Defensive Security Project
by: I am Root

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

Virtual Space Industries (VSI) has been cyber attacked by JobeCorp. Our team (SOC analysts), were tasked to monitor VSI's admin webpage, apache web server, and windows OS.

The team was provided with past logs to help create reports and develop baselines for alerts.

[“Add-On” App]

Website Monitoring

The add-on chosen was Website monitoring. In order to keep VSI site healthy, a website monitoring add-on is needed.

Website Monitoring

Benefits of website monitoring for VSI would help quickly detect downtime and performance problems. The add-on helps support a smooth running system by alerting VSI when the site crashes or a data breach occurrence that could compromise the company and its customers.

Website Monitoring

title	url
VSI-corporation.azurewebsites.net	https://vsi-corporation

Modify the definition of a failure

response	last_checked	response_time	status	a
✓ 200	3 minutes ago	315 ms	OK	

Logs Analyzed

1 Windows Logs

A log of recorded events from a Windows Server on Domain_A, including detailed information on each event signature.

2 Apache Logs

These logs are detailed log entries that record HTTP requests made to the Apache server

Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Signatures and associated signature ID	Allows VSI to view reports on ID numbers associated with specific signature for windows activity
Severity levels	allows VSI to understand severity levels of windows logs viewed
Status	Shows VSI if there is any suspicious amount of failed activities on their server

Images of Reports—Windows

signatures and associated signature IDs

Edit | Export | ...

