Virtual Space Industries vs. JobeCorp

A Defensive Security Project

By Lucas Hartford

Table of Contents

This document contains evaluations of the following:

Monitoring Environment

Scenario

- Our team is a group of SOC Analysts working for Virtual Space Industries (VSI)
- We have been informed that threat actors may be targeting our corporation with cyber attacks
- We have decided to step up our security monitoring practices by utilizing Splunk to gain visibility into our organizations network traffic
- We are monitoring both a Windows Server and an Apache based Web Server
- We've also installed a Splunk-supported add on to aid the SOC in it's security monitoring practices

Add On Application:
Splunk Security Essentials

Splunk Security Essentials

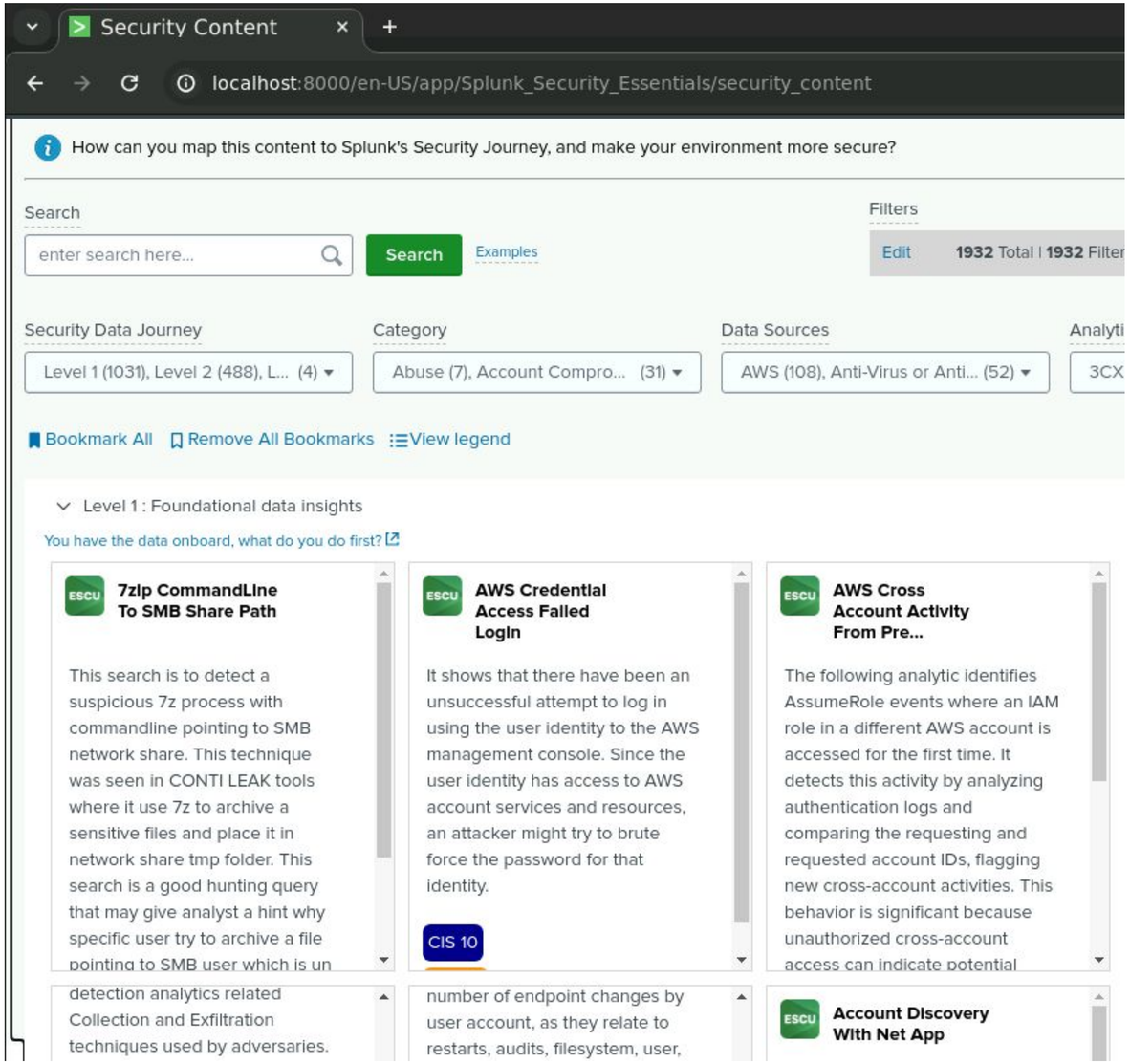
Splunk Security Essentials (SSE) is a free application supported by Splunk. This app contains tools that provide deep insight into an organization's data, and rich documentation on these tools and the SPL queries they are built on. The app contains monitoring solutions designed to detect current known threats and facilitate common cyber-hygiene practices. The security content in SSE is built on the MITRE ATT&CK framework and the Cyber Kill Chain, and it is designed to make robust security monitoring more accessible to smaller organizations and junior cybersecurity professionals.

