Defensive Security Project

Table of Contents

This document contains the following resources:

01

Monitoring Environment

- tools
- methods
- settings

02

Attack Analysis

- observations
- changes
- results

03

Project Summary & Future Mitigations

- assessment
- improvements

Monitoring Environment

Scenario

Our scenario required us to play the role of a SOC analyst at a company called Virtual Space Industries (VSI). VSI designs virtual reality programs for businesses. VSI has intelligence that indicates a competitor called JobeCorp may launch cyber attacks to disrupt the business operations of VSI.

As a SOC analyst, we are required to monitor against potential attacks on the following systems and applications:

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

We were required to use Splunk as a security monitoring solution.

We were provided with historical log data that would enable us to build reports, alerts and dashboards that reflect typical usage patterns.

We were then provided with additional historical log data from a cyber attack that we would use to measure the results from our security monitoring solution and to assess its effectiveness.

Our objective was to demonstrate proficiency in defensive security practices by designing a custom monitoring environment using Splunk.

Splunk Add-On

Splunk Security Essentials

Splunk Security Essentials (SSE) is a free Splunk app that helps organizations improve their security posture by providing a library of pre-built detections and data recommendations. SSE is mapped to the MITRE ATT&CK framework and the Cyber Kill Chain, making it easy to identify and respond to threats.

Key features of SSE:

- Security Content Library: SSE includes over 900 pre-built detections and analytic stories that can be deployed out-of-the-box to improve security monitoring and investigations.
- Cybersecurity Frameworks: SSE automatically maps data and security detections to MITRE ATT&CK and Cyber Kill Chain, helping organizations identify gaps in their defenses and prioritize remediation efforts.
- Data and Content Introspection: SSE provides visibility into the data coming into your environment, helping you add context and telemetry to security events. You can also enrich your security detections with metadata and tags from the Security Content Library.
- Security Data Journey: SSE provides prescriptive security and data recommendations, helping you establish a data strategy and develop a security maturity roadmap.

Overall, SSE is a valuable tool for organizations of all sizes that are looking to improve their security posture. It is easy to use and deploy, and it provides a wide range of features and benefits.

Splunk Security Essentials

VSI is a small company who may be limited in the resources it can allocate to the cyber threats it is concerned about.

Splunk Security Essentials helps to:

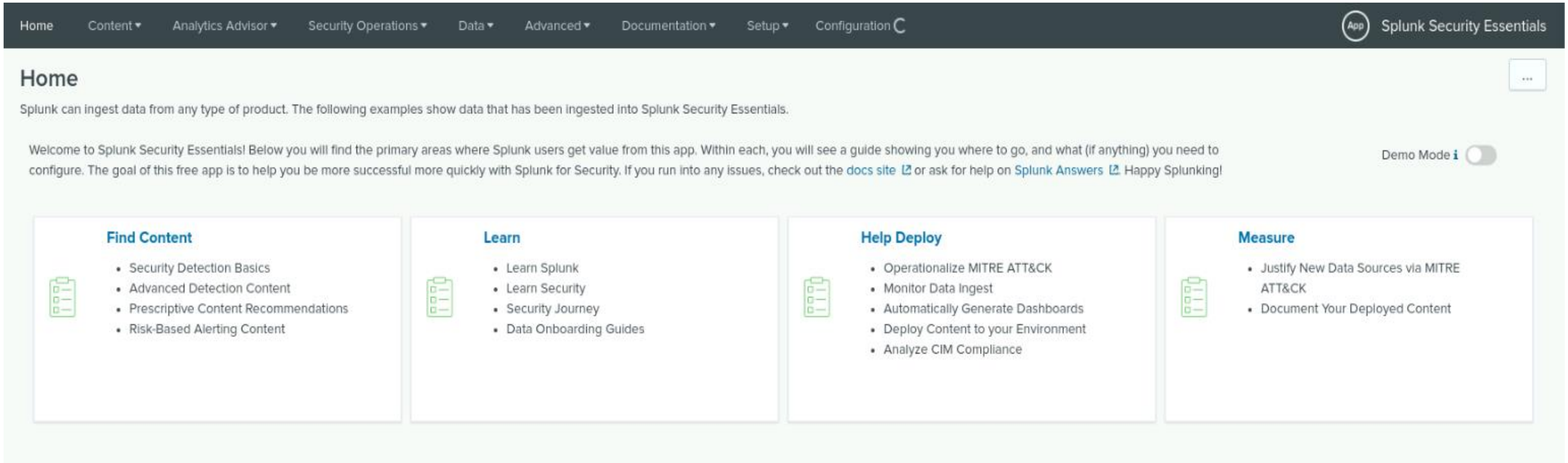
- improve security posture by providing them with the tools and resources they need to detect and respond to threats more effectively.
- reduce risk of data breaches and other security incidents by identifying and remediating security vulnerabilities.
- increase efficiency of their security operations by automating tasks such as threat detection and investigation.
- reduce costs of their security operations by providing them with a free and easy-to-use solution for detecting and responding to threats.

Since VSI is aware of the potential that their network may be exploited, they are able to:

- easily identify potential threats using the content library.
- learn more about threat security with the additional documentation provided.
- more easily deploy and automate monitoring solutions.
- measure success of currently deployed solutions and determine additional solutions that could be added.

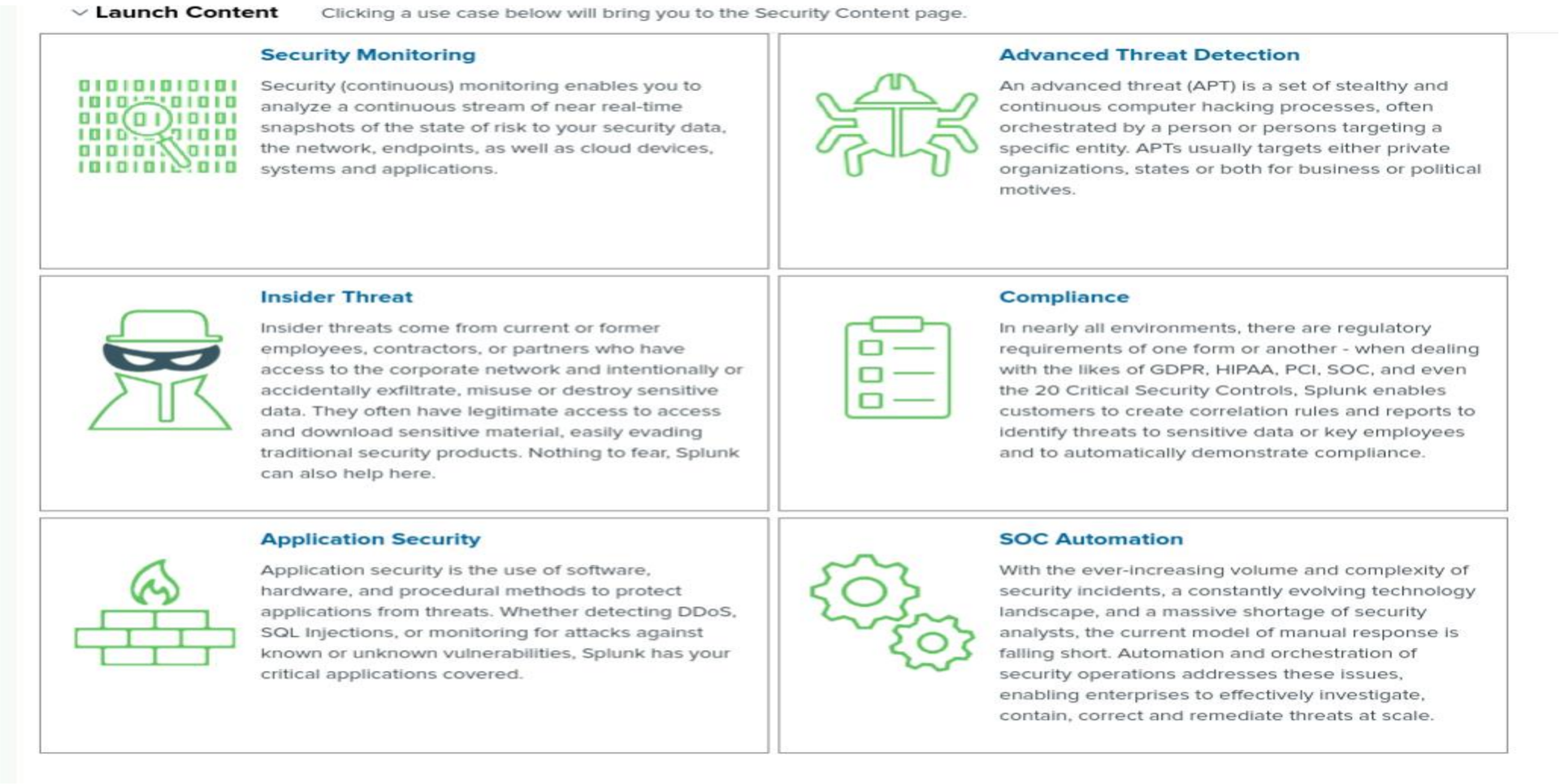
Splunk Security Essentials

To commence using the Splunk Security Essentials Add On you first select the module you wish to use.
In this instance, we chose the “Find Content” module.



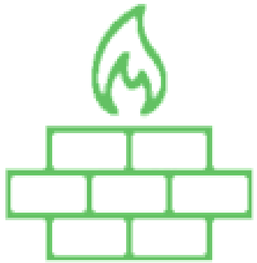
Splunk Security Essentials

Next we choose the type of content we want to explore solutions about.



Splunk Security Essentials

In this case we chose the Application Security content library to explore solutions for.

