Defensive Security Project

by: Tatia Sherozia,Dawa Sherpa,Mohammed Rashied, Jason Acosta,Afful Desmond, Phillip Hale-christofı, Mubarak Abass Illa

Table of Contents

This document contains the following resources:

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

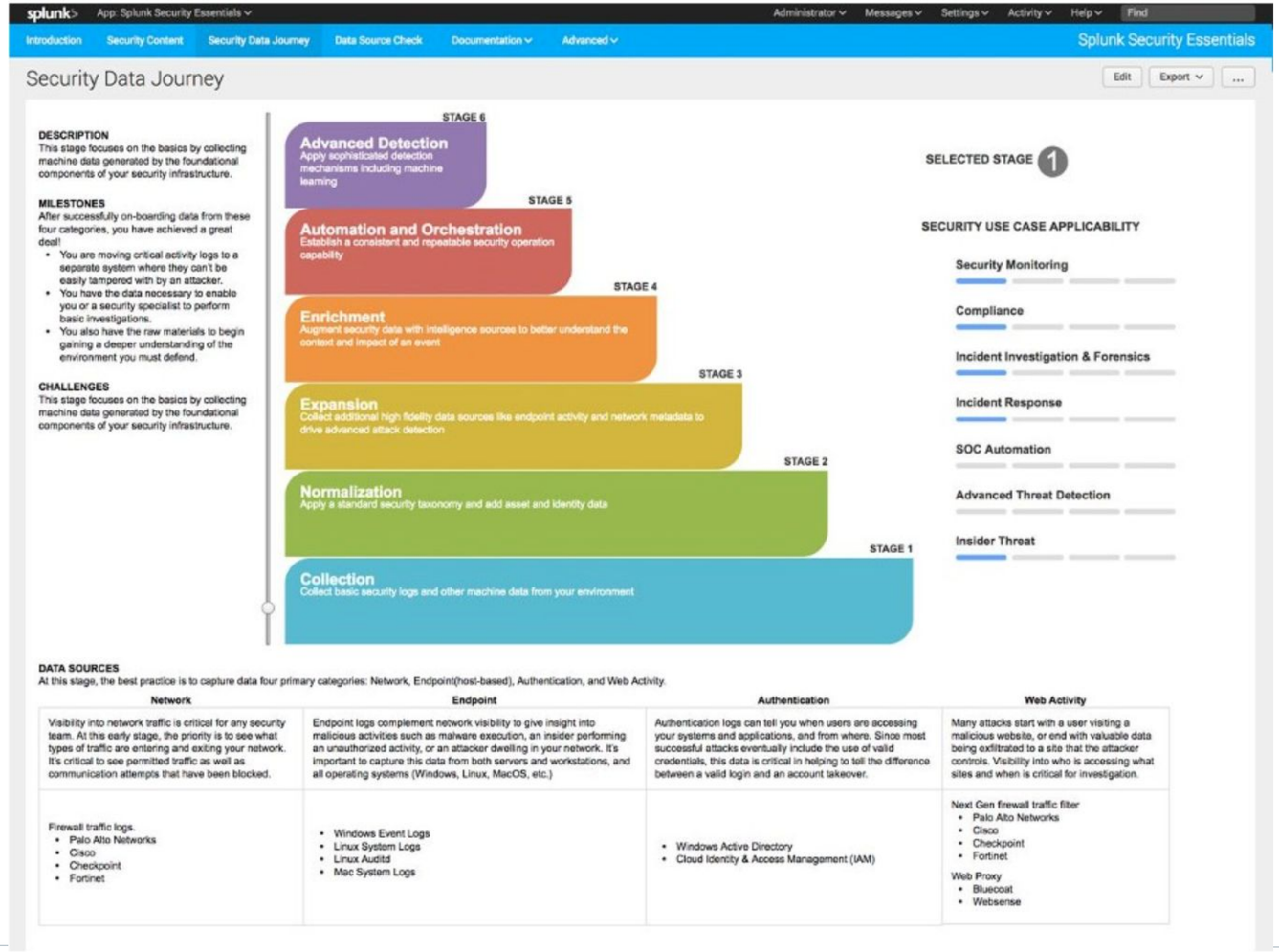
Splunk addon

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:

