Defensive Security Project by:
Anthony Vagg
&
Chris Kimitsis

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

Virtual Space Industries or VSI has gotten wind of a potential attack from a competitor, JobeCorp.

This will be a presentation on the Pre and Post attack monitoring solutions created to detect and determine actions the attackers undertook on March 25th 2020.

Monitor

- Windows Server
- Apache Server
- Website

Create

- Reports, Alerts and dashboards for potential areas of attack within the monitoring areas.

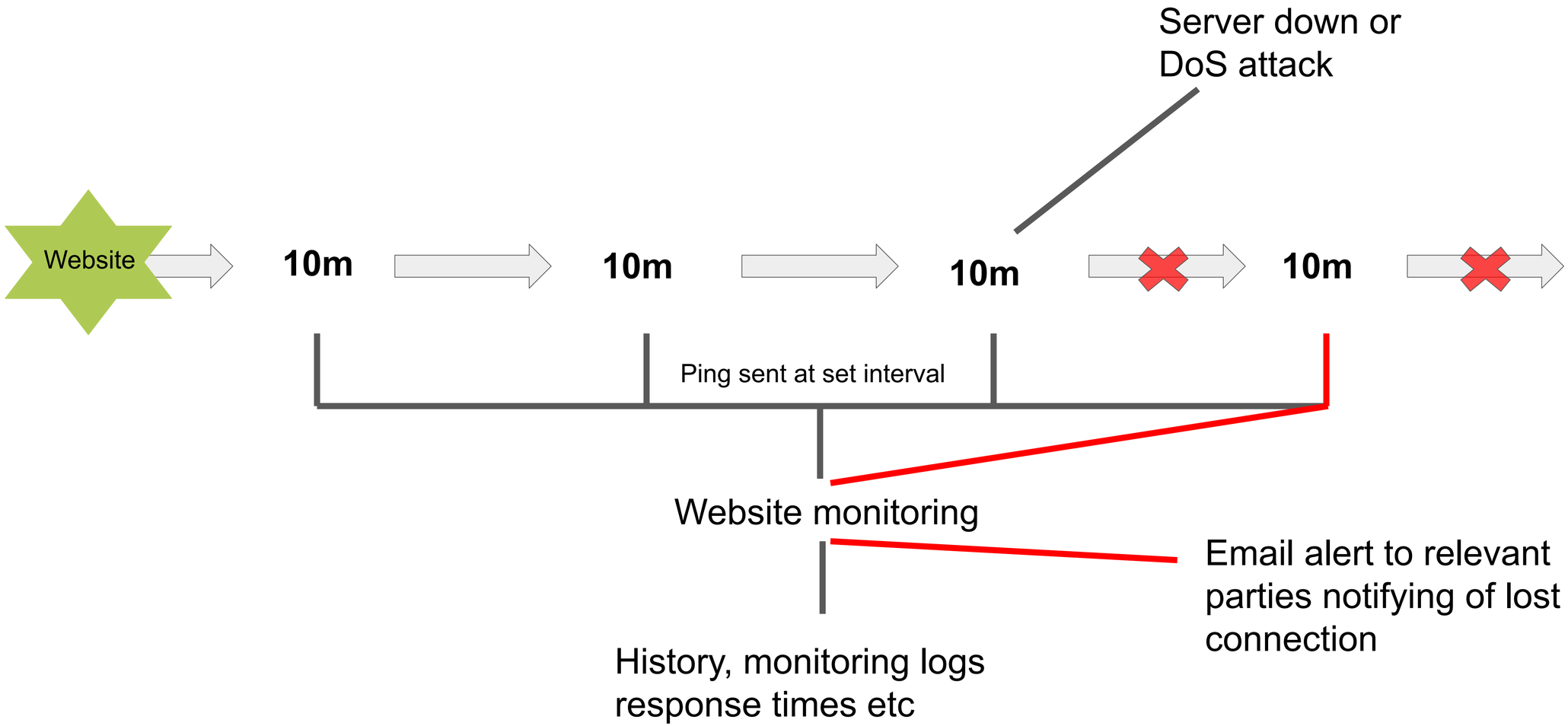
Web Monitoring App

Web Monitoring App

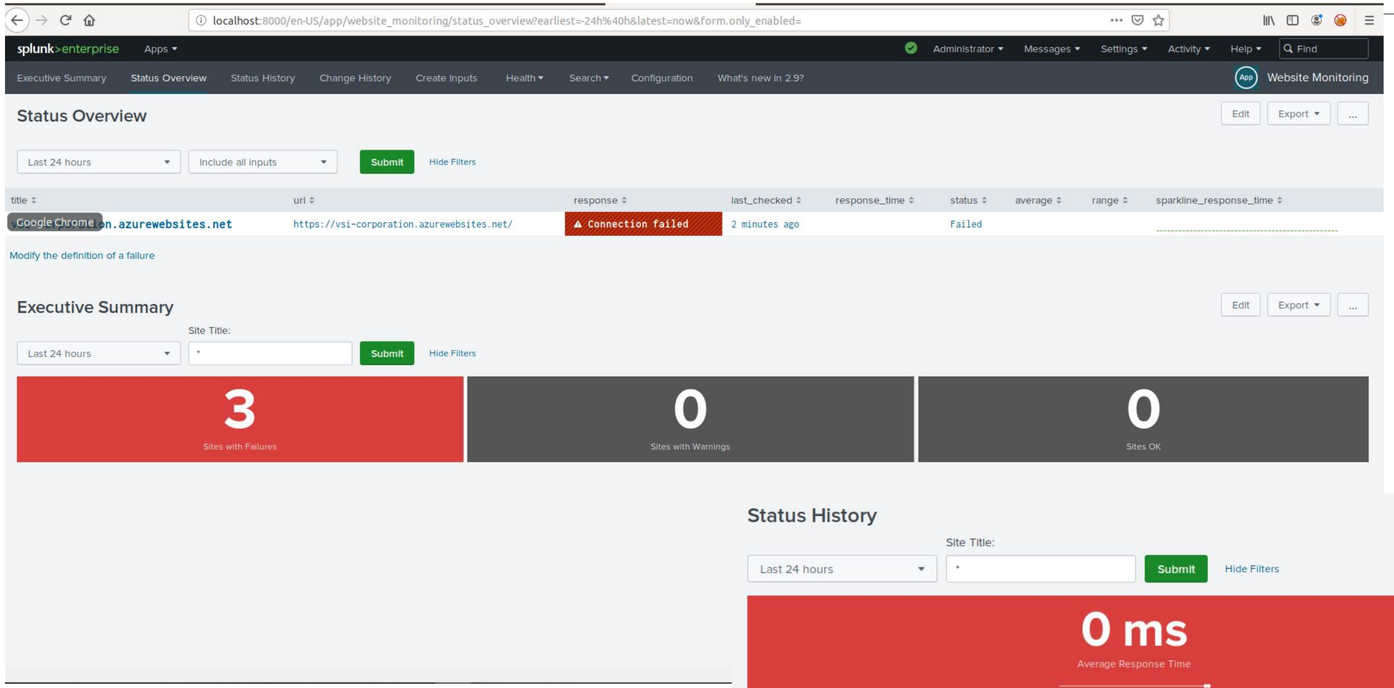
This app was selected as VSI uses a website for their administrative activities.

