Defensive Security Project
by: Bridget Dipalermo, Alice Lee, Sebasteine Marquez, Brandon Nimer, Jeremy Urena

Table of Contents

This document contains the following resources:

01

Monitoring Environment

- Using Splunk to analyze logs and create a baseline

02

Attack Analysis

- Compare data points to identify potential attacks

03

Project Summary & Future Mitigations

- Summary of our finding and recommendations for future

Monitoring Environment

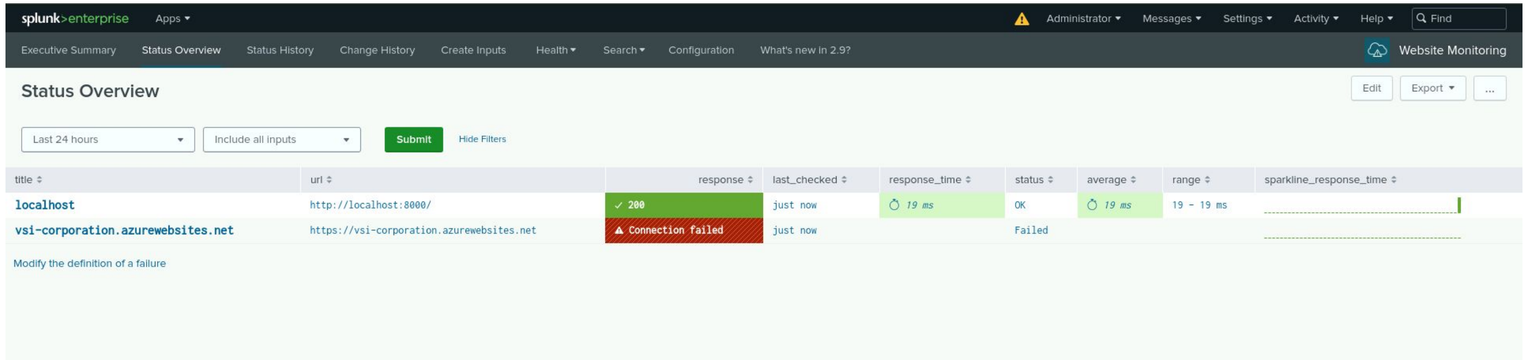
Scenario

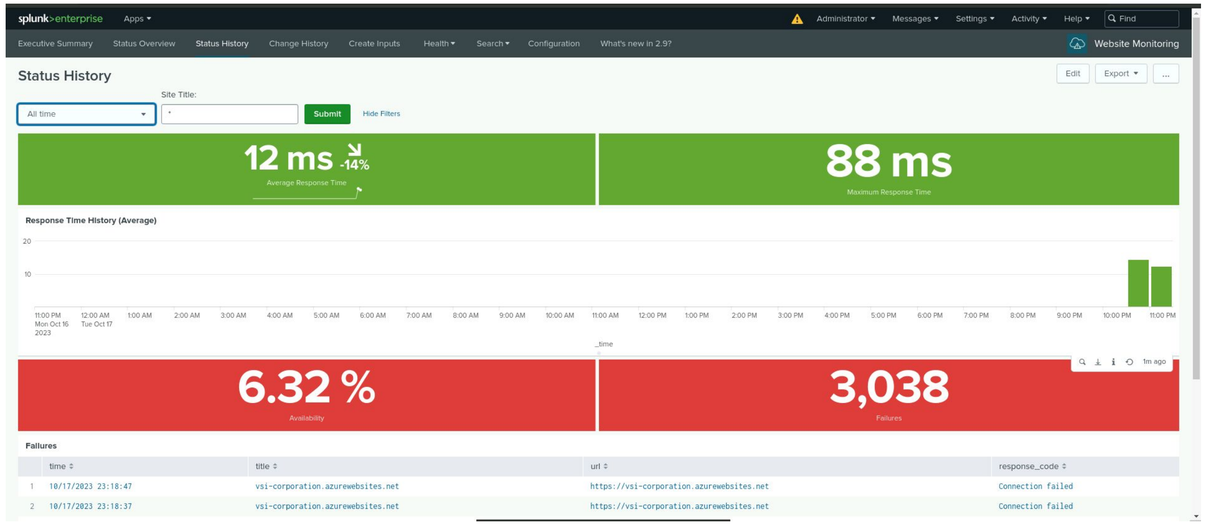
- “SOC it to You” was tasked by VR company, Virtual Space Industries (VSI), with monitoring potential attacks to our systems and applications after hearing rumors that JobeCorp may launch cyberattacks to help gain an edge in the market
- We have been provided with:
  - **Windows Server Logs**
    - Contains the intellectual property of VSI’s next-gen VR programs
  - **Apache Server Logs**
    - Logs for VSI’s main public facing website
- With this information our team will be using Splunk to analyze the data and identify any potential security risks to the company

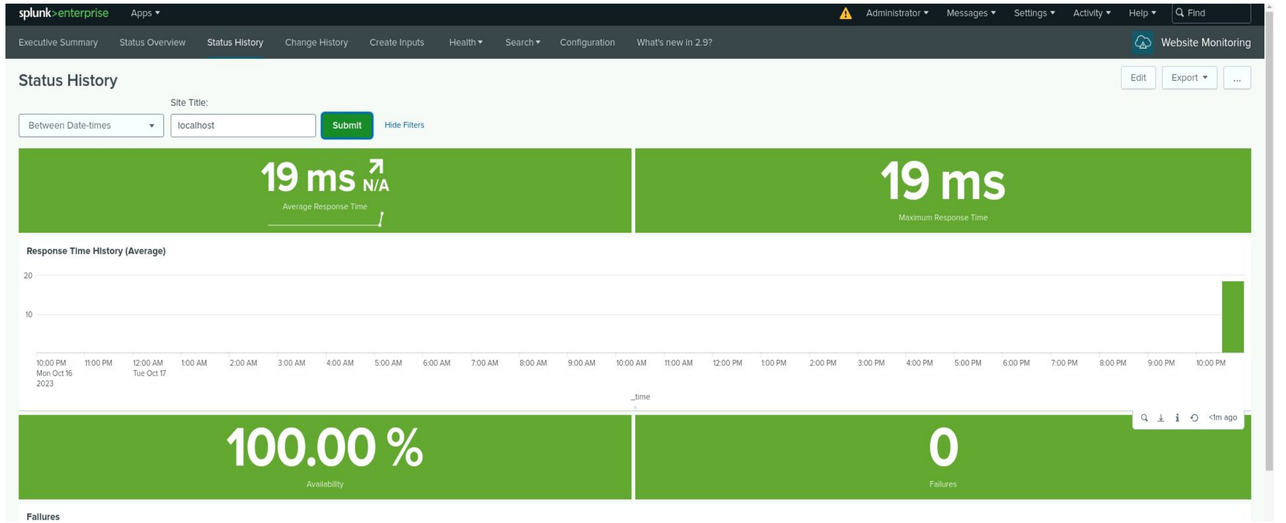
Website Monitoring

Website Monitoring

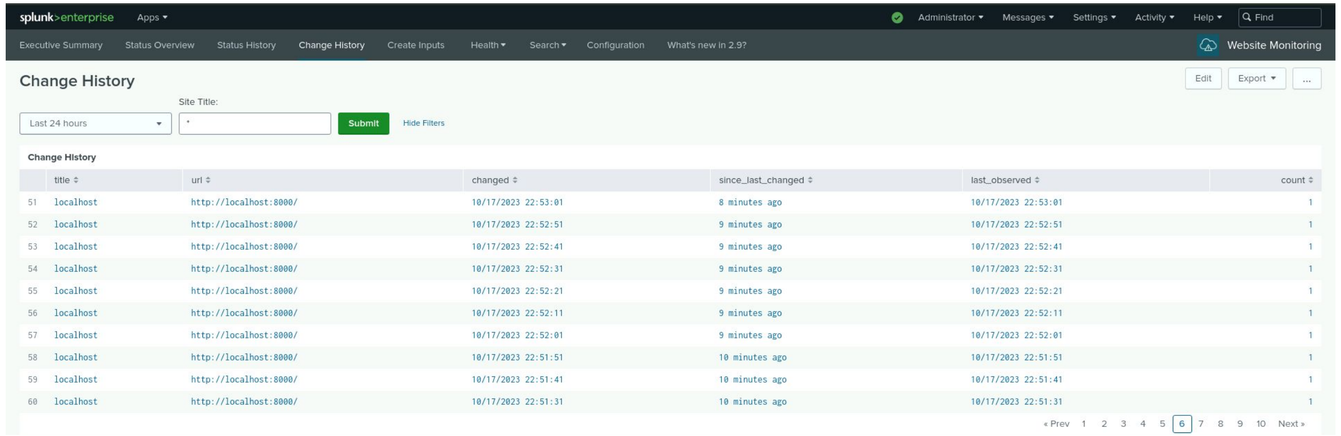
Designed to detect webapp availability and downtime.

