VIRTUAL SPACE INDUSTRIES

DEFENSIVE SECURITY
PROJECT 3

GROUP 5: Auburn Bertuccini, Bryan Zamora, Daniel Farmer, Dylan Miller, Lian Chancay, Matthew Gaddis

CONTENT

Monitoring Environment

- Scenario
- Splunk Add-ons
- Summary of baseline events, alerts, and dashboards for Windows and Apache

Attack Analysis

Summary of attack events, alerts, and dashboards for Windows and Apache

Project Summary & Future Mitigations

Proposed mitigation strategies to prevent future network intrusions

MONITORING ENVIRONMENT

PRESENTED BY: DYLAN MILLER

VIRTUAL SPACE INDUSTRIES

SCENARIO

Introduction

Virtual Space Industries (VSI) specializes in conception and implementation of virtual reality programs

VSI has heard rumors that a competitor, JobeCorp, may launch cyberattacks to disrupt VSI's business

Our Task

Use Splunk to monitor VSI’s systems and applications for potential attacks

LOGS ANALYZED

This server contains intellectual property of VSI’s next-generation virtual-reality programs.

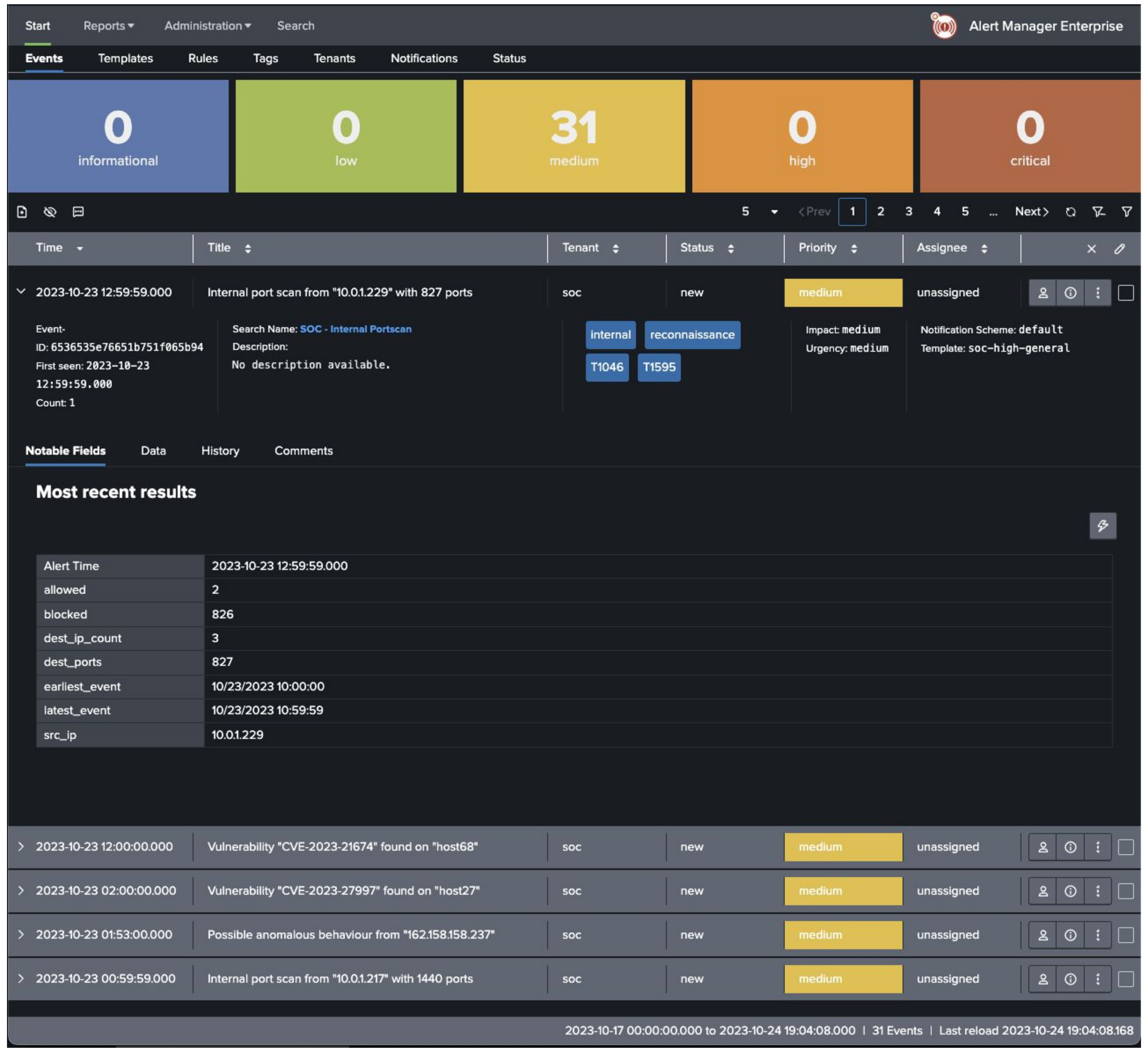
This server is used for VSI’s main public-facing website, vsi-company.com.

ALERT MANAGER ENTERPRISE

A Splunk Add-On
PRESENTED BY: AUBURN BERTUCCINI

VIRTUAL SPACE
INDUSTRIES

ALERT DASHBOARD



Time	Title	Tenant	Status	Priority	Assignee
2023-10-23 12:59:59.000	Internal port scan from "10.0.1.229" with 827 ports	soc	new	medium	unassigned

Event-ID: `6536535e76651b751f065b94`
First seen: `2023-10-23 12:59:59.000`
Count: 1

Search Name: SOC - Internal Portscan
Description:
`No description available.`

internal reconnaissance T1046 T1595

Impact: `medium`
Urgency: `medium`

Notification Scheme: `default`
Template: `soc-high-general`

Notable Fields | Data | History | Comments

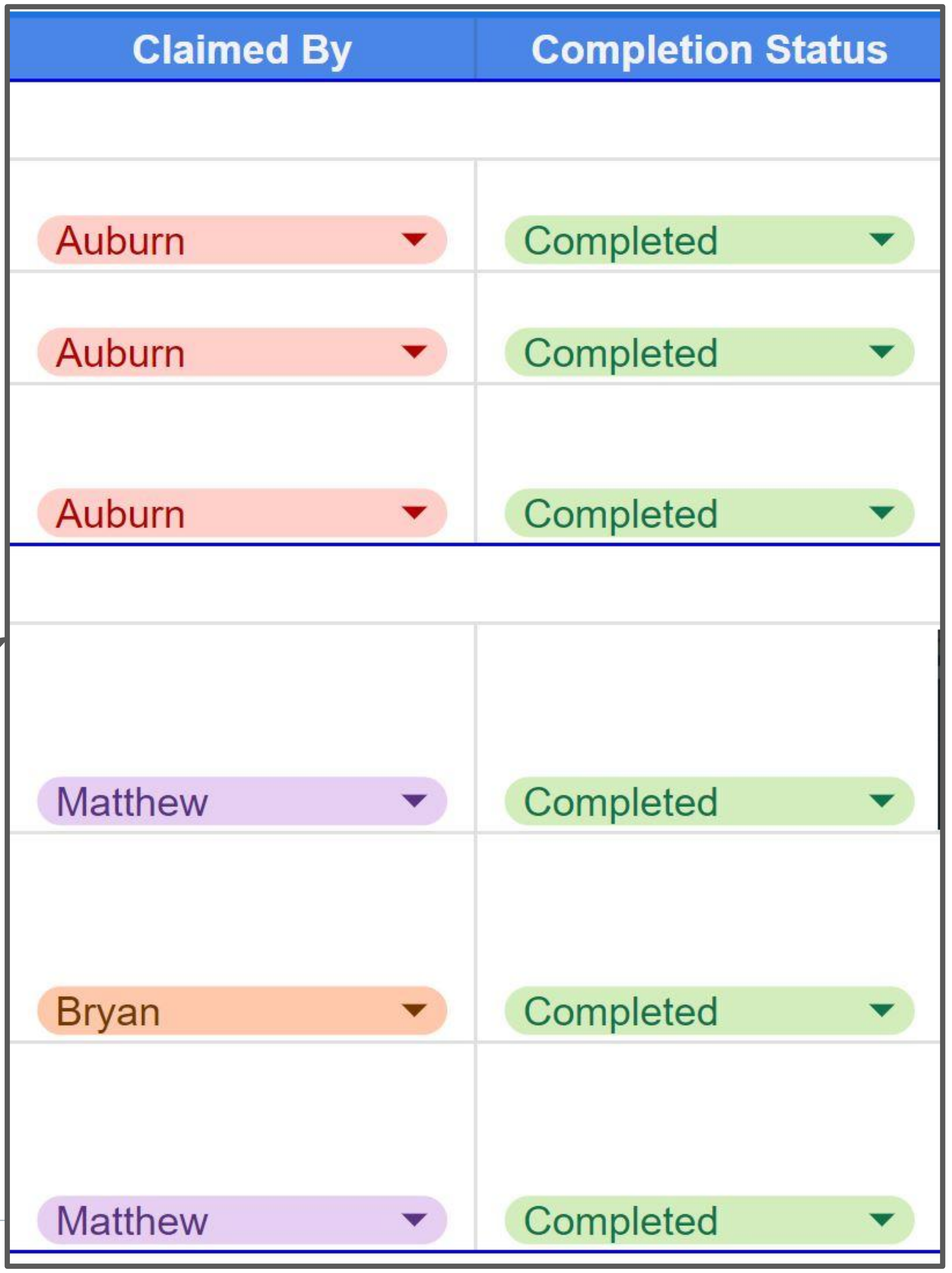
Most recent results

Alert Time	2023-10-23 12:59:59.000
allowed	2
blocked	826
dest_ip_count	3
dest_ports	827
earliest_event	10/23/2023 10:00:00
latest_event	10/23/2023 10:59:59
src_ip	10.0.1.229

Time	Title	Tenant	Status	Priority	Assignee
2023-10-23 12:00:00.000	Vulnerability "CVE-2023-21674" found on "host68"	soc	new	medium	unassigned
2023-10-23 02:00:00.000	Vulnerability "CVE-2023-27997" found on "host27"	soc	new	medium	unassigned
2023-10-23 01:53:00.000	Possible anomalous behaviour from "162.158.158.237"	soc	new	medium	unassigned
2023-10-23 00:59:59.000	Internal port scan from "10.0.1.217" with 1440 ports	soc	new	medium	unassigned

2023-10-17 00:00:00.000 to 2023-10-24 19:04:08.000 | 31 Events | Last reload 2023-10-24 19:04:08.168

Event Time
Title
Tenant
Status
Priority
Assignee
Alert Options



Claimed By	Completion Status
Auburn	Completed
Auburn	Completed
Auburn	Completed
Matthew	Completed
Bryan	Completed
Matthew	Completed

EVENT LIFECYCLES

Global Time Range: Last 30 days

Tenant: soc

Search Name: All

Assignee: All

Tags: All

Event ID: *

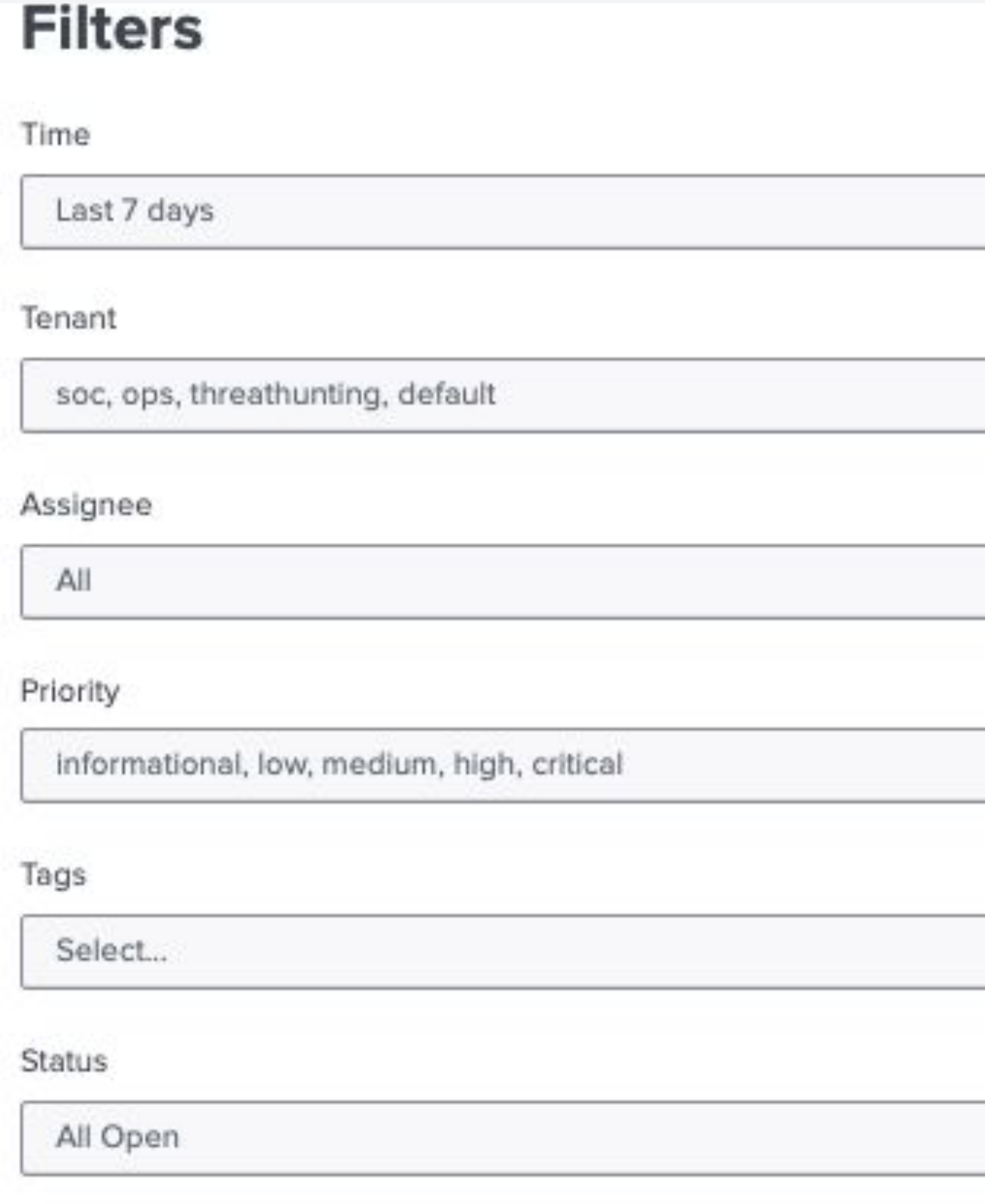
Status Transitions

created
new
assigned
in_progress
resolved
closed
suppressed

The lifecycle of an event starts with a `created` event, which is immediately followed by either a status `new` or `suppressed` event.

IMPROVED EVENT FILTERING

Position your team as forward-thinking by adopting the latest tools that drive operational success.



Filters

Time

Last 7 days

Tenant

soc, ops, threathunting, default

Assignee

All

Priority

informational, low, medium, high, critical

Tags

Select...

Status

All Open

BENEFITS

Optimized event dashboard with a sleek UI and improved features

CLARITY

Event lifecycles aides in operational efficiency and identifying bottlenecks

EFFICIENCY

More notification setup options decreases chances for false-positives.

IMPROVED ALERTS

LOGS ANALYZED

This server contains intellectual property of VSI's next-generation virtual-reality programs.

This server is used for VSI's main public-facing website, vsi-company.com.