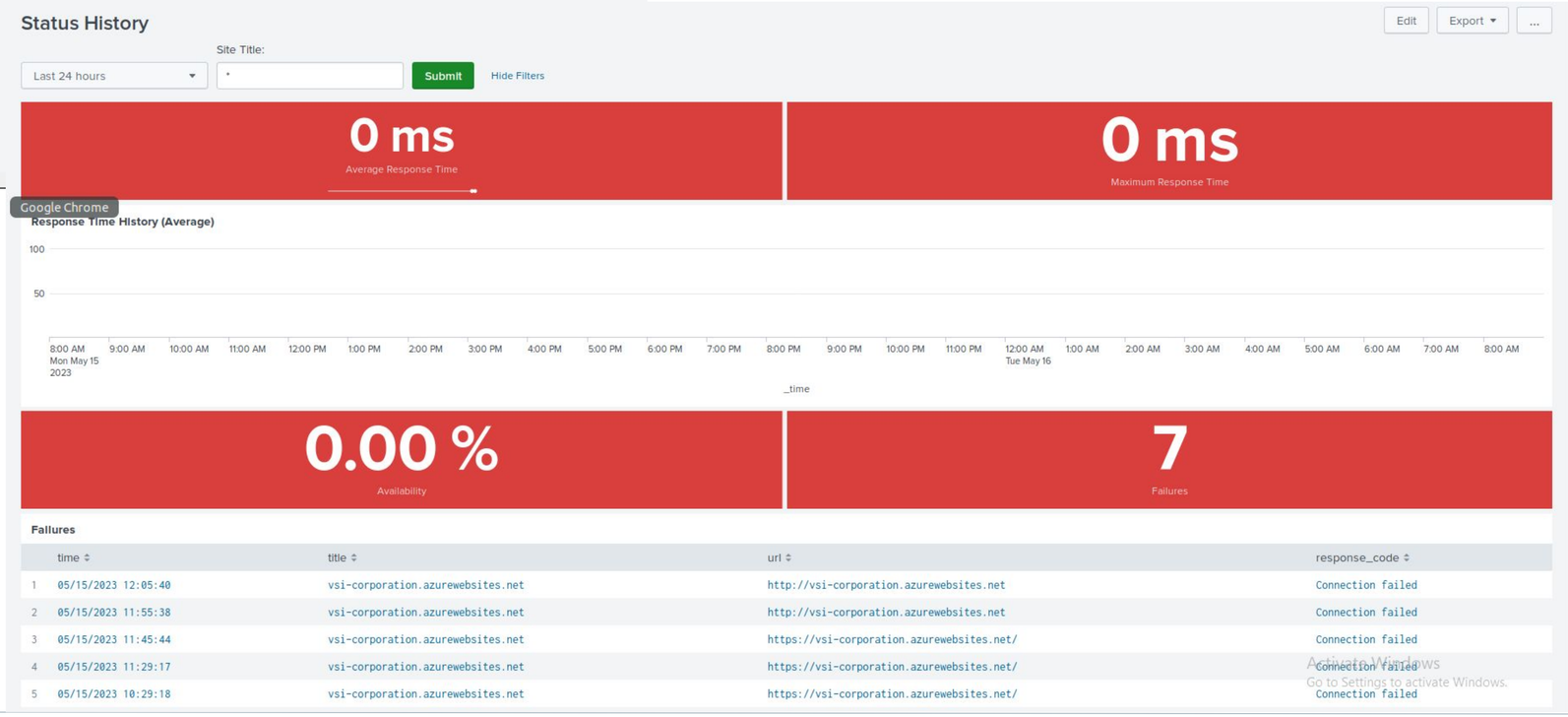
- Calculates the website’s uptime percentage
- Provides information about the response time of website
- Alerts by email when website goes down, responds too slowly or is returning errors
- Provides history when pages are changed
- Helps identify any attacks that significantly slow down the site or take it off-line

