Defensive Security Project
Team Apex Cybersecurity

Masta Wuu
Vinblazer
Nump

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Virtual Space Industries(VSI) has hired us to identify and mediate suspected attacks
- VSI suspects that their main competitor JobeCorp is behind attacks
- Our main tool at our disposal is Splunk

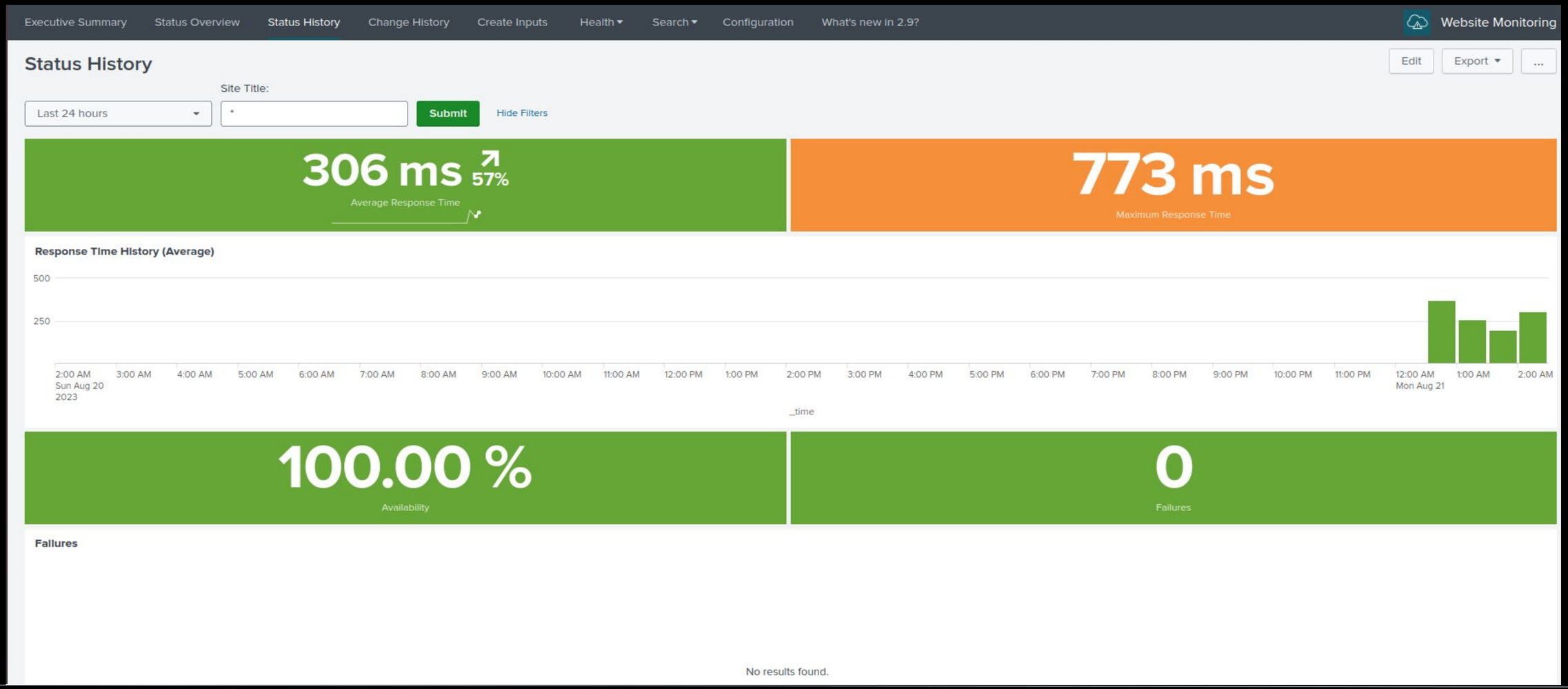
There are 3 main components that VSI have Tasked us to observe and protect

- Admin webpage
- Apache web server
- windows operating system that runs VSI back end ops