Splunk Security Essentials

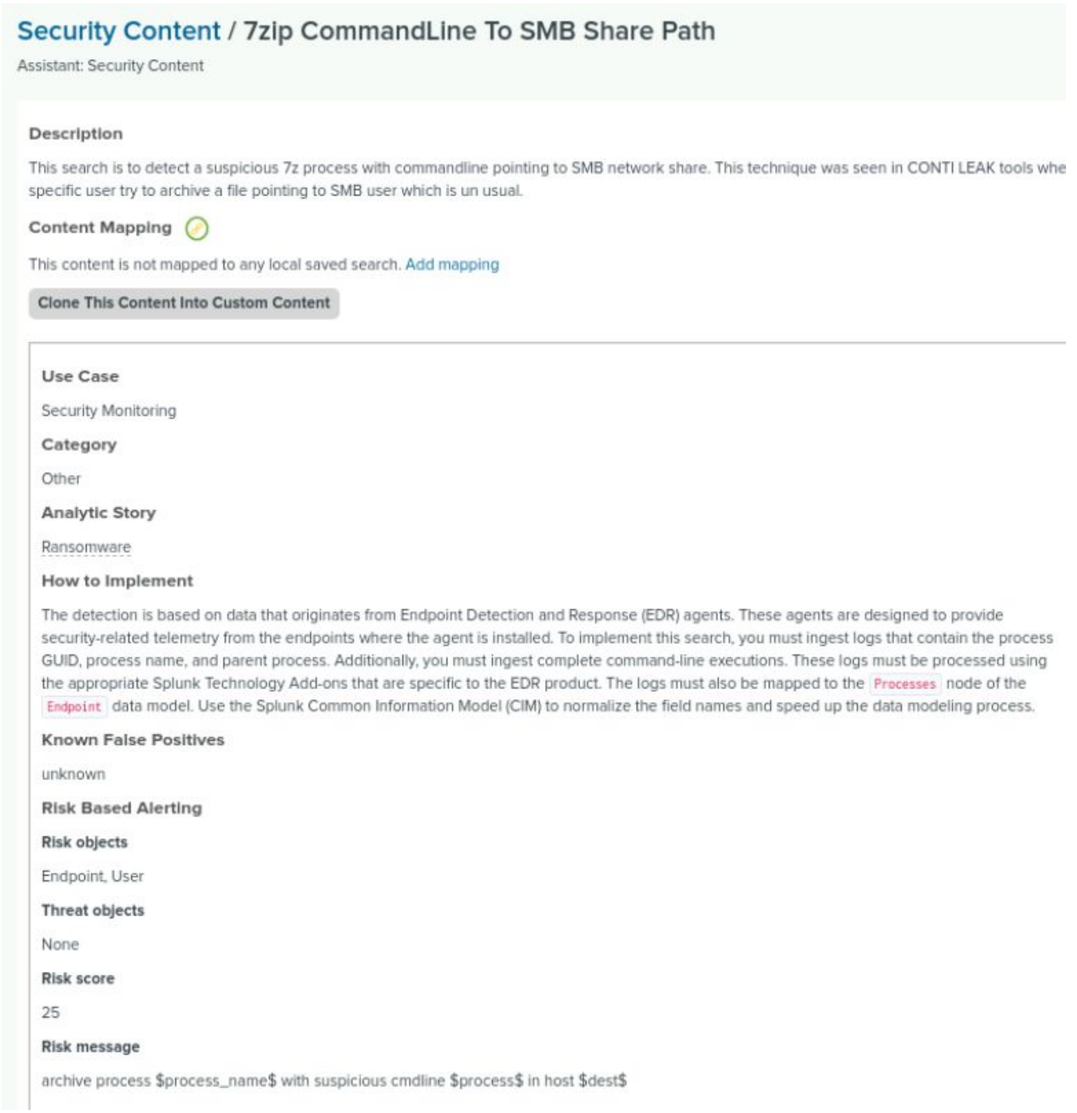
In our Project 3 scenario, we were informed of an imminent threat and we were tasked with quickly setting up a security monitoring environment. The pre-built tools in SSE would allow us to deploy multiple monitoring solutions quickly and allow us to fortify our monitoring capabilities much sooner than if we had to build it by hand. Additionally, because SSE is built on the MITRE ATT&CK framework, it provides a small security team an enhanced ability to monitor their network for threats without adding costs in manpower.

Splunk Security Essentials

Pre-built security monitoring tools



Documentation on the security tools



Logs Analyzed

1 Windows Logs

The Windows Logs contain log data from the organization's Windows Server. They contain information such as timestamps for a given event, windows events and event codes, the user, the account domain, the computer name and other event details within the server. These details can be scoured by a SIEM such as Splunk to detect malicious activity.

2 Apache Logs

The Apache Server acts as a web server, and therefore it logs information about network traffic. The logs contain details such as the client IP address, the request method (GET, POST, HEAD), the size of the packet, the status of the request, the user agent and other relevant information regarding the network traffic.

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signature Table	Table depicting the signatures and their corresponding signature ID’s
Severity Levels	Table exhibiting the severity levels of various events
Success/Failure Rate	Table showing relative rates of successful and failed requests

Images of Reports—Windows Baseline

Signature Table

_time	signature_id	signature
2020-03-24 23:59:54	4726	A user account was deleted
2020-03-24 23:59:53	4720	A user account was created
2020-03-24 23:59:31	4743	A computer account was deleted
2020-03-24 23:57:54	4624	An account was successfully logged on
2020-03-24 23:57:51	4672	Special privileges assigned to new logon
2020-03-24 23:56:41	4724	An attempt was made to reset an accounts password
2020-03-24 23:56:40	4717	System security access was granted to an account
2020-03-24 23:54:46	4673	A privileged service was called
2020-03-24 23:54:42	4648	A logon was attempted using explicit credentials
2020-03-24 23:54:39	4740	A user account was locked out
2020-03-24 23:54:25	4739	Domain Policy was changed
2020-03-24 23:50:07	4738	A user account was changed
2020-03-24 23:48:36	4689	A process has exited
2020-03-24 23:46:27	1102	The audit log was cleared
2020-03-24 23:45:36	4718	System security access was removed from an account

Severity Level

Success/Fail Rates

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Activity	An alert that triggers after a given number of failed activities	Baseline activity was typically between 5-10 failures per hour	12 failures per hour

JUSTIFICATION: We set the alert for 20% higher than baseline so that normal fluctuations do not trigger an alert, but large changes in failures can be investigated by the SOC team.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins	An alert set to trigger when the count of successful logins is exceptionally high	Baseline activity was typically between 12-20 successful logins per hour	25 successful logins per hour

JUSTIFICATION: The threshold is set to 25% above the baseline so that the SOC Team receives an alert when successful logins spike. This could tip us off to an attack involving stolen login credentials.

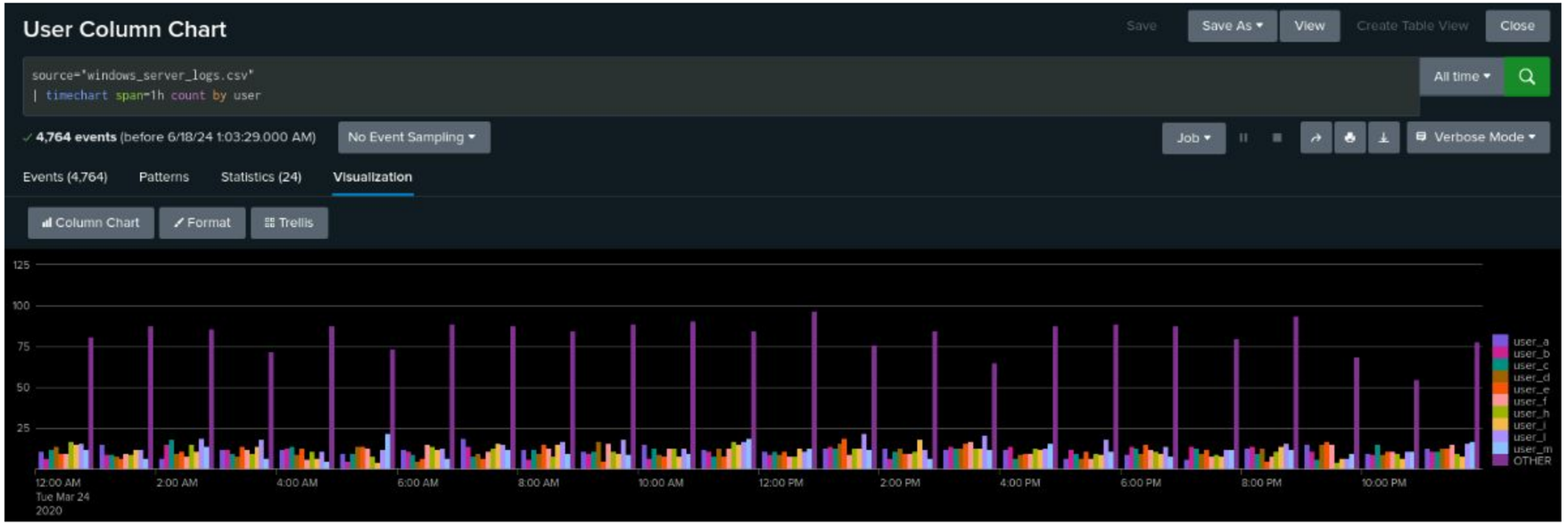
Alerts—Windows

Designed the following alerts:

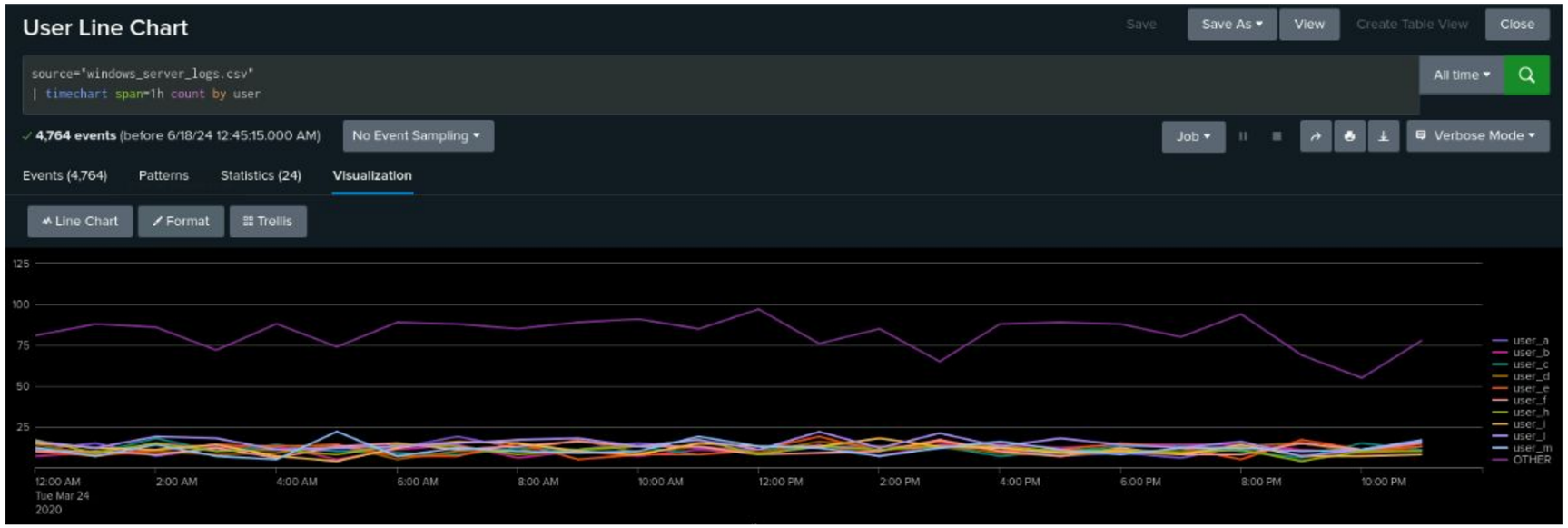
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account Deleted	An alert will trigger when the number of user account deletions drastically exceeds baseline	The baseline activity for deleted accounts is between 12-20 events per hour	The alert will trigger at 25 deletions per hour

JUSTIFICATION: We stuck with 25% above baseline for this alert as well. If the number of deleted accounts increases drastically, we'll want to know as early as possible in order to investigate whether these deletions are legitimate.

Dashboards—Windows Baseline Charts



Dashboards—Windows Server Baseline Charts



Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Table showing the count of requests by HTTP method (GET, POST, HEAD)
Top Domain Referrers	Table showing the top 10 domain referrers
HTTP Response Codes	Table showing the count of HTTP response codes

Images of Reports—Apache Baseline

HTTP Method Table

Apache_methods_table_day2

Edit ▾ | More Info ▾ | Add to Dashboard ▾

All time ▾

✓ **10,000 events** (before 6/20/24 9:59:57.000 PM)

Job ▾

84 results | 20 per page ▾ | < Prev | 1 | 2 | 3 | 4 | 5 | Next >

_time	GET	HEAD	OPTIONS	POST
2020-03-17 10:00	73	0	0	1
2020-03-17 11:00	110	0	0	1
2020-03-17 12:00	112	0	0	3
2020-03-17 13:00	118	0	0	0
2020-03-17 14:00	120	0	0	0
2020-03-17 15:00	123	0	0	2
2020-03-17 16:00	122	2	0	2
2020-03-17 17:00	122	0	0	1
2020-03-17 18:00	116	1	0	1

Status code counts

Top status

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

```
source="apache_logs.txt"
| top status
```

All time ▾

✓ **10,000 events** (before 6/22/24 11:07:25.000 PM) | No Event Sampling ▾ | Job ▾ | Verbose Mode ▾

Events (10,000) | Patterns | **Statistics (8)** | Visualization

100 Per Page ▾ | Format | Preview ▾

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

Top 10 Referrer Domains

Top referer_domains

Edit ▾ | More Info ▾ | Add to Dashboard ▾

All time ▾

✓ **10,000 events** (before 6/20/24 10:11:27.000 PM)

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

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
International Network Traffic	An alert that triggers when traffic from foreign IP addresses spikes	Baseline volume of traffic from outside the US is typically between 80-120 requests per hour	At 140 alerts per hour

JUSTIFICATION: This alert is set for roughly 20% above baseline and is intended to provide notice of high international traffic volume. This alert will prompt the SOC team to investigate whether this traffic poses a threat to our system.

