Defensive Security Project

by: Trevor Humphrey, Marnie Spencer, Abby Ringrose, & Heather Simpson

Table of Contents

This document contains the following resources:

01

Monitoring Environment

Splunk

02

Attack Analysis

Windows

Apache

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- In light of the potential of JobeCorp using cybersecurity attacks to negatively impact our business operations here at VSI, as a SOC team of analysts, we were tasked with monitoring both the Windows logs and Apache logs from the VSI servers.
- As a team, we used Splunk to conduct the monitoring, create alerts and reports, and analyze the logs for potentially suspicious activity.
- During the course of our monitoring operations, VSI experienced a cybersecurity attack that caused significant disruption to the VSI systems.
- Luckily, we were able to use this data to analyze the effectiveness of previous security measures and make recommendations that will help shield VSI from further attacks.

Logs Analyzed

1 Windows Logs

The Baseline data showed, well baseline data, showed how the server should be operating on a daily basis.

The attack scenario showed an attack where many accounts got locked in the early morning, later that morning password change attempts were recorded, shortly after that a noticeable bump in account logins was recorded.

The attack was conducted using three main users.

2 Apache Logs

The Baseline data showed how much web traffic there is on a daily basis.

In the attack scenario, the logs showed where and when the attackers accessed the system. What methods were used, referrer domain, IP geolocation

