Defensive Security Project
by: Peter Groehler, Kiley Smith, Taylour Ousley, Marques Hairston, Connor Tindall

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- During this project, we worked for a company called VSI. Our mission was to use splunk to view security logs. We were to create alerts and reports on the companies standard use and then compare that to attack logs in order to find out where the attack occured.

[“Add-On” App]

Website Monitoring

The Add-On App Website Monitoring was chosen to supplement the Splunk Environment to:

- Monitor customer experience (lag times, speed)
- Gain better insights into common attack paths (denial of service, brute force)
- Determine additional hardware/software needs (more traffic = more servers)

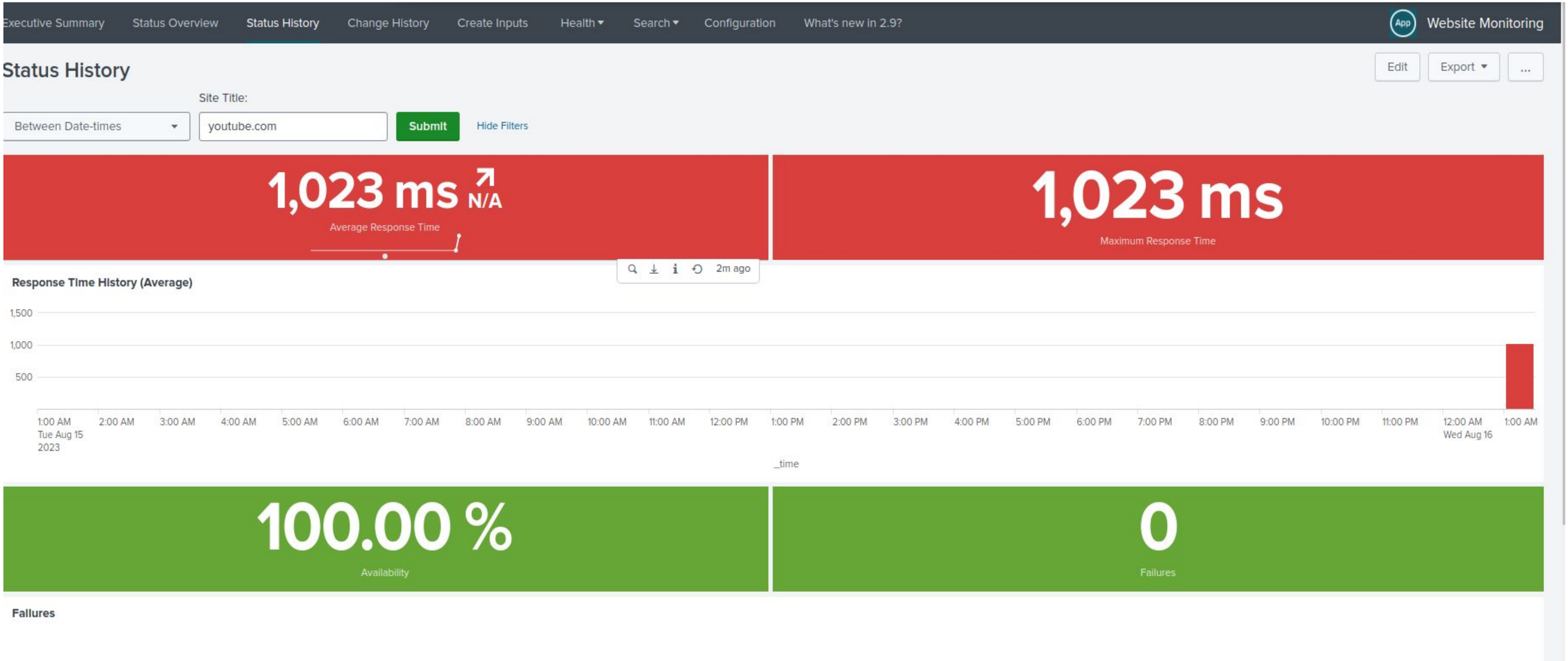
Website Monitoring

Website Monitoring allows for continuous insights into website responsiveness and uptime.

In the event of a Denial of Service (DOS) attack, analysts would be immediately alerted to a drop in website responsiveness and could determine when attack ended based on runtime data.

Daily use for Website Monitoring could be to determine whether additional hosting machines or servers may be needed to balance for increased user traffic.

Website Monitoring



Logs Analyzed

1 Windows Logs

The Windows logs contained information about Users. Information like account creations and deletions, log in failures and successes, etc. Any information regarding the status of the Windows users.

2 Apache Logs

The Apache logs hold information regarding the websites. The apache logs have HTTP methods, request and receiver websites, and HTTP status codes.

