

- Logs for VSI's main public websites
- VSI company
- Apache logs
- Apache attack logs

Windows Logs

Reports - Windows

Designed the following reports:

Report Name	Report Description
Signature ID Associated with Specific Signature	A report that shows the ID number associated with the specific signature for Windows activity.
Severity Levels	A report to quickly understand the severity levels of the activity.
Success and Failure	A report that shows a suspicious level of failed activities on their server.

Signature ID Associated with Specific Signature

Ubuntu@10.10.12.12Cybersecurity | VM Dashboard22.1 Project 3: Defensive Sec

cybersecurity.vmportal.org/guacamole/#/client/NTkONQBjAHNxbHNlcnZlcg

Cybersecurity Cou...GitHubNewest Questions...GitLabEdAid - Fair Stude...ChatGPTVMware Desktop...Hacking Labs | Virt...Amazon.com. Spe...Ubuntu@10.10.12.12Cybersecurity | V...

ApplicationsSignature & Associ...sysadmin@vm-ima...

Signature & Associat

localhost:8000/en-US/app/search/report?s=%2FservicesNS%2Fadmin%2Fs...

Relaunch to update

Signature & Associated IDs - Windows_Server_logs

EditMore InfoAdd to Dashboard

All time

4,764 events (before 10/31/24 1:53:32.000 PM)

Job

15 results20 per page

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

Windows Logs Severity

Severity Levels - Windows_server_logs

Shows severity levels, count and percentage of each.

All time ▾

✓ 4,764 events (before 10/31/24 1:59:37.000 PM)

2 results

20 per page ▾

severity ↕	count ↕	percent ↕	total ↕
high	329	6.91	4764
informational	4435	93.09	4764

Edit ▾

More Info ▾

Add to Dashboard ▾

Job ▾

⏸

■

↺

↻

🖨

⬇

Success and Failure

Success / Failure - Windows_server_logs

All time

✓ 4,764 events (before 10/31/24 2:01:21.000 PM)

Edit

More Info

Add to Dashboard

Job

||

■

↺

↻

🖨

⬇

2 results

20 per page

status	count
failure	142
success	4622

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Failed Windows Activity	Failure of windows activity	5	>10

JUSTIFICATION:

Baseline: We set the baseline at 5, aligning with the average level of activity.

Threshold: Set at >10 to strike a balance between reducing false alarms and promptly identifying significant increases in failed activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI deleted user account	Alert for the hourly count of when a user account was deleted	13	>30

JUSTIFICATION:

Baseline: A baseline of 13 was selected as it aligns with a typical hourly level of activity.

Threshold: Set at >30 to flag any unusual spikes, helping to identify potential issues promptly.

Alerts—Windows

Designed the following alerts:

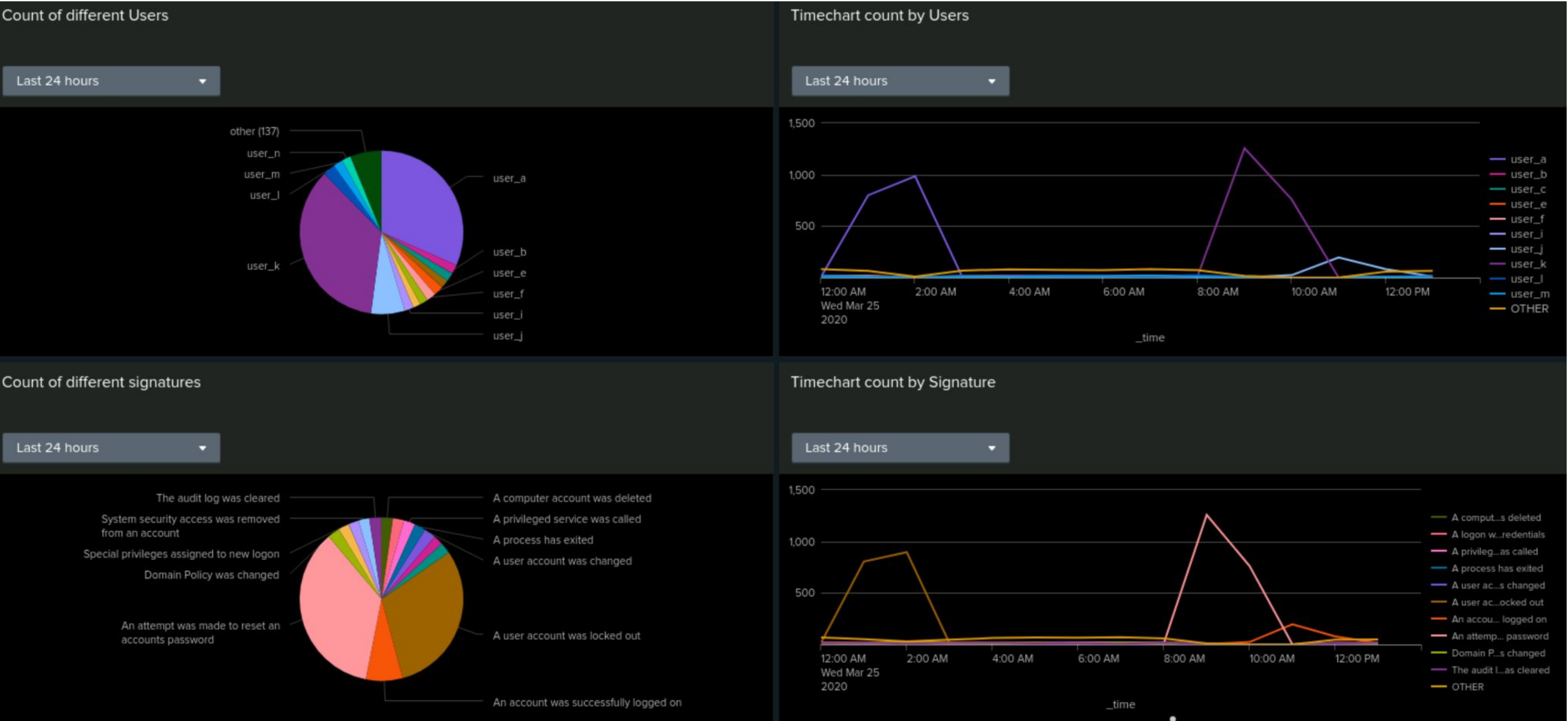
Alert Name	Alert Description	Alert Baseline	Alert Threshold
An account was successfully logged on	This alert triggers when there's a high volume of successful login attempts within set one hour period, potentially indicating unauthorized or unusual access activity.	13	>26

JUSTIFICATION:

Baseline: Set at 13, reflecting the typical hourly activity level for successful logins per user.