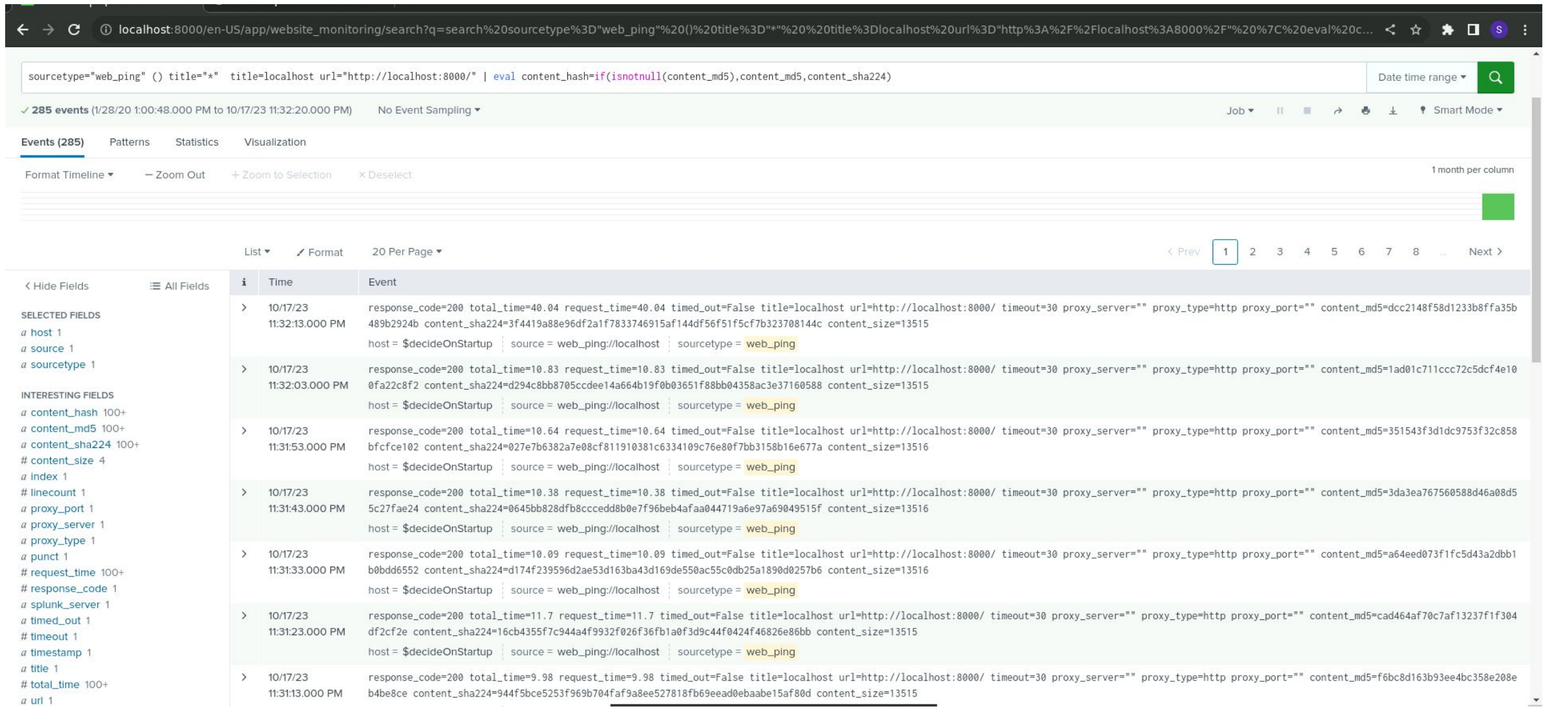




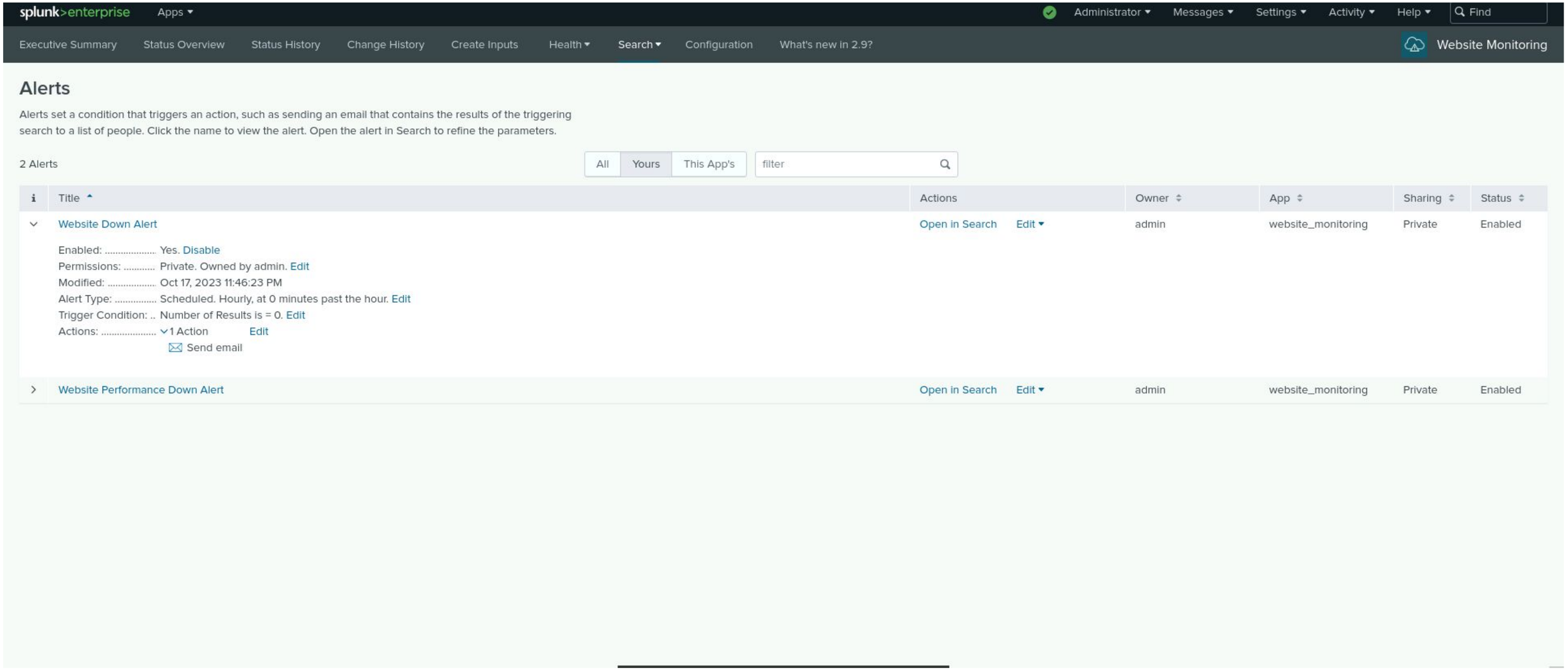


Website Monitoring





Website Monitoring



Logs Analyzed

1 Windows Logs

Account Management Logs

- User Accounts Logins
- User account credential changes
- User account creation and deletions
- Domain Policy changes
- System access