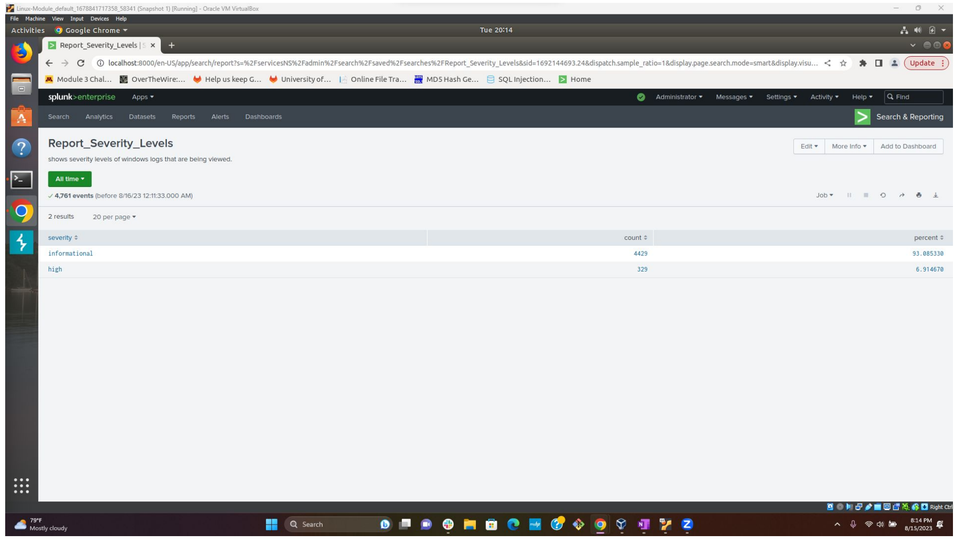
Windows Logs

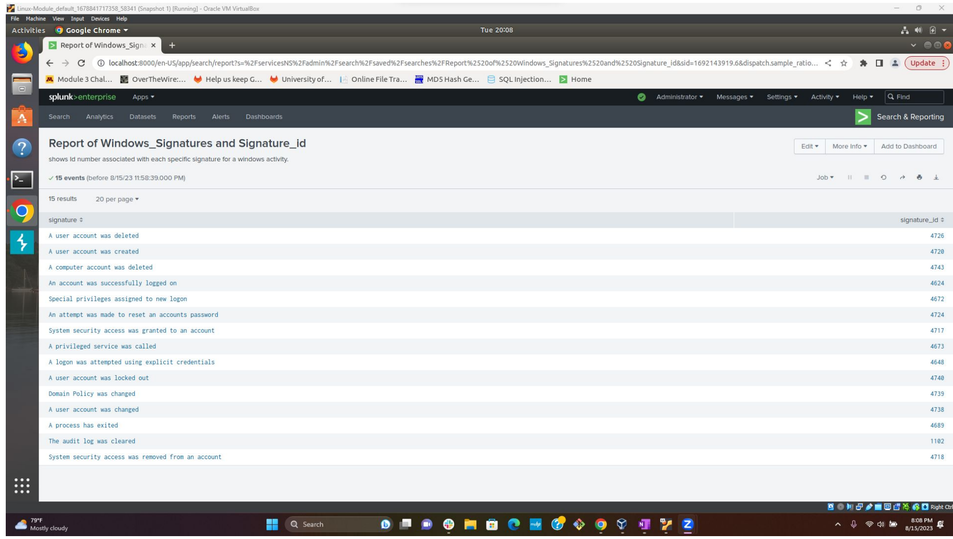
Reports—Windows

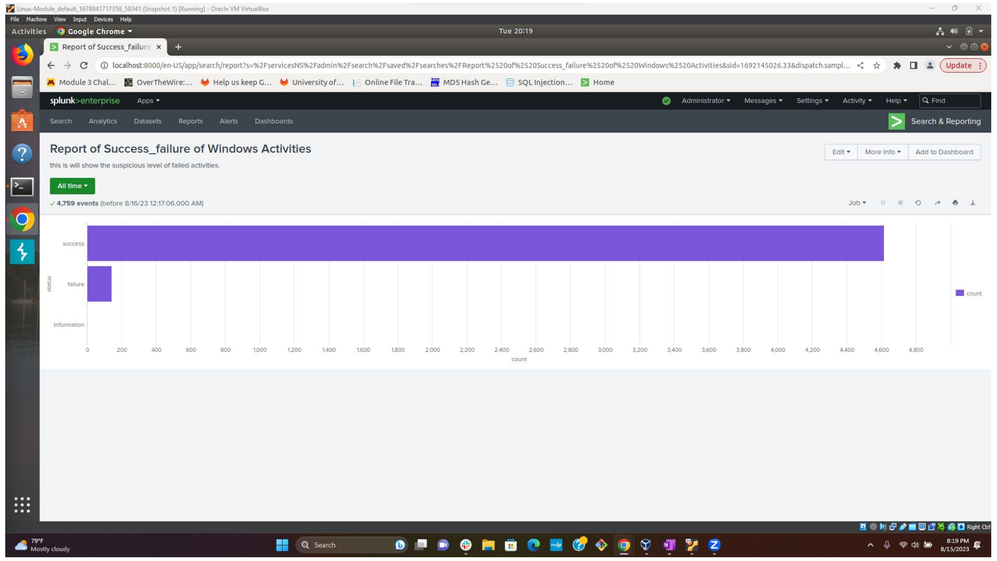
Designed the following reports:

Report Name	Report Description
Signatures	A report showing signatures and the corresponding signature ID.
Severity	This report shows the different severity levels and how many of each were present.
Windows Activities	A report detailing the successes and failures of windows activities.

Images of Reports—Windows







Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert_Account_Delete	Alerts SOC if account deletions for an hour are over the threshold.	10 deletions	15 deletions

JUSTIFICATION: Our baseline is set to the standard number of account deletions per hour, and the threshold of 15 is considered enough to be a potential attack.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful_Logins	Alerts SOC if >=80 successful login attempts in 1 hour	70	80

JUSTIFICATION: Our baseline is the average number of successful logins within 1 hour. Threshold is set at >= 10 additional logins per hour to attempt early detection of brute-force login attempts.

