

Defensive Security Project
by: Bridget Dipalermo, Alice Lee,
Sebastaine 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

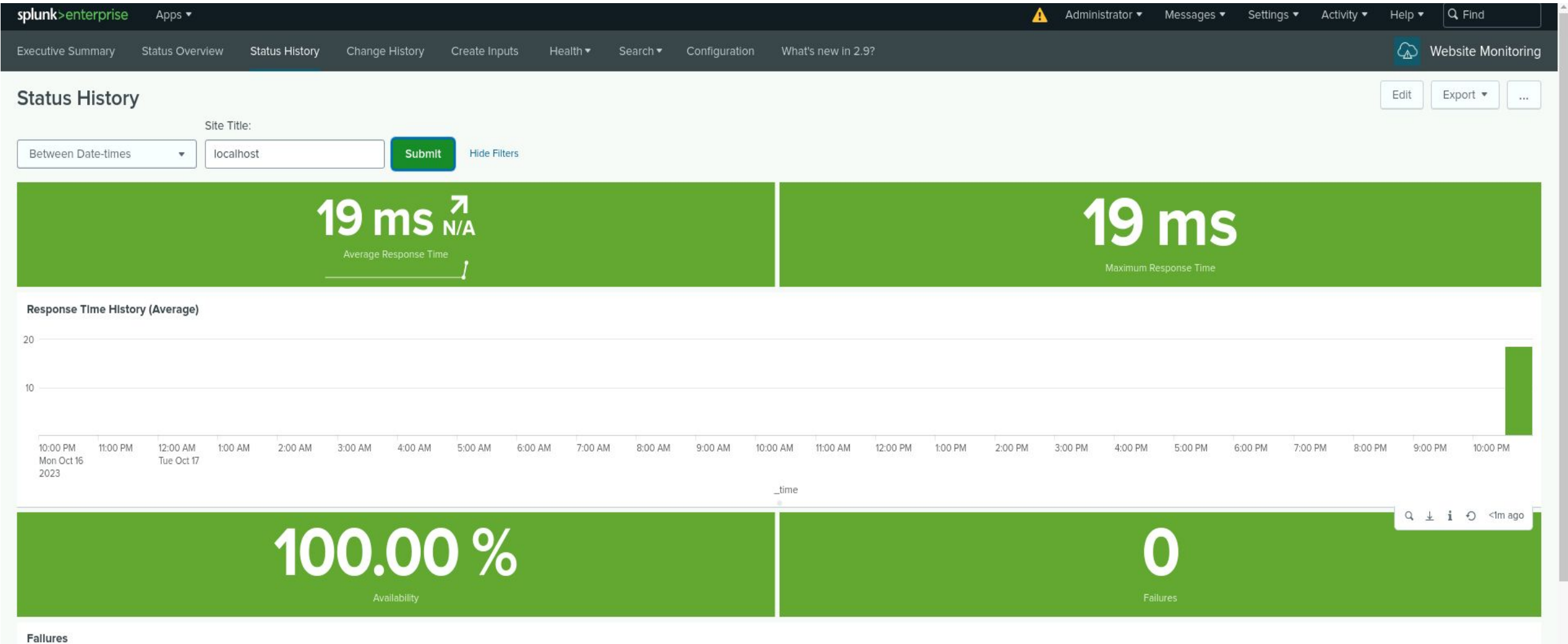
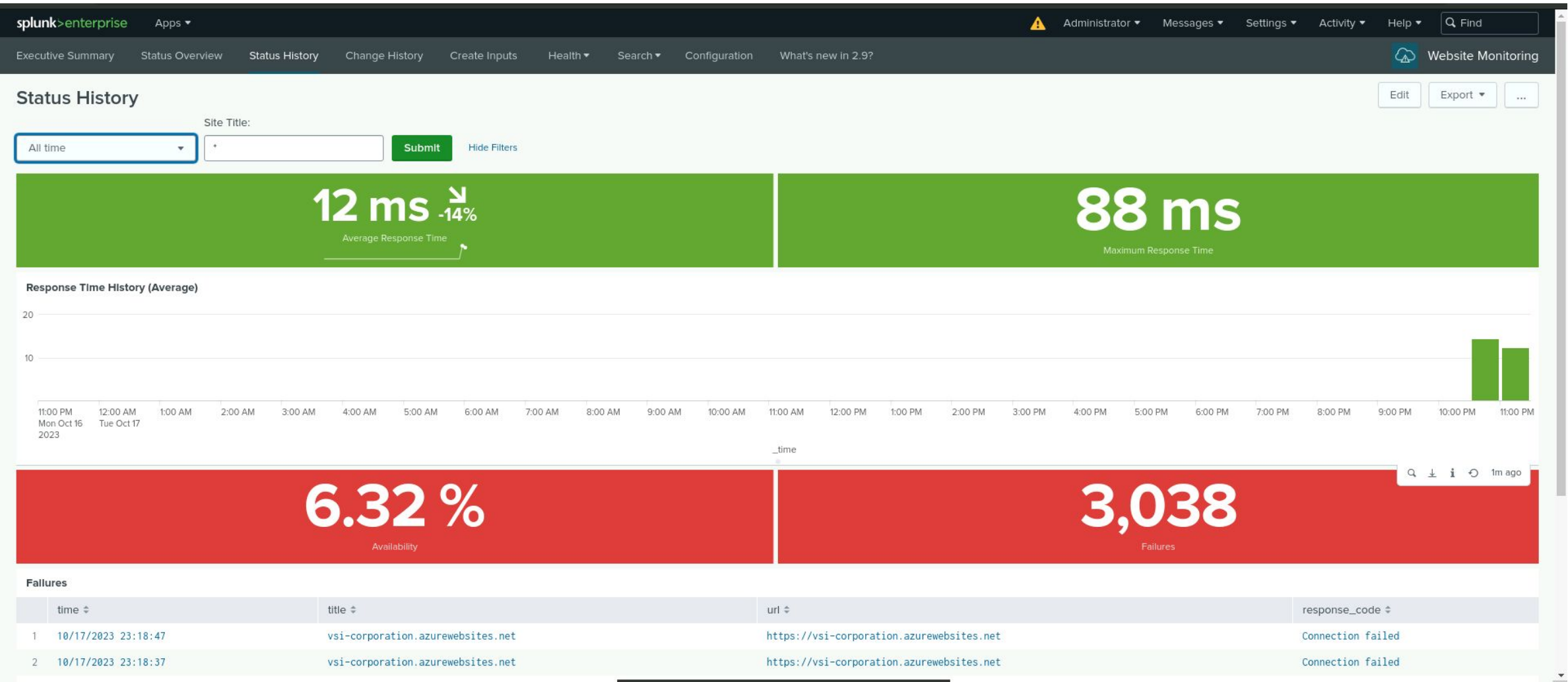
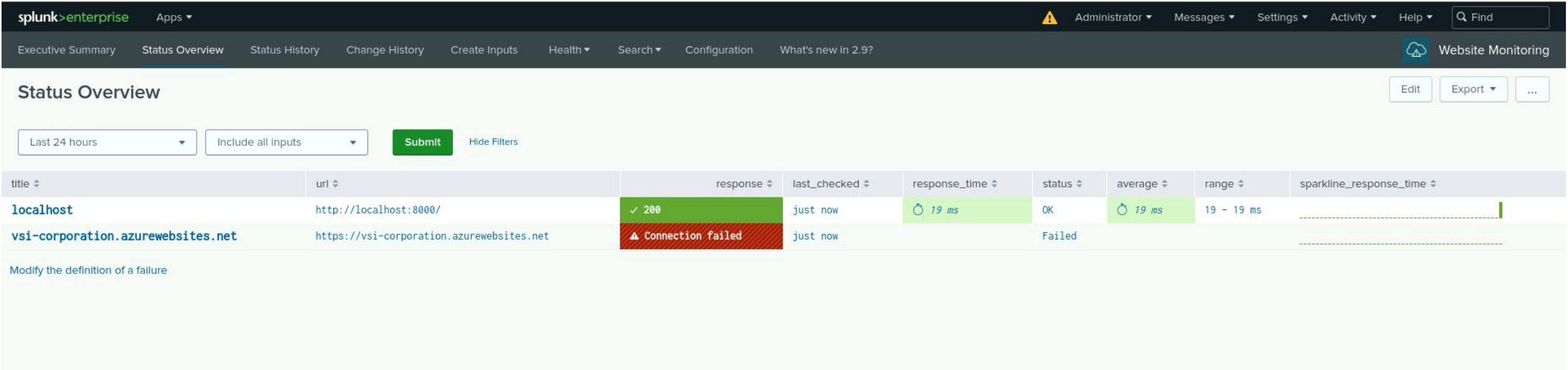
Scenario