Threshold: Defined as >26 to effectively capture unusual spikes in successful logins while minimizing false positives, allowing timely detection of potential security concerns.

Dashboards—Windows



Count of different signatures

Last 24 hours

The audit log was cleared

System security access was removed from an account

Special privileges assigned to new logon

Domain Policy was changed

An attempt was made to reset an accounts password

A computer account was deleted

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

Timechart count by Signature

Last 24 hours

1,500

1,000

500

12:00 AM Wed Mar 25 2020

2:00 AM

4:00 AM

6:00 AM

8:00 AM

10:00 AM

12:00 PM

_time

A comput...s deleted

A logon w...redentials

A privileg...as called

A process has exited

A user ac...s changed

A user ac...ocked out

An accou... logged on

An attempt... password

Domain P...s changed

The audit L...as cleared

OTHER

Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP method	This report will give insight into the types of HTTP activity occurring on VSI's web server
Top Domains	This report will display the top domains that are referring traffic to VSI's website
Count of HTTP Response code	A report that shows the count of each HTTP response code

Images of Reports—Apache

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

All time

✓ 4,497 events (before 10/31/24 3:48:11.000 AM)

No Event Sampling

Job

Verbose Mode

Events (4,497)

Patterns

Statistics (4)

Visualization

50 Per Page

Format

Preview

method	count
GET	3157
HEAD	15
OPTIONS	1
POST	1324

source="apache_logs.txt" | stats count by status

All time

✓ 20,000 events (before 10/31/24 4:08:19.000 AM)

No Event Sampling

Job

Verbose Mode

Events (20,000)

Patterns

Statistics (8)

Visualization

20 Per Page

Format

Preview

status	count
200	18252
206	90
301	328
304	890
403	4
404	426
416	4
500	6

source="apache_logs.txt" | top limit=10 | referer_domain

All time

✓ 20,000 events (before 10/31/24 3:54:52.000 AM)

No Event Sampling

Job

Verbose Mode

Events (20,000)

Patterns

Statistics (10)

Visualization

50 Per Page

Format

Preview

referer_domain	count	percent
http://www.semicomplete.com	6076	51.256960
http://semicomplete.com	4002	33.760756
http://www.google.com	246	2.075249
https://www.google.com	210	1.771554
http://stackoverflow.com	68	0.573646
http://www.google.fr	62	0.523030
http://s-chassis.co.nz	58	0.489286
http://logstash.net	56	0.472414
http://www.google.es	50	0.421799
https://www.google.co.uk	46	0.388055

Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI non-US activity	Alert if the hourly activity from any country besides the United States exceeds the thresholds	100	>150

JUSTIFICATION:

Baseline: A baseline of 100 events per hour was chosen, reflecting the standard activity observed in the logs.

Threshold: Set at >150 events per hour to flag any unusual spikes, ensuring alerts are triggered only when there’s a significant increase, reducing false positives while maintaining effective monitoring.

Alerts—Apache

Designed the following alerts:

