

Defensive Security Project

by:

InfoSec Chillers Study Group

Gorin, Michael
Kamimura, Matt
Maurer, Chris
Meadow, Michael
Mosburg, Leon
Villanueva, Marc

Table of Contents

2

This document contains the following resources:

01

**Monitoring
Environment**

02

Attack Analysis

03

**Project Summary
& Future
Mitigations**

Monitoring Environment



Scenario

4

- Create a dashboard in Splunk that displays a baseline of statistics for Windows and Apache by using existing data logs to determine what normal daily operations look like for Virtual Space Industries (VSI). The baseline statistics are to then used to compare to data logs captured during and after a cyber attack on VSI.
- Detail mitigations to help prevent future attacks.

[“Add-On” App]



[ALERT MANAGER ENTERPRISE]

6

The screenshot shows the Splunkbase app store interface. At the top, there's a header with navigation icons, a URL bar showing `splunkbase.splunk.com/app/6730`, and a blue circular badge with the number '6'. Below the header, a message says 'Welcome to the new Splunkbase! To return to the old Splunkbase, [click here.](#)' The main content area features the 'Alert Manager Enterprise' app by Datapunctum AG. It includes a red icon with a white exclamation mark and a circular signal pattern, the app name, a brief description, and a 'Download' button. Below this, four screenshots of the app's user interface are displayed, showing various dashboards and alert management features. A search bar labeled 'Find an app' and a 'Submit an App' button are also visible at the top of the page.

Alert Manager Enterprise

7

What is Alert Manager Enterprise?

Datapunctum Alert Manager Enterprise (AME) helps IT Ops and Security teams manage their alerts within Splunk Enterprise and Splunk Cloud.

Add the Alert Manager Enterprise Alert Action to your existing searches and manage your alerts immediately.

-<https://docs.datapunctum.com/ame/>

The screenshot shows the Alert Manager Enterprise web interface. At the top, there's a navigation bar with links for Start, Reports, Administration, Documentation, and Search. The title "Alert Manager Enterprise" is displayed in the top right. Below the navigation is a dashboard with five colored boxes showing alert counts: 7 informational (blue), 0 low (green), 60 medium (yellow), 5 high (orange), and 20 critical (red). The main area is titled "Events" and displays a table of alerts. One alert is expanded to show details: "Outbound port scan from *10.0.2.85* with 528 ports" (Event-ID: 660ab0c5d7c512bda20d2346, First seen: 2024-04-01 12:59:53.000, Count: 1). The alert is categorized as "Informational" with priority "Informational". It has tags "reconnaissance", "T1046", and "T1595". Impact and urgency are both listed as "low". A note says "Multiple outbound connections to more than 10 different ports from the same 127.0.0.1 address. This is a possible sign of a portscan." Below the table, there's a section titled "Most recent results" with a table of notable fields:

Field	Value
Alert Time	2024-04-01 12:59:53.000
allowed	3
blocked	527
dest_ip	221.235.112.197 65.73.242.140 71.62.171.97 73.193.191.163
dest_ports	528
earliest_event	04/01/2024 12:00:20
latest_event	04/01/2024 12:59:53
src_ip	10.0.2.85

At the bottom of the interface, a footer bar shows the date range "2024-03-25 00:00:00.000 to 2024-04-01 17:01:32.000", the number of events "92 Events", and the last reload time "Last reload 2024-04-01 17:01:32.293".

7

Alert Manager Enterprise

8

- Useful for organizations handling many alerts.
- Streamlines identification and response to critical issues.
- Provides customizable notifications and access control.
- Helps prioritize and investigate potential threats.
- Enhances security and operational efficiency.
- Moves beyond basic email alerting.
- Integrated notification schemes for targeted communication.

Alert Manager Enterprise

9

The screenshot shows the Alert Manager Enterprise web application. At the top, there's a navigation bar with links like Dash, Apac, Wind, Add, Sear, Over, Alert, Splu, and Alert. Below the navigation is a dark header with the title "splunk>enterprise" and a "Documentation" tab selected. The main area has a dashboard with four colored boxes: blue (informational), green (low), yellow (medium), and orange (high). Each box contains a large zero and the corresponding priority level. Below the dashboard is a search bar with dropdowns for Time, Title, Tenant, Status, Priority, and Assignee. A message says "No events found." To the right of the search bar is a "Filters" modal window containing sections for Time (Last 7 days), Tenant (soc, ops, threathunting, default), Assignee (All), Priority (Informational, low, medium, high, critical), Tags, Status (All Open), Search, Saved Search, Submit button, and Refresh dropdown (Enabled, Disabled, 1 Minute).

The screenshot shows the "KPI Report - Event Status" dashboard. It features a "Status Transitions" chart at the top right, which is a flow diagram showing the progression of events from "created" (orange) through "new" (pink), "assigned" (blue), "in progress" (purple), "resolved" (green), and finally "closed" (light blue). Below the chart is a table titled "Status Changes". The table has columns for _time, event_key, total_duration, action, transition, transition_duration, search_name, assignee, and tnx. The table lists several rows of event data, each with a timestamp, event key, duration, and state transitions. At the bottom of the table, a note says: "The Status Changes table shows the total time from creation to the last state. The transition and transition_duration columns show the status transition durations." There are also navigation buttons for Prev, Next, and page numbers 1-5.