Website Monitoring App

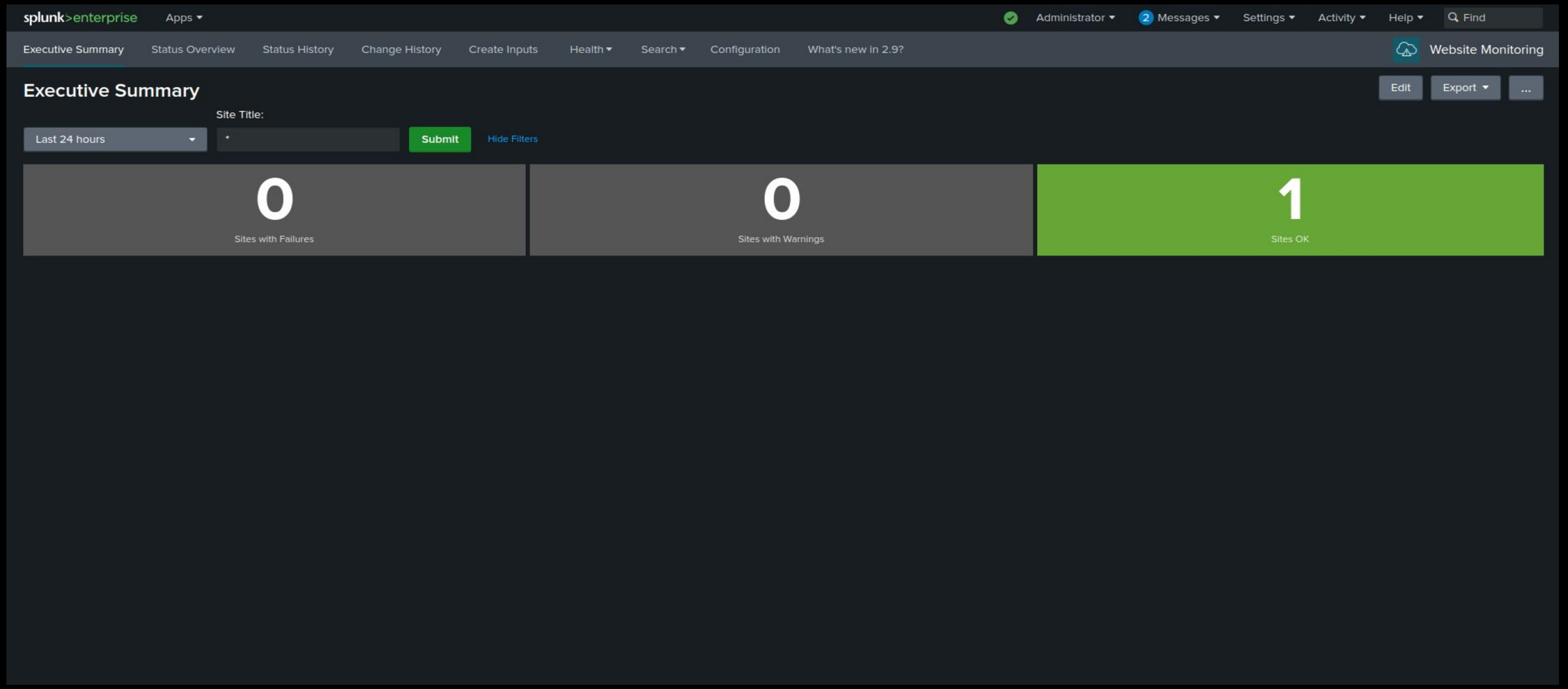
Website Monitoring

This app will ping a website periodically to check if its up or down and measure its availability.

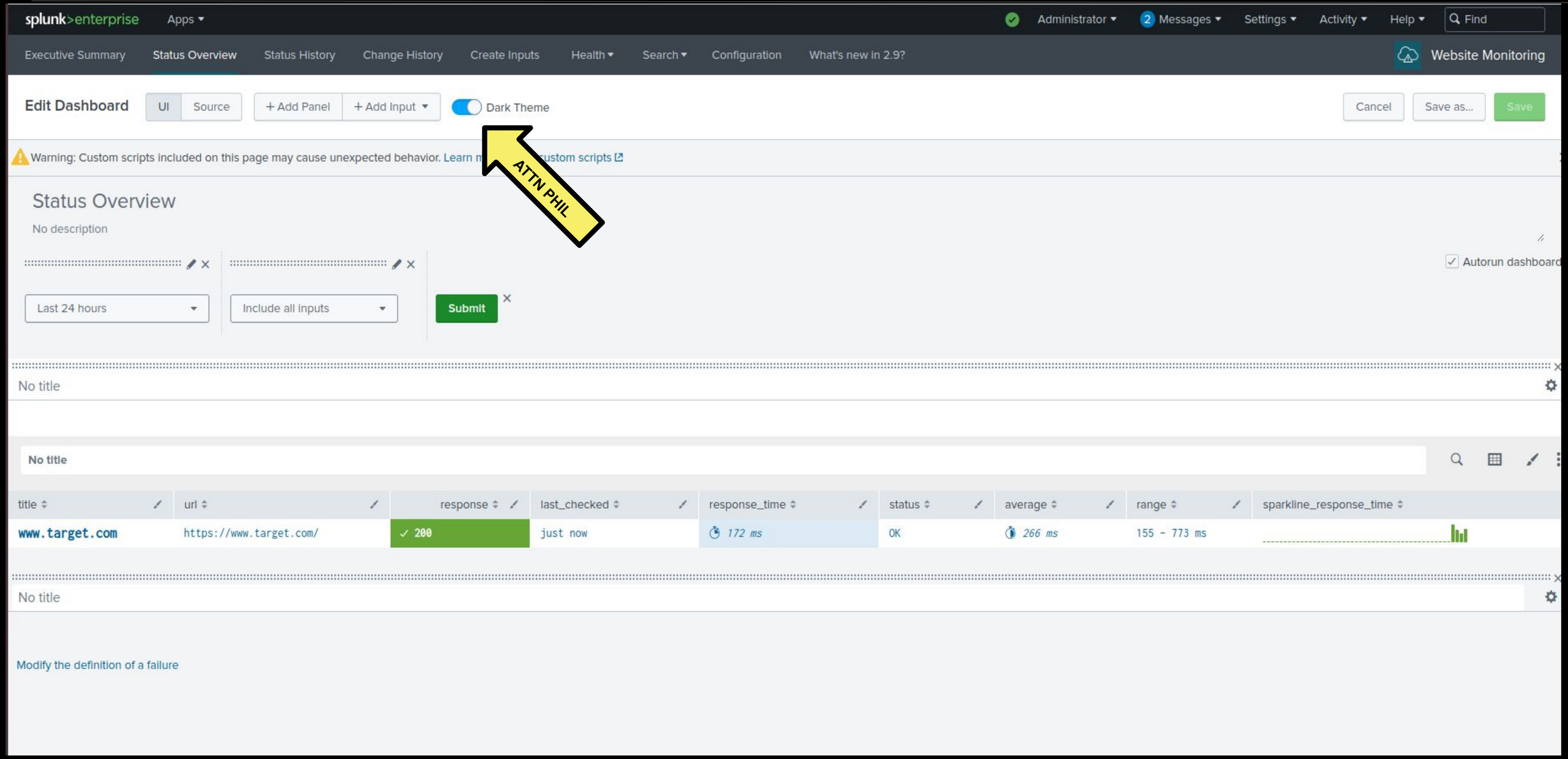


Website Monitoring

This app has the ability to track multiple sites. We only input one site and those results are shown below.