Web Monitoring App



Web Monitoring App





Logs Analyzed

1 Windows Logs

- Signature IDs
- Signatures
- Users activity
- Status
- Severity of events

2 Apache Logs

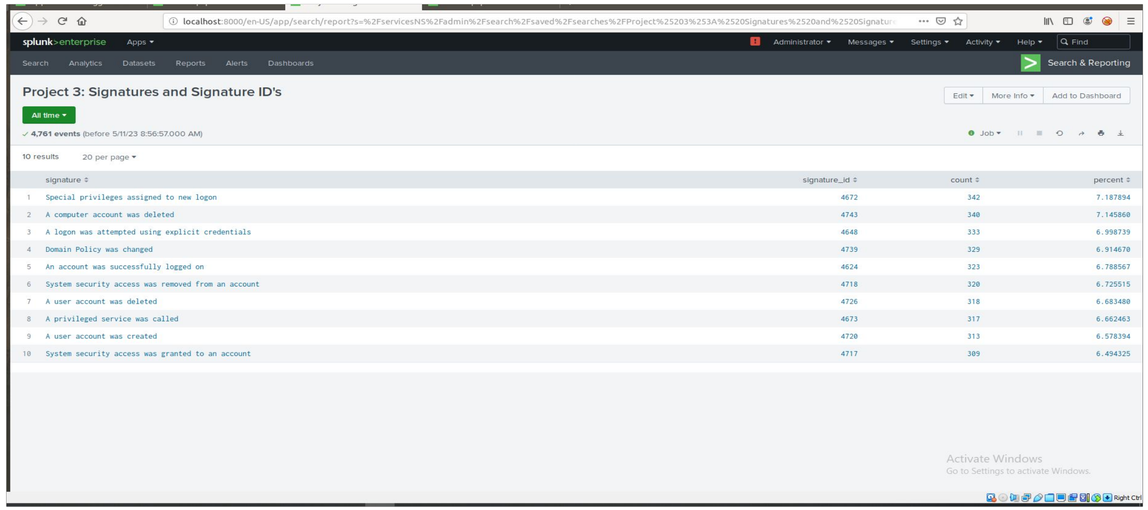
- HTTP Methods
- Referrer domains
- HTTP response codes
- Client IP
- User agents

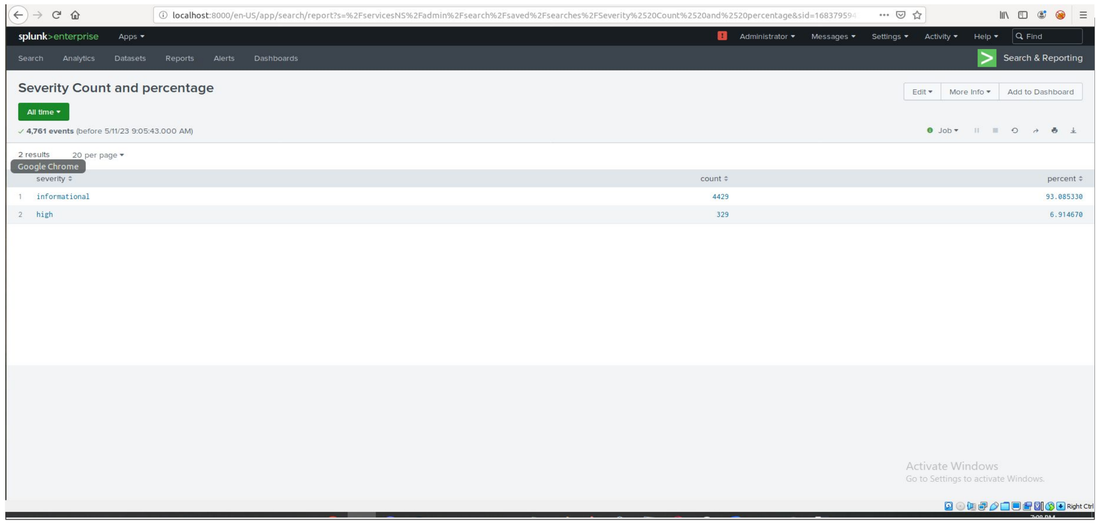
Windows Logs

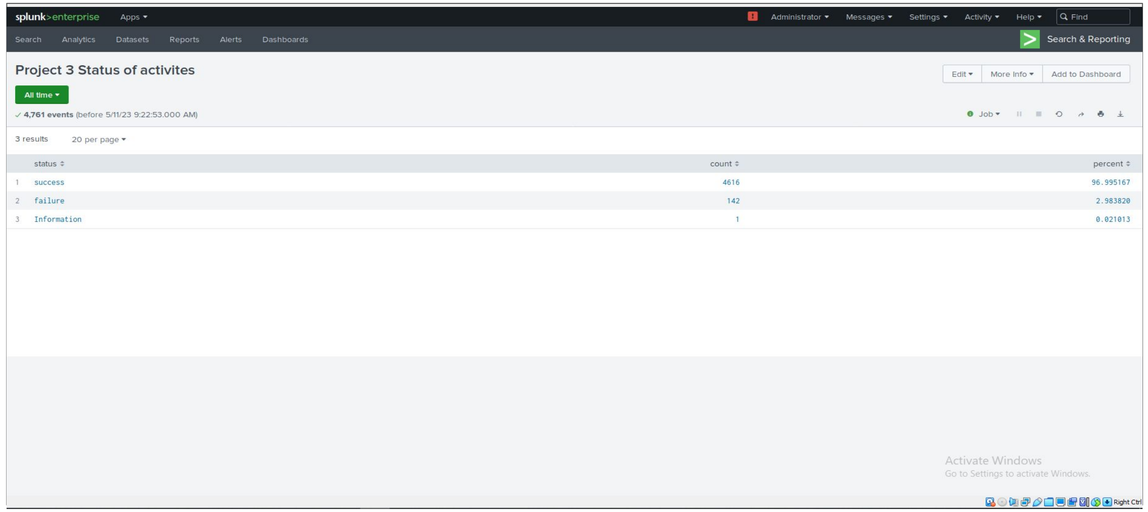
Reports—Windows

Report Name	Report Description
Windows log Signature and Signature ID	Reports the corresponding signature ID for each event that takes place.
Severity Level	Reports if there is a suspicious level of activity on the server.
Windows Success and Failure Report	Reports the success and failure by count.

