Defensive Security Project
by: Jaron Khoury

Table of Contents

This document contains the following resources:

Monitoring Environment

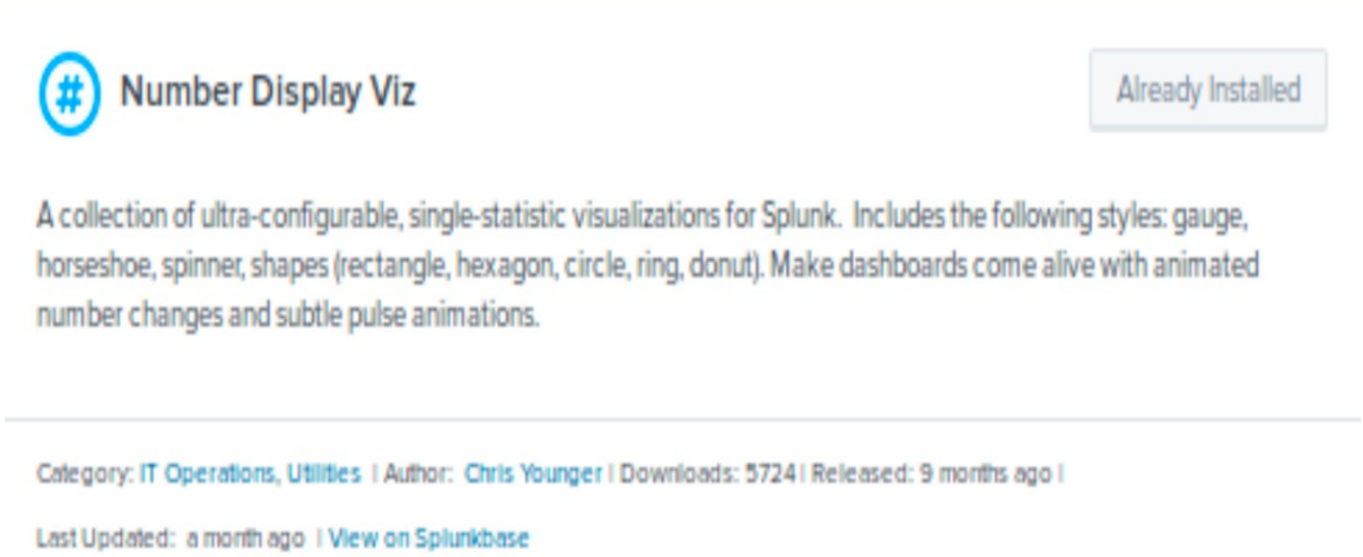
Scenario

- Virtual Space Industries (VSI) received credible information pertaining to the possibility of a cyberattack by a competitor, JobeCorp, that disrupted business operations in March 2020
- Security Operations Center (SOC) analysts were tasked with monitoring the administrative webpage and Windows and Apache Server Logs for signs of an attack
- The networking team provided past logs to help baseline the environment prior to the suspected attack and create reports, alerts and dashboards using

Number Display Viz

Number Display Viz

- **Add on app to the Splunk environment**
- **Includes an array of style choices and configurations that add to data visualization**
- **Subtle animations bring to life the Splunk dashboard and user experience**



Number Display Viz

- **The benefit of this tool would be for quick and easy analysis of log security events**
- **The use of color coded radial gauges when monitoring client IP addresses would be particularly useful**

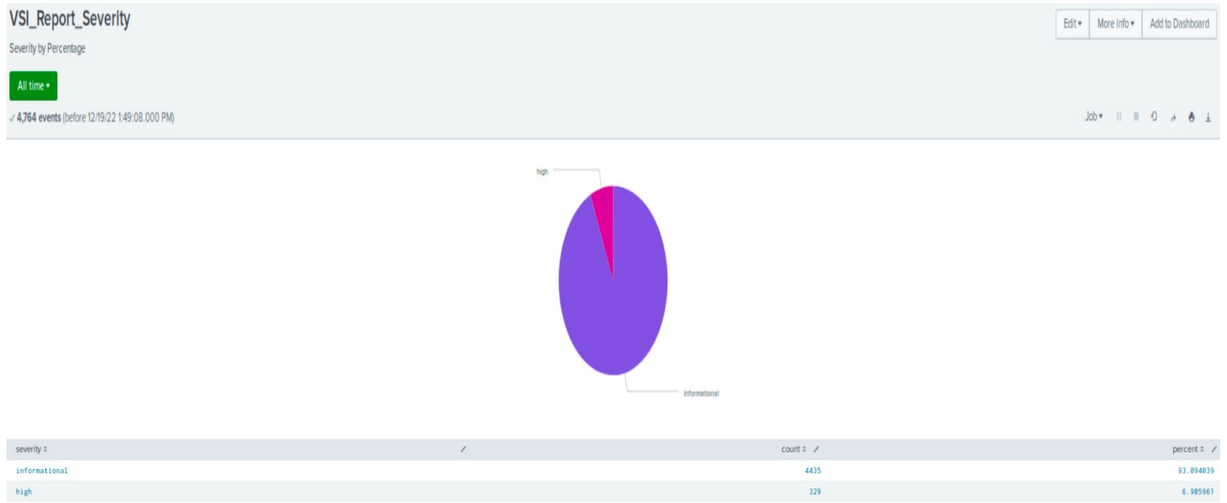
Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
VSI_Report_Signatures	Table of Signatures with their associated Signature ID
VSI_Report_Severity	Severity events by count and percentage
VSI_Report_Status	Comparison of Successful and Failed Windows Activities

Images of Reports—Windows



Alerts—Windows

Designed the following alerts:

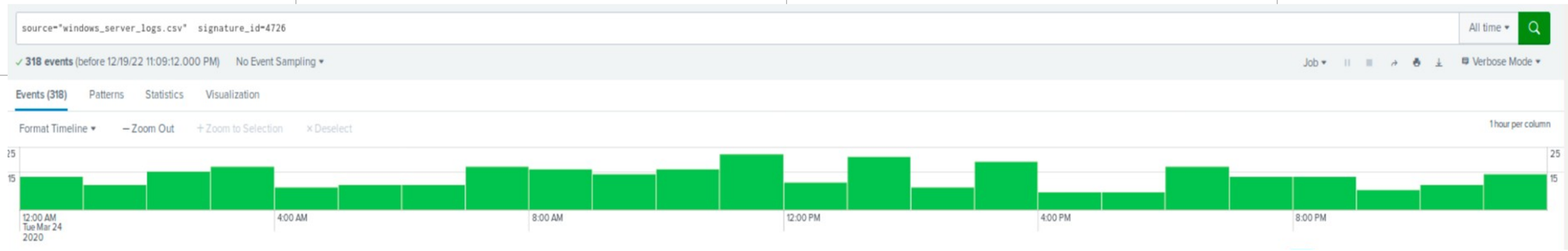
Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI_Alert_Failed	Triggered when the threshold for failed windows activity is reached	5 events per hour	30 events per hour

With a baseline of 5 per hour, an alert threshold of 30 per hour was determined effective without subjecting the team to alert fatigue.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI_Alert_Deleted_Accounts	Triggered when the threshold for deleted user accounts is	12	20

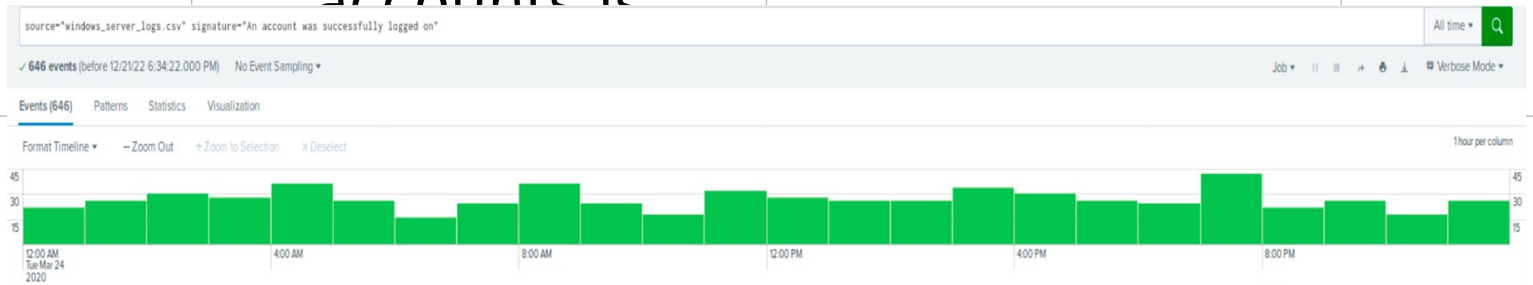


With a baseline of 12 per hour, an alert threshold of 20 per hour was determined effective without subjecting the team to alert fatigue.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI_Alert_Successful_Login	Triggered when the threshold for successfully logged on accounts is	15 events per hour	65 events per hour



With a baseline of 15 per hour, an alert threshold of 65 per hour was determined effective without subjecting the team to alert fatigue.

Dashboards—Windows

Dashboards—Windows

Users Count

VSI_Report_Users_Count

user	count	percent
user_k	2118	35.602622
user_a	1878	31.568331
user_j	398	6.690200
user_l	145	2.437384
user_e	117	1.966717
user_m	113	1.899479
user_f	109	1.832241
user_b	109	1.832241
user_i	106	1.781812
user_n	105	1.765003
user_c	105	1.765003
user_g	98	1.647336
user_d	92	1.546478
user_h	87	1.462431

Windows Server Log Dashboard Panels - Users Statistical Table and Radial Gauge, Signatures Pie Chart