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

<1m ago

New Search

Save As ▾ | Create Table View | Close

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv"| top limit=20 status
```

All time ▾

✓ 4,764 events (before 2/3/23 2:59:12.000 AM) | No Event Sampling ▾ | Job ▾ | Smart Mode ▾

Events | Patterns | Statistics (2) | Visualization

20 Per Page ▾ | Format | Preview ▾

status	count	percent
success	4622	97.019312
failure	142	2.980688

Severity Level

severity	count	percent
informational	4435	93.094039
high	329	6.905961

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Deleted Account Win Event Alert	Alert triggers when threshold for deleted accounts per hour has been reached	7	22

JUSTIFICATION: Based on the provided dataset, reaching 22 4726 (account deleted) events in an hour should prompt SOC notification.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Login Threshold	Alert triggers when threshold for logons per hour is reached	10	20

JUSTIFICATION: Based on the provided dataset, reaching 20 failed windows events in an hour should prompt SOC notification.

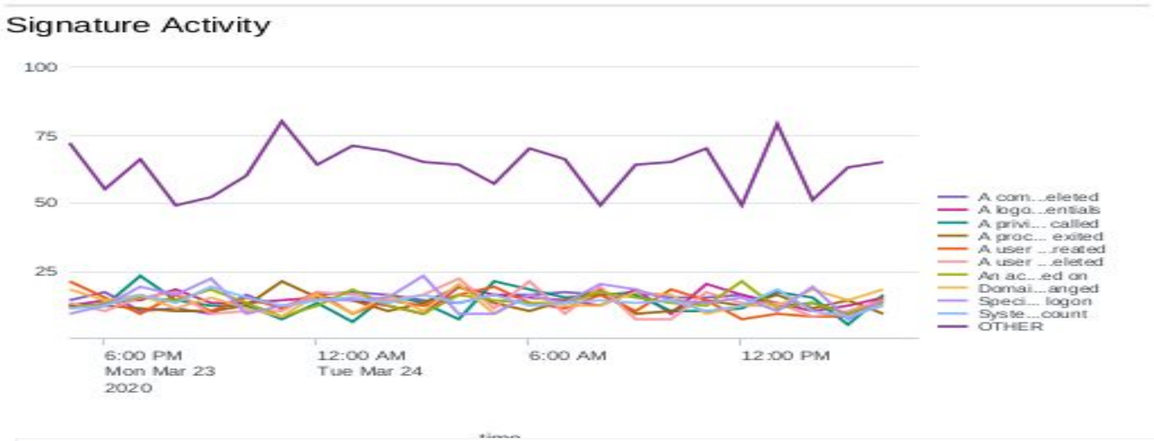