2 Apache Logs

WebApp HTTP Request logs

- Accessing webapp resources
- Logins
- URI
- User Agents
- Client IP

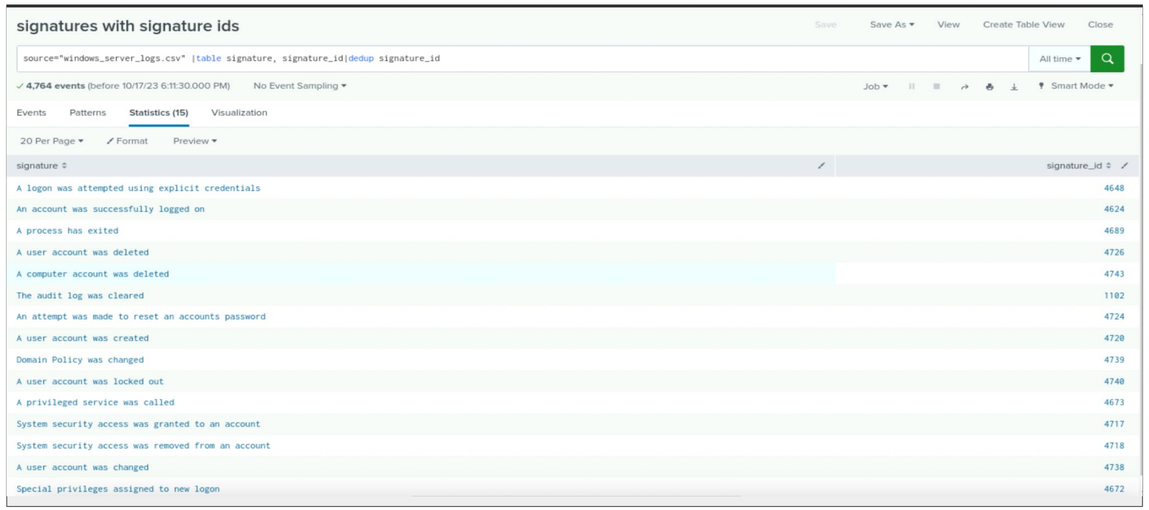
Windows Logs

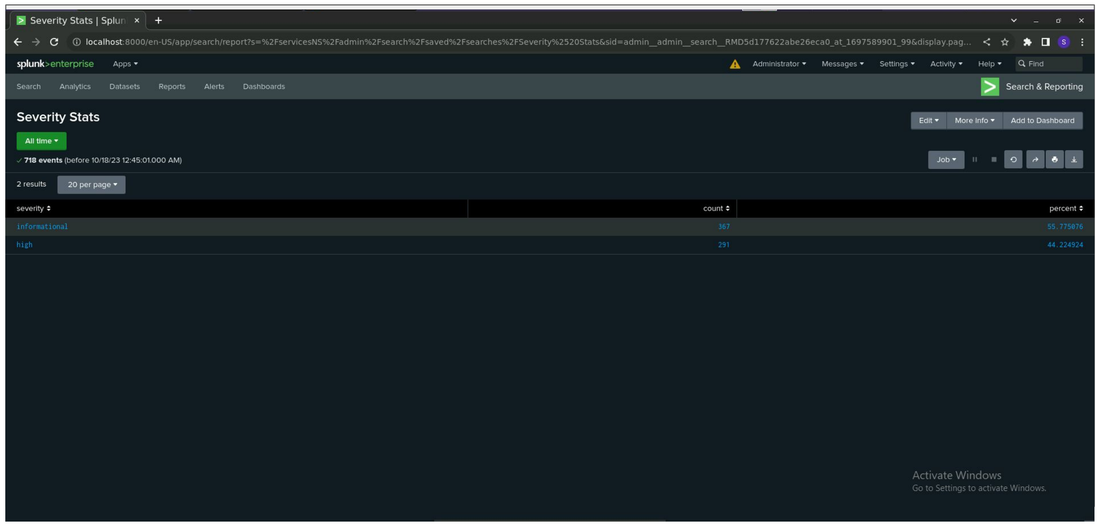
Reports—Windows

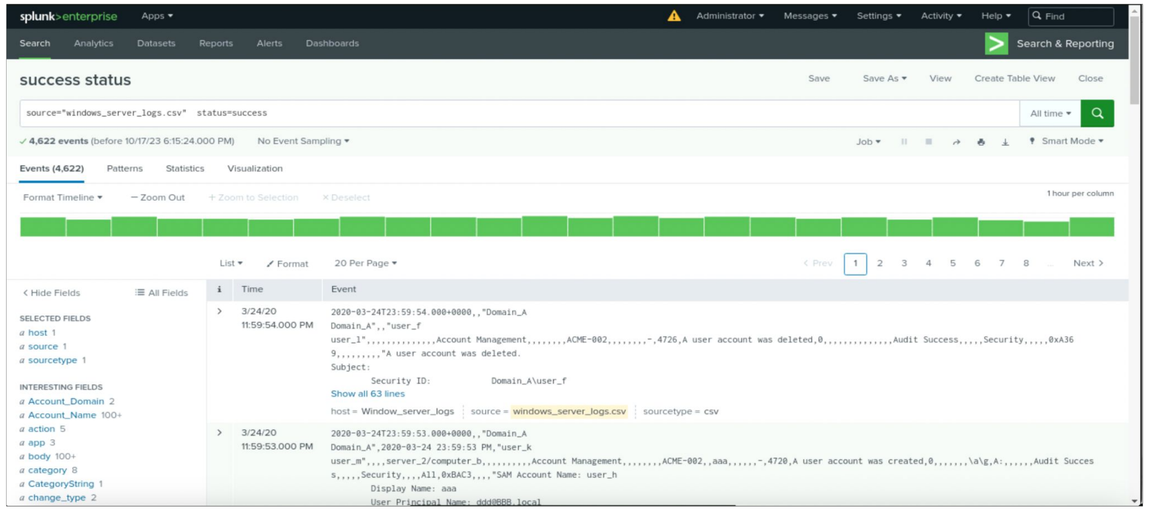
Designed the following reports:

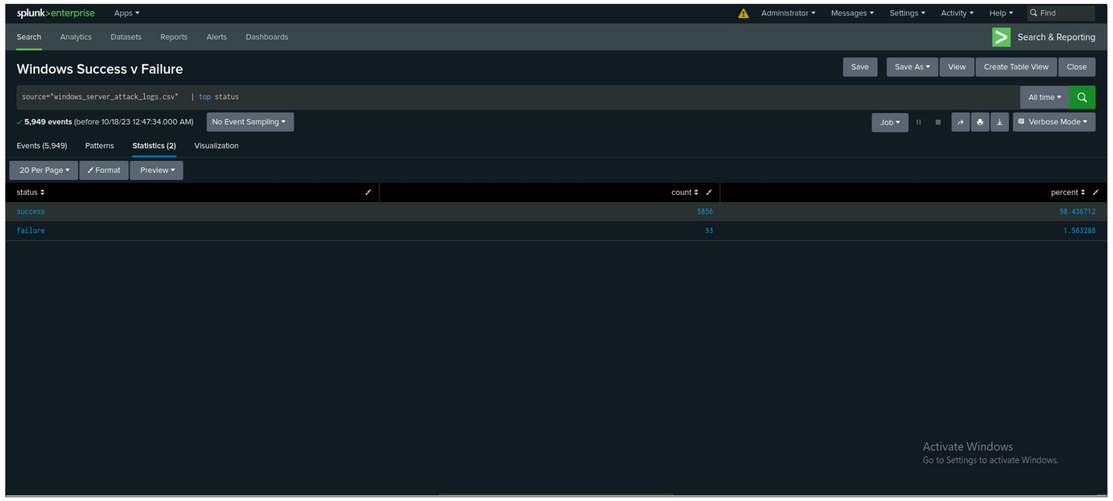
Report Name	Report Description
Signatures with signature IDS	A report that shows the ID associated with the signature
Severity levels	A report that displays the severity levels of the window logs being used
Success and failures	A report that compares the success and failures of Windows activites

Images of Reports—Windows









Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly level of failed activity	Triggers alert when threshold of failed activity is reached	6	15