[Departures Board Visualization]

10

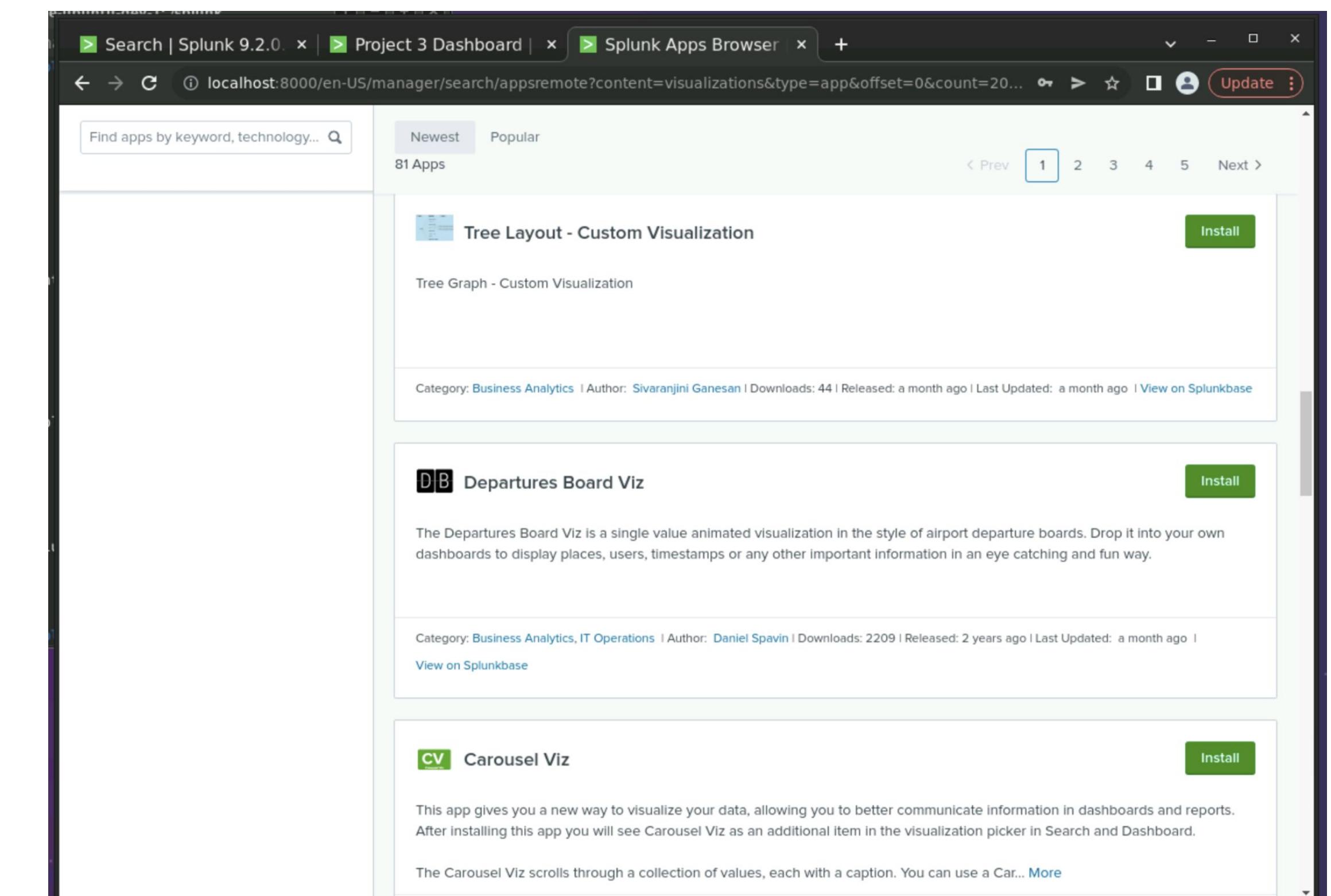
The screenshot shows the Splunk Enterprise web interface. At the top, the navigation bar includes 'splunk>enterprise' (highlighted in green), 'Apps ▾', 'Administrator ▾' (with a warning icon), 'Messages ▾', 'Settings ▾', 'Activity ▾', 'Help ▾', and a search bar with 'Find' and 'DEPARTURES BOARD' buttons. Below the bar, the main content area displays the 'About' page for the 'Departures Board Visualization' app. The page includes the app's name, version (1.3.0), creator (Daniel Spavin, daniel@spavin.net), and a large graphic of a flip-dot display board showing the text 'P 5 9 J H A 8 N K J'. The page also lists 'Version Support' (8.2, 8.1, 8.0, 7.3, 7.2, 7.1, 7.0), 'Who Is this app for?' (described as for anyone wanting a single-value panel display), 'How does the app work?' (described as providing a visualization for both text and numerical search results), and 'Use cases for the Departures Board Visualization:' (localhost:8000/en-US, server names, locations, or user names). A footer bar at the bottom contains the URL 'localhost:8000/en-US'.

[Departures Board Visualization]

11

“The Departures Board Viz is a single value animated visualization in the style of airport departure boards. Drop it into your own dashboards to display places, users, timestamps or any other important information in an eye catching and fun way.”

-<https://splunkbase.splunk.com/app/4292>



[Departures Board Visualization]

12

INT. CLASSROOM - NIGHT

A COMPUTER MONITOR sits on a 1950s school desk. The camera pushes in close to the screen, which is playing a video of an old BLACK AND WHITE TELEVISION COMMERCIAL....

MATT

Hello, friends. I'm your Departures Board Visualization guy.
Are you tracking timestamps, user data, and info?

Do you get tired of terminal? Are you untechnical?

The answer to all your problems is in this little add-on:
Departures Board Visualization.

Yes, Departures Board Visualization displays places,
users, timestamps, and any other important information.