WINDOWS LOGS

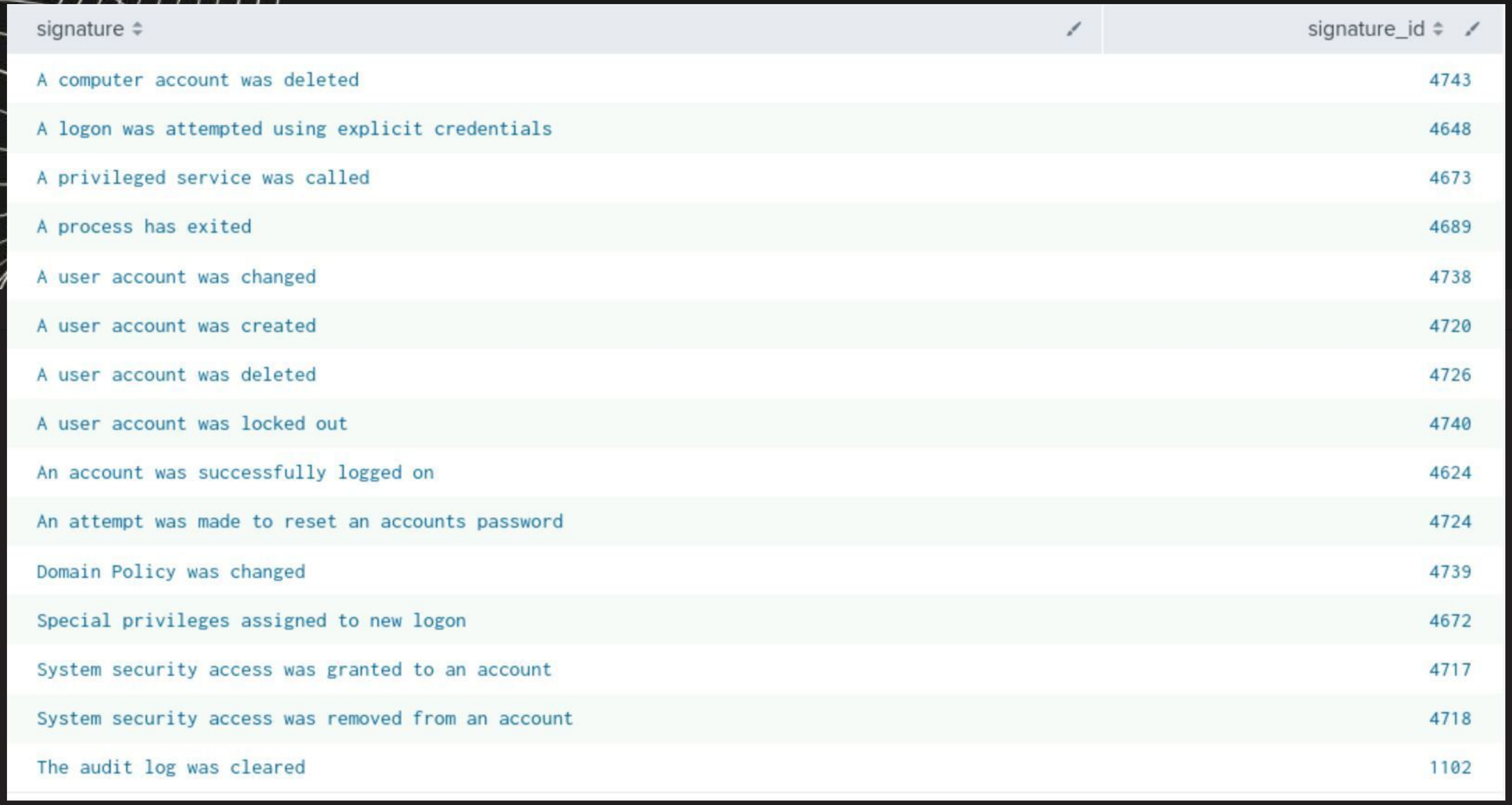
PRESENTED BY: MATTHEW GADDIS and LIAN CHANCAY

VSI
VIRTUAL SPACE
INDUSTRIES

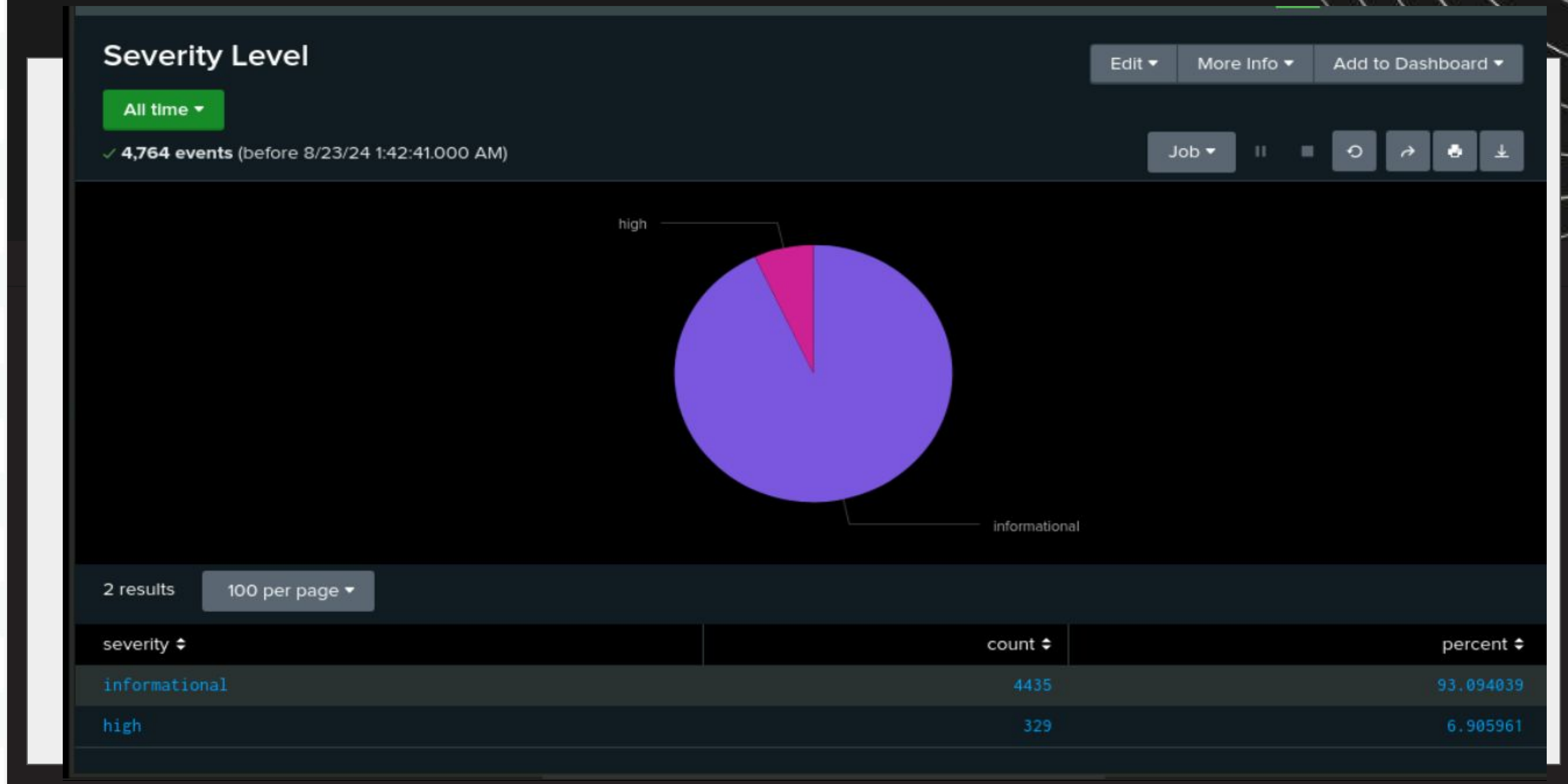
WINDOWS REPORTS

Report Name	Report Description
Signatures and Signature IDs	Displays the ID number associated with the specific signature ID for windows activity, removing duplicate values.
Severity Levels	Tracks severity events, counts, and percentages by severity level.
Success vs. Failure of Windows Activities	Compares and tracks levels of success and failure of Windows activities.

WINDOWS REPORTS



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

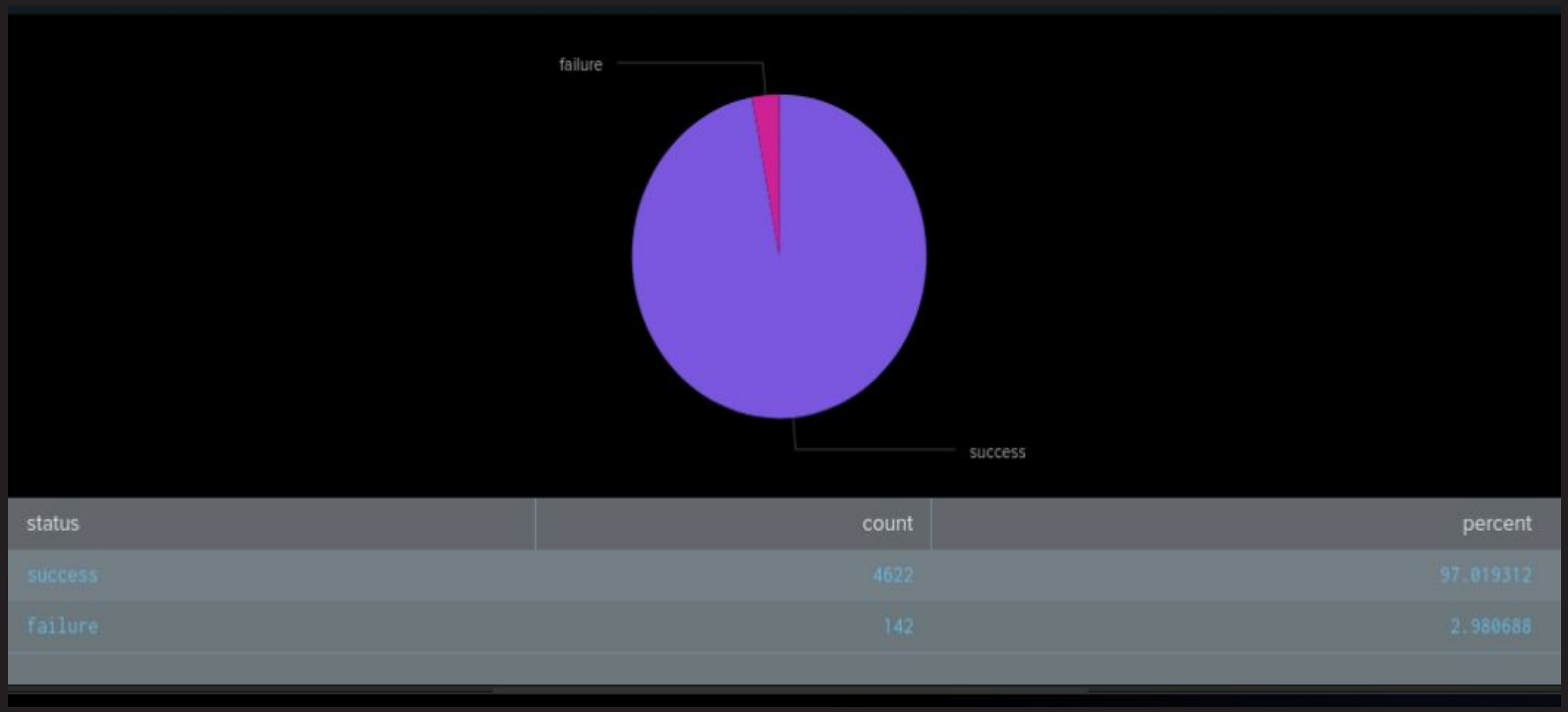


Severity Level

✓ 4,764 events (before 8/23/24 1:42:41.000 AM)

2 results

severity	count	percent
informational	4435	93.094039
high	329	6.905961



status	count	percent
success	4622	97.019312
failure	142	2.980688

WINDOWS ALERTS

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly level of Failed Windows Activity	Tracks status=failure	5	8

JUSTIFICATION: The level of failures often hover around 5, and surges above 8 are rare enough to justify investigation.

WINDOWS ALERTS

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Deletion Threshold	Exists to quantify suspicious amount of user deletion	14	18

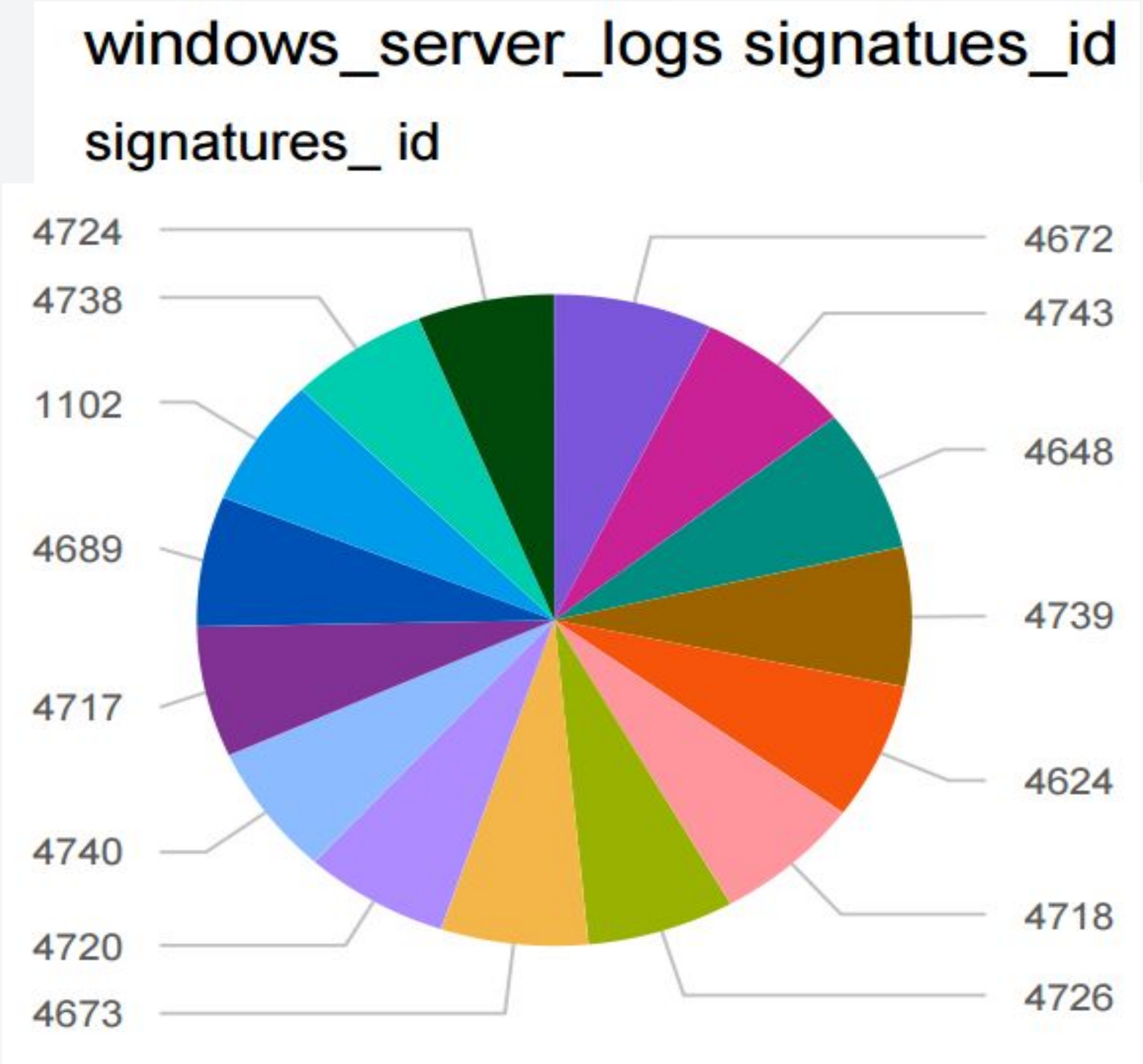
JUSTIFICATION: A high amount of User deletion can indicate suspicious activity. Normal activity was around 14, and spikes above 18 were rare and could merit attention.