JUSTIFICATION: the baseline was made from the average count of failed activity logs, the threshold is highest value shown, therefore the alert would trigger if it goes above that

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly count of signature logged on	Determine a baseline and threshold for the hourly count of the signature “an account was successfully logged on.”	13	25

JUSTIFICATION: the baseline was made from the average count of successful logins, the threshold is highest value shown, therefore the alert would trigger if it goes above that

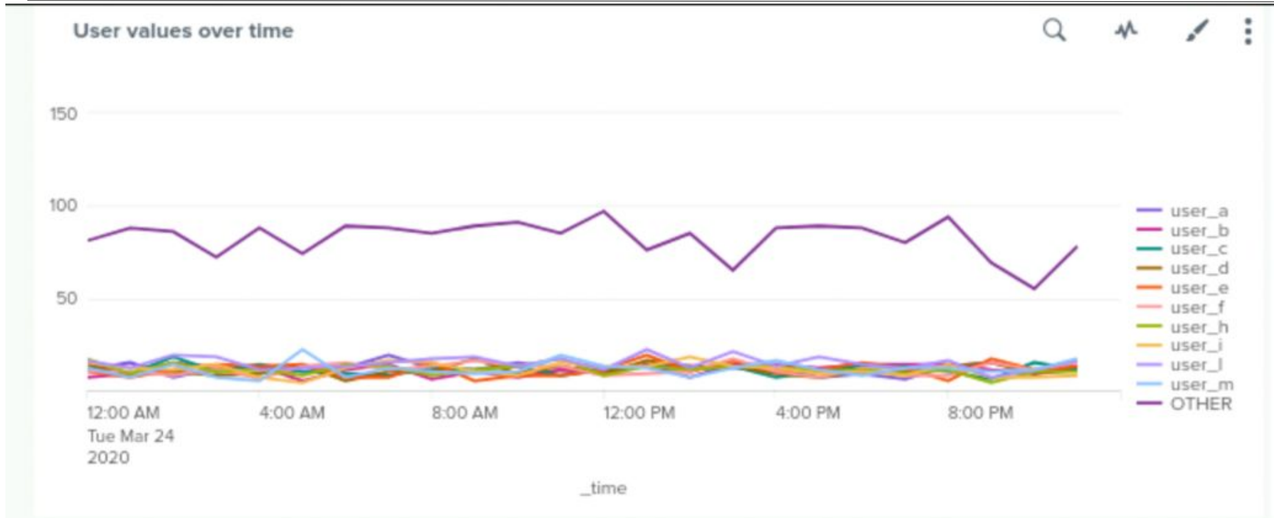
Alerts—Windows

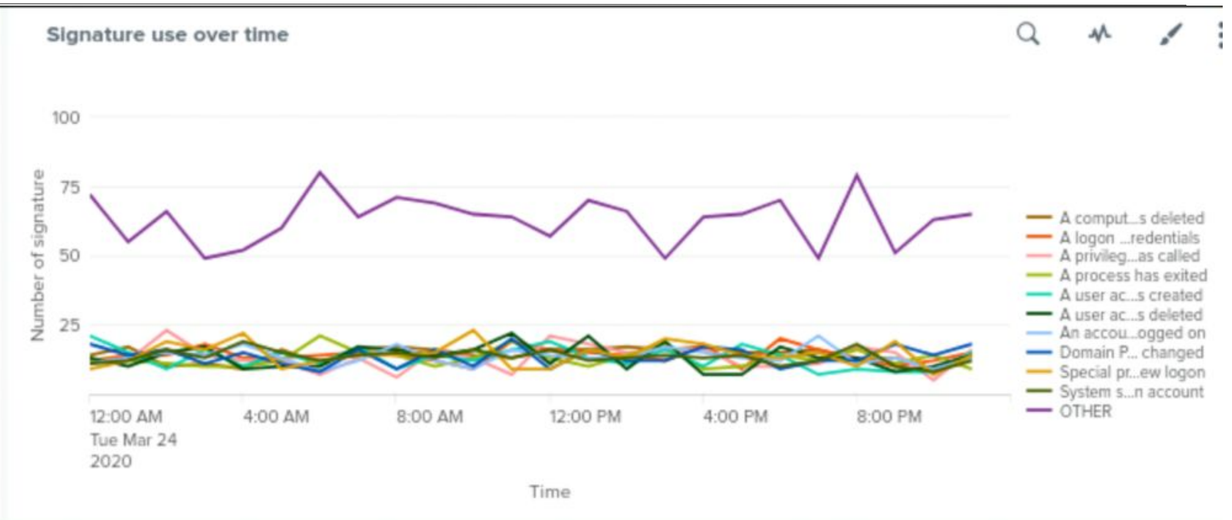
Designed the following alerts:

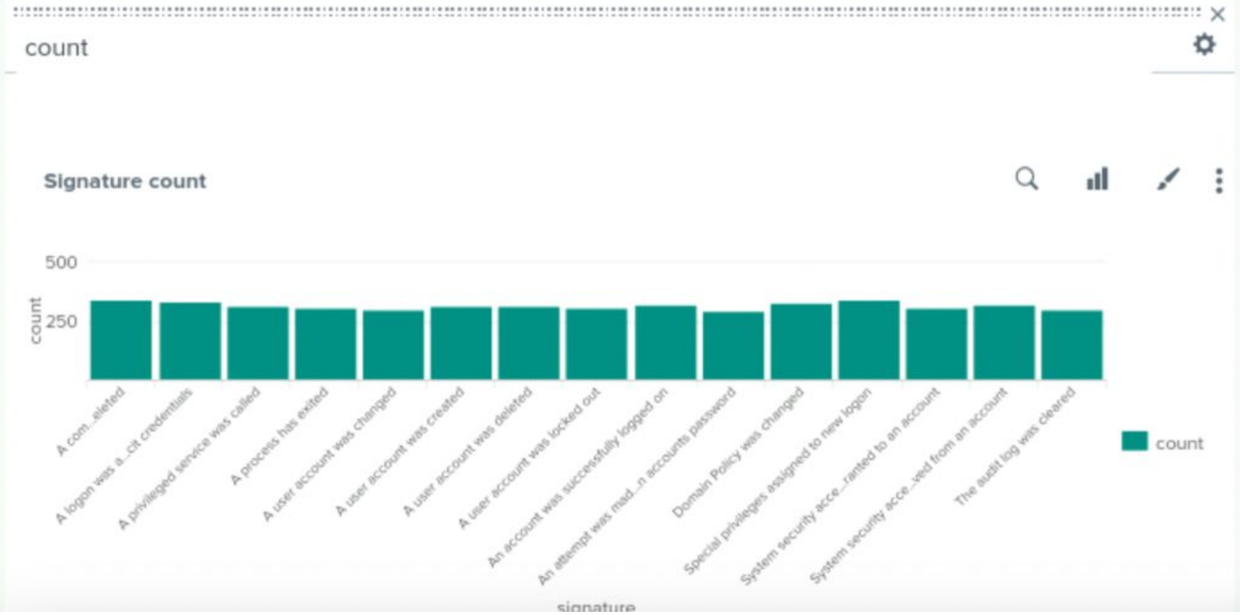
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly count of signature deleted	triggers alert when a user’s account was deleted	13	18