Images of Reports—Windows





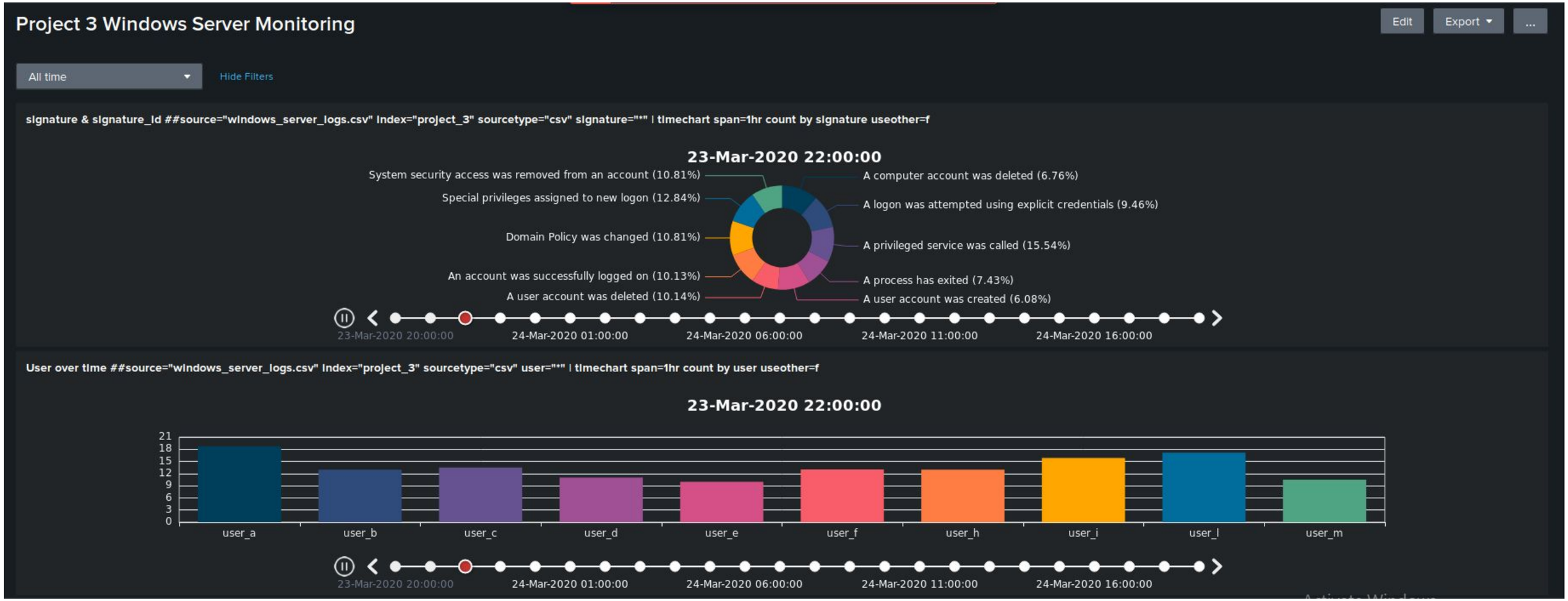


Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	Alert sent when failed activity threshold is exceeded	6	12
Account Successfully logged in	successful account logins has exceeded the threshold	13	22
A user account was deleted	An Alert issued when the deleted accounts threshold is exceeded.	14	22

JUSTIFICATION: Baseline is the average of all hourly values and the threshold is average + standard deviation times 3 which effectively covers 99.7% of presented data or 3 standard deviations away from the mean in normal distributions.

