Defensive Security Project

By:

Habib Ullah
Dinelka Balasuriya
Hamza Ozsehitoglu
Hudayfa Bashir

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- We’re a team of SOC analysts for VSI (Virtual Space Industries)

- We have been hearing rumours of a potential cyber attack intended to disrupt our companies systems.

  - Main suspect is VSI’s competitor JobeCorp

- As SOC analysts, we designed reports, alerts and a dashboard to stay on top of the going’s on of our systems.

- Utilising these tools, we confirmed that there was a cyberattack on our systems which will be explained shortly…

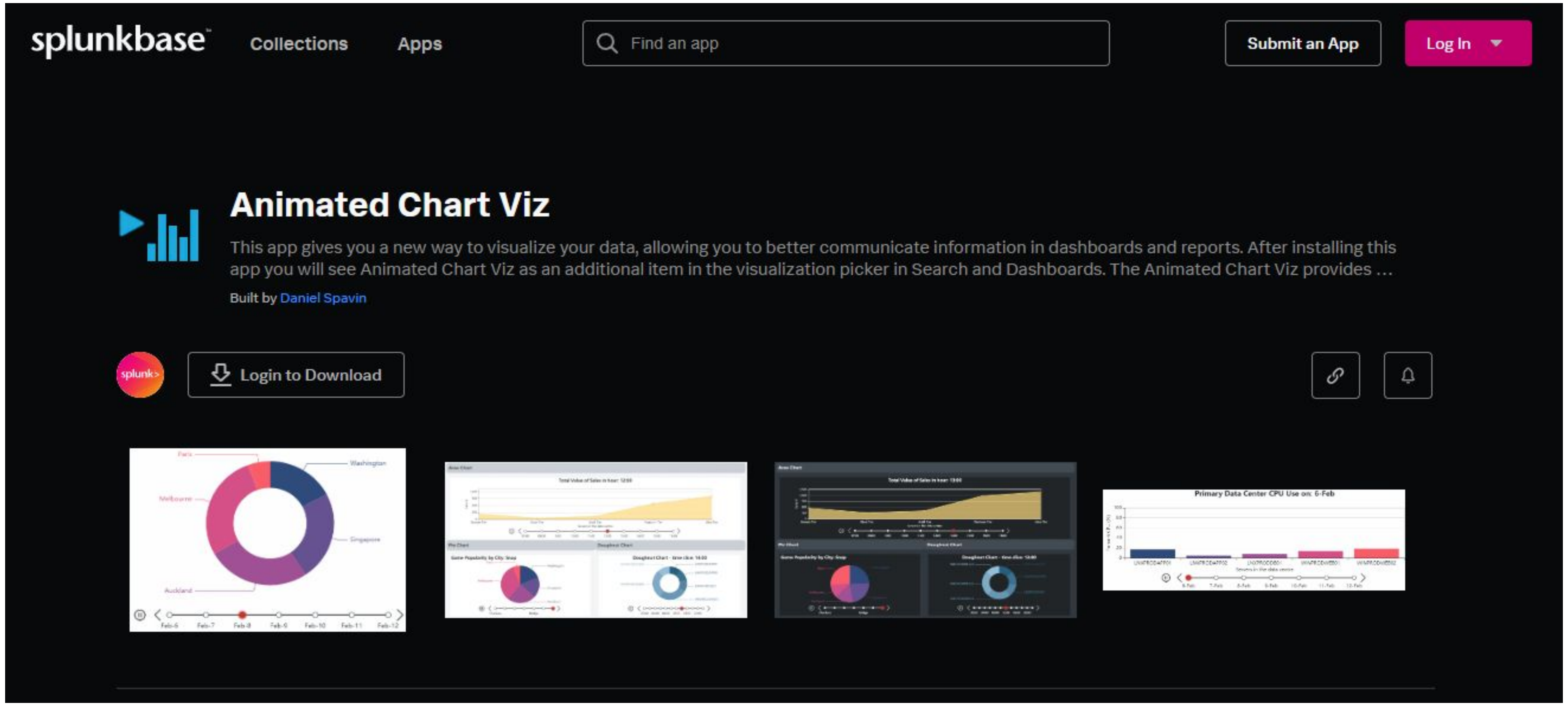
Animated Chart Viz

Animated Chart Viz

- This app allows us to make our dashboards and reports far more interactive.
- Utilizes ‘timechart’ command
- Animated charts divide the time-based data into segments and displays them sequentially.
- This allows the team to keep an eye out for any suspicious activities peripherally in addition to routine checks.

App supports:

- Pie charts
- Bar Charts
- Line Charts
- Area Charts
- Doughnut Charts



Animated Chart Viz

This app gives you a new way to visualize your data, allowing you to better communicate information in dashboards and reports. After installing this app you will see Animated Chart Viz as an additional item in the visualization picker in Search and Dashboards. The Animated Chart Viz provides …

Built by Daniel Spavin

Logs Analyzed

1 Windows Logs

- Windows servers running VSI's back-end systems.

- Severity Levels in the form of % and counts hourly
- Signatures of events on an hourly basis
- Users active during attack
- Status of activities (whether successful or unsuccessful)

2 Apache Logs

- Apache web servers hosting VSI's web application.

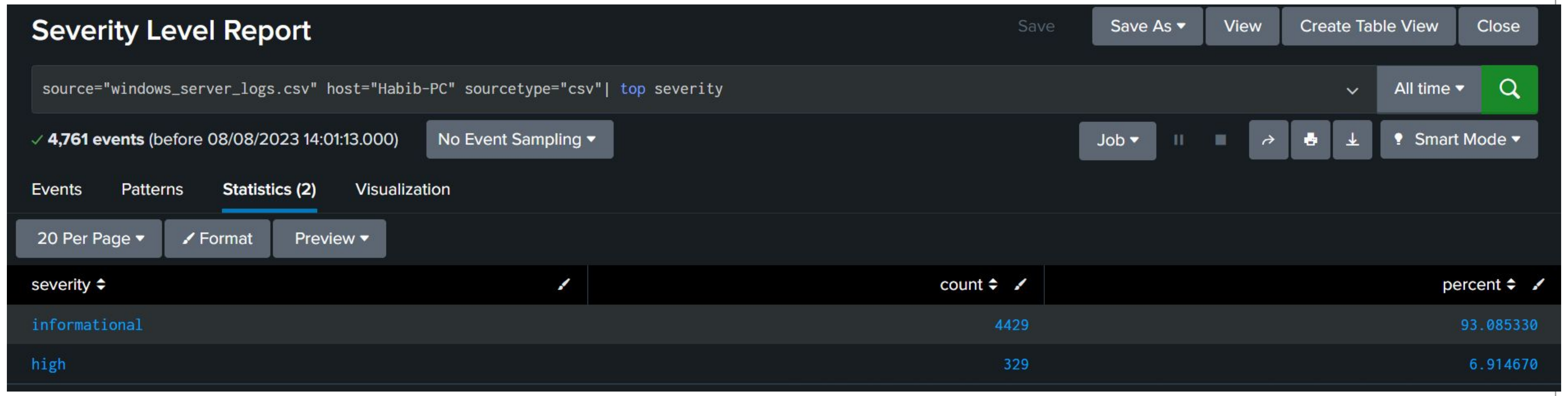
- Useragents (Particular web browsers used)
  + Clients IP
- Methods
  + Status of HTTP responses
-

Windows Logs

Reports—Windows

Report Images

Report Description



Severity Level Report

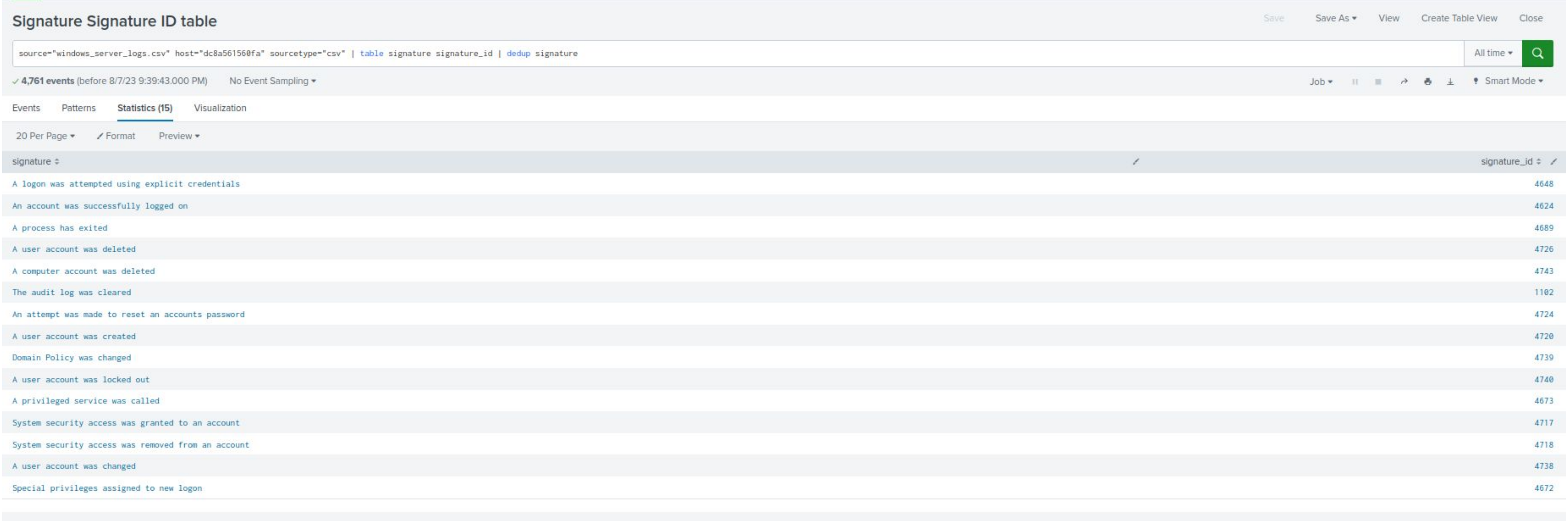
```
source="windows_server_logs.csv" host="Habib-PC" sourcetype="csv"| top severity
```

✓ 4,761 events (before 08/08/2023 14:01:13.000)

severity	count	percent
informational	4429	93.085330
high	329	6.914670

Severity Level Report

Provides quick understanding of severity levels of certain event signatures. (inc. counts and %)



Signature Signature ID table

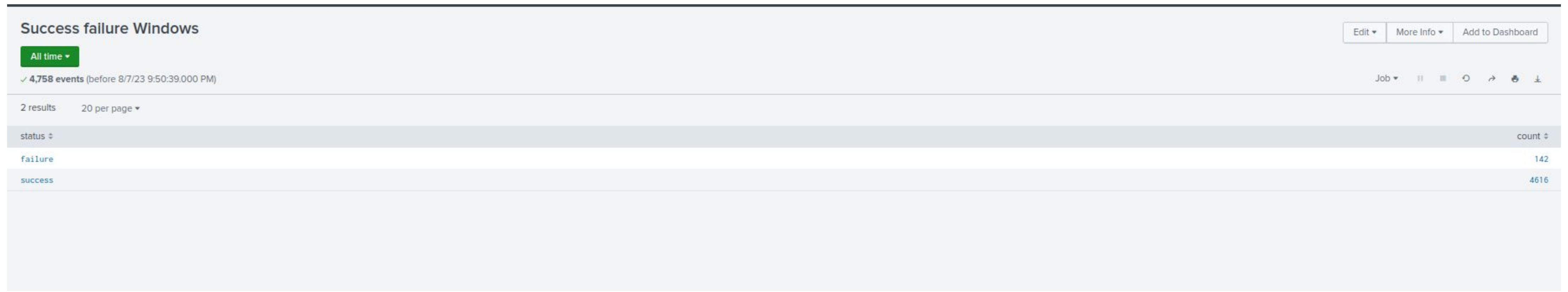
```
source="windows_server_logs.csv" host="dc8a561560fa" sourcetype="csv" | table signature signature_id | dedup signature
```

✓ 4,761 events (before 8/7/23 9:39:43.000 PM)

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

Signature & Signature ID Report

Displays ID number's along with the respective signature.



Success failure Windows

✓ 4,758 events (before 8/7/23 9:50:39.000 PM)

2 results

status	count
failure	142
success	4616

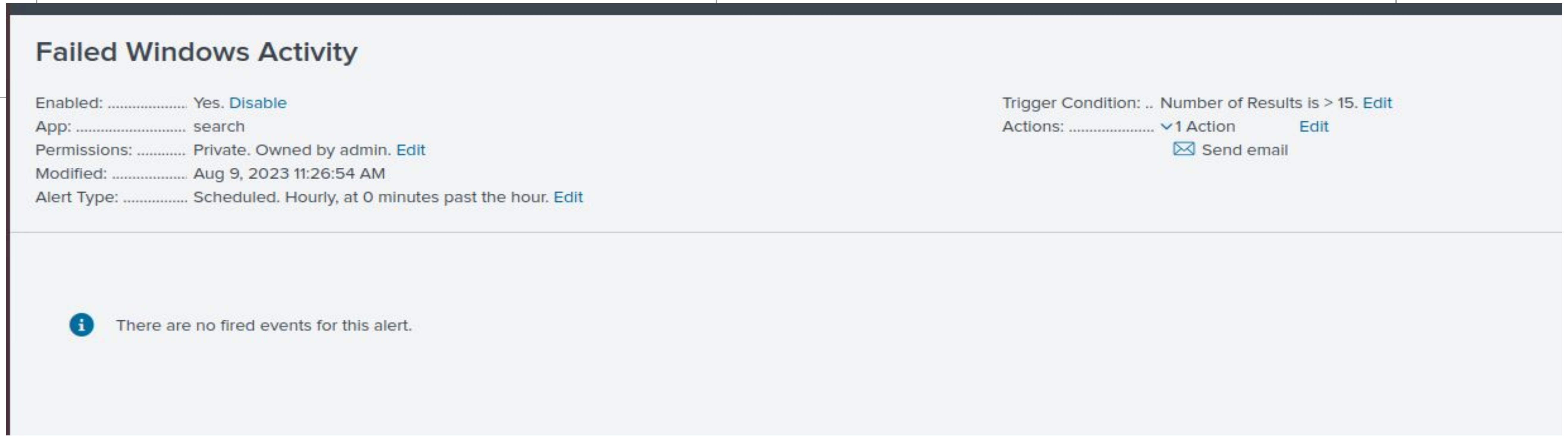
Status - Success/failure Report

Report's if there is an unusual amount of failed Windows activities.

