Defensive Security Project

SecureTech Solutions, LLC

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

Virtual Space Industries (VSI), a virtual reality program designing company, has suspicions that their competitor, JobeCorp, may try to launch cyber attacks against their system. VSI has a web application run by an Apache Linux server and a Windows operating system that runs VSI’s backend server operations.

“Add on” or App

OT Security

We chose OT Security Add-on for Splunk that operate assets, networks, and facilities across both IT and OT (Operational Technology) environments, we found features that we liked such as threats and attacks, compliance, incident investigation, forensics, and incident response across the broad spectrum of assets and topologies from email servers to PLCs. Once we installed the app and did further research on how to configure it we found that the configuration was to intense for this particular project.

https://splunkbase.splunk.com/app/5151

OT Security

We chose the following scenarios to illustrate some of the reports available:

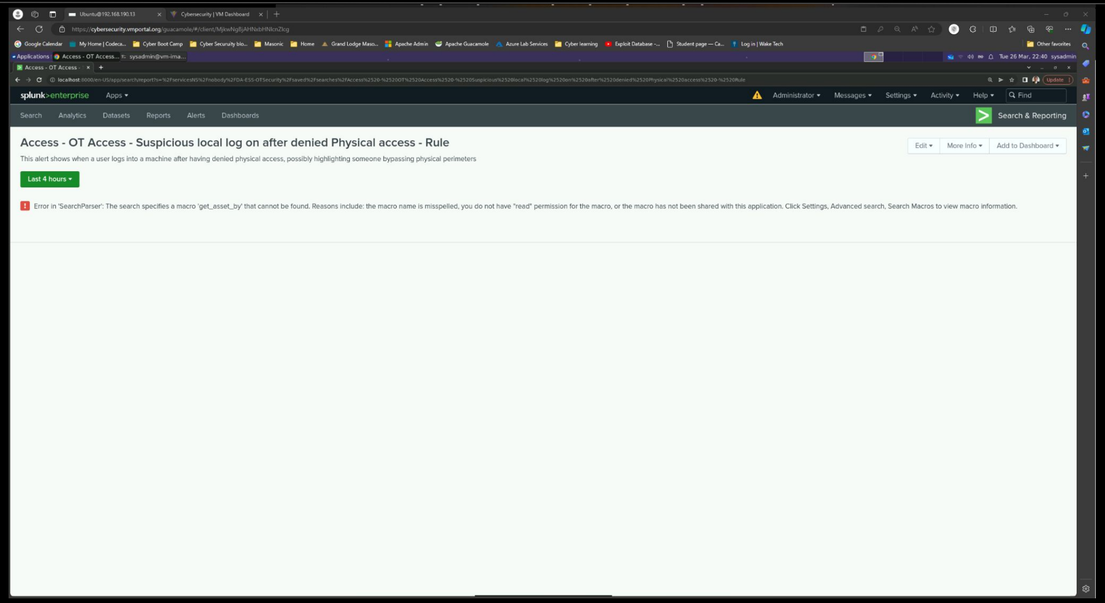
1. Access - OT Access - Suspicious local log on after denied Physical access - Rule- This report provides İnsight into possible piggybacking or other unauthorized physical access to a facility that may have resulted in system compromise.

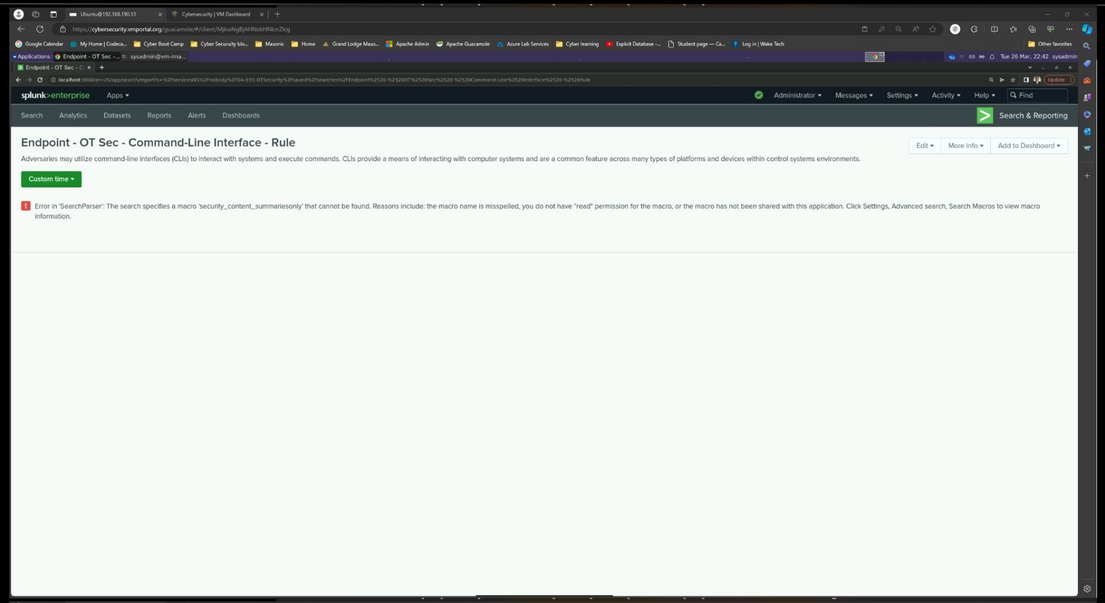
2. Endpoint - OT Sec - Command-Line Interface - Rule- This type of alert in combination with a list of white listed users would be useful in intrusion detection.