- “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

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Executive SummaryStatus OverviewStatus HistoryChange HistoryCreate InputsHealthSearchConfigurationWhat's new in 2.9?Website Monitoring

Change History

Site Title:

Last 24 hours

*

Submit

Hide Filters

Change History						
	title	url	changed	since_last_changed	last_observed	count
51	localhost	http://localhost:8000/	10/17/2023 22:53:01	8 minutes ago	10/17/2023 22:53:01	1
52	localhost	http://localhost:8000/	10/17/2023 22:52:51	9 minutes ago	10/17/2023 22:52:51	1
53	localhost	http://localhost:8000/	10/17/2023 22:52:41	9 minutes ago	10/17/2023 22:52:41	1
54	localhost	http://localhost:8000/	10/17/2023 22:52:31	9 minutes ago	10/17/2023 22:52:31	1
55	localhost	http://localhost:8000/	10/17/2023 22:52:21	9 minutes ago	10/17/2023 22:52:21	1
56	localhost	http://localhost:8000/	10/17/2023 22:52:11	9 minutes ago	10/17/2023 22:52:11	1
57	localhost	http://localhost:8000/	10/17/2023 22:52:01	9 minutes ago	10/17/2023 22:52:01	1
58	localhost	http://localhost:8000/	10/17/2023 22:51:51	10 minutes ago	10/17/2023 22:51:51	1
59	localhost	http://localhost:8000/	10/17/2023 22:51:41	10 minutes ago	10/17/2023 22:51:41	1
60	localhost	http://localhost:8000/	10/17/2023 22:51:31	10 minutes ago	10/17/2023 22:51:31	1

« Prev

12345678910

Next »

localhost:8000/en-US/app/website_monitoring/search?q=search%20sourcetype%3D"web_ping"%20()%20title%3D"*"%20%20title%3Dlocalhost%20url%3D"http%3A%2F%2Flocalhost%3A8000%2F"%20%7C%20eval%20c...