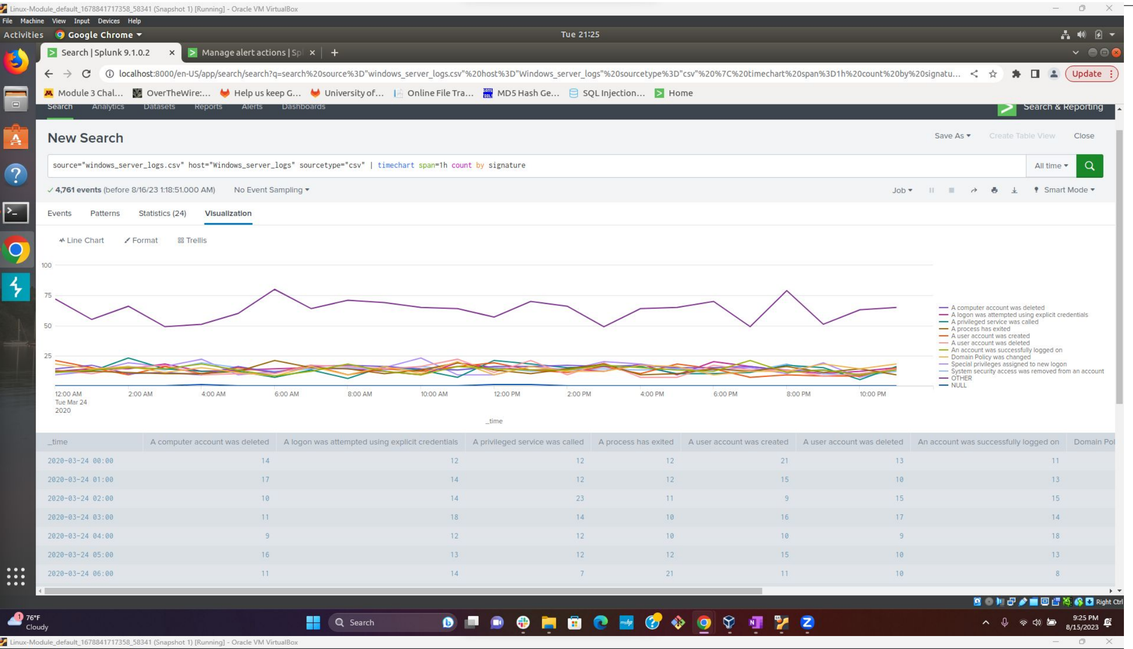
Alerts—Windows

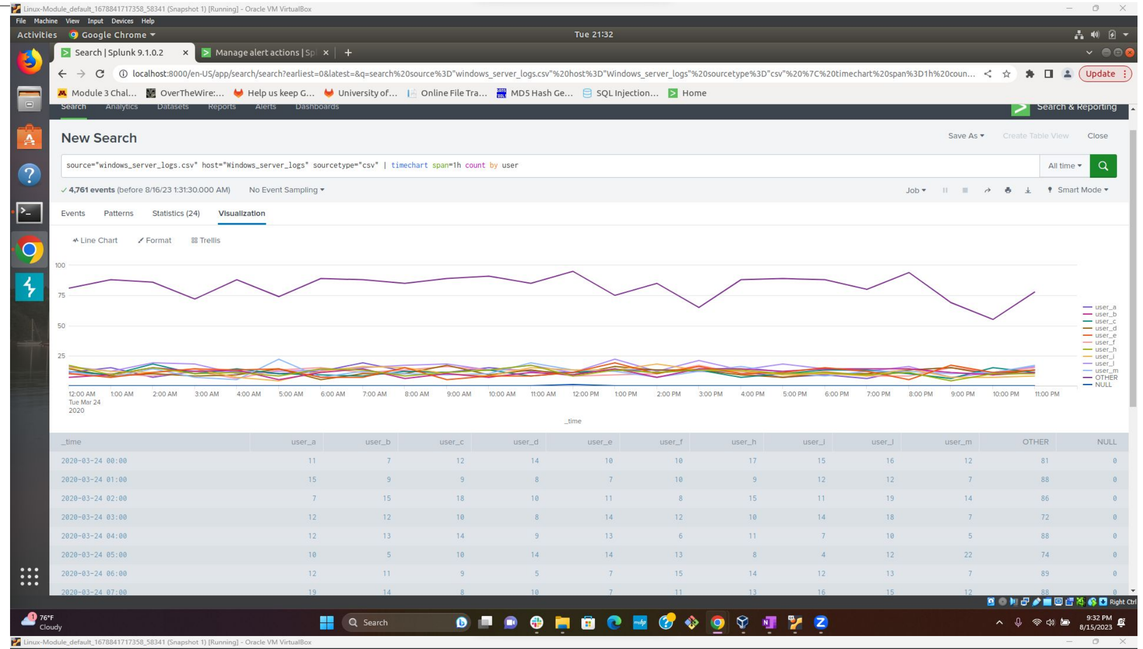
Designed the following alerts:

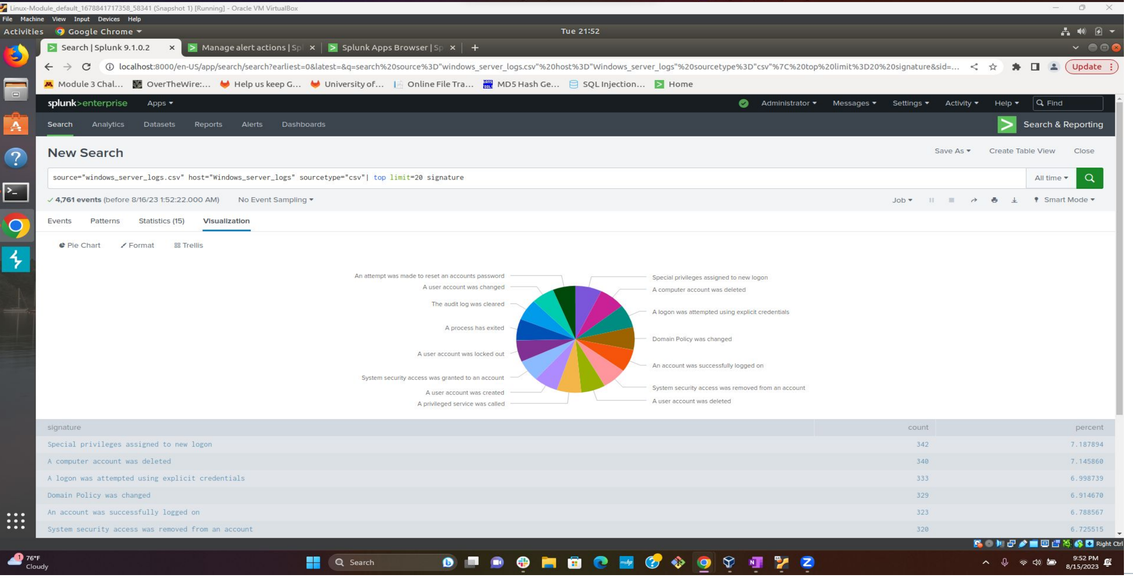
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed_Logins	Alerts SOC if >= 11 failed logins occur in 1 hour	7	11

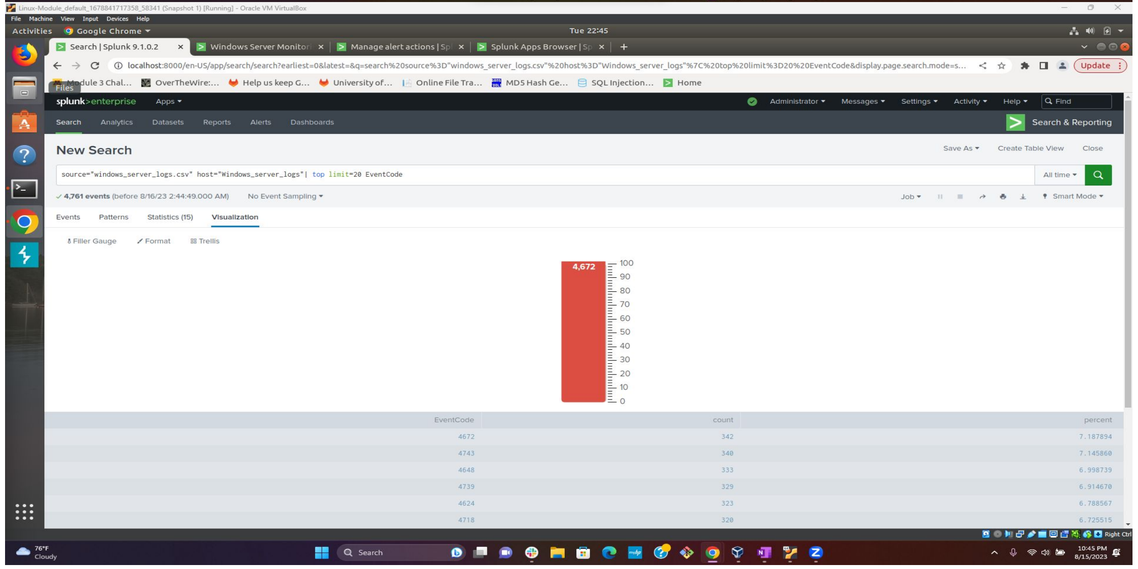
JUSTIFICATION: 7 is the average number of failed logins per hour. The threshold is set at 11 to both allow fluctuation in failed logins after extended breaks (holidays/vacations), but also to attempt early detection of brute-force attacks.