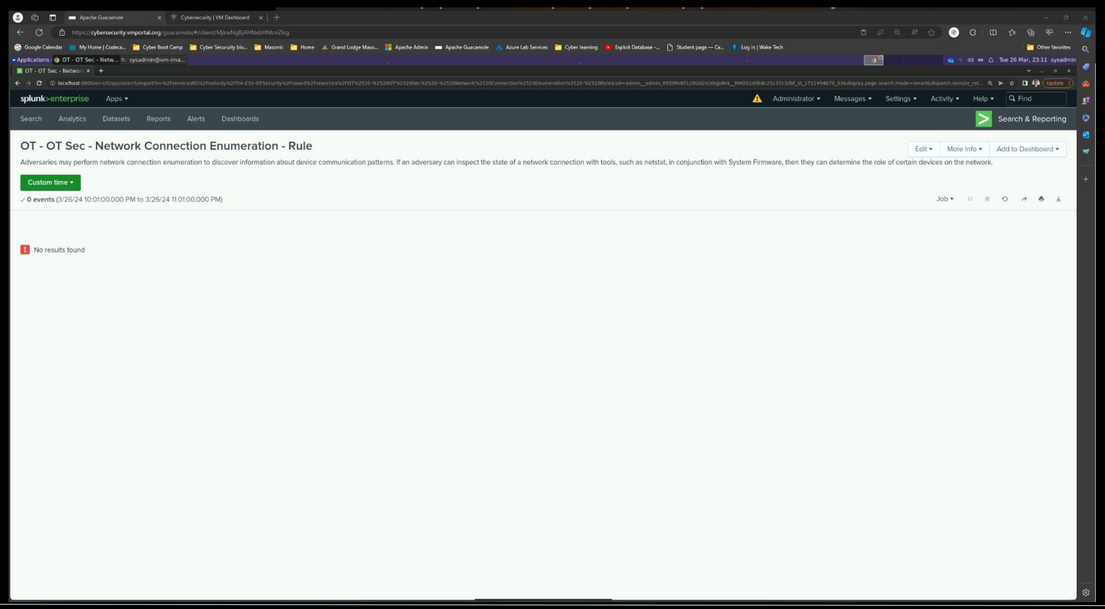
3. OT - OT Sec - Network Connection Enumeration - Rule- Alerts related to enumeration maybe able to detect attacks at that phase of the penetration.

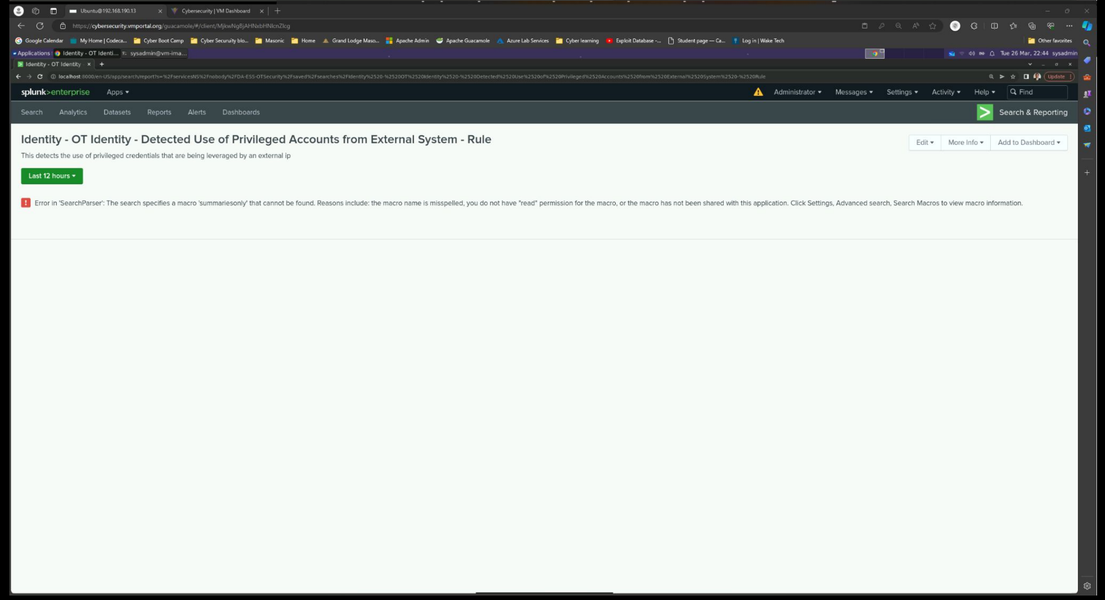
4. Identity - OT Identity - Detected Use of Privileged Accounts from External System - Rule- This type of alert would provide insight into high risk compromises based on users with the ability to do damage if misused. Since it flags by external IPs on these accounts watching these more closely would increase security.

OT Security


Access - OT Access - Suspicious local log on after denied Physical access - Rule
This alert shows when a user logs into a machine after having denied physical access, possibly highlighting someone bypassing physical perimeters
Last 4 hours
Error in 'SearchParser': The search specifies a macro 'get_asset_by' that cannot be found. Reasons include: the macro name is misspelled, you do not have "read" permission for the macro, or the macro has not been shared with this application. Click Settings, Advanced search, Search Macros to view macro information.


Endpoint - OT Sec - Command-Line Interface - Rule
Adversaries may utilize command-line interfaces (CLIs) to interact with systems and execute commands. CLIs provide a means of interacting with computer systems and are a common feature across many types of platforms and devices within control systems environments.
Custom time
Error in 'SearchParser': The search specifies a macro 'security_content_summariesonly' that cannot be found. Reasons include: the macro name is misspelled, you do not have "read" permission for the macro, or the macro has not been shared with this application. Click Settings, Advanced search, Search Macros to view macro information.


OT - OT Sec - Network Connection Enumeration - Rule
Adversaries may perform network connection enumeration to discover information about device communication patterns. If an adversary can inspect the state of a network connection with tools, such as netstat, in conjunction with System Firmware, then they can determine the role of certain devices on the network.
Custom time
0 events (3/26/24 10:01:00.000 PM to 3/26/24 11:01:00.000 PM)
No results found


Identity - OT Identity - Detected Use of Privileged Accounts from External System - Rule
This detects the use of privileged credentials that are being leveraged by an external ip
Last 12 hours
Error in 'SearchParser': The search specifies a macro 'summariesonly' that cannot be found. Reasons include: the macro name is misspelled, you do not have "read" permission for the macro, or the macro has not been shared with this application. Click Settings, Advanced search, Search Macros to view macro information.

Logs Analyzed

1 Windows Logs

- Windows administrative event codes and amounts
- User login information
- Attack activity
- account management
- security policy changes

2 Apache Logs

- Server HTTP requests and response codes
- Referer Domains
- Client IPs and location data
- HTTP status codes.