Alerts—Windows

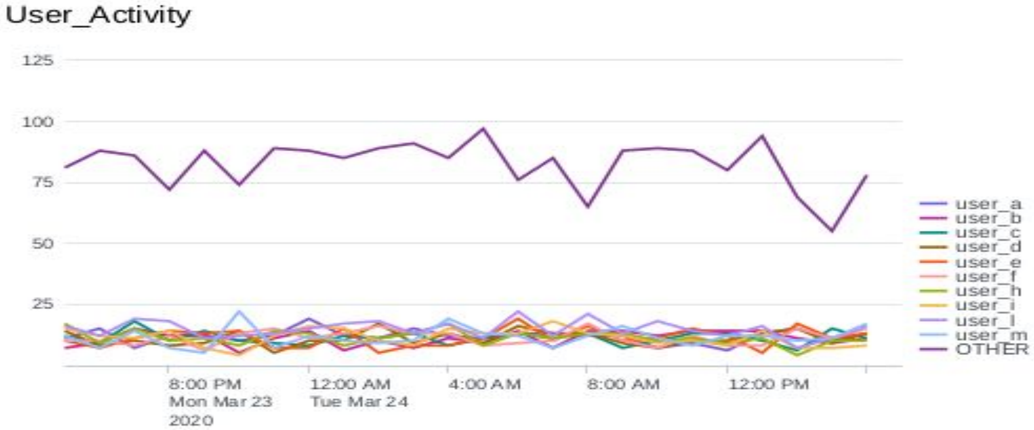
Designed the following alerts:

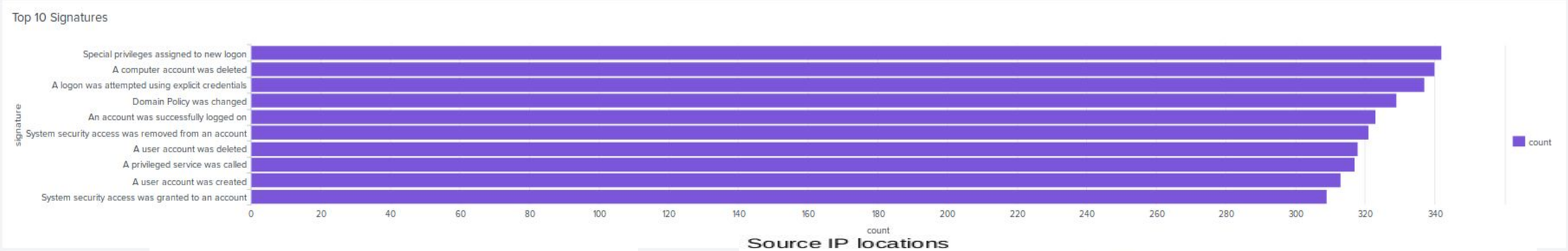
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Events	Threshold set for failed windows events in one hour	3	10

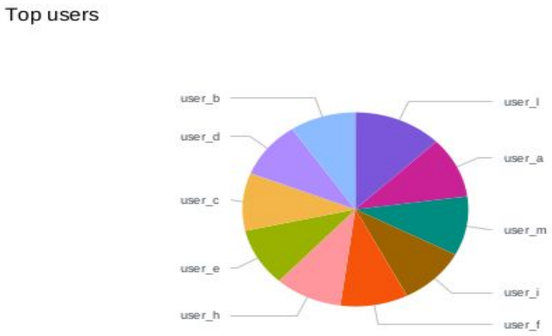
JUSTIFICATION: Based on the provided dataset, reaching10 failed windows events in an hour should prompt SOC notification.

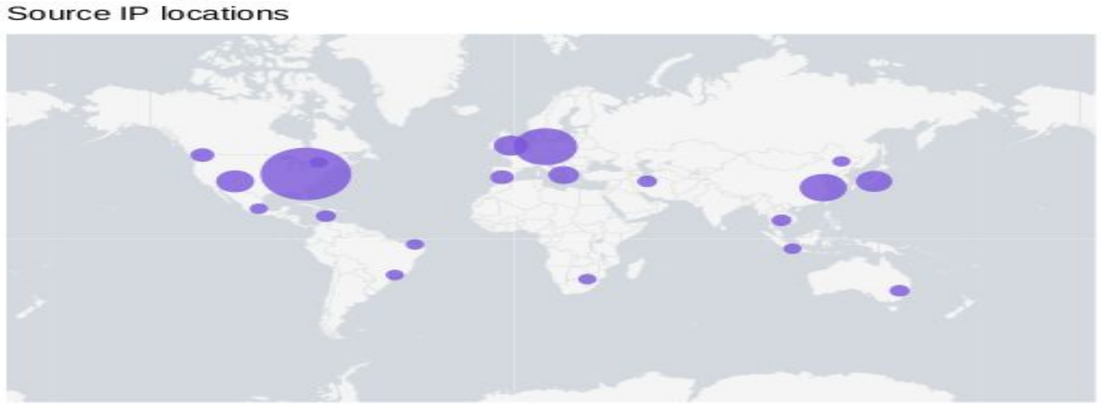
Dashboards—Windows



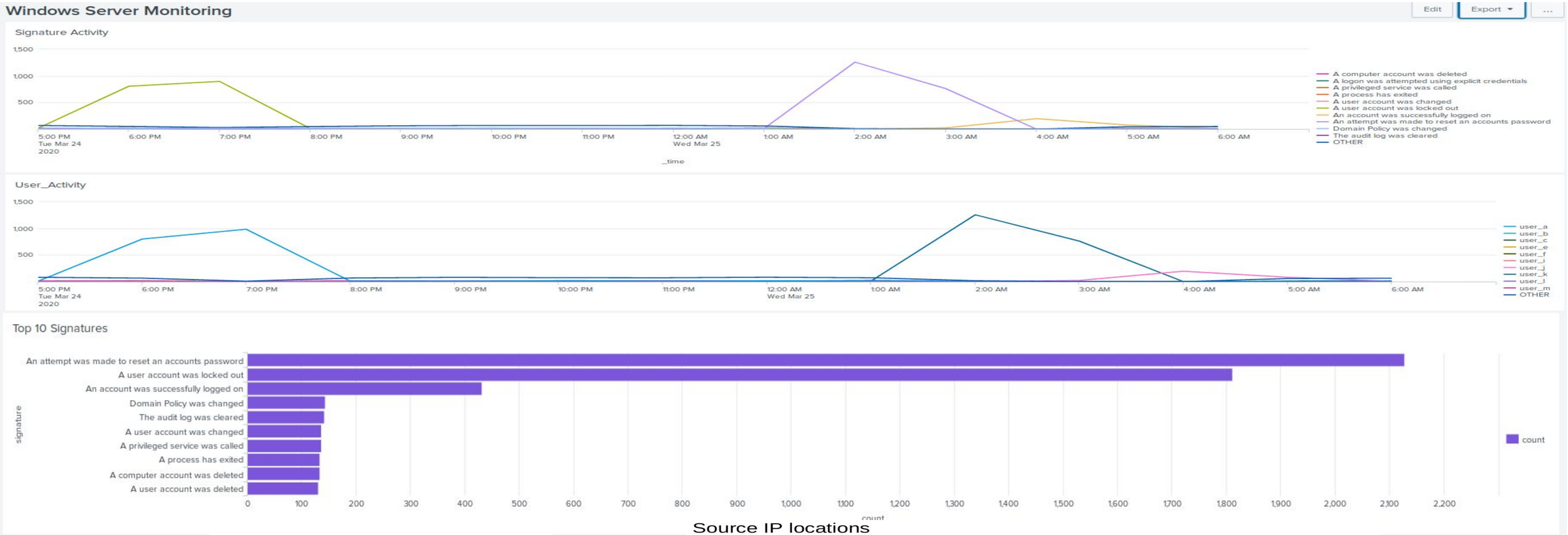




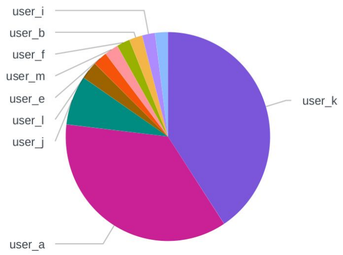




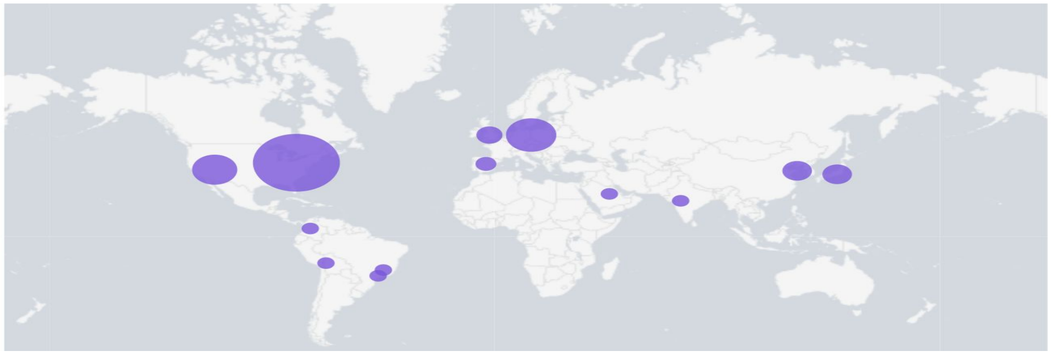
Dashboards—Windows



Top users



Source IP locations



Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP methods	provides insight into the type of HTTP activity being requested against VSI's web server
Top 10 domains	Helps VSI identifying suspicious referrers
HTTP response code count	insight on any suspicious levels of HTTP responses

Images of Reports—Apache

Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

11 Reports

All | Yours | This App's

filter

i	Title	Actions		Next Schedu