searchsourcetype="web_ping" () title="*" title=localhost url="http://localhost:8000/" | eval content_hash=if(isnull(content_md5),content_md5,content_sha224)

Date time range

285 events (1/28/20 1:00:48.000 PM to 10/17/23 11:32:20.000 PM)No Event Sampling

Job

Smart Mode

Events (285)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect

1 month per column

< Hide FieldsAll Fields

SELECTED FIELDSa host 1a source 1a sourcetype 1INTERESTING FIELDSa content_hash 100+a content_md5 100+a content_sha224 100+# content_size 4a index 1# linecount 1a proxy_port 1a proxy_server 1a proxy_type 1a punct 1# request_time 100+# response_code 1a splunk_server 1a timed_out 1a timeout 1a timestamp 1a title 1a total_time 100+a url 1

ListFormat20 Per Page

>

10/17/2311:32:13.000 PM

response_code=200 total_time=40.04 request_time=40.04 timed_out=False title=localhost url=http://localhost:8000/ timeout=30 proxy_server="" proxy_type=http proxy_port="" content_md5=dcc2148f58d1233b8ffa35b489b2924b content_sha224=3f4419a88e96df2a1f7833746915af144df56f51f5cf7b323708144c content_size=13515 host = \$decideOnStartup | source = web_ping://localhost | sourcetype = web_ping

>

10/17/2311:32:03.000 PM

response_code=200 total_time=10.83 request_time=10.83 timed_out=False title=localhost url=http://localhost:8000/ timeout=30 proxy_server="" proxy_type=http proxy_port="" content_md5=1ad01c711ccc72c5dcf4e100fa22c8f2 content_sha224=d294c8bb8705ccdee14a664b19f0b03651f88bb04358ac3e37160588 content_size=13515 host = \$decideOnStartup | source = web_ping://localhost | sourcetype = web_ping

>

10/17/2311:31:53.000 PM

response_code=200 total_time=10.64 request_time=10.64 timed_out=False title=localhost url=http://localhost:8000/ timeout=30 proxy_server="" proxy_type=http proxy_port="" content_md5=351543f3d1dc9753f32c858bfcfce102 content_sha224=027e7b6382a7e08cf811910381c6334109c76e80f7bb3158b16e677a content_size=13516 host = \$decideOnStartup | source = web_ping://localhost | sourcetype = web_ping

>

10/17/2311:31:43.000 PM

response_code=200 total_time=10.38 request_time=10.38 timed_out=False title=localhost url=http://localhost:8000/ timeout=30 proxy_server="" proxy_type=http proxy_port="" content_md5=3da3ea767560588d46a08d55c27fae24 content_sha224=0645bb828dfb8cccedd8b0e7f966beb4afaa044719a6e97a69049515f content_size=13516 host = \$decideOnStartup | source = web_ping://localhost | sourcetype = web_ping

>

10/17/2311:31:33.000 PM

response_code=200 total_time=10.09 request_time=10.09 timed_out=False title=localhost url=http://localhost:8000/ timeout=30 proxy_server="" proxy_type=http proxy_port="" content_md5=a64eed073f1fc5d43a2dbb1b0bdd6552 content_sha224=d174f239596d2ae53d163ba43d169de550ac55c0db25a1890d0257b6 content_size=13516 host = \$decideOnStartup | source = web_ping://localhost | sourcetype = web_ping

>

10/17/2311:31:23.000 PM

response_code=200 total_time=11.7 request_time=11.7 timed_out=False title=localhost url=http://localhost:8000/ timeout=30 proxy_server="" proxy_type=http proxy_port="" content_md5=cad464af70c7af13237f1f304df2cf2e content_sha224=16cb4355f7c944a4f9932f026f36fb1a0f3d9c44f0424f46826e86bb content_size=13515 host = \$decideOnStartup | source = web_ping://localhost | sourcetype = web_ping

>

10/17/2311:31:13.000 PM

response_code=200 total_time=9.98 request_time=9.98 timed_out=False title=localhost url=http://localhost:8000/ timeout=30 proxy_server="" proxy_type=http proxy_port="" content_md5=f6bc8d163b93ee4bc358e208eb4be8ce content_sha224=944f5bce5253f969b704faf9a8ee527818fb69eead0ebaabe15af80d content_size=13515

7

Website Monitoring

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Executive SummaryStatus OverviewStatus HistoryChange HistoryCreate InputsHealthSearchConfigurationWhat's new in 2.9?Website Monitoring

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

2 Alerts

AllYoursThis App'sfilter

i	Title	Actions	Owner	App	Sharing	Status
Website Down Alert	Enabled: Yes. Disable Permissions: Private. Owned by admin. Edit Modified: Oct 17, 2023 11:46:23 PM Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit Trigger Condition: .. Number of Results is = 0. Edit Actions: 1 Action Edit Send email	Open in Search Edit	admin	website_monitoring	Private	Enabled
Website Performance Down Alert		Open in Search Edit	admin	website_monitoring	Private	Enabled

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

signatures with signature ids

source="windows_server_logs.csv" |table signature, signature_id|dedup signature_id

4,764 events (before 10/17/23 6:11:30.000 PM) No Event Sampling

Events Patterns Statistics (15) Visualization

20 Per Page Format Preview

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

Severity Stats | Splunk

localhost:8000/en-US/app/search/report?ts=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FSeverity%2520Stats&sid=admin__admin__search__RMD5d177622abe26eca0_at_1697589901_99&display=pag...