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signatures and sig_ids	This is a reference report that matches the fields.
Severity level percentages	This shows the event breakdown of severity levels and their percentage amount
successful event percentage	This shows the percent of successful and failed events

Images of Reports—Windows

Severity Totals and Percents

Edit ▾ | More Info ▾ | Add to Dashboard ▾

All time ▾

✓ **4,764 events** (before 3/26/24 11:51:10.000 PM)

Job ▾

2 results | 100 per page ▾

severity ⇕	count ⇕	percent ⇕
informational	4435	93.094039
high	329	6.905961

Signatures and sig_ids

Edit ▾ | More Info ▾ | Add to Dashboard ▾

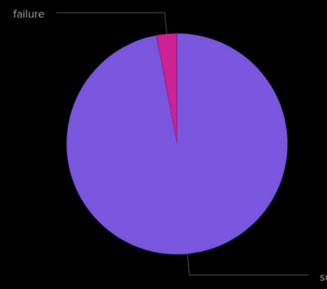
All time ▾

✓ **15 events** (before 3/26/24 1:23:35.000 AM)

Job ▾

15 results | 100 per page ▾

signature ⇕	signature_id ⇕
A computer account was deleted	4743
A logon was attempted using explicit credentials	4648
A privileged service was called	4673
A process has exited	4689
A user account was changed	4738
A user account was created	4720
A user account was deleted	4726
A user account was locked out	4740
An account was successfully logged on	4624
An attempt was made to reset an accounts password	4724
Domain Policy was changed	4739
Special privileges assigned to new logon	4672
System security access was granted to an account	4717
System security access was removed from an account	4718
The audit log was cleared	1102



status	count	percent
success	4622	97.019312
failure	142	2.980688

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High level of event Failure	Alert the IT team when the server experiences High levels of event Failure	The server see’s ~1% to ~5% failure rate an hour	We set the threshold at 6% failure rate in an hour

JUSTIFICATION: With a rather careful nature we chose a rather close threshold to the baseline to ensure we saw any anomalous activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High level of successful logins	Alert the IT team when the server experiences High levels of successful logins	The server sees ~16 to ~ 36 events an hour	We set the threshold at 40 successful logins an hour

JUSTIFICATION: With abundant caution we set the threshold at 40 the ensure we did not miss any anomalies in the server.

Alerts—Windows

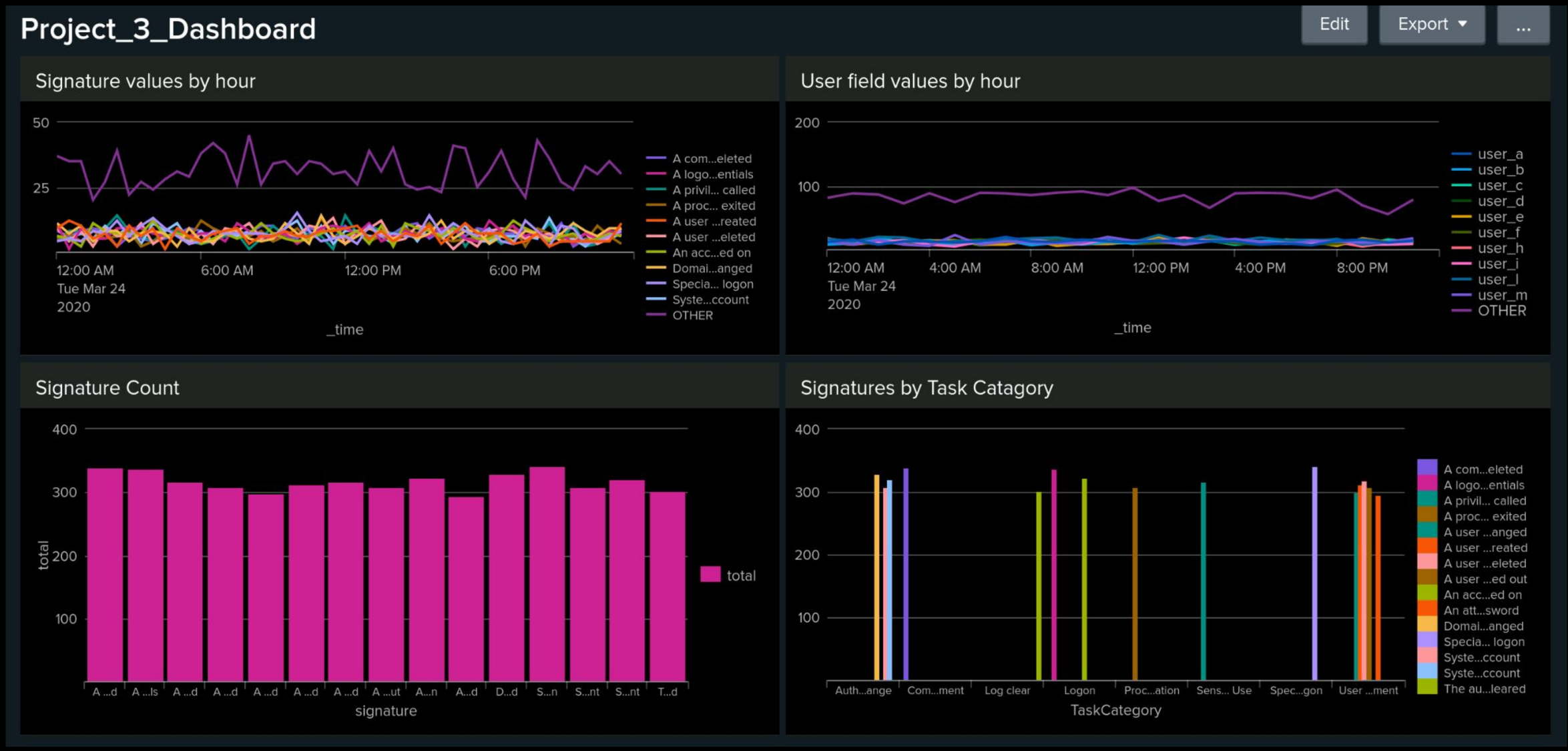
Designed the following alerts:

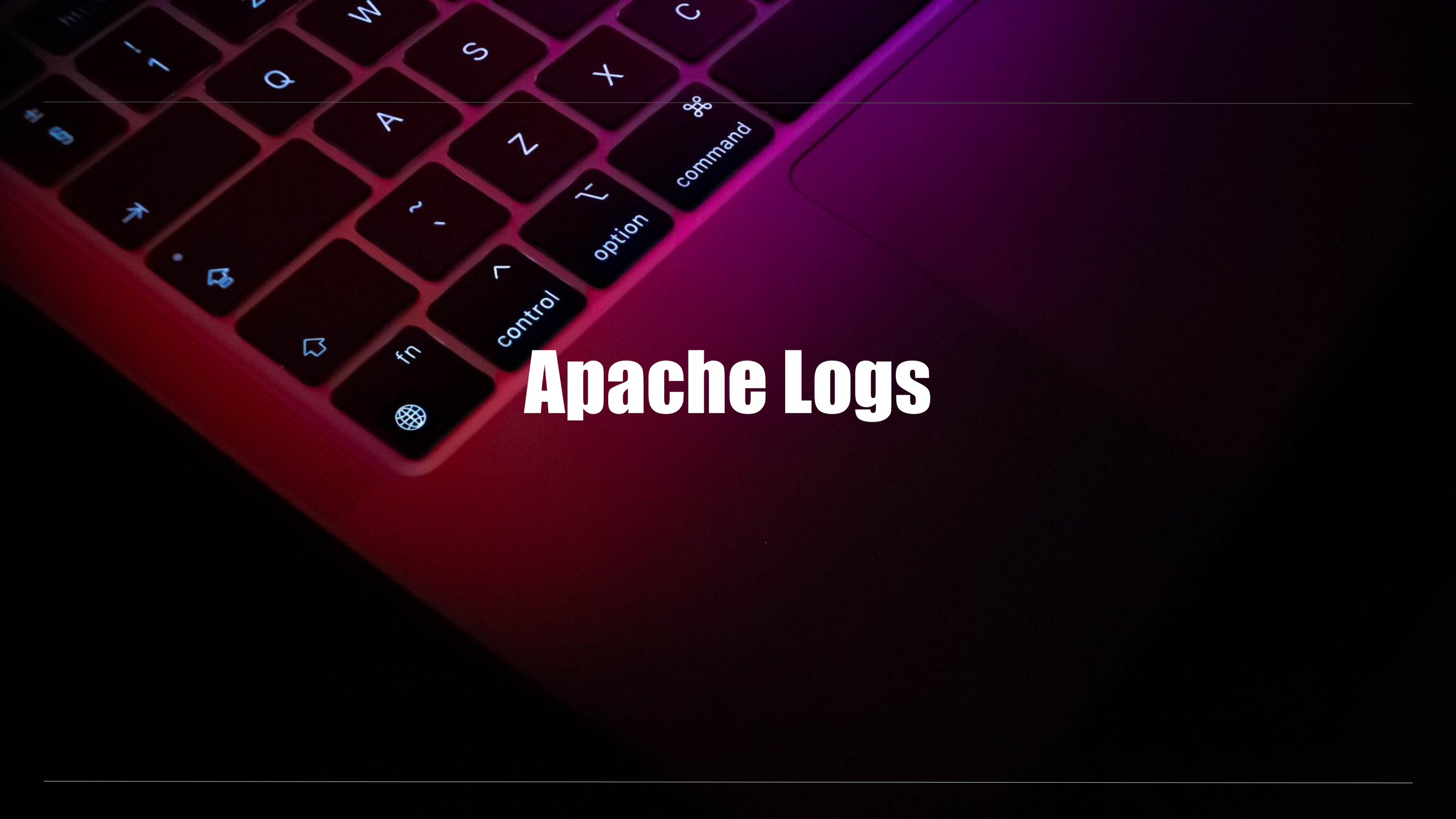
Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Rate Of account deletion	Alert the IT team when the server experiences High levels of account deletion	The server sees a range of ~8 to ~22 events an hour	We set the threshold at 30 events in an hour

JUSTIFICATION: With the number of events fluctuating as much as it does, the threshold needed to have a good level of room above the baseline.