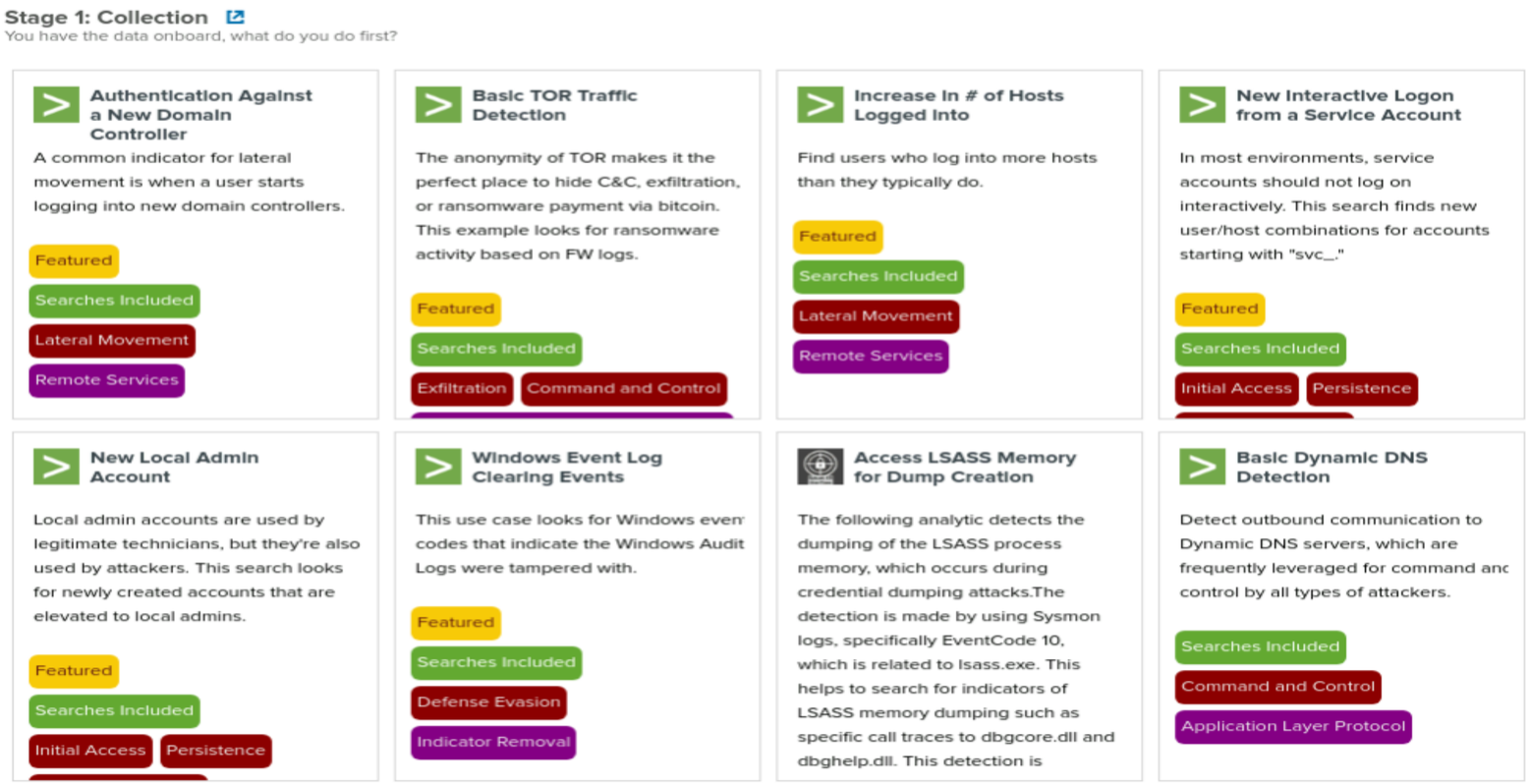


Application Security

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.

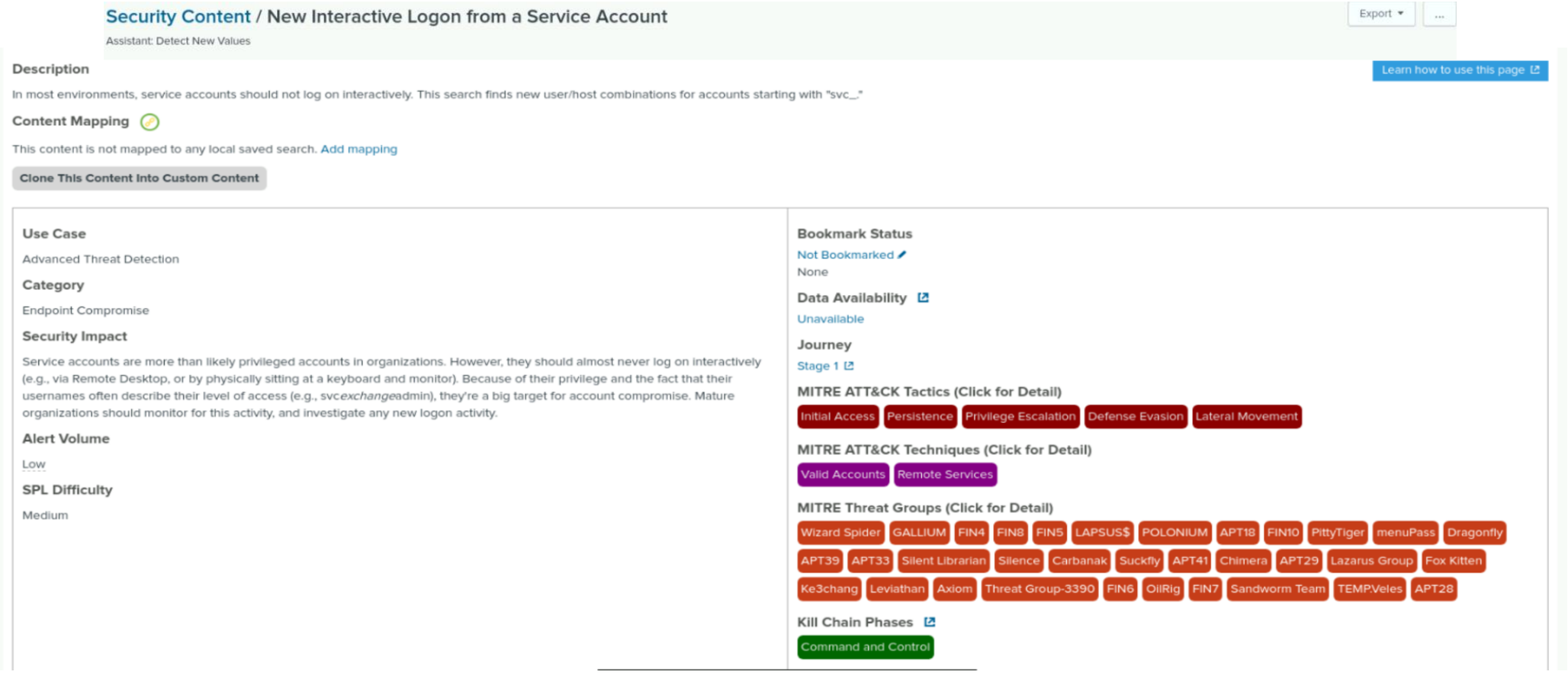
Splunk Security Essentials

In the Application Security content library there are hundreds of solutions to search for.



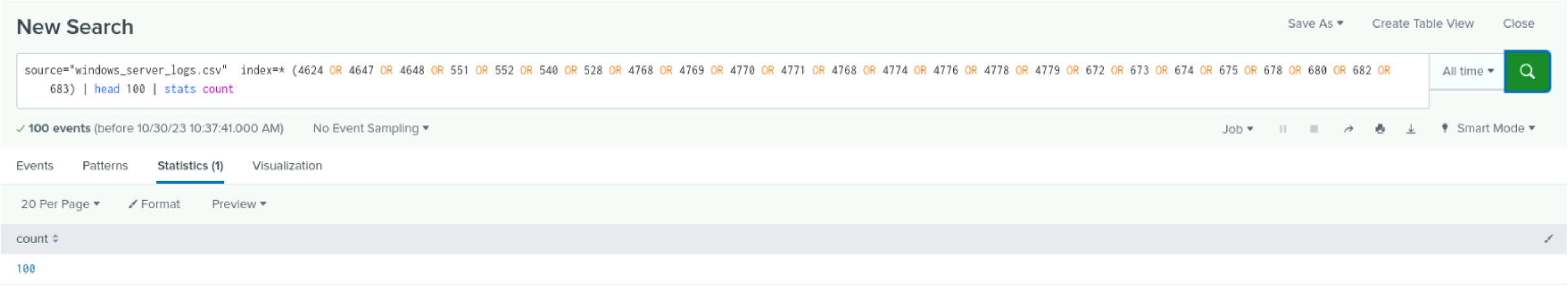
Splunk Security Essentials

For our purposes we chose the New Interactive Logon from a Service Account. On the content card there is a lot of valuable information that explains what security risks this particular solution solves. There are also details about the MITRE ATT&CK strategy and Kill Chain Phase the solution aligns with. This information acts as an educational tool for less experienced cyber security professionals.



Splunk Security Essentials

The content card includes the command syntax to run the solution which helps to make the implementation process more efficient.



Logs Analyzed

1 Windows Logs

The Windows server runs the backend systems for VSI.

The logs from the Windows server represent baseline of normal activity that include data about account creations and deletions, successful and failed user login attempts as well as other hardware and software events that occur on a Windows server.

2 Apache Logs

The Apache web server hosts the web applications for VSI.

The logs from the Apache web server represent a baseline of normal activity that include data about HTTP methods, status codes and source web traffic as well as other web operation events that occur on an Apache web server.

Windows Logs

Reports—Windows

Our SOC team designed the following reports:

Report Name	Report Description
ID Number associated with Signatures	This report shows signatures and the corresponding signature ID.
Severity Levels	This report quickly identifies the severity of an event and the number of those events.
Success and Failure of Windows Activities	This report identifies the ratio of successful and failed activities on the windows server.