WINDOWS ALERTS

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logon Threshold	Limit for successful logins per account	12	25

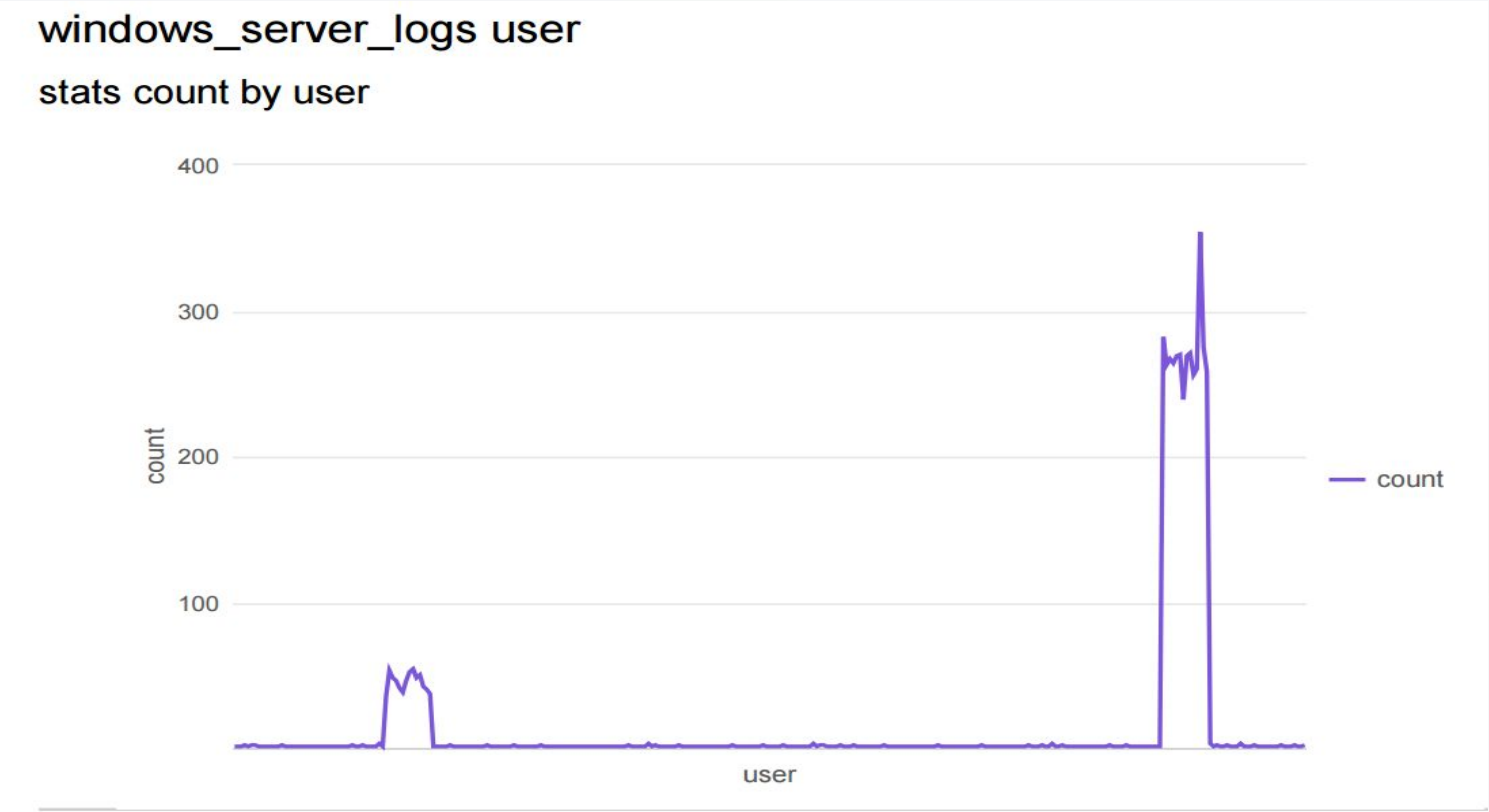
JUSTIFICATION: A high amount of Successful Logins under a limited amount of time could indicate suspicious activity and might warrant attention. 12 logins were around the normal level of activity and spikes above 25 could potentially represent malicious activity.

WINDOWS DASHBOARDS



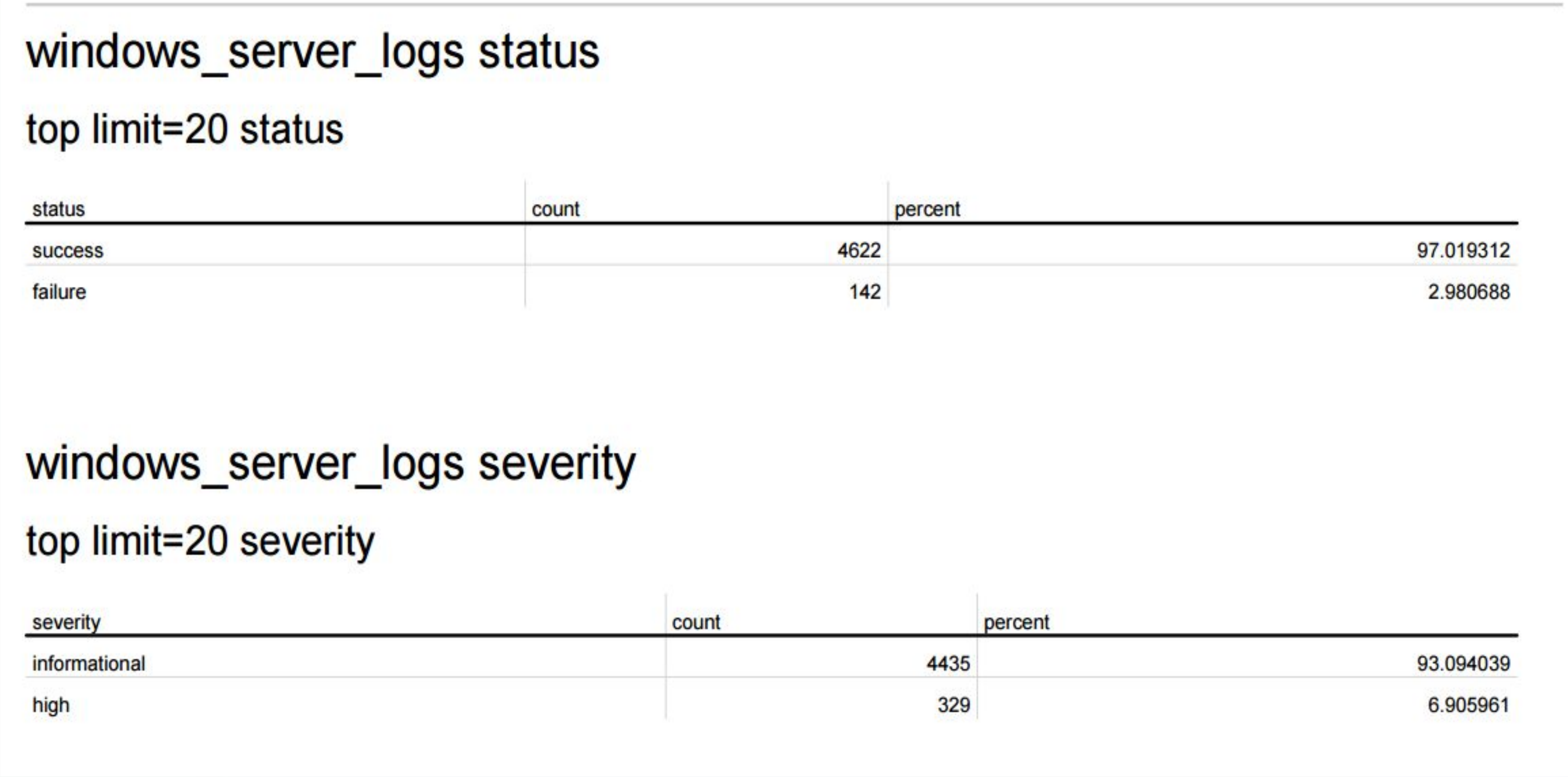
windows_server_logs signatues_id

signatures_ id



windows_server_logs user

stats count by user



windows_server_logs status

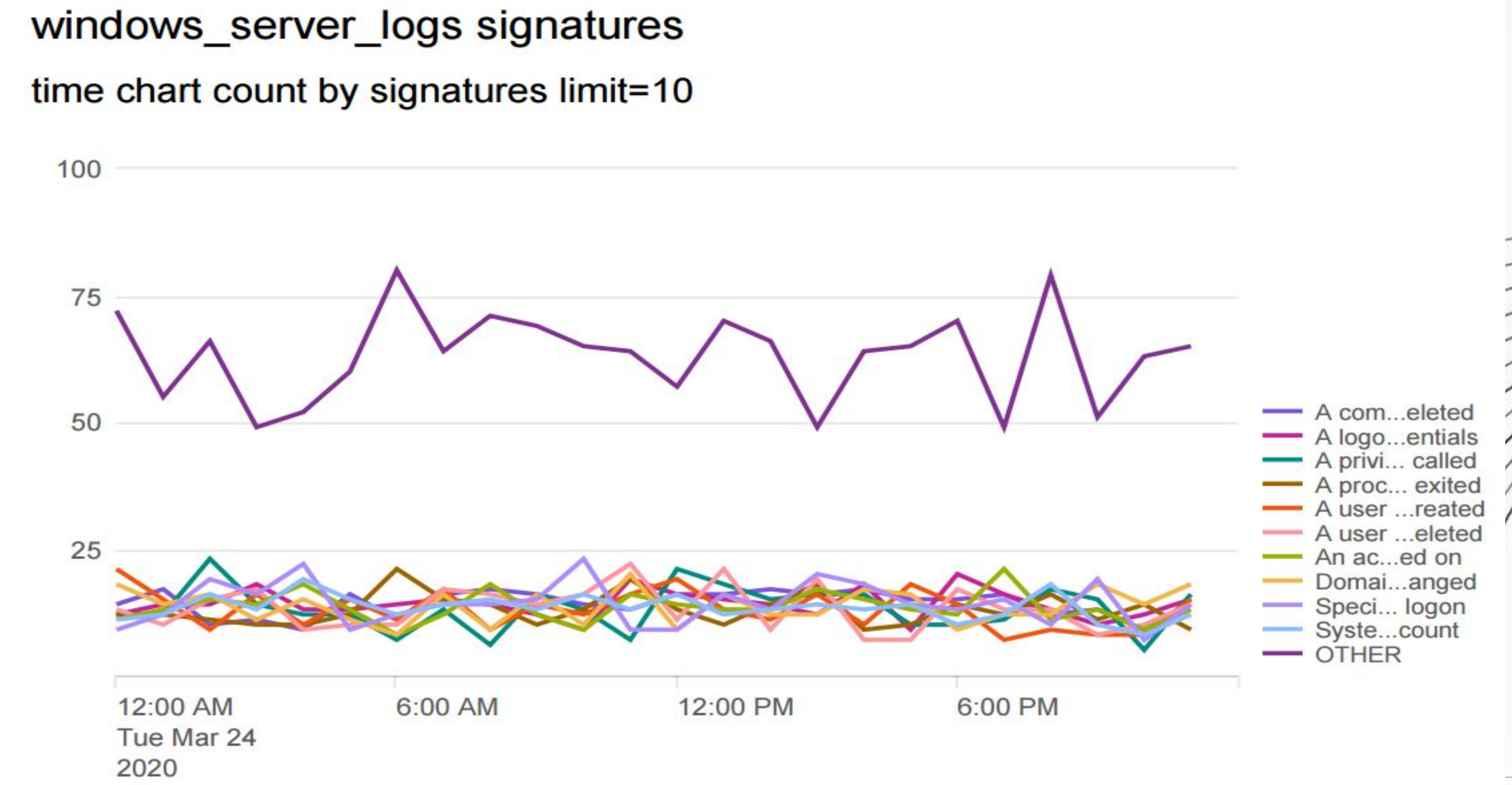
top limit=20 status

status	count	percent
success	4622	97.019312
failure	142	2.980688

windows_server_logs severity

top limit=20 severity

severity	count	percent
informational	4435	93.094039
high	329	6.905961



windows_server_logs signatures

time chart count by signatures limit=10

APACHE LOGS

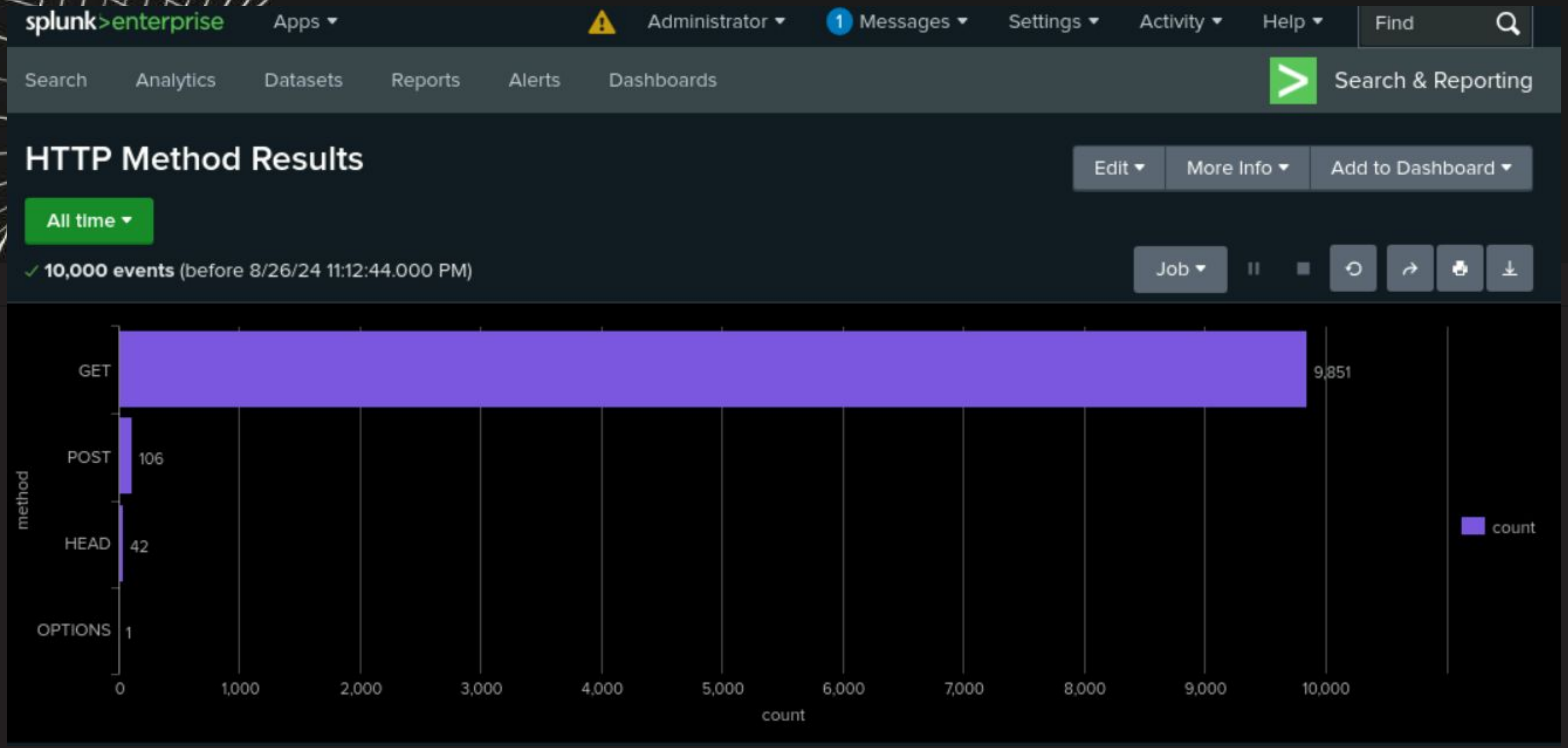
PRESENTED BY: BRYAN ZAMORA and LIAN CHANCAY