Dashboards—Windows Post-Attack

Dashboards—Windows Pre-Attack





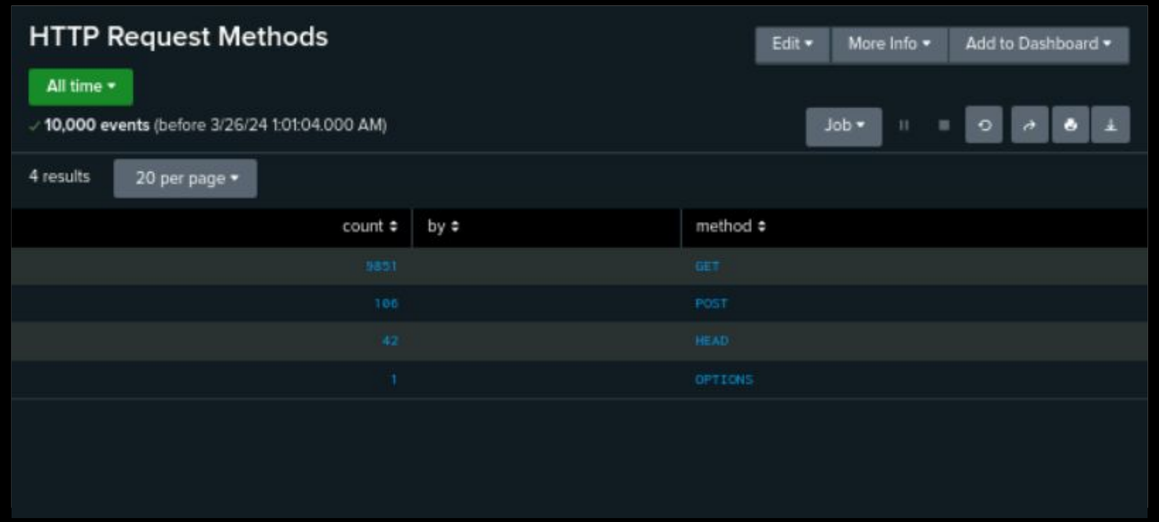
Apache Logs

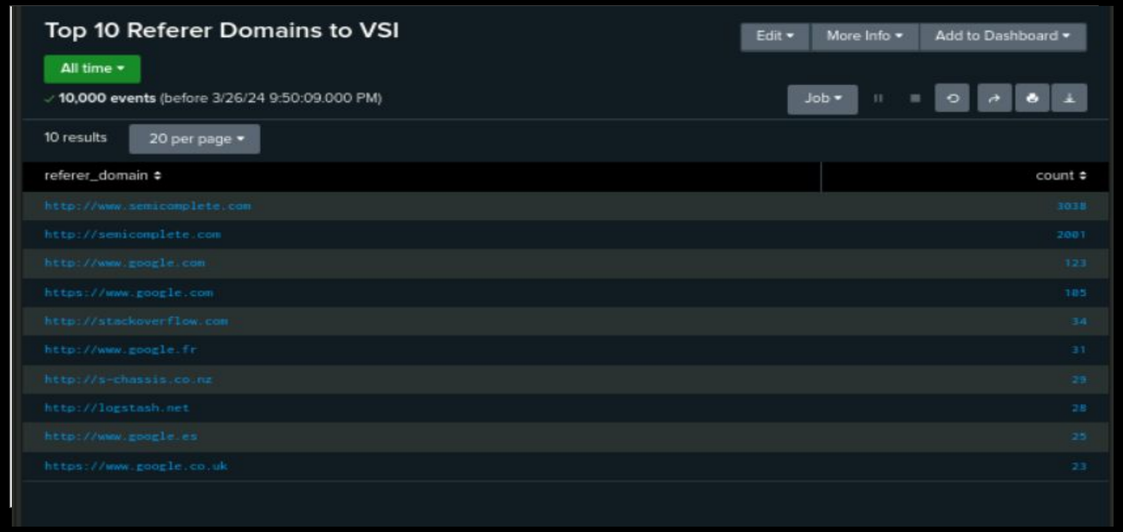
Reports—Apache

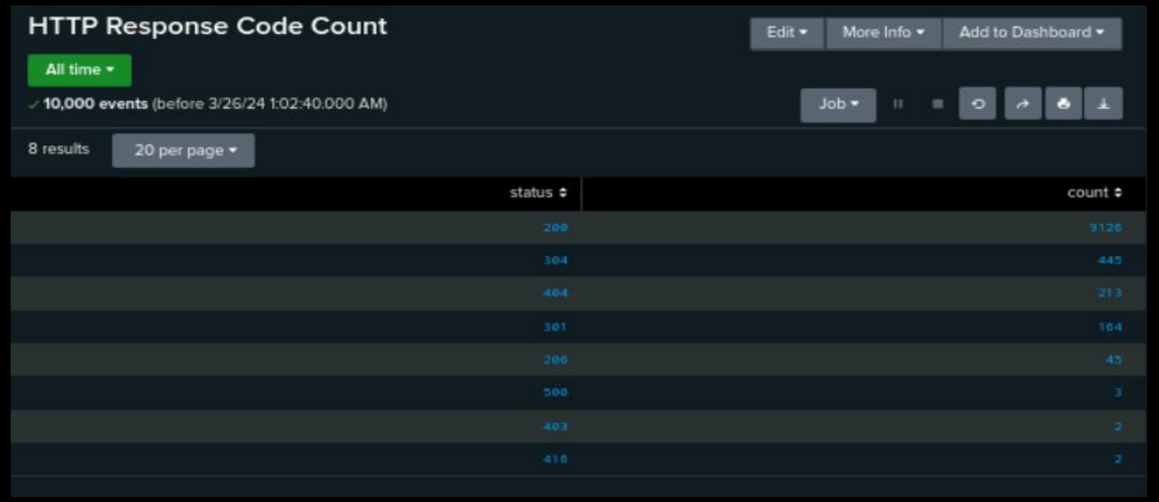
Designed the following reports:

Report Name	Report Description
HTTP Methods Table	Table showing the total amounts for each HTTP method present in the log file
Top 10 Referer Domains	Report showing the top 10 domains that refer to VSI’s website.
HTTP Response Status Codes	Report showing the count of each HTTP response code in the log file.

Images of Reports—Apache







Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
POST Request Monitor	Trigger an alert the number of HTTP POST requests per hour passes the threshold	With normal activity ranging from 1 to it's top number of 7, we set the baseline at 5	10

JUSTIFICATION: With the threat of DDoS attacks on the rise, we needed to monitor HTTP requests to the server. Specifically POST requests. When the POST requests to create or update information to the server passes a certain amount, it must be investigated.

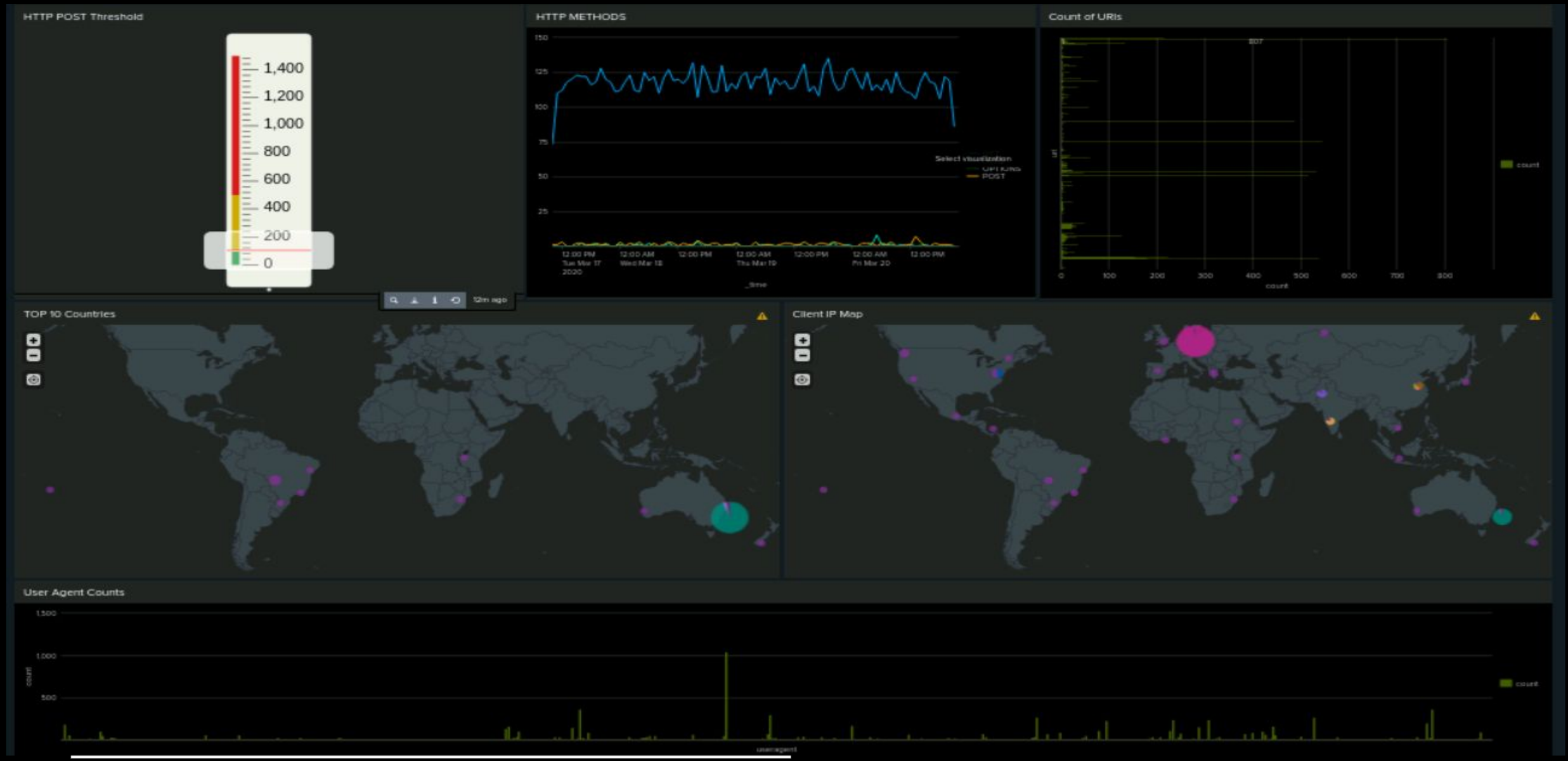
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Foreign Access	Monitor the hourly activity of clientip's outside of the United Stats.	The high end of the total international activity per hour was ~120 per hour so we set the baseline at 100	We set the alert threshold at 200, allowing for slightly more normal activity.