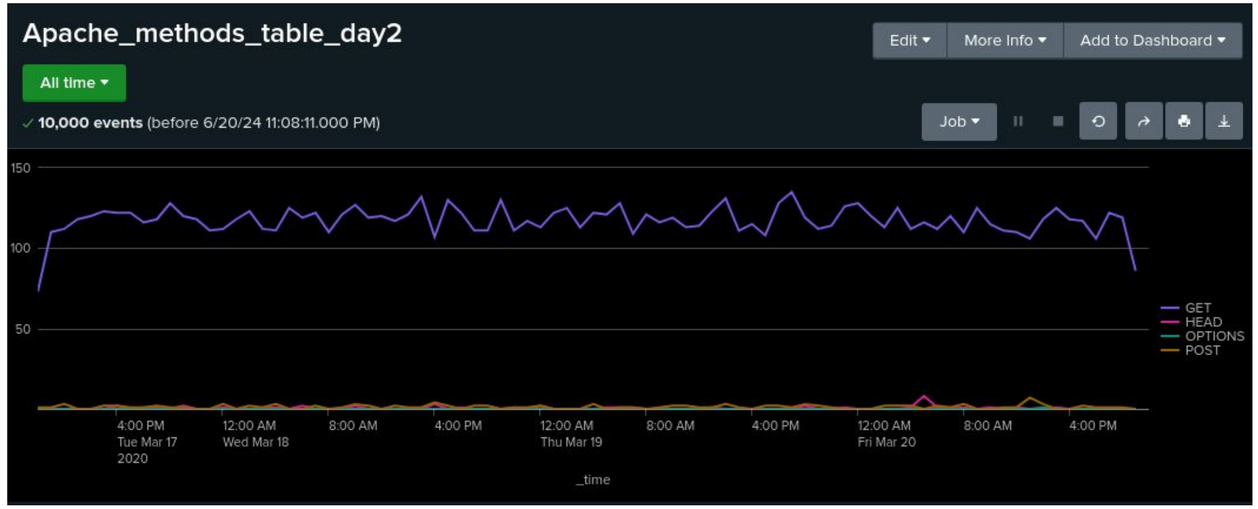
Alerts—Apache

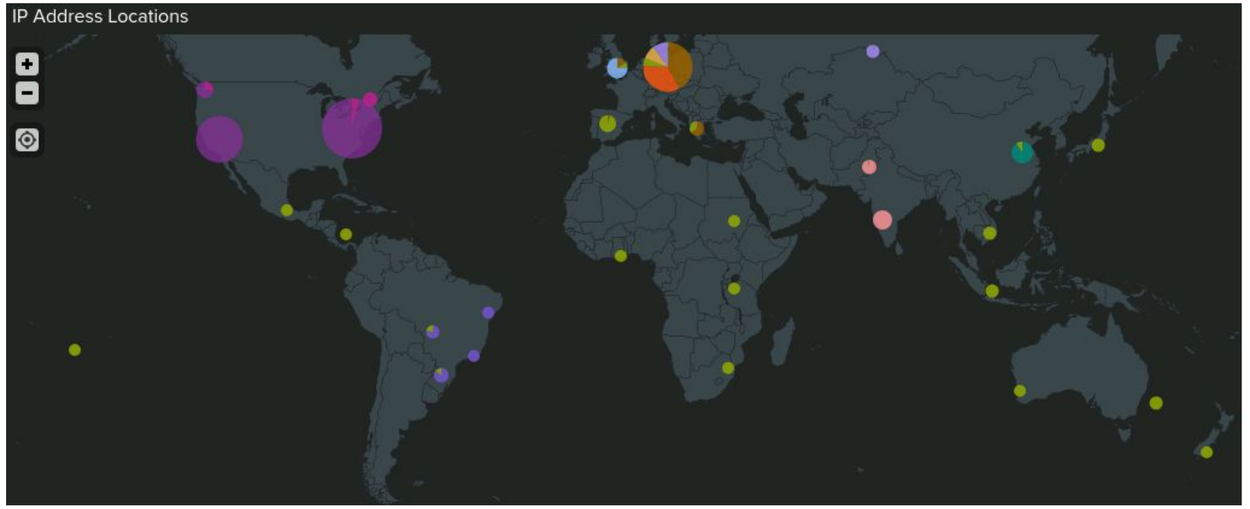
Designed the following alerts:

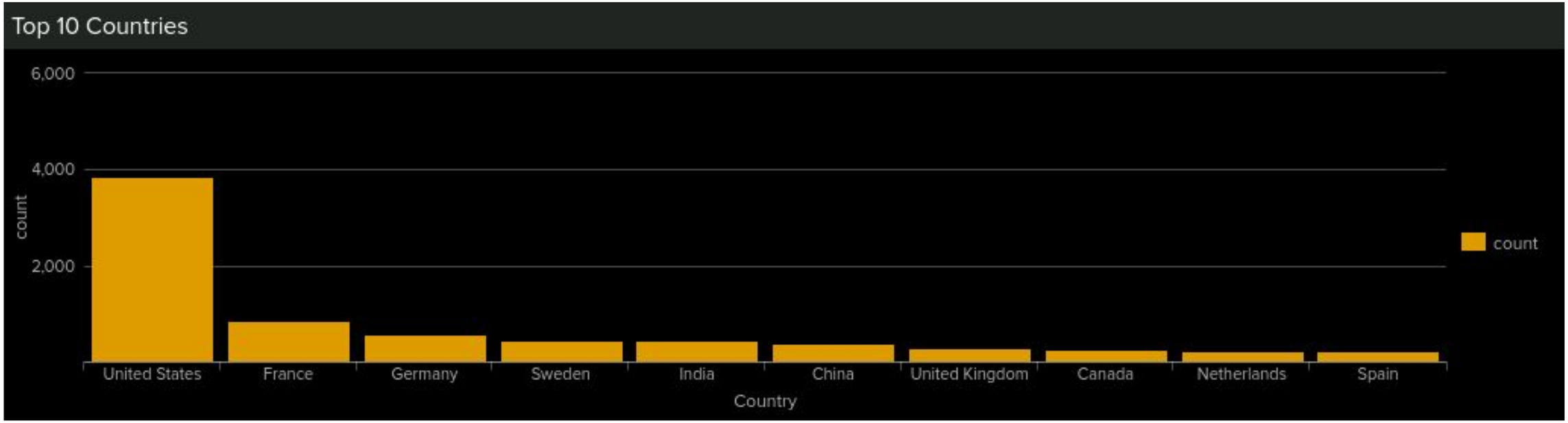
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST	Monitors the number of HTTP POST requests per hour	Baseline POST request was volatile, but typically between 3-7	10 HTTP POST requests per hour

JUSTIFICATION: The threshold for this alert was 10 POST's per hour and baseline traffic peaked at 7 events per hour. This alert would aid the SOC team in identifying potential attacks by providing immediate notice of the deviation.