VIRTUAL SPACE INDUSTRIES

APACHE REPORTS

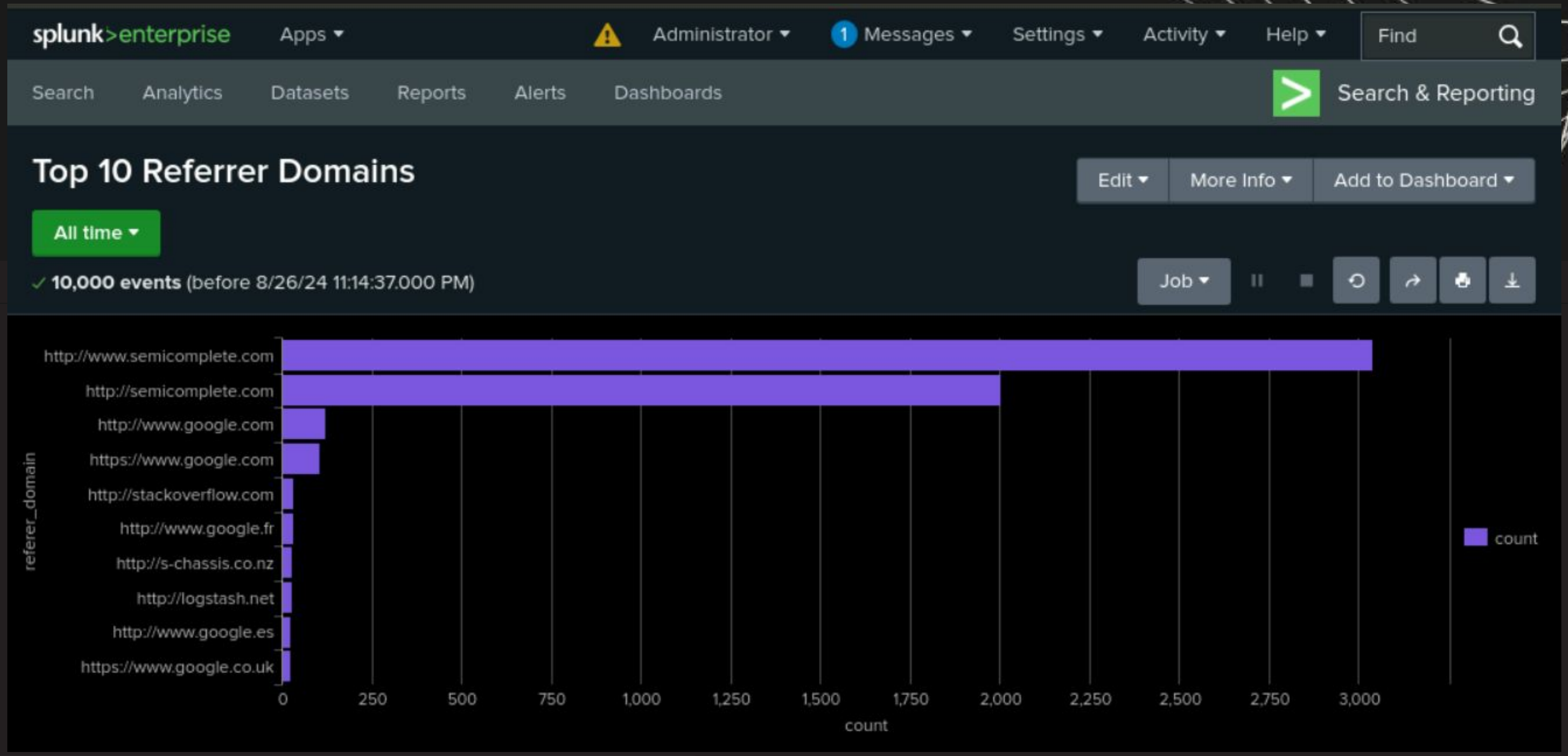
Report Name	Report Description
HTTP Method	Shows different HTTP methods (GET, POST, HEAD, etc.) to provide insight into the type of HTTP activity methods used.
Top 10 Referring Domains	Tracks the top 10 domains that refer to VSI’s website, helping to identify suspicious referrers.
HTTP Response Codes	Counts each HTTP response code to identify any suspicious levels of HTTP responses.

APACHE REPORTS



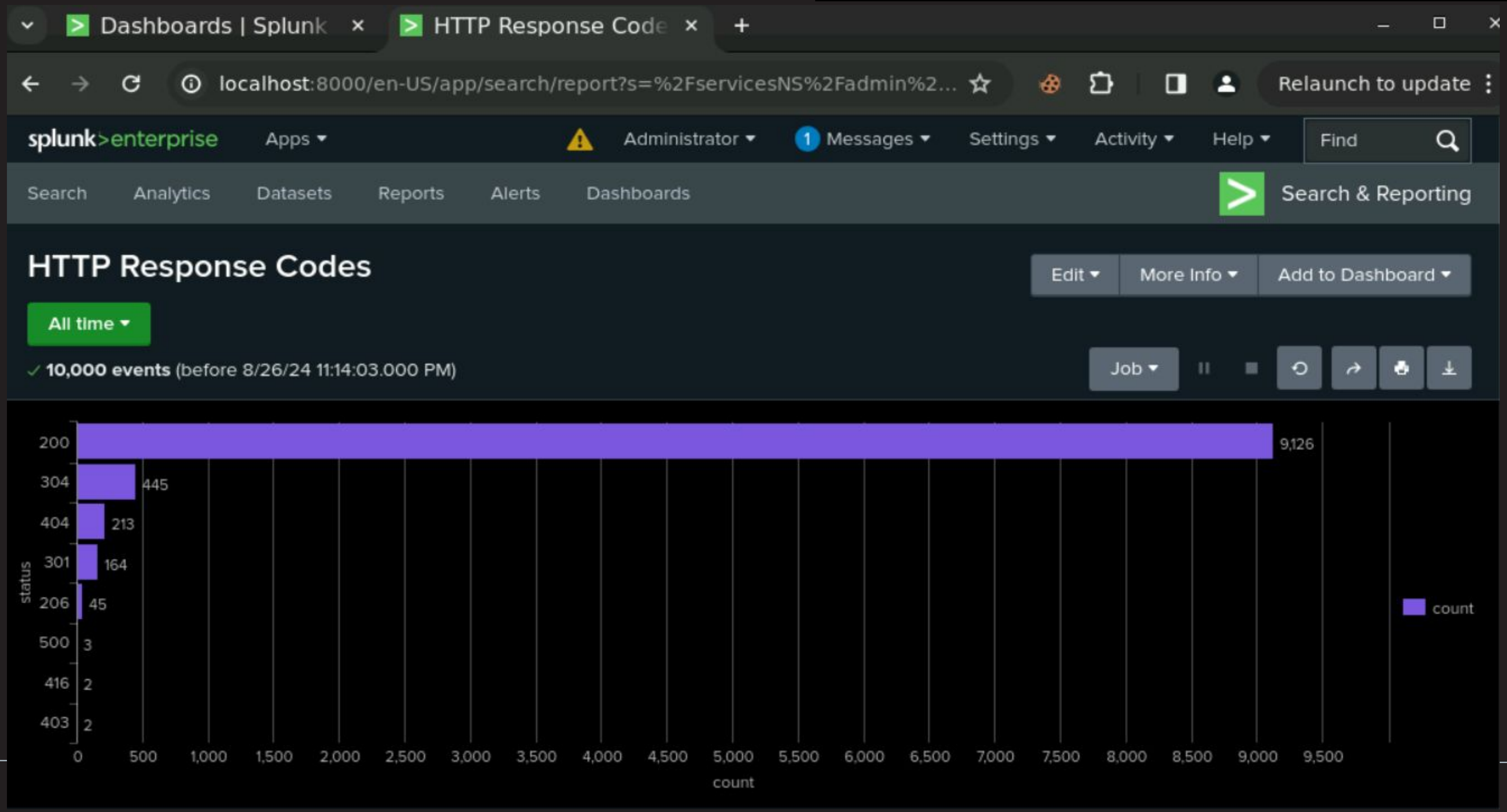
HTTP Method Results

✓ **10,000 events** (before 8/26/24 11:12:44.000 PM)



Top 10 Referrer Domains

✓ **10,000 events** (before 8/26/24 11:14:37.000 PM)



HTTP Response Codes

✓ **10,000 events** (before 8/26/24 11:14:03.000 PM)

VIRTUAL SPACE INDUSTRIES

APACHE ALERTS

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-US Activity Threshold	Hourly activity from countries other than the United States	2	5

JUSTIFICATION: A high amount of Non-US Activity Threshold can indicate suspicious behavior. Normal activity was around 2, and spikes above 5 were rare and may warrant attention.

APACHE ALERTS

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI HTTP POST Count	Alert if the hourly count of the HTTP POST method exceeds the threshold.	3	12

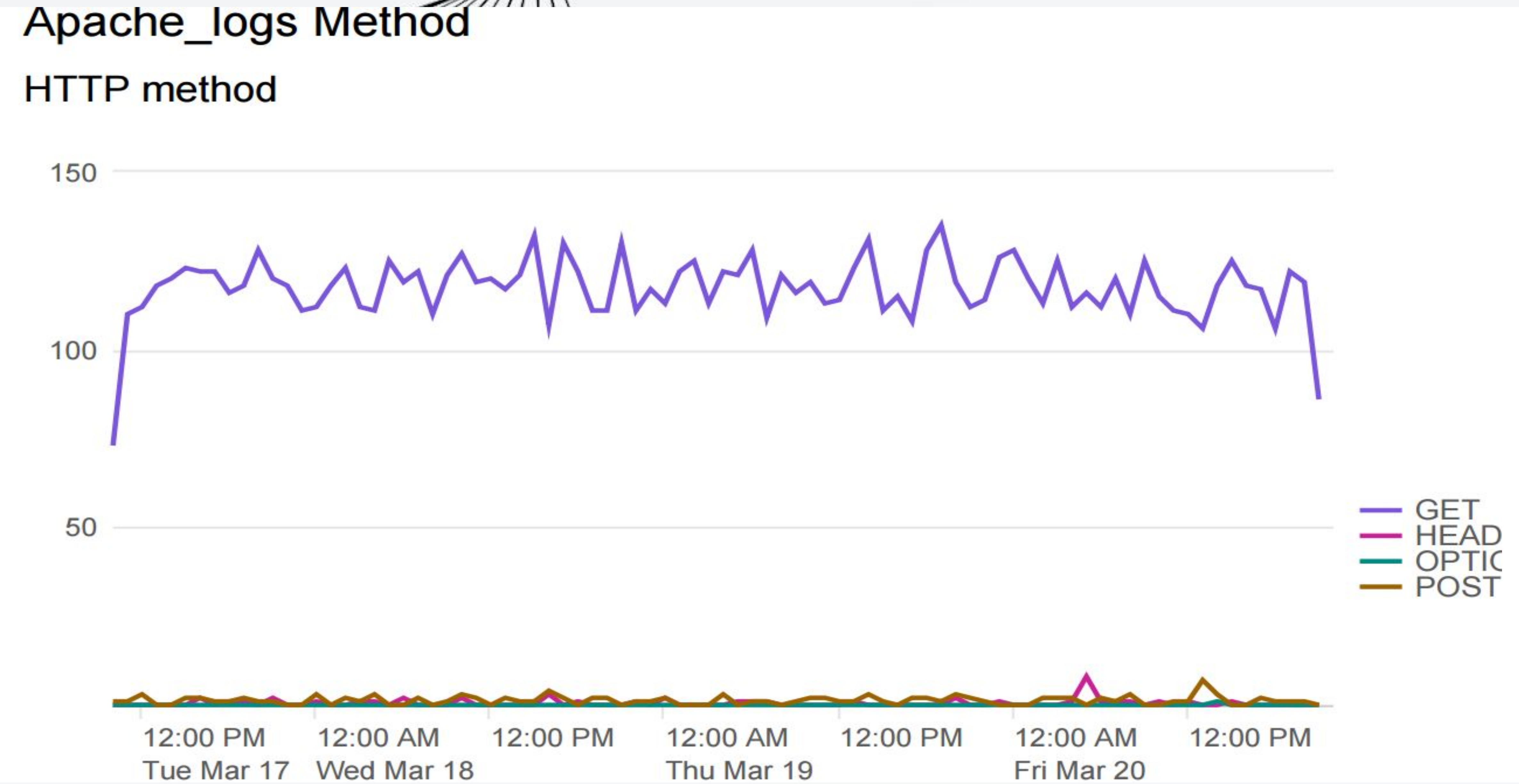
JUSTIFICATION: Most Events per hour hovered between 1 and 4 and never surpassed 7. A threshold of 12 seemed like a number that would be out of reach of “normal” hourly events but low enough to catch malicious activity.

APACHE ALERTS

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP Post Method	Alert tracks POST	4	5

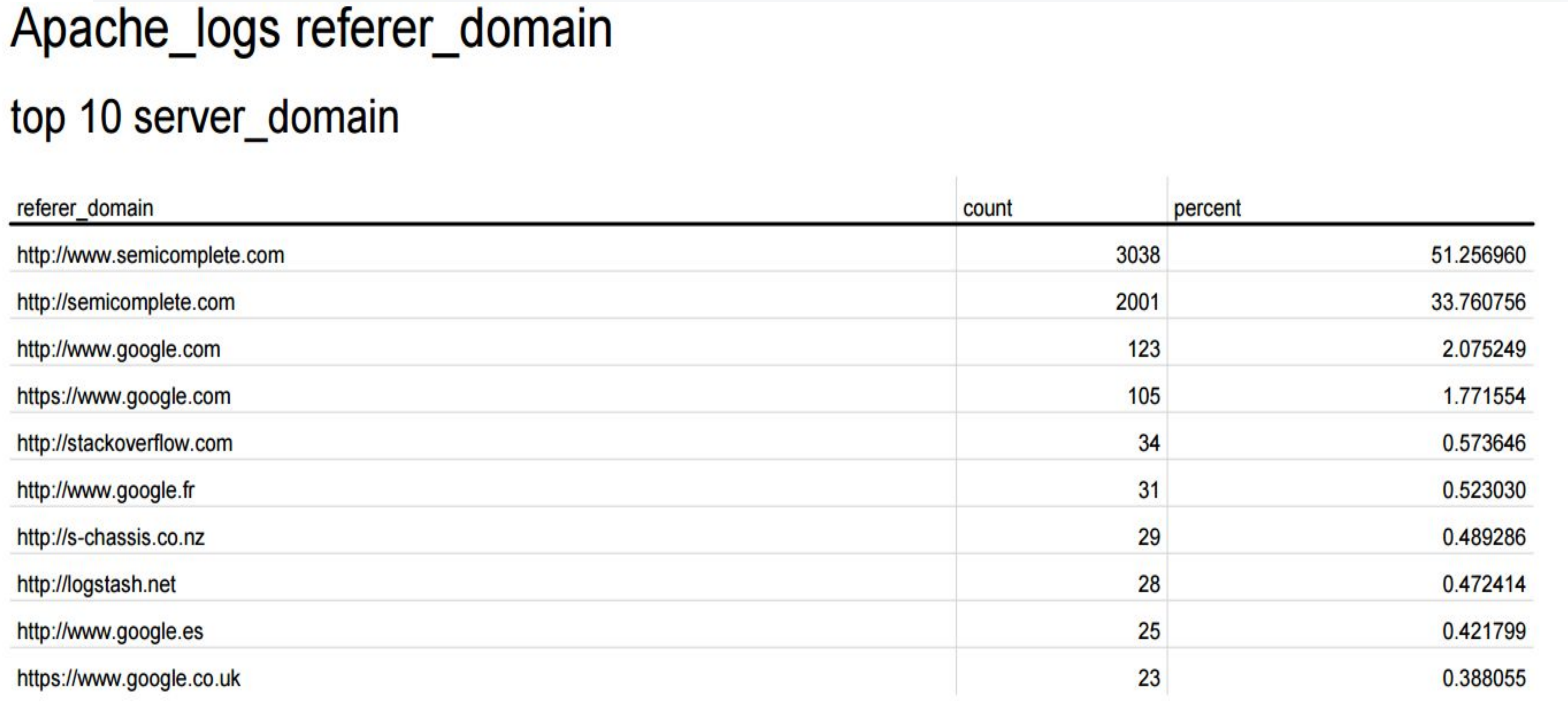
JUSTIFICATION: Amount of POST rarely goes above 4 in the data sample. Spikes above 5 are rare.