JUSTIFICATION: As an international platform with potential threats coming from all over the world, we needed to monitor countries outside of the US for activity per hour.

Dashboards—Apache




Attack Analysis

Attack Summary—Windows

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

- It appears that there was abnormal activity during the 1 am hour on User_a's account.
- That compromise appears to have lead to further compromise of user_k's account which was used during the 9 and 10 am hours to brute force additional credentials.
- During the 10 and 11 am hours there was a substantial increase in successful activity (all) 2100 (650%) over baseline for the 10 am hour and 1100 (350%) for the 11 am hour.
- During the 11 and 12 am hours there was a substantial increase in successful login100 (650%) over baseline for the 10 am hour and 1100 (350%) for the 11 am hour.

Attack Summary-Windows

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

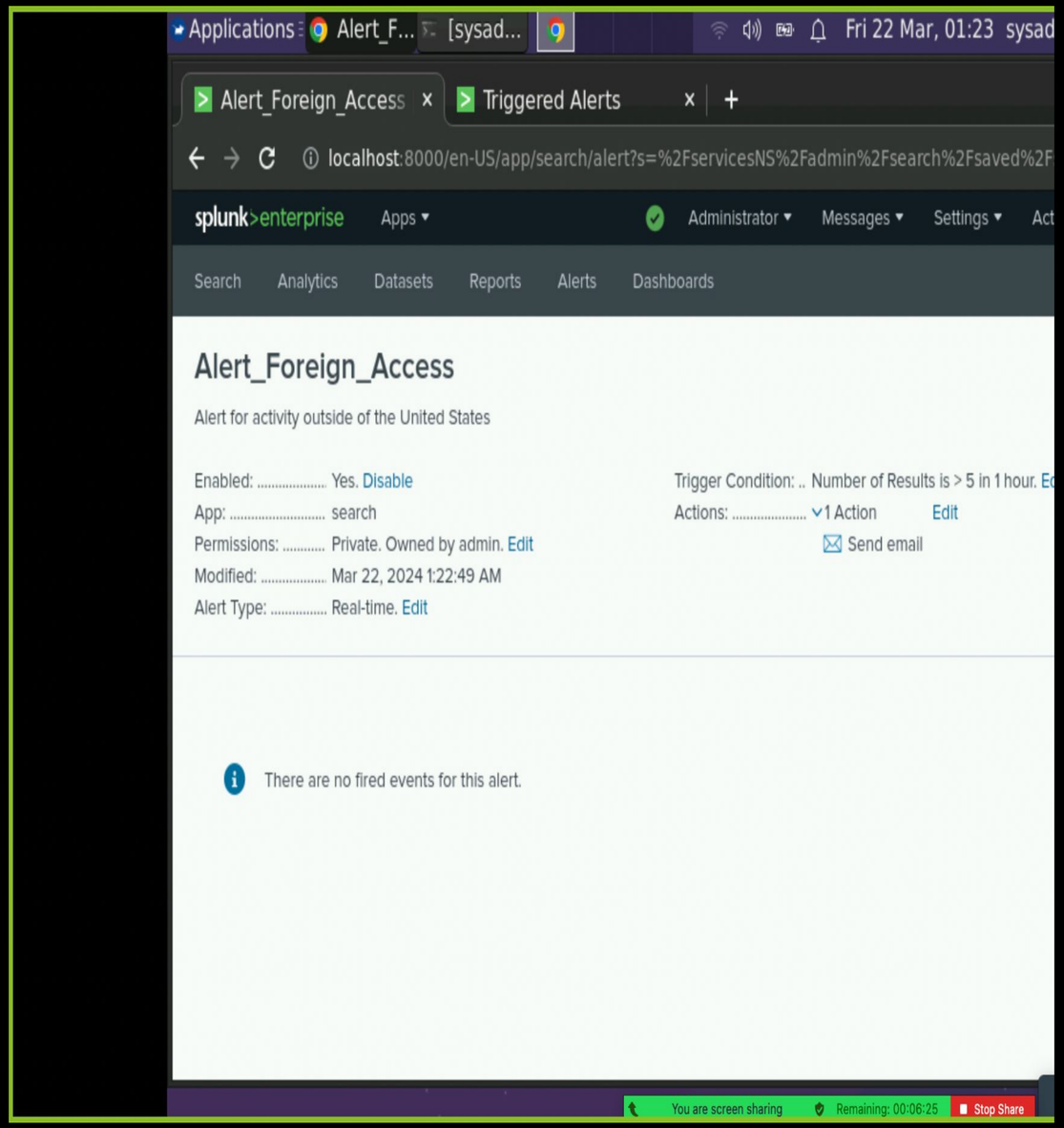
- With the server event failure rate our threshold of 6% proved to be effective, but 17% is far greater of a spike than we were expecting, so our threshold proved to be a little over cautious and could be lowered to help prevent alert fatigue
- The login rate threshold of 40 would have caught the activity, with over 300 and nearly 200, but also it showed high risk of false positive and along with our failure rate I should be loosed to ensure we don't wear our analysts
- Deletion was not triggered but also was not too far from baseline to worry us so this threshold does not seem like it would not need alteration