!!ALERTS!!

Alerts—Windows

Alert Name	Alert Description	Baseline	Threshold
Failed_Windows_Activity	Alert sent to SOC email after 15 failed windows activities.	10	15



Failed Windows Activity

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 9, 2023 11:26:54 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

JUSTIFICATION:

BASELINE: After reviewing the count of failed windows activities on a regular day, we concluded 10 is the average.

THRESHOLD: Low enough to detect an attack and high enough to allow room for human error or outliers. This also makes sure we aren’t unaware of unusual spikes.

- Such a spike occurred on the 25th; 35 failed activities between 8am-9am.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful_logins	Email sent to SOC team when threshold is triggered when successful logins hourly threshold is surpassed.	20	25

JUSTIFICATION:

BASELINE: After reviewing business logs on a regular day, we concluded the average was 20.

THRESHOLD: We then raised the threshold to 25 to allow room for regular user accounts.

- An alert was triggered on the 25th; at 11am the count peaked at 196, far exceeding the threshold.

Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows_Account_was_deleted	Triggers alert when threshold of deleted accounts is met. Email sent to SOC team.	15	25

JUSTIFICATION:
BASELINE: After reviewing activities on regular business days, we saw the average was 15.
THRESHOLD: We then gave it a threshold of 25 deleted accounts to allow room, however, we didn’t raise it too high as having the wrong accounts deleted could be detrimental.

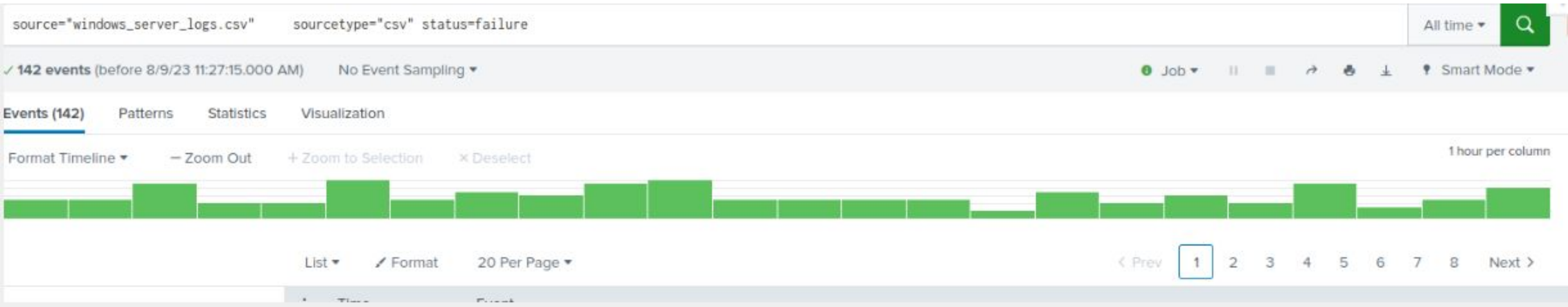
- However, this may result in alert fatigue as the gap is narrow; set to be reviewed by SOC team.

Summary of Windows Attack

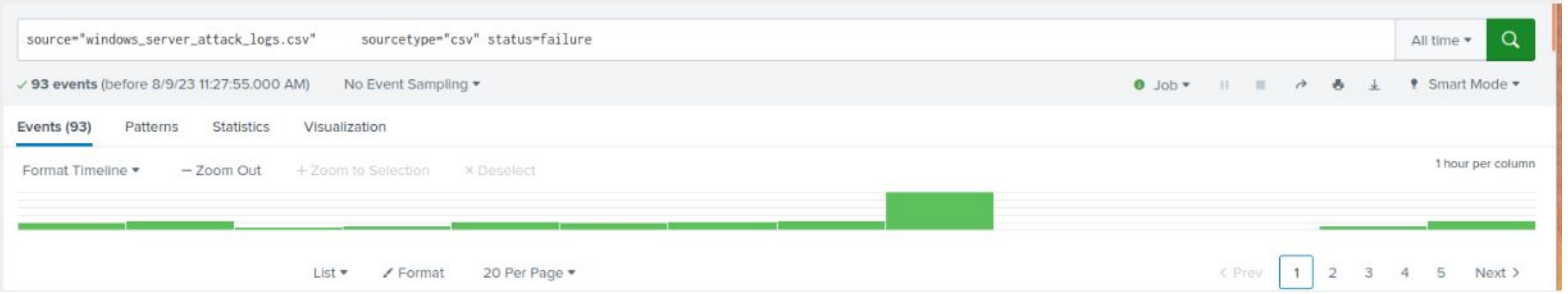
Failed windows activity-

- There was an attack initiated against our systems on the 25th of March 2020.

  -Although there is a lower level of overall failed windows activity, there is a spike of 35 at 9:00am March 25th

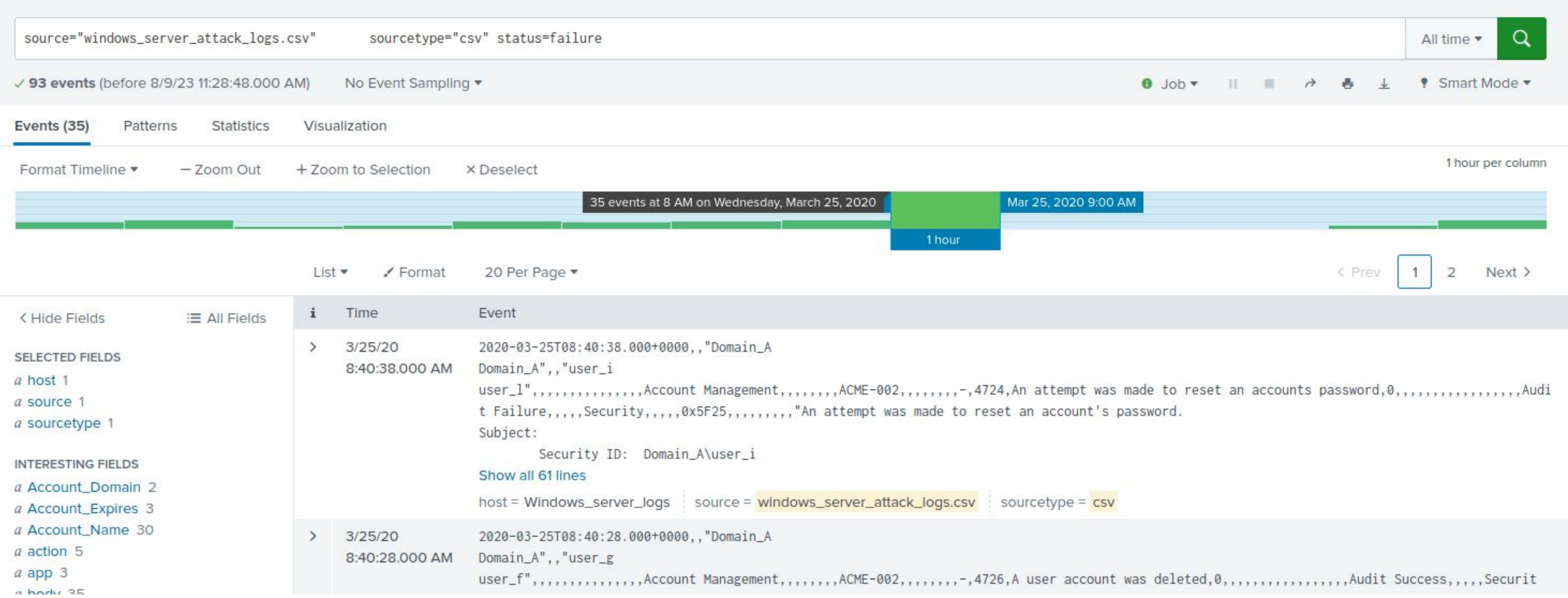


```
source="windows_server_logs.csv"    sourcetype="csv" status=failure
✓ 142 events (before 8/9/23 11:27:15.000 AM)    No Event Sampling
```



```
source="windows_server_attack_logs.csv"    sourcetype="csv" status=failure
✓ 93 events (before 8/9/23 11:27:55.000 AM)    No Event Sampling
```

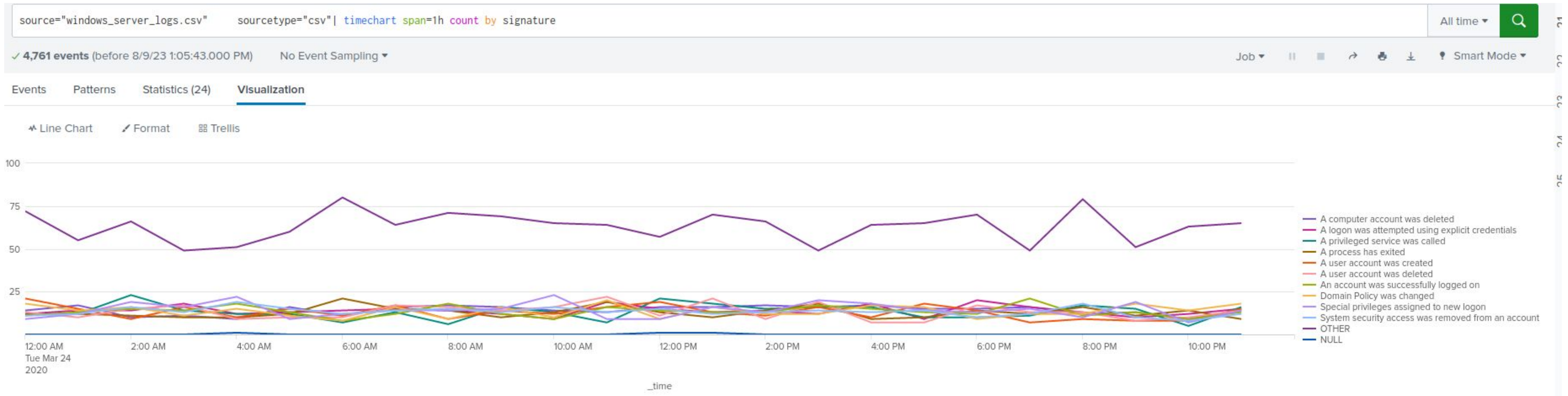
we wouldve received an alert for Windows failed login activities because the alert is set to be triggered when the number of failed logins exceeds 15 within an hour



```
source="windows_server_attack_logs.csv"    sourcetype="csv" status=failure
✓ 93 events (before 8/9/23 11:28:48.000 AM)    No Event Sampling
```

```
3/25/20          2020-03-25T08:40:38.000+0000,,"Domain_A
8:40:38.000 AM   Domain_A",,"user_i
                 user_l",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audi
                 t Failure,,,,,Security,,,,,0x5F25,,,,,,,,,"An attempt was made to reset an account's password.
                 Subject:
                         Security ID:  Domain_A\user_i
                 Show all 61 lines
                 host = Windows_server_logs   source = windows_server_attack_logs.csv   sourcetype = csv

3/25/20          2020-03-25T08:40:28.000+0000,,"Domain_A
8:40:28.000 AM   Domain_A",,"user_g
                 user_f",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Securit
```

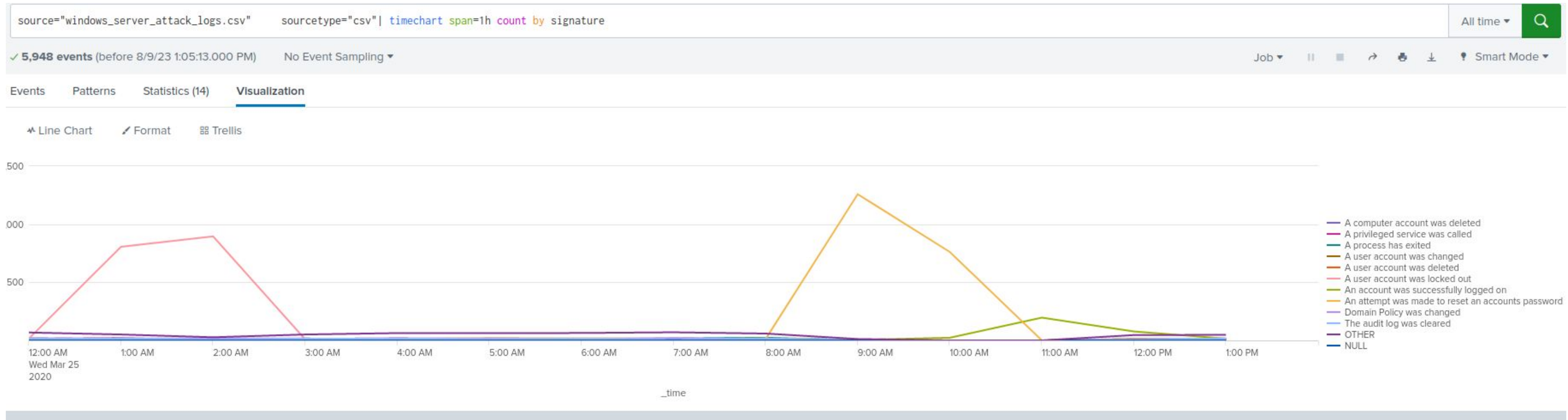
Windows time chart of signatures



```
source="windows_server_logs.csv"    sourcetype="csv"| timechart span=1h count by signature
```