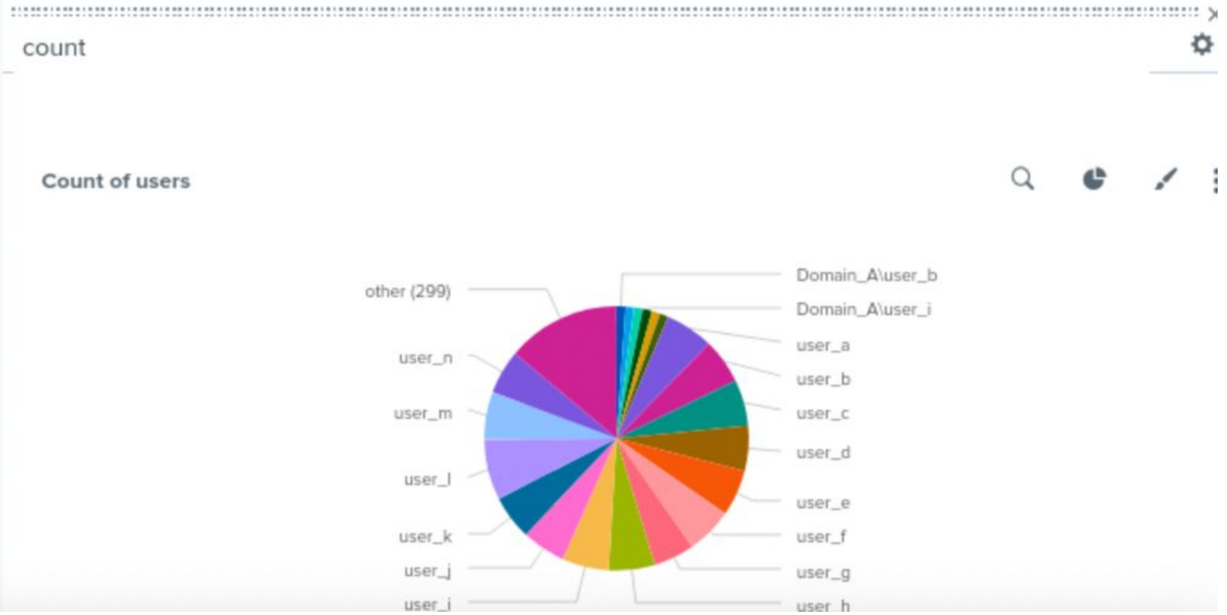
JUSTIFICATION: the baseline was made from the average count of deleted accounts the threshold is highest value shown, therefore the alert would trigger if it goes above that

Dashboards—Windows









Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP methods	stats count of HTTP request methods (GET, POST, HEAD, OPTIONS)
Top 10 Referrer Domains	top 10 referrer domains of VSI’s web server
HTTP Response Codes	total count of HTTP response codes

Images of Reports—Apache

HTTP Methods

Edit ▾ | More Info ▾ | Add to Dashboard

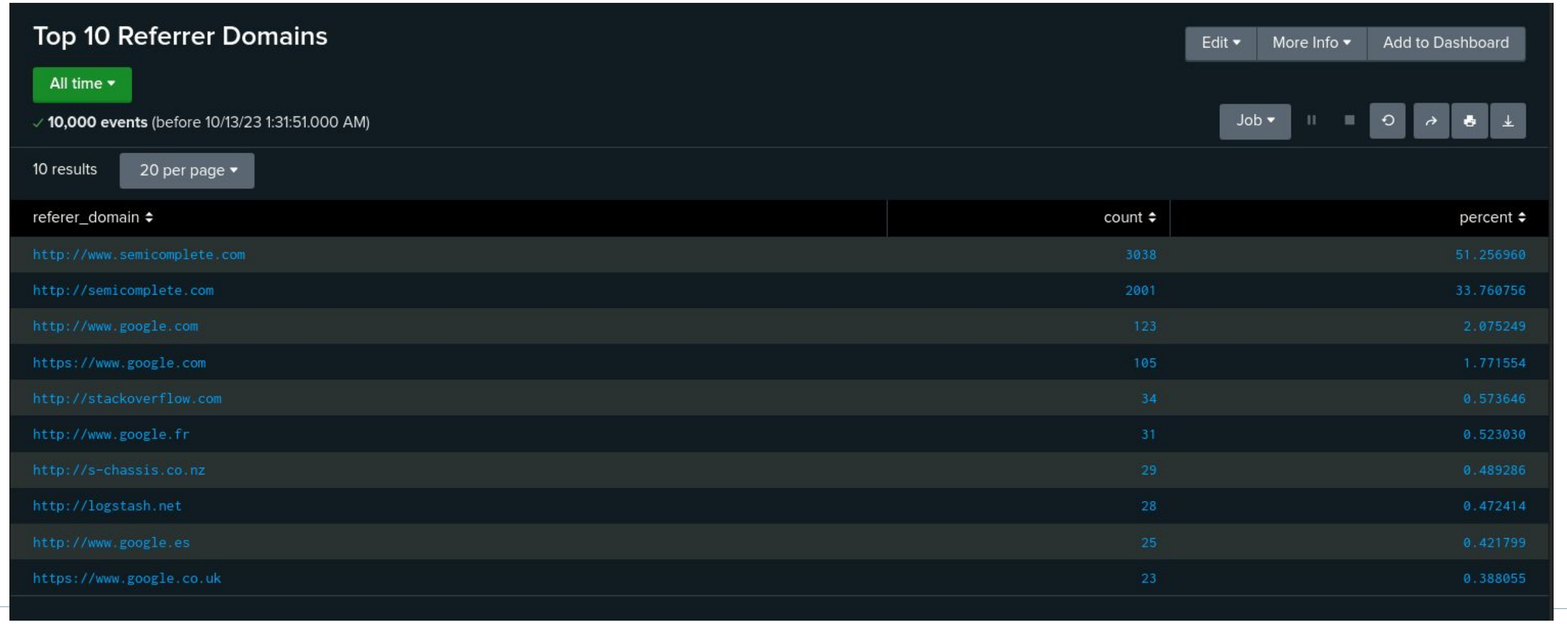
All time ▾

✓ **10,000 events** (before 10/13/23 1:34:47.000 AM)

Job ▾

4 results | 20 per page ▾

method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000



Top 10 Referrer Domains

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **10,000 events** (before 10/13/23 1:31:51.000 AM)

Job ▾

10 results | 20 per page ▾

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

Images of Reports—Apache (cont.)

status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
International Activity Alert	This alert is triggered if the condition of 125 counts of IP addresses from outside the US accesses the web server within one hour	115	>125

JUSTIFICATION: number of events ranged between 1 and 120. Alert threshold was chosen closer to the highest number from the provided range while still giving room for the possibility of a higher count than normal.

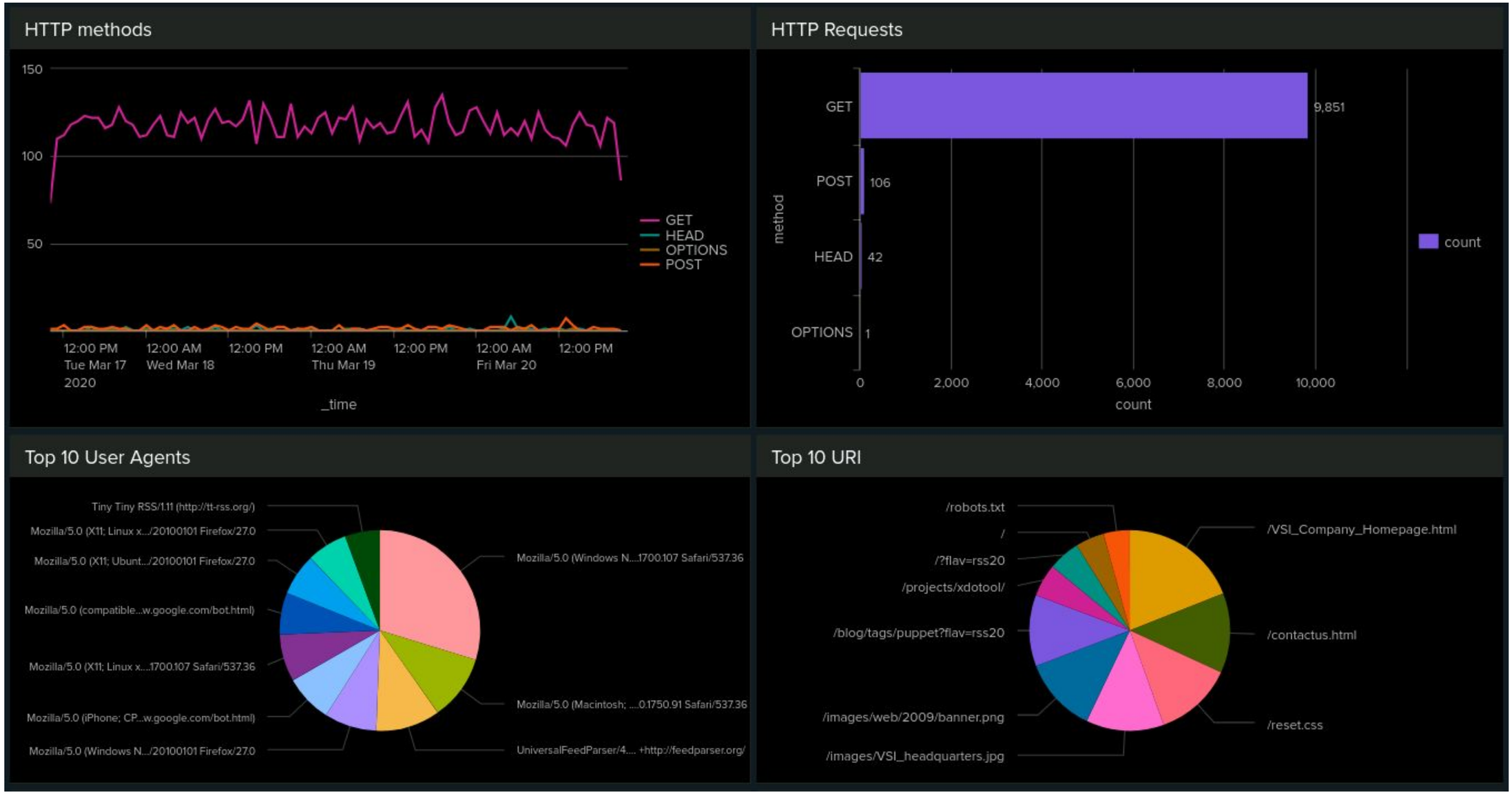
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Alert	This alert is triggered if the condition of 10 counts of HTTP POST requests was to be exceeded within one hour.	5	>10