Severity Stats

All time

718 events (before 10/18/23 12:45:01.000 AM)

2 results 20 per page

severity	count	percent
informational	367	55.775076
high	291	44.224924

splunk>enterprise

success status

source="windows_server_logs.csv" status=success

4,622 events (before 10/17/23 6:15:24.000 PM) No Event Sampling

Events (4,622) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

< Hide Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Account_Domain 2

a Account_Name 100+

a action 5

a app 3

a body 100+

a category 8

a CategoryString 1

a change_type 2

i	Time	Event
>	3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,"Domain_A Domain_A",,"user_f user_1",,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,,4726,A user account was deleted,0,,,,,,,,,Audit Success,,,,Security,,,,,0xA36 9,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_f Show all 63 lines host = Window_server_logs source = windows_server_logs.csv sourcetype = csv
>	3/24/20 11:59:53.000 PM	2020-03-24T23:59:53.000+0000,"Domain_A Domain_A",,2020-03-24 23:59:53 PM,"user_k user_m",,,,server_2/computer_b,,,,,,,,,Account Management,,,,,,,,ACME-002,,,aaa,,,,-,4720,A user account was created,0,,,,,,\a\g,A:,,,,,Audit Succes s,,,,Security,,,A11,0xBAC3,,,,"SAM Account Name: user_h Display Name: aaa User Principal Name: ddd@BBB.local

splunk>enterprise

Windows Success v Failure

source="windows_server_attack_logs.csv" | top status

5,949 events (before 10/18/23 12:47:34.000 AM) No Event Sampling

Events (5,949) Patterns Statistics (2) Visualization

20 Per Page Format Preview

status	count	percent
success	5856	98.436712
failure	93	1.563288

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

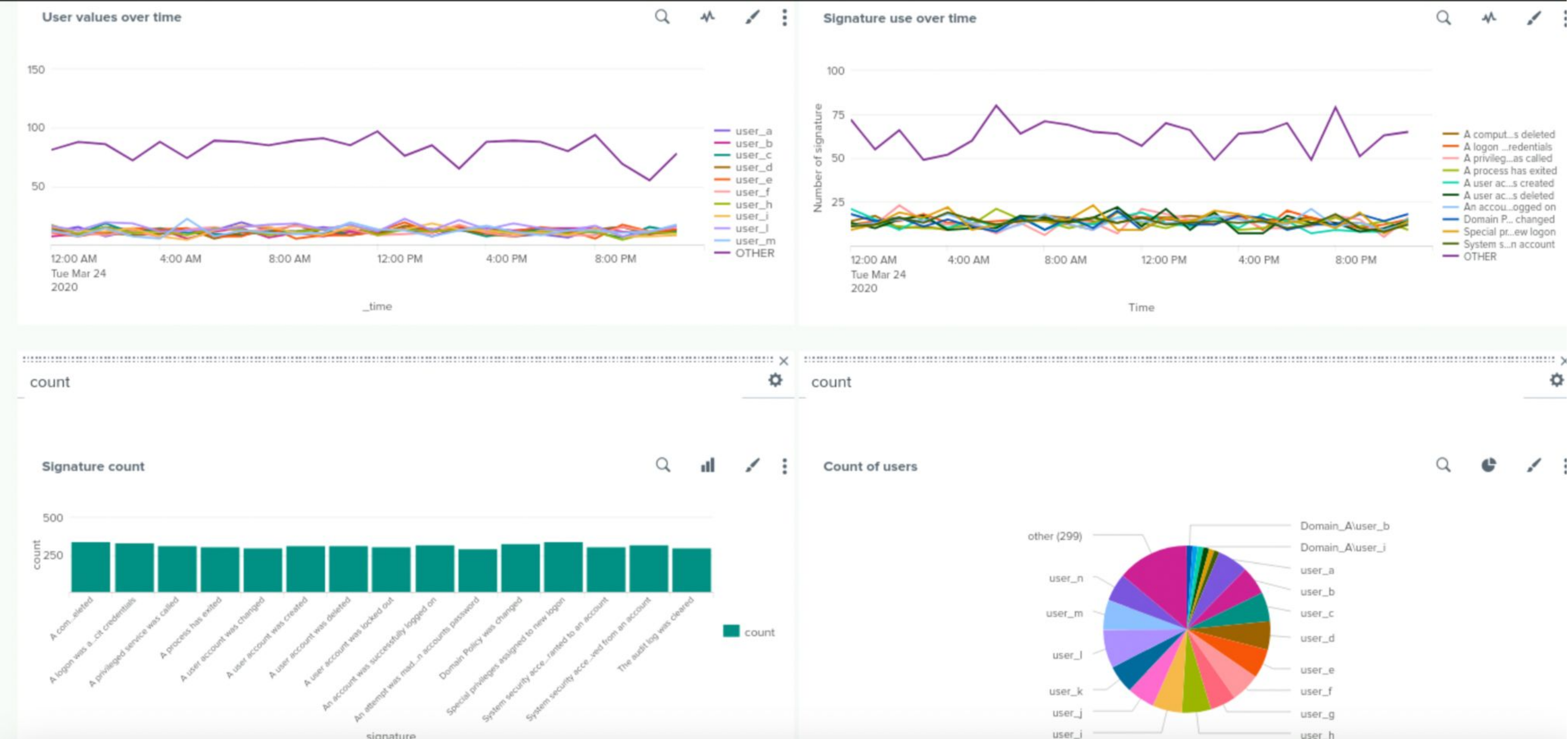
Alerts—Windows

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

All time

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

Edit

More Info

Add to Dashboard

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

All time

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

Edit

More Info

Add to Dashboard

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.)