Dashboards—Apache Baseline

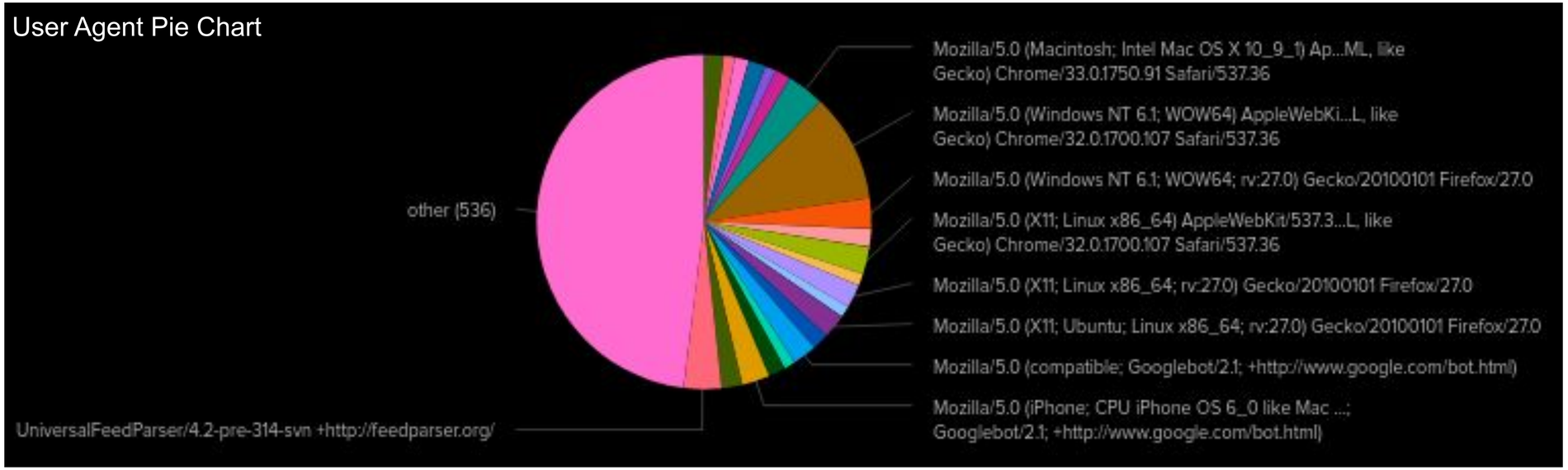




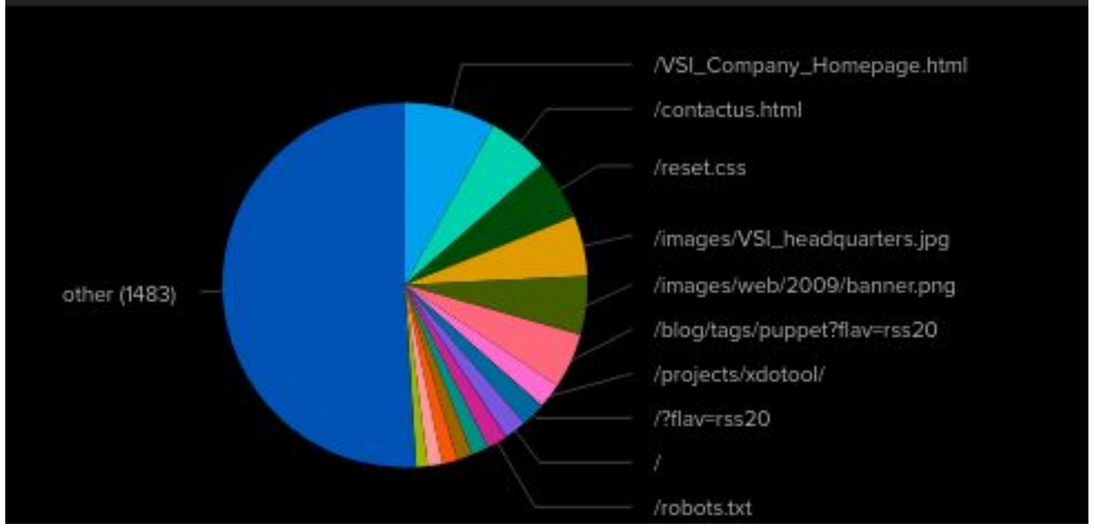


Dashboards—Apache Baseline

User Agent Pie Chart



URL Path Pie Chart



Number of 404 errors

Attack Analysis

Attack Report Summary—Windows

- The percentage of High severity alerts jumped from 6.9% to 20.2% on the day of the attack. When viewed by the hour, we see two noticeable bumps in activity beginning at 1:00 AM and at 9:00 AM.

- Analyzing the report for failed activities by hour, we saw a large peak in failure counts between 8:00-9:00 AM.

Attack Alert Summary—Windows

- An alert for failed activity triggered between 8:00-9:00 AM. The alert threshold was set to 12 failures per hour, and that time span saw 35 failures.
  - A drill down into the source of these failure messages revealed that attempts were made to create new accounts and to reset the passwords of multiple users.
- An alert for successful logon’s triggered shortly after 11:00 AM with a surge in activity of 196 events per hour. The alert threshold was set to 25 events per hour.

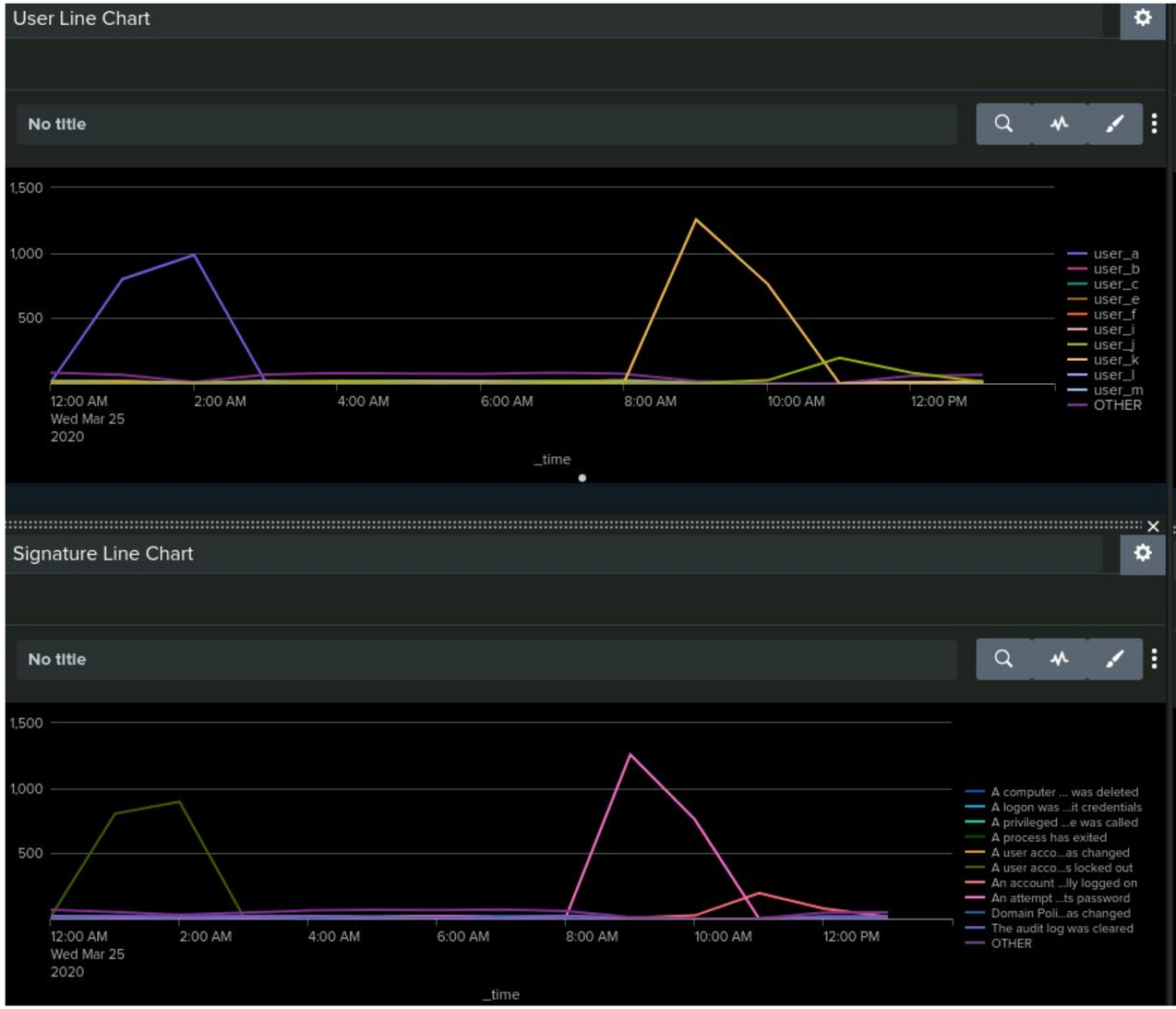
Attack Dashboard Summary—Windows

- The line chart and the column chart for the ‘user’ field show that *user_a* was responsible for a peak in activity between 1:00-3:00 AM and *user_k* was responsible for another peak between 9:00-11:00 AM.