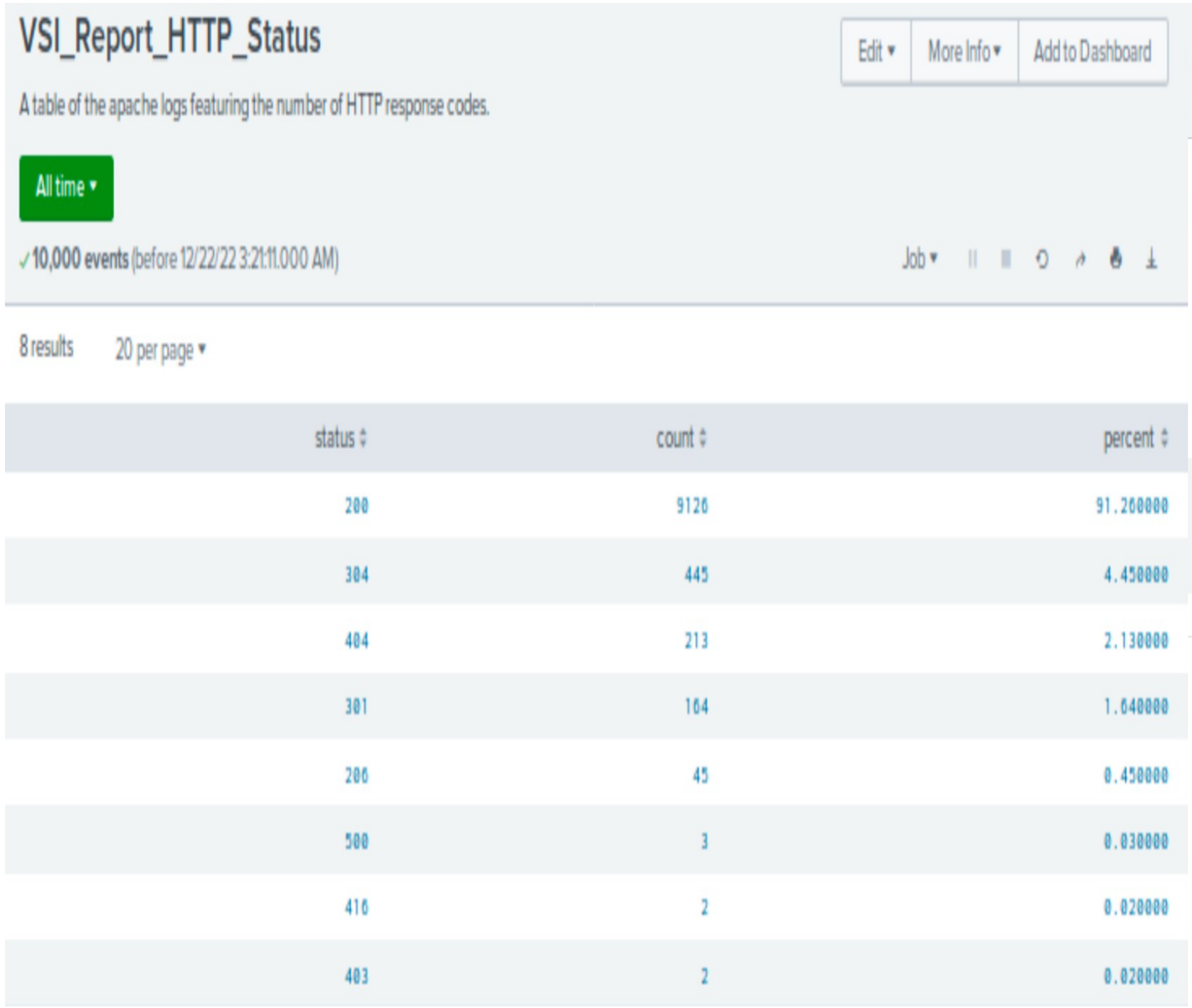
Apache Logs

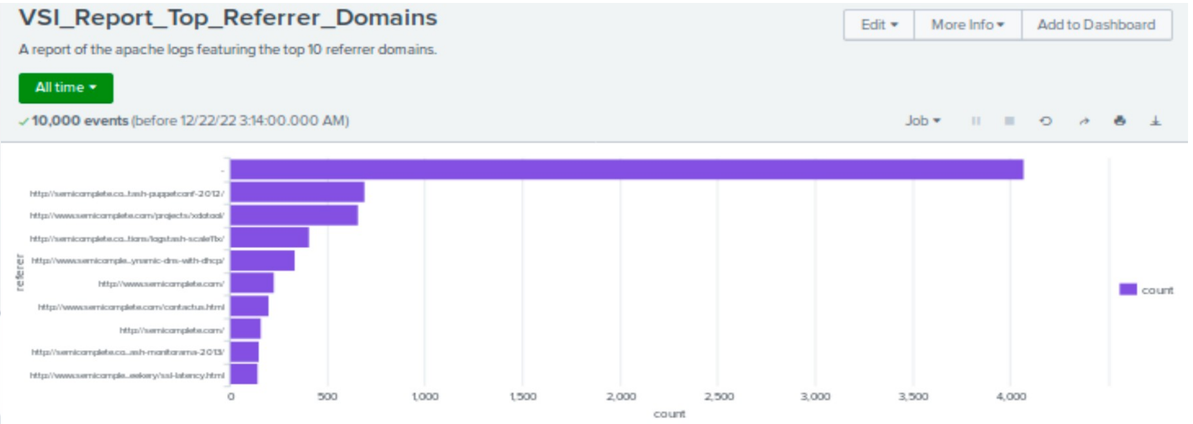
Reports—Apache

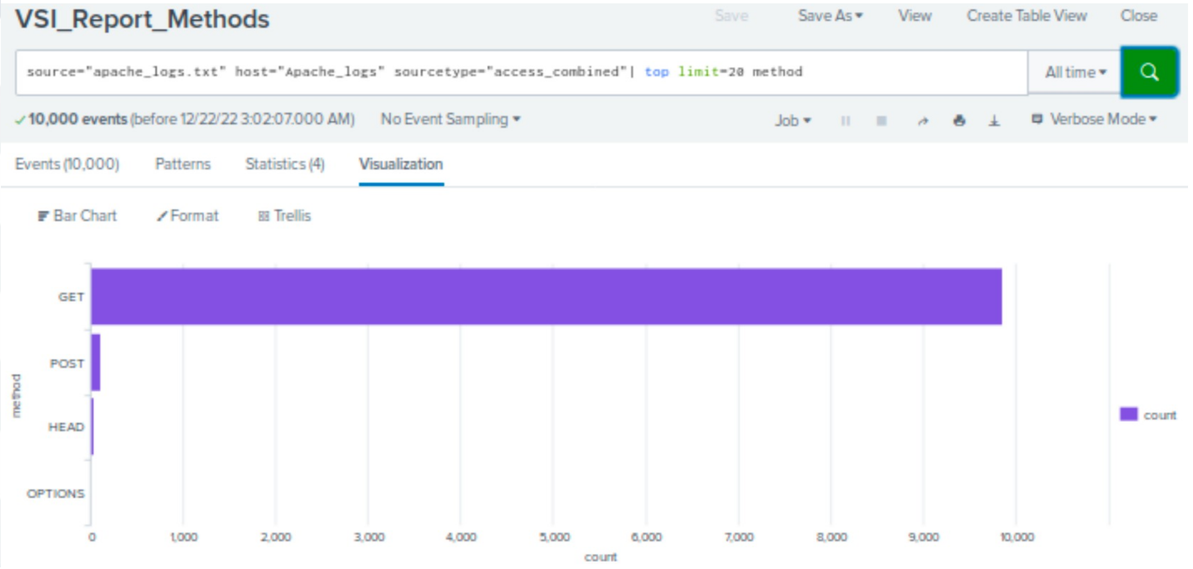
Designed the following reports:

Report Name	Report Description
VSI_Report_Methods	Chart of HTTP Methods by Count
VSI_Report_Top_Referrer_Domains	Chart of Top 10 referrer domains
VSI_Report_HTTP_Status	Table of HTTP Response Codes by Count