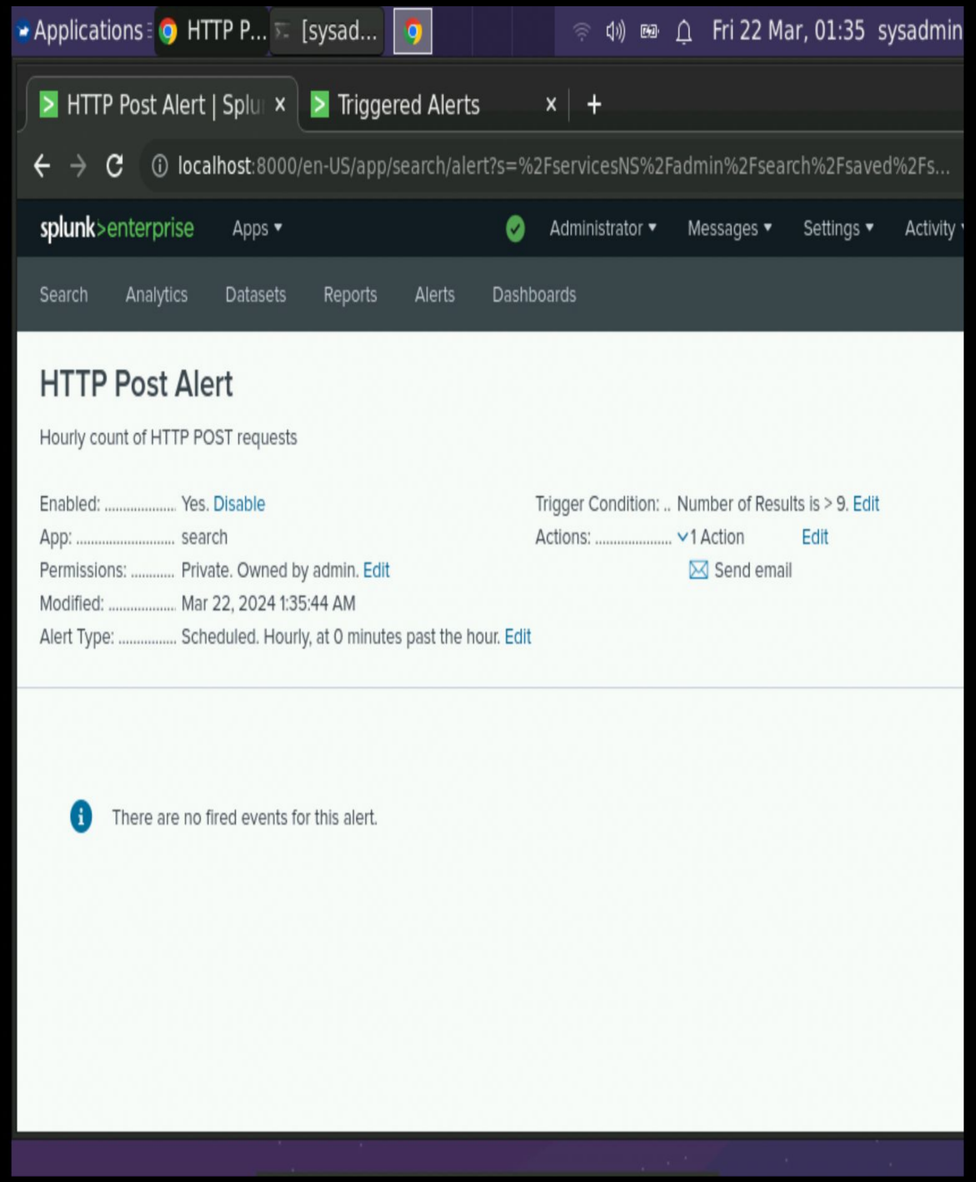
Attack Summary—Windows

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

- Our Signature values by hour chart gives a quick and easy visualization of when and what was happening during moments of the the attacks, this gave us quick insights on where to look for the effects of the attack
- The user field values by hour alerted us as to what users and let us see previously unnoticed potentially compromised user as well
- With the Signature count charts insight into what type of events were taking assisted with our identifying the anomalous activity and the volume there of it
- Signature by task Showed us insights of how the attack affected the environment and how the attackers engaged with multiple systems during the time of their activity

Screenshots of Alerts





Attack Summary—Apache

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

- HTTP POST request activity jumped from the established normal level of 106 to 1296 at the peak of the attack
- Other HTTP methods were decreased, for example, GET went from a normal 9851 to 3157. All others were also reduced.
- The main domain activity came from semicomplete.com, however, we didn’t deem anything as suspicious
- Suspicious changes in HTTP response codes
  - The requested resource moved permanently to a new location

Attack Summary—Apache

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

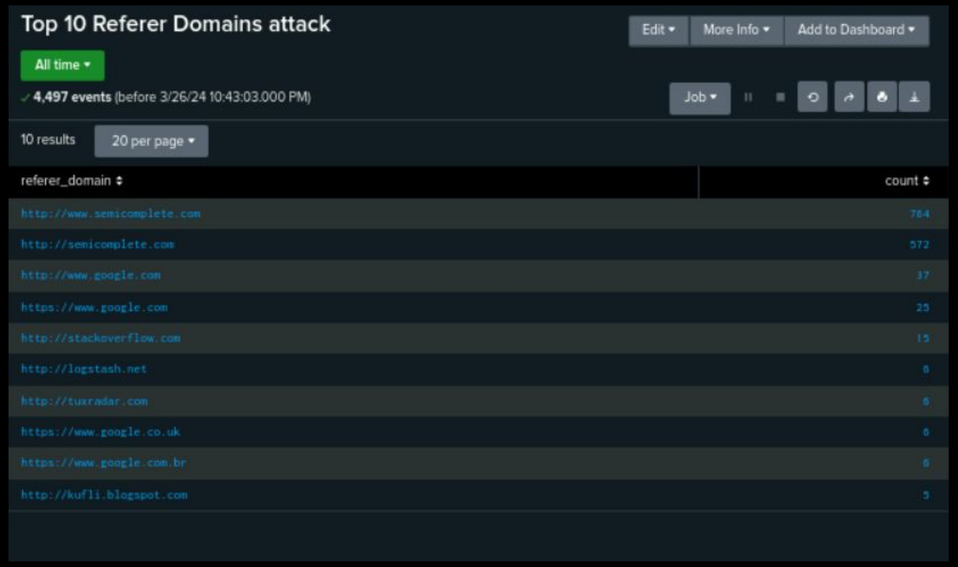
- Suspicious volume of international activity was detected:
  - Ukraine went from 89 (normal) to 877 at 8pm on March 25, 2020
- After reviewing, we determined we would lower the threshold
- Suspicious volume of HTTP POST activity:
  - Jumped from 106 (normal) to 1324
  - Occurred for 1 hour
- These events occurred on March 25, 2020 at 8pm
- It was determined we needed to lower the threshold