Website Monitoring



Logs Analyzed

1

Windows Logs

The Windows Logs contain user login attempts to the server.

2

Apache Logs

Apache Logs contain information on website traffic and HTTPS methods used on web server.

Windows Logs

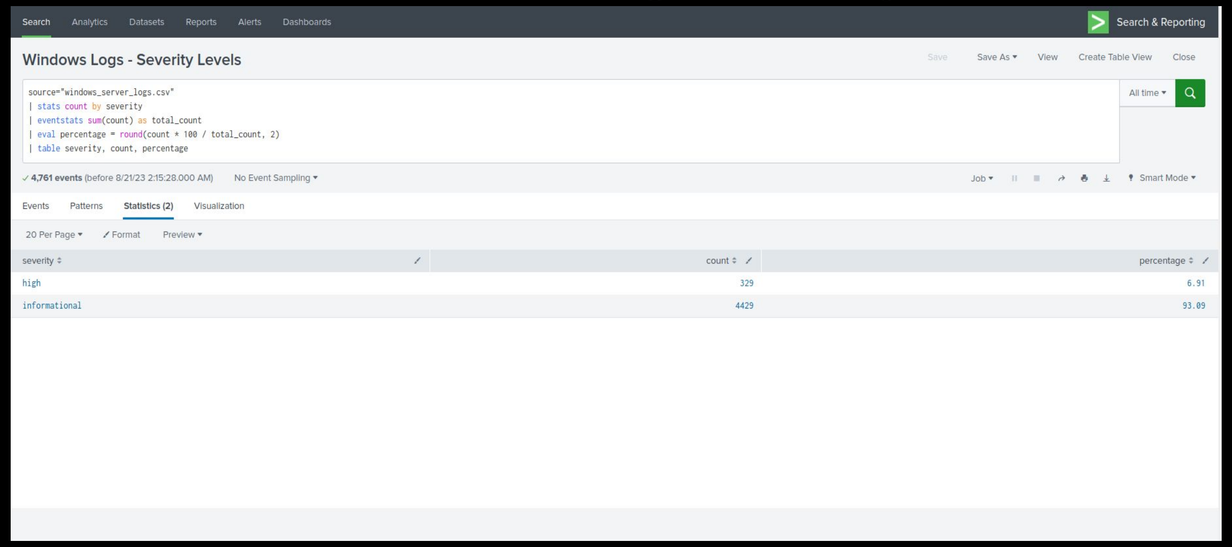
Reports—Windows

Designed the following reports:

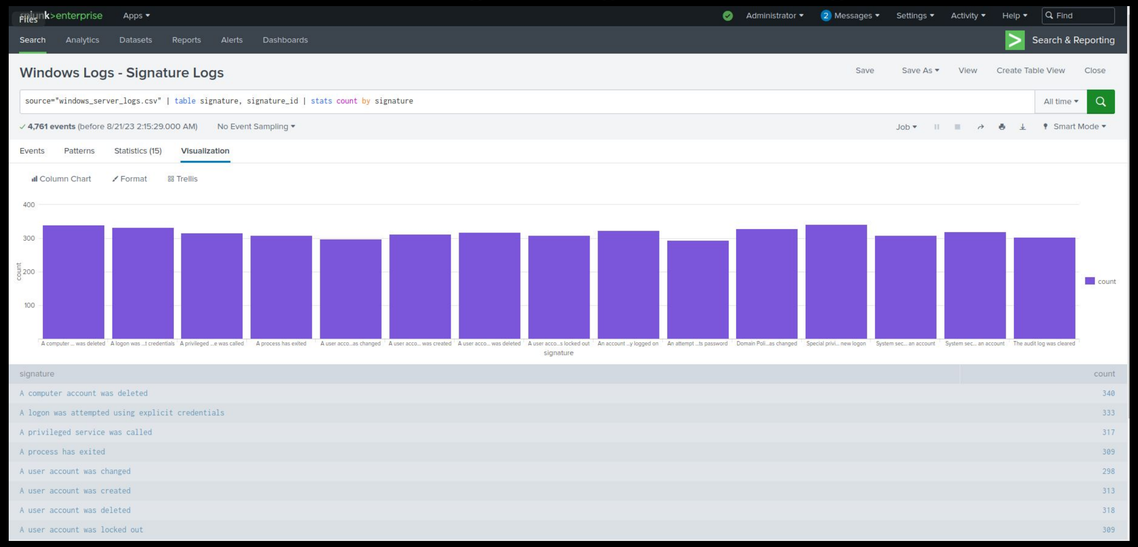
Report Name	Report Description
Windows Severity Levels	Details the percentage of high severity level versus informational severity level.
Windows Signature Logs	Details the amount of signature logs that were generated (A user account was created / deleted, etc).
Windows Success & Failure Comparison	Details the amount of failed and successful windows activities.