Images of Reports—Apache



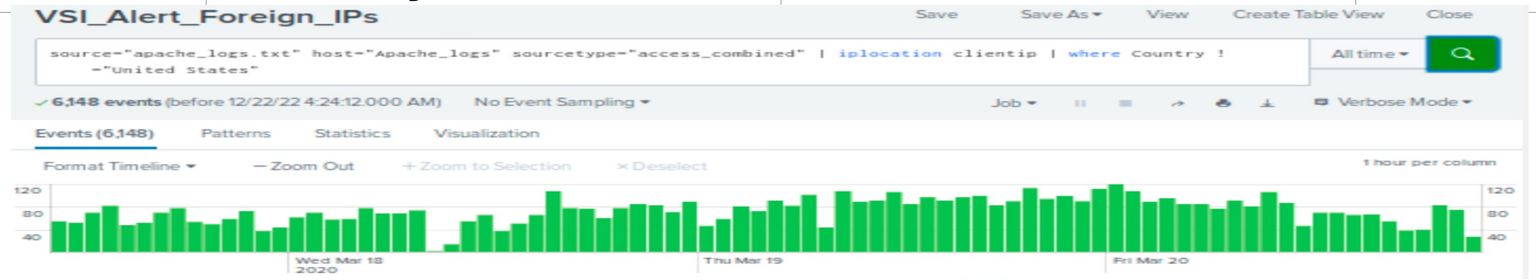




Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI_Alert_Forein_IPs	Triggered when the threshold for foreign client IP activity is reached	120 events per hour	200 events per hour

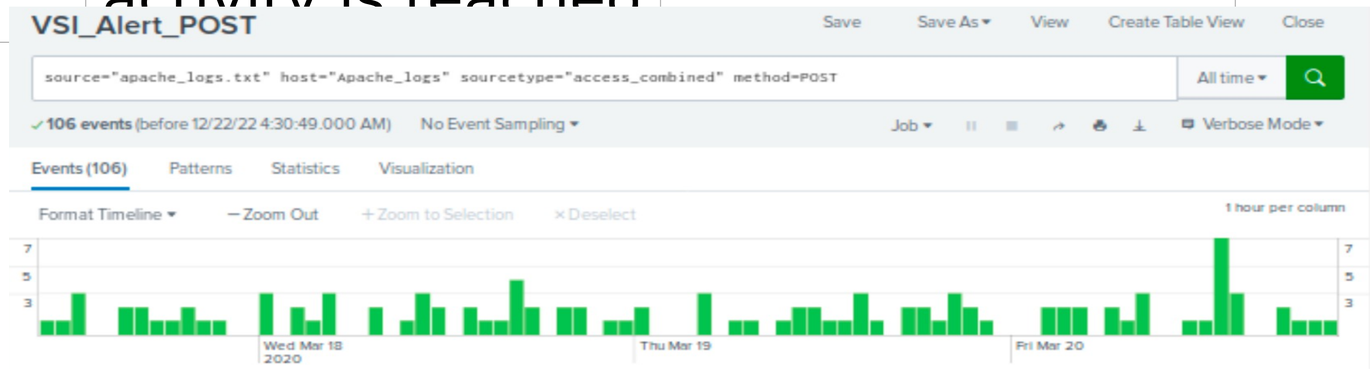


With a baseline of 10 per hour, an alert threshold of 200 per hour was determined effective without subjecting the team to alert fatigue.

Alerts—Apache

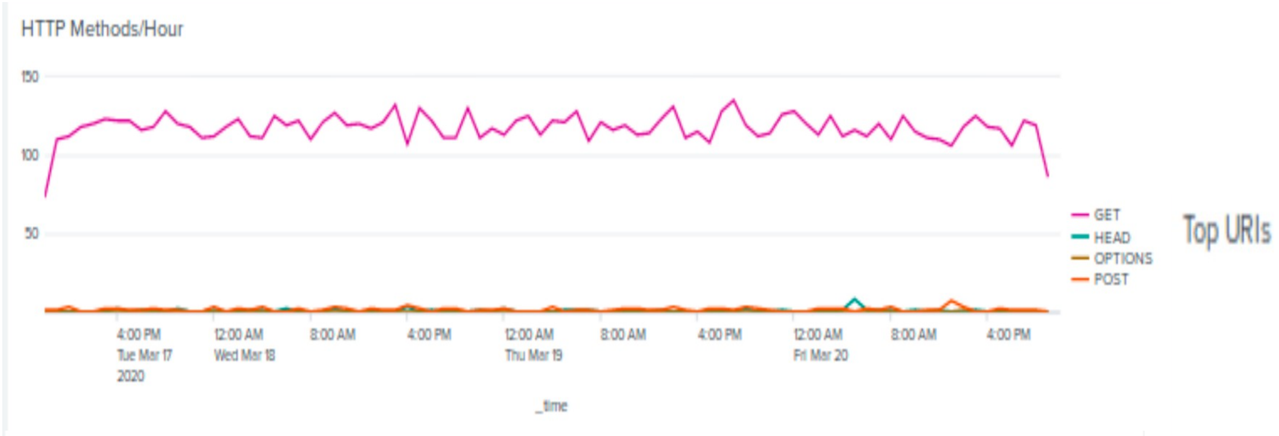
Designed the following alerts:

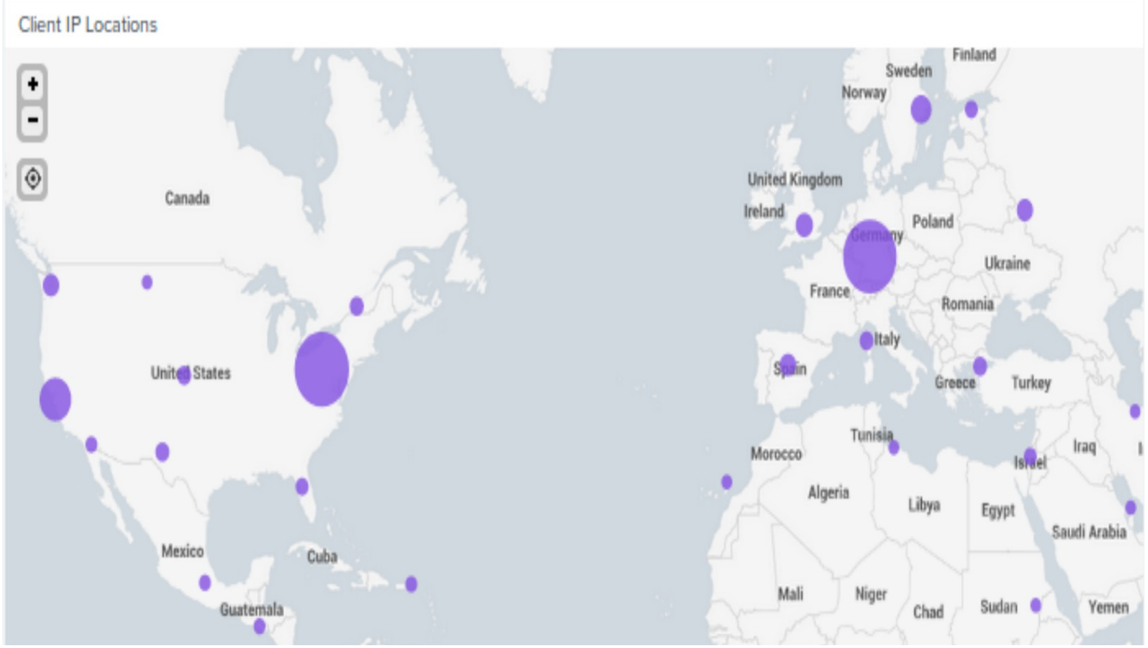
Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI_Alert_POST	Triggered when the threshold for HTTP POST activity is reached	10	20

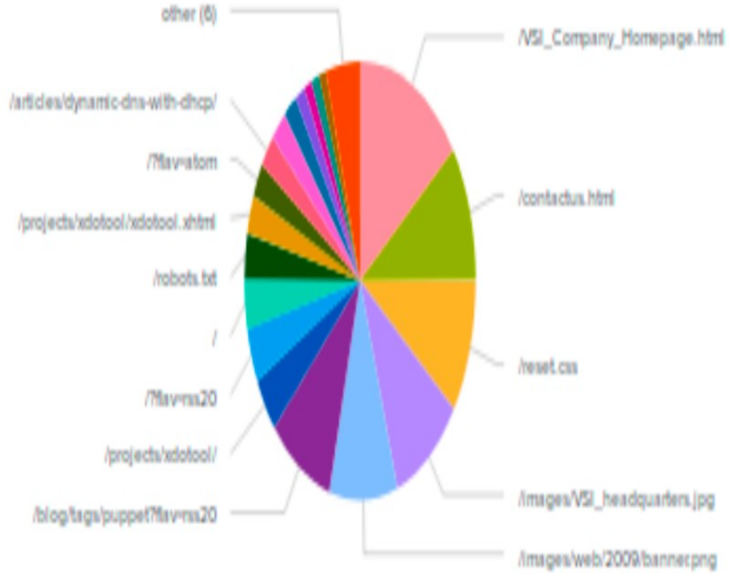


With a baseline of 10 per hour, an alert threshold of 20 per hour was determined effective without subjecting the team to alert fatigue.

Dashboards—Apache







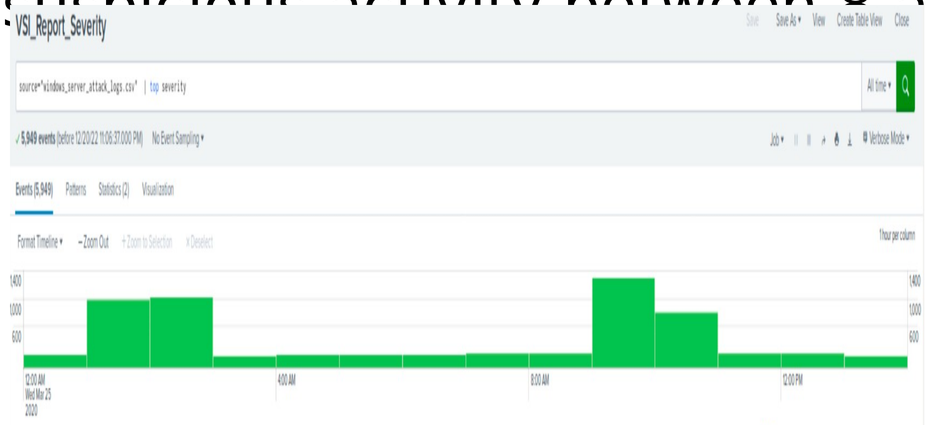
Apache Log Reports - HTTP Methods by Hour, Client IP Location Map and Top URIs being accessed

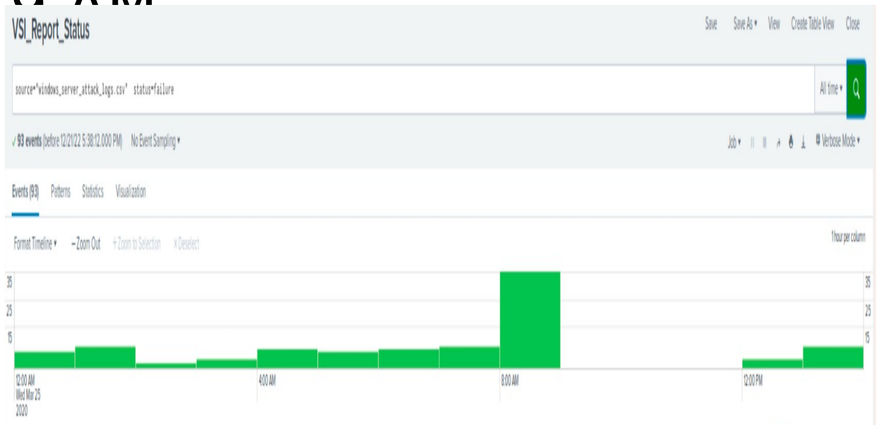
Attack Analysis

Attack Summary—Windows

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

- The severity report for the attack logs suggests suspicious activity between 1 and 3 AM on Wednesday, March 25, 2020 and again later that morning between 9 and 11 AM
- Analysis of the failed windows activity for the day also observed suspicious activity between 8 and 9 AM