Dashboards—Windows

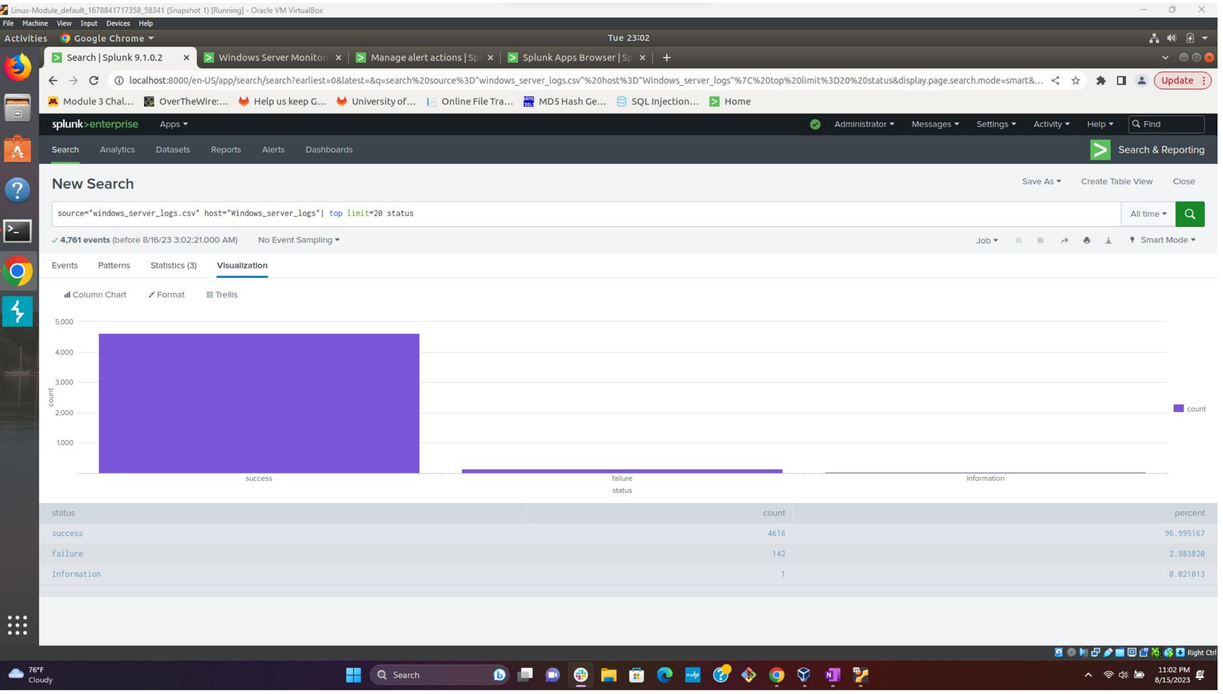


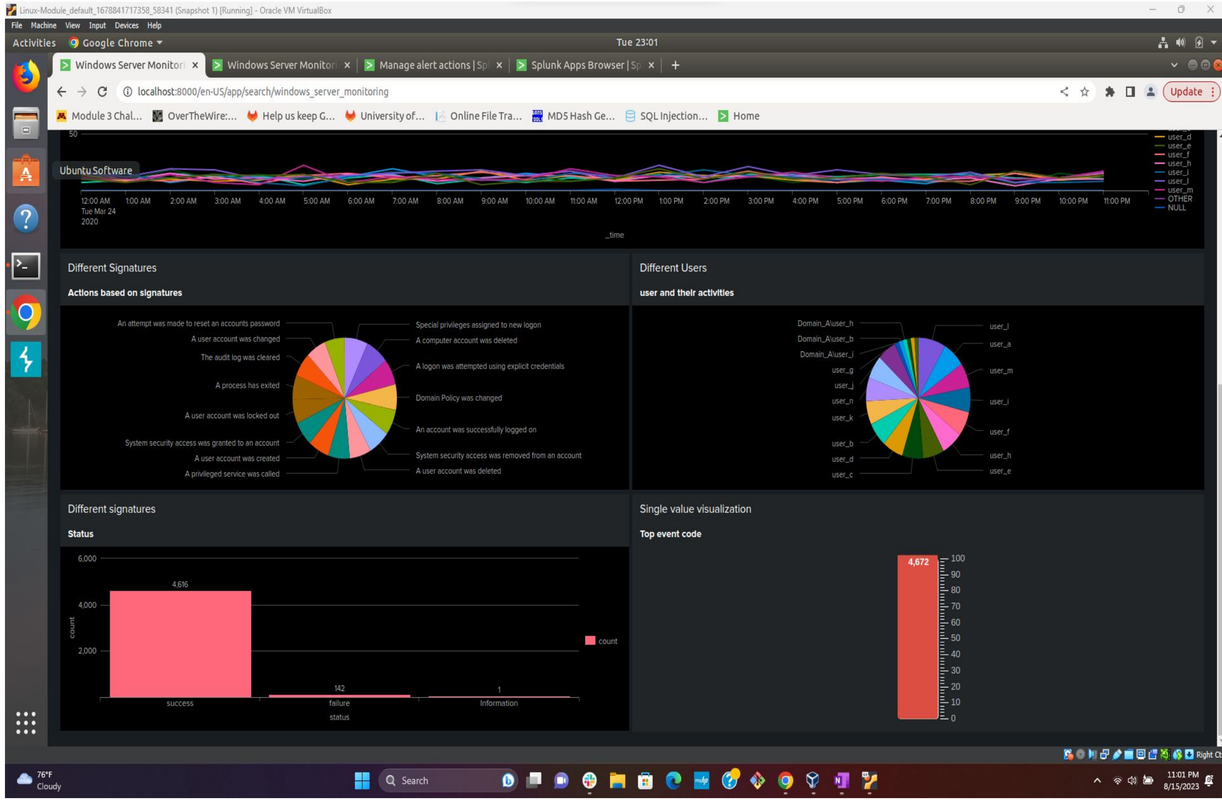






Dashboards—Windows





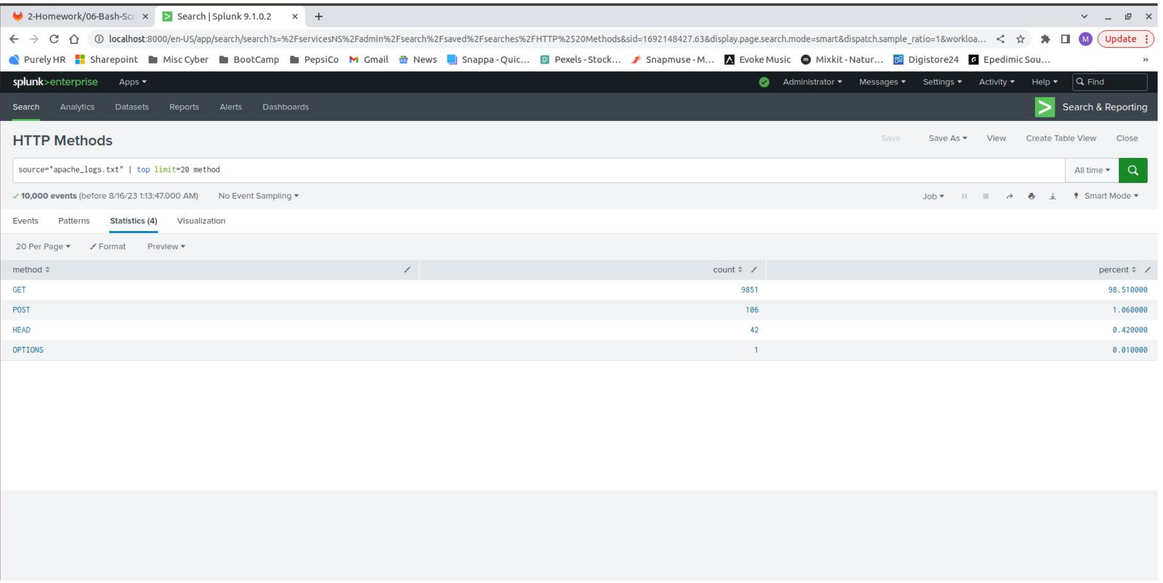
Apache Logs

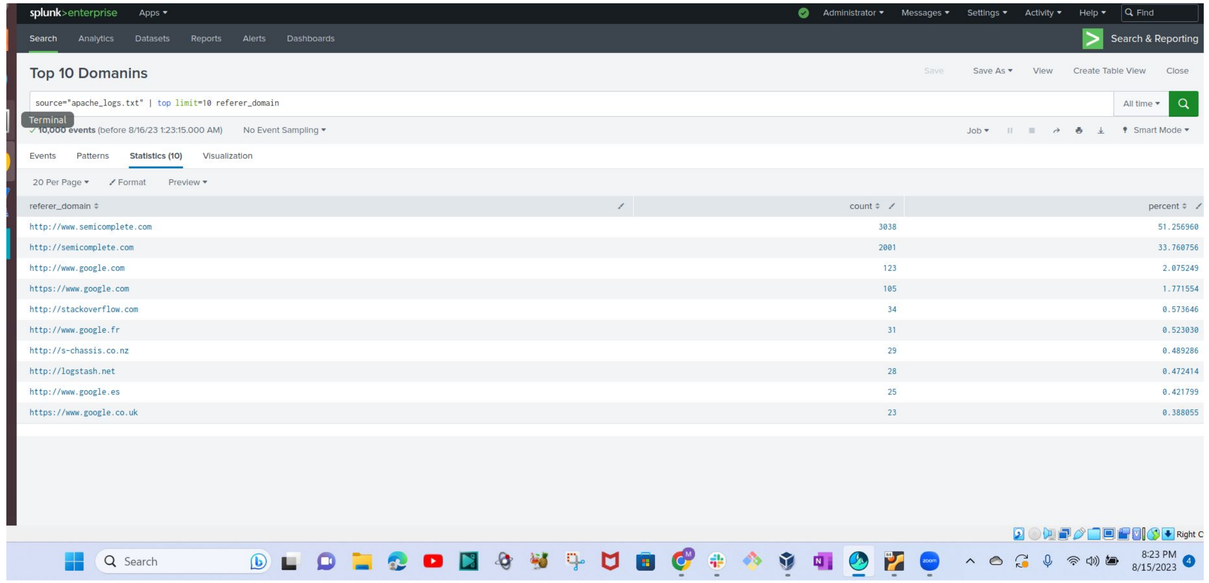
Reports—Apache

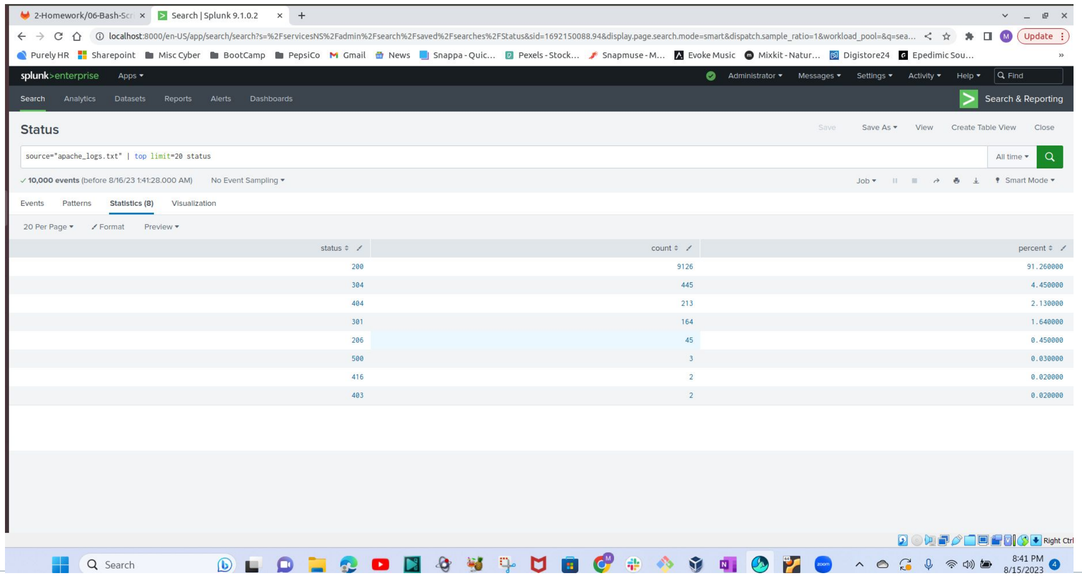
Designed the following reports:

Report Name	Report Description
HTTP Methods	A report of all the HTTP methods given to the Apache server.
Referrer Domains	Shows the top 10 domains that refer to our website.
HTTP Response Codes	Shows the different response codes