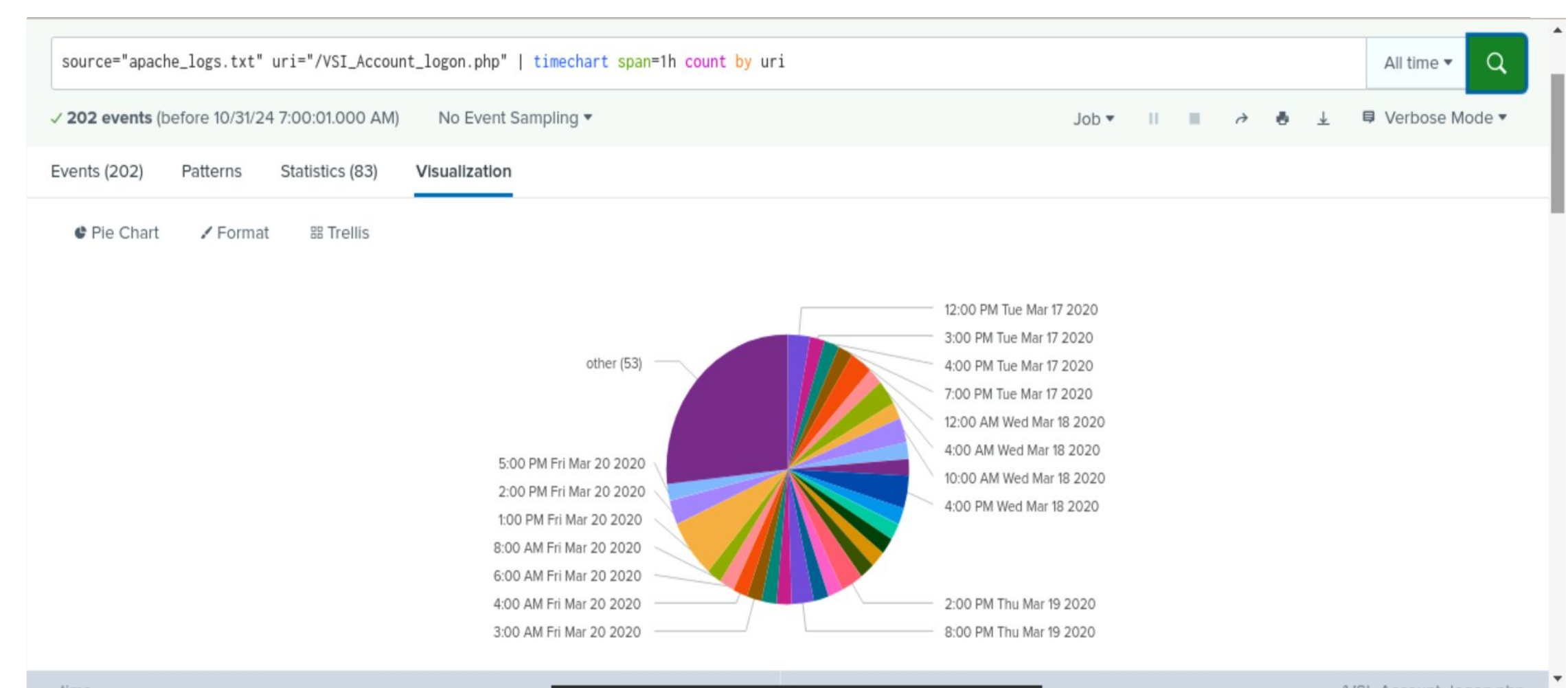
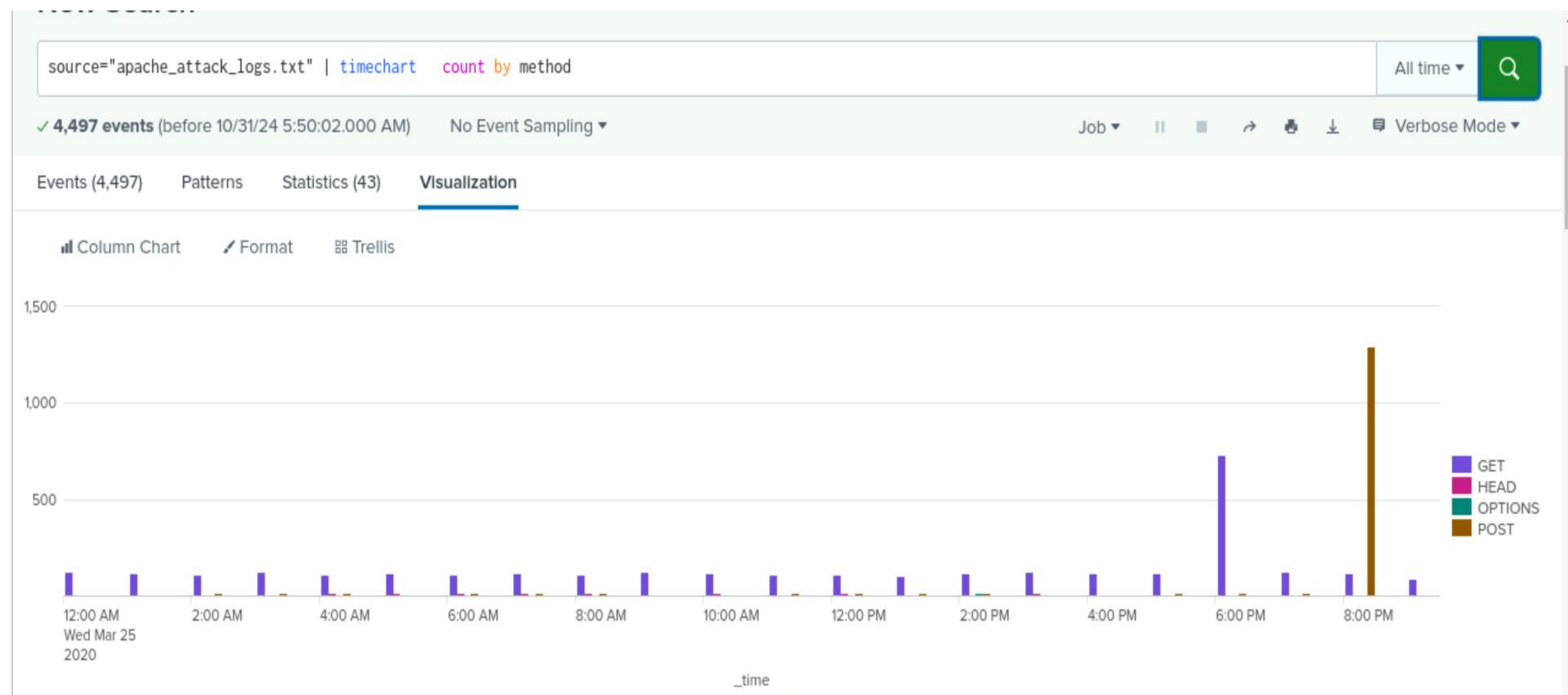
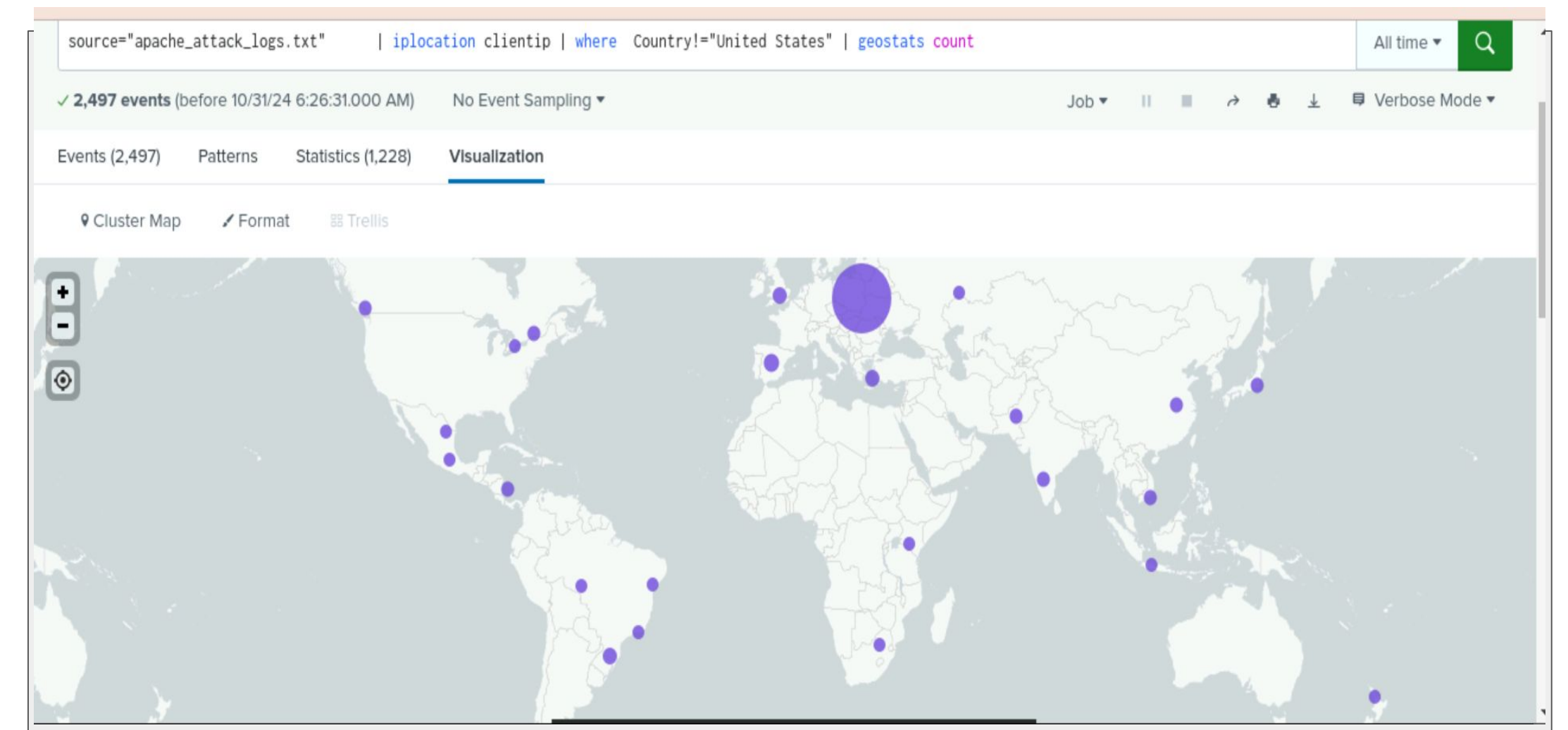
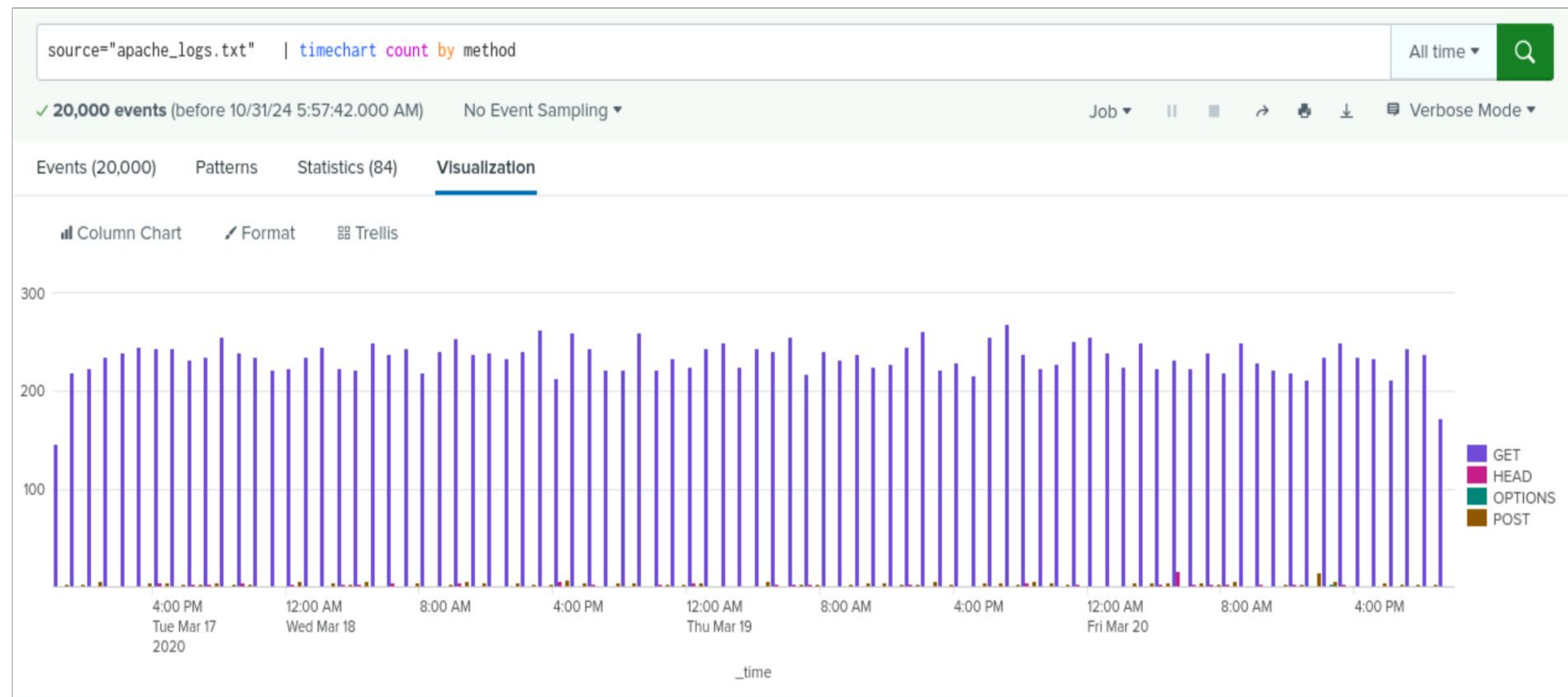
Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI HTTP POST count	Alert if the hourly count of the HTTP POST method exceeds the thresholds	3	>6