✓ 4,761 events (before 8/9/23 1:05:43.000 PM)

All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (24)
Visualization
Line Chart
Format
Trellis
100
75
50
25
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_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 Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER
NULL



```
source="windows_server_attack_logs.csv"    sourcetype="csv"| timechart span=1h count by signature
```

✓ 5,948 events (before 8/9/23 1:05:13.000 PM)

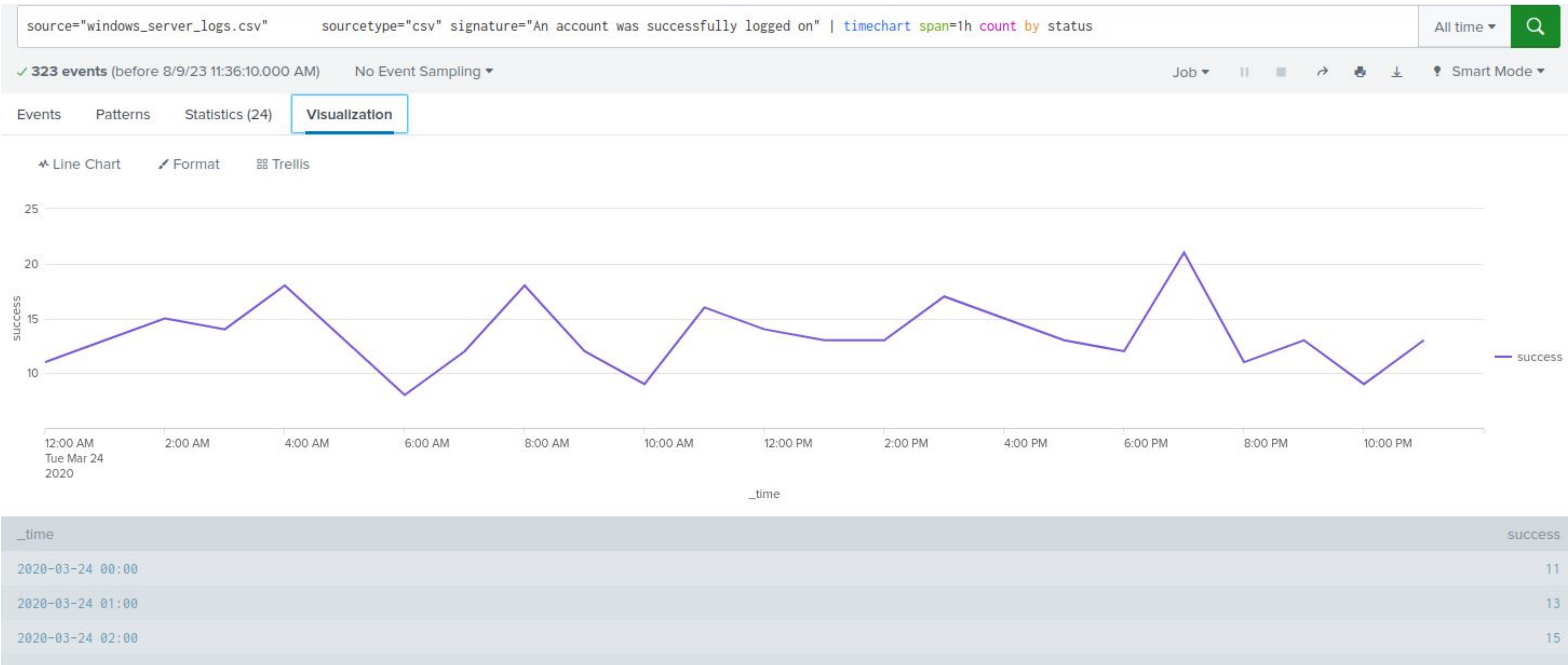
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (14)
Visualization
Line Chart
Format
Trellis
500
000
500
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
_time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts password
Domain Policy was changed
The audit log was cleared
OTHER
NULL

in the windows events by signature, the time chart shows significant increases in:
-Account password reset attempt
- A user account was locked out

The user account locked down attack began around 1:00 AM and ended at 3:00 AM on March 25, 2020 with a peak count of 896. Where password reset attack started at 9:00 AM and was carried out till 11:00 AM on March 25, 2020.The peak for password reset attempts was 1258,

Analysis for Successful Logins

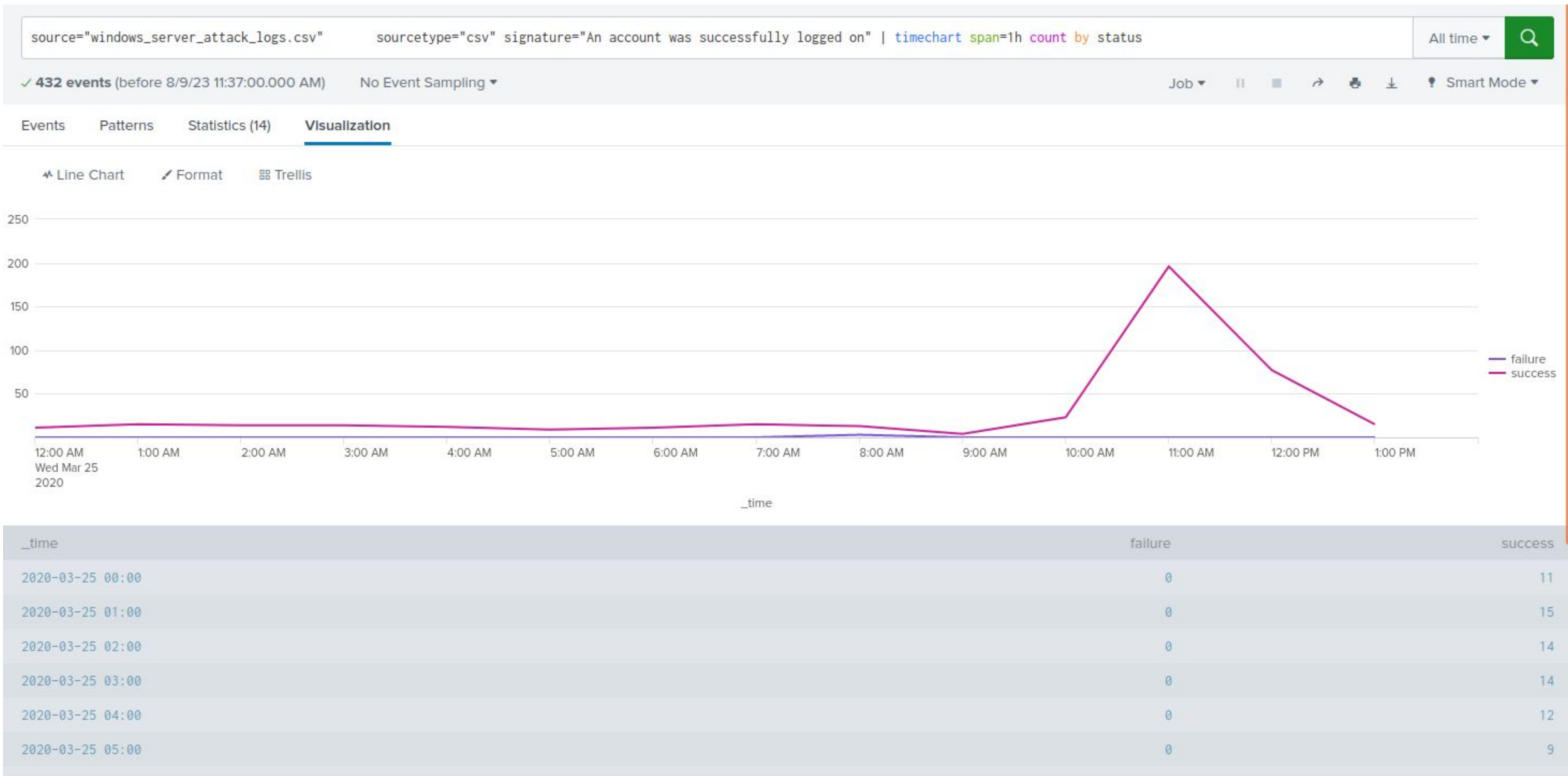
The data shows an increase in the total number an account was successfully logged on. The usual data shows a top of 21, whereas during the day of the attack, we can see it exceeding our threshold of 25 and peaking at 196 allowing our alert to be sent



```
source="windows_server_logs.csv"       sourcetype="csv" signature="An account was successfully logged on" | timechart span=1h count by status
```

✓ **323 events** (before 8/9/23 11:36:10.000 AM)   No Event Sampling ▾

_time	success
2020-03-24 00:00	11
2020-03-24 01:00	13
2020-03-24 02:00	15

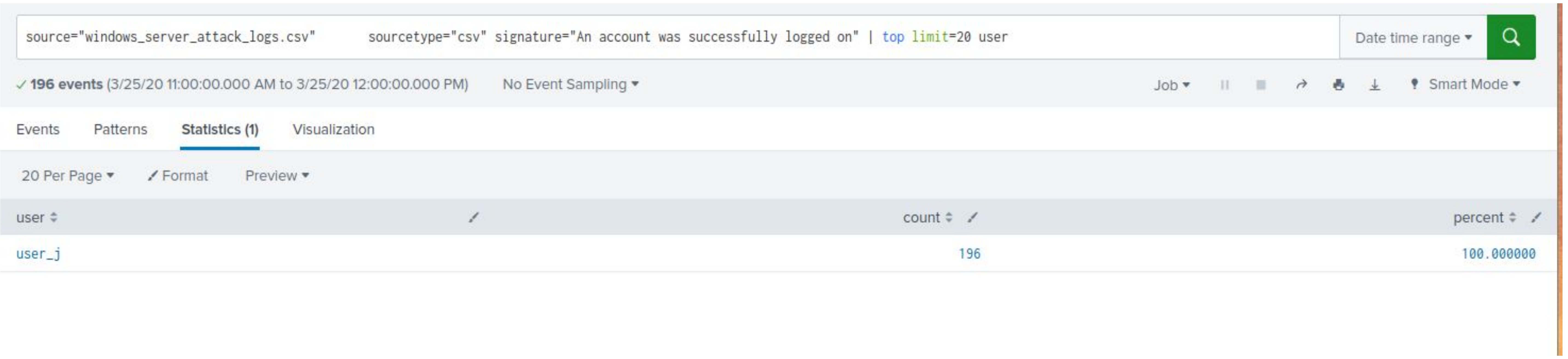


```
source="windows_server_attack_logs.csv"       sourcetype="csv" signature="An account was successfully logged on" | timechart span=1h count by status
```

✓ **432 events** (before 8/9/23 11:37:00.000 AM)   No Event Sampling ▾

_time	failure	success
2020-03-25 00:00	0	11
2020-03-25 01:00	0	15
2020-03-25 02:00	0	14
2020-03-25 03:00	0	14
2020-03-25 04:00	0	12
2020-03-25 05:00	0	9

the primary user logging during the spike @11am was user_j

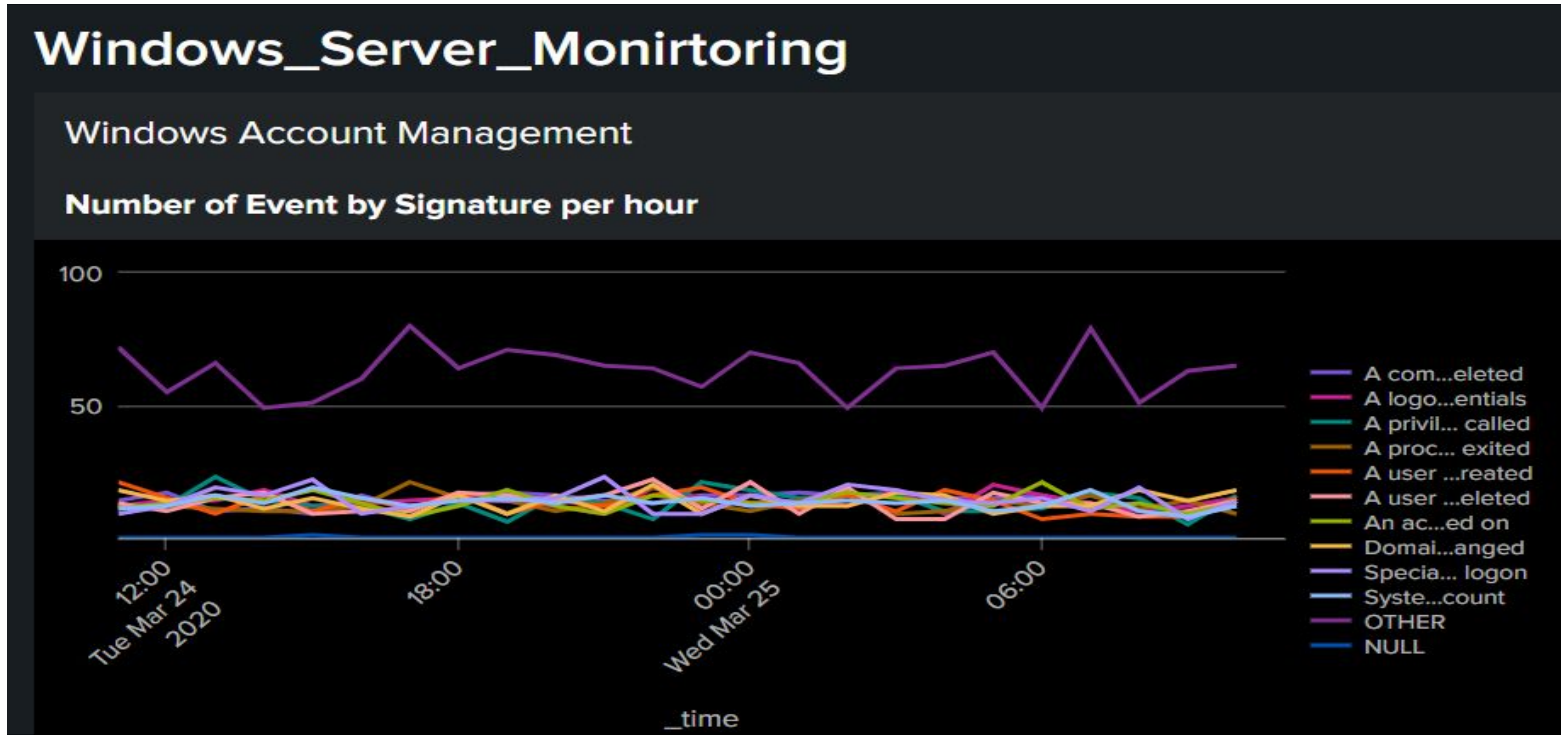


```
source="windows_server_attack_logs.csv"       sourcetype="csv" signature="An account was successfully logged on" | top limit=20 user
```