Images of Reports—Apache







Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non_US_Traffic	Alerts SOC if >= 80 non-US IPs identified in traffic in 1 hour	65	80

JUSTIFICATION: A baseline of 65 is the average number of non-US IPs seen in traffic in 1 hour. A threshold of 80 accounts for possible traffic for legitimate non-US clients, but provides early notification to foreign attacker activities.

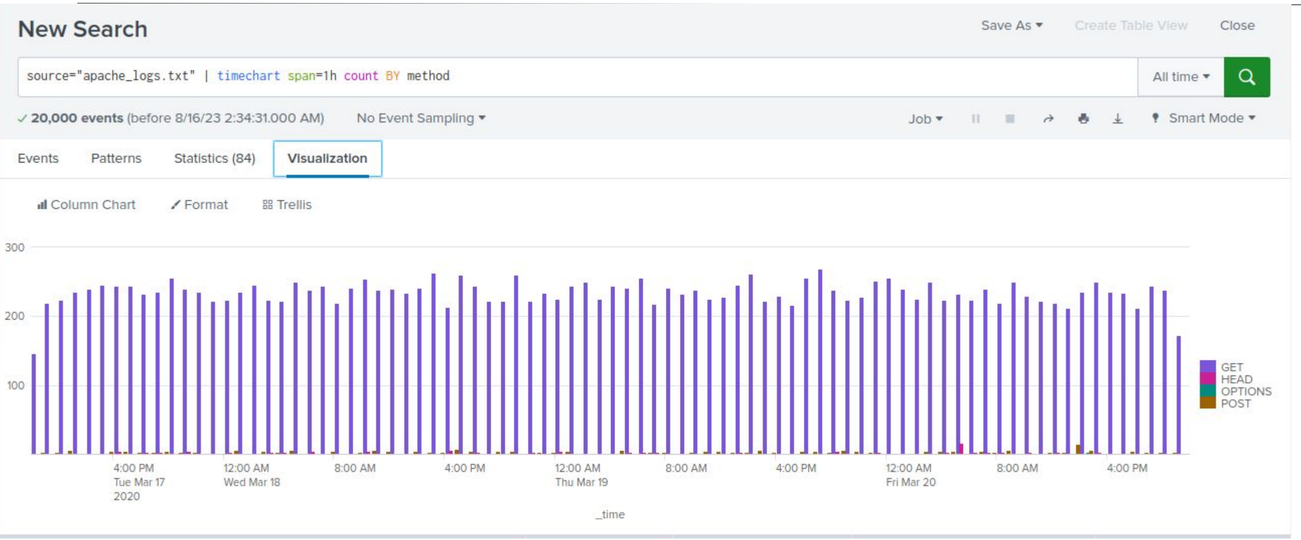
Alerts—Apache

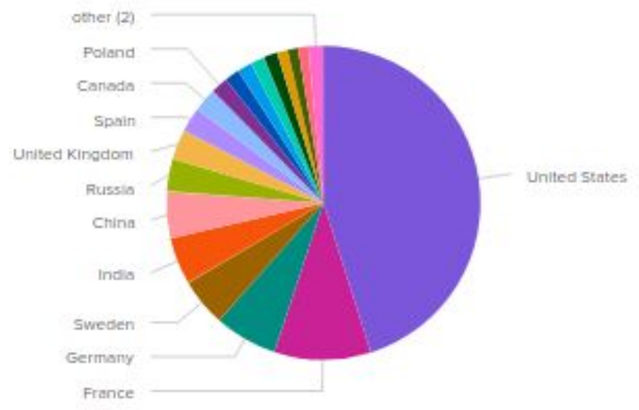
Designed the following alerts:

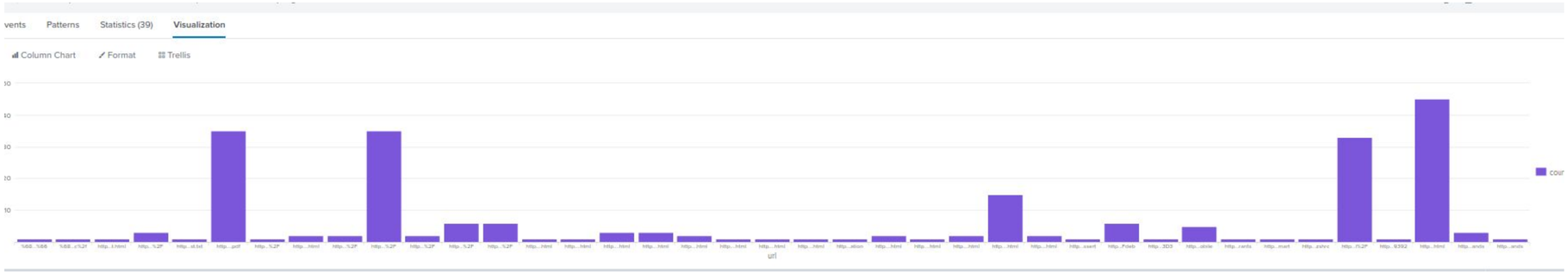
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP_POSTs	Alerts SOC if >= 7 HTTP POST requests are made in 1 hour.	4	7

JUSTIFICATION: A baseline was set at 4 as the high-end average of HTTP POST requests sent in 1 hour. A threshold of 7 per hour was set to account for any additional posts made above baseline by legitimate users, yet set low enough for early alerts on possible attacks.

Dashboards—Apache







Attack Analysis

Attack Summary—Windows

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

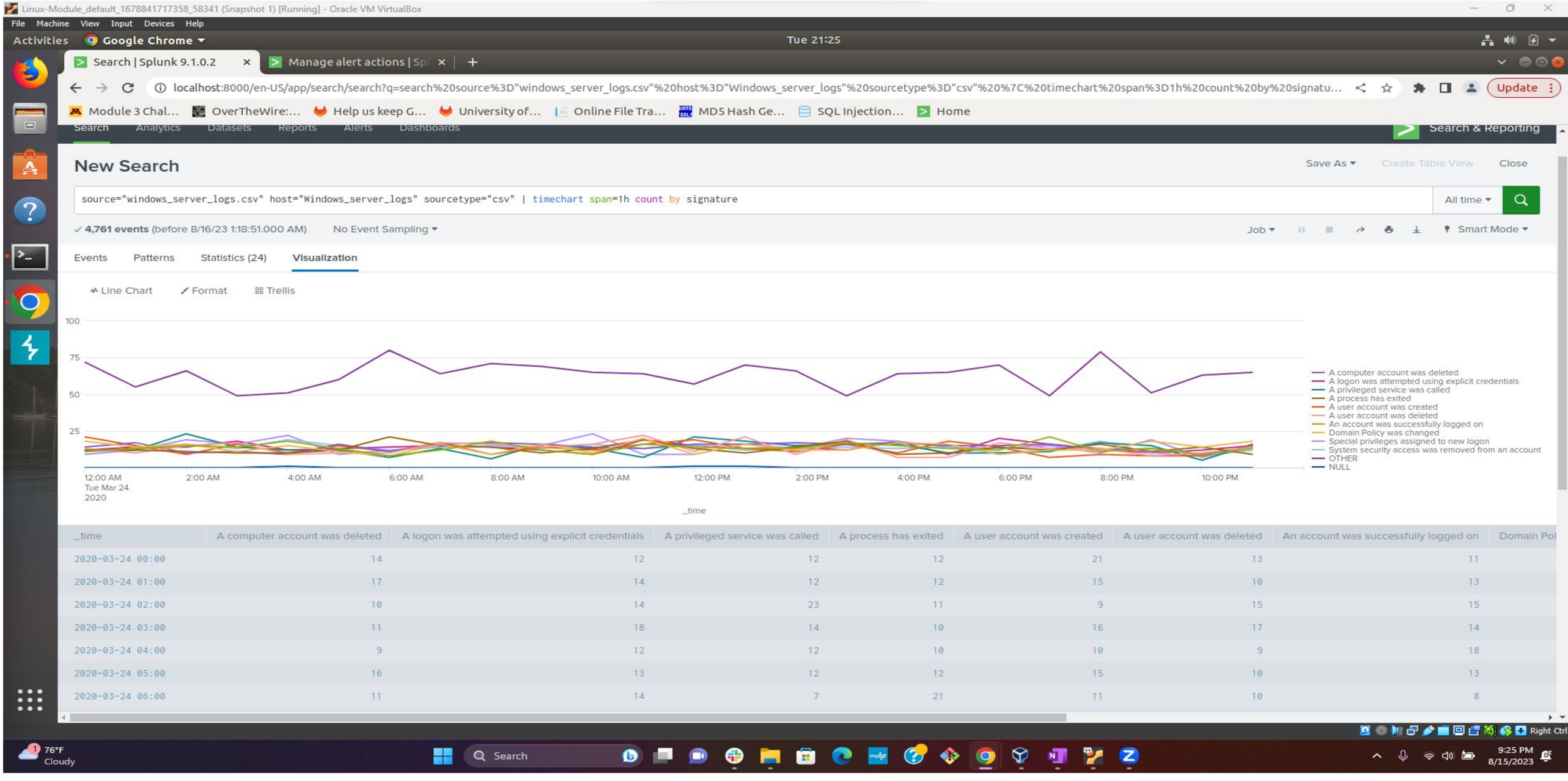
- Windows attack logs indicated a large influx of failed login attempts and password reset attempts that are indicative of a brute-force style attack.