Dashboards—Windows



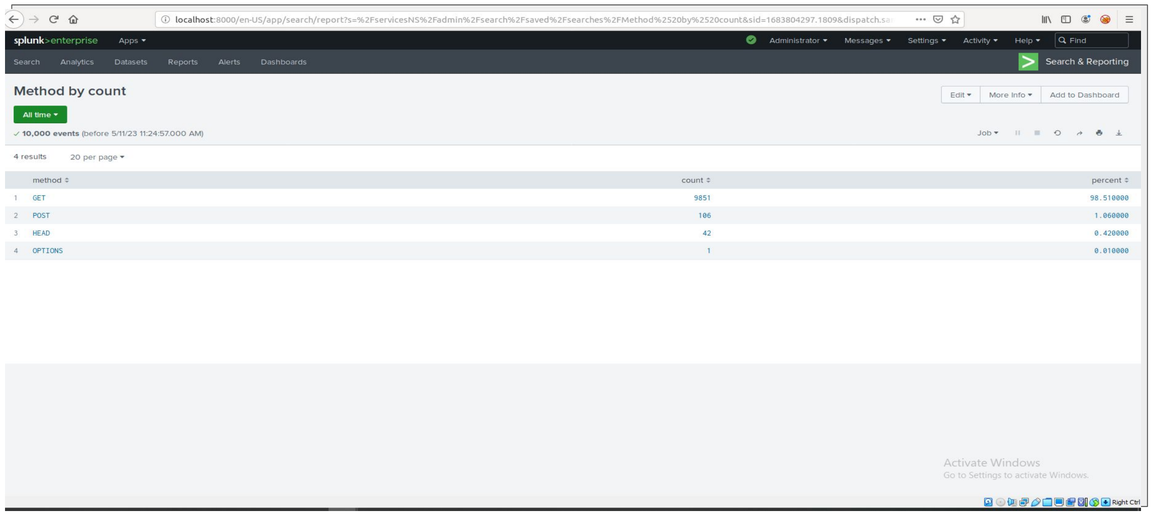
Dashboards—Windows

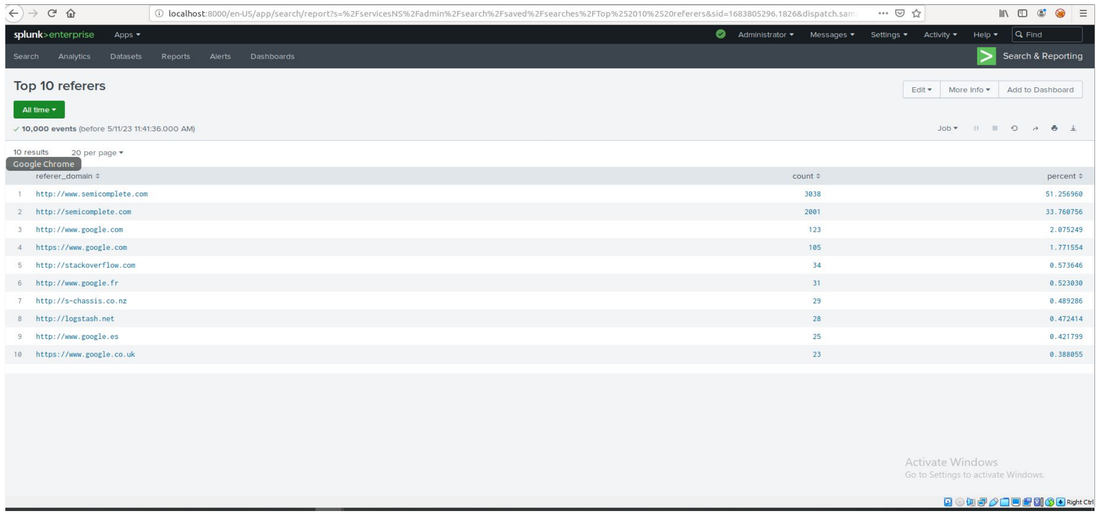
Apache Logs

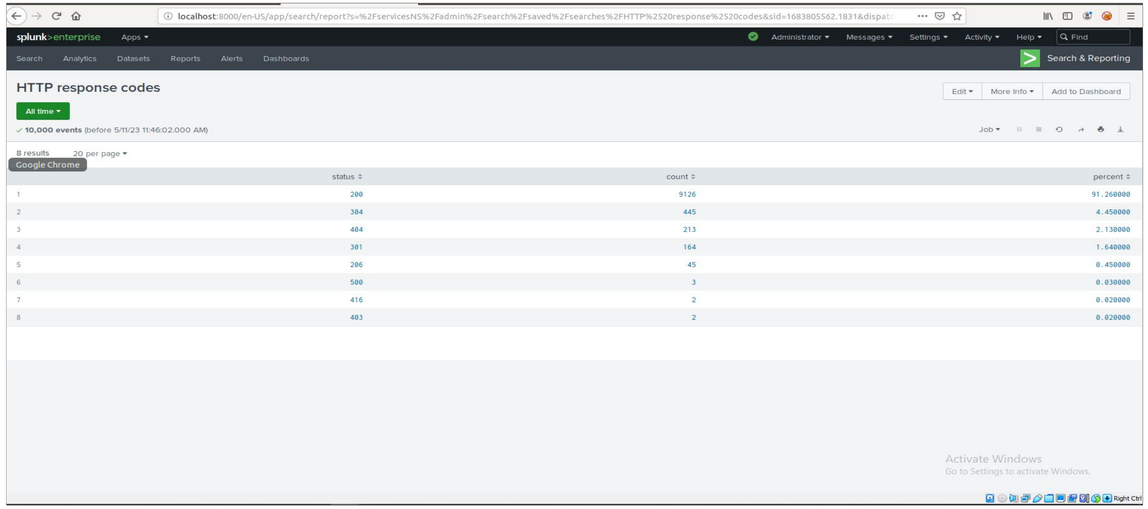
Reports—Apache

Report Name	Report Description
HTTP Methods	Table that shows the count of GET, POST, HEAD and OPTIONS
Top 10 Domains	Top 10 domains that refer to VSI’s web server
HTTP Response codes	Shows the count of HTTP response code