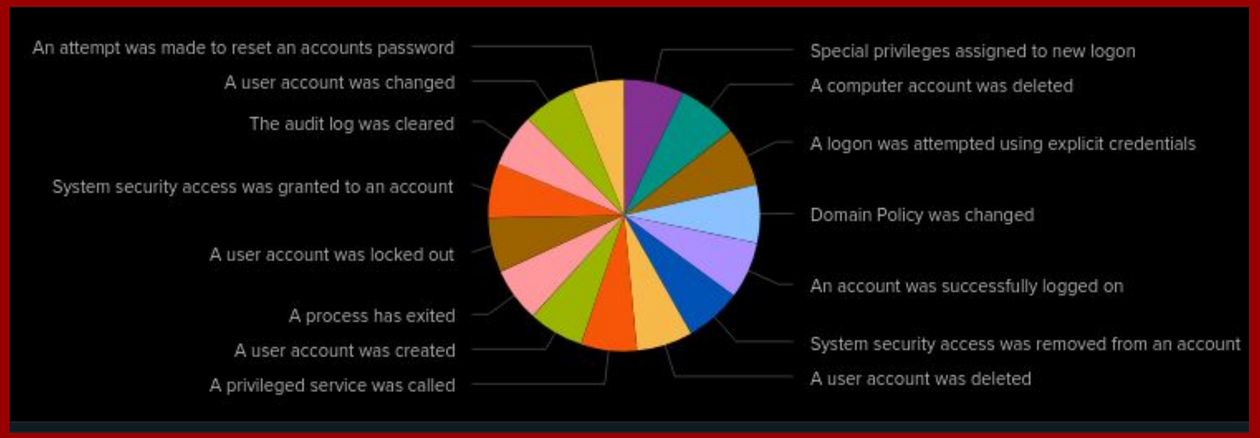
Windows Logs

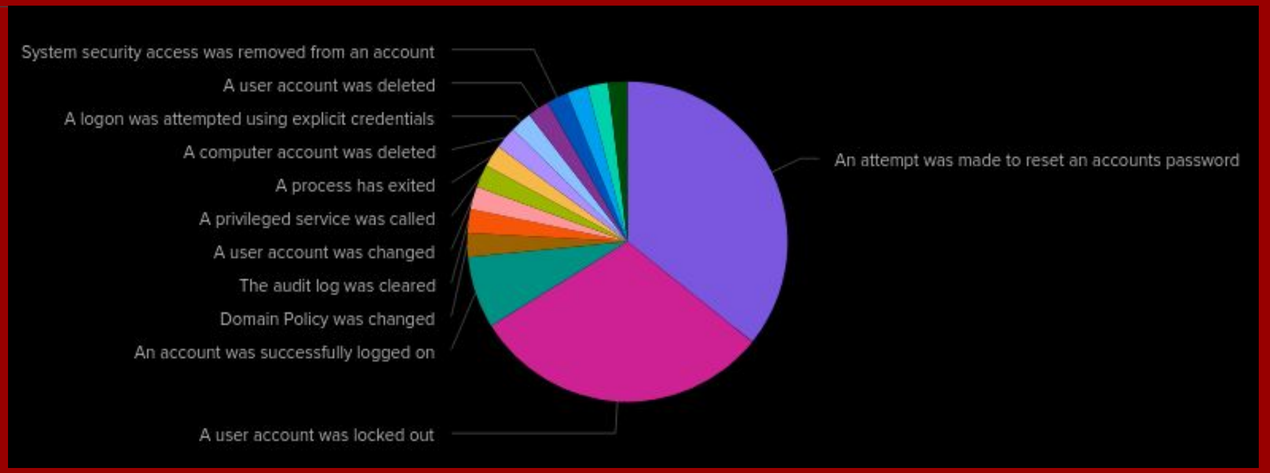
Reports—Windows

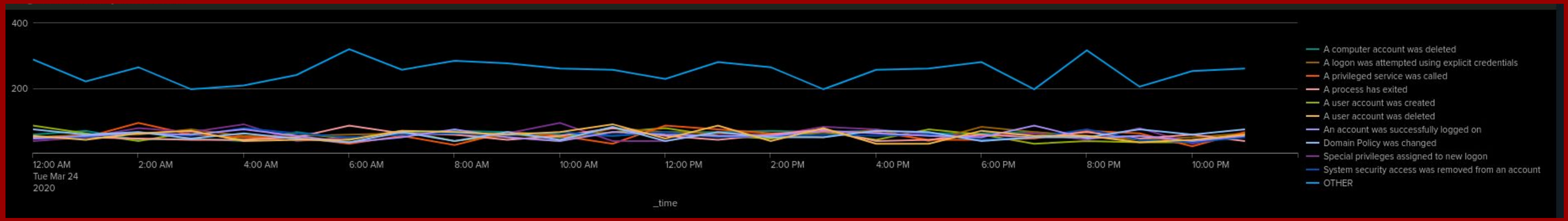
Designed the following reports:

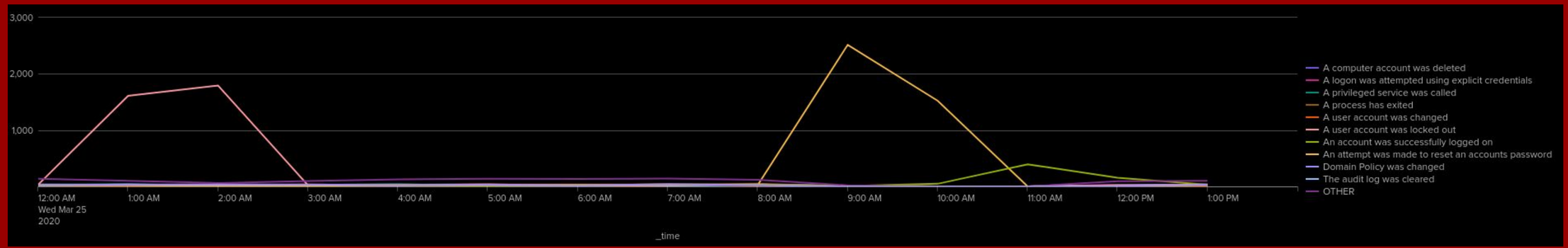
Report Name	Report Description
Signatures and Signature IDs	Shows a table with the highest recorded signature and signature IDs
Top Signatures	Pie graph showing the top signatures
Failure/Success tracker	Table showing failure and success events
Failed Logins	Radial Gauge showing failed events
User Activity	Tracks the usage by user on line graph

Signature Counts Over time Baseline vs. Attack









Images of Reports - Windows

Signature ID Mapping Report

Lists each unique ID and its associated Signature/message. quickly identifiy what a specific signatrure ID refers to.