Report - Signatures and ID’s

✓ **15 events** (before 11/5/23 2:41:34.000 AM) No Event Sampling

Events Patterns **Statistics (15)** Visualization

20 Per Page Format Preview

signature_id	signature
4726	A user account was deleted
4720	A user account was created
4743	A computer account was deleted
4624	An account was successfully logged on
4672	Special privileges assigned to new logon
4724	An attempt was made to reset an accounts password
4717	System security access was granted to an account
4673	A privileged service was called
4648	A logon was attempted using explicit credentials
4740	A user account was locked out
4739	Domain Policy was changed
4738	A user account was changed
4689	A process has exited

Table showing Signature ID’s and their associated Signature

Report - Severity Levels

The severity levels, and the count and percentage

Save | Save As | View | Create Table View | Close

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| top severity
```

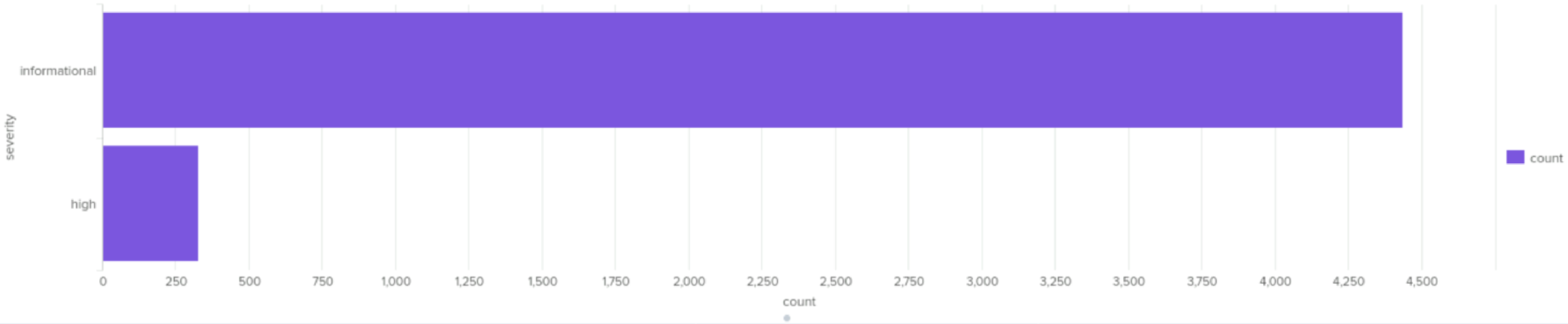
All time

✓ **4,764 events** (before 11/5/23 2:52:49.000 AM) No Event Sampling

Job | Smart Mode

Events | Patterns | Statistics (2) | **Visualization**

Bar Chart | Format | Trellis



severity	count	percent
informational	4435	93.094039
high	329	6.905961

The Severity levels, and the count and percentage

Report - Success / Failure of Windows Activities

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| top status
```

All time

✓ **4,764 events** (before 11/5/23 3:08:37.000 AM) No Event Sampling Job Smart Mode

Events Patterns Statistics (2) **Visualization**

Number display Format Trellis

status	count	percent
success	4622	97.019312
failure	142	2.980688

Comparison between the success and failure of Windows activities.

Alerts—Windows

Our SOC team designed the following alert:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Login Attempts	This alert is triggered when an abnormal number of login attempts have been made on the windows server over an hour.	5	10

JUSTIFICATION: 5 failed login attempts per hour was not uncommon. It occurred 40% of the time. Under normal conditions there were no more than 10 failed login attempts per hour and so setting a threshold at 10 would seem to indicate potential suspicious activity.

Alerts—Windows

Our SOC team designed the following alert:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Account Logins	This alert is triggered by an abnormal number of successful login attempts per hour to a user account	15	25

JUSTIFICATION: 15 successful login attempts per hour occurred 35% of the time. There were no more than 21 successful attempts so setting a threshold of 25 would seem to be a reasonable trigger to suspicious activity.

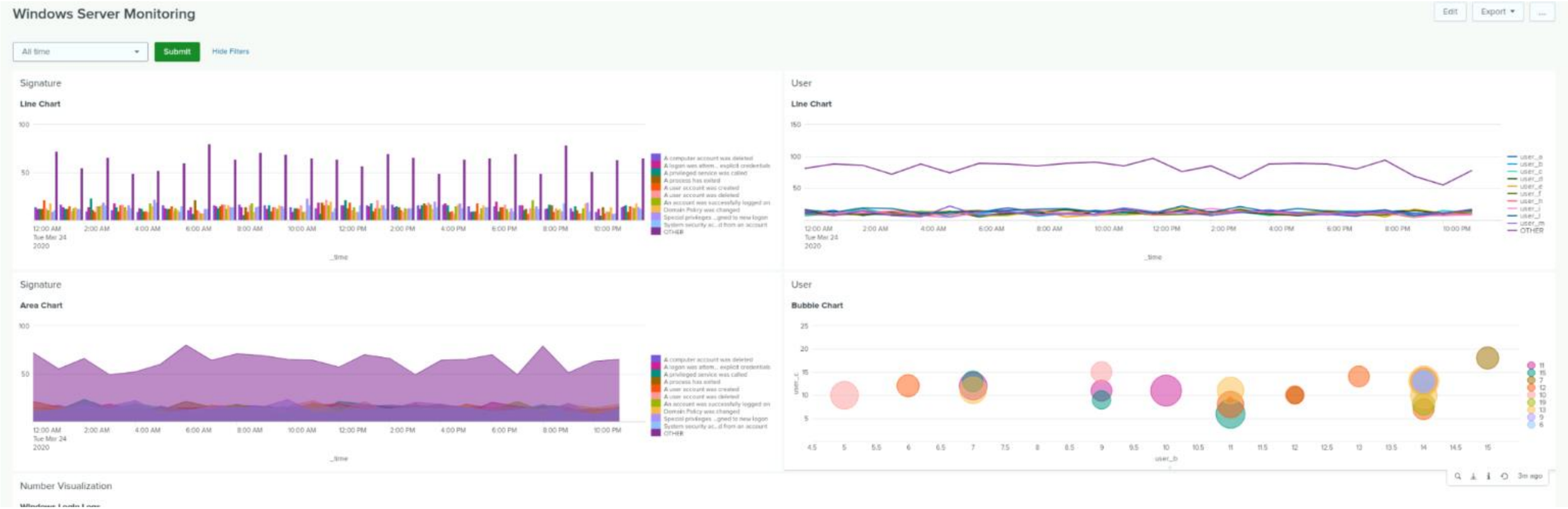
Alerts—Windows

Our SOC team designed the following alert:

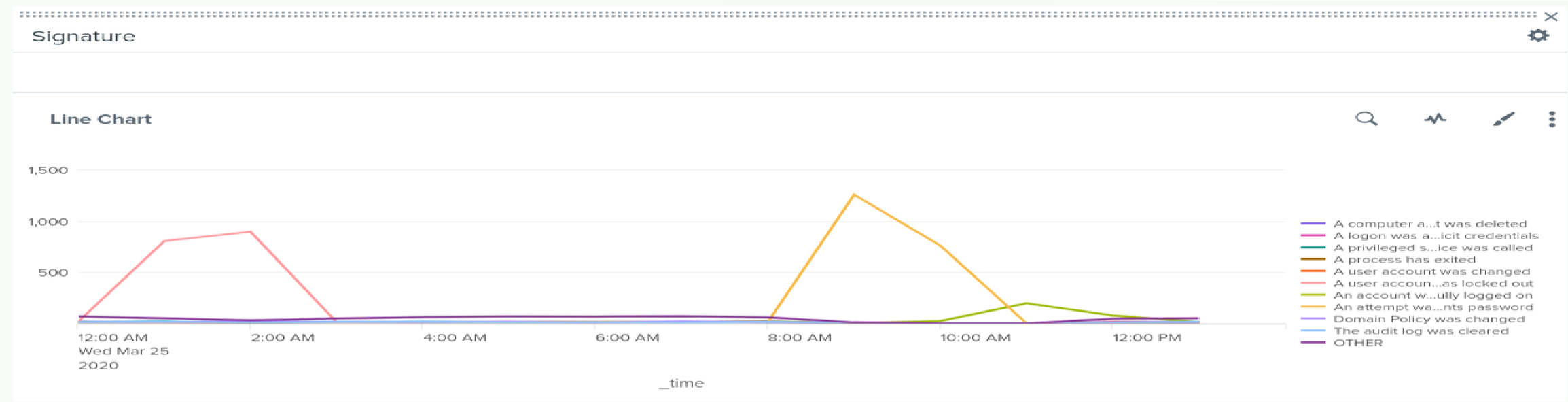
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Deleted User Accounts	This alert is triggered by an abnormal number of user accounts deleted each hour	15	25

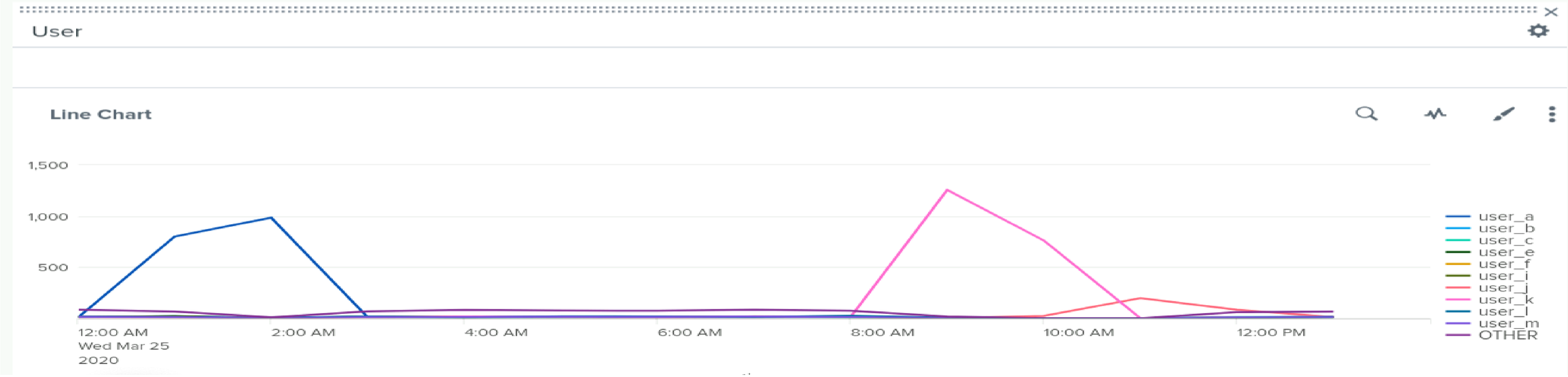
JUSTIFICATION: 15 account deletions per hour was not abnormal. It occurred approximately 30% of the time. Anytime there is more than 25 account deletions per hour might raise suspicion.