Images of Reports—Windows

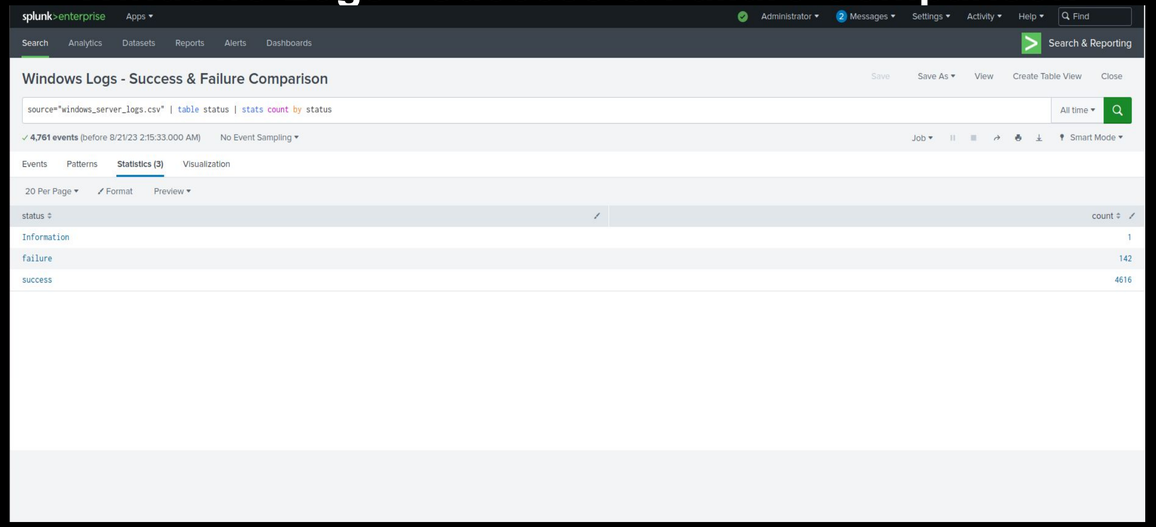
Windows Logs - Severity



Windows Logs - Signature Logs



Windows Logs - Success & Failure Comparison



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Logs - Event 4726	Details Accounts Deleted	Between 7 and 10	12

JUSTIFICATION: We saw fluctuations in accounts deleted ranging between 7 and 10 per hour with spikes that ranged from 15 to 21. As a result we moved to place our baseline at 12 to avoid alert fatigue.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Logs - Event Code 4624	Successful Login	8-13	15

JUSTIFICATION: The majority of the successful logins per hour were between 8 and 13. As a result we set our threshold to 15 to avoid alert fatigue.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Logs - Failed Attempts	Failed Password Reset Attempt	4-7	10

JUSTIFICATION: The majority of the failed password attempts were between 4 and 7 per hour. We decided that an alert threshold of 10 would be the best option.

Windows Server Monitoring Dashboard

Windows Server Monitoring Logs

Windows Server Monitoring - Severity Levels

Severity Level
Informational
4,429

Severity Level
High
329

Windows Server Monitoring - Signature

Signature Alerts

Successful Logins
323

Signature Alert
User Account Locked ...
309

Signature Alert
User Account Dele...
318

Windows Logs - Signature Status

Signature Status
Success
4,616

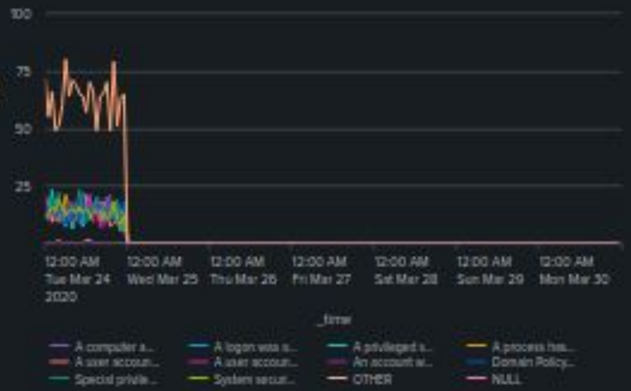
Signature Status
Failures
142

Trending User Activity

The following line chart displays the count of user activities over the duration of the filtered timeframe

Trending Signature Activity

The following line chart that displays the various signatures that occurred over the duration of the filtered time frame