JUSTIFICATION:

Baseline: The baseline is set at 3 events per hour, as this aligns with typical hourly activity.

Threshold: Set at >6 events to effectively capture any unusual activity, while staying above typical fluctuations to reduce false positives.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

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

- The attack logs showed an increase in high severity events, indicating more serious issues or threats.
- This increase in high severity events suggests a potential severe attack on the system.
- There was a decrease in the percentage of failed activities in the attack logs.
- This decrease could suggest successful activities by an unauthorized user.
- The combination of increased successful activities and decreased failures could indicate a security breach.
- These findings highlight the need for continuous monitoring and robust security measures.

Attack Summary—Windows

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

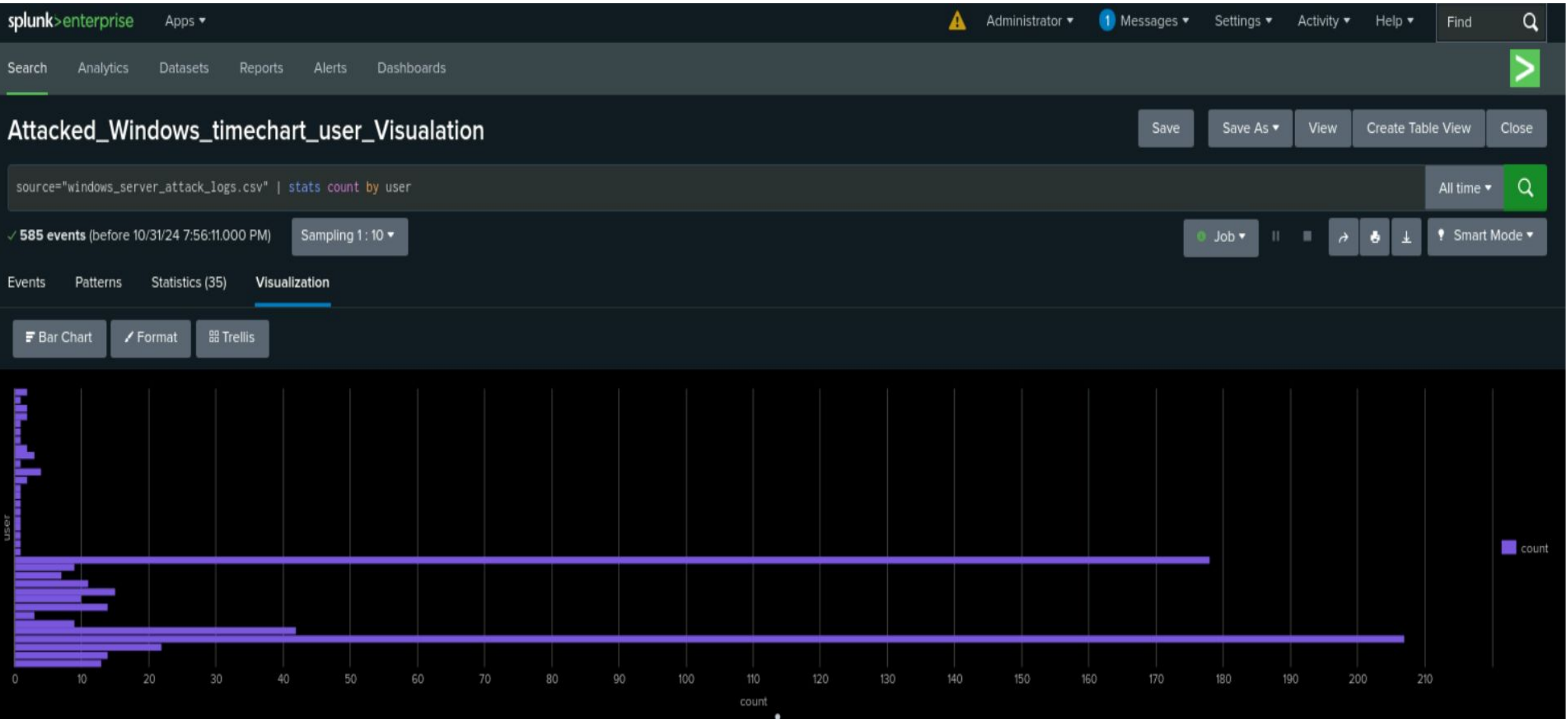
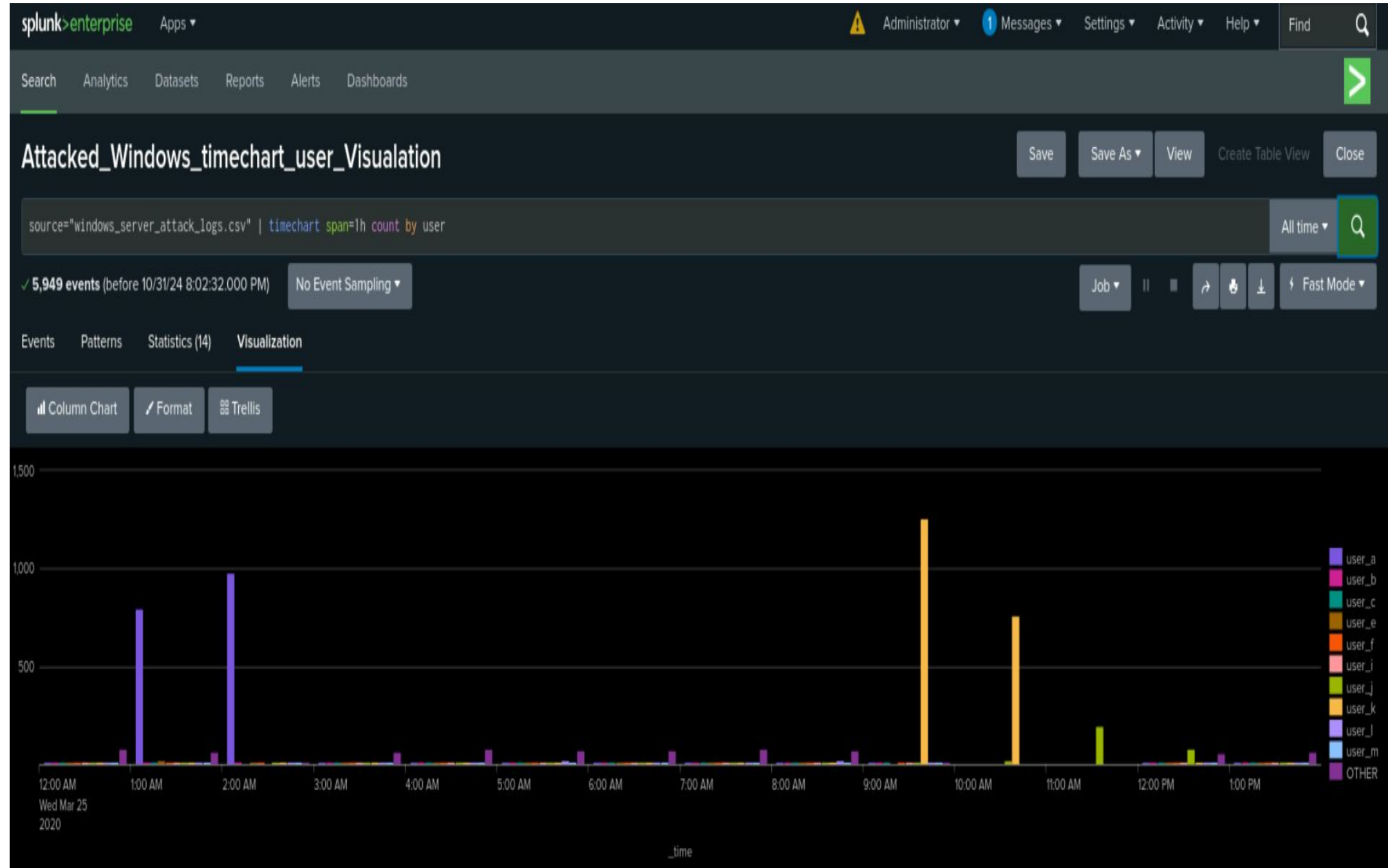
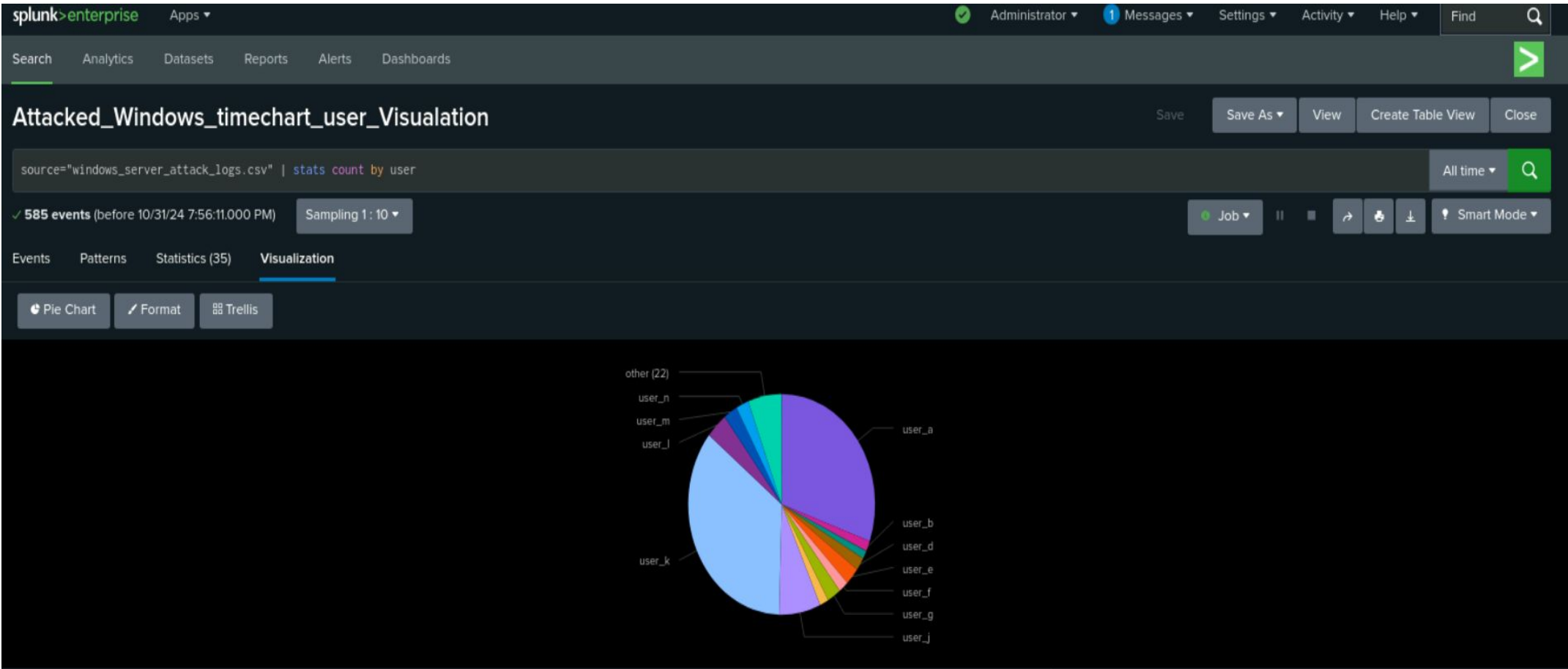
- Two signatures stood out as suspicious in the line chart: "attempt to reset account password" and "user account locked out". These signatures had significantly higher counts during the attack compared to the previous log.
- The suspicious activity for these signatures occurred at specific times. For "user account locked out", it was between 12 am and 3 am. For "attempt to reset account password", it was between 8 am and 11 am.
- Two users, user_a and user_k, were identified as suspicious in the user analysis. They had high peak counts in the line graph and took up large proportions in the pie chart.