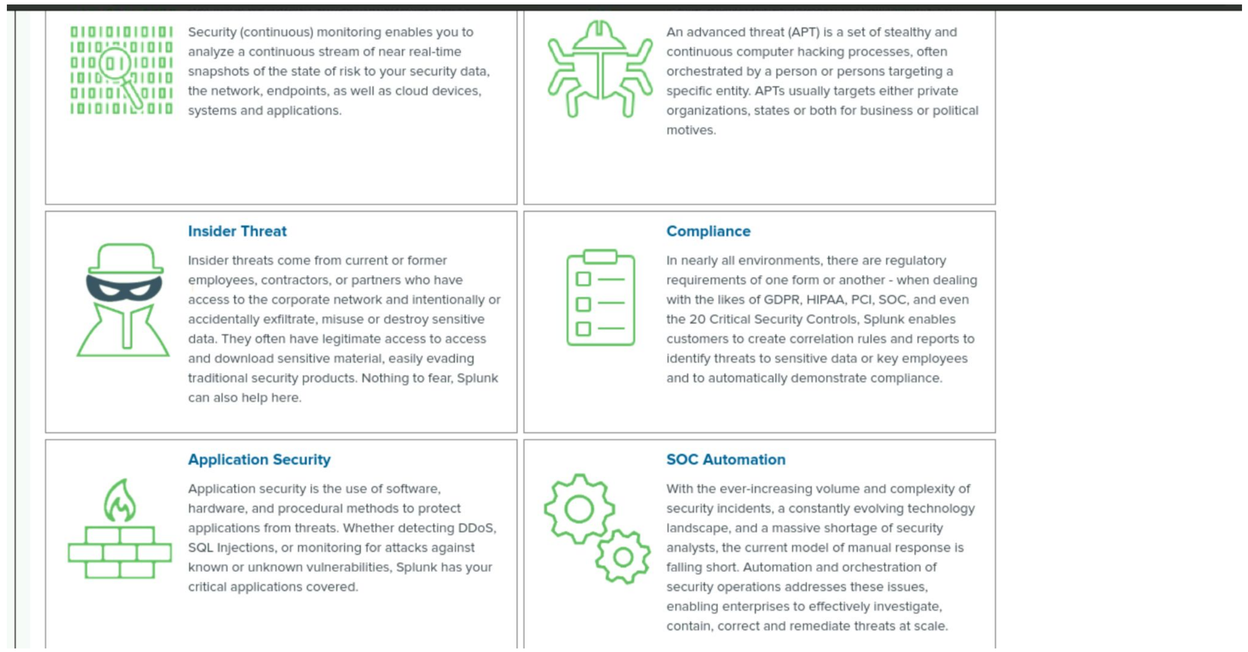
- Pre-built Use Cases
- Dashboards and Visualizations
- Search Queries and Alerts
- Testing Environment
- Continuous Updates
- Community Collaboration



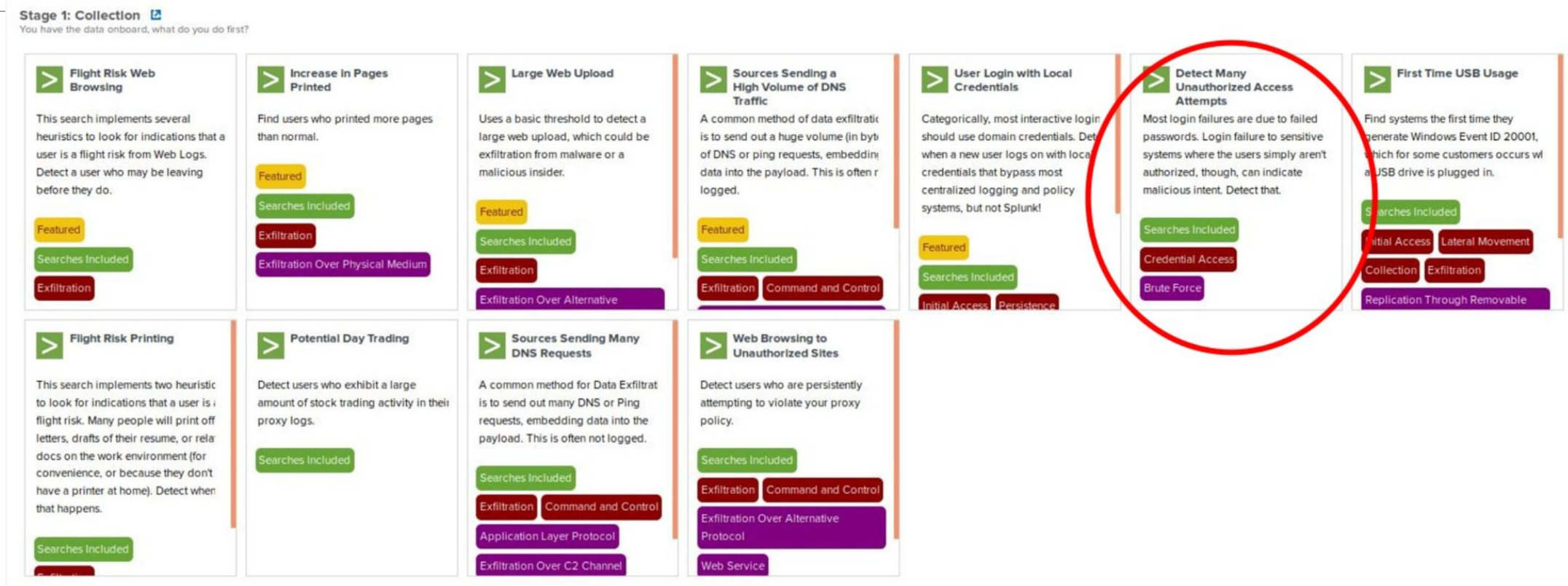
Splunk Security Essential (SSE)