Images of Reports—Apache





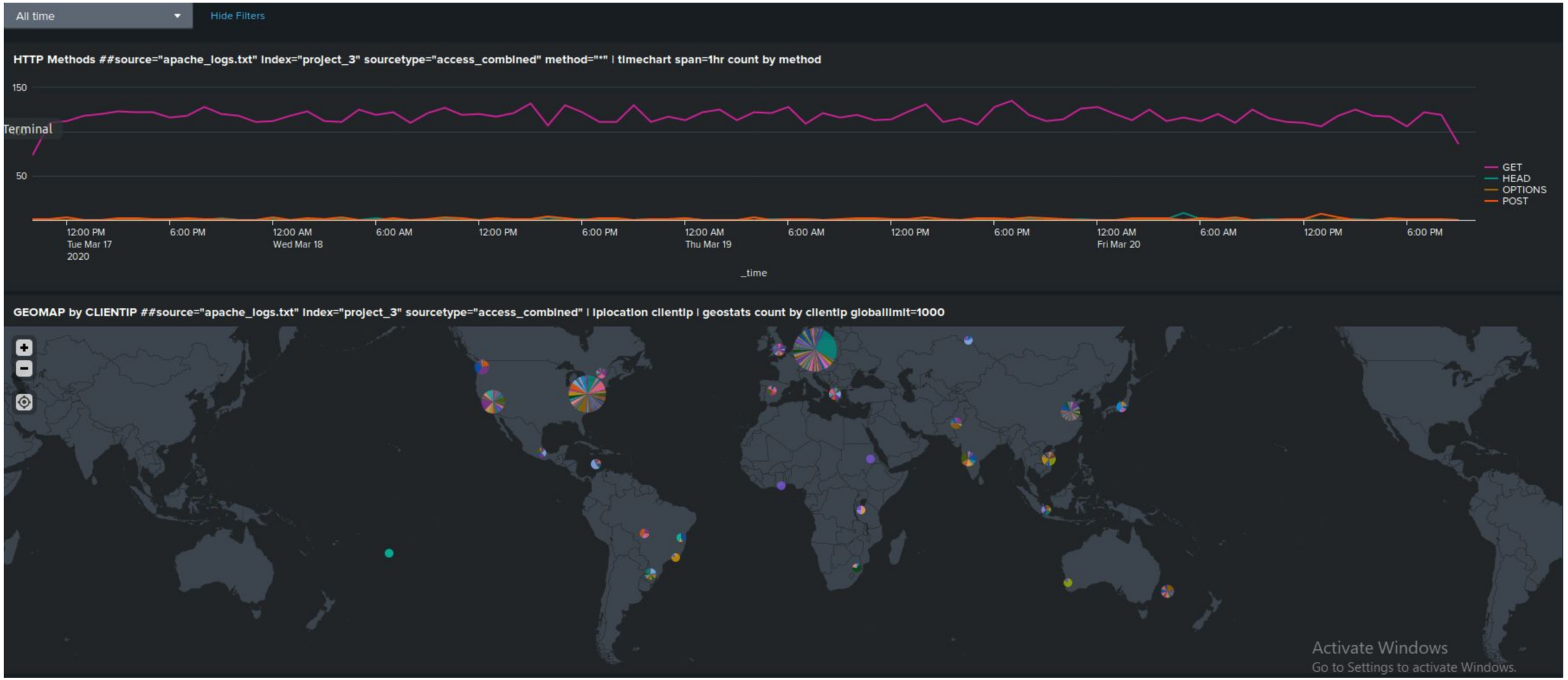


Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Country activity by the hour, excluding the USA	Alert that triggered when the threshold country activity is exceeded.	73	140
Hourly count of the HTTP post method	Hourly count of Post activity	1	5

JUSTIFICATION: Baseline is the average of all hourly values and the threshold is average + standard deviation times 3 which effectively covers 99.7% of presented data or 3 standard deviations away from the mean in normal distributions.

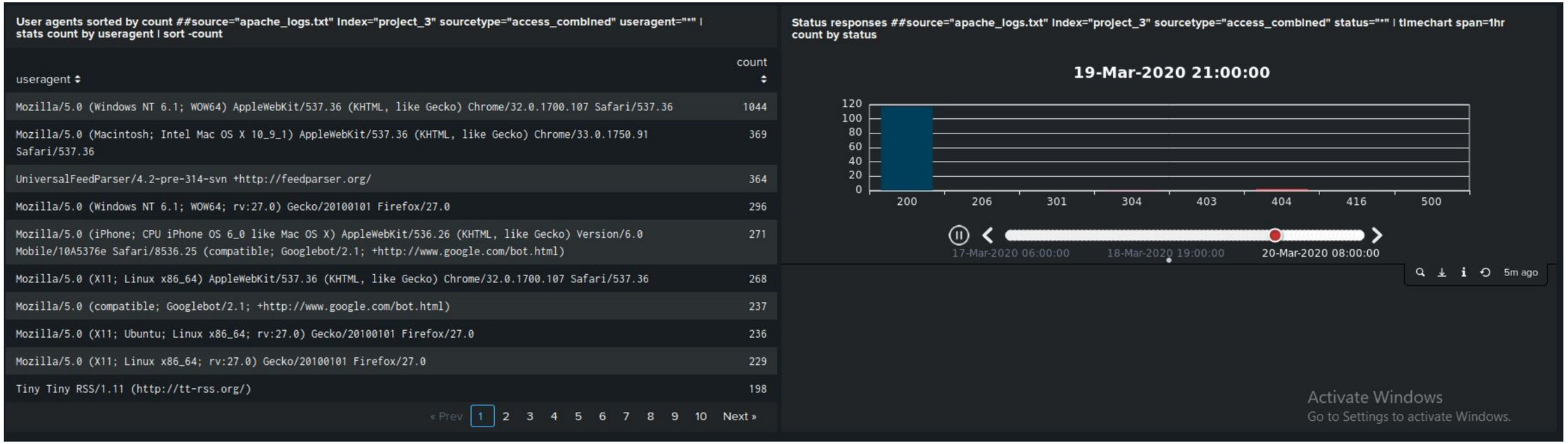
Dashboards—Apache



Dashboards—Apache

While adding the total count value of user agents and number of URI’s may not have been necessary it gives you an at a glance view on your values in normal operation.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

- Increase of 13.31% in High classification severity returns from 329 to 1111

2 results 20 per page

	severity	count	percent
1	informational	4429	93.085330
2	high	329	6.914670

	severity	count	percent
1	informational	4381	79.770575
2	high	1111	20.229425

- Several spikes in successful activity that deviates from apparent norms

	status	count	percent
1	success	4616	96.995167
2	failure	142	2.983820
3	Information	1	0.021013

	status	count	percent
1	success	5854	98.436186
2	failure	93	1.563814

Attack Summary—Windows

- Increase in Failed activities by 500%. This would have triggered the alert as threshold is set to 5 and peak value was 35.
- A disappearance of successful logins suggesting scrubbed logs so no alert was triggered and different signature id’s were used. However it would have triggered the alert as user activity when searched via users it would have returned values in the hundreds and the threshold is 22.
- A similar disappearance of deleted account also suggesting scrubbed logs so this also would not trigger an alert. The user activity for this activity is harder to surmise that the threshold would work correctly as it is easier to scrub this activity from the logs.