JUSTIFICATION: number of events typically ranged between 3 and 7. Alert threshold was chosen closer to the highest count with reasonable space.

Dashboards—Apache



Dashboards—Apache (cont.)

Attack Analysis

Attack Summary—Windows

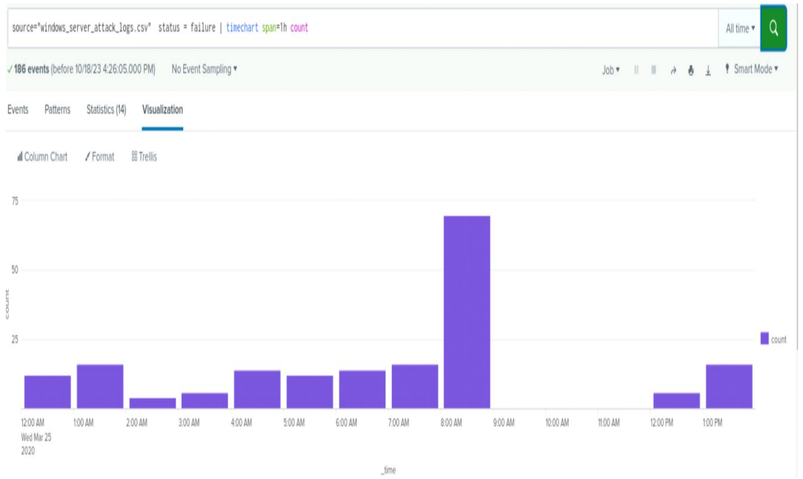
Summarize your findings from your reports when analyzing the attack logs.

- Some findings after analyzing the attack logs were that the amount of accounts locked out, and amount of accounts that needed to reset password greatly increased
- The success of window activities increased for attackers
- The time of which successful logins happened were very concentrated compared to server logs which varied throughout the day

Attack Summary—Windows

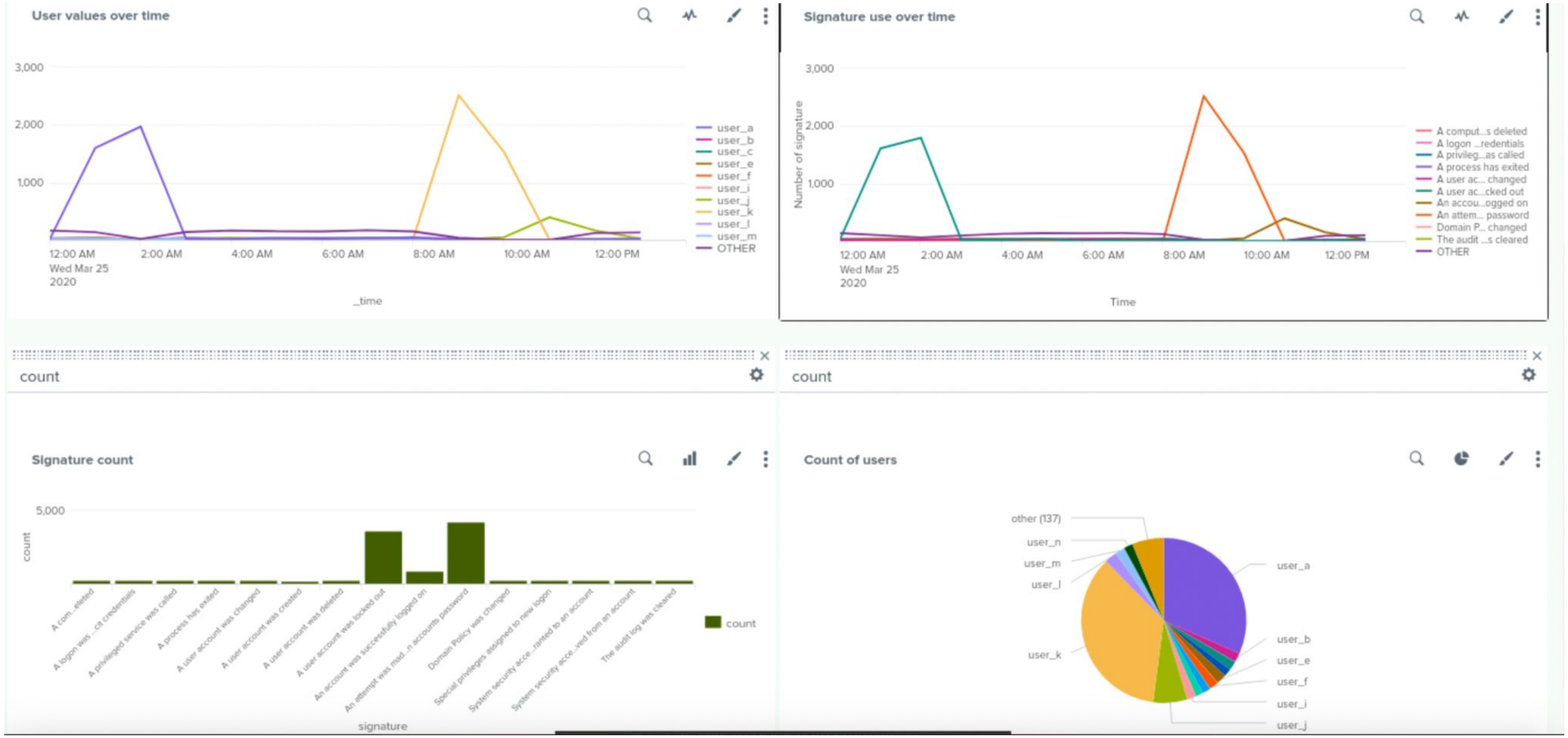
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- Accounts deleted still occurred, but less often overtime
- Spikes in time of account failure, 8am
- Thresholds were mostly accurate, the threshold for failed activity could be increased
- Threshold was 60 events