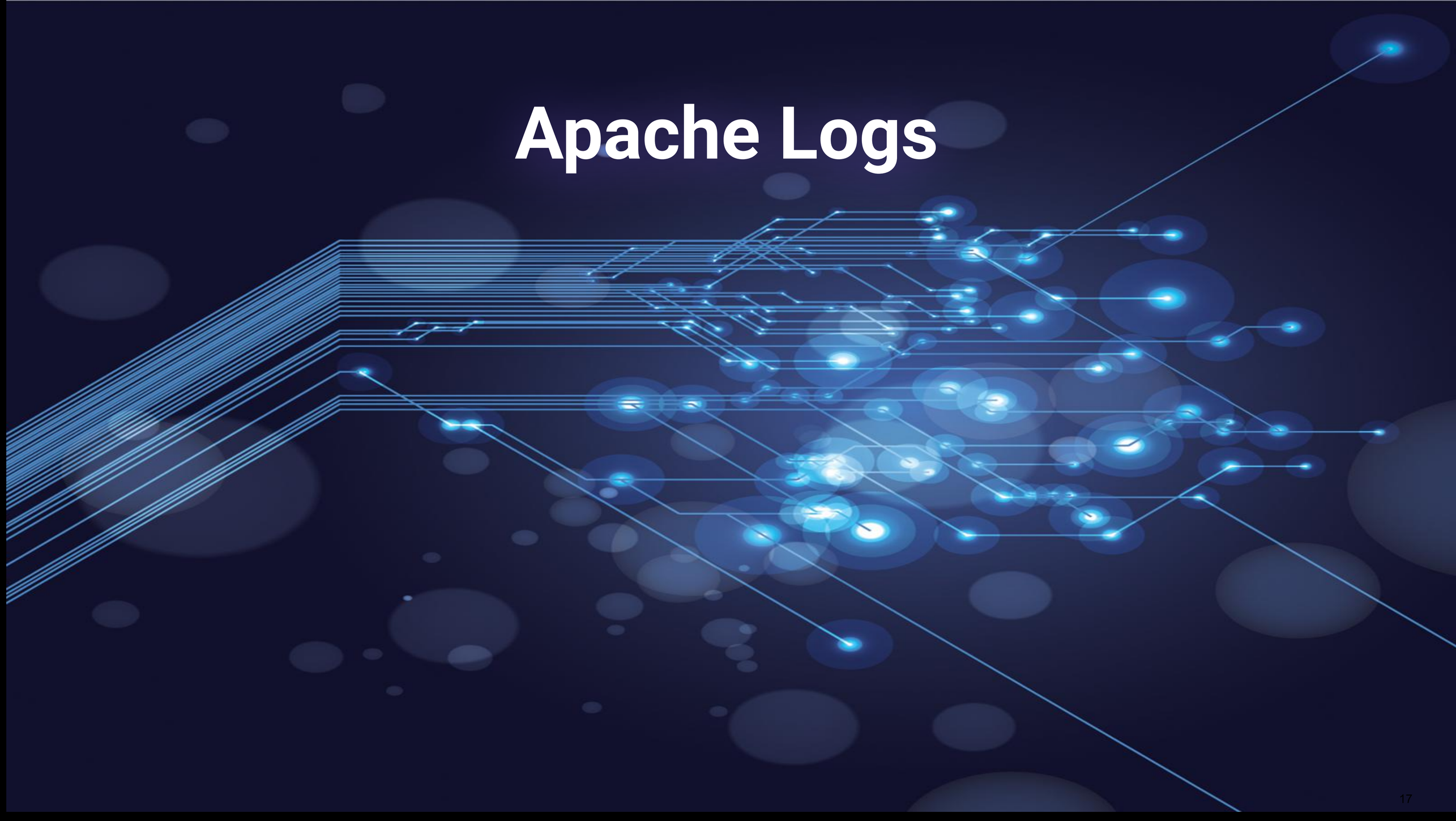


Windows Server Monitoring - Users

user	count
19abz	1
1Girlclumenta	1
1literofvodka	1
ACME-002	1
Alansari42	1

‹ Prev 1 2 3 4 5 ... Next ›

Apache Logs

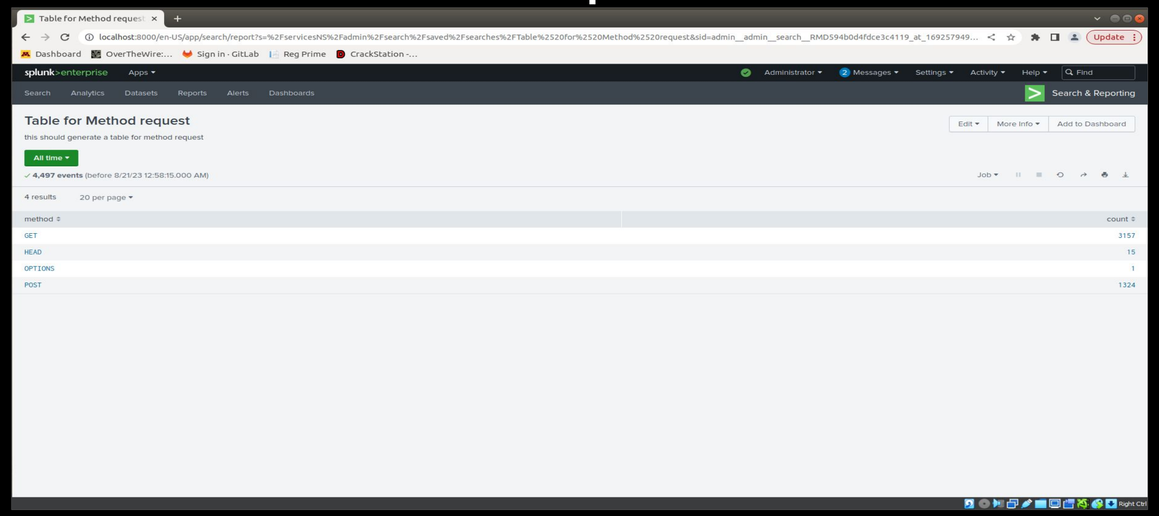


Reports—Apache

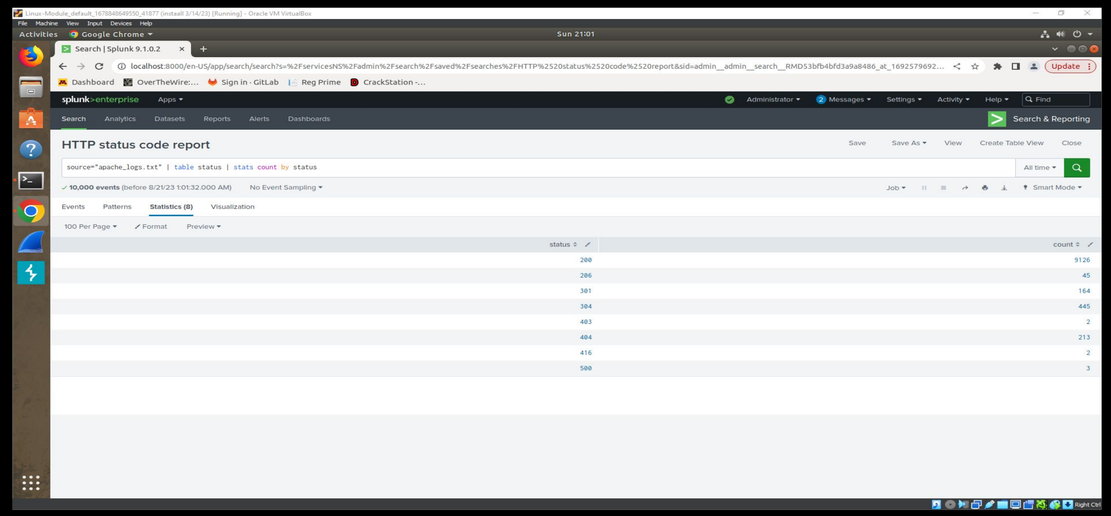
Report Name	Report Description
HTTP Status Code Report	Details the count of status codes
Table for Method Request	Details the different types of status codes
Top 10 Domains	Details the top ten Domains that refer to VSI’s website