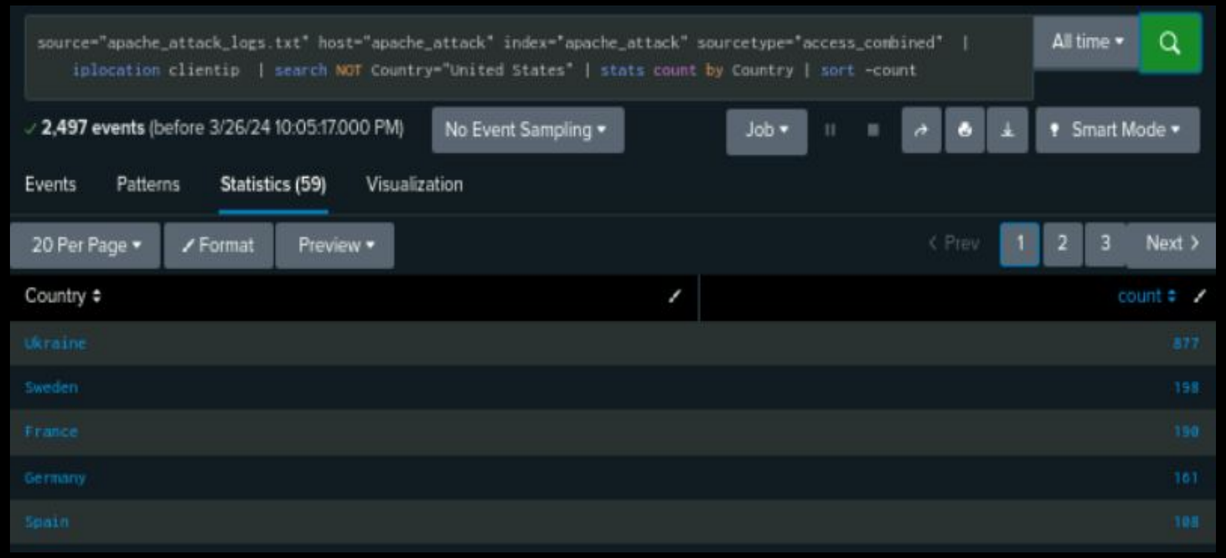
Attack Summary—Apache

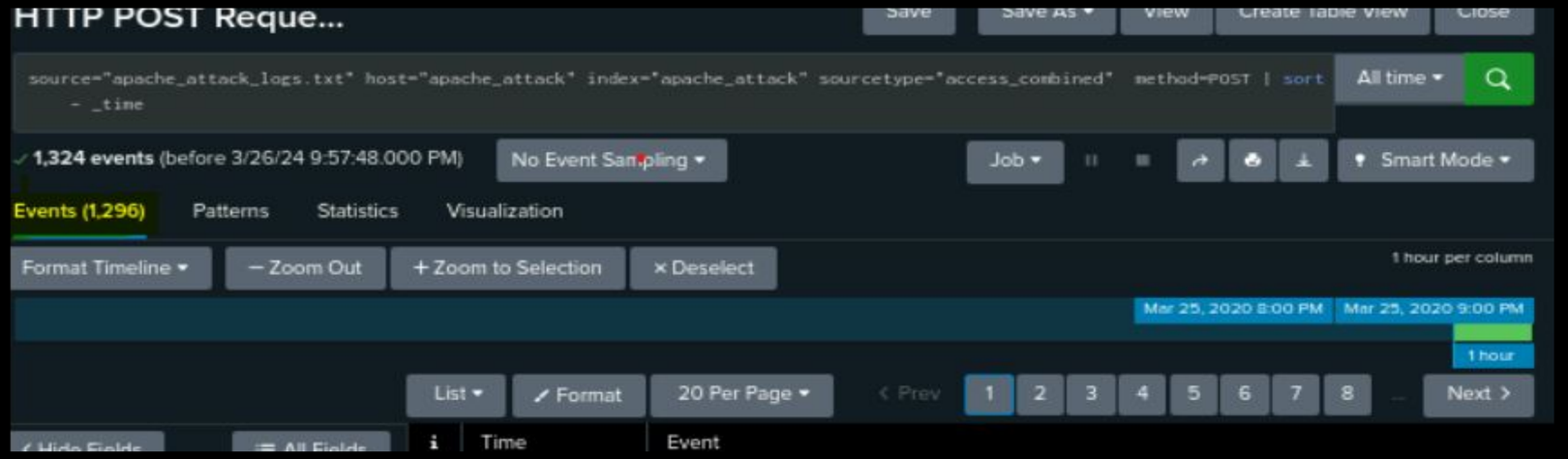
Summarize your findings from your dashboards when analyzing the attack logs.

- Increase in POST Requests
- POST:
  - Attack started at 7pm and stopped at 9pm
- Peak count of the top method (POST) was 1296
- Suspicious activity from Kyiv, Ukraine was detected

Screenshots of Attack Logs







Summary and Future Mitigations

Project 3 Summary

Overall findings from the attack on March 25, 2020:

- **The windows back end server was compromised**
  - **1 AM-2 AM user_a's credentials were used to enumerate the system.**
  - **9 AM-10 AM- user k was used to escalate privileges and create persistence.**
- **Apache at approximately 8 PM, suffered from an HTTP POST Flood DDoS attack on the web application, based on location there would be increased suspicion on Ukraine.**
  - Apache - there was an HTTP POST Flood DDoS attack on the web application
    - location data suggests that it came from Ukraine

Our Recommendations

- Implement real time monitoring of the system logs from the SOC.
- Use or strengthen a network and Web Server Firewall
- Block traffic from countries that are known for originating cyber crime.
- We would rank the over all cybersecurity program Tier 1- Partial maturity. We strongly recommend working toward formalizing the cybersecurity program by implementing a Framework such as NIST.