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

« Prev 1 2 Next »

signature and signature ID

signature_id	signature
4724	An attempt was made to reset an accounts password
4717	System security access was granted to an account
4689	A process has exited
4726	A user account was deleted
1102	The audit log was cleared
4672	Special privileges assigned to new logon
4720	A user account was created
4743	A computer account was deleted
4624	An account was successfully logged on
4738	A user account was changed

Windows Login Success vs Failure Report

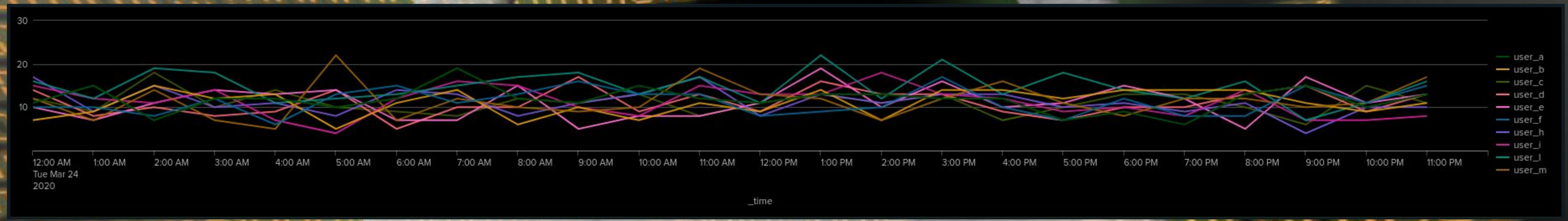
Compares success and failure counts in Windows activites

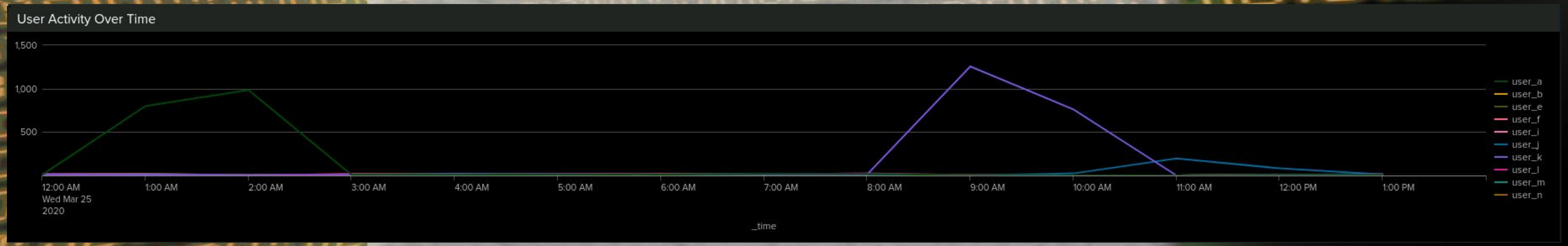
outcome	count	percentage
failure	4441	93.22
success	323	6.78

Windows Login Success vs Failure Report

outcome	count	percentage
failure	5578	93.76
success	371	6.24

Images of Report - Windows





Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	If there is more than the threshold amount of failed logins within an hour, an email will be sent to the SOC team.	The baseline of failures per hour was approximately 400.	The alert threshold is more than 480 failures in an hour.

JUSTIFICATION: The justification for the baseline is an approximate average of the data gathered. The threshold is 20% higher than the baseline.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins	If there are less than 20 successful logins in an hour period, an email will get sent to the SOC team.	The baseline was set to more than 20 successful logins in an hour period.	If there are less than 20 successful logins in an hour period.

JUSTIFICATION: The baseline was approximate average of the successful logins per hour period, and the threshold was anything lower than the average number of logins per hour.