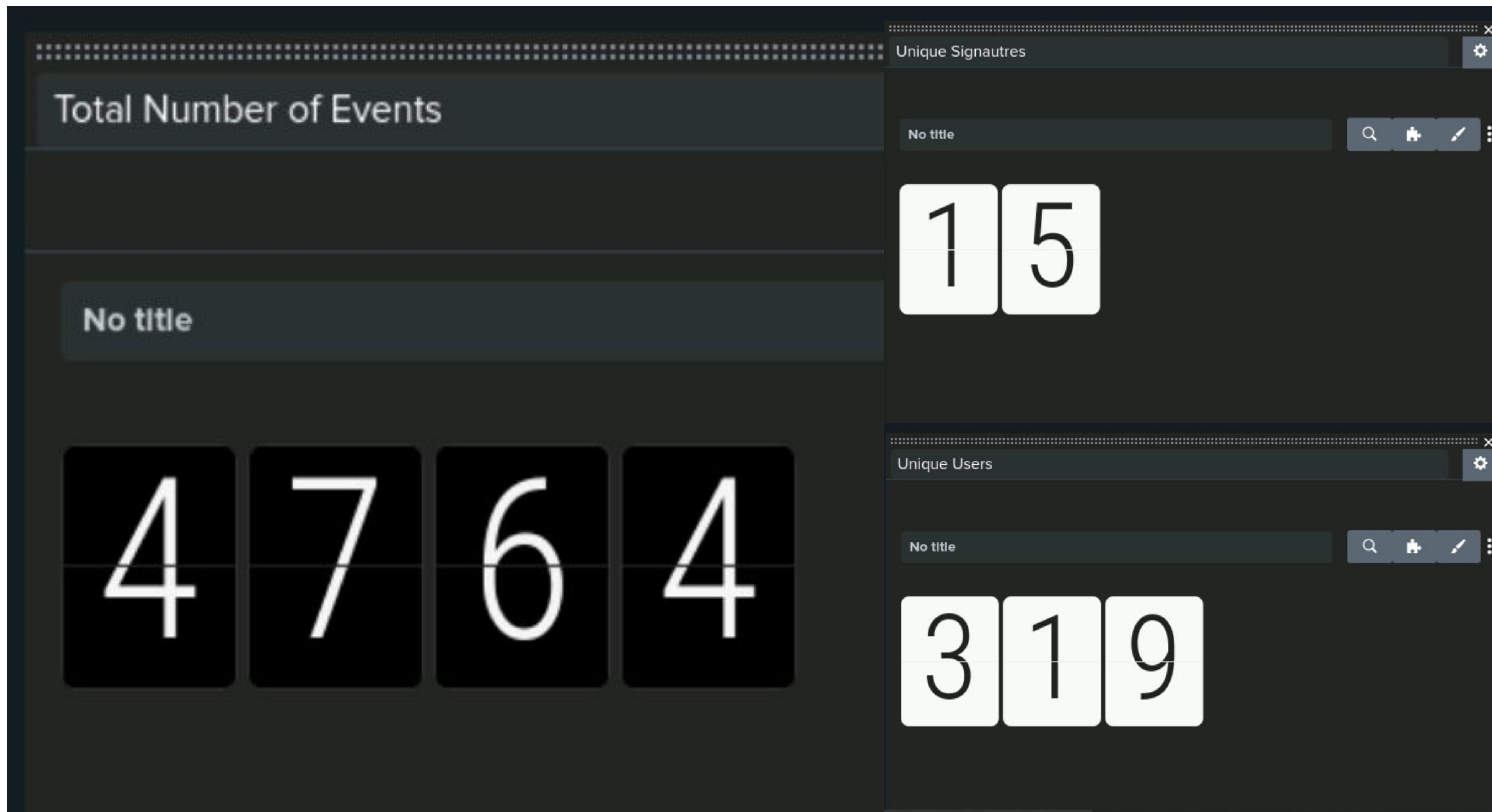
Yes, with Departures Board Visualization, you can code your
way to visualizing. All you do is link a big Splunk report
after every data add.

It's so easy, too. It's just like taking candy from a baby!

So, why don't you join the thousands of happy, peppy people,
and download a great big add-on of
Departures Board Visualization tomorrow.
That's Departures Board Visualization.

[Departures Board Visualization]

13



Logs Analyzed

14

1

Windows Logs

The windows logs primarily contain windows security events. Data is provided on existing user accounts, created accounts, deleted accounts, login attempts and successes and so on. The logs also provide potential security compromise data as well as event timings.

2

Apache Logs

HTTP Response Headers, HTTP Request Methods, Referring Domains, HTTP Status Codes, Geographical Location of IP Addresses, Times events occurred.

Windows Logs

Reports—Windows

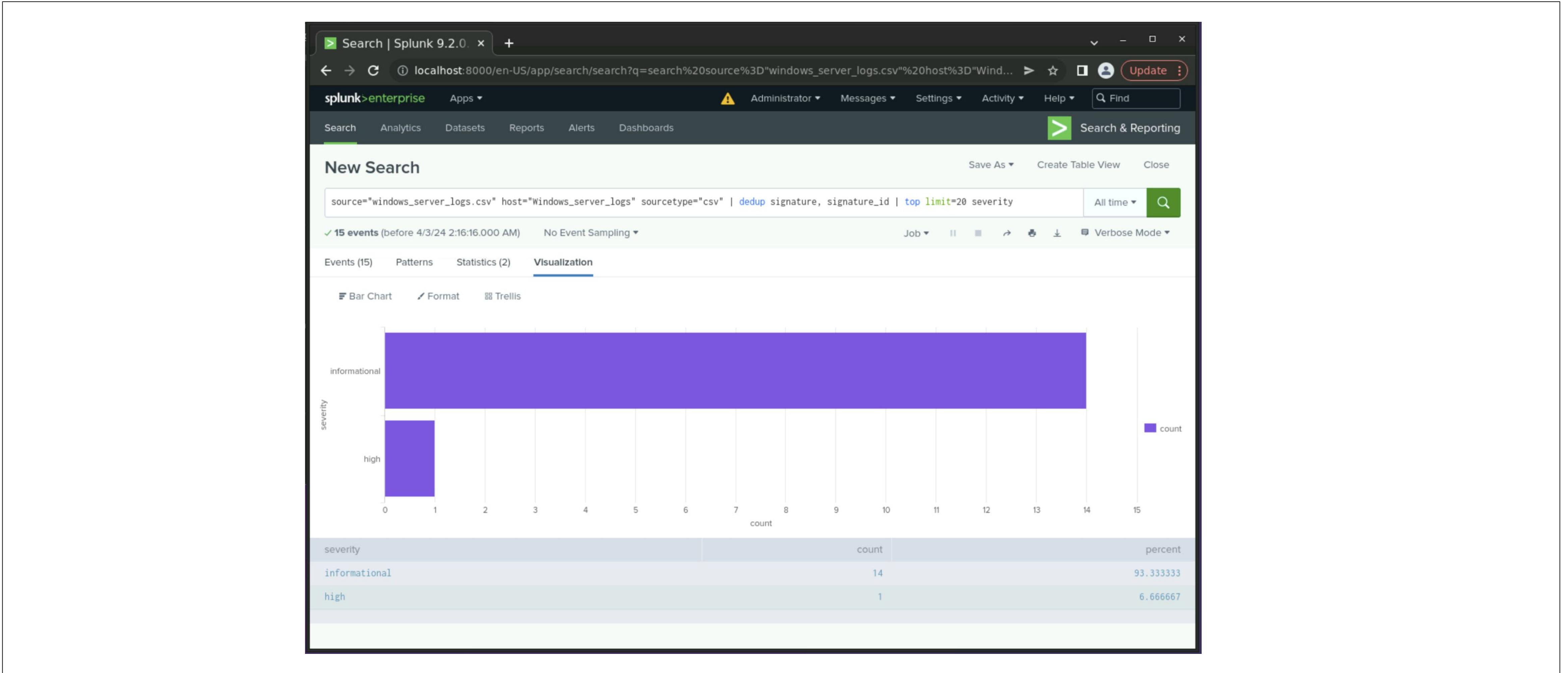
Designed the following reports:

16

Report Name	Report Description
Security Levels (Count & Percentage) REPORT	Bar chart showing various security events throughout a span of time by severity.
Signature & Signature ID REPORT	Bar chart that shows the counts and percentages of various system events as labelled by their Signature_ID.
Signature & Signature ID Stats REPORT	Statistics showing what system events the Signature_ID's are tied to.
Success and Failure of Signature REPORT	Statistics showing the counts and percentages of various system events based whether they successfully or unsuccessfully executed.
Total Number of Events REPORT	The total number of events throughout the given report.
Unique Signatures REPORT	The amount of overall unique signatures throughout the report.
Unique Users REPORT	The amount of unique user accounts recorded throughout the report.
Users Over Time REPORT	A Linechart representing user logins over the span of an hour.

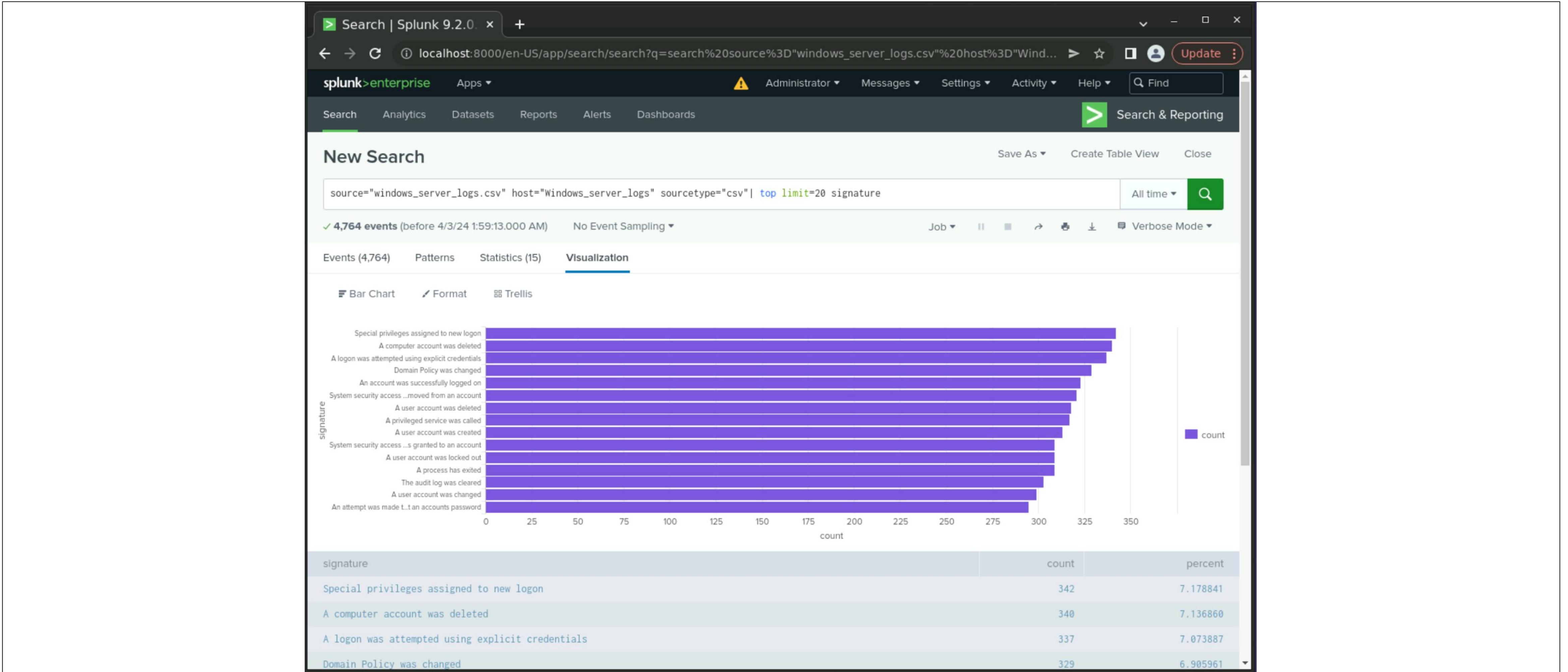
Images of Reports—Windows

17



Images of Reports—Windows

18



Images of Reports—Windows

19

The screenshot shows the Splunk 9.2.0.1 search interface. The search bar contains the query: `source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | dedup signature, signature_id | table signature, signature_id`. The results show 15 events from before April 3, 2024, at 2:08:30.000 AM. The Statistics tab is selected, displaying a table of log entries:

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

Images of Reports—Windows

20

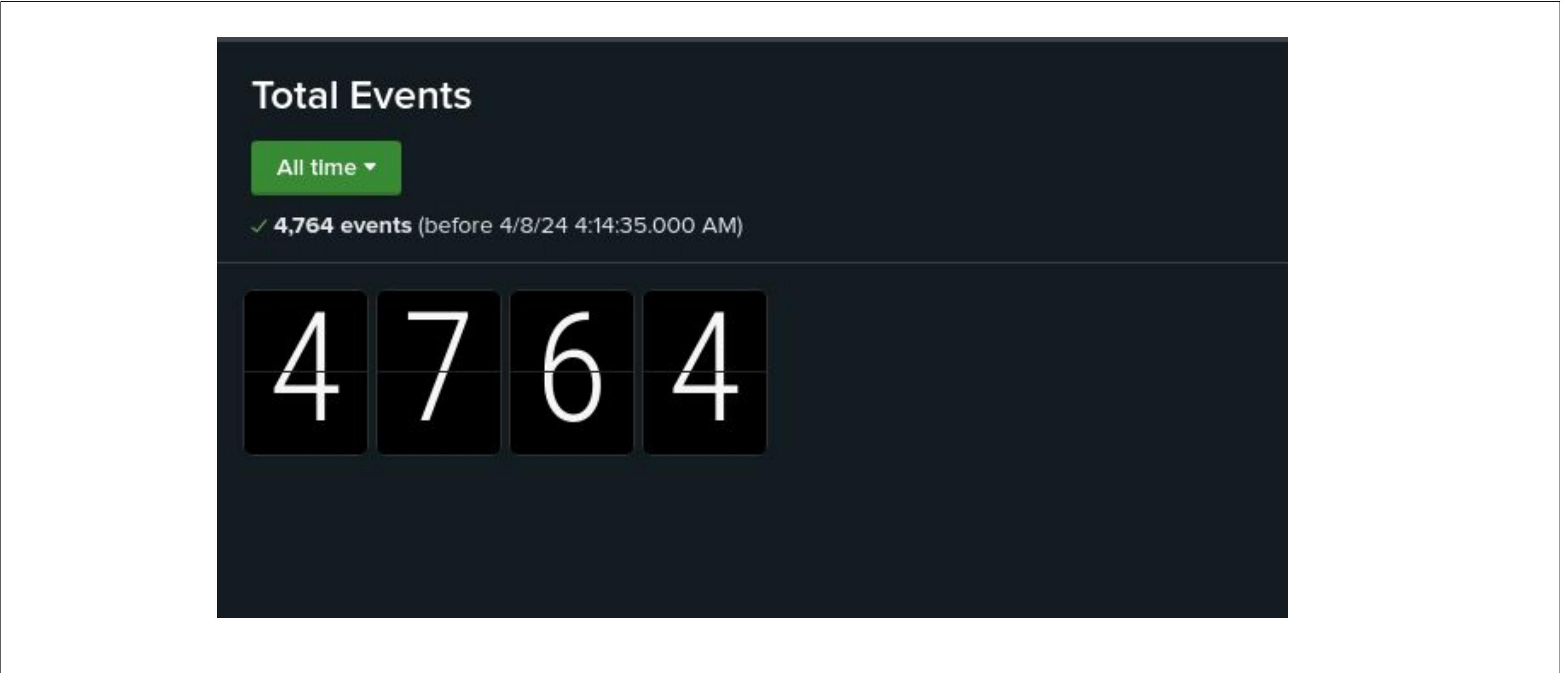
The screenshot shows the Splunk 9.2.0 web interface. The top navigation bar includes a search bar ('Search | Splunk 9.2.0.'), a URL bar ('localhost:8000/en-US/app/search/search?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FSOC...'), and a header with 'splunk>enterprise', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' button. Below the header is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports' (which is selected), 'Alerts', and 'Dashboards'. A green 'Search & Reporting' button is also present.

The main content area is titled 'SOC_Report_Windows_Signatures'. It displays a search command in the search bar: `source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | top limit=20 status`. The results show 4,764 events from before April 3, 2024, at 2:24:54.000 AM. The 'Statistics (2)' tab is selected, showing a table with two rows:

status	count	percent
success	4622	97.019312
failure	142	2.980688

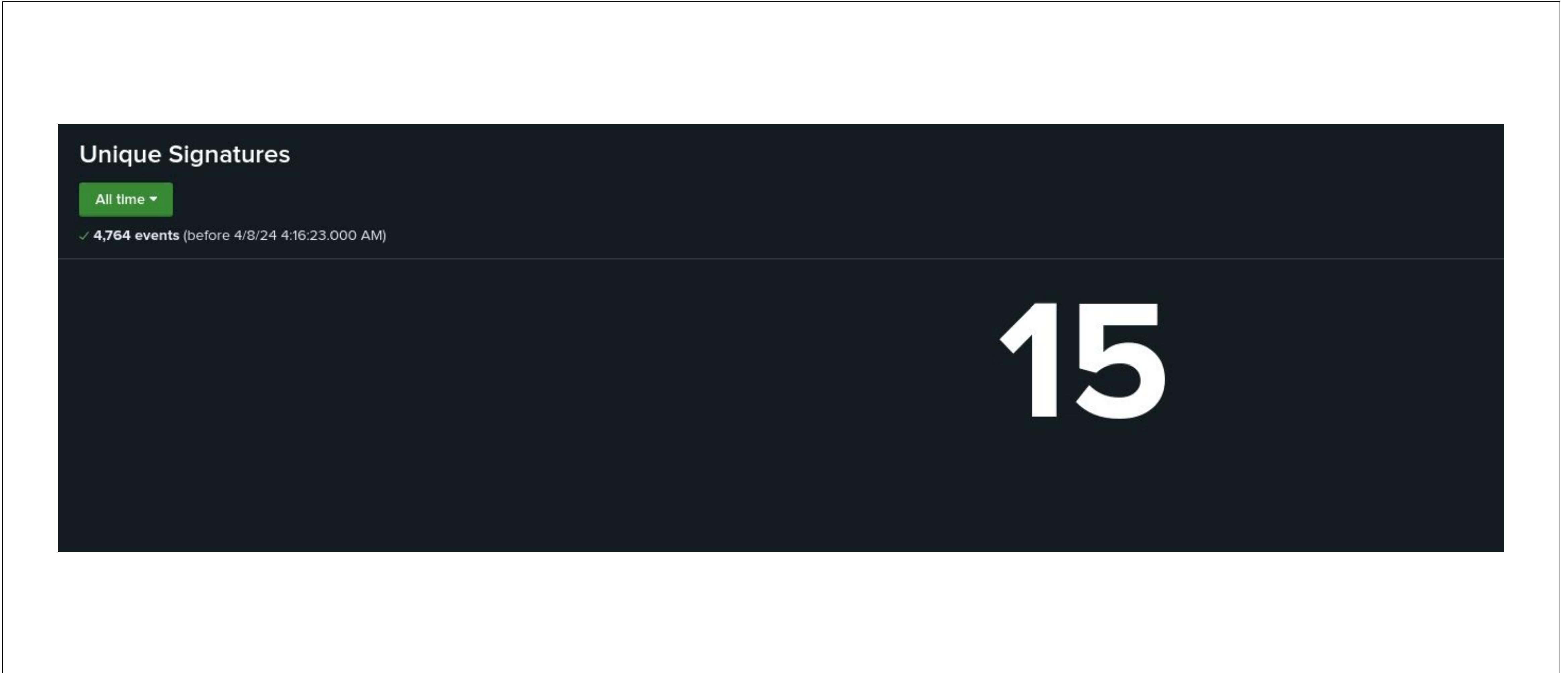
Images of Reports—Windows

21



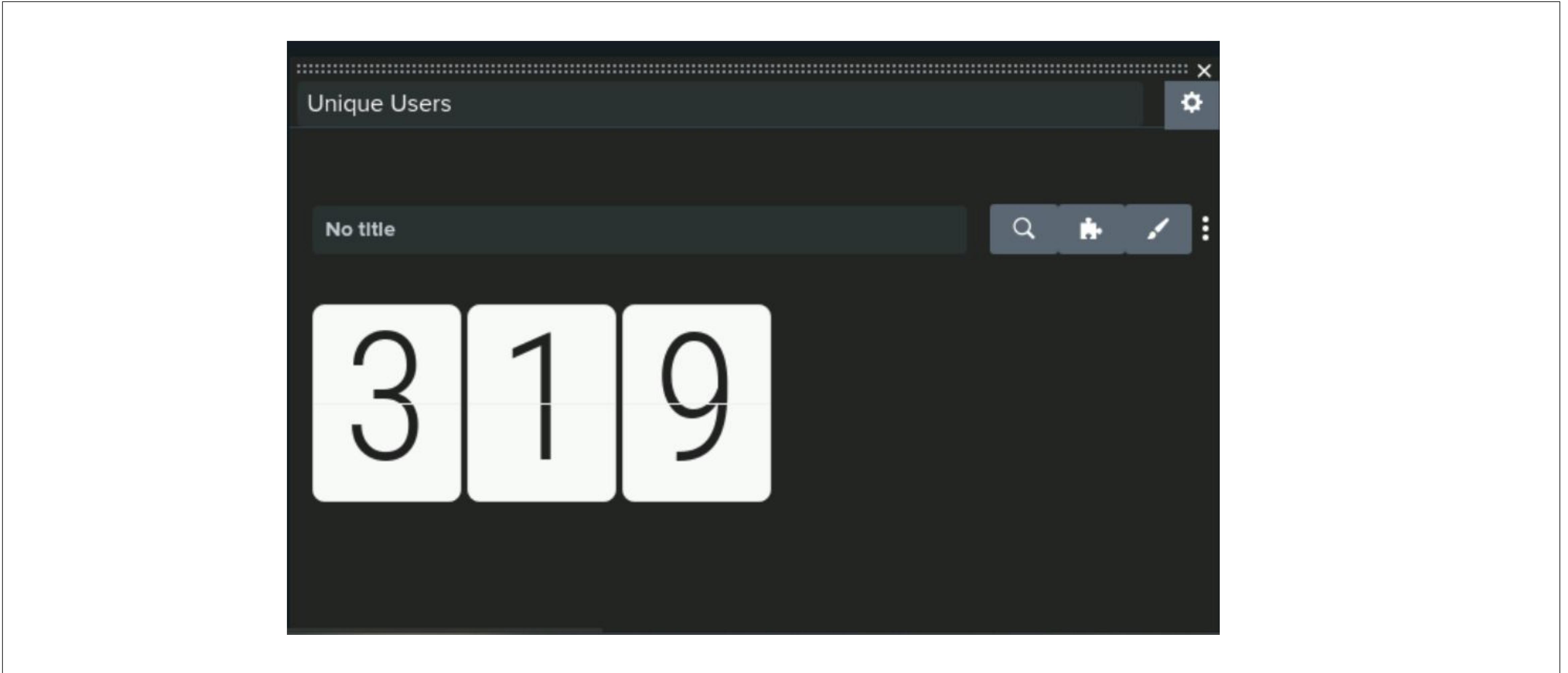
Images of Reports—Windows

22



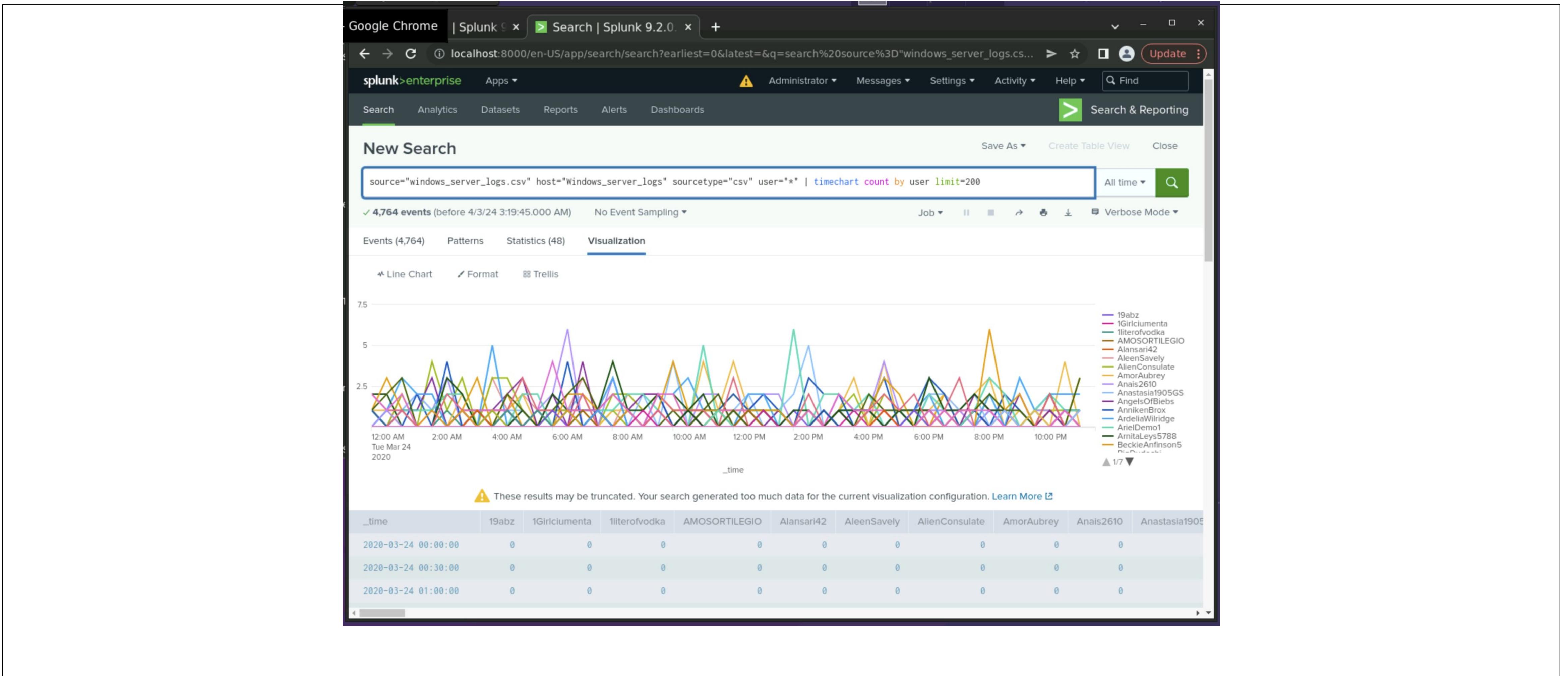
Images of Reports—Windows

23



Images of Reports—Windows

24

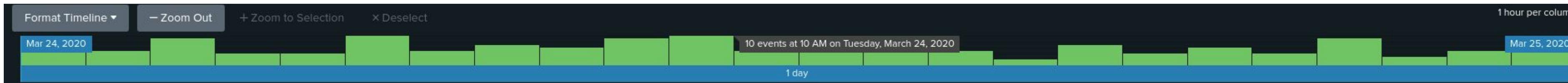


Alerts—Windows

25

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Failure Rate of Windows Activity	[Send e-mail to: SOC@VSI-company.com]	[10]	[>15 in 60 minutes]



High Failure rate of windows activity

Enabled: Yes. [Disable](#)
App: search
Permissions: Private. Owned by admin. [Edit](#)
Modified: Apr 3, 2024 2:46:36 AM
Alert Type: Real-time. [Edit](#)

Trigger Condition: .. Number of Results is > 15 in 60 minutes. [Edit](#)