HTTP Response Codes

All time ▾

✓ 10,000 events (before 10/13/23 1:33:52.000 AM)

Edit ▾

More Info ▾

Add to Dashboard

Job ▾

⏸

■

↺

↻

🖨

⬇

8 results20 per page ▾

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.

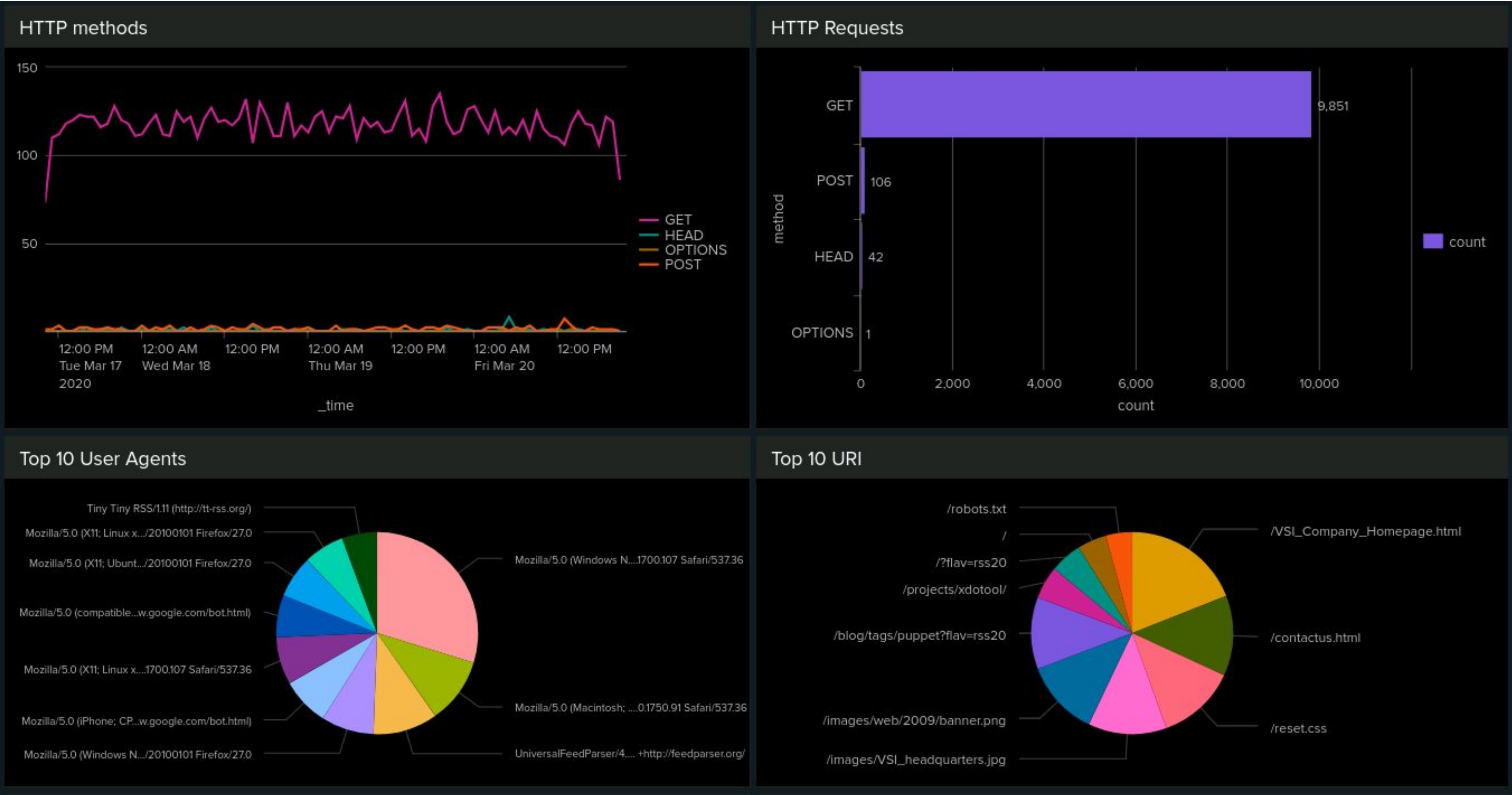
Alerts—Apache

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