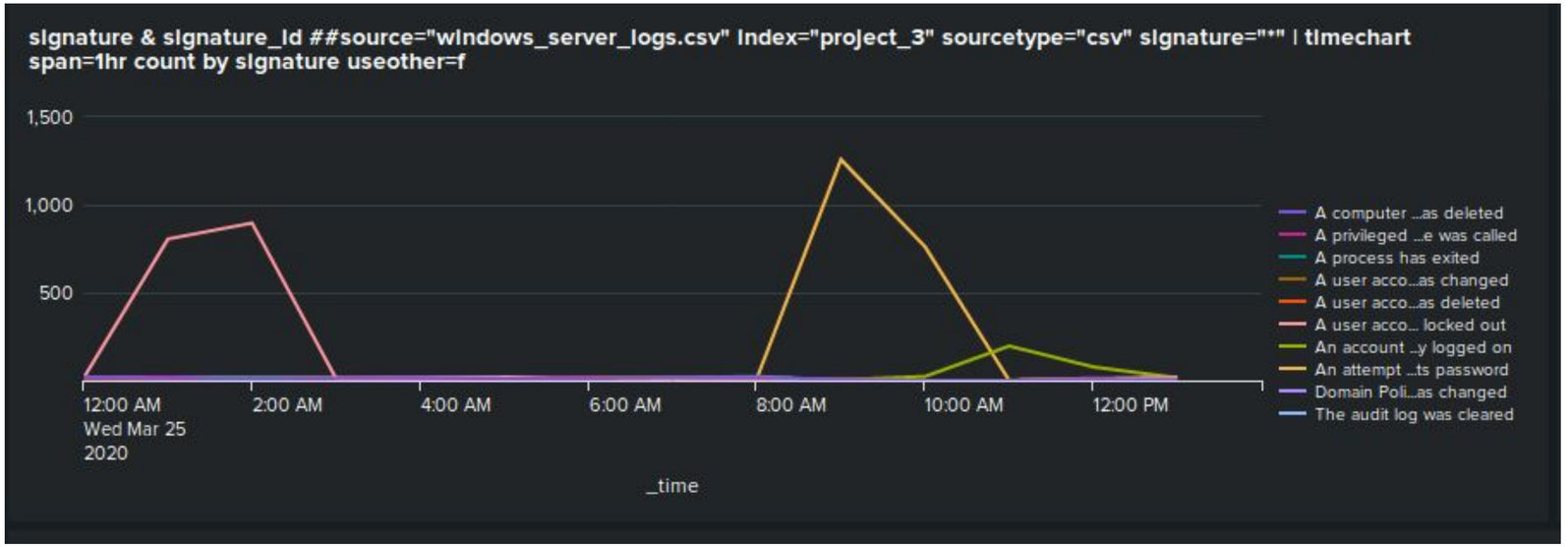
Attack Summary—Windows

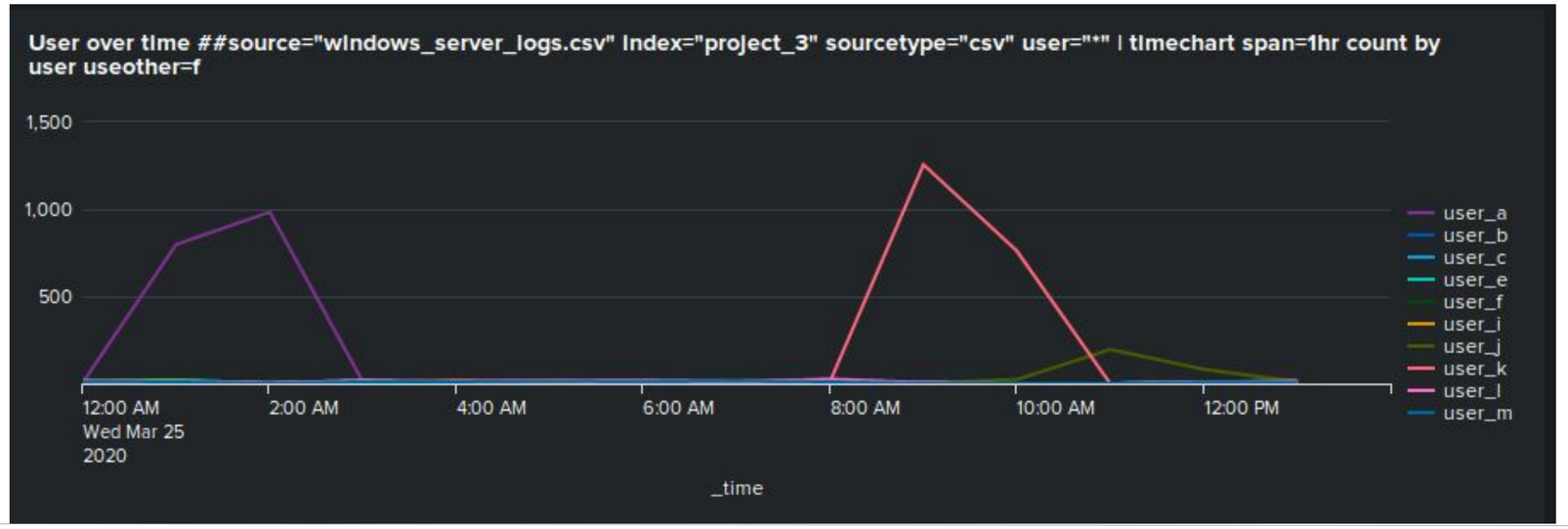
- A large spike in user account lockouts returning 1686 between 1AM and 2AM
- A large spike in user_a activity at 2AM

- A large spike in attempts to change passwords returning 2016 between 8AM and 11AM
- A large spike in user_k activity at 9AM

- A spike in successful user account logins returning 294 between 9AM and 1PM
- A spike in user_j activity at 11AM