✓ **196 events** (3/25/20 11:00:00.000 AM to 3/25/20 12:00:00.000 PM)   No Event Sampling ▾

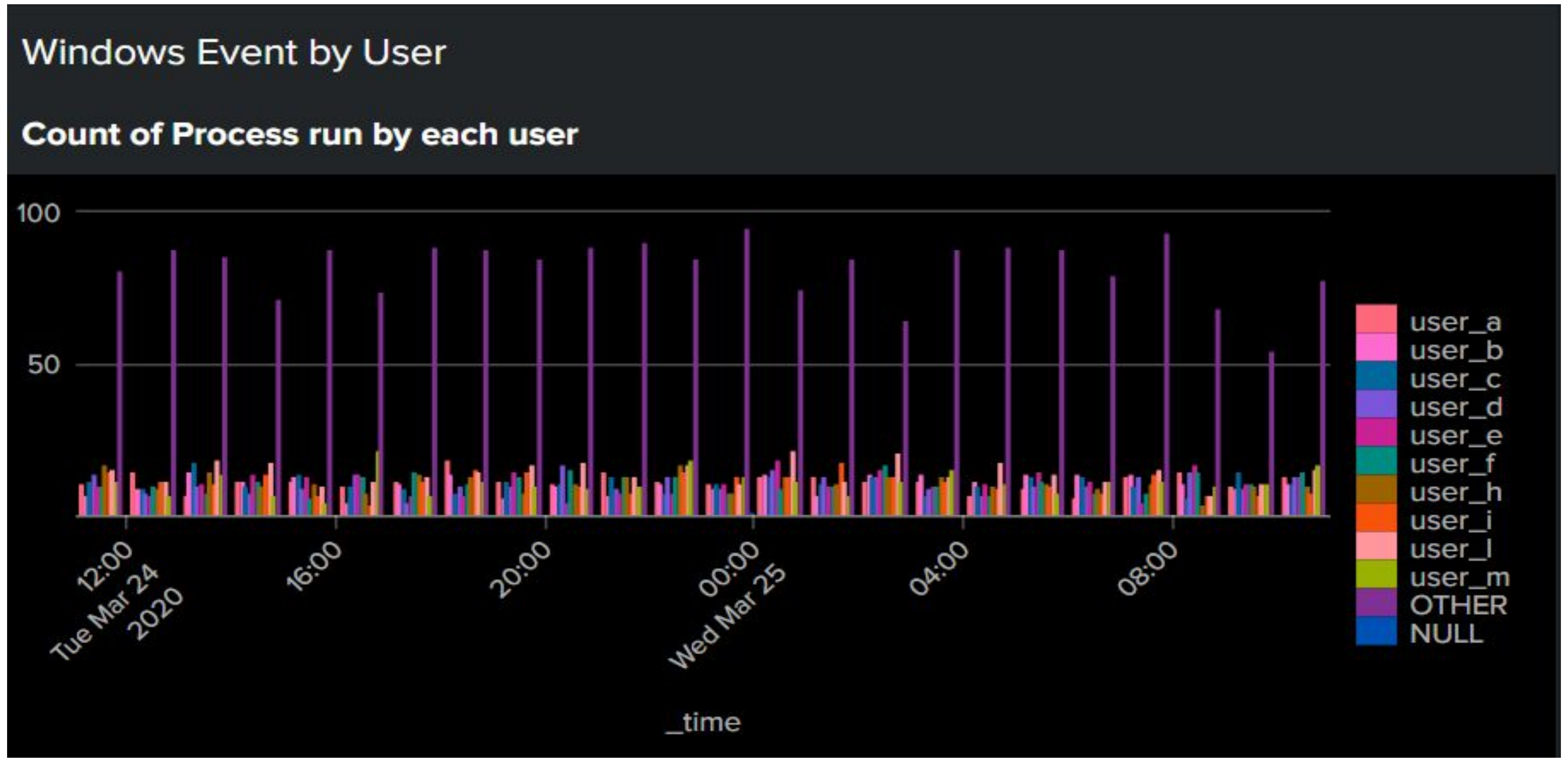
user	count	percent
user_j	196	100.000000