- Both charts for the ‘signature’ field show that to 3 peak consisted mostly of “*a user account was locked out*” signatures, indicating a likely password attack. The 9 to 11 peak was made up of “*an attempt was made to reset an accounts password*” signatures.

Screenshots of Windows Attack Logs vs Baseline Logs

ATTACK LOGS



BASELINE LOGS

Attack Report Summary—Apache

- Our table of HTTP method counts revealed that 1296 POST’s were made at 8:00 PM. Typical POST traffic was less than 7 per hour.

- The report for 404 errors indicated that those increased from 2.1% in the baseline to over 15% of total requests on the day of the attack. The bulk of these error codes are grouped into two peaks, one at 6:00 PM and one at 8:00 PM.

Attack Alert Summary—Apache

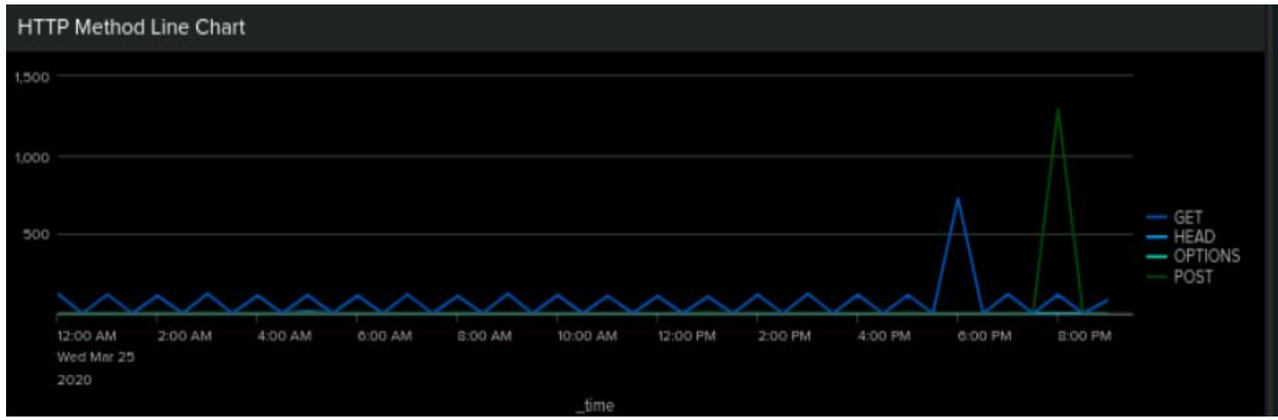
- The alert for traffic from international IP address’ triggered shortly after 8:00 PM, and we ultimately received 937 requests from outside the US between 8:00 and 9:00. The alert threshold was set at 140 packets per hour.

- The alert for HTTP POST requests triggered around the same time, with 1296 requests in an hour. The alert threshold was set to 10 requests per hour.

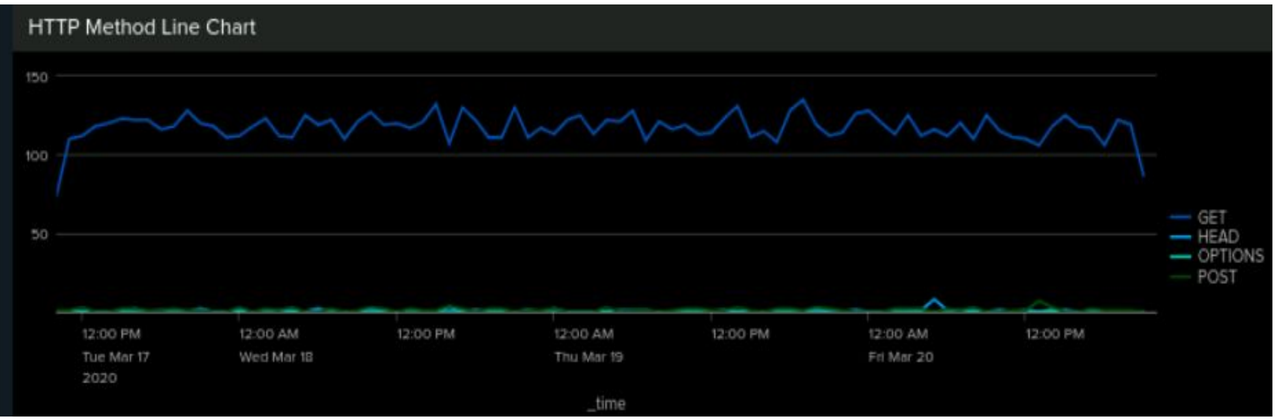
Attack Summary—Apache

- After noticing the spike in HTTP POST’s, we charted the method data and noticed a peak in POST’s around 8:00 PM and a peak in GET’s at 6:00 PM.
  - The 6 o’clock peak in GET requests correlates with a bump in traffic from the US.
  - The peak in POST requests between 8:00 and 9:00 correlates with a surge of HTTP traffic from Ukrainian IP addresses