Attack Summary—Windows

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

- The threshold for a suspicious amount of failed activities was calculated to be 30 events per hour. This threshold was crossed from 8-9 AM on Wednesday, March 25, 2020.
- The threshold for a suspicious amount of successful logins was calculated to be 65 events per hour. This suggests that from the attack logs, there was observed suspicious activity between 11 AM and 1 PM on Wednesday, March 25, 2020.
- There was not found to be a suspicious volume of deleted accounts as the threshold was set > 20 events per hour.

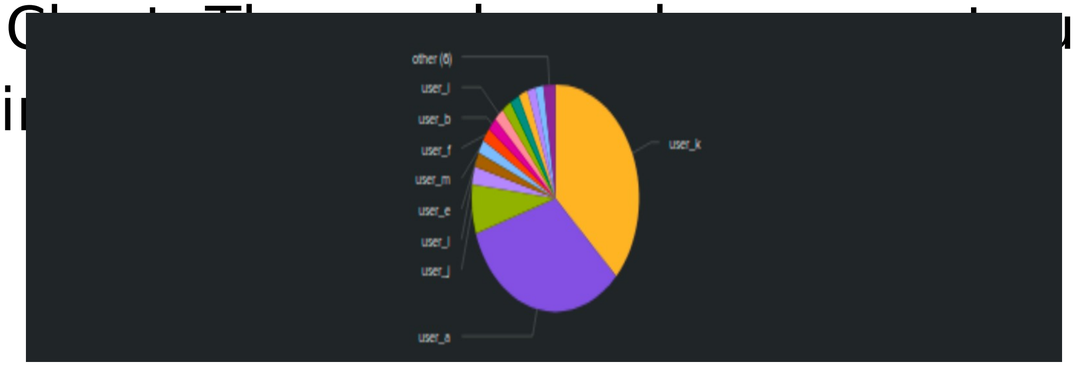
Attack Summary—Windows

Screenshots of Alert Reports

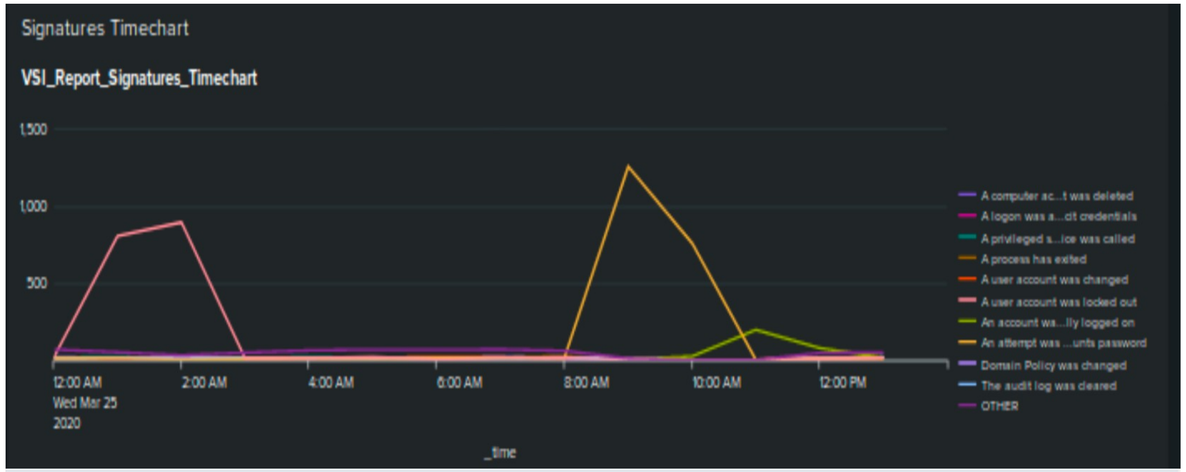
Attack Summary—Windows

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

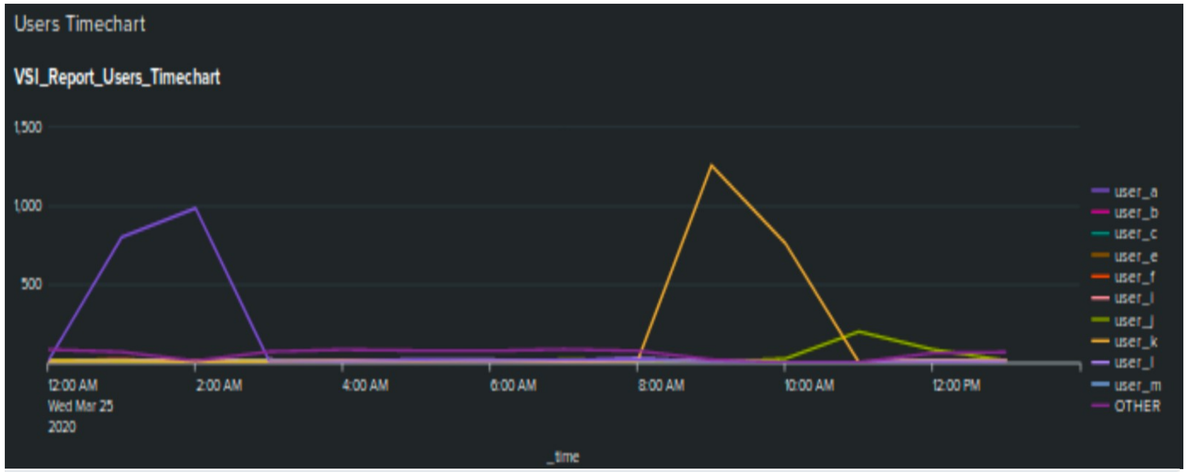
- There were three signatures that stood out in the attack log. “An attempt was made to reset an account's password,” “A user account was locked out,” and an account was successfully logged on. These are represented by the peaks in the time chart.
- The Users Time Chart has three peaks that coincide with the Signatures Time C[illegible]user_a, the yellow user_k, and the li[illegible]