Dashboards—Windows

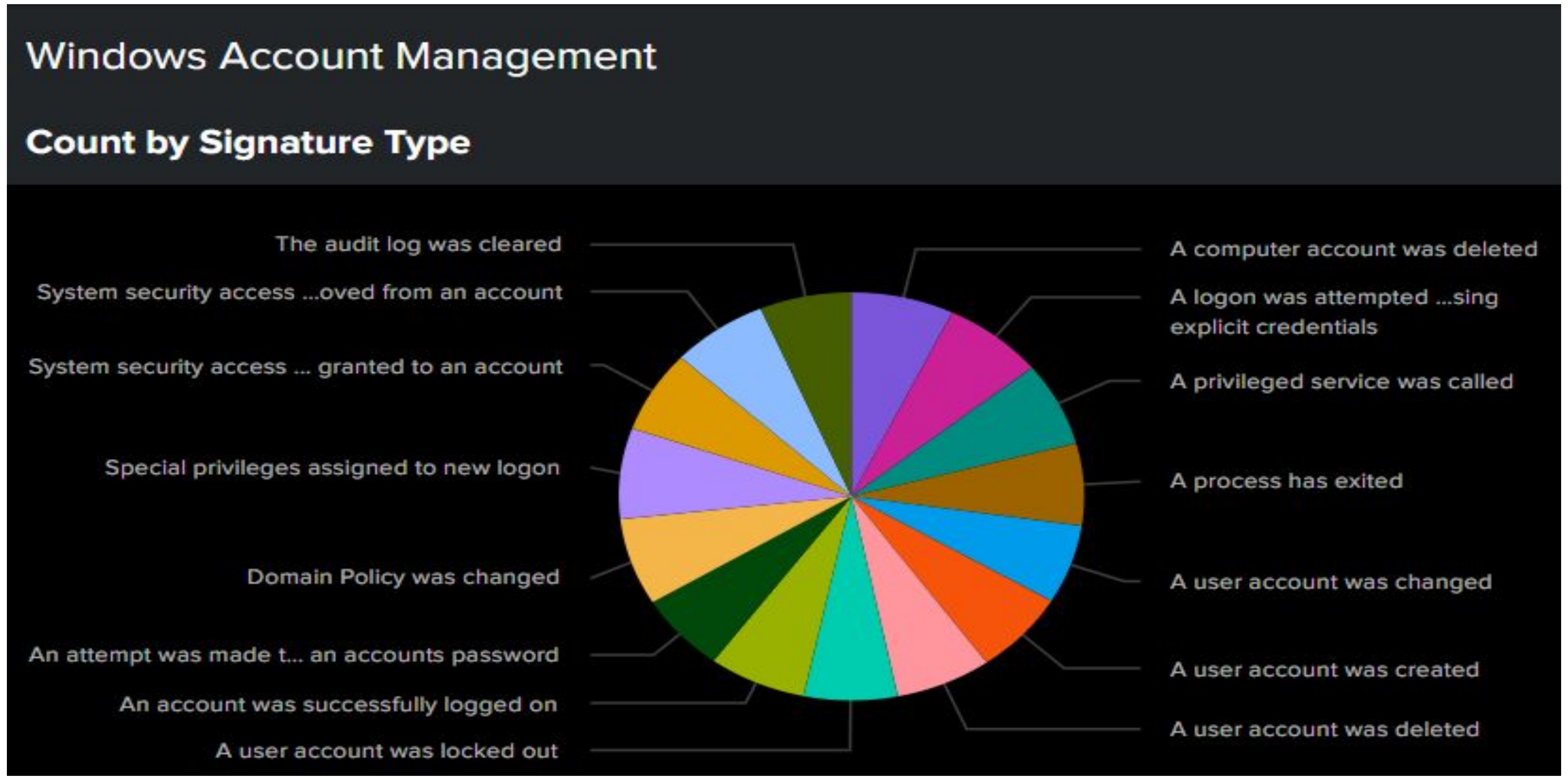

Windows_Server_Monirtoring

Windows Account Management

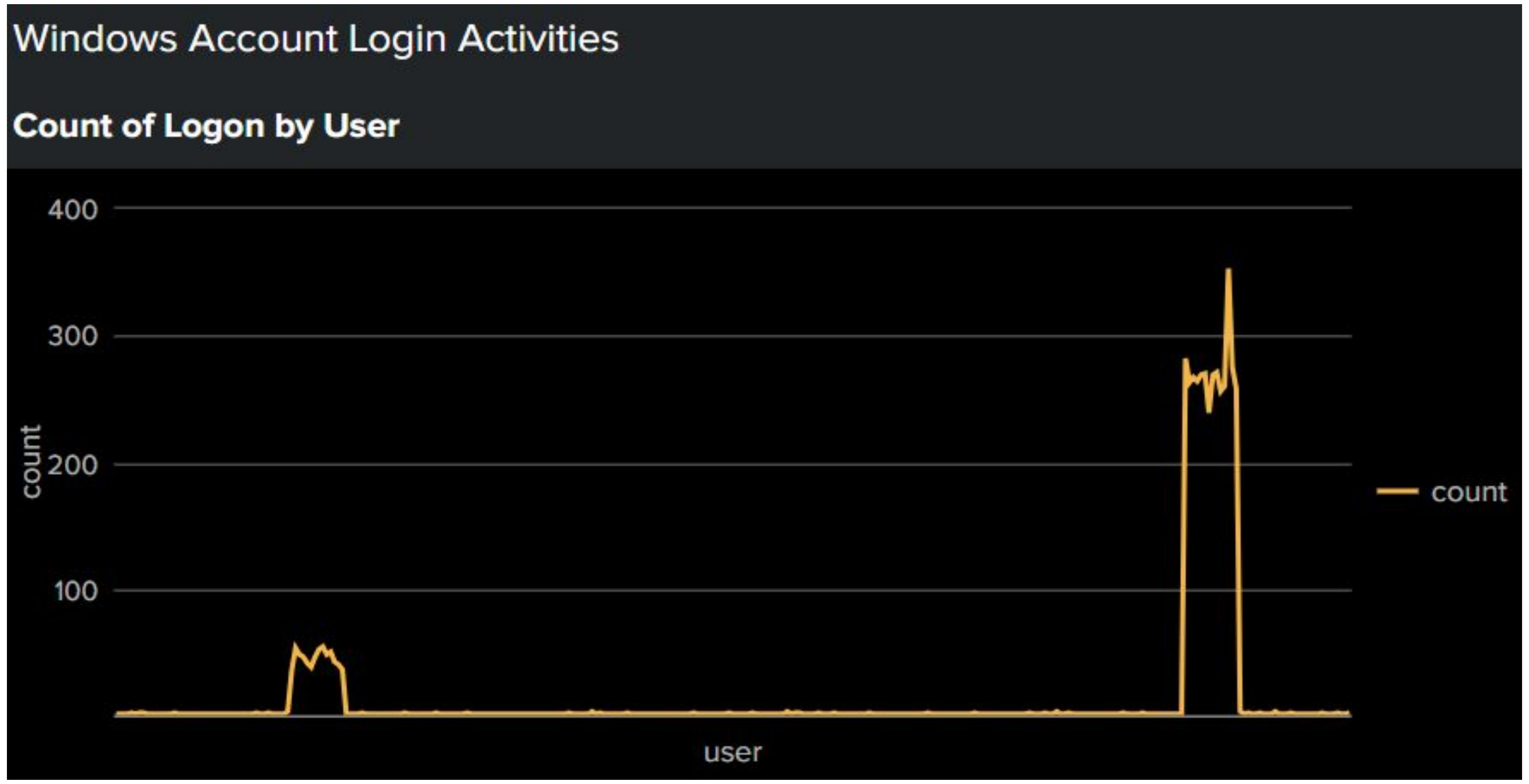
Number of Event by Signature per hour


Windows Event by User

Count of Process run by each user


Windows Account Management

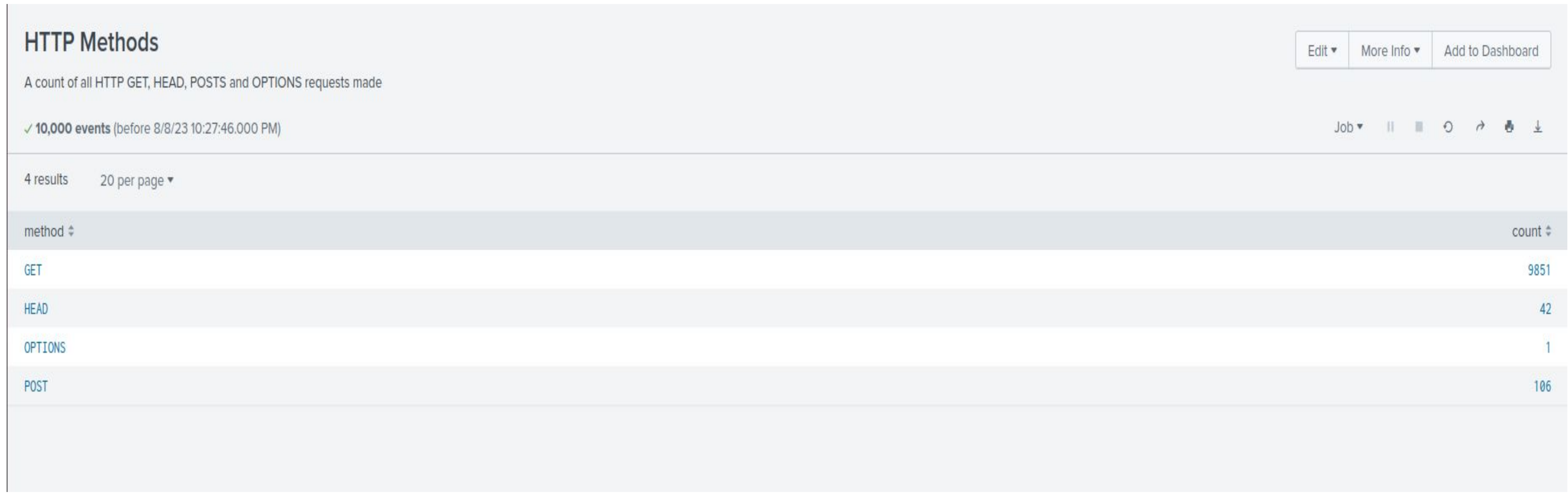
Count by Signature Type


Windows Account Login Activities

Count of Logon by User

Apache Logs

Reports—Apache



HTTP Methods

A count of all HTTP GET, HEAD, POSTS and OPTIONS requests made

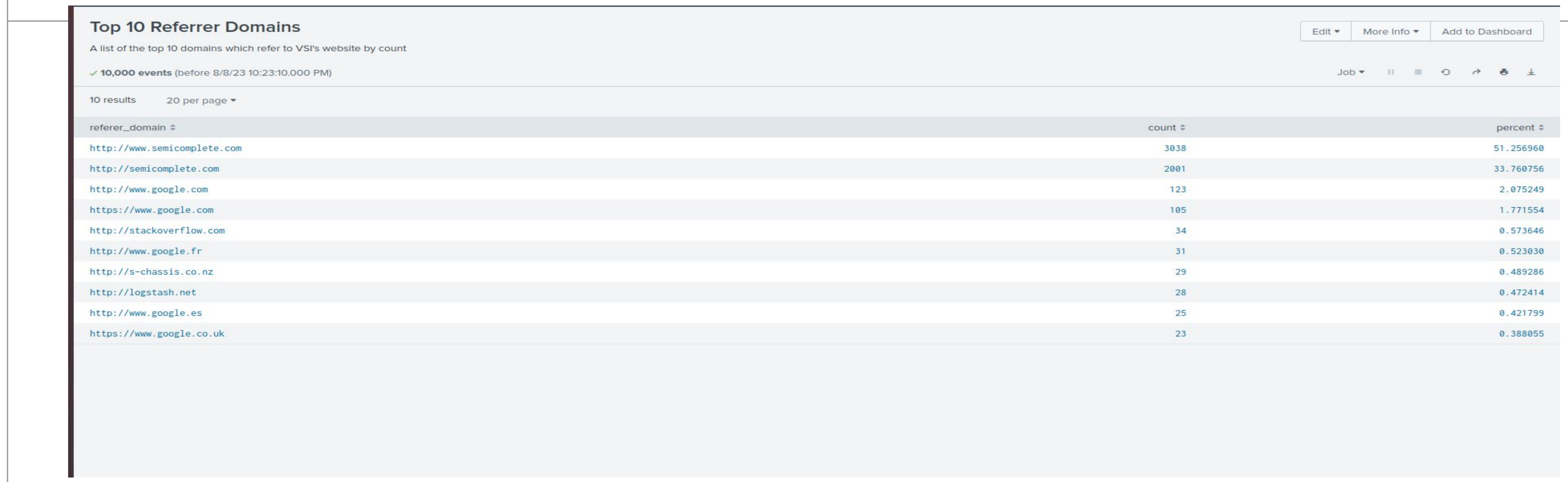
✓ **10,000 events** (before 8/8/23 10:27:46.000 PM)

4 results 20 per page ▾

method ⇕	count ⇕
GET	9851
HEAD	42
OPTIONS	1
POST	106

HTTP METHODS:

A count of all HTTP GET, HEAD, POSTS and OPTIONS requests made



Top 10 Referrer Domains

A list of the top 10 domains which refer to VSI's website by count

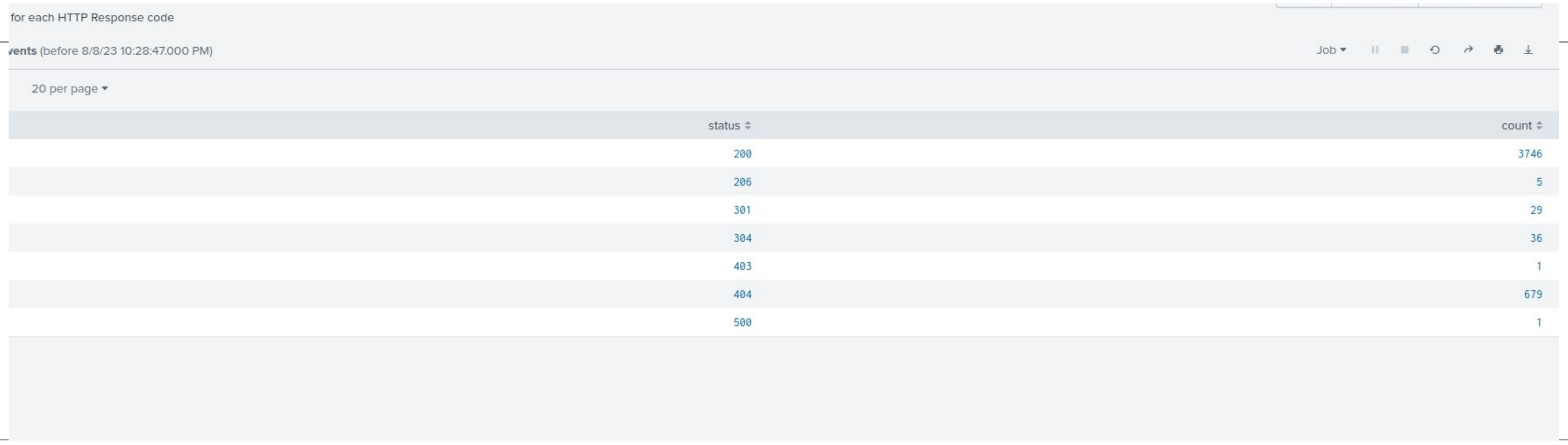
✓ **10,000 events** (before 8/8/23 10:23:10.000 PM)

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

Top 10 Referrer Domains:

A list of the top 10 domains which refer to VSI's website by count



for each HTTP Response code

vents (before 8/8/23 10:28:47.000 PM)

20 per page ▾

status ⇕	count ⇕
200	3746
206	5
301	29
304	36
403	1
404	679
500	1

HTTP CODES:

The count for each HTTP Response code

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Global level alert	Check hourly activity from outside of the US in order to determine potential cyber attacks	75	150

JUSTIFICATION:

Baseline: Mean is calculated at 73, so baseline has been rounded up (to nearest five) to 75

Threshold: 150 was selected in order to allow some room for natural variations that may occur in global activity. An alert would run if the thresholds conditions are met.

Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP Post Alert	Monitor for suspicious levels of HTTP POST requests	1.3	10

JUSTIFICATION:

Baseline: Average count of POST is 1.28, so baseline has been rounded up to nearest decimal place.

Threshold: It has been set to 10 to account for the count of 7 at 1:05PM which seems to be an outlier. .

However, since all activity prior to the attack is considered as non-suspicious, we have set the threshold at higher than 7 while giving additional ‘flexibility’ before alerts are emailed to the SOC team

Attack Summary—Apache

Were the thresholds correct?

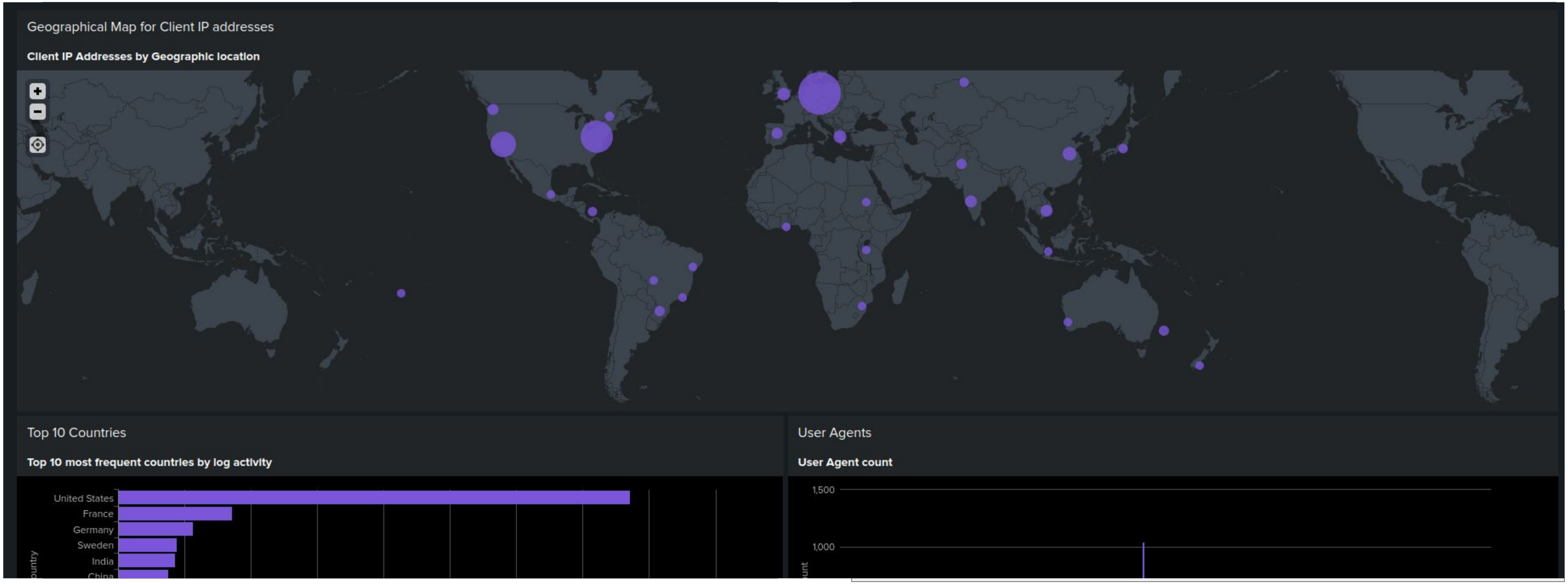
- The global threat alert reveals that the brute force attack came from the Ukraine with an equal number of counts from the cities of Kyiv and Kharkiv.

  The threshold count was chosen at 150 to avoid alert fatigue and potential false positives. As this attack shows, the threshold was accurate.

- The HTTP POST alert threshold was set to 10.

  When VSI experienced a brute force attack at 8:05 PM on March 25 of 2020, the alert would have been successfully triggered since the count of POST activity far surpassed the set threshold