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.



Splunk Security Essential (SSE)



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

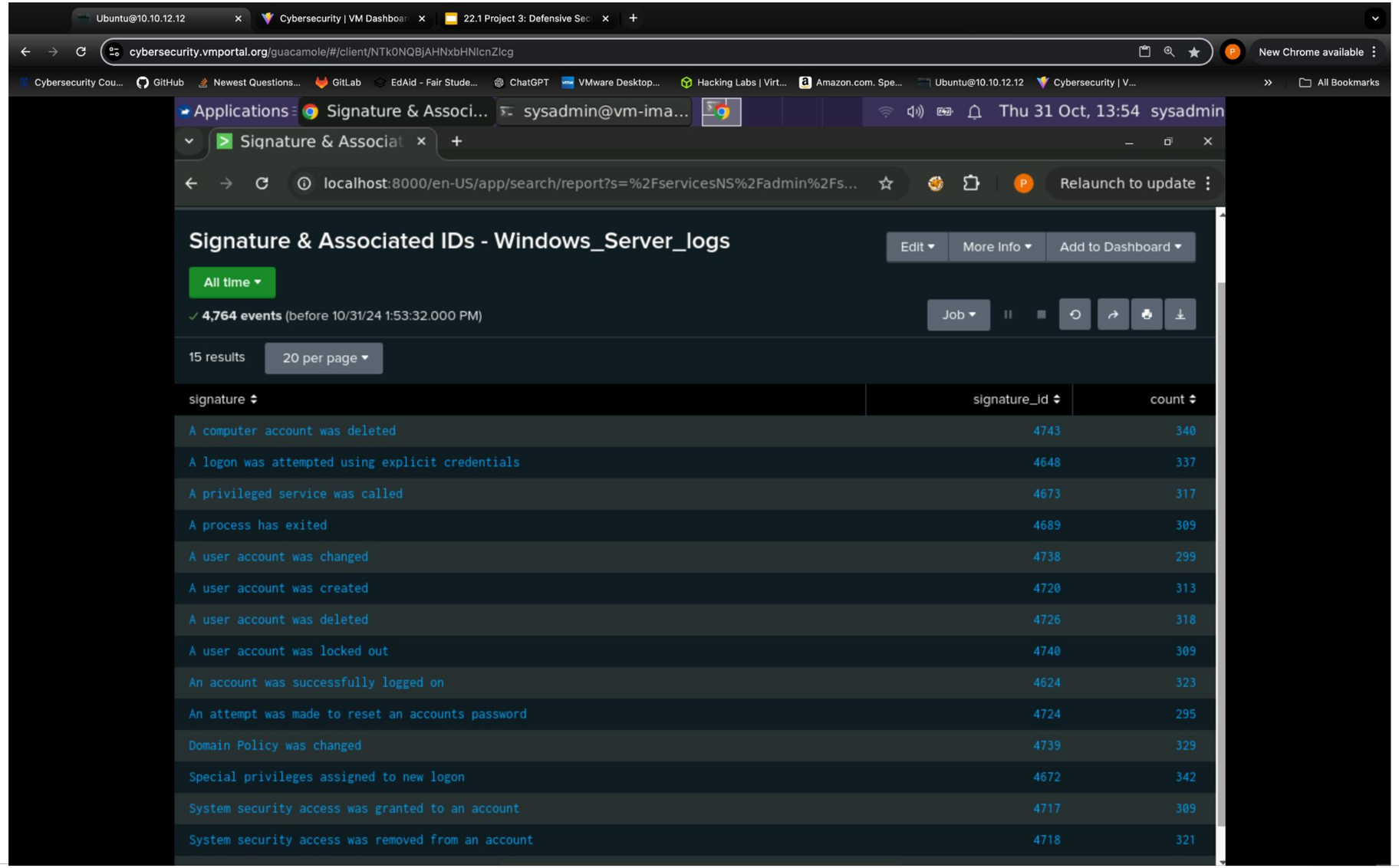
Windows Logs

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



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