>	Brute Force Attack	Open in Search	Edit	2023-02-09
>	HTTP Methods	Open in Search	Edit	None
>	HTTP response code count	Open in Search	Edit	None
>	POST REQUESTS	Open in Search	Edit	None
>	Post_Request_Monitor	Open in Search	Edit	None
>	Requests by Country	Open in Search	Edit	None
>	Severity Levels	Open in Search	Edit	None
>	Signature - ID number	Open in Search	Edit	None
>	Success vs. Failure	Open in Search	Edit	None
>	TOP 10 URI_PATHS	Open in Search	Edit	None
>	Top 10 domains	Open in Search	Edit	None

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Monitoring Foreign Activity	This alert is designed to send out an alert when there is a suspicious number of users from a foreign country	10 requests per hour	The alert is triggered at more than 20 requests per hour from a foreign country

The Reason for this alert is because our services are not often used in other countries so when we get an increase of traffic from one we need to make sure it is not with malicious intent.

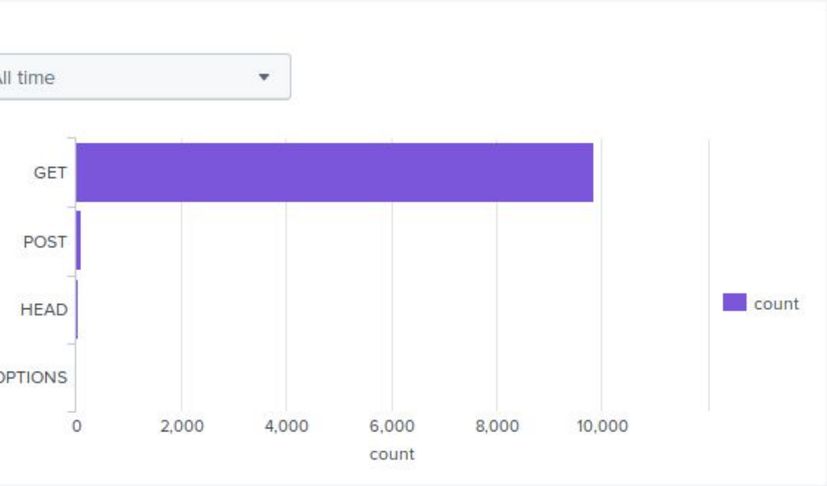
Alerts—Apache

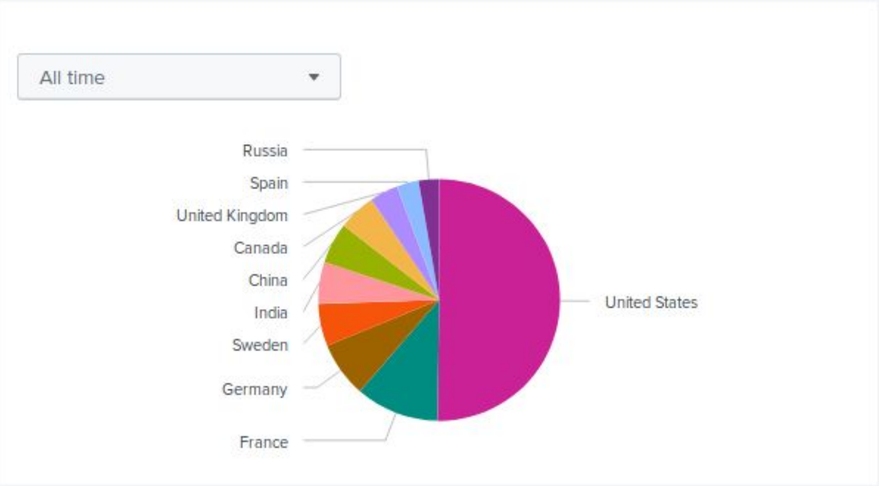
Designed the following alerts:

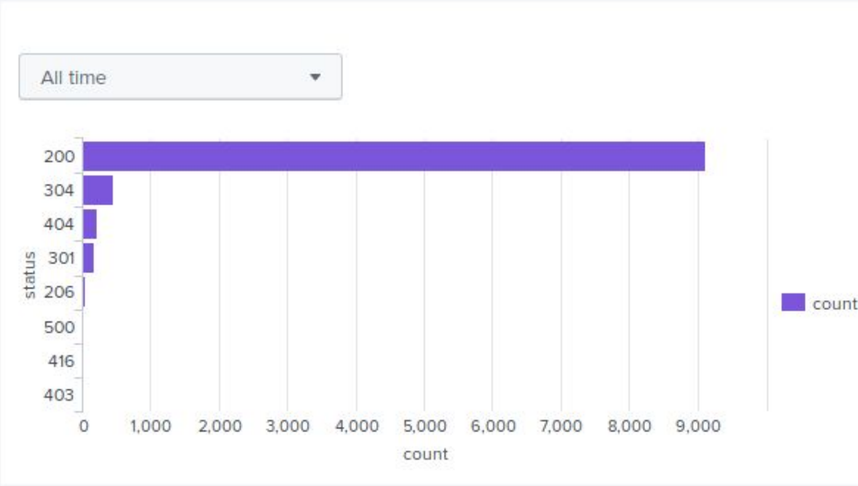