Attack Summary—Windows

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

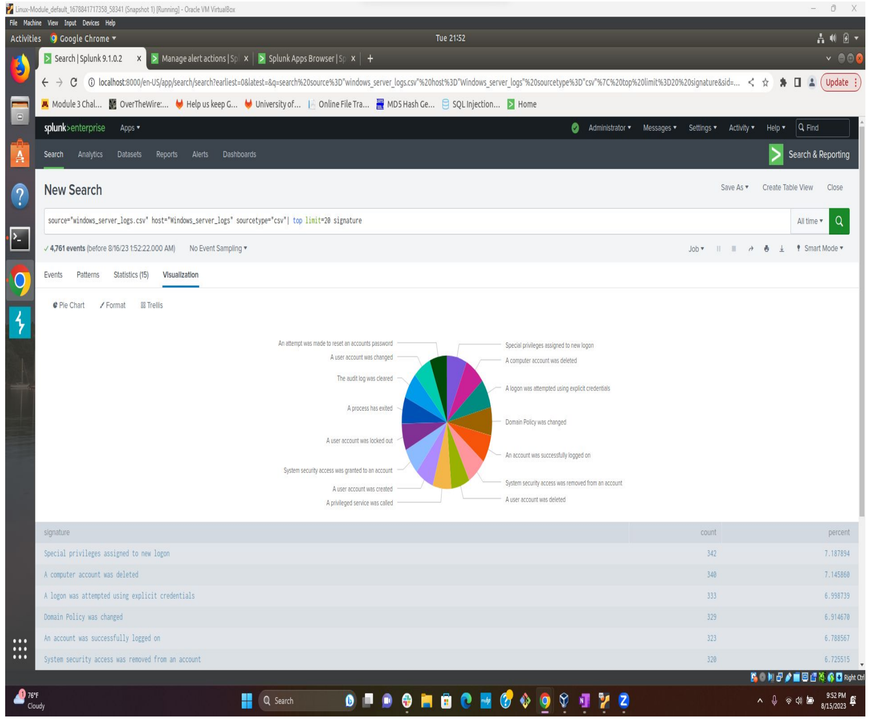
- A large number of events on a single user peaked during the attack at approx. 1,200 login attempts throughout the attack.

Pre-Attack Levels



_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was created	A user account was deleted	An account was successfully logged on	Domain Pol
2020-03-24 00:00	14	12	12	12	21	13	11	
2020-03-24 01:00	17	14	12	12	15	10	13	
2020-03-24 02:00	10	14	23	11	9	15	15	
2020-03-24 03:00	11	18	14	10	16	17	14	
2020-03-24 04:00	9	12	12	10	10	9	18	
2020-03-24 05:00	16	13	12	12	15	10	13	
2020-03-24 06:00	11	14	7	21	11	10	8	

Attack Levels

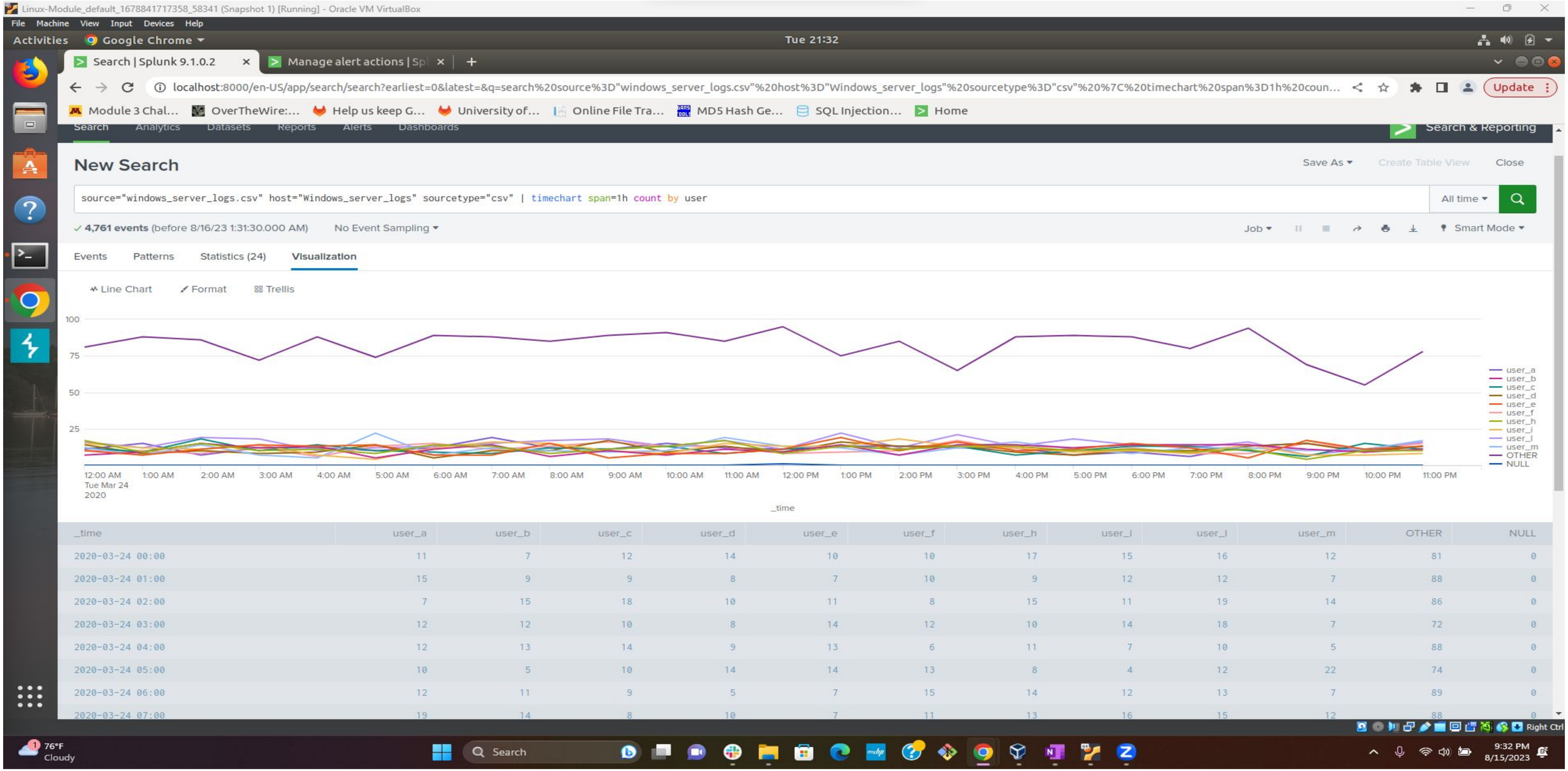


Attack Summary—Windows

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

- Password reset attempt lockouts for user k peaked at 1,258 during the attack
- `Peak for account lockout is 896 user a`