Attack Summary—Windows

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

- The bar graph for signatures confirmed the findings from the time chart, with "user was locked out", "account successfully logged on", and "attempt made to reset account password" showing high counts.
- The pie chart for users also confirmed the findings from the line graph, with user_a and user_k standing out due to their high counts and large proportions.
- The statistical charts provided a comprehensive view of user activities and helped identify outliers. However, they were more difficult to interpret and lacked the temporal context provided by the line graphs.

Screenshots of Attack Logs



Attack Summary—Apache

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

- There was a dramatic increase in GET requests and in POST requests. This could suggest the attacker's tactics was possibly to exploit vulnerabilities or perform actions on the server.
- The referrer domains showed suspicious changes. The proportions of top referrers shifted, and new referrer domains appeared in the attack logs. This could indicate a shift in traffic source or type related to the attack.
- The HTTP response codes also showed suspicious changes. There was a significant decrease in 200 (OK) responses and a dramatic increase in 404 (Not Found) responses. This could suggest that the attacker was making requests for resources that do not exist on the server, possibly in an attempt to find vulnerabilities or misconfigurations.

Attack Summary—Apache

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

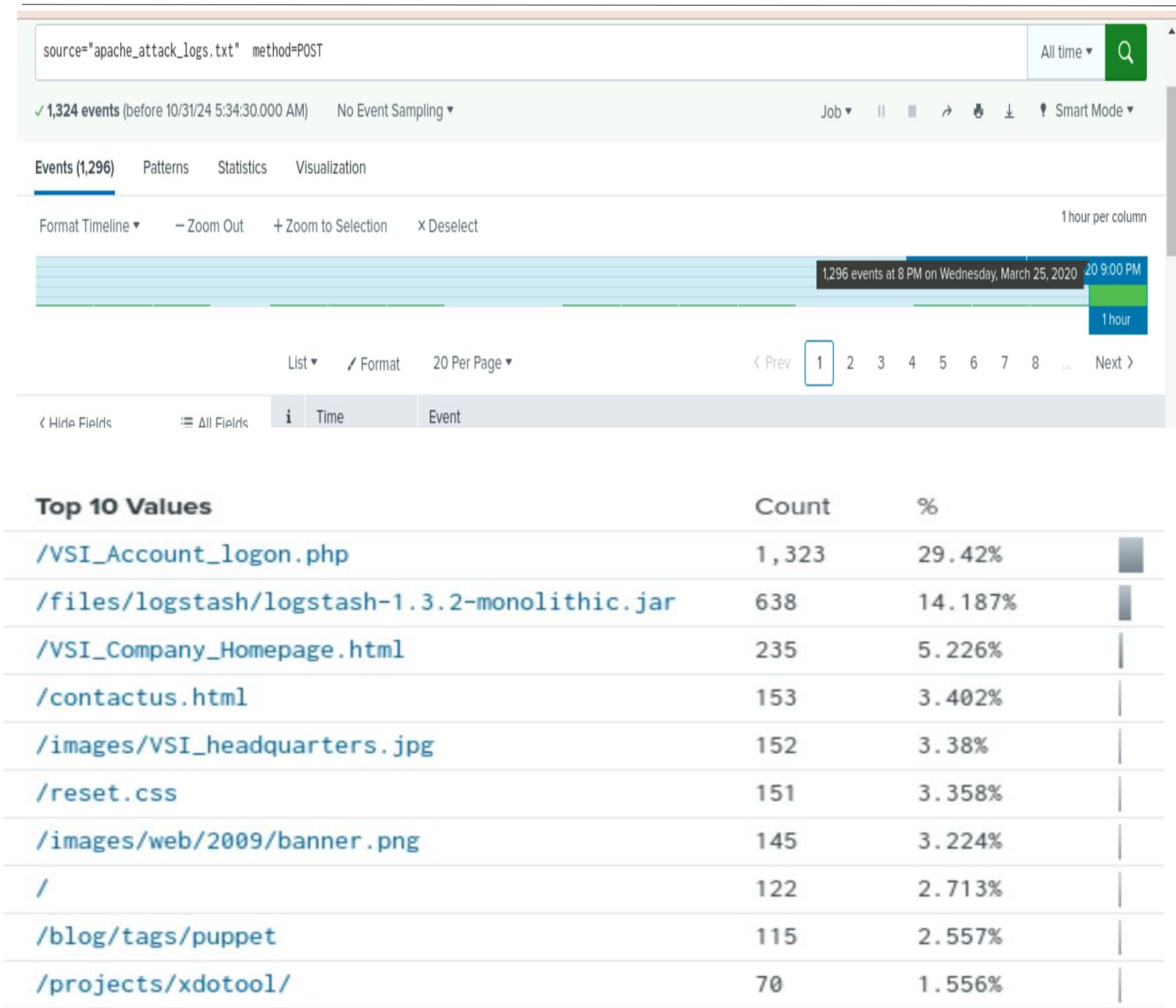
- We detected a suspicious volume of international activity between 8pm and 9pm.
- Our threshold was correct and our alert would have been triggered.
- We detected a suspicious volume of HTTP POST activity between 8pm and 9pm on March 25th. It peaked at 1,296.
- Our threshold was correct and our alert would have triggered.