Images of Reports—Apache

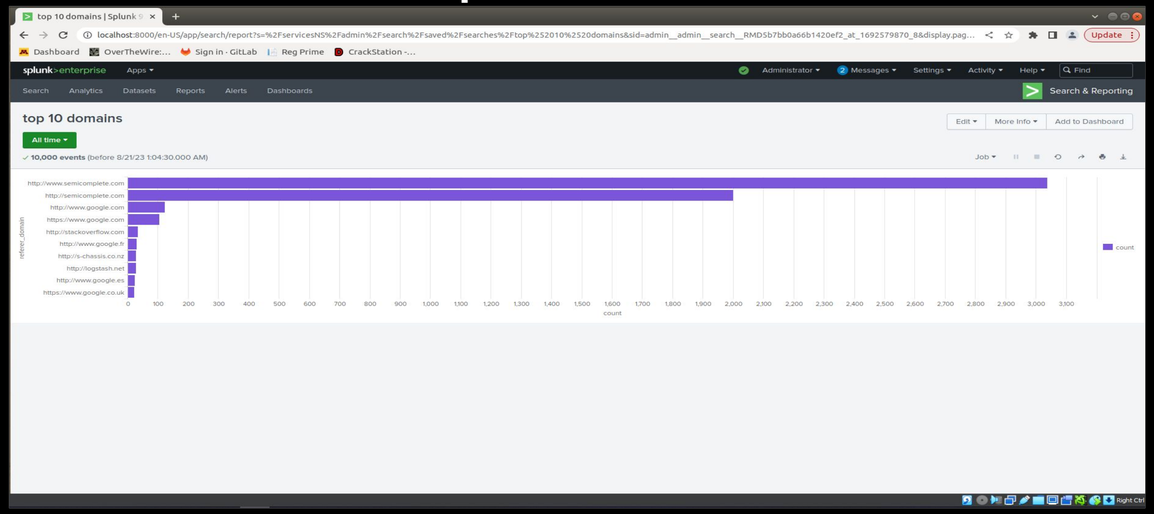
Method Request Table



HTTP Status Codes



Top 10 Domains



Alerts—Apache

Designed the following alerts

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Response	sends alert when POST response passes baseline	1-3	>5

JUSTIFICATION: This baseline was set to 1-3 for POST because the usual traffic shows that amount then escalates to past 4 when the attack occurs

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity NOT USA	Alert for counts of countries that attempt to connect to VSI website	50	>110

JUSTIFICATION: This baseline was observed to be between 20-110 as most of the report average was sitting at that level.

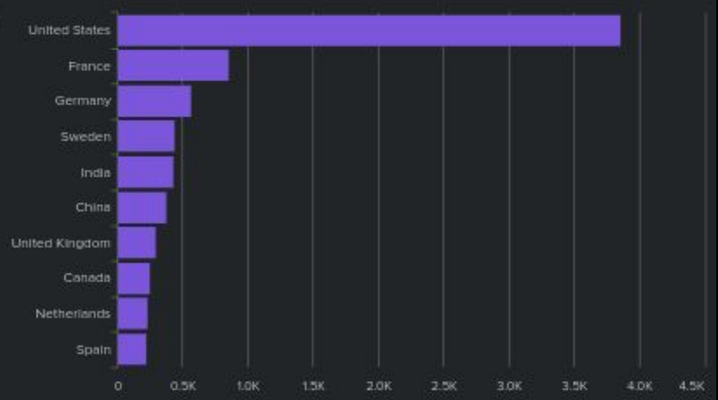
Apache Web Server Monitoring Dashboard

Apache Web Server Monitoring

Visualizing Web Server Traffic and Trends

The "Apache Web Server Monitoring" dashboard provides a comprehensive overview of your web server's activity. It highlights trending HTTP methods along with their corresponding timestamps, allowing you to track the server's usage patterns over time. The interactive map visually pinpoints client IP addresses on a global scale, revealing the prominent countries accessing your server. Additionally, the dashboard displays frequently accessed URIs along with their occurrence frequency, enabling you to identify the most visited content on your website. This consolidated information empowers you to make informed decisions about optimizing your server's performance and enhancing user experience.