Dashboard - Change in Signatures & Users



Line Charts - Signatures / Users



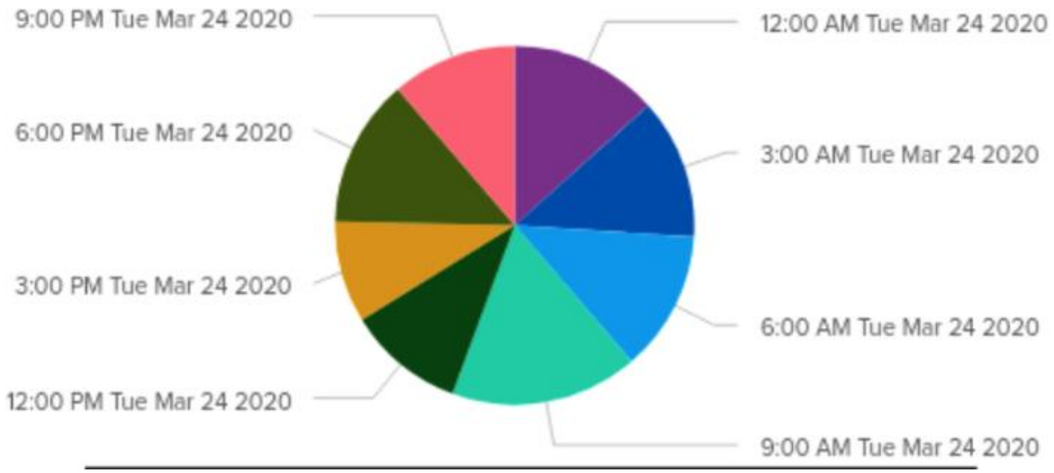


Dashboard -

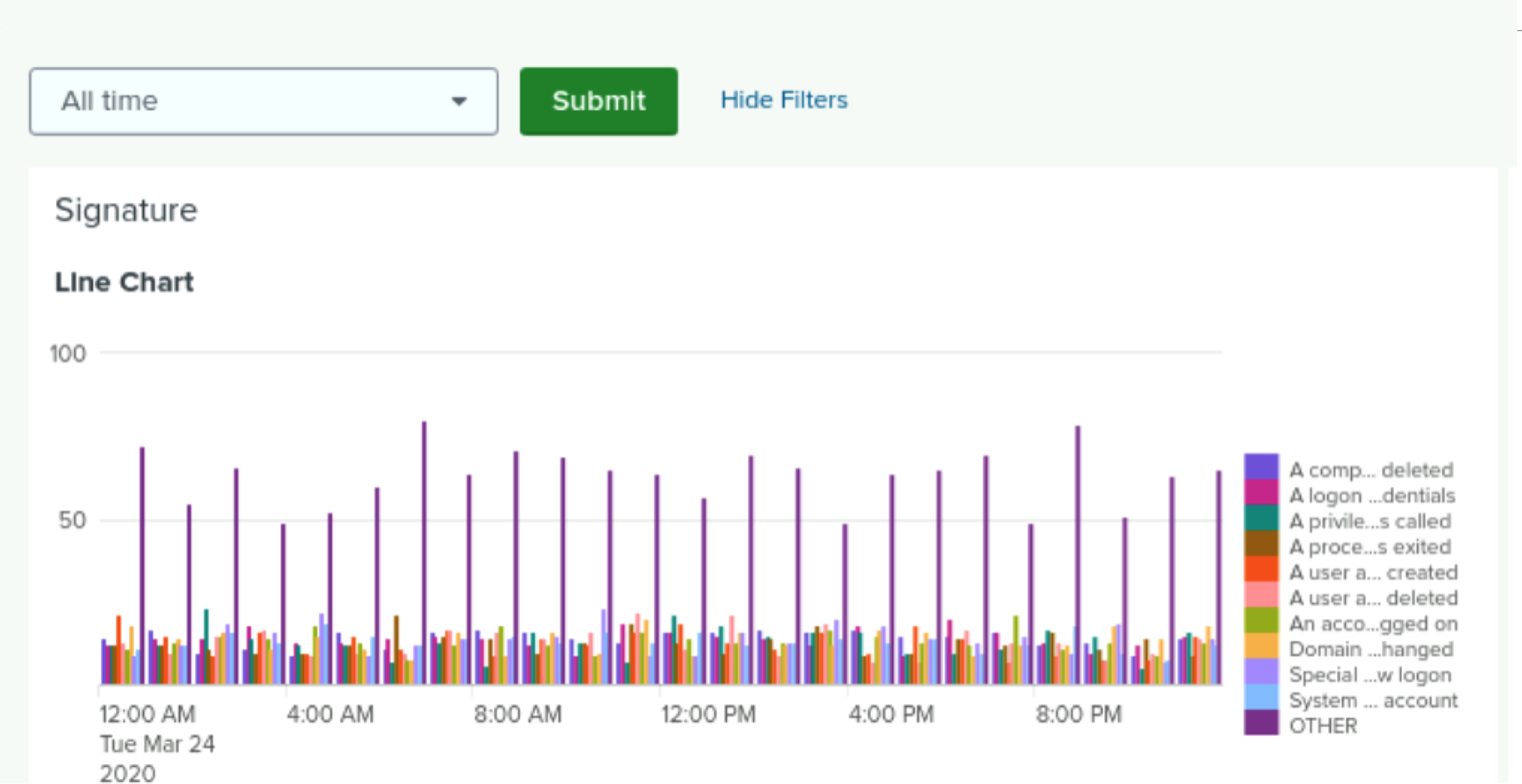
Number Visualization

Windows Login Logs

Windows Logon Failure



Dashboard - Change in Signatures with Time Range



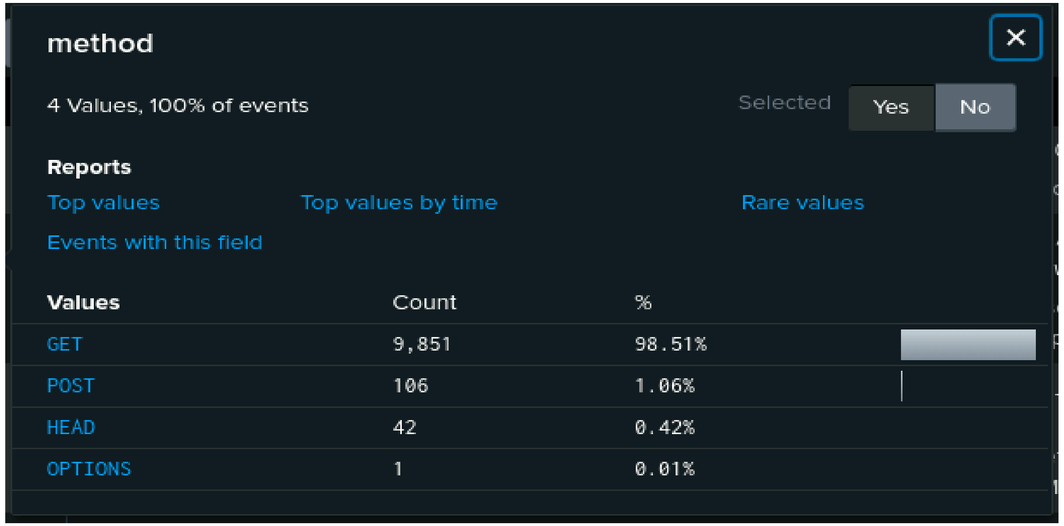
Apache Logs

Reports Apache

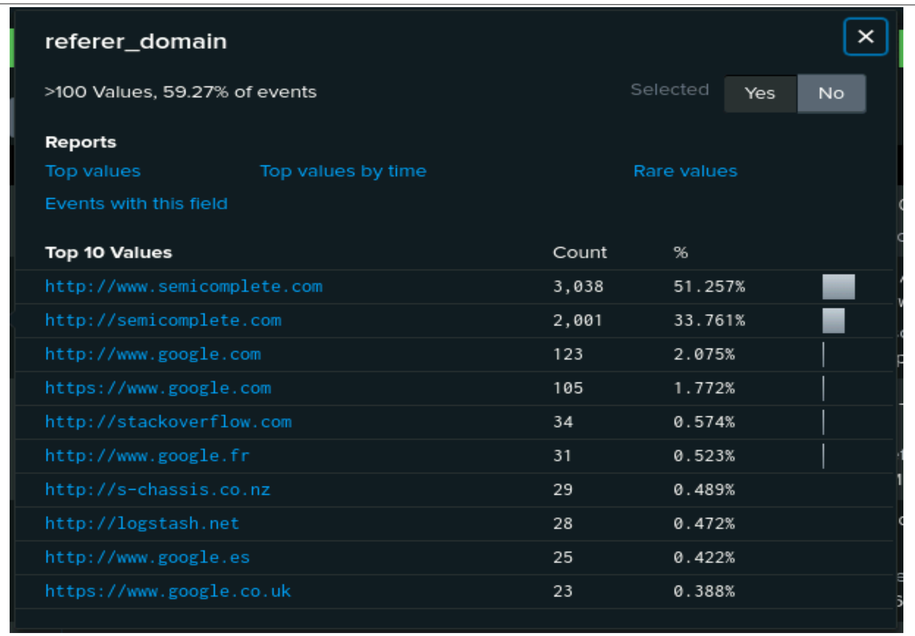
Our SOC team designed the following reports:

Report Name	Report Description
HTTP Methods	This report shows the range of request methods used to interact with the VSI server.
Top 10 Referrer Domains	This report shows the top 10 domains used to refer to the https://vsi-corporation.azurewebsites.net/ web application.
HTTP Response Code	This report identifies the HTTP response code from the web server that relates to a request method and whether the request method has been successfully completed or not.