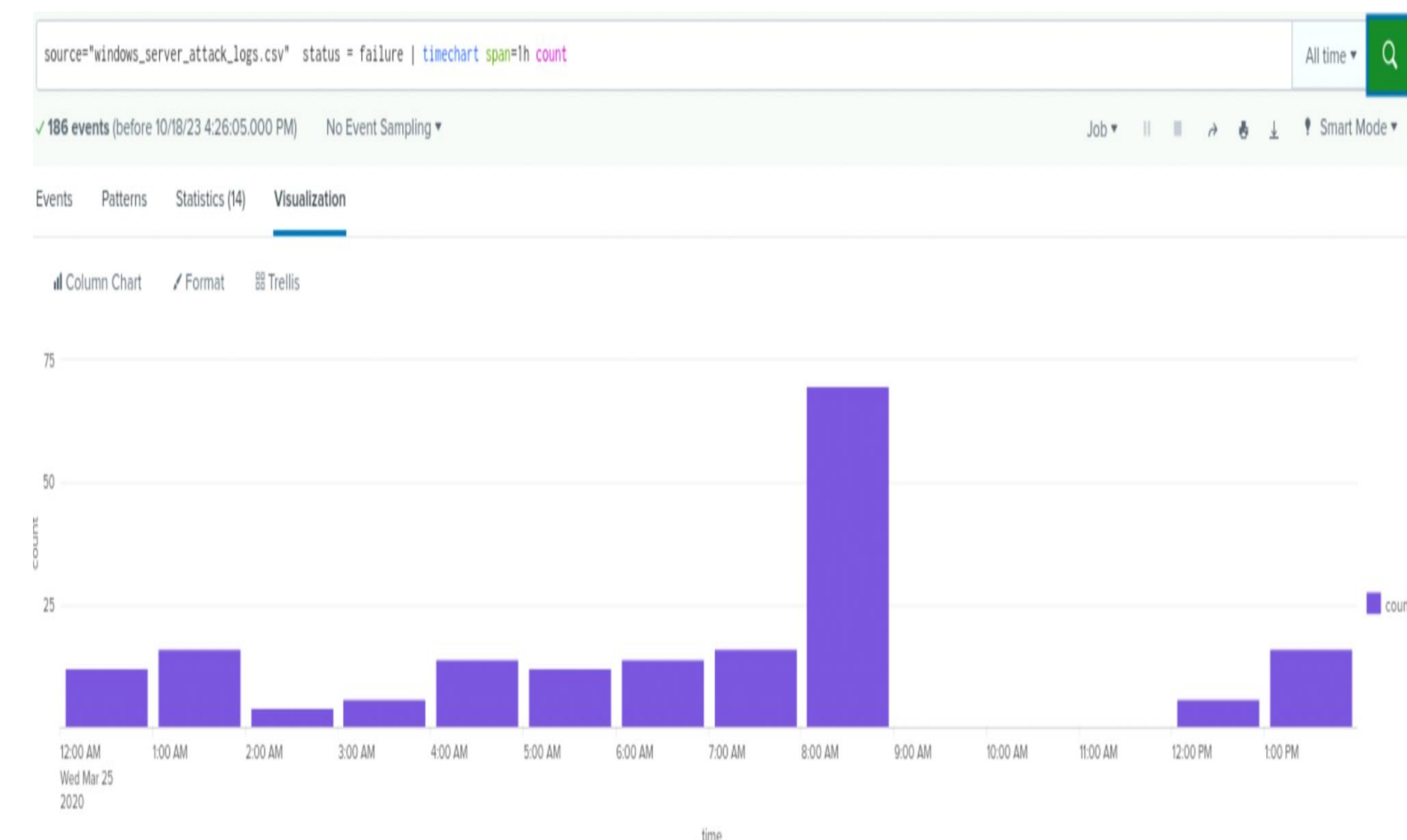
Summarize your findings from your reports when analyzing the attack logs.

- 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

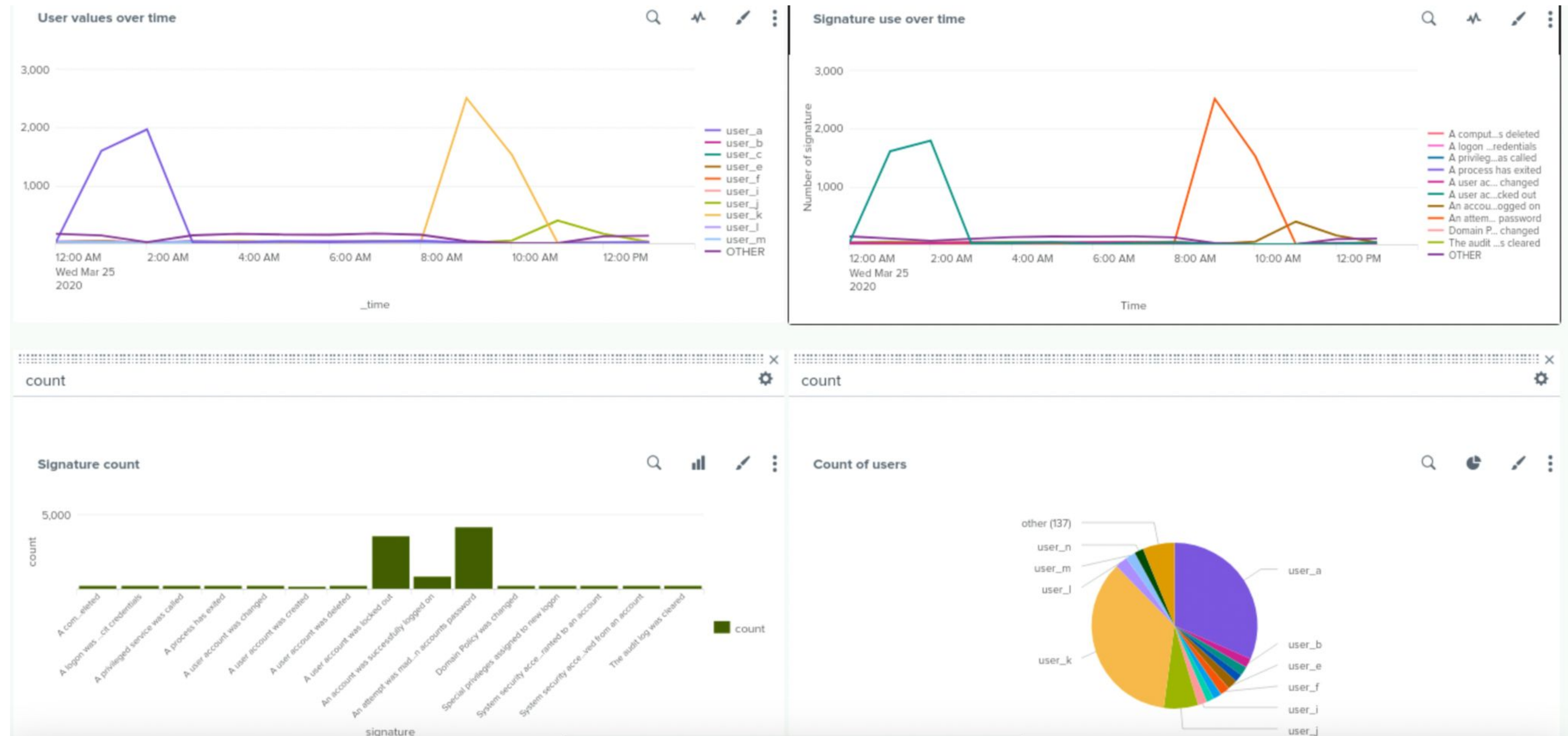
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- 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