Attack Summary—Apache

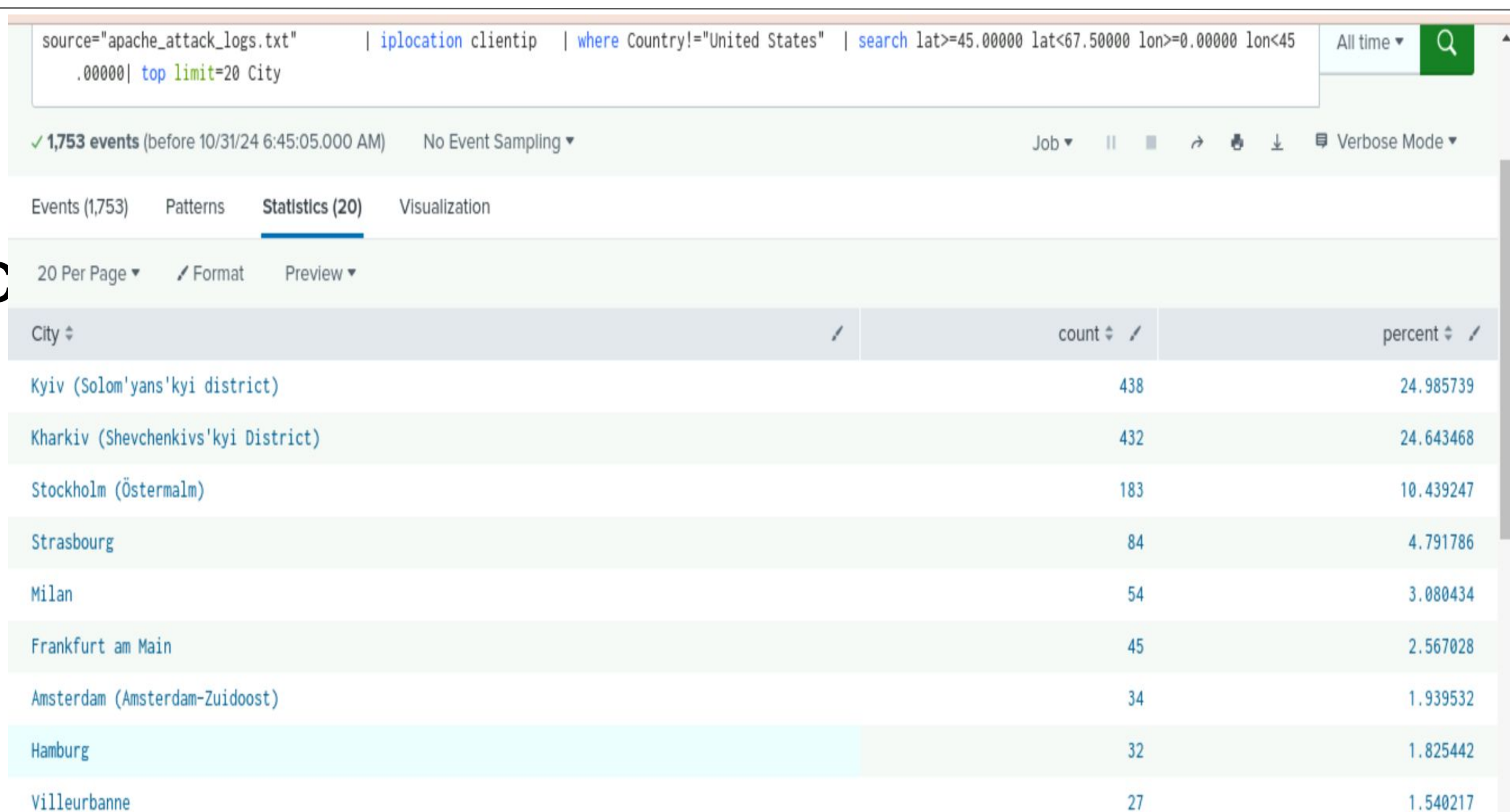
Summarize your findings from your dashboards when analyzing the attack logs.

- Our Time Chart of HTTP methods revealed suspicious volumes of GET and POST methods.
 - The GET attack went from 5pm to 7pm and peaked with a count of 729.
 - The POST attack went from 7pm to 9pm and peaked with a count of 1,296.
- Our Cluster Map revealed suspicious activity from a couple cities.
 - Kiev (439), Kharkiv (433), D.C. (714), and NYC(549) all had high volumes of activity.
- Our URI Data flagged “/VSI_Account_logon.php” as having suspiciously high volume.

Screenshots of Attack Logs



ac



Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
 1. Increase in high severity events, suggesting a serious attack.
 2. Decrease in failed activities, indicating potential unauthorized access.
 3. Suspicious signatures: "attempt to reset account password" and "user account locked out".
 4. Users 'user_a' and 'user_k' showed suspiciously high activity.
 5. Significant increase in GET and POST requests.
 6. Changes in referrer domains, indicating a possible shift in traffic source.
 7. Increase in 404 (Not Found) HTTP responses, suggesting attempts to access non-existent resources.

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

1. Implement continuous monitoring and robust security measures.
2. Adjust alert thresholds based on new findings for early attack detection.
3. Regularly update the list of suspicious signatures and users.
4. Monitor HTTP requests and response codes for unusual patterns.
5. Keep track of referrer domains and traffic sources.
6. Train employees on cybersecurity best practices.
7. Implement Two-factor authentication, the first line of defence against brute-force attacks.
8. Lock users out after a certain number of login attempts to prevent future attacks.