Alert Name	Alert Description	Alert Baseline	Alert Threshold
POST-UP	This alert is designed to trigger when more than 5 POST requests are made in an hour.	2 POST requests an hour	5 POST requests in an hour

The reason we have this alert in place is because POST requests upload files to our site. If they are not properly monitored a bad actor can use this to upload malicious code such as reverse shells.

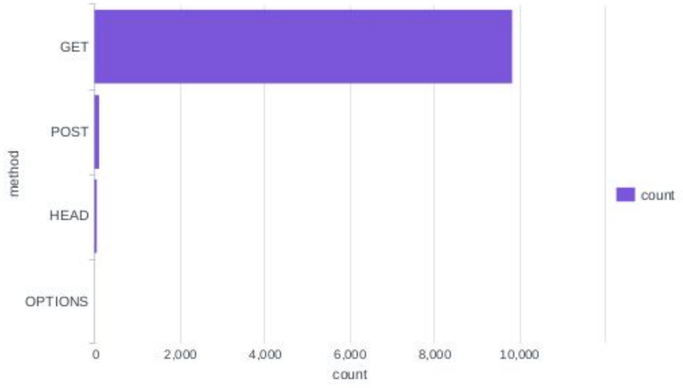
Dashboards—Apache







Dashboards—Apache

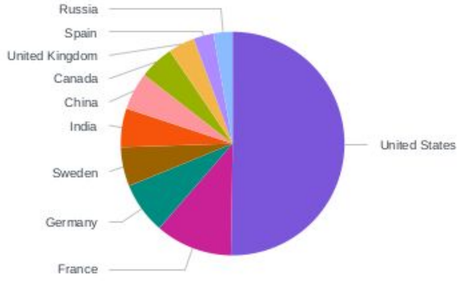


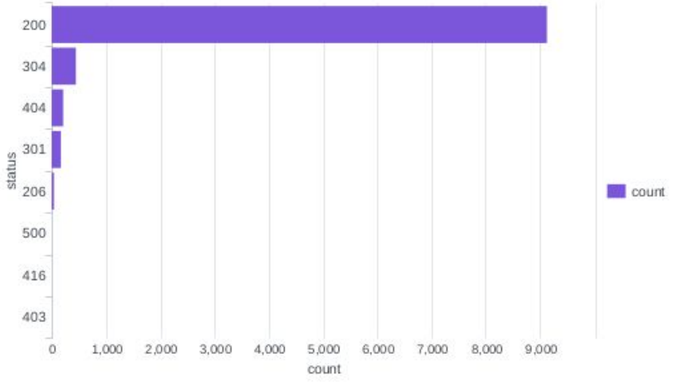
splunk>

ApacheReport

2023-02-08 01:49:13 UTC

Page 1





splunk>

ApacheReport

2023-02-08 01:49:13 UTC

Page 2

Attack Analysis

Attack Summary—Windows

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

signature	count
An attempt was made to reset an accounts password	2128
A user account was locked out	1811
An account was successfully logged on	432
Domain Policy was changed	143
The audit log was cleared	142
A user account was changed	137
A privileged service was called	136
A process has exited	134
A computer account was deleted	133