Trending Countries



Trending HTTP Method

HTTP Method
GET
9,851

HTTP Method - By Hour
GET

HTTP Method
POST
106

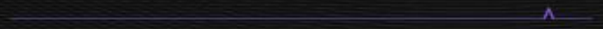
HTTP Method - By Hour
POST

HTTP Method
HEAD
42

HTTP Method - By Hour
HEAD

HTTP Method
OPTIONS
1

HTTP Method - By Hour
OPTIONS



Trending URIs

uri	count
/VSI_Company_Homepage.html	807
/contactus.html	546
/reset.css	538
/images/VSI_headquarters.jpg	533
/images/web/2009/banner.png	516
/blog/tags/puppet?flav=rss20	488
/projects/xdotool/	224
/?flav=rss20	217
/	197
/robots.txt	180
/projects/xdotool/xdotool.xhtml	154
/?flav=atom	137
/articles/dynamic-dns-with-dhcp/	135
/presentations/logstash-scale11x/images/ahhh___rag...	128

< Prev 1 2 3 4 5 ... Next >

Attack Analysis

Attack Summary—Windows (Reports)

- **Severity Levels Report** - Major increase in high severity results. A jump from 6.91% severity to **20.23%**.

- **Signature Logs Report** - Major increase in “a user account was locked out” and “an attempt was made to reset an accounts password”.
  - A user account was created
    - increase from 309 to 1,811**(+486%)**
  - an attempt was made to reset an accounts password
    - increase from 295 to 2,128 **(+621%)**

- **Success & Failure Report** - Major increase in successful windows activities.
  - increase from 4616 to 5854 **(+26%)**

Attack Summary—Windows (Alerts)

- **Windows Logs - Event 4726 (Accounts Deleted)**
  - After reviewing the attack logs and seeing the activity spike up to 75 we would move the threshold 30 to further refine this alert.
- **Windows Logs - Event 4624 (Successful Login)**
  - After reviewing attack logs and seeing the activity spike up to 90 successful logins we would adjust the threshold to be 30 to reduce false positives.
- **Windows Logs - Failed Attemps**
  - After reviewing the attack logs we would keep this alert threshold set to 10.

Attack Summary—Windows (Dashboard)

- After setting the source to the attack logs these were our findings.

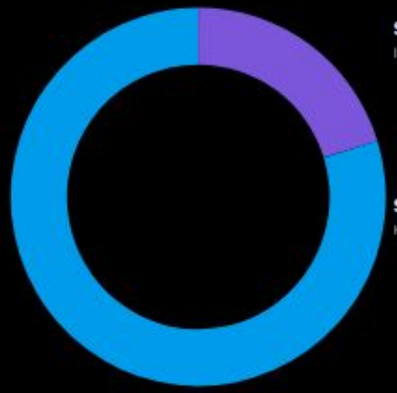
1. “A user account was locked out” signature results spiked starting at midnight and ended at 3am.
2. “An attempt was made to reset an accounts password” signature results spiked at 8am and ended at 11am.
3. “User_a” activity spiked starting at midnight and ended at 3am.
4. “User_k” activity spiked starting at 8am and ended at 11am.

Windows Server Attack Dashboard

Windows Server Attack Logs

This dashboard provides comprehensive insights into Windows server attacks.

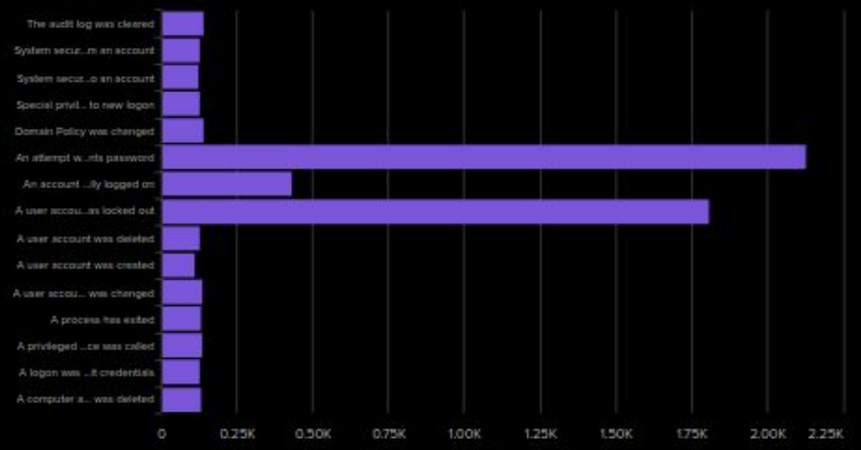
Windows Attack Logs - Severity Levels



Severity Level
Informational
4,381
79.77

Severity Levels
High
1,111
20.23

Windows Attack Logs - Signature

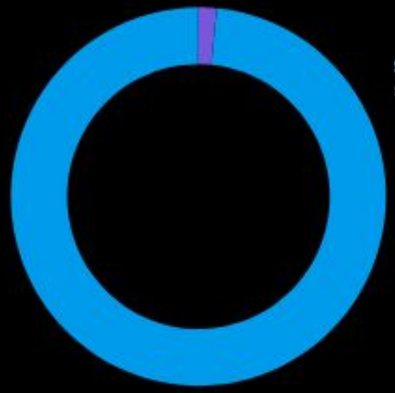


Signature Alert
Successful Logins
432

Signature Alert
User Account Deleted
130

Signature Alert
User Account Locked Out
1,811

Windows Attack Logs - Signature Status

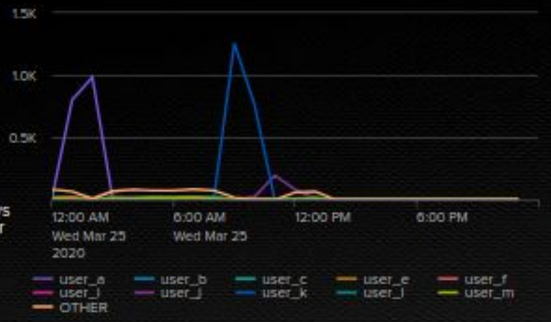


Signature Status
Success
5,854

Signature Status
Failures
93

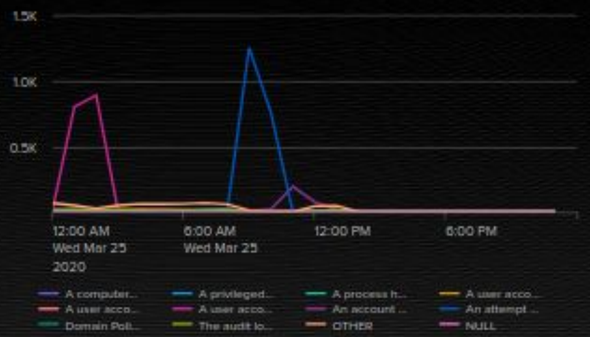
Trending User Activity

The following line chart displays the count of user activities over the duration of the filtered timeframe