ATTACK LOGS



BASELINE LOGS



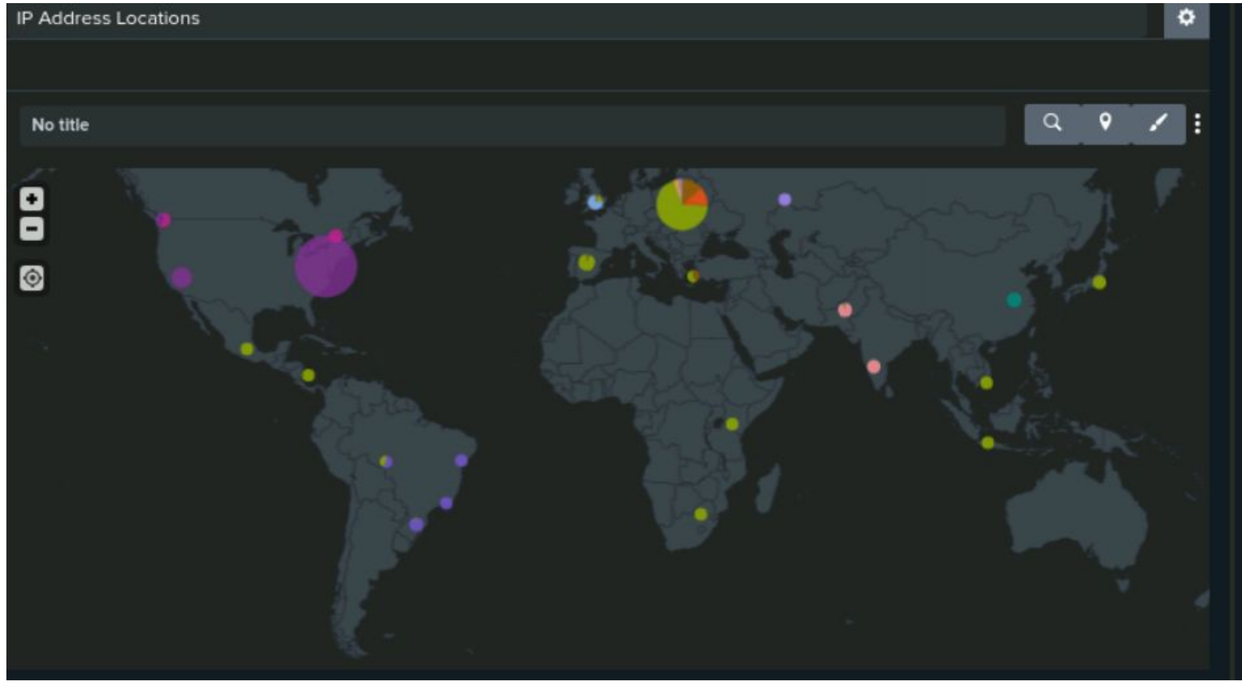
Attack Summary—Apache

- An analysis of the IP address country of origin in the 8 to 9 o’clock window revealed most of the traffic was coming from Ukraine, specifically from Kyiv and Kharkiv which are the two largest cities in Ukraine.

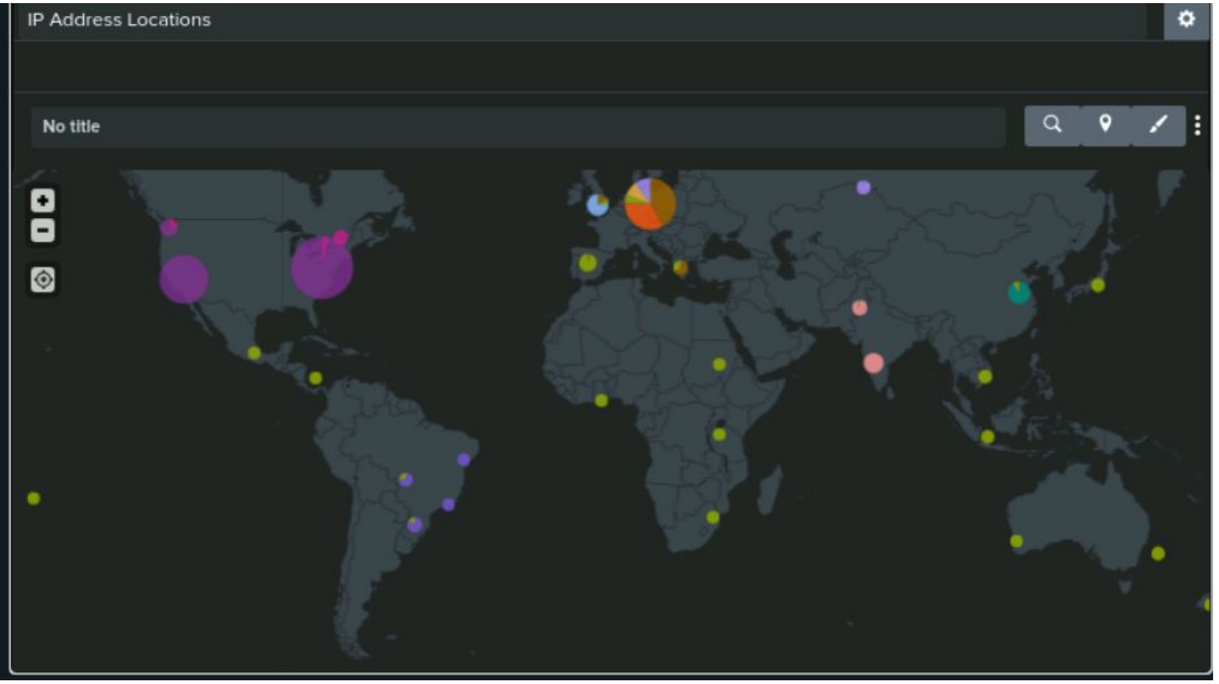
- The 6:00 PM peak in GET requests correlates with a bump in traffic from the US.

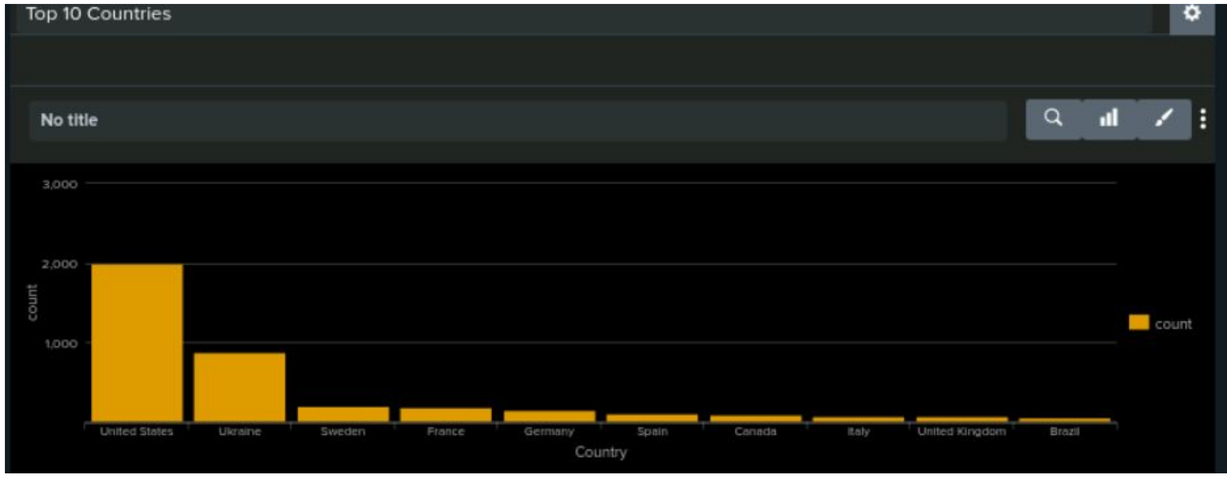
Screenshots of Attack IP Geodata Dashboards