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Shows severity levels, count and percentage of each.

All time ▾

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

Job ▾

2 results | 20 per page ▾

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

Success and Failure

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

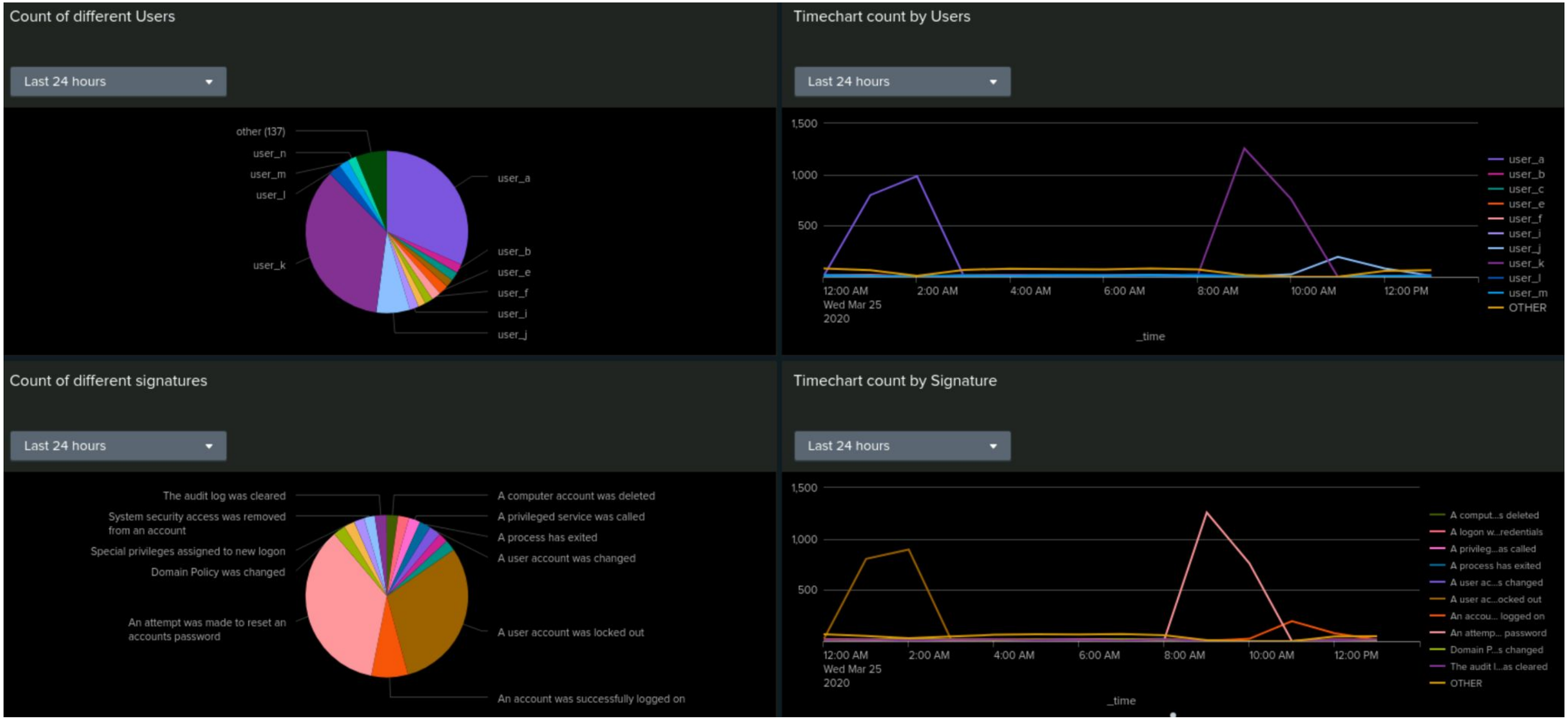
Designed the following alerts:

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



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

Apps Cyber Secur... Home - Boo... Apache Gua... Columbia U... Ethical hack... TryHackme... Azure Lab

```
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:

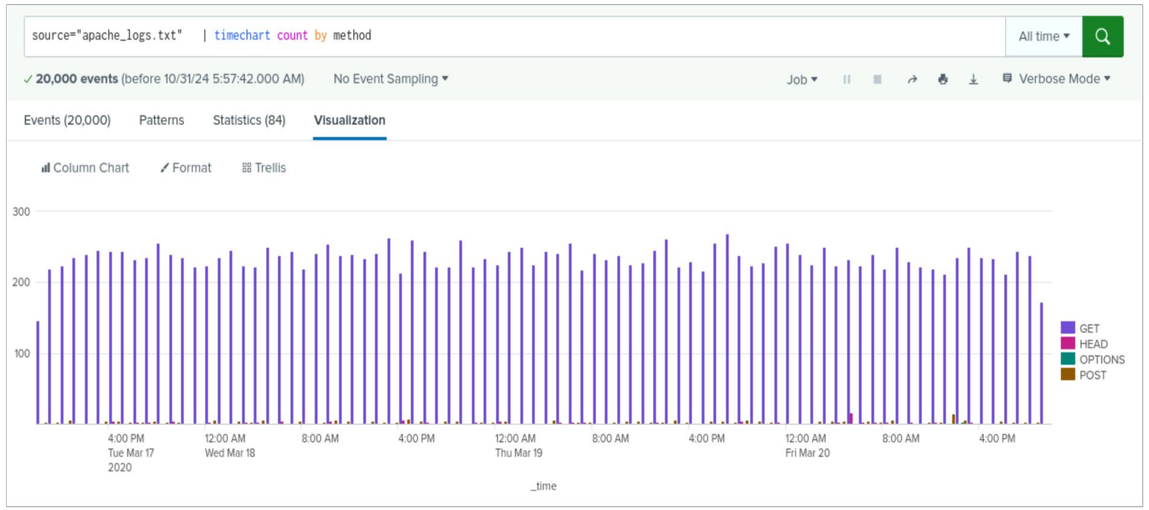
Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI HTTP POST count	Alert if the hourly count of the HTTP POST method exceeds the thresholds	3	>6

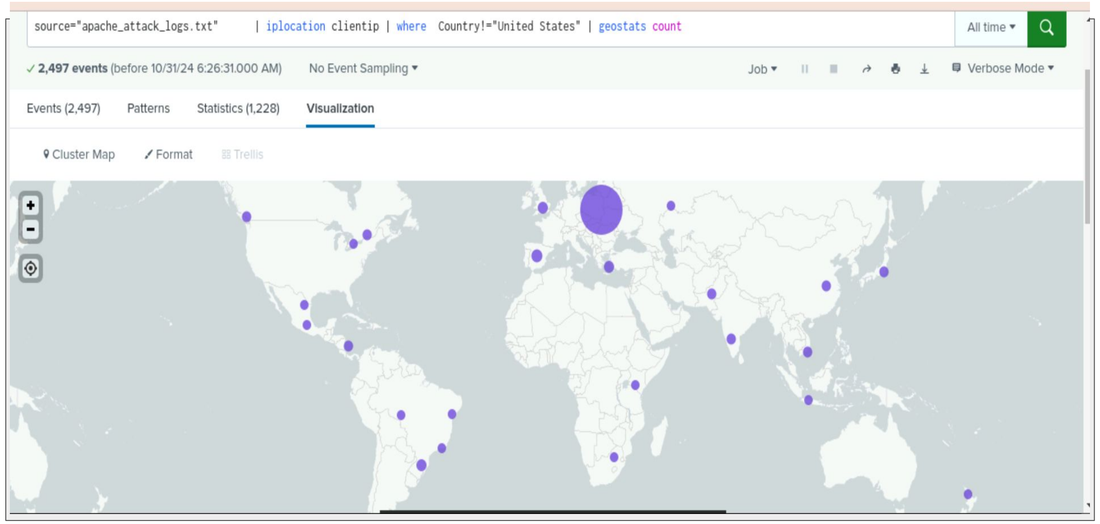
JUSTIFICATION:

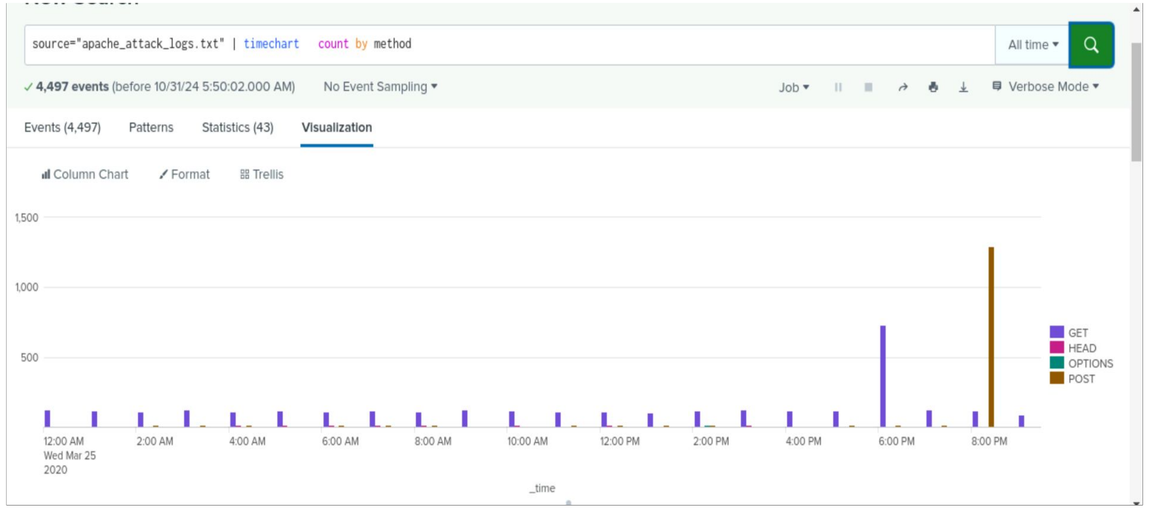
Baseline: The baseline is set at 3 events per hour, as this aligns with typical hourly activity.