Dashboards—Apache



Geographical Map for Client IP addresses

Client IP Addresses by Geographic location

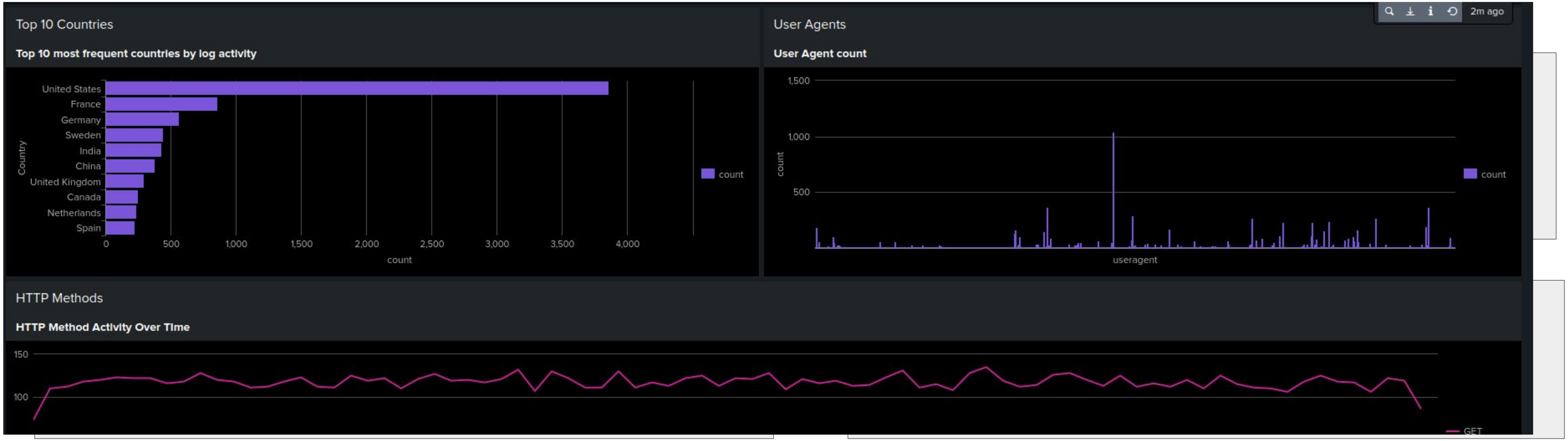
Top 10 Countries

Top 10 most frequent countries by log activity

User Agents

User Agent count

Dashboards—Apache



Top 10 Countries

Top 10 most frequent countries by log activity

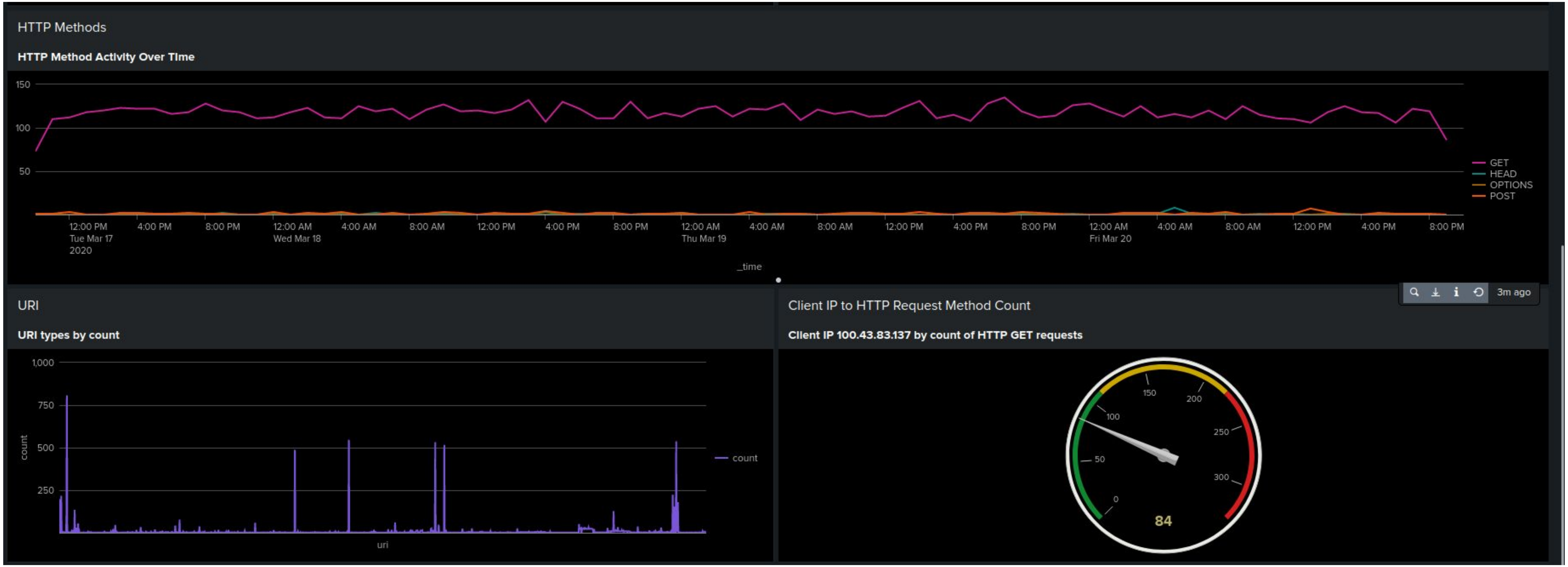
User Agents

User Agent count

HTTP Methods

HTTP Method Activity Over Time

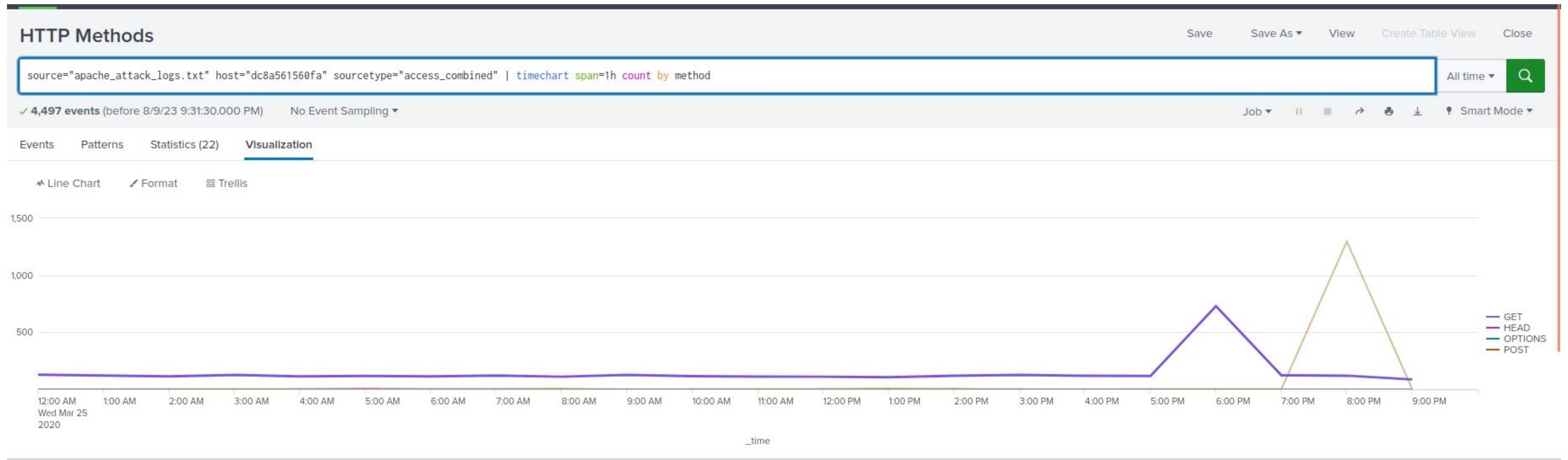
Dashboards—Apache



Attack Summary—Apache

Summary of findings from reports analyzing the attack logs:

- When looking at the line chart for HTTP count activity, there are two clear spikes. One is at 6pm which corresponds to GET requests and the other at 8pm, corresponding to POST requests.



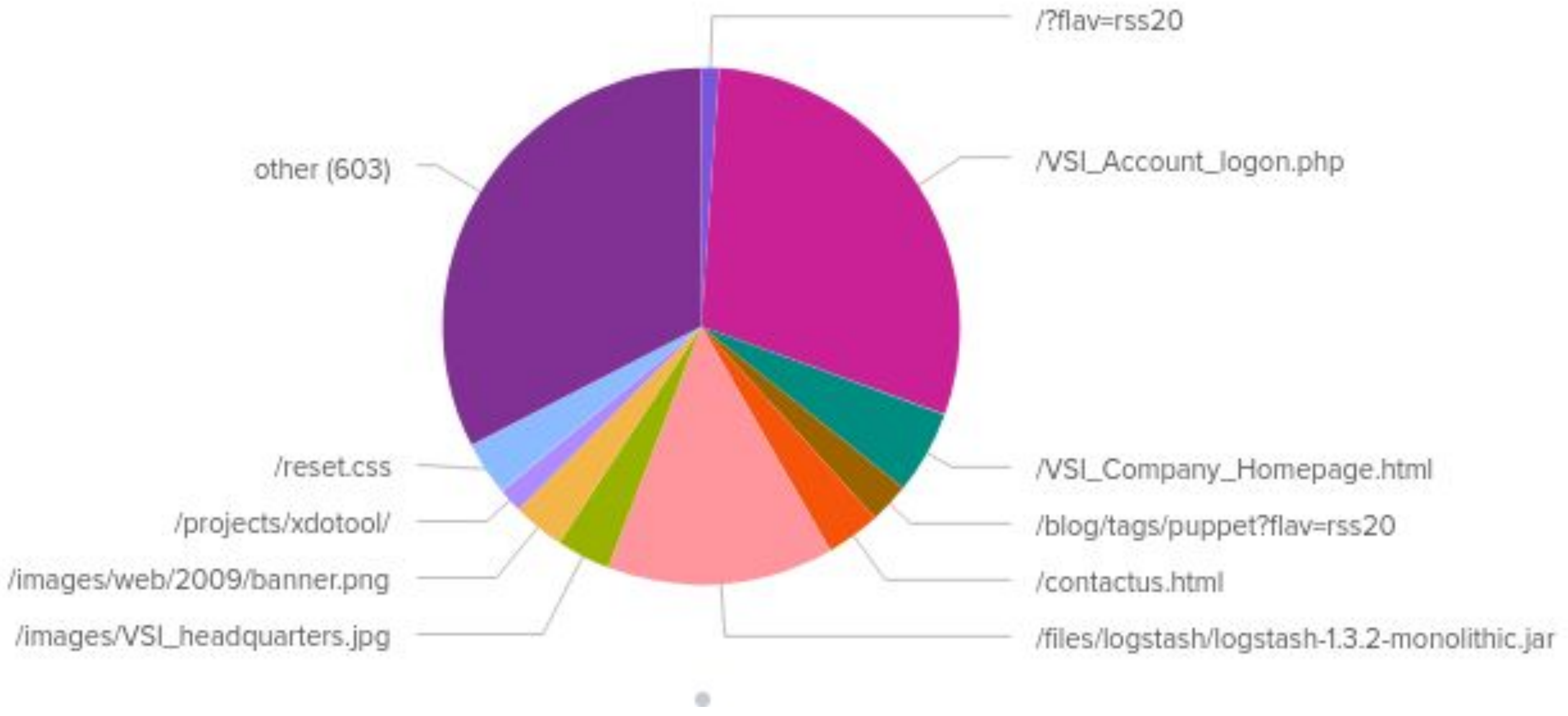
HTTP Methods

```
source="apache_attack_logs.txt" host="dc8a561560fa" sourcetype="access_combined" | timechart span=1h count by method
```

✓ 4,497 events (before 8/9/23 9:31:30.000 PM)

- HTTP 200 status code drops from 9126 to 3746 but a closer examination into the attack logs reveal 1415 counts at 8:05 PM on the day of the attack. There is a major increase in the occurrence of 404 error codes during the time of attack and a closer look reveals that 624 counts of 404 status codes were retrieved at 6:05 PM

Screenshots of Attack Logs



2020-03-25 20:04:00	0
2020-03-25 20:05:00	1415
2020-03-25 20:06:00	0
2020-03-25 20:07:00	0
2020-03-25 20:08:00	0

2020-03-25 18:04:00	0
2020-03-25 18:05:00	624
2020-03-25 18:06:00	0
2020-03-25 18:07:00	0

Attack Summary—Apache

Summary of our findings from the dashboard when analyzing the attack logs:

- When analyzing the top URI hits, there are two major deviations from the baseline (period prior to attack).

- 6:05pm: The resource /files/logstash/logstash-1.3.2-monolithic.jar returns a count of 624.
- 8:05pm: VSI's login portal returns 1,296 hits. The first is a GET request and the second a POST request. This explains the concerning counts for both HTTP methods during the timeframe of the attack.

The threat group have launched a brute force attack against VSI's server using logstash 1.3.2 to collect user details such as usernames.

- Analyzing the user agents report from the dashboard reveals that the attackers used Mozilla 4.0 browser on a Windows Server 2003 OS.

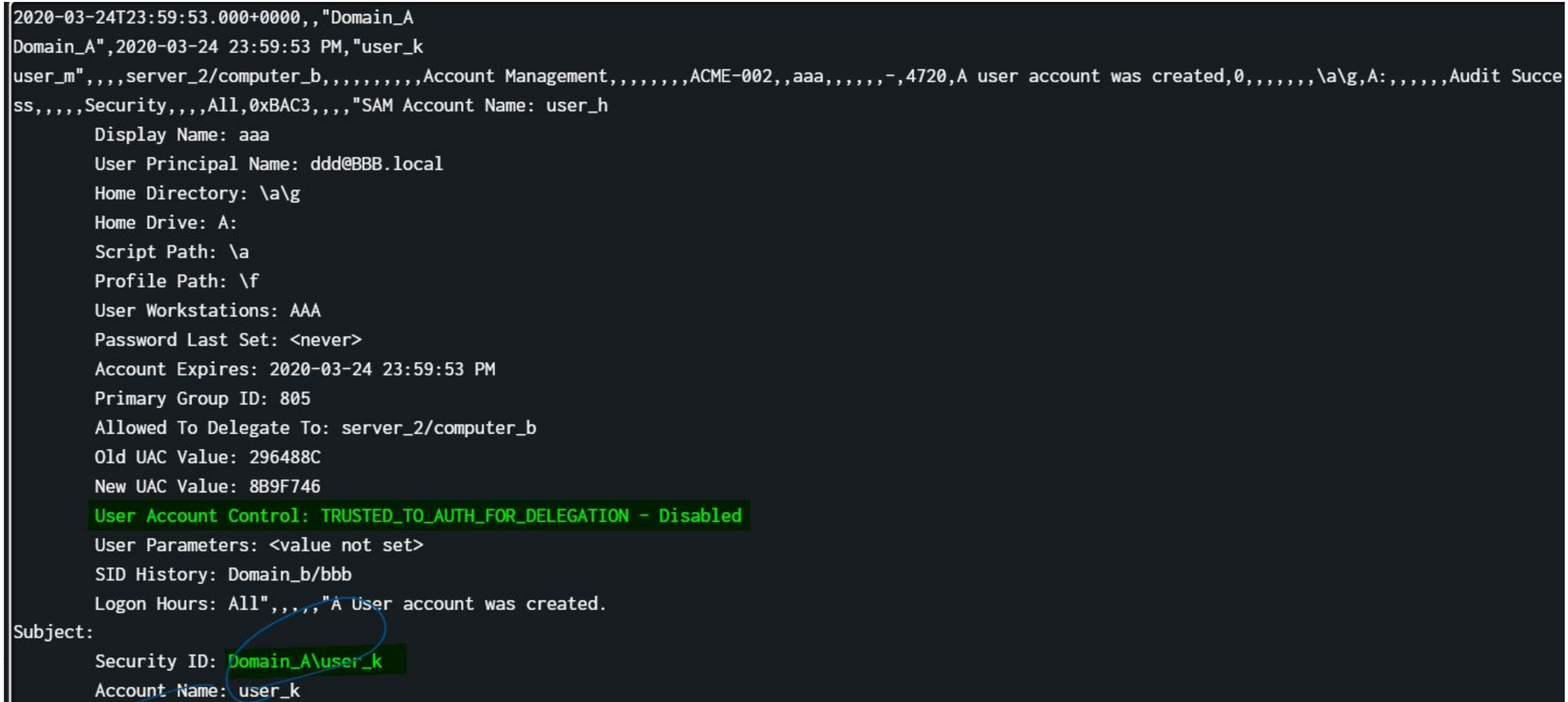
Summary and Future Mitigations

How the attacker got access to VSI Domain ?