APACHE DASHBOARDS



Apache_logs Method

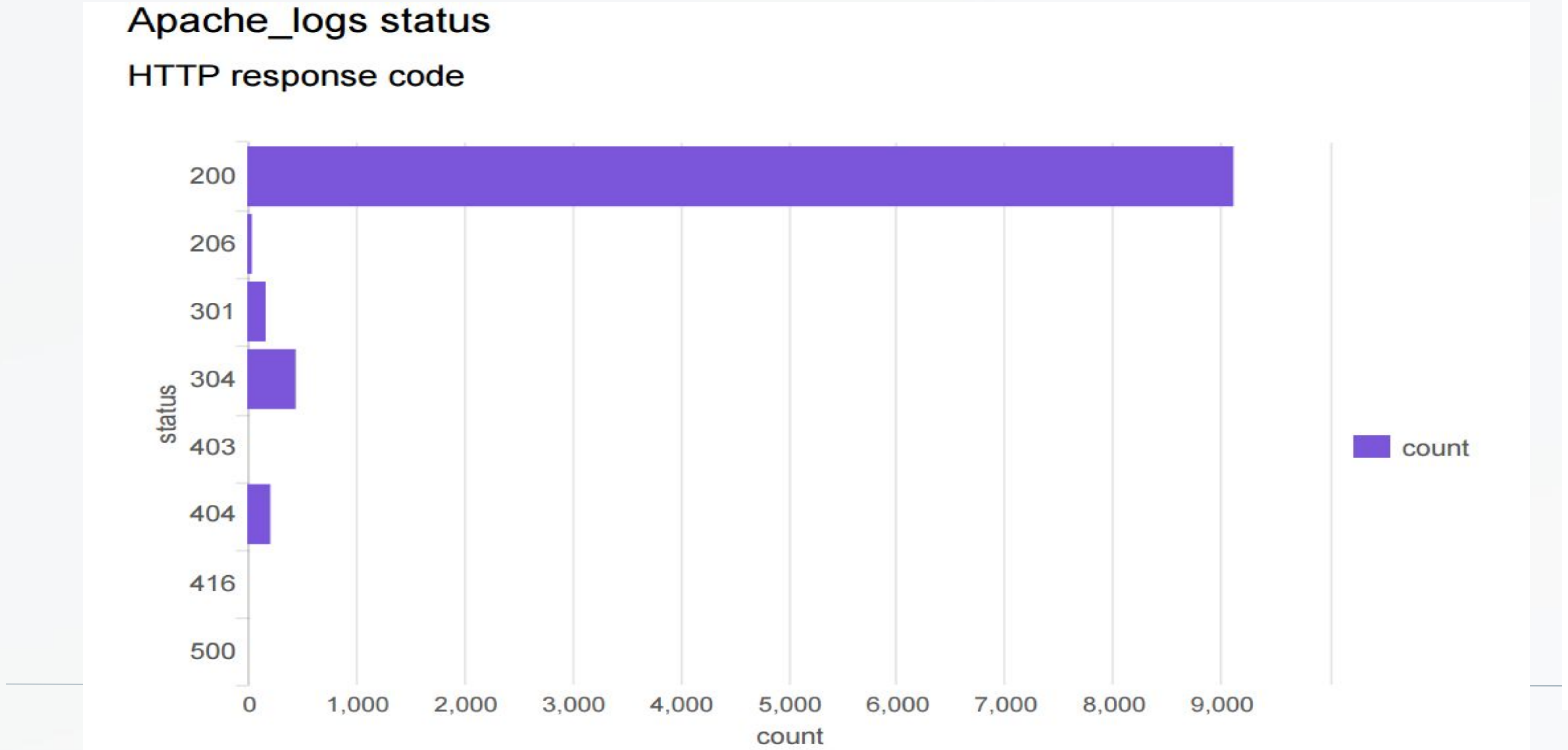
HTTP method



Apache_logs referer_domain

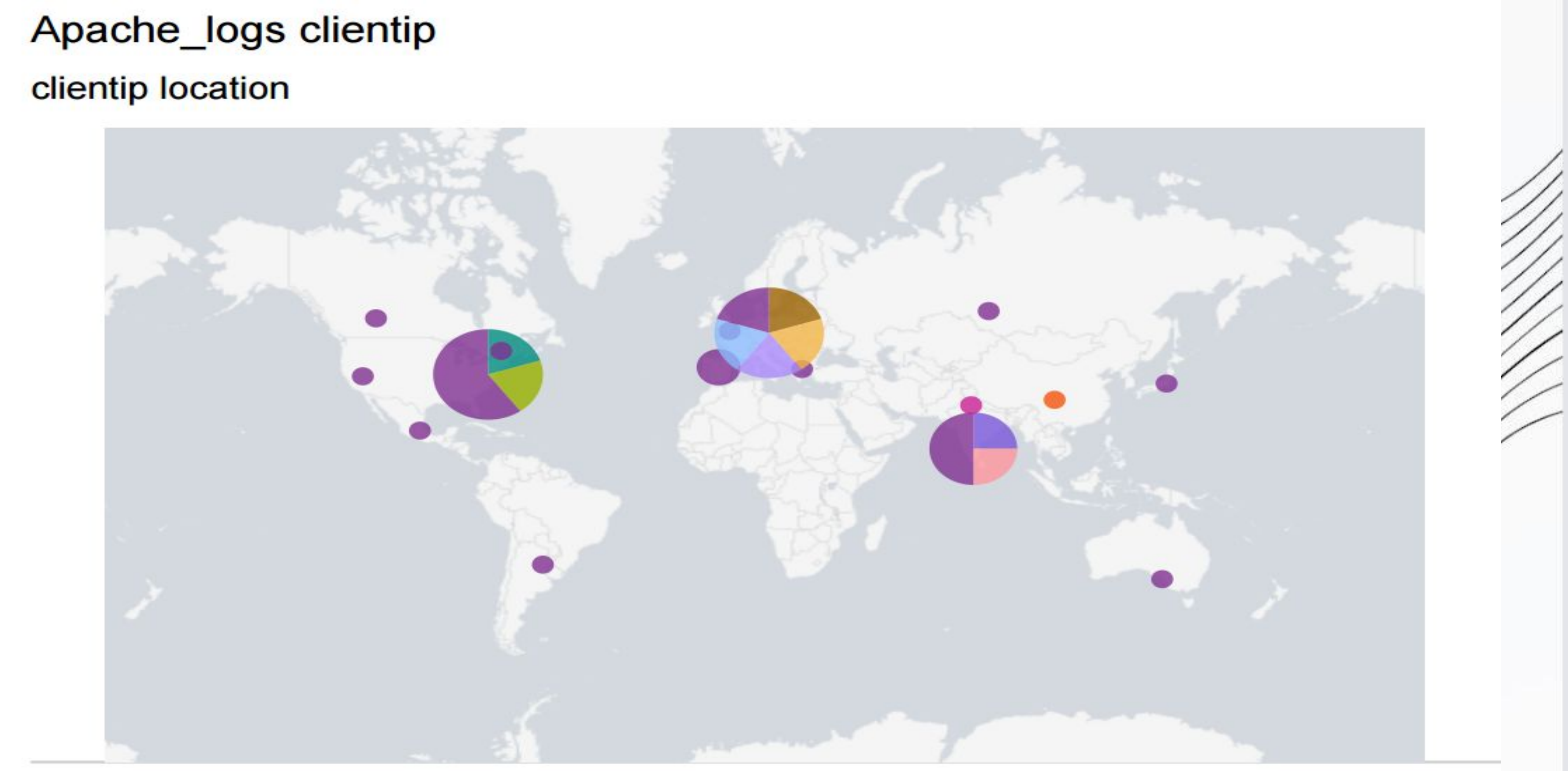
top 10 server_domain

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



Apache_logs status

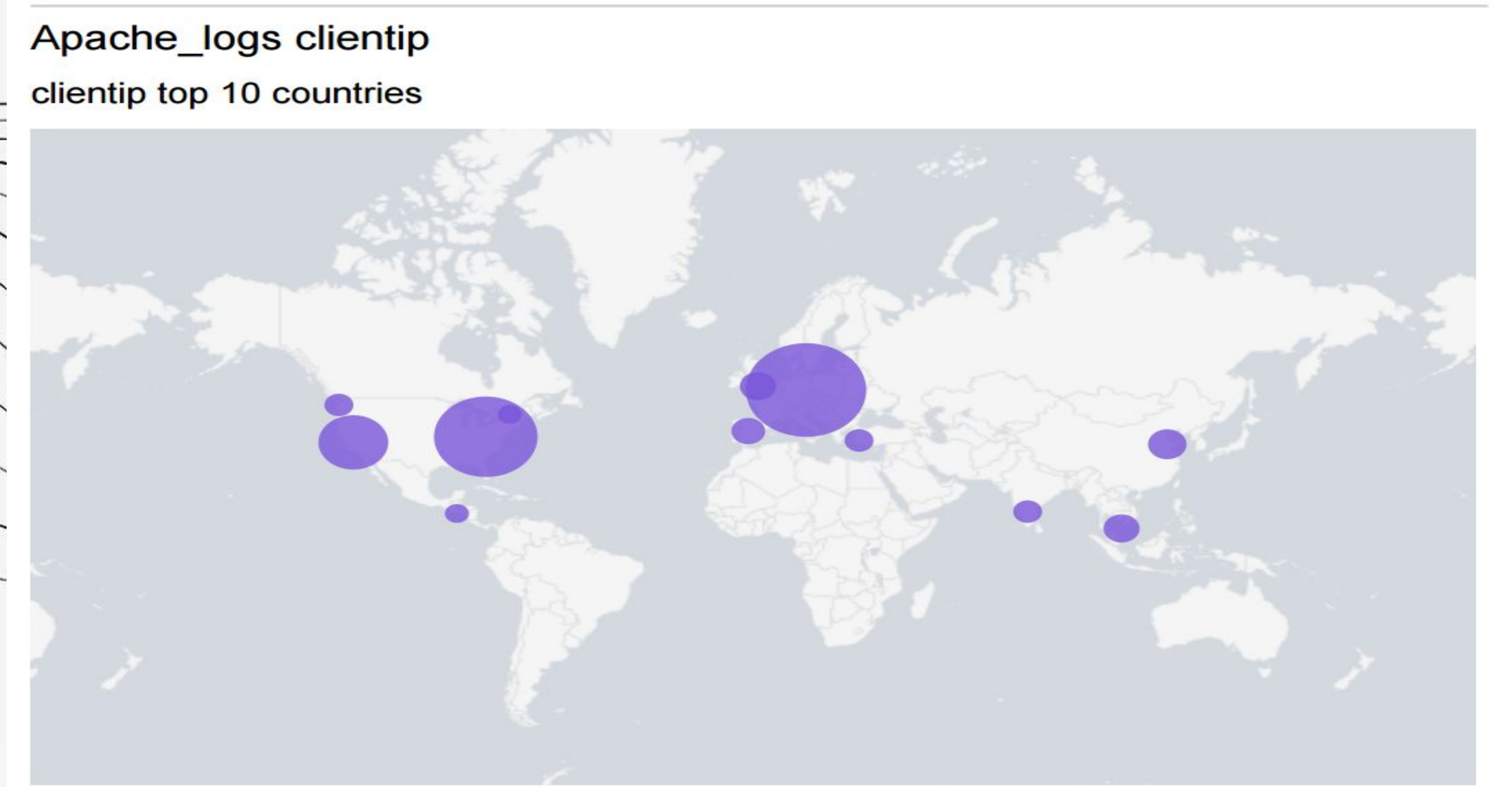
HTTP response code



Apache_logs clientip

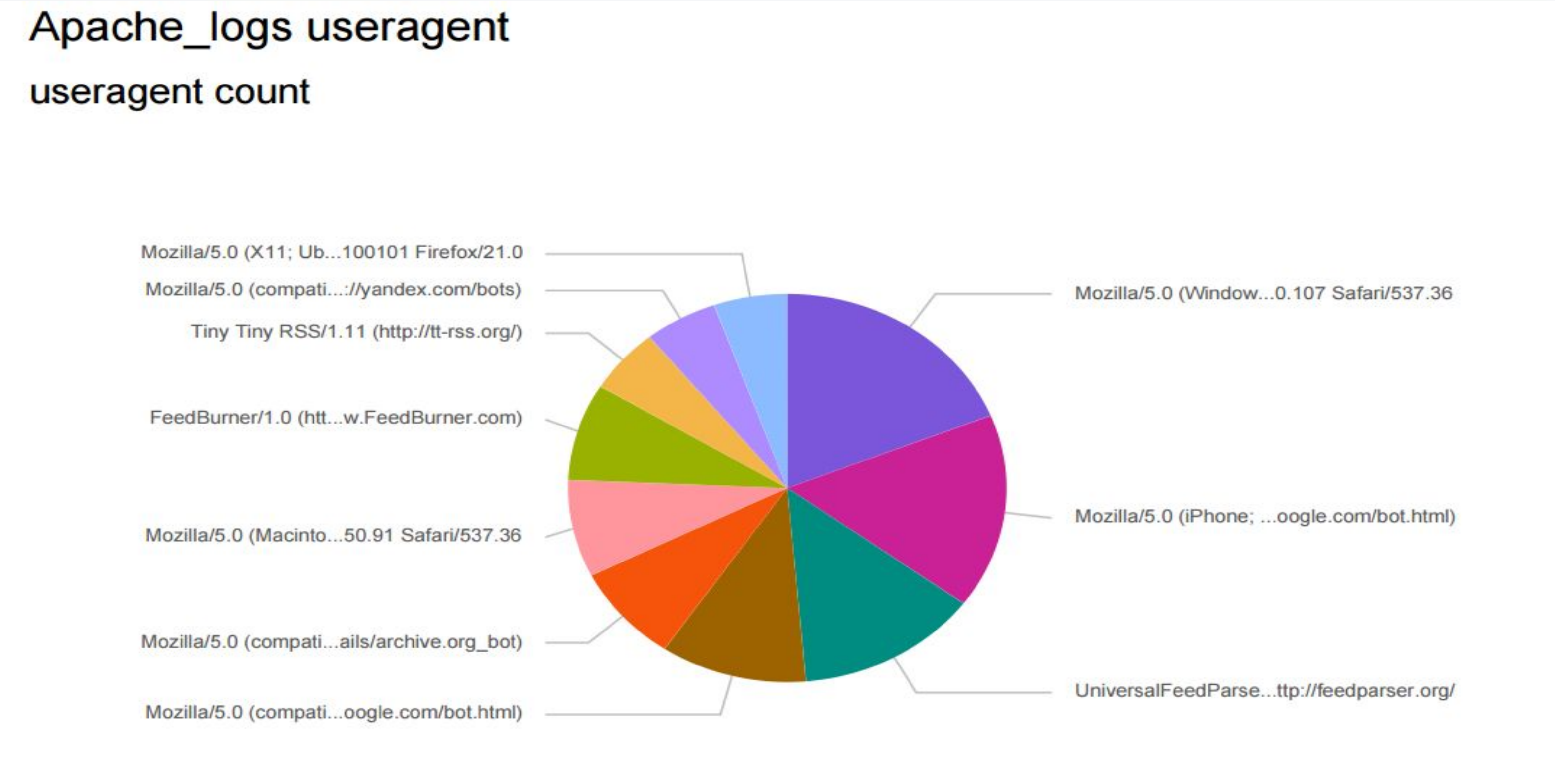
clientip location

APACHE DASHBOARDS



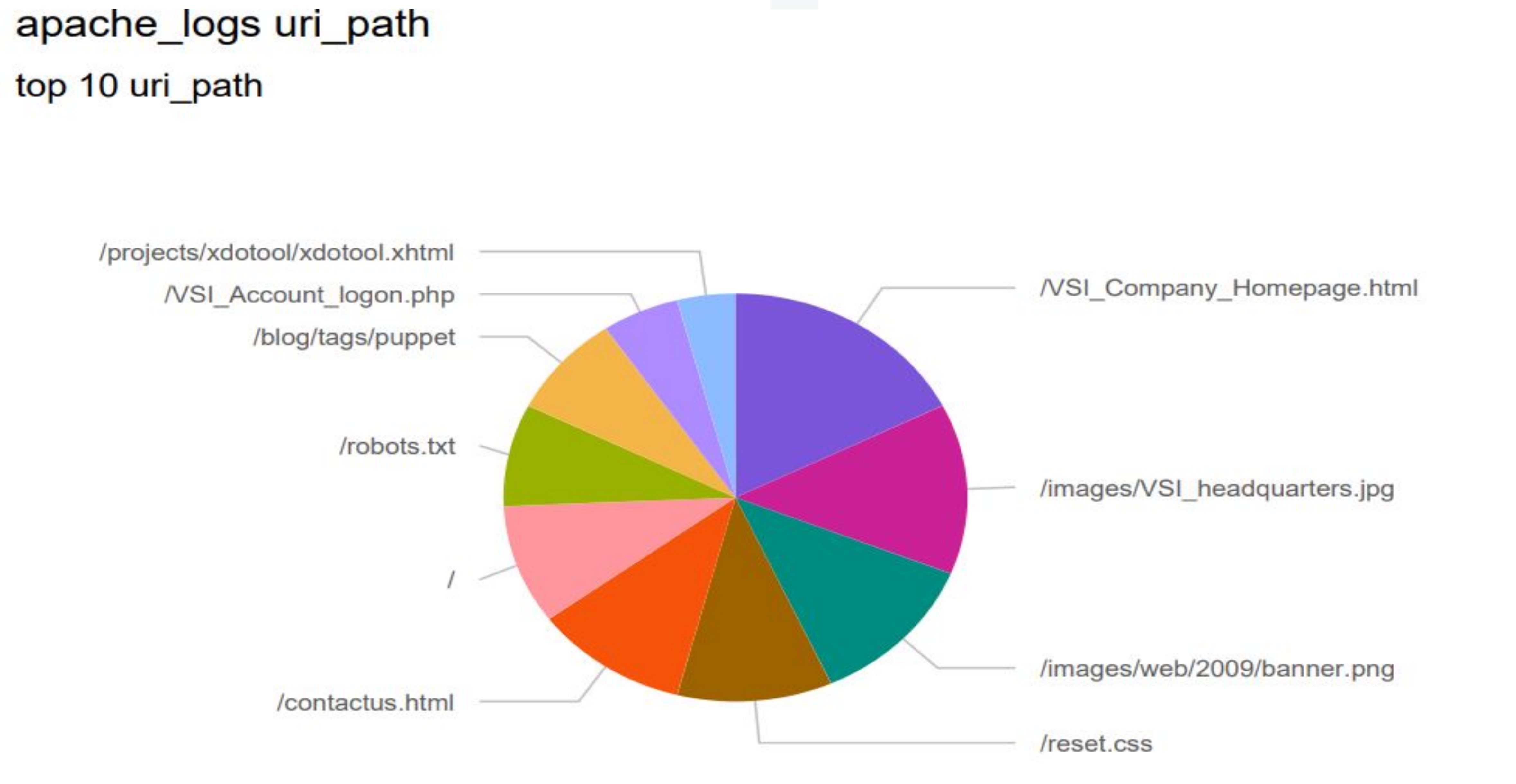
Apache_logs clientip

clientip top 10 countries



Apache_logs useragent

useragent count



apache_logs uri_path

top 10 uri_path

ATTACK ANALYSIS

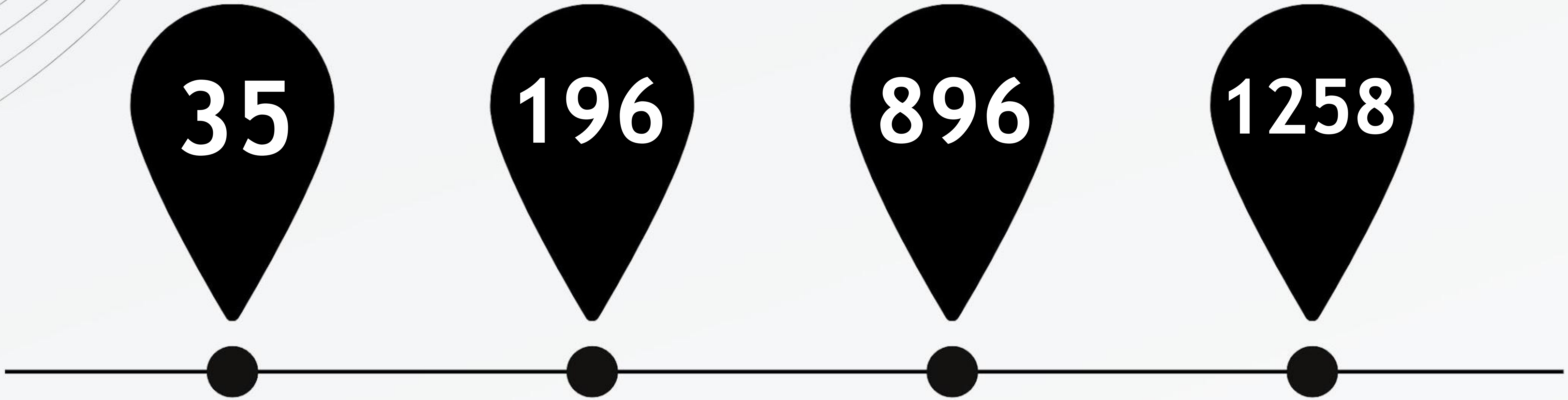
PRESENTED BY: GROUP 5

VSI
VIRTUAL SPACE
INDUSTRIES

MICROSOFT ATTACK SUMMARY

Analysis reveals several concerning patterns that suggest a targeted attack on VSI's Windows Server.

The alerts and dashboards were effective in identifying and visualizing these anomalies.



35

FAILED LOGINS

A spike in failed activity was detected at 8:00 AM on March 25th.