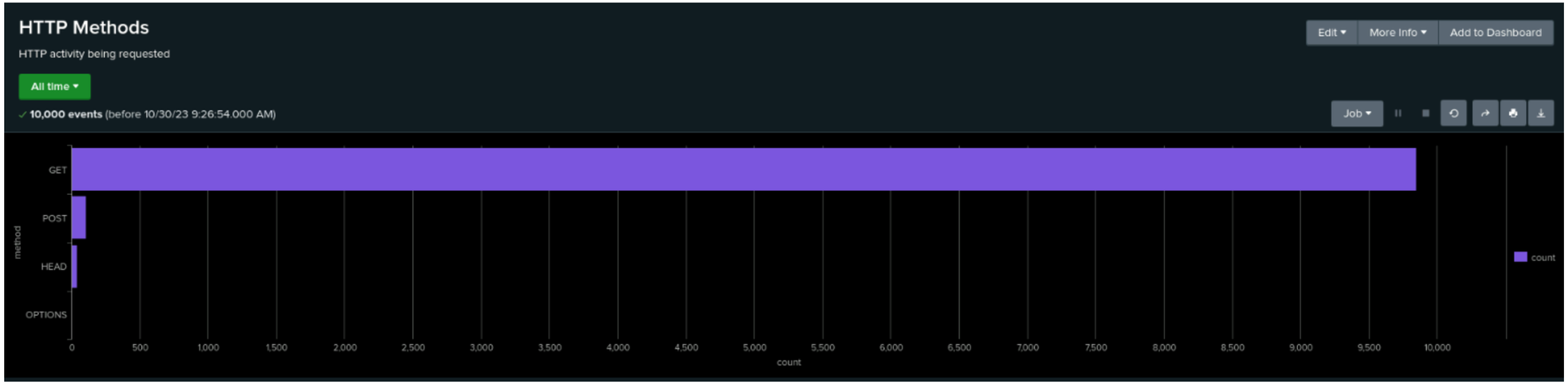
Reports - HTTP Method / Response Code / Referrer Domains

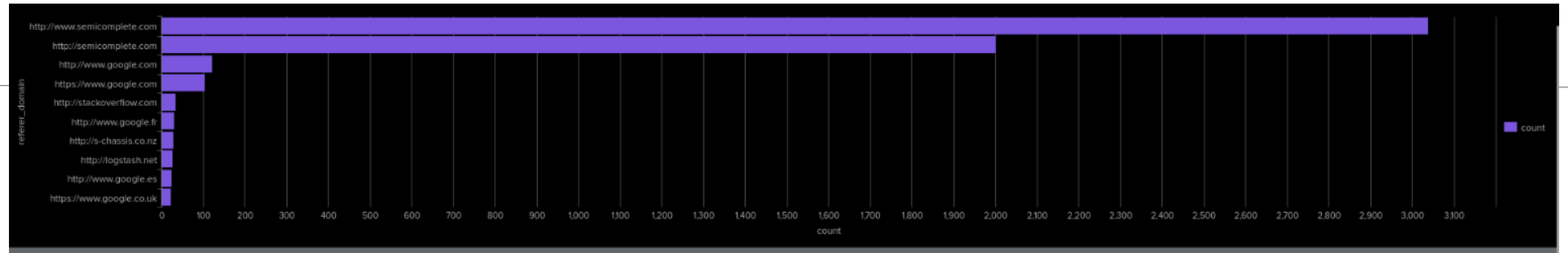


Values	Count	%
GET	9,851	98.51%
POST	106	1.06%
HEAD	42	0.42%
OPTIONS	1	0.01%

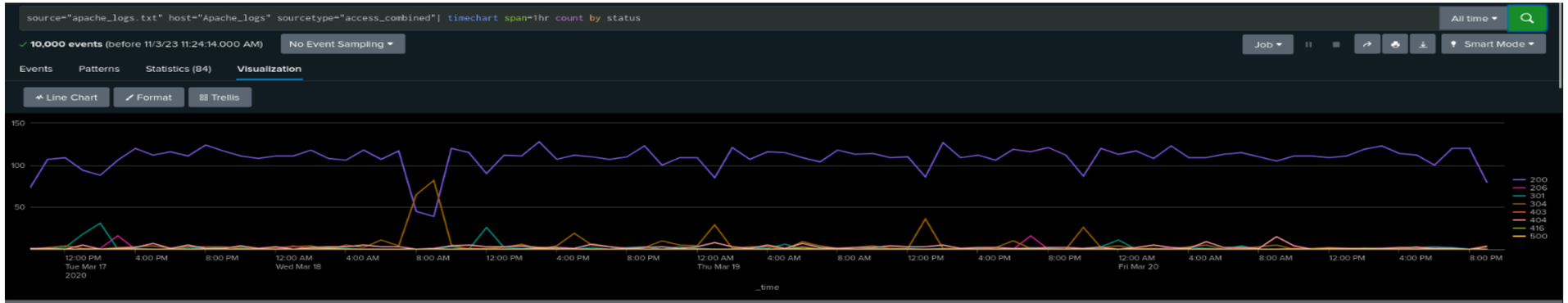


Top 10 Values	Count	%
http://www.semicomplete.com	3,038	51.257%
http://semicomplete.com	2,001	33.761%
http://www.google.com	123	2.075%
https://www.google.com	105	1.772%
http://stackoverflow.com	34	0.574%
http://www.google.fr	31	0.523%
http://s-chassis.co.nz	29	0.489%
http://logstash.net	28	0.472%
http://www.google.es	25	0.422%
https://www.google.co.uk	23	0.388%





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



_time	200	206	301	304	403	404	416	500
2020-03-17 10:00	73	0	0	0	0	1	0	0
2020-03-17 11:00	107	0	1	2	0	1	0	0
2020-03-17 12:00	109	0	2	4	0	0	0	0
2020-03-17 13:00	94	0	18	1	0	5	0	0
2020-03-17 14:00	88	1	31	0	0	0	0	0

Alerts Apache

Our SOC team designed the following alert:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
International Traffic	This alert is triggered when the hourly activity from any country besides the United States exceeds normal levels.	8	11

JUSTIFICATION: We set the baseline at 8 visits per hour for web visits from countries other than the United States. The baseline We set the threshold at 11. When the number of hourly web application visits from international sources exceeds this threshold, it triggers the alert.

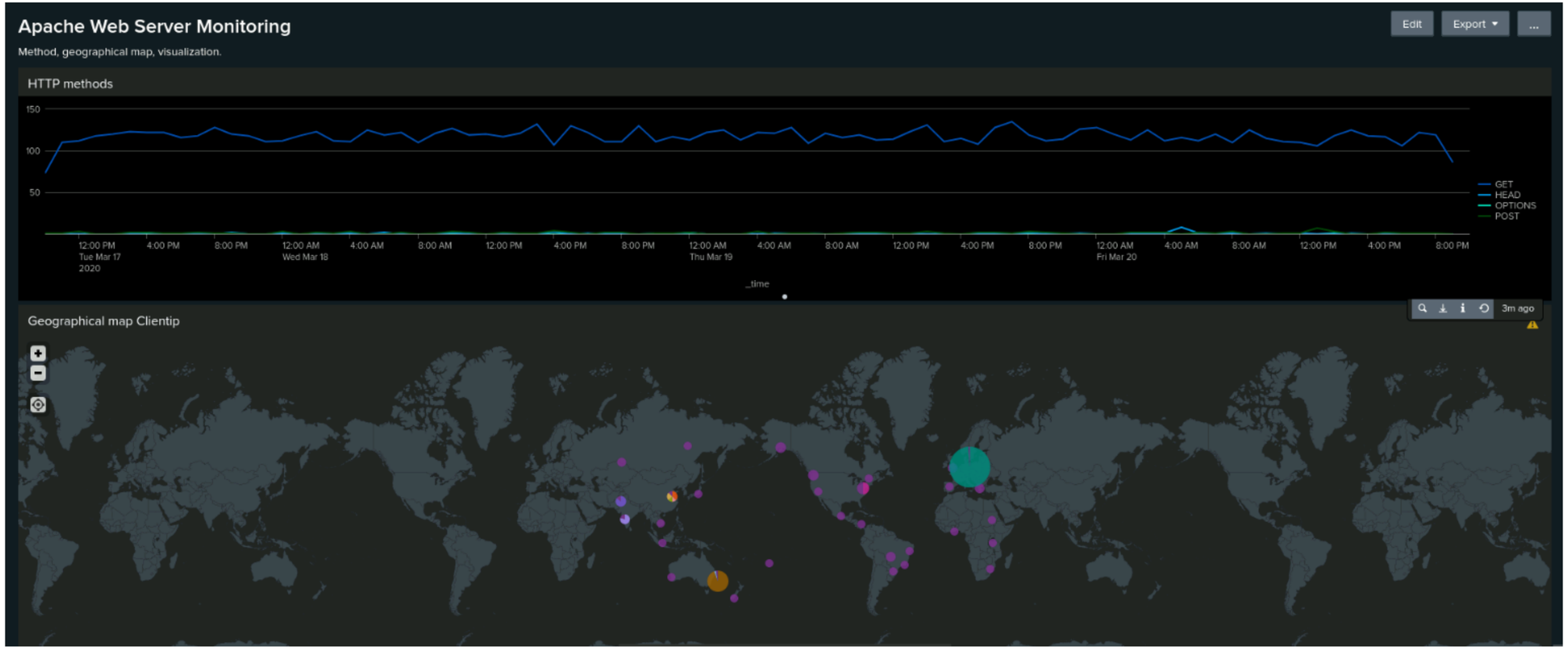
Alerts Apache

Our SOC team designed the following alert:

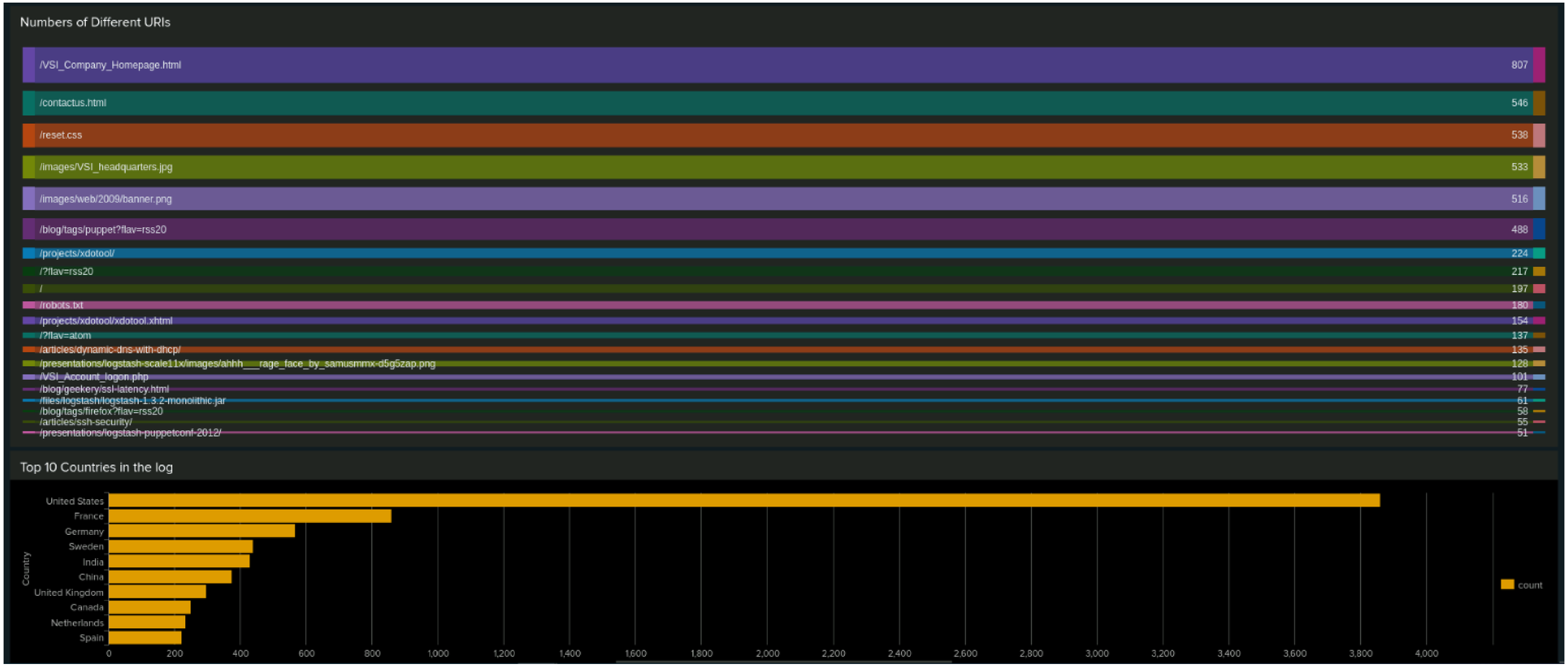
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Method	This alert is triggered when the number of HTTP POST requests exceed a normal level.	2	7

JUSTIFICATION: The baseline is set at 2, indicating the typical level of HTTP POST method activity during a specified time period. The threshold is set at 7. This threshold is chosen to trigger an alert when the count of HTTP POST method activities exceeds this value.

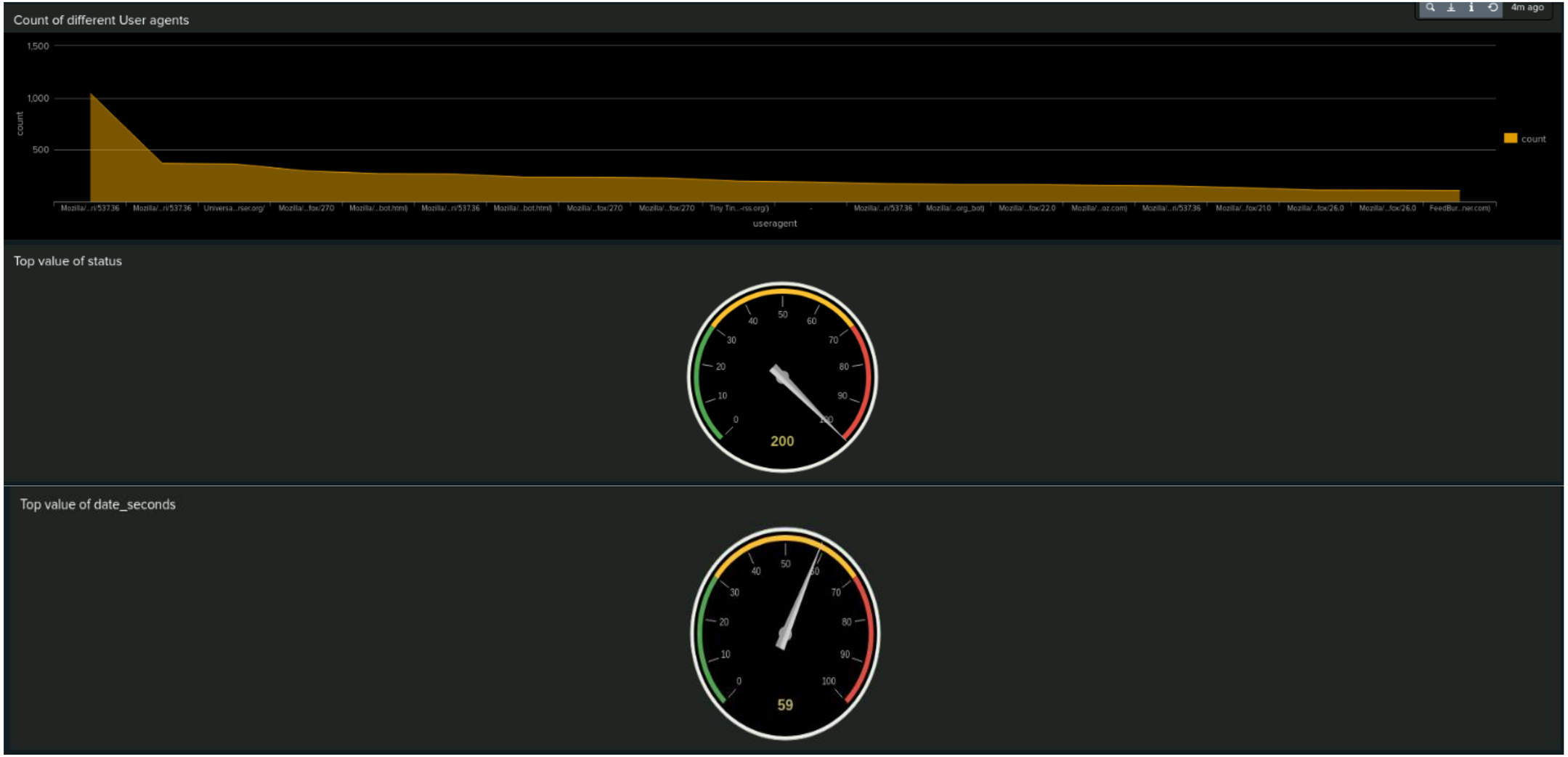
Dashboard - HTTP Method / Geographical Map with Client IP



Dashboard - Different URIs and Top10 Countries



Dashboard - User Agents with Status Top values of status



Attack Analysis

Attack Summary—Windows

Report analysis for Event Severity:

Suspicious changes to the severity of event signatures were detected in our reports.

- There was a significant increase in high severity events, indicating a potential security threat.
- Under normal operating conditions 329 events (6.91%) were reported high severity. During the cyber attack 1,111 events (20.22%) were reported high severity.

Report analysis for Failed Activities:

Suspicious changes in failed activities on the Windows server were detected in our reports.

- Failed activity descriptions included “logon attempts using explicit credentials”, “attempts to reset account passwords”, and “user accounts locked out”.

This change in severity suggests that there may be ongoing attacks or suspicious activities that need further investigation. These patterns of activity are typically indicative of malicious intent and raise serious concerns about the security of the Windows Server environment.

Attack Summary—Windows

- Alert analysis for Failed Windows Activity:

A suspicious change in volume of failed Windows activity was detected by our alerts.

- There was an increase in failed login attempts to the Windows server.
- Our alerts detected 35 failed login attempts that occurred in the hour from 8am on March 25, 2020.
- The threshold we established (12 per hour) triggered our alert for this type of activity.
- Upon review, there is no need to change the determined threshold.

- Alert analysis for Successful Logins:

A suspicious increase in volume of successful logins to the Windows server was detected by our alerts.

- There was a sustained period of increased login attempts during a 3 hour period of time. There were 196 login attempts between 11am and 12pm suggesting the attack wasn’t over the full 3 hours.
- Most of the login attempts were attributed to "user_J,".
- The threshold we established (25 per hour) triggered our alert for this type of activity.
- Upon review, there is no need to change the determined threshold.

Attack Summary—Windows

- Alert analysis for Deleted Accounts:

Our alert did not detect any suspicious change in volume of deleted accounts.

- Under normal operating conditions the highest number of deleted accounts in any hour was 22.
- The attack logs showed only a maximum of 17 deleted accounts in any hour (5am).

The increase in failed login attempts combined with the increase in successful login attempts suggest a brute force attack that resulted in successful logins to the Windows server.

We would need to investigate the deleted accounts to determine if they were genuine or part of the malicious attack. Even under normal conditions 22 deleted accounts in one hour seems to be a lot of account deletions. It would be advisable to monitor and check the account deletions to ensure there is no malicious intent.

Attack Summary—Windows

- Dashboard analysis for time chart of Signatures:

Suspicious activity with regard to Signatures was detected on our monitoring dashboard.

- Our dashboard analysis highlights specific signatures, such as "A user account was locked out" and "An attempt was made to reset an account's password," which are indicative of potential security threats.
- Our dashboard shows that "A user account was locked out" 785 times whilst "An attempt was made to reset an account's password" 397 times
- Our dashboard shows that "A user account was locked out" occurred between 1:40AM and 2:40AM whilst "An attempt was made to reset an account's password" occurred between 9:10AM and 11:00AM.

- Dashboard analysis for Users:

Suspicious activity was detected on our monitoring dashboard by some users.

- Our dashboard shows User_A was monitored to have 785 suspicious activities between 1:40AM and 2:40AM.
- Our dashboard shows User_K was monitored to have 397 suspicious activities between 9:10AM and 11:00AM.

Attack Summary—Windows

- Dashboard analysis for Signatures with Bar, Graph and Pie Charts:

The same suspicious activity was detected on our Bar, Graph and Pie Charts as that on our time chart.

- Dashboard analysis for Users with Bar, Graph and Pie Charts:

The same suspicious activity was detected on our Bar, Graph and Pie Charts as that on our time chart.