Three user accounts are used for the attack:
user_a, user_k, and user_j

user_k logs

Bad account configuration by admin at the time of account creation.



```
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 Succe
ss,,,,,Security,,,,All,0xBAC3,,,,"SAM Account Name: user_h
        Display Name: aaa
        User Principal Name: ddd@BBB.local
        Home Directory: \a\g
        Home Drive: A:
        Script Path: \a
        Profile Path: \f
        User Workstations: AAA
        Password Last Set: <never>
        Account Expires: 2020-03-24 23:59:53 PM
        Primary Group ID: 805
        Allowed To Delegate To: server_2/computer_b
        Old UAC Value: 296488C
        New UAC Value: 8B9F746
        User Account Control: TRUSTED_TO_AUTH_FOR_DELEGATION - Disabled
        User Parameters: <value not set>
        SID History: Domain_b/bbb
        Logon Hours: All",,,,,"A User account was created.
Subject:
        Security ID: Domain_A\user_k
        Account Name: user_k
```

user_a privilege escalation

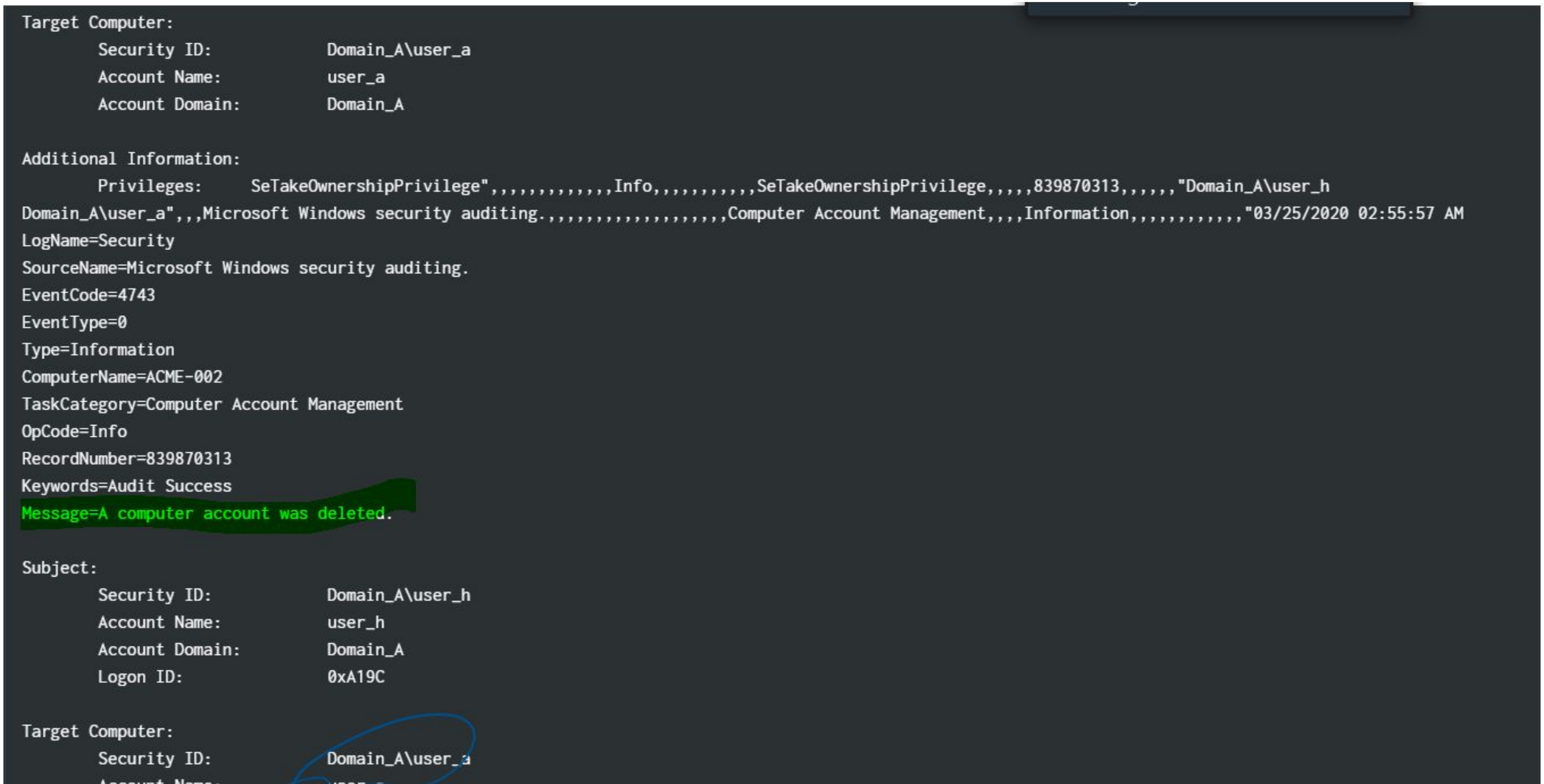
To Domain System Administrator

Talking: Bashir, Hudayfa

```
2020-03-25T02:49:43.000+0000,SeNetworkLogonRight,Domain_A,,"ACME-002
Domain_A\user_n",,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4717,System security access was granted to an account,0,,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x4D7
6,,,,,,,,,"System security access was granted to an account.

Subject:
        Security ID:            Domain_A\SYSTEM
        Account Name:           ACME-002
        Account Domain:         Domain_A
        Logon ID:               0x4D76

Account Modified:
        Account Name:           Domain_A\user_n

Access Granted:
        Access Right:           SeNetworkLogonRight",,,,,,,,,,,,,Info,,,,,,,,,,,,,,,,900908720,,,,,,Domain_A\SYSTEM,,,Microsoft Windows security auditing.,,,,,,,,,,,,,
hentication Policy Change,,,,Information,,,,,,,,,,,,"03/25/2020 02:49:43 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4717
EventType=0
Type=Information
ComputerName=ACME-002
TaskCategory=Authentication Policy Change
OpCode=Info
RecordNumber=900908720
Keywords=Audit Success
Message=System security access was granted to an account.

Subject:
        Security ID:            Domain_A\SYSTEM
        Account Name:           ACME-002
        Account Domain:         Domain_A
```

user_a logs

Account has been deleted



```
Target Computer:
        Security ID:            Domain_A\user_a
        Account Name:           user_a
        Account Domain:         Domain_A

Additional Information:
        Privileges:     SeTakeOwnershipPrivilege",,,,,,,,,,,,,Info,,,,,,,,,,,SeTakeOwnershipPrivilege,,,,,839870313,,,,,,"Domain_A\user_h
Domain_A\user_a",,,Microsoft Windows security auditing.,,,,,,,,,,,,,,,,,,,,Computer Account Management,,,,Information,,,,,,,,,,,,"03/25/2020 02:55:57 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4743
EventType=0
Type=Information
ComputerName=ACME-002
TaskCategory=Computer Account Management
OpCode=Info
RecordNumber=839870313
Keywords=Audit Success
Message=A computer account was deleted.

Subject:
        Security ID:            Domain_A\user_h
        Account Name:           user_h
        Account Domain:         Domain_A
        Logon ID:               0xA19C

Target Computer:
        Security ID:            Domain_A\user_a
```

Project 3 Summary

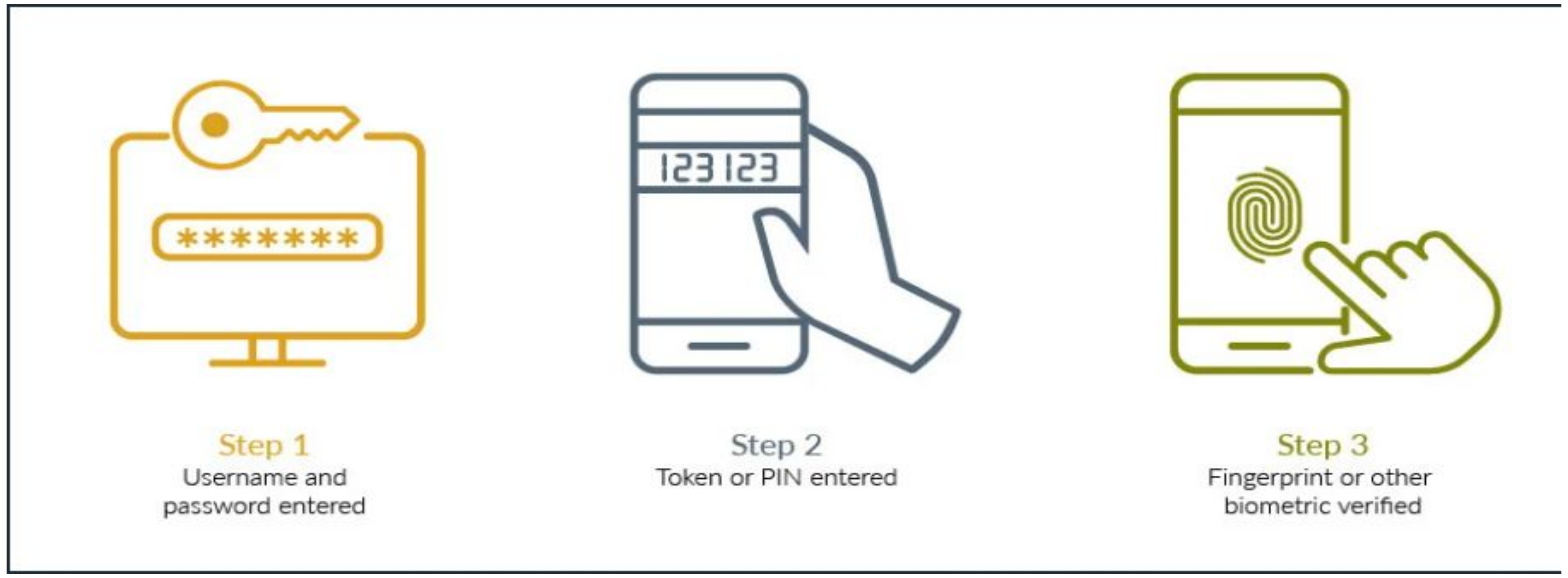
- What were your overall findings from the attack that took place?

- It is clear our systems were attacked on the 25th of March.

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

Window Domain Risk Mitigation Strategies

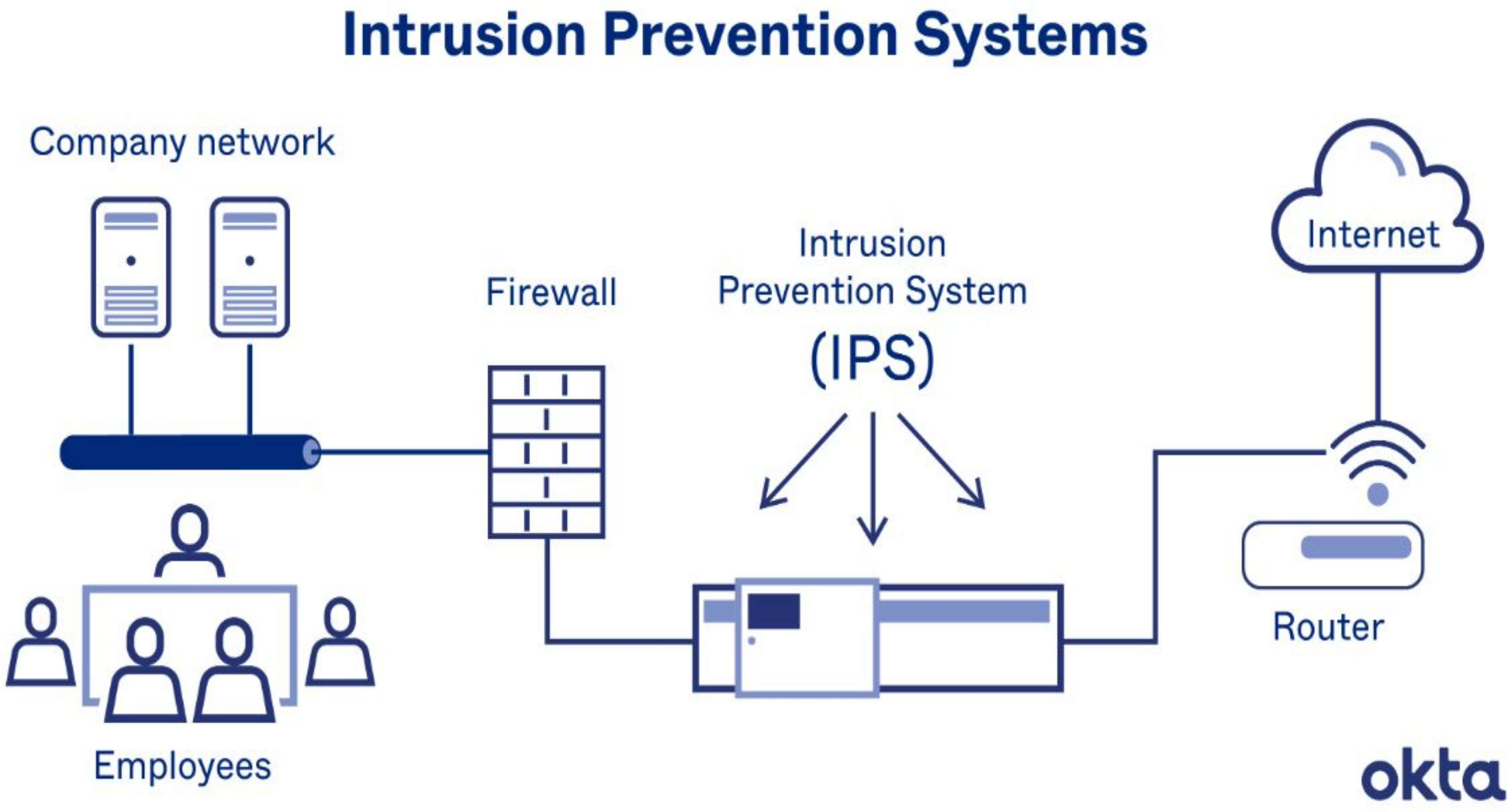
- Regular Patching and Updates
- Least Privilege Principle
- Multi-Factor Authentication (MFA)
- Secure Administrative Accounts