Screenshots of Attack Logs



_time	A computer account was deleted	A logon was attempted using explicit credentials	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	An attempt was made to reset an accounts password	Domain Policy was changed	The audit log was cleared	OTHER
2020-03-25 00:00	19	14	14	8	10	16	11	10	10	12	68
2020-03-25 01:00	12	8	20	13	7	805	15	11	16	16	50
2020-03-25 02:00	9	2	3	16	9	896	14	3	17	8	30
2020-03-25 03:00	13	13	13	12	16	10	14	6	16	14	47
2020-03-25 04:00	12	15	18	8	11	12	12	11	10	16	62
2020-03-25 05:00	11	11	14	12	16	19	9	8	14	10	68
2020-03-25 06:00	9	11	14	12	17	3	11	14	8	13	66
2020-03-25 07:00	15	14	8	15	17	11	15	16	20	7	69
2020-03-25 08:00	17	11	13	23	11	16	16	12	11	16	59
2020-03-25 09:00	5	5	2	1	3	1	4	1258	0	4	10
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	7	14	9	7	11	6	77	6	6	9	45
2020-03-25 13:00	4	12	8	7	9	16	15	12	15	17	49

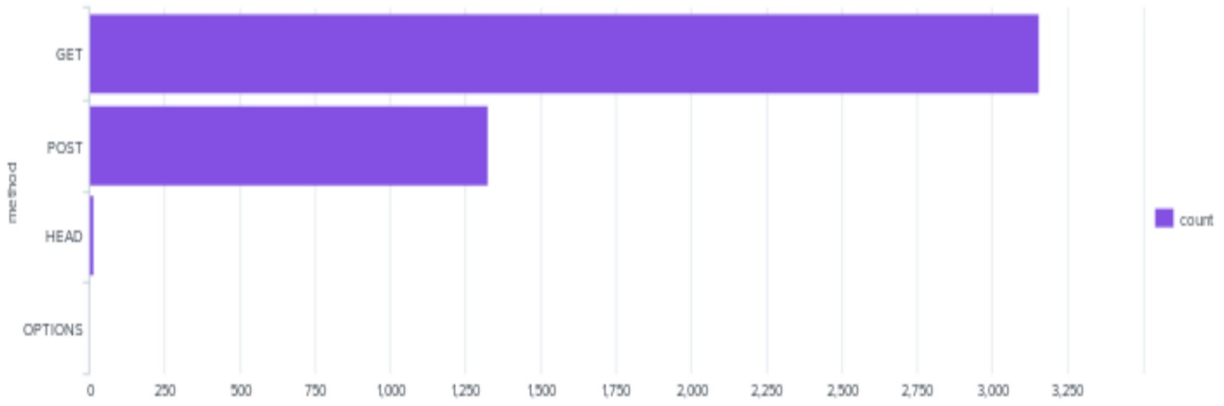


_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9
2020-03-25 03:00	8	13	8	17	9	12	8	4	17	10	68
2020-03-25 04:00	8	10	10	5	15	9	15	16	8	10	81
2020-03-25 05:00	13	6	9	14	9	10	9	13	19	15	75
2020-03-25 06:00	10	9	11	14	14	9	2	7	17	12	73
2020-03-25 07:00	16	11	9	15	14	8	18	7	10	16	83
2020-03-25 08:00	18	14	7	9	12	12	13	12	25	10	73
2020-03-25 09:00	3	1	5	0	1	2	2	1256	5	1	17
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	4	8	10	3	6	4	82	8	6	7	59
2020-03-25 13:00	8	5	12	9	8	11	11	15	12	8	65

Attack Summary—Apache

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

- A large increase in POST methods was observed on March, 25, 2020. The POST method is used to send data to a web server. It is used to create or update resources.
- A large increase in 200 and 404 codes were observed as well

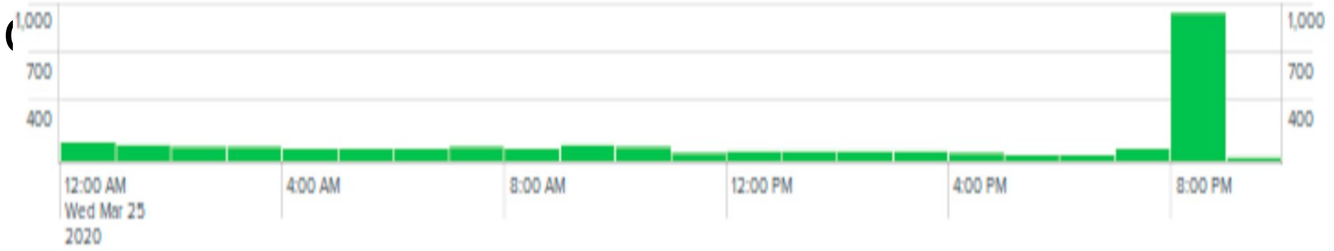


status ⇕	count ⇕	percent ⇕
200	3740	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

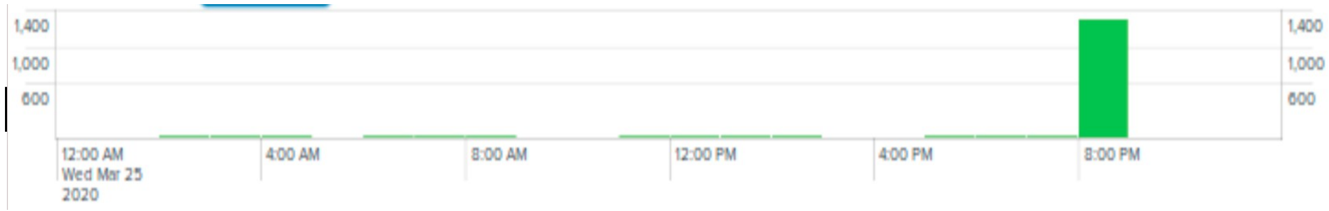
Attack Summary—Apache

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

- The threshold for a suspicious amount of international activity was determined to be > 200 per hour. This alert would have been triggered (