The alert was correctly triggered.

196

SUCCESSFUL LOGINS

Suspicious login activity observed at 11:00 AM (196) and 12:00 PM (77) on March 25th; Primary user identified as ‘user_j’

The alert was correctly triggered.

896

LOCKOUTS

The attack on “An attempt was made to reset an account password” started at 8:00 AM, ended at 11:00 AM.

Peak count is 896, in dashboard analysis we can see a significant increase in the whole count.

1258

PASSWORD RESETS

The attack on this signature“A user account was locked out” started at 12:00 AM, ended at 3:00 AM.

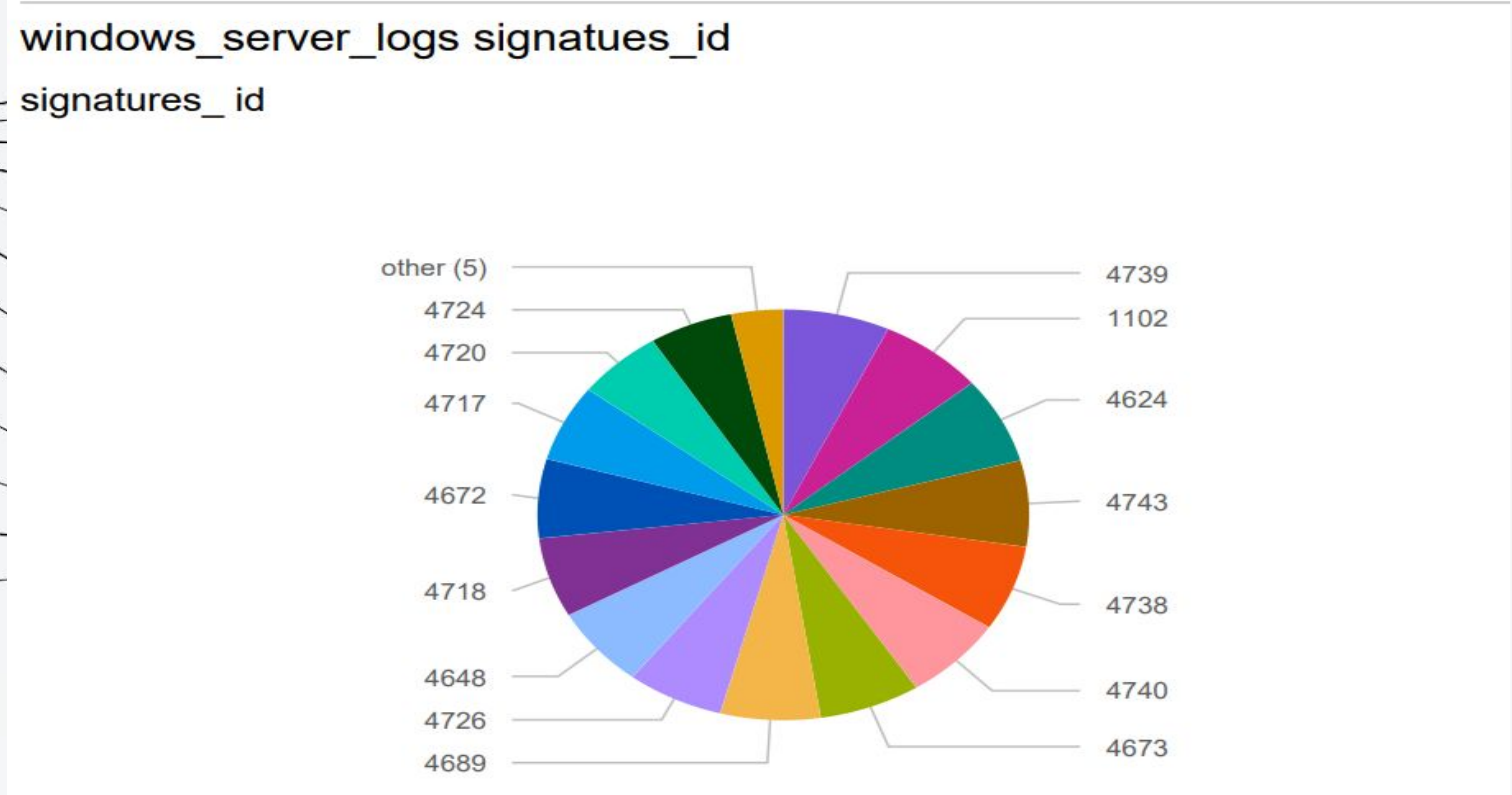
Peak count of 1,258, on dashboard analysis shows the increase on this signature.

DASHBOARD SUMMARY

The time chart and statistical analysis confirmed the suspicious patterns of account lockouts and password reset attempts.

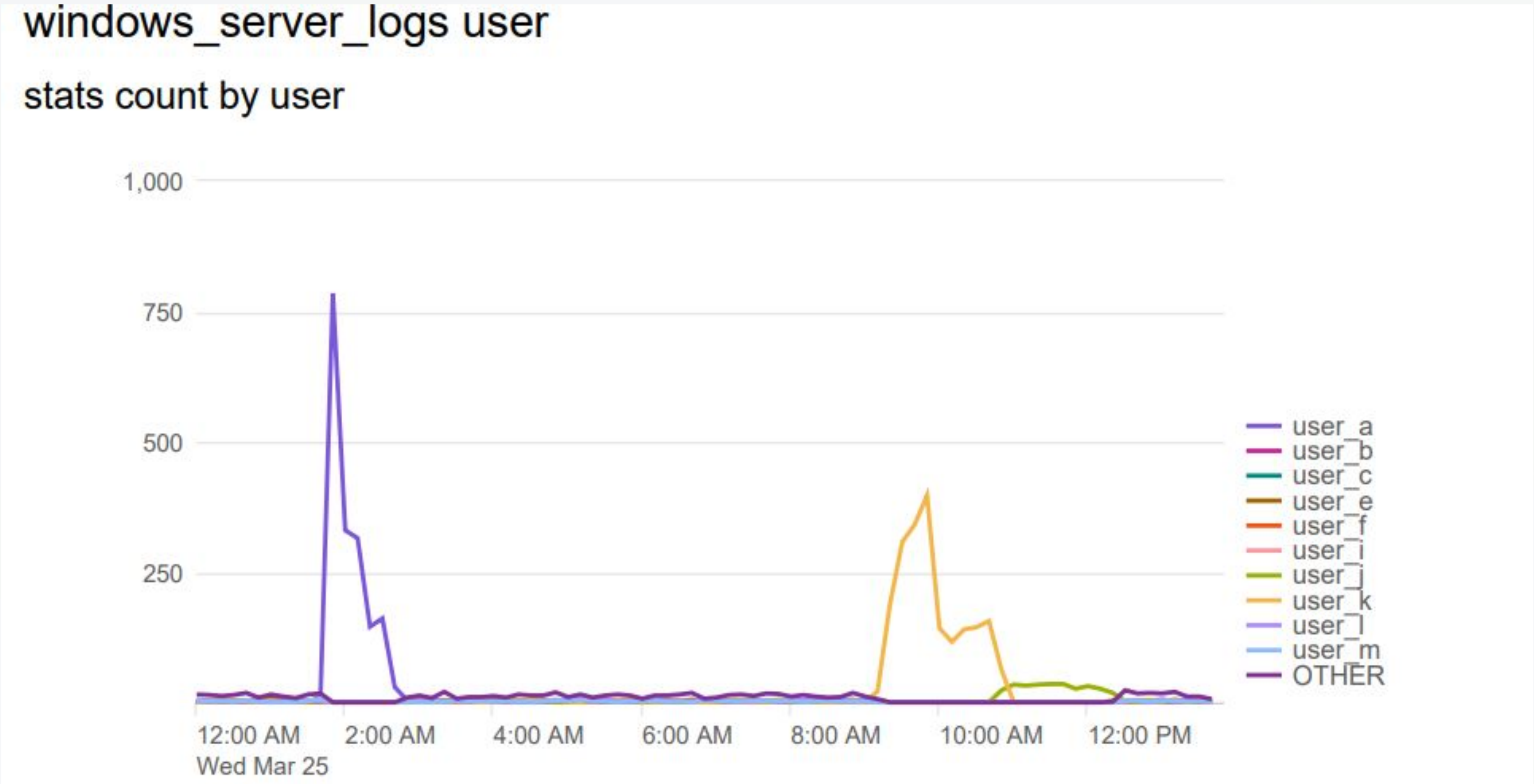
Both **user_a** and **user_k** stood out for their high levels of activity during the attack period.