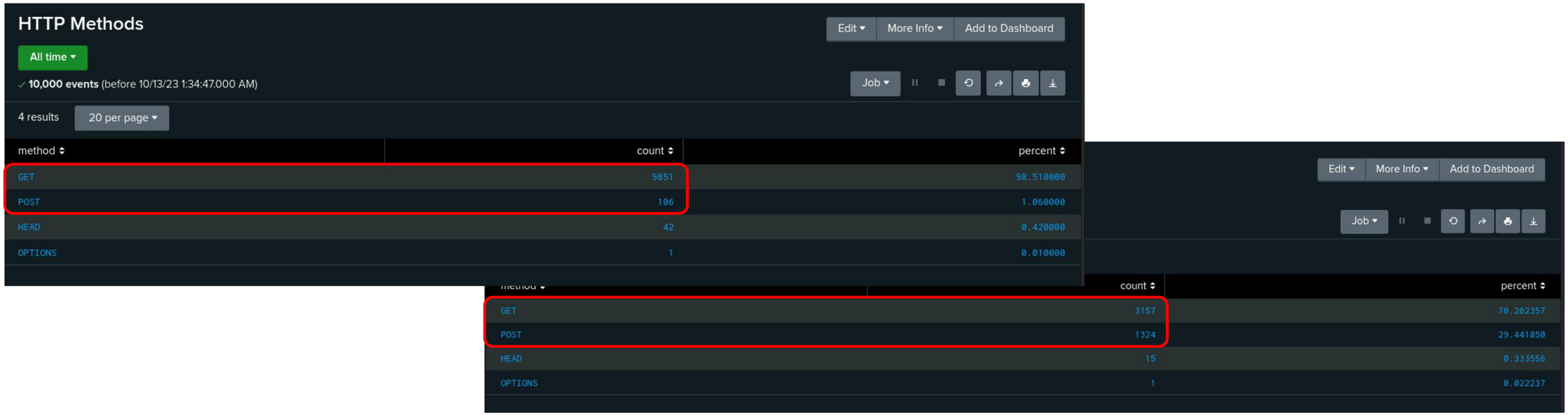
Attack Summary—Windows

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

- 

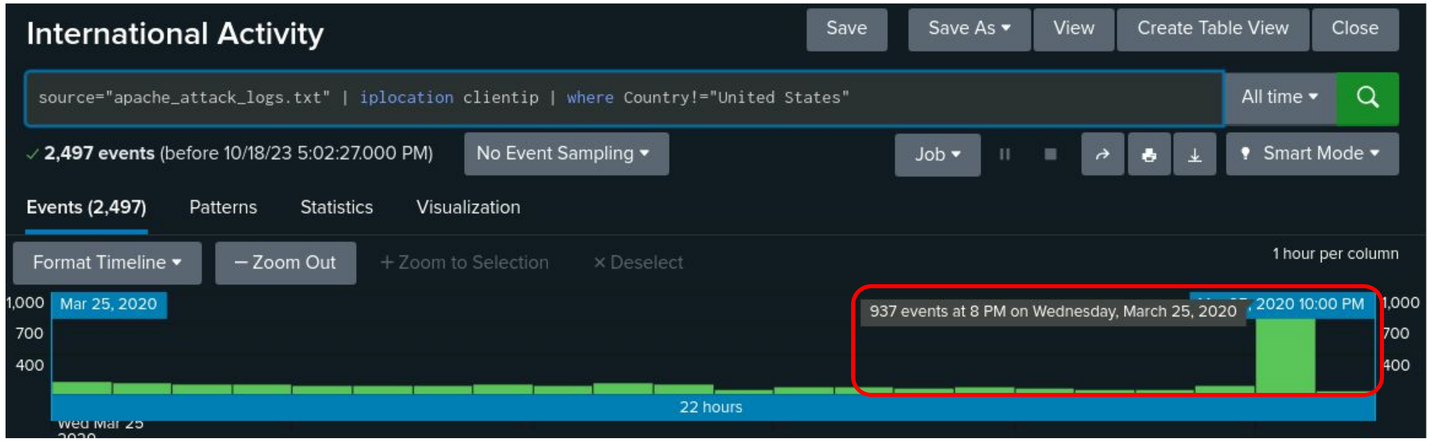
Attack Summary—Apache

- HTTP Request Method
  - GET - significant decrease from normal activity (9851 to 3157)
  - POST - significant increase from normal activity (106 to 1324)
- Referrer Domains and HTTP response codes
  - significant decrease in event count