Alerts—Windows

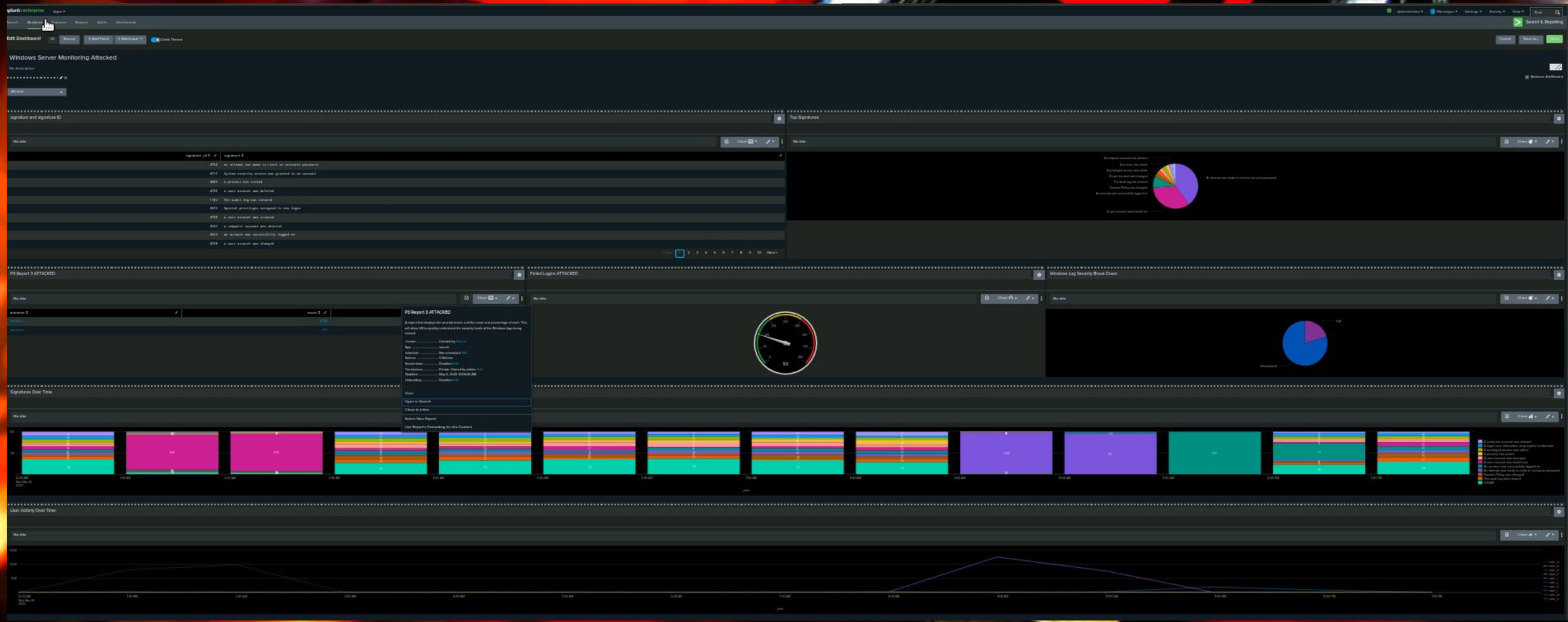
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Deleted User Accounts	If the amount of account deletions drops below 18 in an hour, an email will be sent to the SOC team.	The baseline was 20 account deletions within a one hour period.	If there are less than 18 account deletions within an hour.

JUSTIFICATION: The baseline was the the bottom 10% of average experienced account deletions, so the account threshold was anything lower than the baseline.