WINDOWS ATTACK LOGS



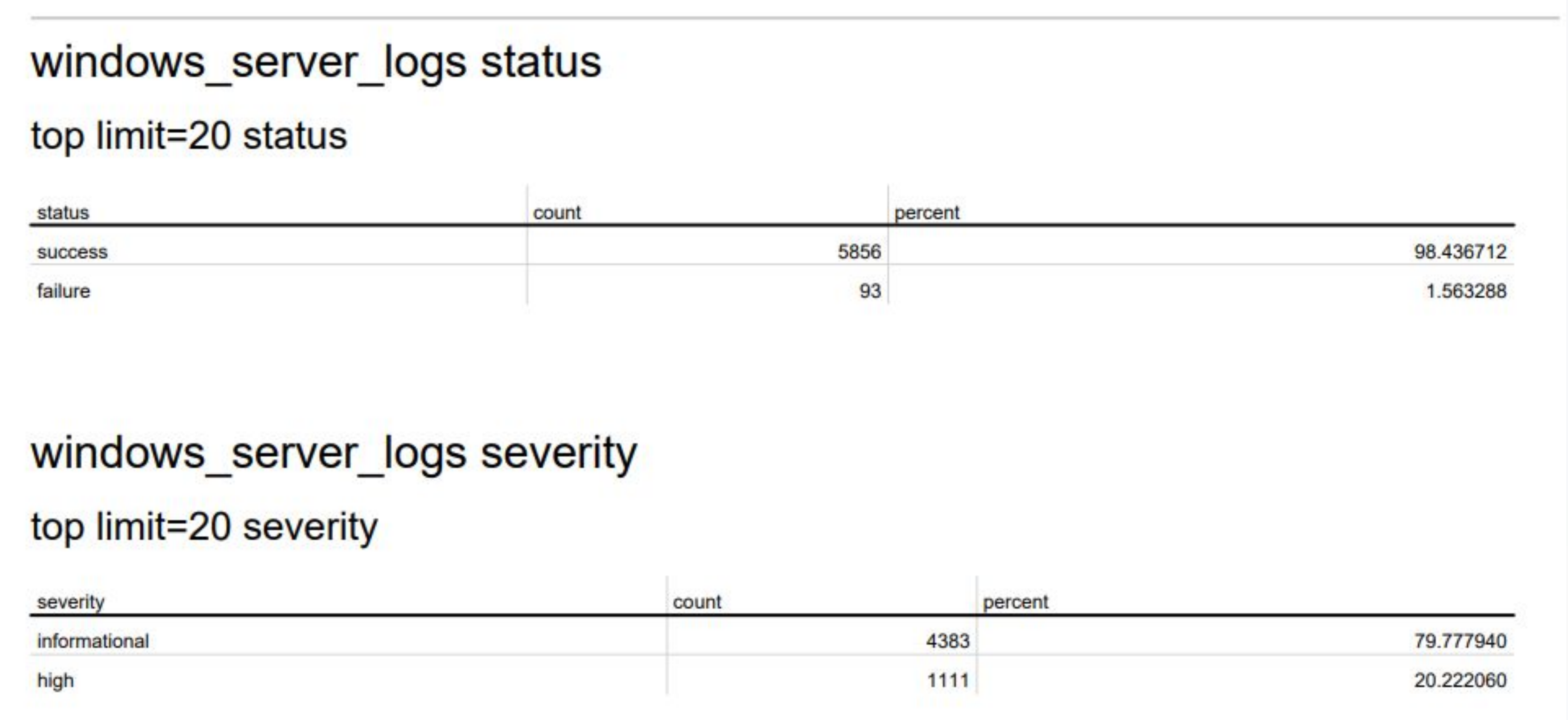
windows_server_logs signatues_id

signatures_ id



windows_server_logs user

stats count by user



windows_server_logs status

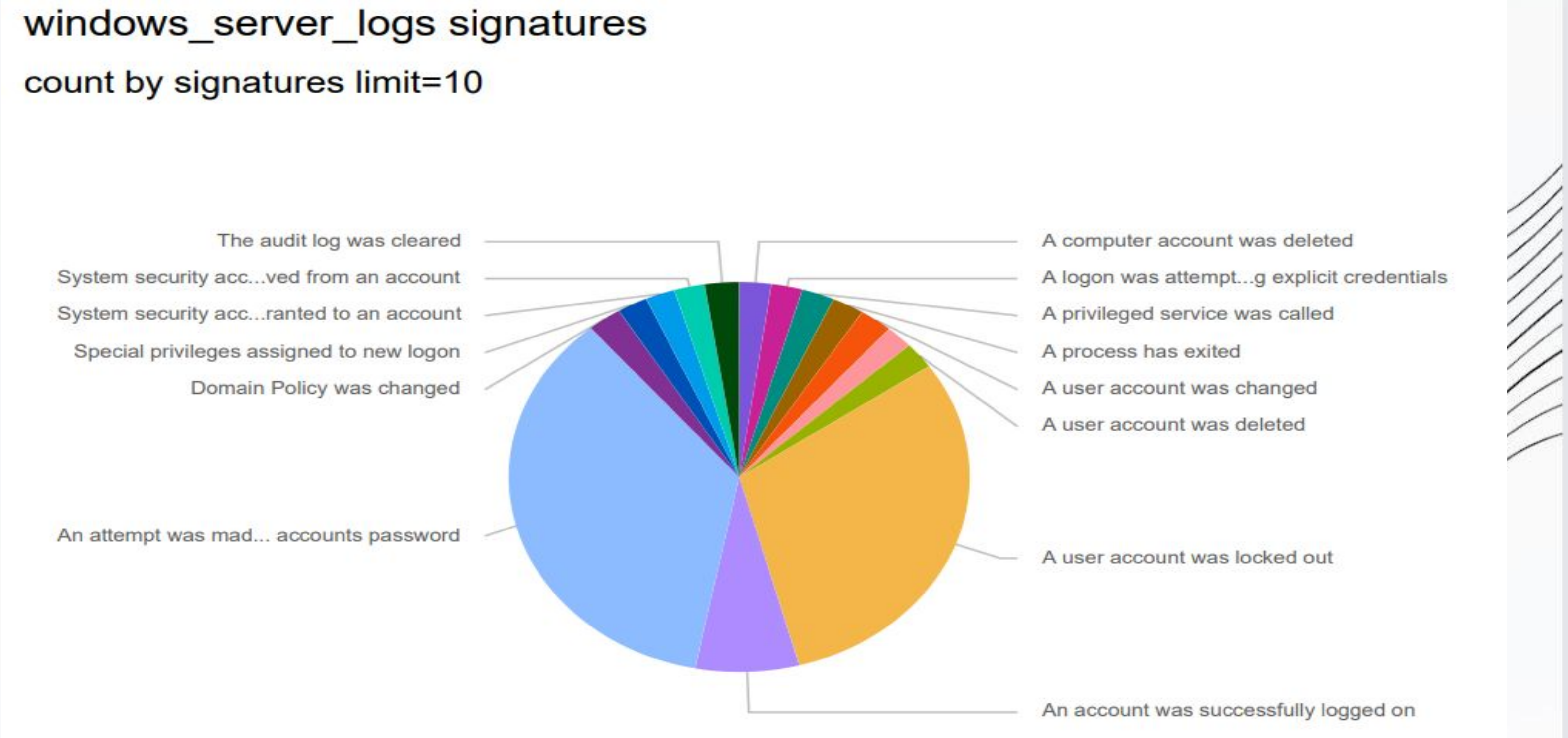
top limit=20 status

status	count	percent
success	5856	98.436712
failure	93	1.563288

windows_server_logs severity

top limit=20 severity

severity	count	percent
informational	4383	79.777940
high	1111	20.222060



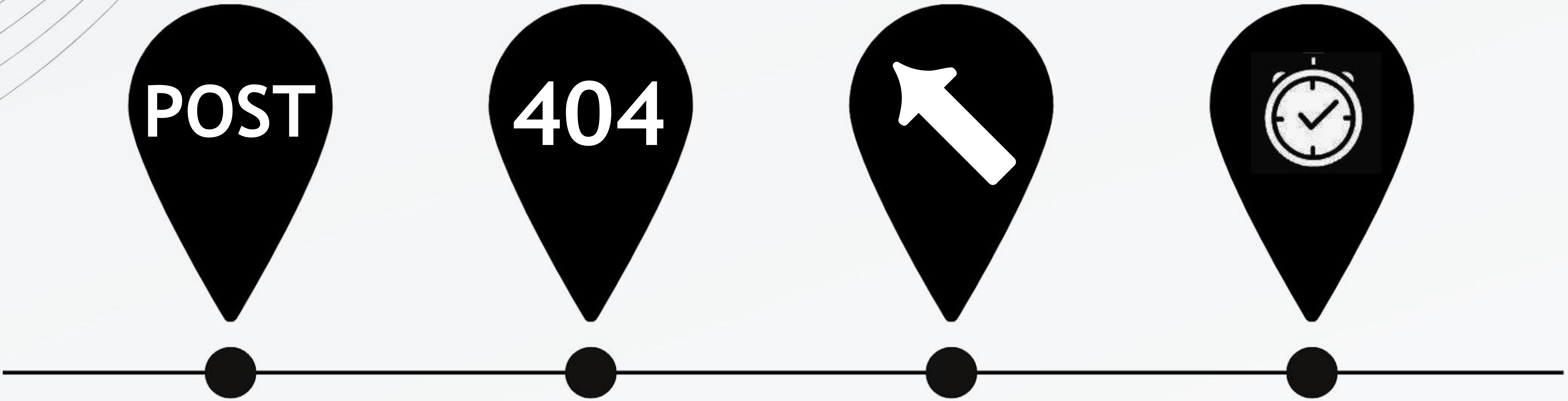
windows_server_logs signatures

count by signatures limit=10

APACHE ATTACK SUMMARY

Overall, the Apache Web Server logs reveal several indicators of a concerted effort to probe for vulnerabilities, potentially compromise the server, and disrupt services.

The alerts and dashboards played a crucial role in detecting and visualizing these threats.



HTTP METHODS

POST, DELETE, and TRACE HTTP methods each saw a major increase.

The alert was correctly triggered.

ERROR CODES

Significant increase in the 404 category for the HTTP Response code report. Reaching well over 500 “404 HTTP Response codes”

The alert was correctly triggered.

IP TRAFFIC

There was a spike in traffic from IPs associated with regions outside of the usual traffic patterns, particularly from Eastern Europe and Southeast Asia.

TRAFFIC ANOMALIES

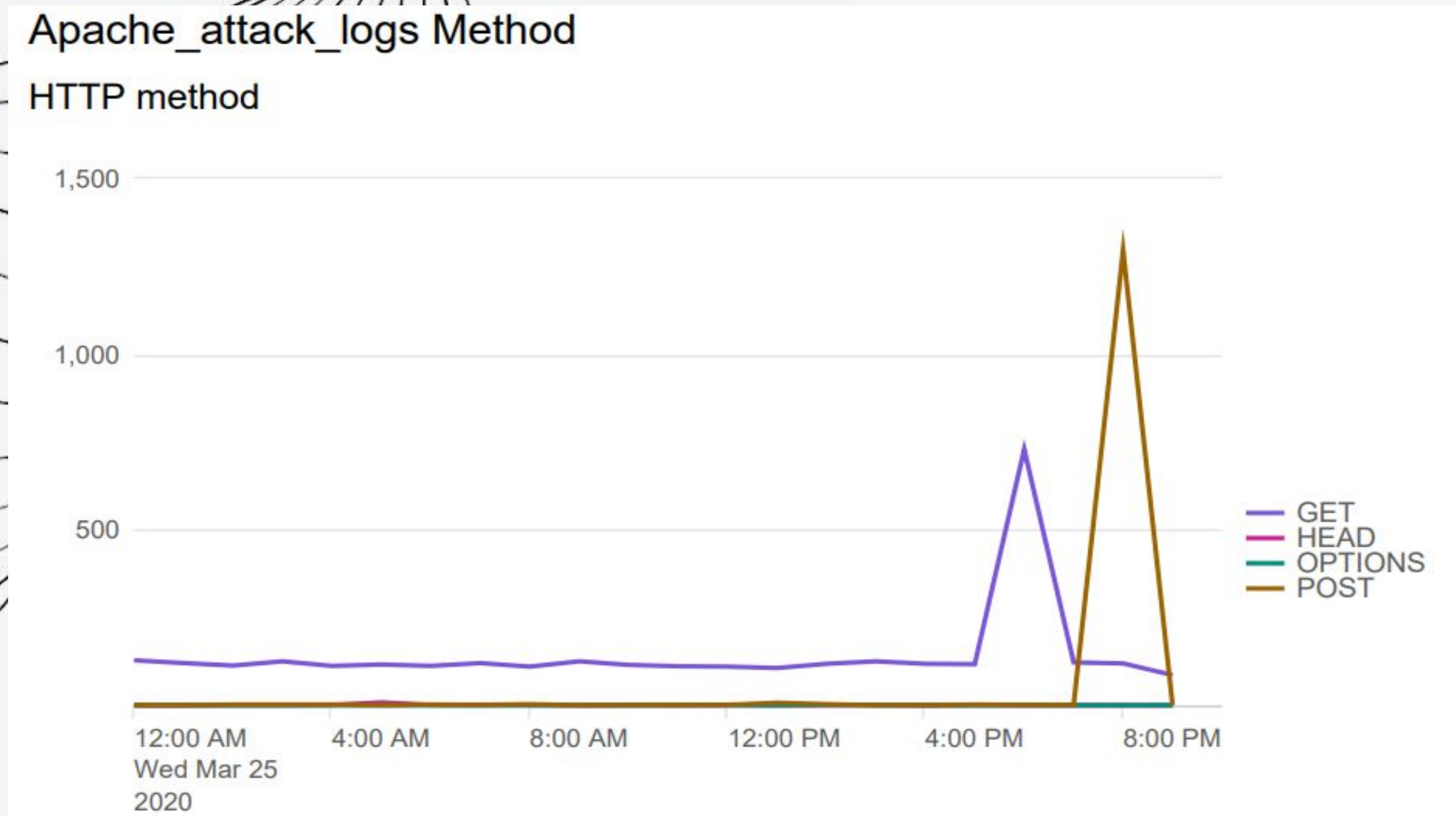
Significant spikes in traffic during off-peak hours were detected, often correlated with suspicious IP addresses or HTTP methods.

DASHBOARD SUMMARY

In the different geographical maps and time chart we can see an increase of the activity suggesting a denial of service by the attacker in several parts of the world.

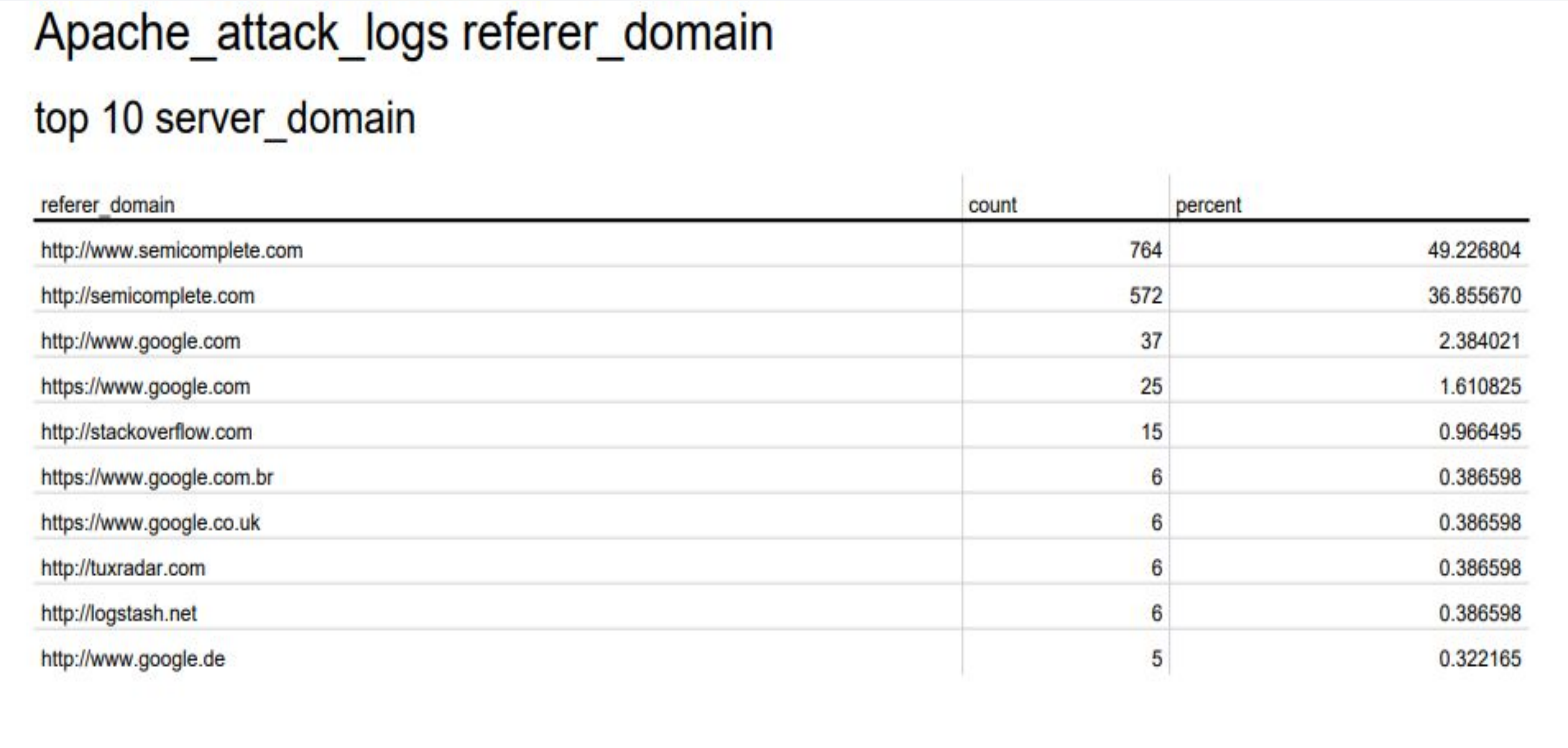
POST activity on a high level during the attack on March/25/2020 at 8:00pm, URI most hit was /VSI_Account_logon.php