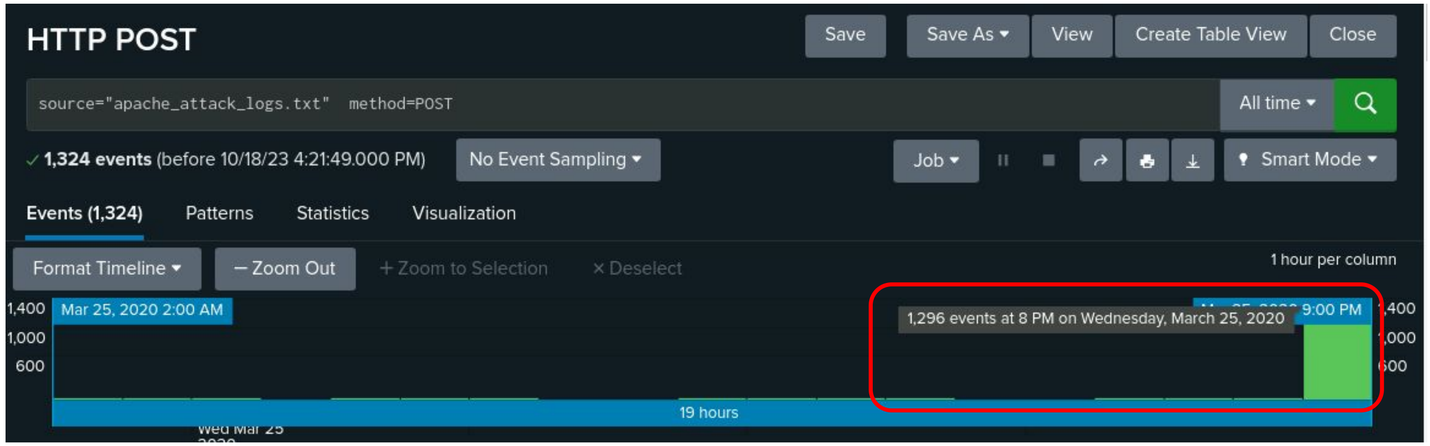


Attack Summary—Apache

- International Activity Alert
  - > 125 condition per hour
    - 937 events



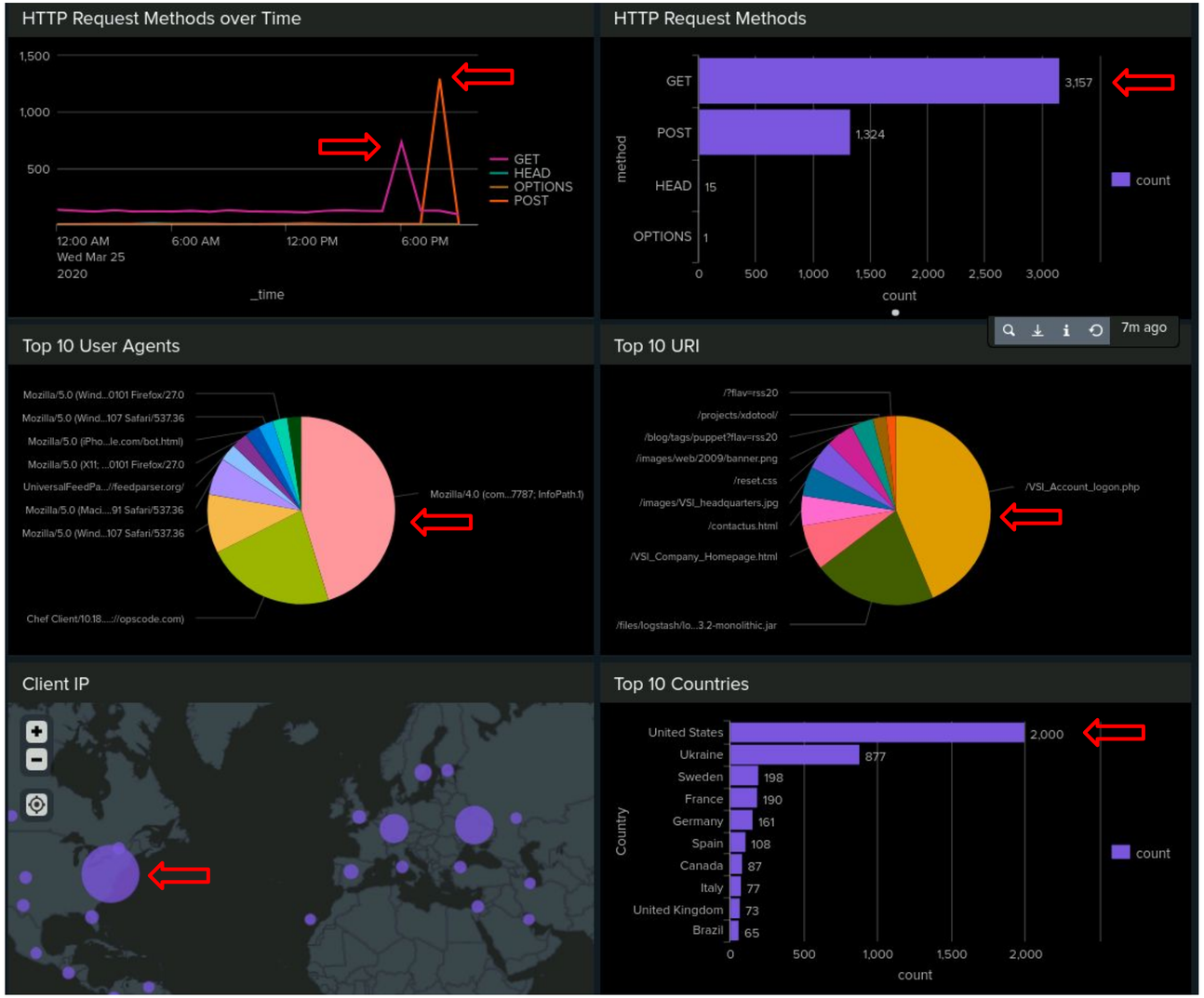
- HTTP POST Alert
  - > 10 events per hour
    - 1,296 events



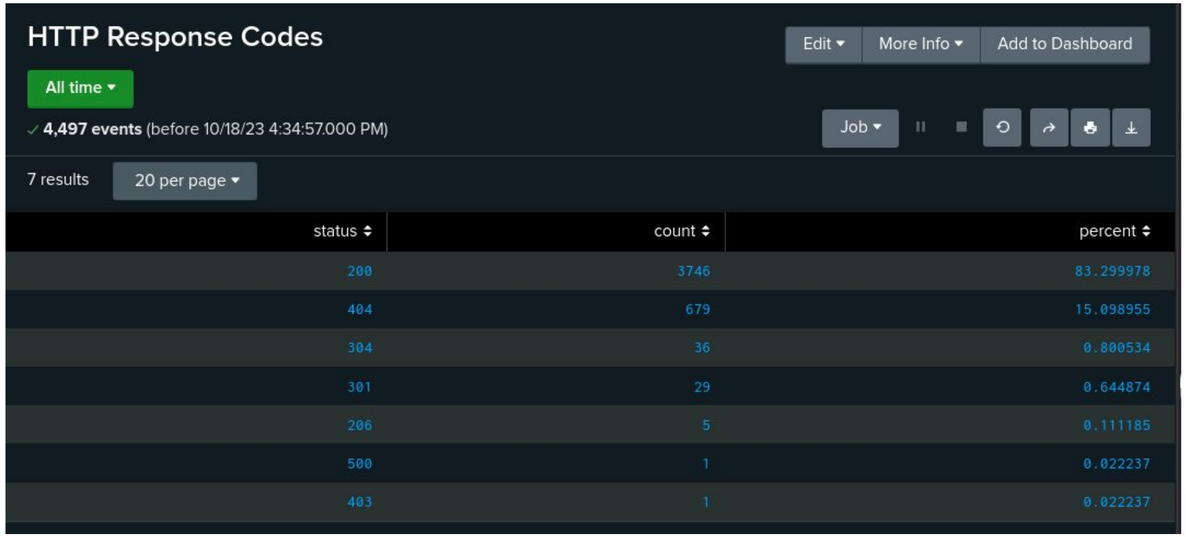
alerts would have been triggered, but the SIEM would further benefit from increasing the threshold

Attack Summary—Apache

- HTTP Methods
  - GET
  - POST
- User Agents
  - Mozilla/4.0
- URI
  - /VSI_Account_logon.php
- Client IP
  - US
  - Ukraine



Screenshots of Attack Logs



HTTP Response Codes

Edit ▾ | More Info ▾ | Add to Dashboard

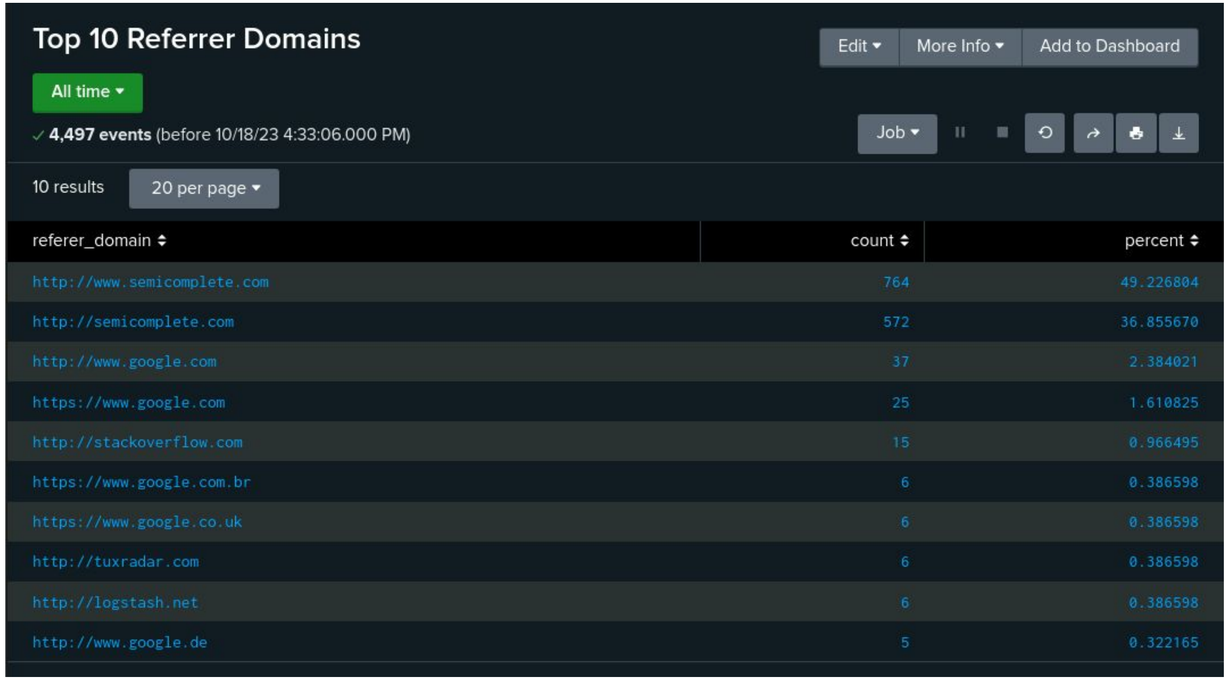
All time ▾

✓ **4,497 events** (before 10/18/23 4:34:57.000 PM)

Job ▾

7 results | 20 per page ▾

status ⇕	count ⇕	percent ⇕
200	3746	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



Top 10 Referrer Domains

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **4,497 events** (before 10/18/23 4:33:06.000 PM)

Job ▾

10 results | 20 per page ▾

referer_domain ⇕	count ⇕	percent ⇕
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

Summary and Future Mitigations

Project 3 Summary

- Based off the attack logs provided, JobeCorp’s attack was most likely a brute force attack that was performed on VSI’s account logon page which also resulted in a DoS attack on March 25th, 2020.

- Future Mitigations:
  - Dual MFA
  - Add CAPTCHA
  - Strong password policy
  - Phishing Training

Questions?