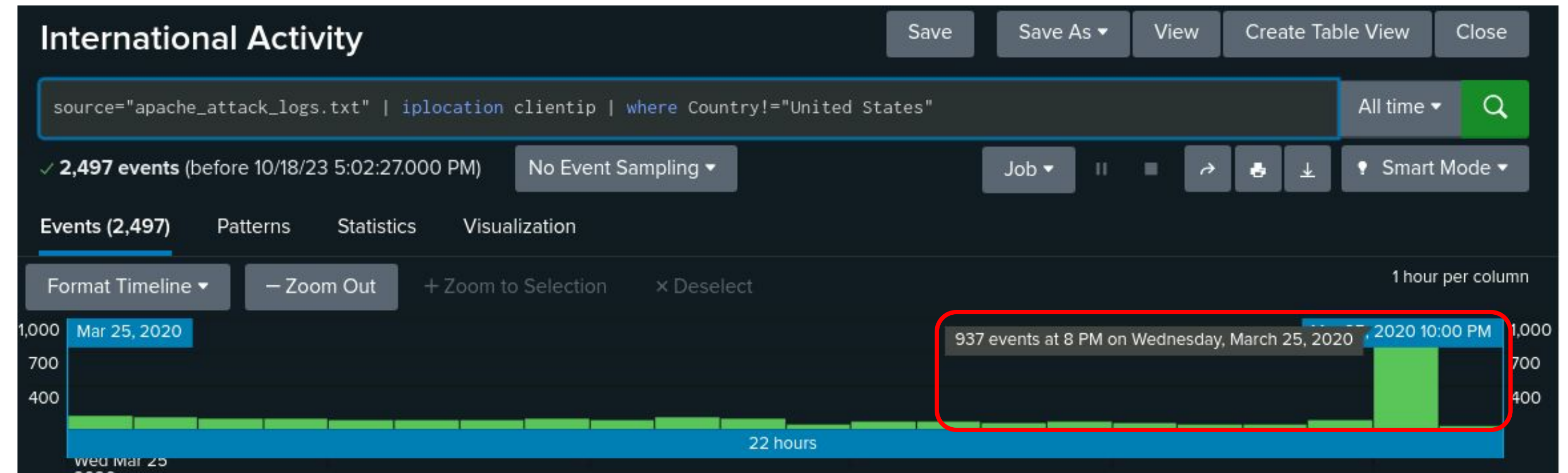
The image displays two screenshots of a 'HTTP Methods' dashboard. The top screenshot shows normal activity with 10,000 events before 10/13/23 1:34:47.000 AM. The bottom screenshot shows activity during an attack, with a significant decrease in GET requests and an increase in POST requests.