APACHE ATTACK LOGS



Apache_attack_logs Method

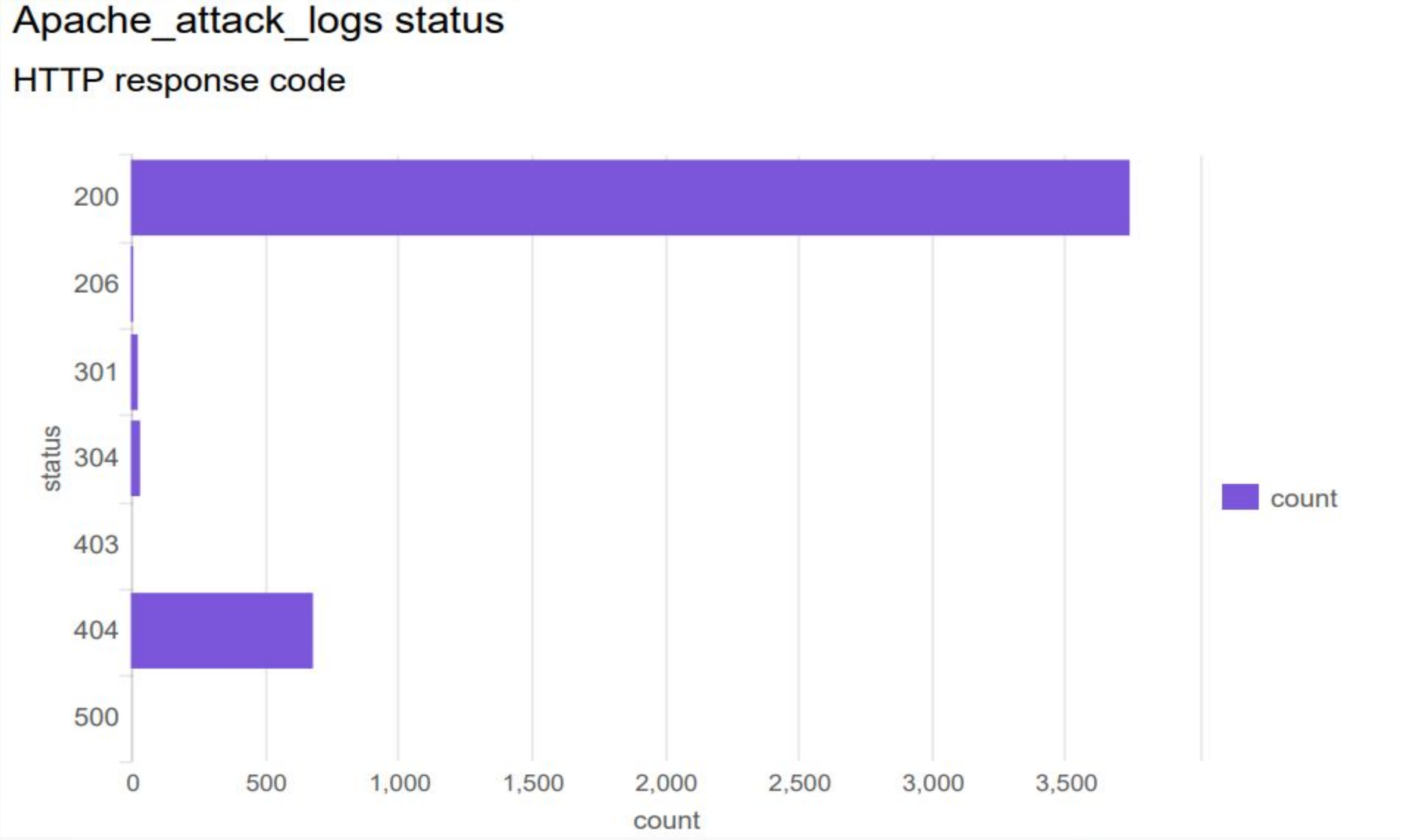
HTTP method



Apache_attack_logs referer_domain

top 10 server_domain

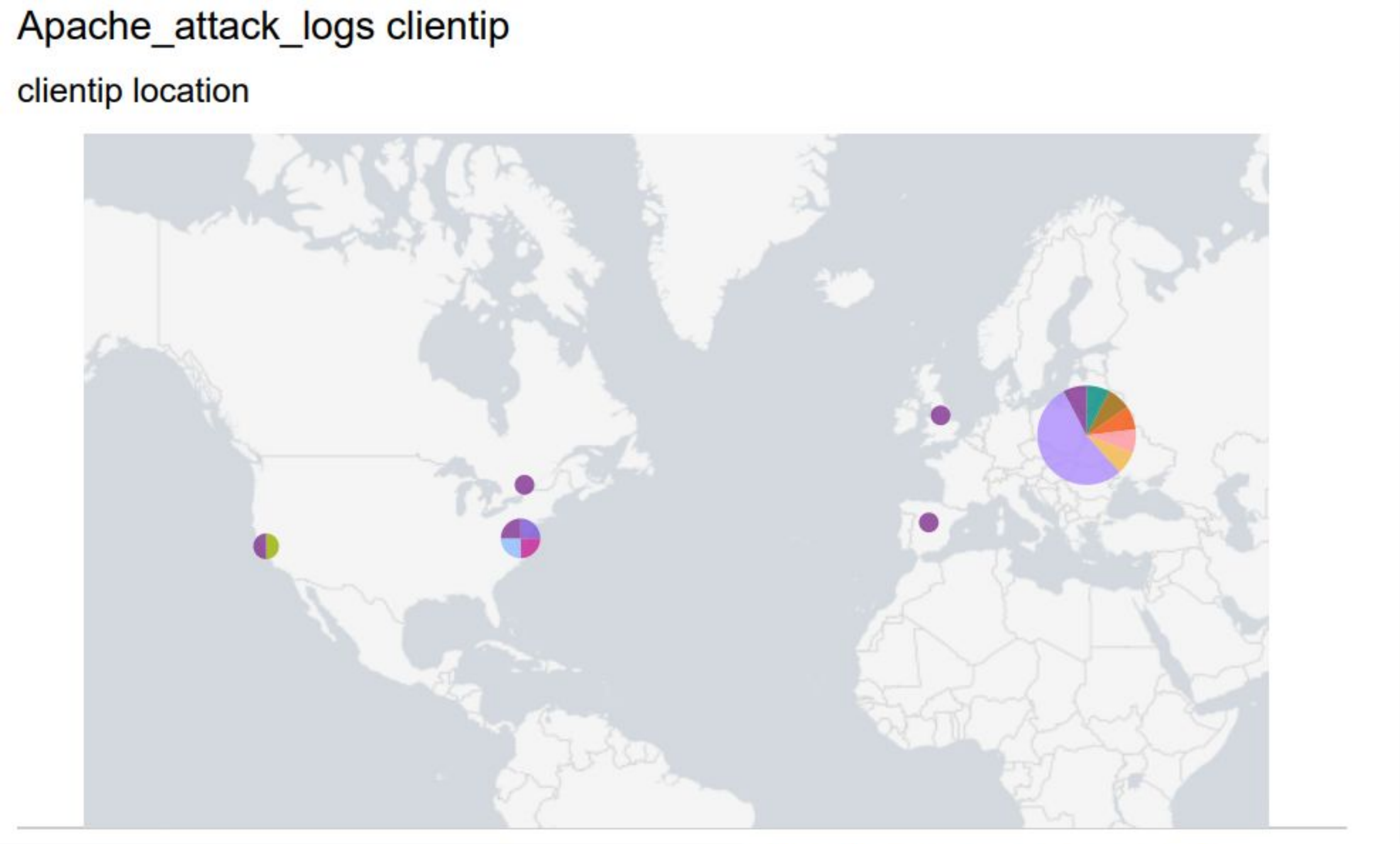
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com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



Apache_attack_logs status

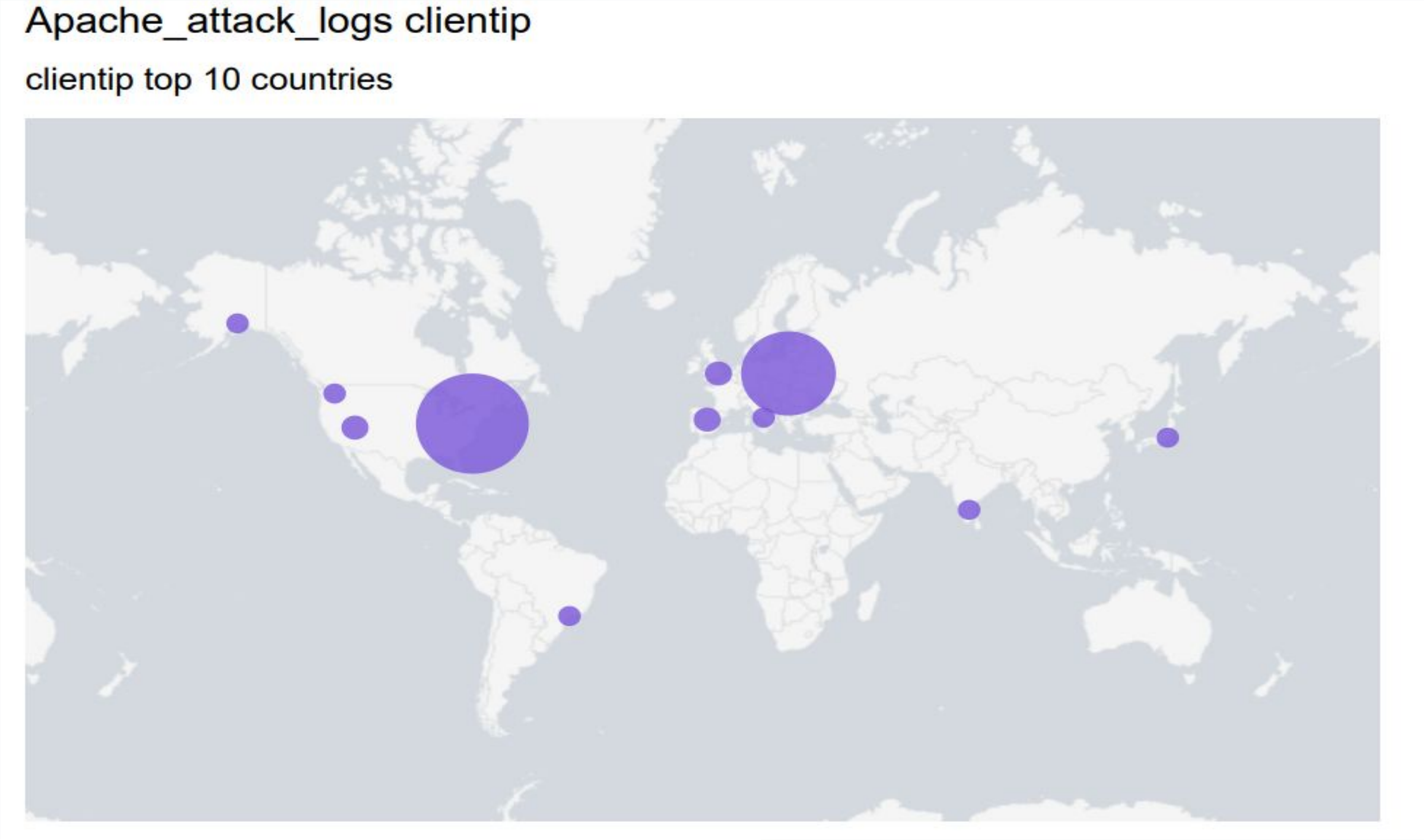
HTTP response code

APACHE ATTACK LOGS



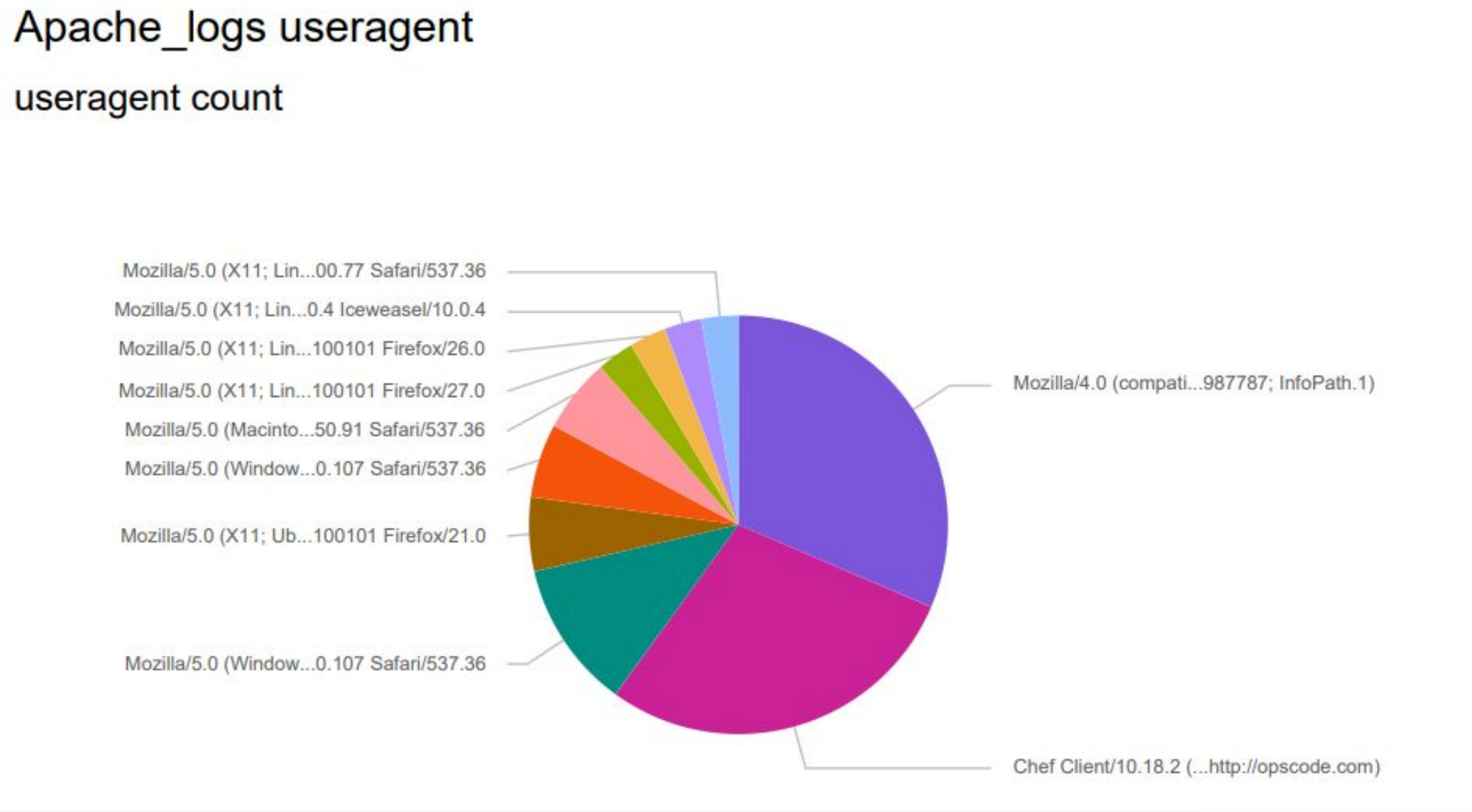
Apache_attack_logs clientip

clientip location



Apache_attack_logs clientip

clientip top 10 countries



Apache_logs useragent

useragent count

SUMMARY AND FUTURE MITIGATIONS

PRESENTED BY: DANIEL FARMER

VIRTUAL SPACE INDUSTRIES

SUMMARY

Virtual Space Industries (VSI) had multiple attacks on their windows and apache server on March-25-2020.

Key findings include signs of **unauthorized access attempts**, vulnerabilities related to **weak authentication** mechanisms, potential **misconfigurations**, and a lack of robust **monitoring and logging** practices.

VSI

VIRTUAL SPACE INDUSTRIES

MITIGATION

01 Strengthening Access Controls

02 Enhancing Logging and Monitoring

03 System Hardening

04 Improving Incident Response

05 User Awareness Training

06 Defense-in-Depth

07 Regular Security Assessments

08 Backup and Recovery Planning

09 Restricting Remote Access

THANK YOU

VSI
VIRTUAL SPACE
INDUSTRIES