Dashboards—Windows Baseline

Dashboards—Windows Attack



Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Request Method	Tracks what type of HTTP method being used.
Top 10 Referer Domain	A table showing the top 10 domains that refer to the VSI website
Count of HTTP Response Codes	A Table showing the count of HTTP response codes

Apache Reports

HTTP Request Summary

Chart

method	clientip	status	count
GET	66.249.73.135	200	420
GET	46.105.14.53	200	364
GET	130.237.218.86	200	288
GET	75.97.9.59	304	174
GET	50.16.19.13	200	113
GET	209.85.238.199	200	102
GET	68.180.224.225	200	95
GET	75.97.9.59	200	93
GET	198.46.149.143	200	82
GET	208.115.111.72	200	82

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Top 10 Referrer Domains to VSI Website

Chart

referer_domain	count
-	4073
www.semicomplete.com	3038
semicomplete.com	2001
www.google.com	228
www.google.fr	46
www.google.co.uk	37
stackoverflow.com	34
www.google.de	31
s-chassis.co.nz	29
www.google.es	29

HTTP Method Count

Chart

status	count
200	9126
304	445
404	213
301	164
206	45
500	3
403	2
416	2

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity by Country	It monitors the hourly activity from any country. Excluding the US	The baseline was set at 60 hits in an hour.	The threshold was set at greater than 130 hit in an hour

JUSTIFICATION: The baseline was set according to the average numbers of hits the system got in an hour.. The threshold was set at 130 because the average threshold range was above 100 but less than 130.

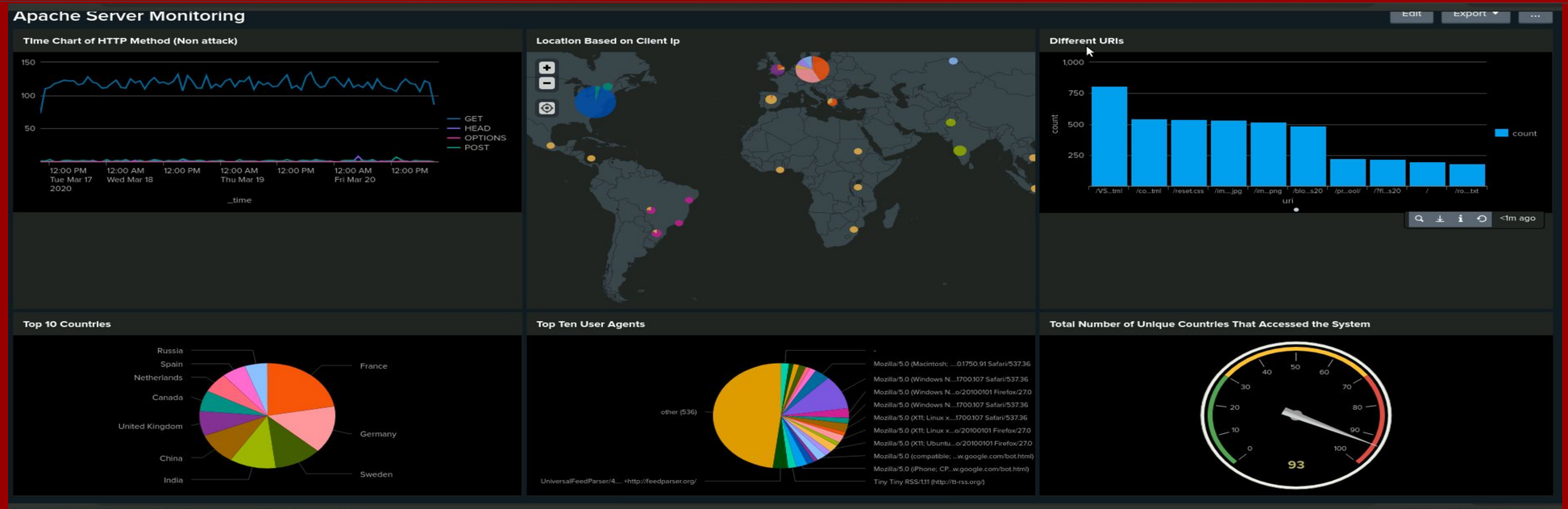
Apache Alerts

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Requests	Designed to send and email to SOC@VSI-company.com if there is a high volume of POST requests.	The baseline was set at 4	The threshold was set at greater then 10 requests in an hour.