****
123 123
Step 1
Username and password entered
Step 2
Token or PIN entered
Step 3
Fingerprint or other biometric verified

Future Mitigation

Window Domain

- Credential Management
- Audit and Monitoring
- Network Segmentation
- Password Policies
- Group Policy Security
- Secure DNS Configuration
- Regular Backups
- Firewall and Intrusion Detection
- Privilege Escalation Mitigation
- Secure Replication
- Regular Security Assessments


Intrusion Prevention Systems
Company network
Firewall
Intrusion Prevention System (IPS)
Internet
Router
Employees
okta

Windows Domain

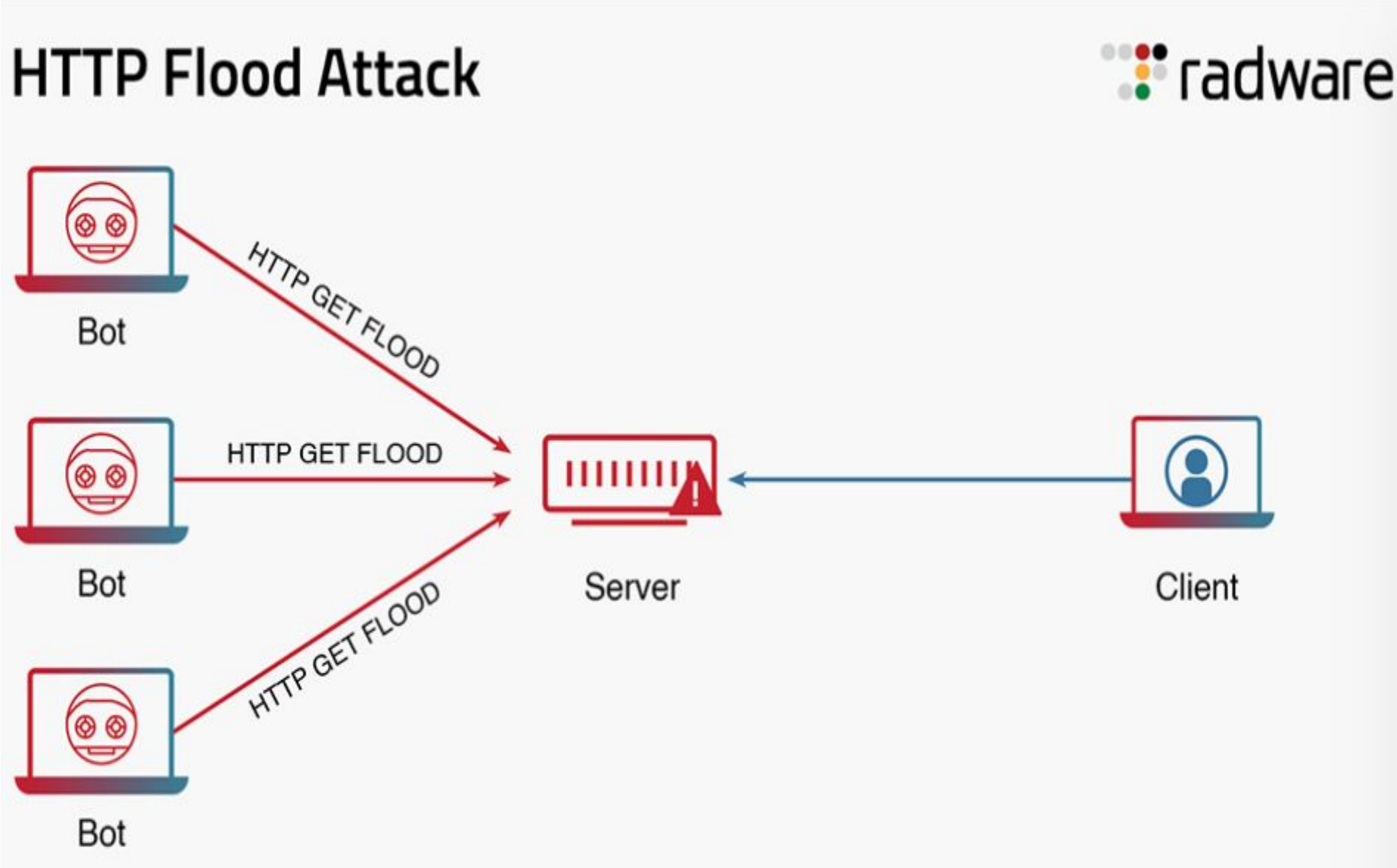
Mitigation Strategies

- Employee Training and Awareness
- Disable Unused Protocols and Services
- Implementing Security Baselines

Apache Web Server Attack

Some Highlighted One

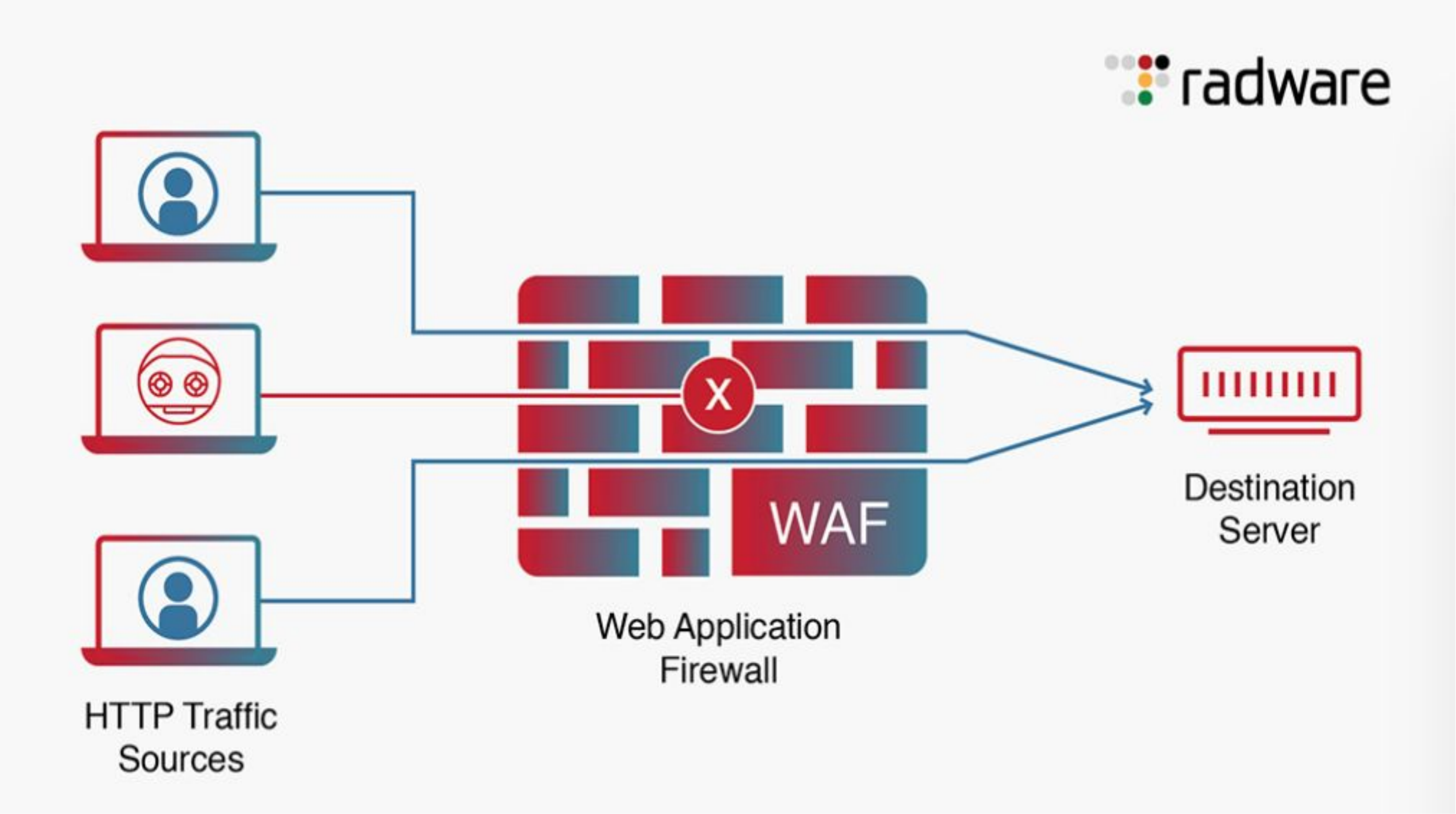
- HTTP Flood Attack
- Page Not found 404
- Regional base Access
- Mozilla Browser Outdated



Apache Web Server

Mitigation Strategies

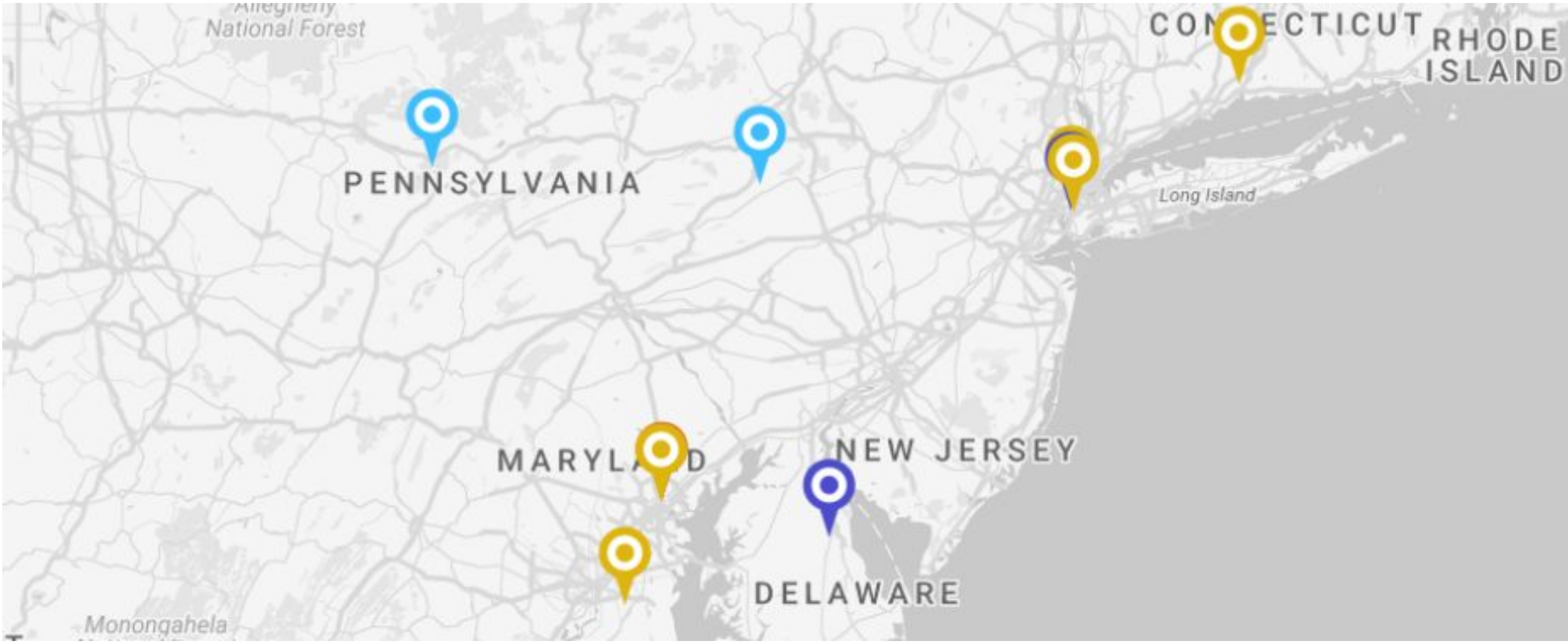
- Content Delivery Network (CDN)
- Rate Limiting and Traffic Shaping
- Web Application Firewall (WAF)
- IP Whitelisting and Blacklisting
- Load Balancing
- Server Resources Management
- CAPTCHA and Challenge Pages



Apache Web Server

Mitigation Strategies

- Traffic Monitoring and Anomaly Detection
- DNS Protection
- **Geolocation Filtering**
- Emergency Response Plan
- Cloud-Based Protection Services
- Network Level Protection
- Regular Updates and Patches
- Redundancy and Failover


Allegheny National Forest
CONNECTICUT
RHODE ISLAND
PENNSYLVANIA
Long Island
MARYLAND
NEW JERSEY
DELAWARE
Monongahela