A user account was deleted	130
A logon was attempted using explicit credentials	129
System security access was removed from an account	128
Special privileges assigned to new logon	127
System security access was granted to an account	123
A user account was created	114

Attack Summary—Windows Part 2

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

In summary, the attackers were successful in logging into some user accounts and changing the Domain Policy.

New accounts were made and given special and security privileges, while pre-existing accounts were stripped of security permissions.

Attack Summary—Windows

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

- No alerts for logon failures triggered.
- 393 counts of suspicious logins with User_A being the main culprit from 1AM to 10AM.
- 133 accounts were deleted triggering our alert.

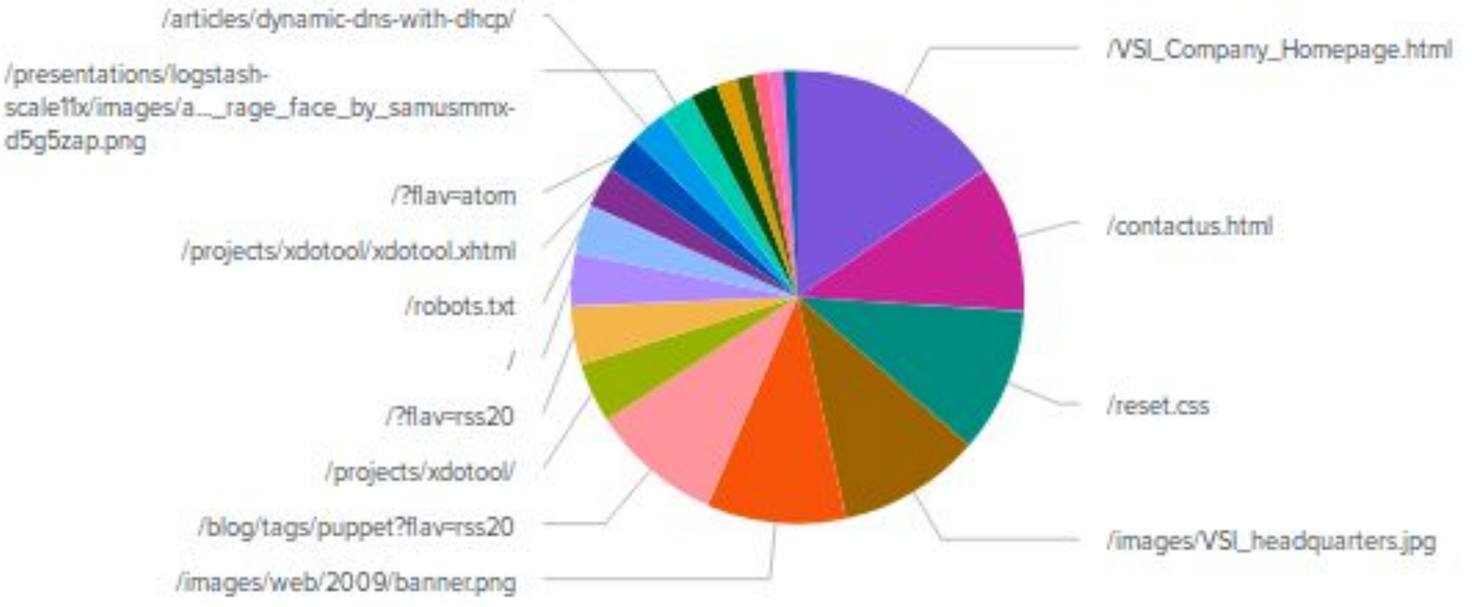
Attack Summary—Windows

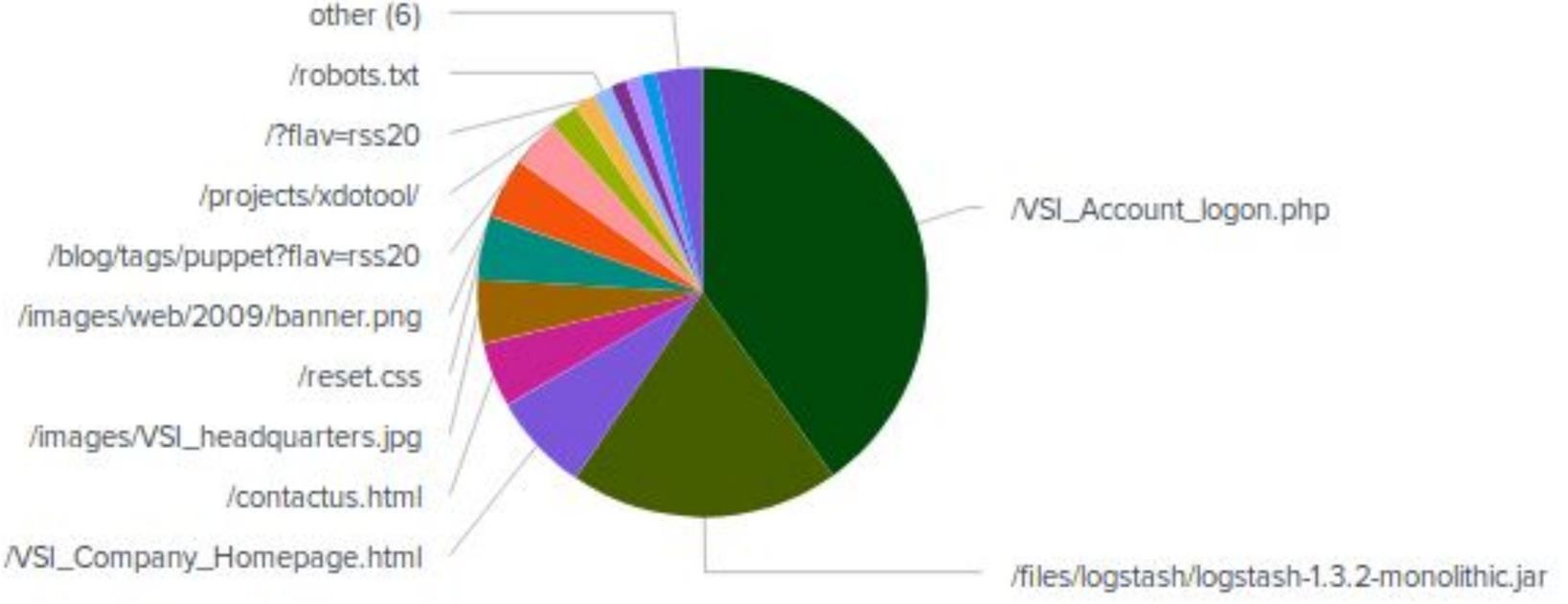
Summarize your findings from your dashboards when analyzing the attack logs.