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

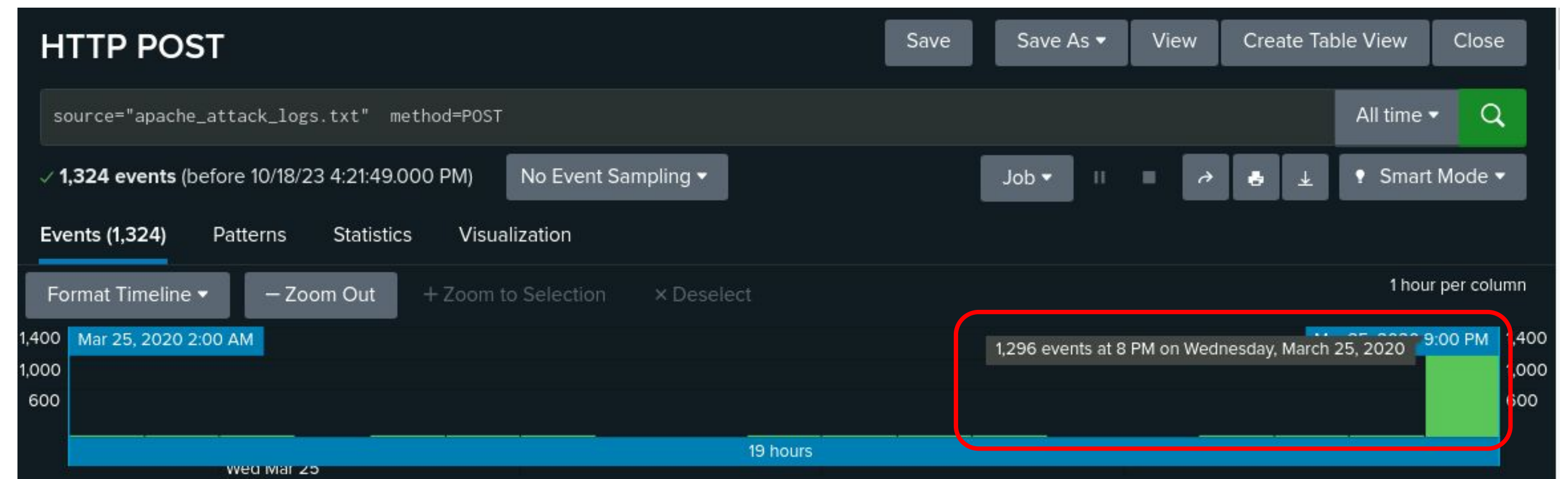
method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237

Attack Summary—Apache

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



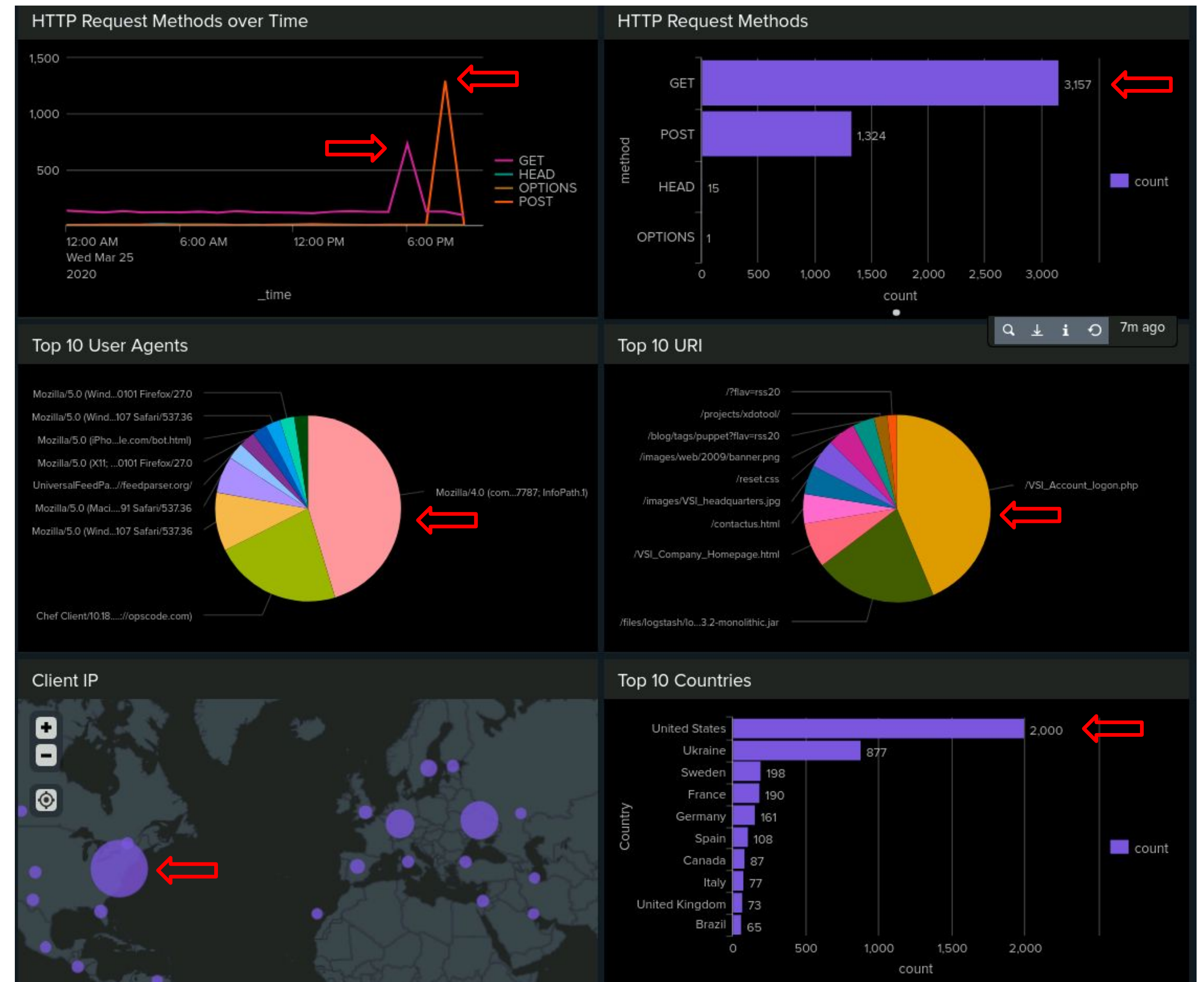
- HTTP POST Alert
 - > 10 events per hour
 - 1,296 events



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

referrer_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

32

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?