The difference with the statistical charts and graphs is that they provide for easy visual cues relating to abnormal activity. The time charts allow for detail relating to time and duration of an attack.

The threat actors successfully gained access to the Windows server.

It seems that User_A may have been locked out of an account on 785 occasions as the number of “user account locked out” signatures between 1:40AM and 2:40AM was identical to the suspicious activity for User_A during the same time period.

It seems that User_K may have attempted to change an account’s password on 397 occasions as the number of “an attempt was made to reset an account's password” signatures between 9:10AM and 11:00AM was identical to the suspicious activity for User_K during the same time period.

Report - HTTP methods (Attack Log)

```
source="apache_attack_logs.txt"  host="Apache_logs" sourcetype="access_combined" | top limit=20 method
```

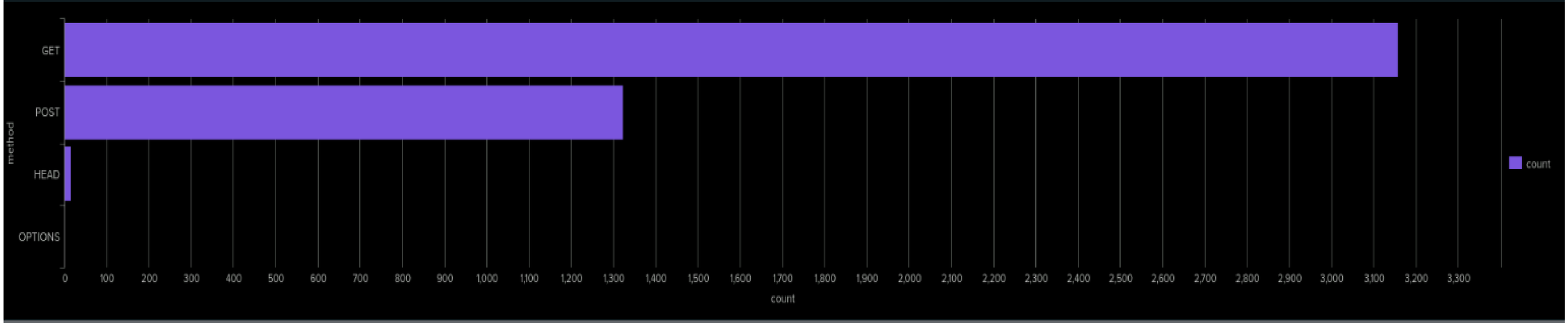
All time

✓ **4,497 events** (before 11/3/23 10:11:01.000 AM) No Event Sampling

Job Smart Mode

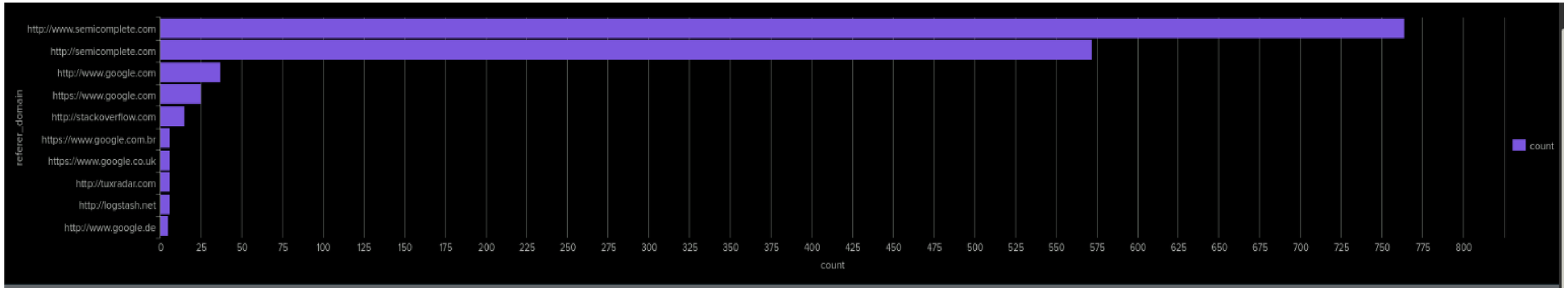
Events Patterns Statistics (4) Visualization

Bar Chart Format Trellis



method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237

Report - Top 10 Referrer Domains (Attack Log)



referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

Attack Summary of Apache Reports

- Report analysis for HTTP methods:

Suspicious changes to the volume of HTTP methods were detected in our reports.

- HTTP POST requests are used to create or update resources on a server with private data and the reports showed a significant increase in POST requests.
- HTTP GET requests are used for retrieving data and resources from a server and the report showed a significant increase in GET requests.

- Report analysis for Referrer Domains:

Suspicious changes to the volume of referrer domains was observed in our reports.

- There was a significant decrease in Referrer Domain activity. We suspect a Distributed Denial of Service (DDoS) attack may have denied users access to https://vsi-corporation.azurewebsites.net/ from other web applications.
- During the cyber attack there were 764 referred domains compared with typical 3,038.
- We did not detect any suspicious domains themselves.

Attack Summary of Apache Reports

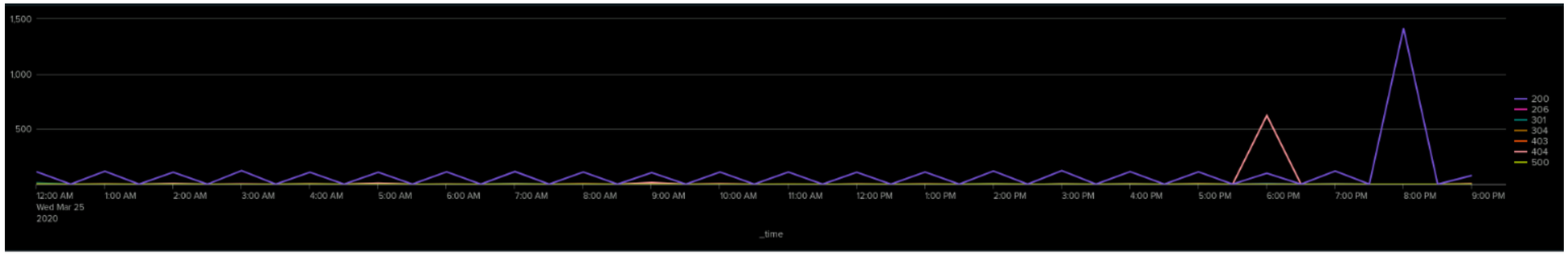
- Report analysis for HTTP Response Codes:

Suspicious changes to volume of HTTP response codes were detected in our reports.

- There was an increase in status code 404 which indicates a requested resource was not found on the server and therefore unsuccessful.
- There was a decrease in status code 200 which indicates a request was successful.

The increase in HTTP POST requests combined with the increase in 404 response codes and the decrease in referrer domains suggests the Apache web server experienced a DDoS attack.

Dashboard - Top 10 Countries Source Traffic (Attack Log)



clientip	count	percent	City	Country	Region	lat	lon
194.105.145.147	438	12.443182	Kyiv (Solom'yans'kyi district)	Ukraine	Kyiv City	50.42240	30.50600
79.171.127.34	432	12.272727	Kharkiv (Shevchenkivs'kyi District)	Ukraine	Kharkiv	50.03680	36.22020
194.146.132.138	432	12.272727	New York	United States	New York	40.71280	-74.00600
130.237.218.86	183	5.198864	Stockholm (Östermalm)	Sweden	Stockholm	59.34990	18.06970
46.105.14.53	84	2.386364	Strasbourg	France	Grand Est	48.57340	7.75211
89.107.177.18	37	1.051136	Tres Cantos	Spain	Madrid	40.61290	-3.69500
184.66.149.103	37	1.051136	Courtenay	Canada	British Columbia	49.68410	-124.99000
200.31.173.106	34	0.965909	Antiguo Cuscatlán	El Salvador	La Libertad	13.66490	-89.25320
38.99.236.50	33	0.937500	Miami (Downtown Miami)	United States	Florida	25.78240	-80.19310
24.0.194.37	32	0.909091	Plainfield	United States	New Jersey	40.63370	-74.40740

Report - HTTP POST Method (Attack Log)

Attack Summary of Apache Alerts

- Alert analysis for International Traffic:

Suspicious web traffic from international sources generated our predetermined alert.

- There were 432 events between 7:00PM and 8:00 PM on March 25, 2020.
- The threshold we established (11 per hour) triggered our alert for this type of activity.
- Upon review, there is no need to change the determined threshold.