JUSTIFICATION: At any given time on any given day the POST requests have not exceeded 10. The baseline of 4 was the approximate average in an hour.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

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

- Signature-based analysis revealed a significant surge in account-related security events during the attack window, with password reset attempts and account lockouts comprising approximately two-thirds of all detected signatures. This pattern marked a clear deviation from baseline behavior and was confirmed by a substantial spike in signature frequency over time.
- User activity analysis identified abnormal account behavior concentrated across three individual user accounts, each showing short-duration activity spikes. Concurrently, overall user activity across the environment decreased, suggesting a targeted engagement or potential account misuse during the attack period.
- Windows event log severity levels escalated from a baseline average of ~7% to over 20% during the observed attack timeframe, indicating a heightened volume of high-risk or critical events correlating with malicious activity

Attack Summary—Windows

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

Upon inspection of the attack logs, we determined that:

- The threshold for failed logins was within a reasonable range to catch the attack and provide alerts.
- The threshold for successful logins that we originally set would not have captured and alerted in the event of this attack, so we had to adjust the alert criteria for future attacks of similar parameters.
- The threshold for account deletions that we originally set would not have captured and alerted in the event of this attack, so we had to adjust the alert criteria for future attacks of similar parameters.

Attack Summary—Windows

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

- Based on the evidence in the logs, we were able to determine that the attackers attempted a brute force attack between 1:00 am and 2:00 am on March 25, 2020.
- The attack was then continued and activity spiked between 9:00 am and 10:00 am on March 25, 2020, the attackers attempted to change passwords.
- Following the attempt to change passwords we did see a spike in successful logins indicating the attackers did have some success at changing passwords and getting into the server network, this event occurred at 11:00 am on March 25, 2020
- Three use accounts were used in this attack event.

Attack Summary—Apache

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

- Using HTTP methods we were able to determine how much activity, date and time, and what kind of methods were being requested.
- On 3/25/2020 at 8pm there was a spike in 200 HTTP response codes. 1,296 were POST requests indicating a brute force attack.
- When analyzing the referrer domains and we found that there was a domain logstash.net. Logstash is a tool used to collect and process logs from different systems and websites. logstash.net isn't actually the domain. elastic.co/logstash this the actual domain. This domain logstash.net is a way to make malicious request appear legitimate.

Attack Summary—Apache

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

- On March 25, 2020 at 8PM there was spike in international activity.
- On March 25, 2020 at 12AM there was an uptick in POST requests that didn’t taper off till 10PM. With the highest amount being at 8PM with 1415 requests in an hour.

Attack Summary—Apache

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

- On the day of the attack there was a lot of activity in Ukraine. 444 in Kiev and 433 in Kharkiv.
- Upon analyzing the logs from March 25, 2020 there was 1,323 POST requests to VSI_Account_logon.php.
- There was an uptick in GET requests leading up to the attack then a major spike in POST requests during.

Summary and Future Mitigations

Windows Summary & Future Mitigation Recommendation

- In the early morning hours, the attackers were able to use a brute force attack to gain access to the server and lock server user accounts; presumably by utilizing admin rights on the server. They were able to continue using a denial of service attack. Several hours later, they attempted to reset the passwords to a large volume of user accounts. They were able to login to about 10% of those user accounts. This was accomplished mainly by three user accounts.

Future Recommendations

- Ensure the implementation of load-balancing with replication to efficiently ensure redundancy in the server functionality.
- An overall recommendation would be more strictly enforced password requirements as well as the usage of multi-factor authentication.
- To protect VSI from future attacks we identified two additional alerts that should be implemented for Windows:
  - Adjust for successful logins that are greater than the baseline login.
  - Adjust for account deletions that are higher than the baseline number of account deletions.