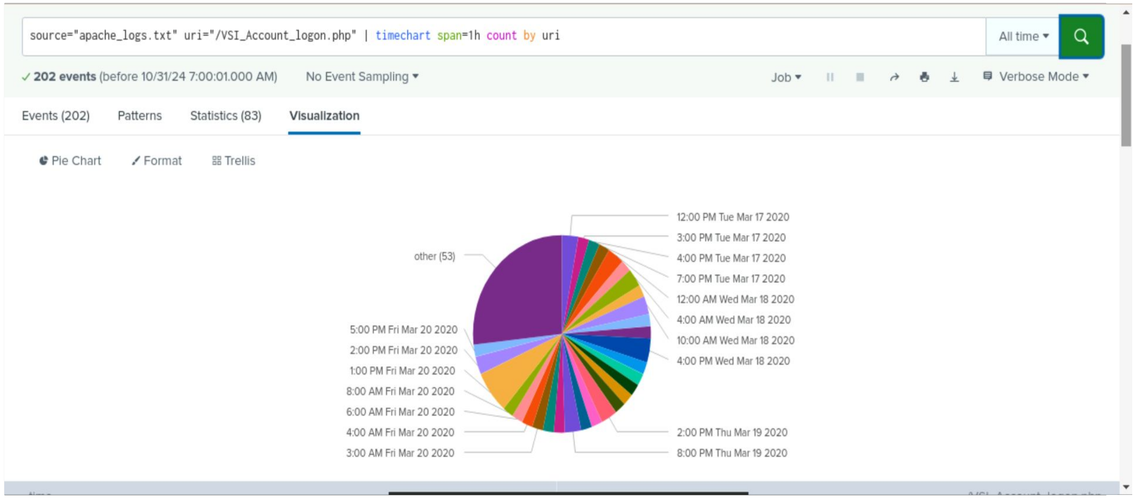
Threshold: Set at >6 events to effectively capture any unusual activity, while staying above typical fluctuations to reduce false positives.

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

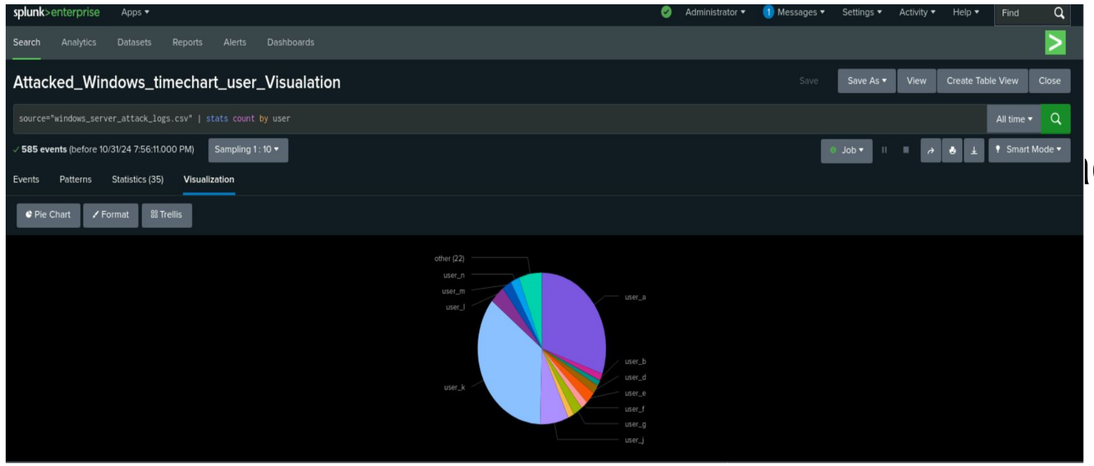
Summarize your findings from your dashboards when analyzing the attack logs.

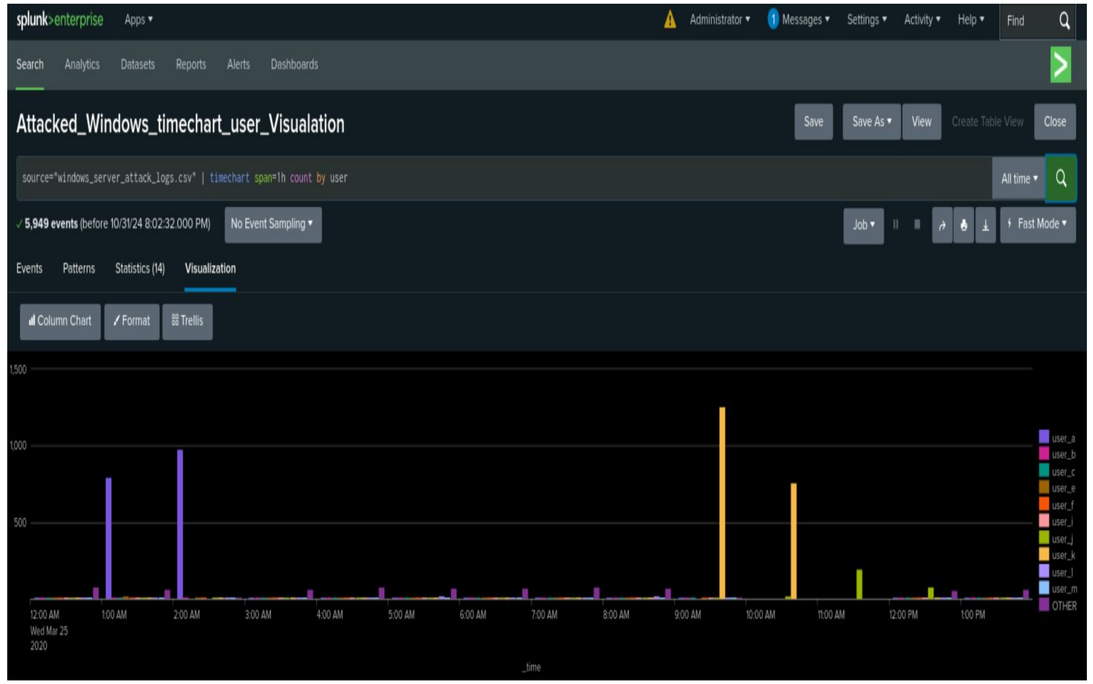
- The bar graph for signatures confirmed the findings from the time chart, with "user was locked out", "account successfully logged on", and "attempt made to reset account password" showing high counts.

- 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?