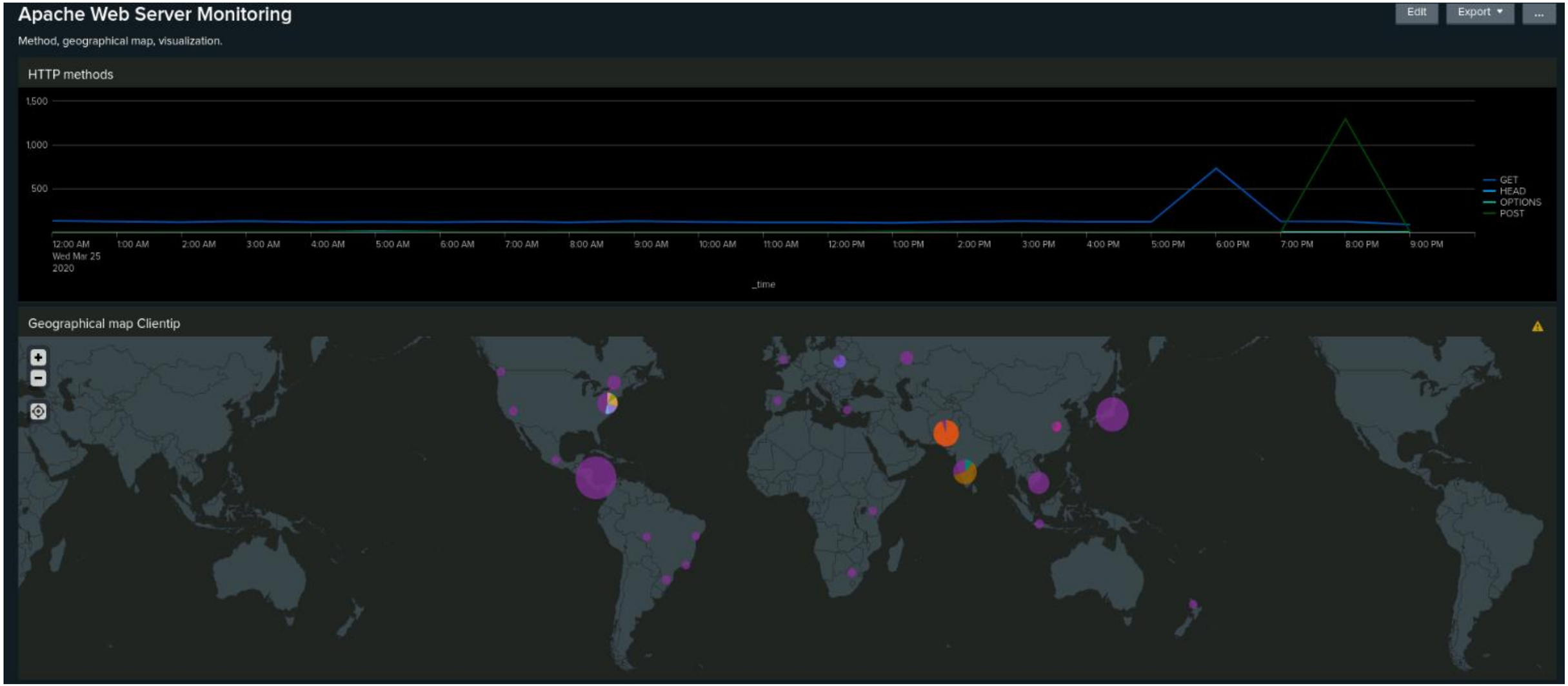
- Alert analysis for HTTP POST activity:

Suspicious HTTP POST activity generated our predetermined alert.

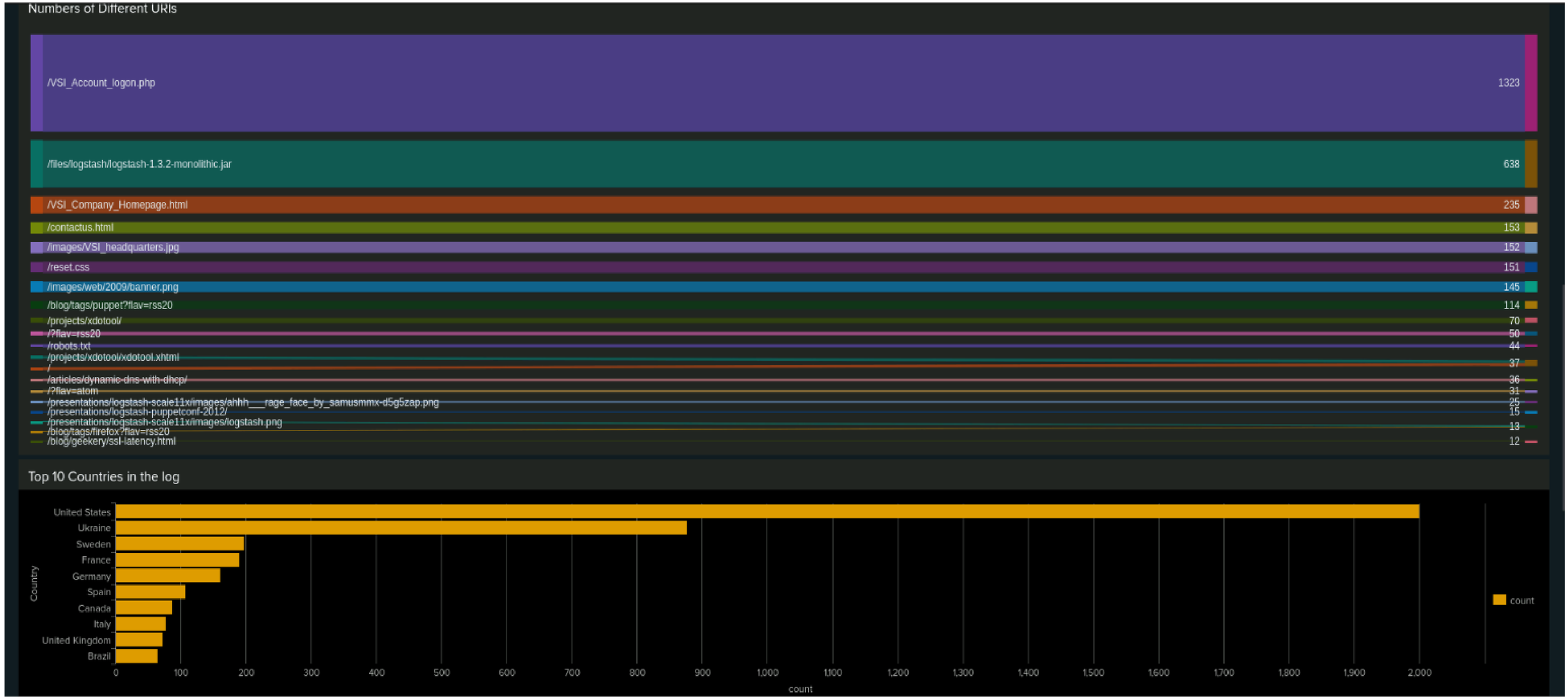
- Between 7:00PM until 8:00PM on March 25, 2020 there were 1296 POST requests recorded.
- The threshold we established (7 per hour) triggered our alert for this type of activity.
- Upon review, there is no need to change the determined threshold.

Our alerts suggest either a DDoS attack or an attempt to upload malicious files to the web server.

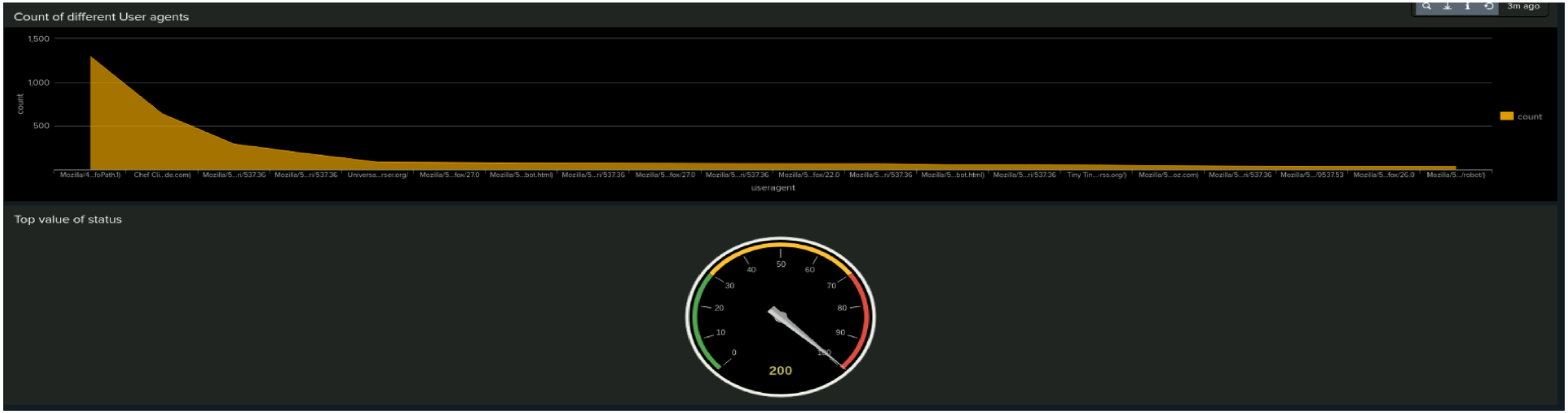
Dashboard - International Map with Client IP (Attack Log)



Dashboard - URI Traffic (Attack Log)



Dashboard - User Agent Count (Attack Log)



Attack Summary of Apache Dashboard

- Dashboard analysis for time chart of HTTP Methods:

Suspicious HTTP request activity was detected on our monitoring dashboard.

- There was an increase in GET requests and POST requests to the web server during the suspected cyber attack.
- GET requests increased between 5:00PM and 7:00PM while POST requests increased between 7:00PM and 9:00PM.
- There were 729 GET requests and 1,296 POST requests.

- Dashboard analysis for International Cluster Map:

Suspicious international web traffic was observed on our monitoring dashboard.

There was a significant increase in web traffic from Ukraine.

- Dashboard analysis for URI Data

Suspicious web page traffic was observed on our monitoring dashboard.

- Web traffic to the page URI https://vsi-corporation.azurewebsites.net/vsi_account_logon.php/ was extremely high with 1323 visits.
- We believe the attacker might be attempting to gain access to the database by brute forcing login attempts using credentials obtained from from the Windows server.

The increase in HTTP POST requests from the Ukraine in conjunction with the increase in traffic to the account logon page indicates a brute force attack.

Summary and Future Mitigations

Project 3 Summary

Our SOC team determined that there was a cyber attack on each of the VSI systems and applications.

To begin with there was an increase in malicious activity on the Windows server that included attempts to login using explicit credentials and reset account passwords that caused user accounts to be locked out. Given the increase in failed login attempts as well as successful login attempts, it appears threat actors conducted a brute force attack on the Windows server with some credentials enabling access to the server. Further investigation is required to determine whether there is malware on the server.

Using the credentials obtained from the Windows server the threat actors attempted to exploit the Apache web server. There was a substantial increase in HTTP POST requests which suggests they may have been trying to upload malicious files to the web server. The malicious activity seems to have originated from the Ukraine.

There was a brute force attack on the Apache web server with a significant amount of login attempts on the account logon page of the web application.

It appears the threat actors tried to compromise the Windows server in the first instance with the intent of using credentials obtained to gain access to the Apache web server. The attacks commenced on the WIndows server in the morning on March 25, while the attacks on the Apache web server commenced in the evening of March 25.

Project 3 summary

To protect VSI systems and applications from future attacks, our SOC team recommends taking the following actions:

- Continue to improve the monitoring parameters in our Security Information and Event Management System (SIEM)
- Increase password security
- Implement multi-factor authentication
- Implement rate limiting on HTTP request methods
- Introduce a Web Application Firewall