Pre-Attack Levels



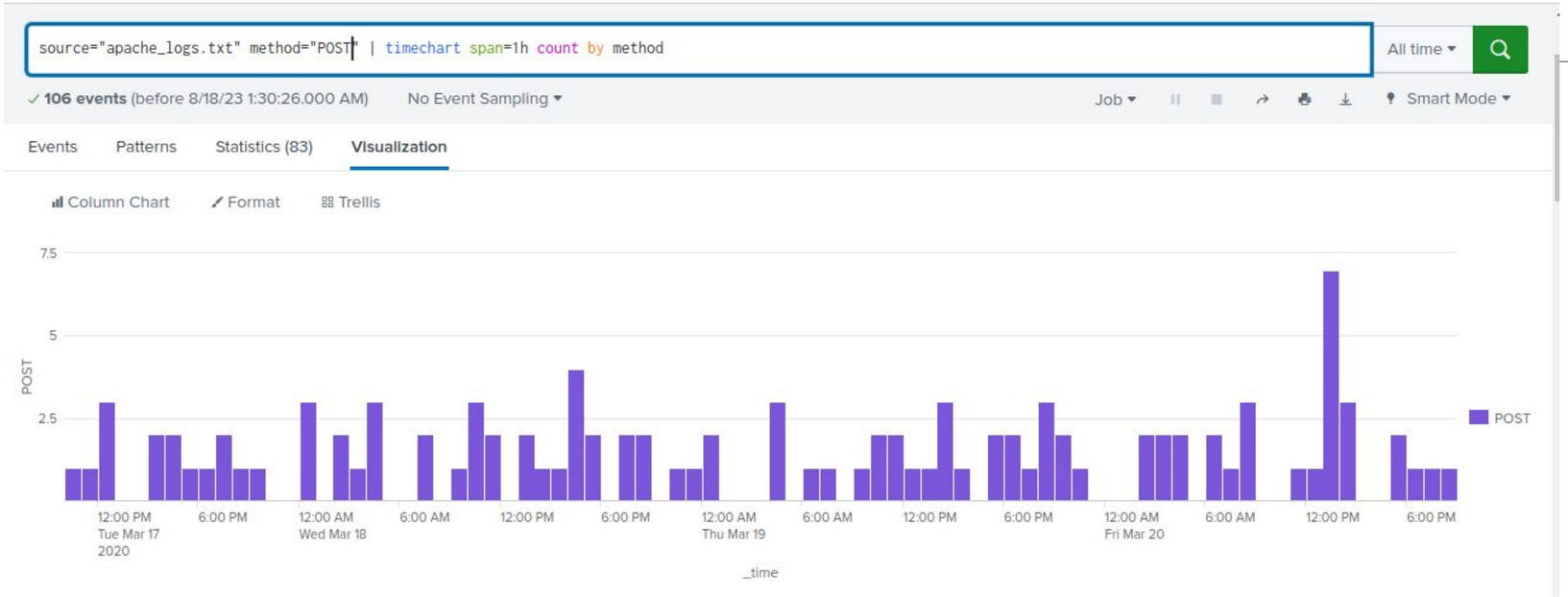
_time	user_a	user_b	user_c	user_d	user_e	user_f	user_h	user_i	user_j	user_m	OTHER	NULL
2020-03-24 00:00	11	7	12	14	10	10	17	15	16	12	81	0
2020-03-24 01:00	15	9	9	8	7	10	9	12	12	7	88	0
2020-03-24 02:00	7	15	18	10	11	8	15	11	19	14	86	0
2020-03-24 03:00	12	12	10	8	14	12	10	14	18	7	72	0
2020-03-24 04:00	12	13	14	9	13	6	11	7	10	5	88	0
2020-03-24 05:00	10	5	10	14	14	13	8	4	12	22	74	0
2020-03-24 06:00	12	11	9	5	7	15	14	12	13	7	89	0
2020-03-24 07:00	19	14	8	10	7	11	13	16	15	12	88	0

Attack Summary—Apache

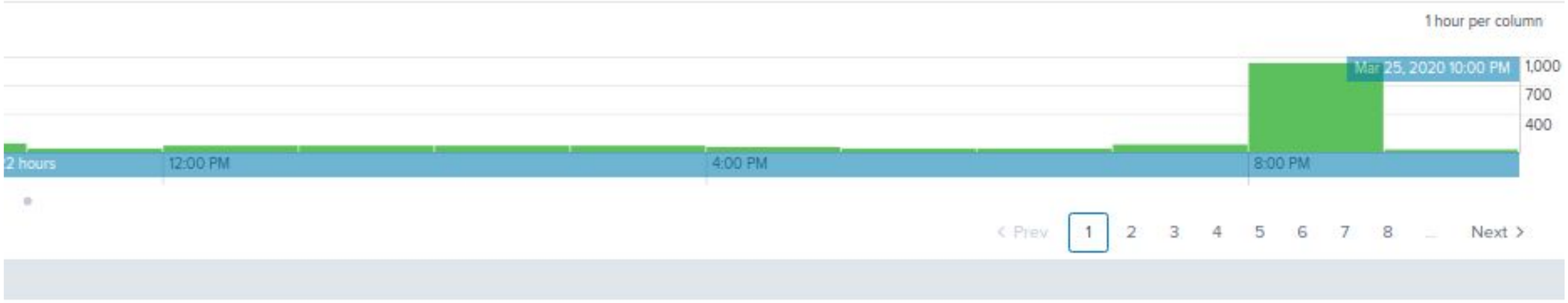
Summarize your findings from your reports when analyzing the attack logs.

- During the attack, a large increase was seen in the number of HTTP POST requests (1,296) over baseline (7)

Pre-Attack Levels



Attack Levels

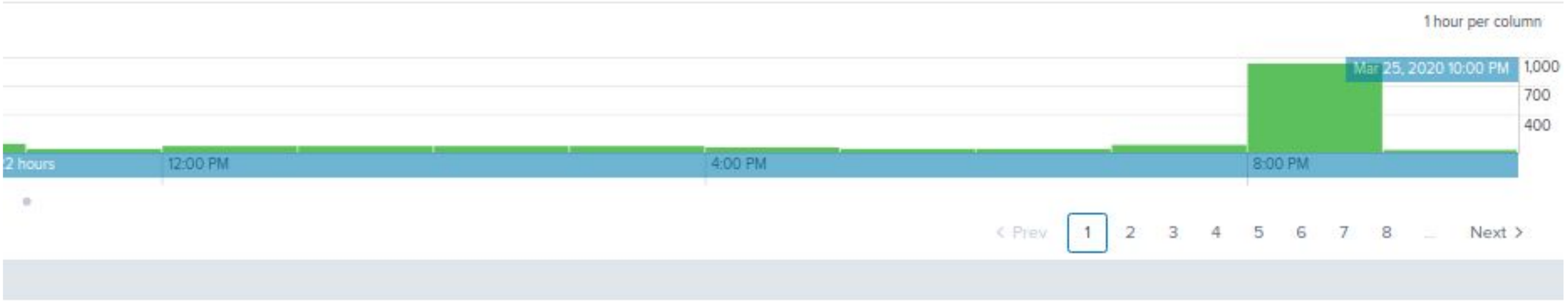


:ompatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)"

Attack Summary—Apache

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

- Amount of non-US IP traffic both rapidly increases and diversifies during the attack



:ompatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)"

Attack Summary—Apache

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

- Apache attack logs showed a large increase in HTTP POST requests from foreign sources, which would indicate a Denial of Service style attack.

Summary and Future Mitigations

Project 3 Summary

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

  Foreign state actors executed a Denial of Service (DOS) style attack against VSI by flooding HTTP POST requests to attempt to crash the website.

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

  Use rate limiting to put a cap on HTTP methods over to prevent DOS Attacks like GET/POST floods

  Increase load balancing so future attacks are not as effective