Trending Signature Activity

The following line chart that displays the various signatures that occurred over the duration of the filtered time frame



Windows Attack Logs - Users

#	user	count
1	ALiaALanziQ8	1
2	AMOSORTILEGIO	1
3	Adorethickems	1
4	AlienConsulate	1
5	AmandaZnz	1

‹ Prev 1 2 3 4 5 ... Next ›

Attack Summary—Apache (Reports)

- Methods Request Attack report- shows the type of request method that was most used during the attack time frame that can be used to pinpoint the type of attack that was used.
- HTTP Status code report- this report can be used to further identify what type of attack is occuring.
- Top 10 Domains attack report- this report can be used to pinpoint the location the attack is coming from

Attack Summary—Apache (Alerts)

- Attack logs show a spike in POST Request from 106 to 1324 that originate from Ukraine during the time of the attack
- Baselines and Thresholds were set correctly as the attack vectors increased exponentially during attack occurrence.

Attack Summary—Apache (Dashboard)

- The Dashboard shows the traffic from Kyiv spiked to 877 counts during the attack and that the method that was most prominent during the attack time frame was the POST method with 1296 counts.
- this information can be used to determine which IPs to prevent connections from the Ukraine to mitigate any damages.

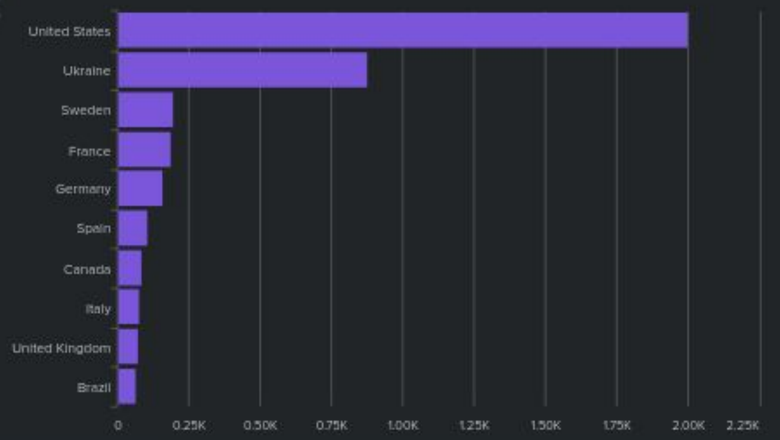
Apache Web Server Attack Dashboard

Apache Web Server Attacks

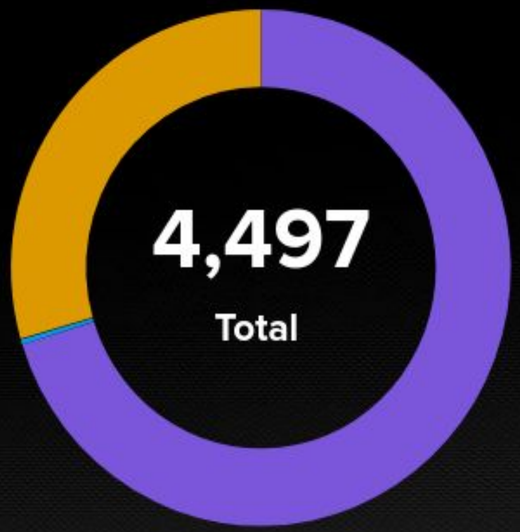
Visualizing Web Server Traffic and Trends

The "Apache Web Server Attacks" dashboard provides a comprehensive overview of your web server's activity. It highlights trending HTTP methods along with their corresponding timestamps, allowing you to track the server's usage patterns over time. The interactive map visually pinpoints client IP addresses on a global scale, revealing the prominent countries accessing your server. Additionally, the dashboard displays frequently accessed URIs along with their occurrence frequency, enabling you to identify the most visited content on your website. This consolidated information empowers you to make informed decisions about optimizing your server's performance and enhancing user experience.

Trending Countries



Trending HTTP Method



HTTP Method
GET
3,157

HTTP Method - By Hour
GET

HTTP Method
POST
1,324

HTTP Method - By Hour
POST

HTTP Method
HEAD
15

HTTP Method - By Hour
HEAD

HTTP Method
OPTIONS
1

HTTP Method
OPTIONS

Trending URIs

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
/robots.txt	44
/	37
/projects/xdotool/xdotool.xhtml	37

‹ Prev 1 2 3 4 5 … Next ›

Summary and Future Mitigations

Project 3 Summary

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

- **User_a** - this account was locked out after what appears to be a brute force attempt
- **User_k** - with this account the attacker attempted to reset the password but was unsuccessful.
- Large amount of incoming traffic from Ukraine

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

- Lock user for 1 hour after multiple failed attempts
- Rate Limiting and Connection Limits:
  - Implement rate limiting to control the number of connections from a specific IP address or range.
  - Set connection limits to prevent automated scanning and brute-force attacks.