Screenshots of Attack Logs





Attack Summary—Apache

- Nearly 30% increase in POST requests - 106 to 1324
- Large drop in referrer traffic - 5437 to 1442
- Large decrease in HTTP response codes and large increase in 404 responses
  Main ones being 200 - 9126 to 3746 and 404 - 213 to 679

Attack Summary—Apache

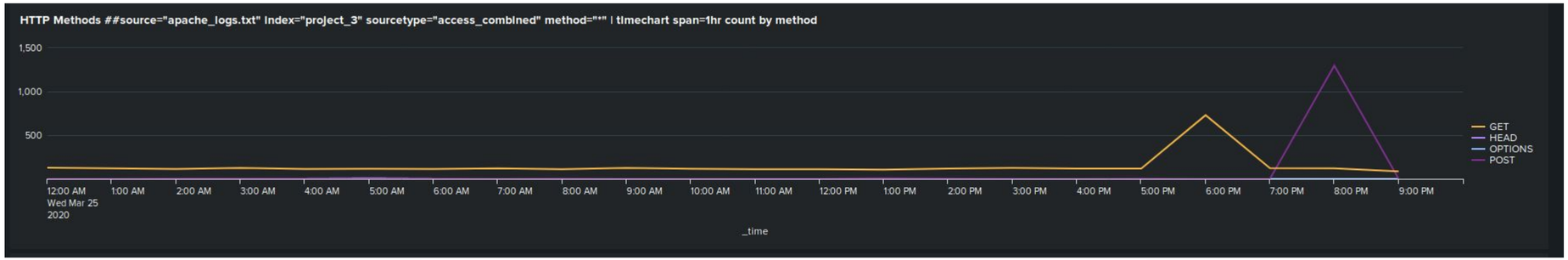
- Large increase in international traffic which passed the threshold and would have alerted to the attack at 8PM as there was a peak of 939 and the threshold is set to 140.

- Coinciding increase in HTTP POST requests. Threshold was set at 5 so this would have triggered the alert as it returned 1,296 requests.

Attack Summary—Apache

- Increase in GET requests beginning at 5PM
- Increase in POST requests beginning at 7PM
- High volume of traffic accessing /VSI_account_logon
- Large amount of activity from Ukraine, specifically Kiev and Kharkiv
- High Volume of traffic accessing /files/logstash/logstash-1.3.2-monolithic.jar which indicates someone may have altered the logs further reinforced by the gaps in the windows logs.

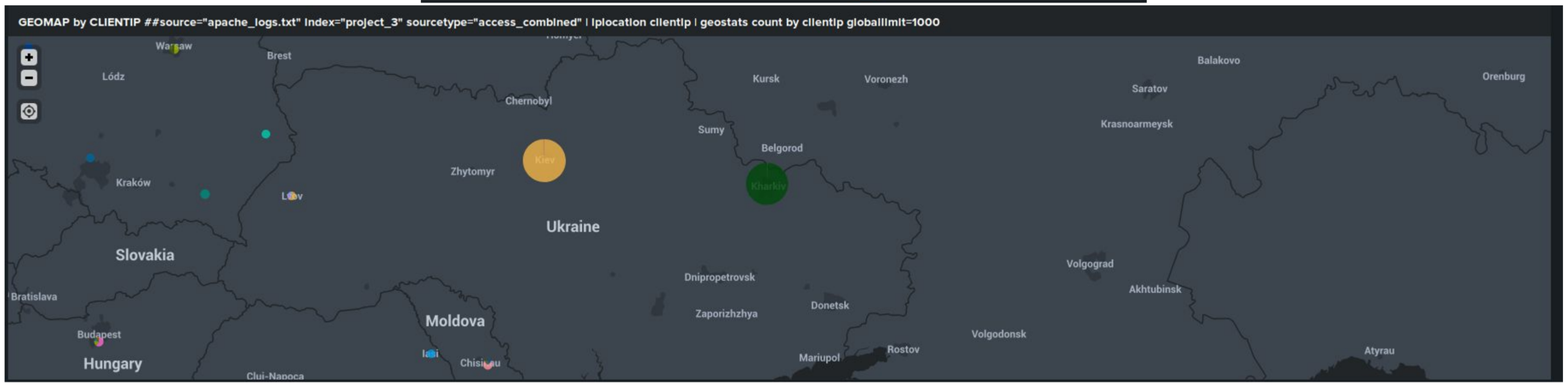
Screenshots of Attack Logs



Number of URI's -count ##source="apache_logs.txt" index="project_3" sourcetype="access_combined" uri="*" | stats count by uri | sort -count

uri	count
/VSI_Account_logon.php	1323
/files/logstash/logstash-1.3.2-monolithic.jar	638
/VSI_Company_Homepage.html	235
/contactus.html	153
/images/VSI_headquarters.jpg	152
/reset.css	151
/images/web/2009/banner.png	145
/blog/tags/puppet?flav=rss20	114
/projects/xdotool/	70
/?flav=rss20	50

« Prev 1 2 3 4 5 6 7 8 9 10 Next »



Summary and Future Mitigations

Project 3 Summary

- Overall findings from the attack

➢ There was an attack on the Windows Server on March 25th by one or more individuals identified as users A, J & K. During these attacks there were attempts at resetting passwords, a number of these were unsuccessful and resulted in account lockouts, however some resulted in successful logins. This is indicative of a Brute force attack.

➢ During the attack there are a large number of post requests and a high amount of connections relating to the Logstash files. This paired with the absence of successful logins and deleted accounts shows that the log files were potentially altered to cover the tracks of the attackers.

Project 3 Summary

- Future Mitigation suggestions

➢ Recommend setting a limit on the number of login attempts and introducing multi-factor authentication.
➢ Implement NIST password recommendations and reset all passwords.
➢ Continue monitoring the server with the reports and alerts created.
➢ Increase the user privileges on the Logstash or change the file to read-only as to avoid log tampering.