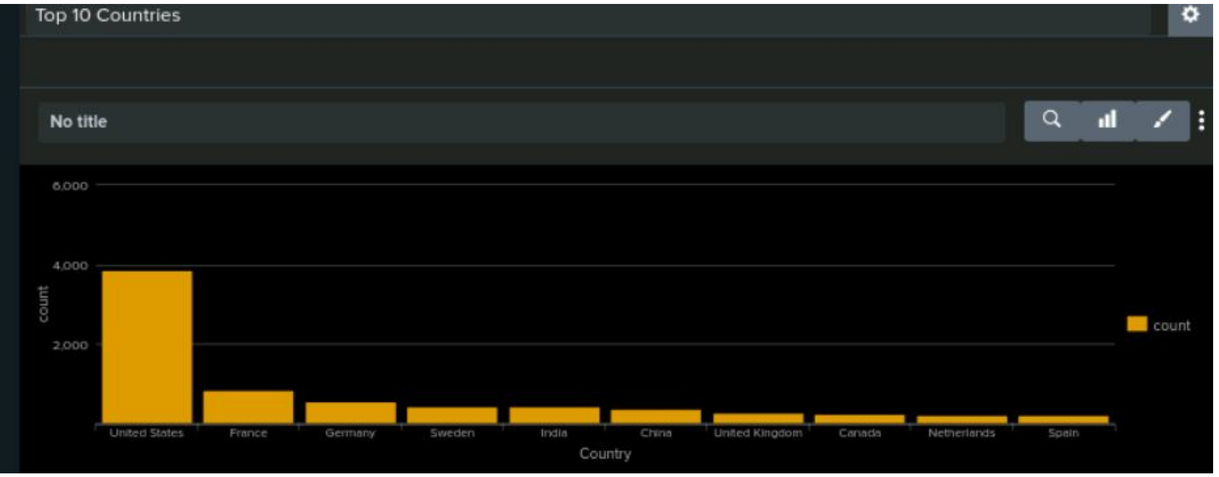
ATTACK MAP



BASELINE MAP



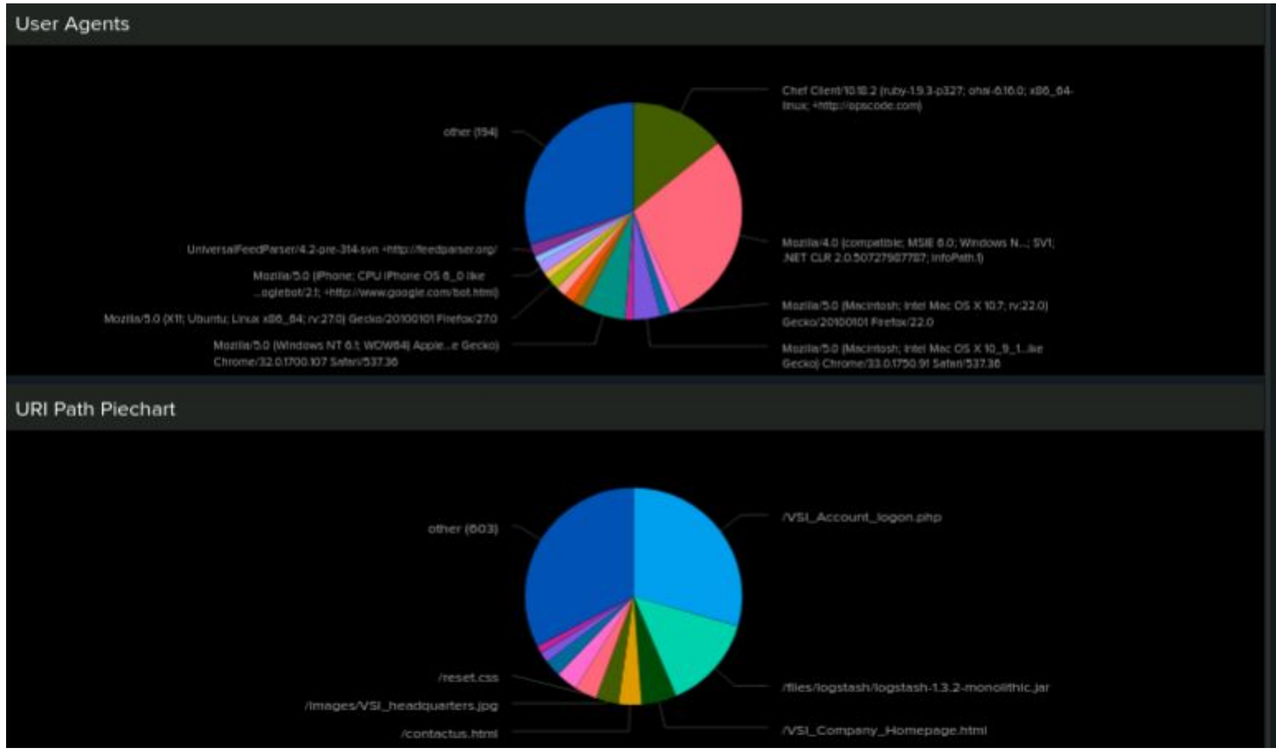




Screenshots of Attack Dashboards

- We noticed a sharp increase in Mozilla 4.0 user agents, this is an older Mozilla version.
- The most common URI path on attack day was to /VSI_Account_logon.php indicating that the attackers were targeting the employee login portal.

ATTACK LOGS



BASELINE LOGS

Summary and Future Mitigations

Project 3 Summary - Windows Server

- Our investigation has ended and we've determined that on Wednesday March 25, 2020 VSI was targeted in a cyber attack that affected a Windows Server and an Apache web server.
  - The Windows Server was compromised around 1:00 AM and an immediate surge in account lockouts indicates a password attack. The account for user_a was very active in this time frame.
  - Between 8:00-9:00 AM, a surge in attempts to reset account passwords indicates that attackers may have been trying to establish persistence by changing the passwords to stolen accounts.
- We recommend that VSI begin using Multi-Factor Authentication. MFA would prevent the compromised user credentials from escalating into unauthorized account access.
- Additionally, we recommend an Intrusion Prevention System (IPS) to prevent a single user from attempting additional logins after a number of failed attempts.

Project 3 Summary - Apache Server

- Our investigation has ended and we've determined that on Wednesday March 25, 2020 VSI was targeted in a cyber attack that affected a Windows Server and an Apache web server.
    - The Apache server was targeted around 6:00 PM at which time a large number of GET requests were sent. At 8:00 PM a more pronounced surge in POST requests were made. The 8 o'clock surge correlates with a bump in traffic to /VSI_Account_Logon.php.
    - We believe that the credentials stolen from the Windows Server attack were used to log on to the VSI web portal at 8:00 PM. Most of the POST traffic originated in Ukraine from a Mozilla 4.0 user agent.
- We again recommend an IPS with custom rules to block traffic from a given geographic region if traffic from that area surges beyond a set threshold. This would buy the SOC team time to implement a permanent solution.
- An 'allow list' should also be utilized in order to prevent outdated user agents or unfamiliar IP address from accessing sensitive pages, such as a login portal.