- The threshold for POST activity was set to 20 per hour, so it would have been team would leave the t

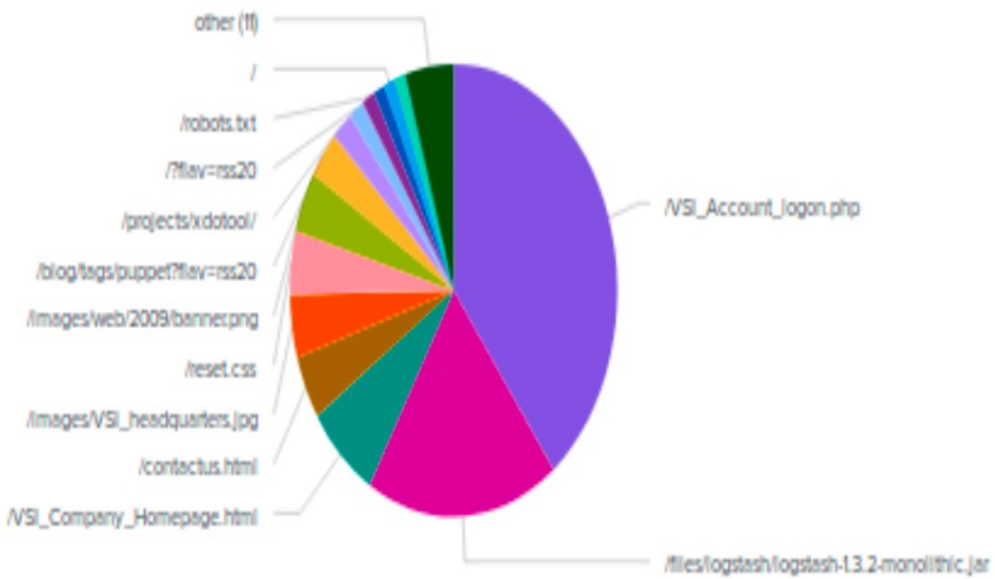


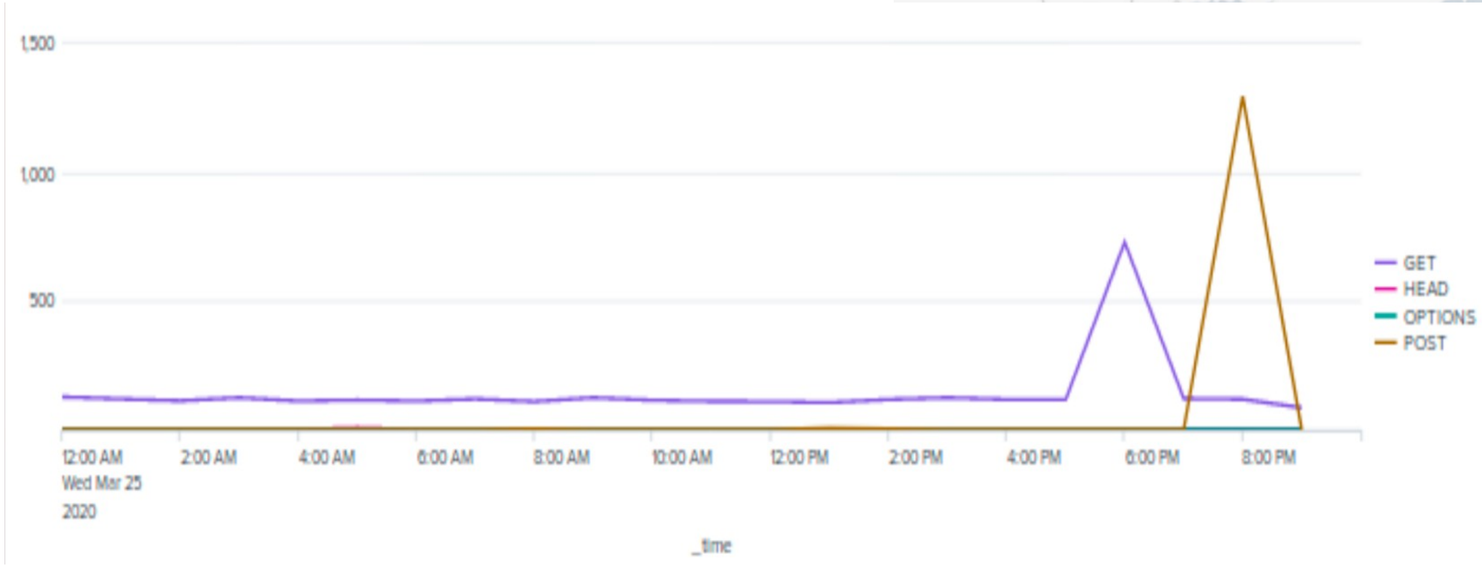
Attack Summary—Apache

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

- Between 5 and 7 PM saw a spike in GET requests, and between 7 and 9 PM there was a spike in POST requests.
- 439 events took place in Kiev and 433 events in Kharkiv.
- The URI hit the most was /VSI_Account_logon.php

Screenshots of Attack Logs





Summary and Future Mitigations

Project Summary

- What were your overall findings from the attack that took place?

  Based on the information that was gathered during the course of this investigation, our team found sufficient evidence of a brute force attack directed at VSI Apache and Windows servers on March 25, 2020 from the Kiev and Kharkiv region

- To protect VSI from future attacks, what future mitigations would you recommend?
  - ➔ Firewall configurations are a great way to block IP traffic from specific geographical locations, like Ukraine
  - ➔ Complex passwords and two-factor authentication can help safeguard user account access