- The dashboard indicates that two users stood out after reviewing the attack logs: user_k, with a 40.746% count, and user_a, with 36.129%. Additionally, user_j was also noticeable with 7.657%, higher than the remaining users.
- The signature activity and top 10 analysis show that user_a caused the most user account lockouts, with a count of 896 peaking at 7PM. This event was from 5 PM - 8 PM on March 24th, 2020. User_k tried resetting passwords from 1 AM - 4 AM with a count of 1,258 peaking at 2:00 AM on March 25th. User_j was successful in logging on with 196 counts, peaking at 4:00 AM. This event was from 3 AM - 6 AM on March 25th.

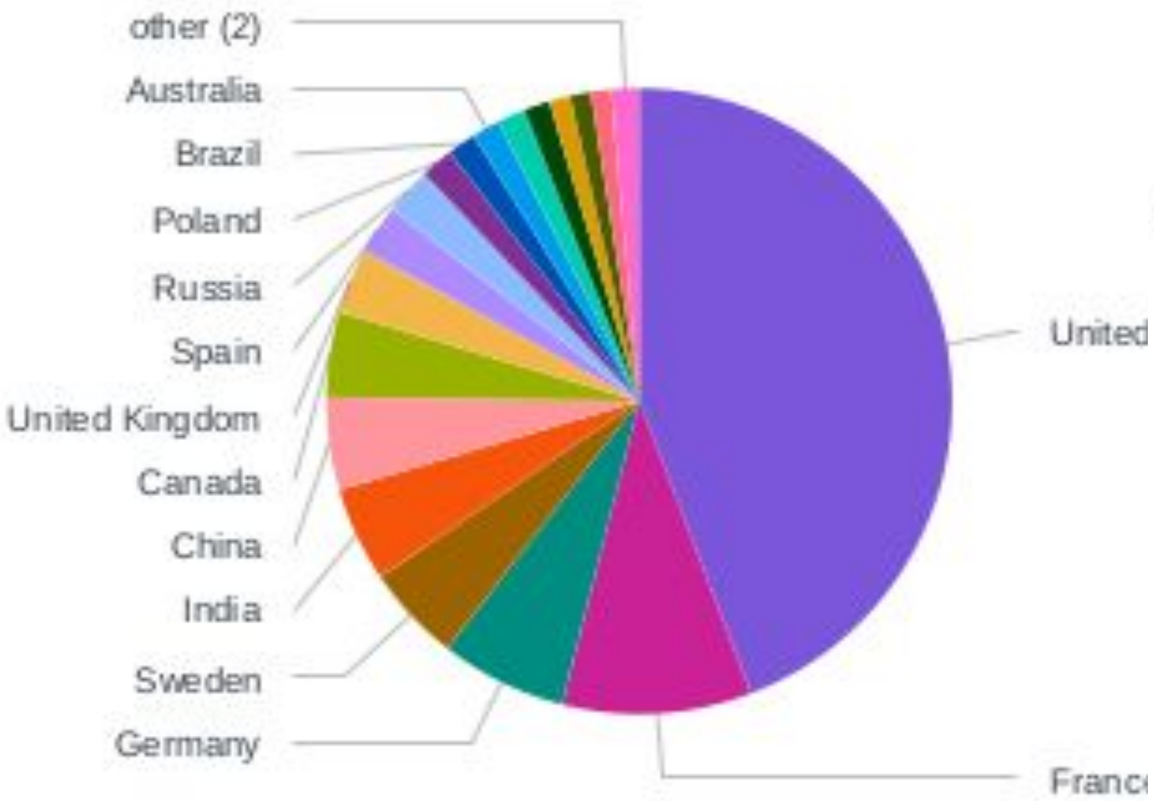
Attack Summary—Apache

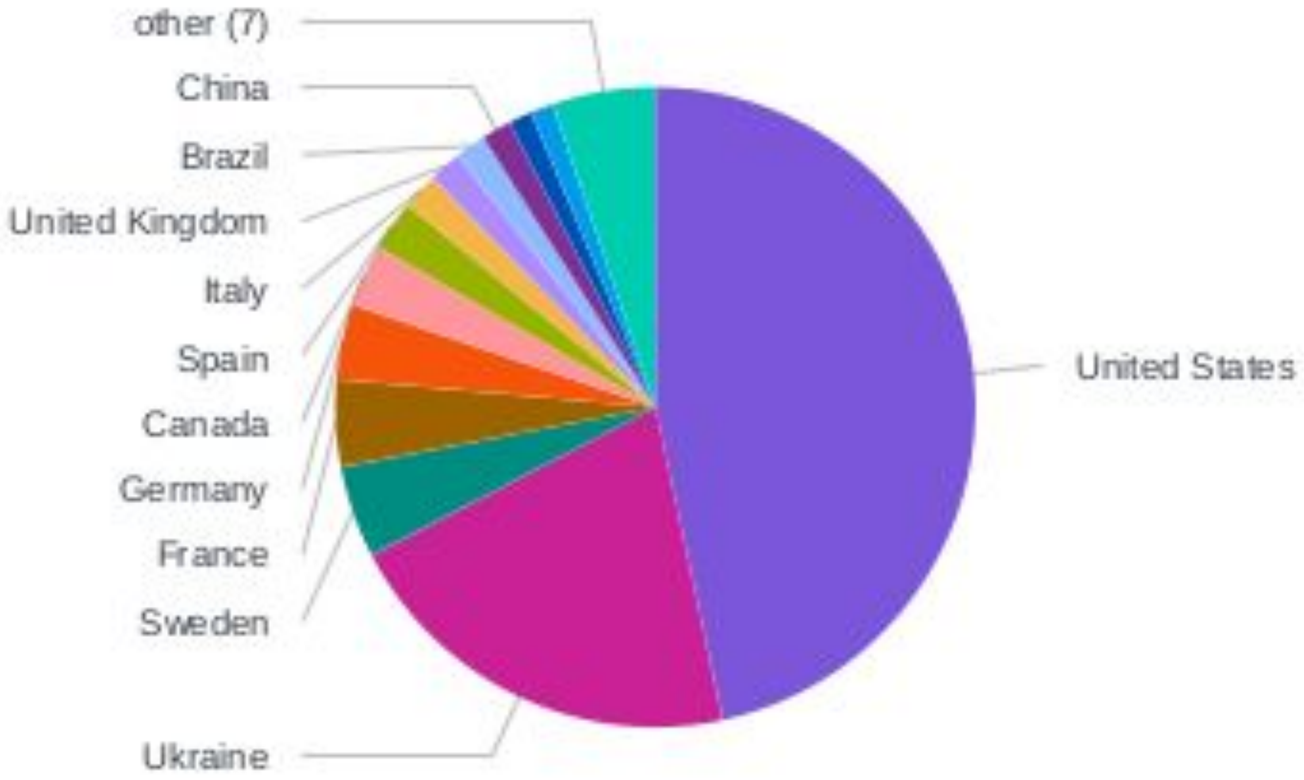
- Overall POST requests in the attack logs were at 29%- a 28% jump in the time period but the majority of requests happened on March 25 around 8pm
- The response code 404 increased from 1% to 15%
- Overall traffic from Ukraine increased from .9% up to 19.5% with a majority of that traffic happening March 25 around 8pm.
- On closer inspection Kiev and Kharkiv each had ½ of the total POST requests
- The top URI in the attack logs is /VSI_Account_logon.php


/articles/dynamic-dns-with-dhcp/
/presentations/logstash-scale1fx/images/a..._rage_face_by_samusmmx-d5g5zap.png
/?flav=atom
/projects/xdotool/xdotool.xhtml
/robots.txt
/
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/VSI_Company_Homepage.html
/contactus.html
/reset.css
/images/VSI_headquarters.jpg


other (6)
/robots.txt
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/reset.css
/images/VSI_headquarters.jpg
/contactus.html
/VSI_Company_Homepage.html
/VSI_Account_logon.php
/files/logstash/logstash-1.3.2-monolithic.jar

Attack Summary—Apache





Attack Summary—Apache

an	Bangladesh	Brazil	Germany	India	Iran	Iraq	Mexico	OTHER	Ukraine
									432
									432

Summary and Future Mitigations

Project 3 Summary

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

  Overall, the attackers were successful in their exploit. It appears the attackers may have used a brute force attack given the elevated login attempts observed through our SIEM platform.

- To protect VSI from future attacks, what future mitigations would you recommend?

  Create alternate servers and data centers to to keep the company in a running-state during future attacks.