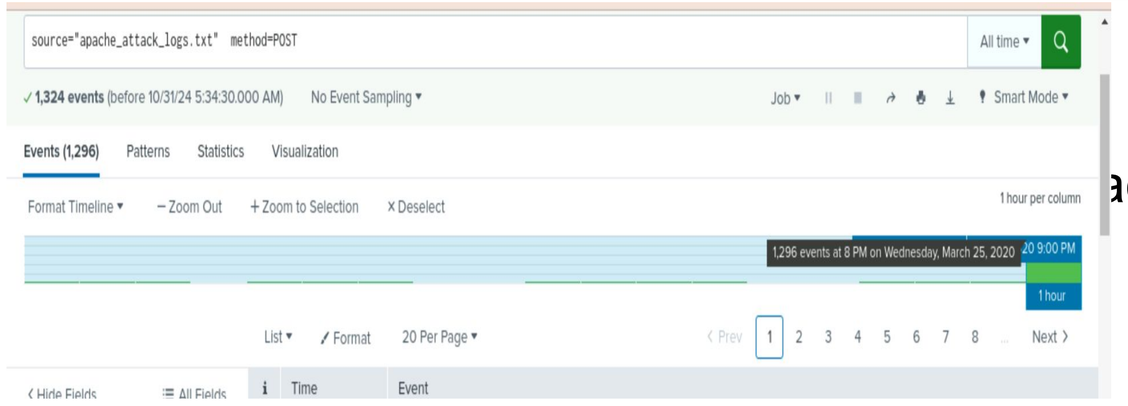
- We detected a suspicious volume of international activity between 8pm and 9pm.
- Our threshold was correct and our alert would have been triggered.
- We detected a suspicious volume of HTTP POST activity between 8pm and 9pm on March 25th. It peaked at 1,296.
- Our threshold was correct and our alert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

Attack Summary—Apache

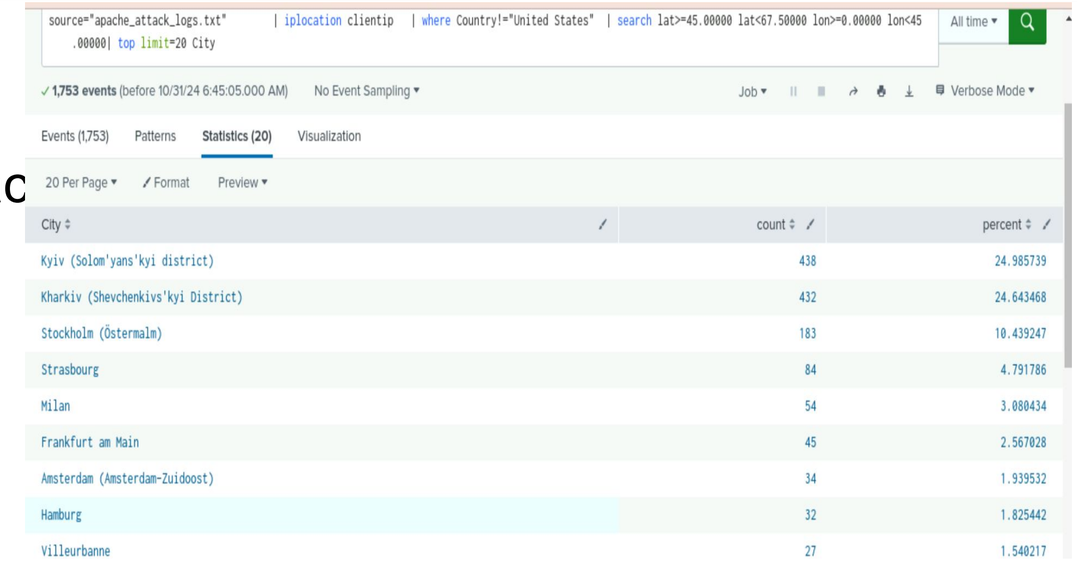
Summarize your findings from your dashboards when analyzing the attack logs.

- 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



Top 10 Values	Count	%
/VSI_Account_logon.php	1,323	29.42%
/files/logstash/logstash-1.3.2-monolithic.jar	638	14.187%
/VSI_Company_Homepage.html	235	5.226%
/contactus.html	153	3.402%
/images/VSI_headquarters.jpg	152	3.38%
/reset.css	151	3.358%
/images/web/2009/banner.png	145	3.224%
/	122	2.713%
/blog/tags/puppet	115	2.557%
/projects/xdotool/	70	1.556%



City	count	percent
Kyiv (Solom'yans'kyi district)	438	24.985739
Kharkiv (Shevchenkivs'kyi District)	432	24.643468
Stockholm (Östermalm)	183	10.439247
Strasbourg	84	4.791786
Milan	54	3.080434
Frankfurt am Main	45	2.567028
Amsterdam (Amsterdam-Zuidoost)	34	1.939532
Hamburg	32	1.825442
Villeurbanne	27	1.540217

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.