Actions: Action [Edit](#)
 Send email

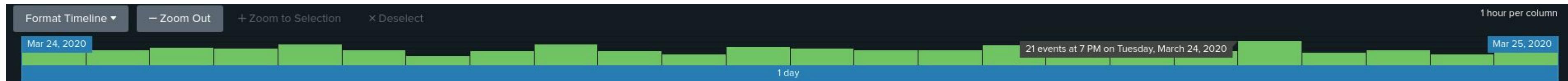
JUSTIFICATION: [Highest number hit was 10 over 24 hours.]

Alerts—Windows

26

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Number of Account Logins	[Send e-mail to: SOC@VSI-company.com]	[21]	[>30 in 60 minutes]



High number of account log ins

a higher number of account log ons has occurred (>30)

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Apr 3, 2024 3:00:01 AM

Alert Type: Real-time. [Edit](#)

Trigger Condition: ... Number of Results is > 30 in 60 minutes. [Edit](#)

Actions: [1 Action](#) [Edit](#)

Send email

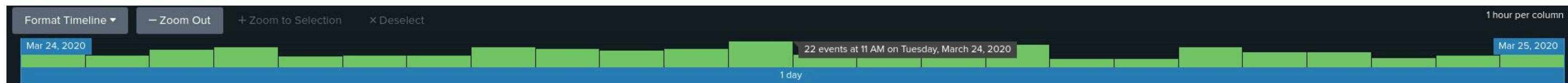
JUSTIFICATION: [Highest number of log in an hour was 21 over 24 hours.]

Alerts—Windows

27

Designed the following alerts:

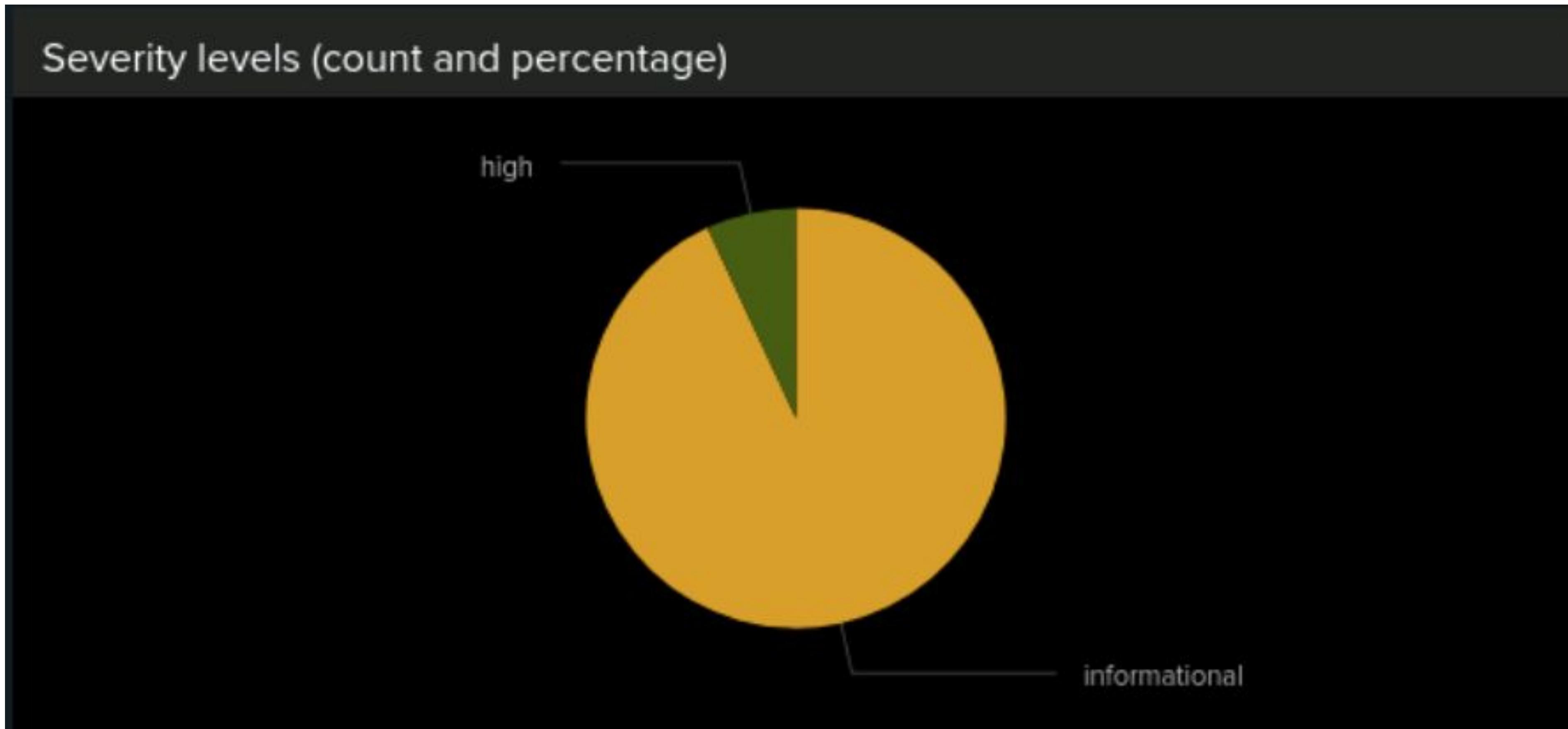
Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Amount of User Accounts Deleted	[Send e-mail to: SOC@VSI-company.com]	[22]	[>30 in 60 minutes]



JUSTIFICATION: [Highest number of deleted users signatures did not surpass 22/hour in 24 hours.]

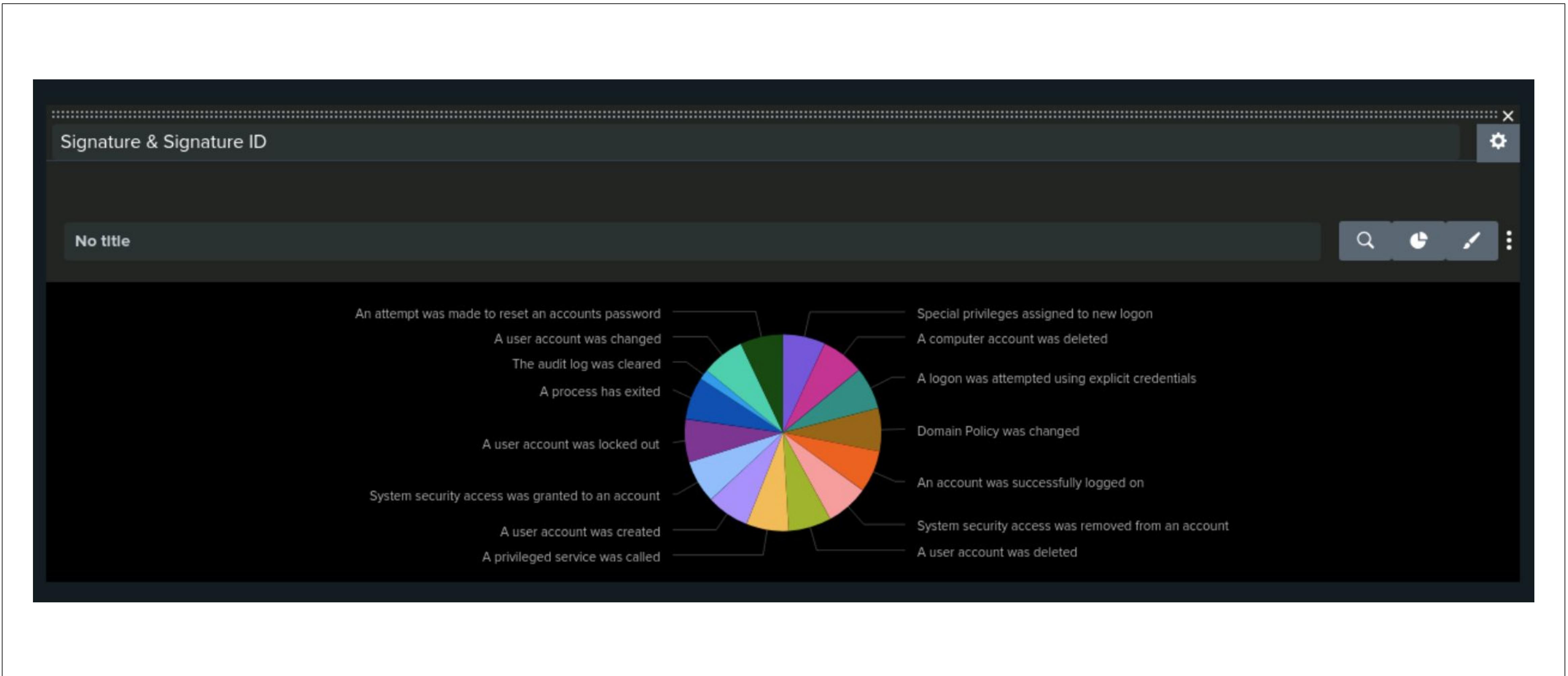
Dashboards—Windows

28



Dashboards—Windows

29



Dashboards—Windows

30

signature	signature_id	count	percent
Special privileges assigned to new logon	4672	342	7.178841
A computer account was deleted	4743	340	7.136860
A logon was attempted using explicit credentials	4648	337	7.073887
Domain Policy was changed	4739	329	6.905961
An account was successfully logged on	4624	323	6.780017
System security access was removed from an account	4718	321	6.738035
A user account was deleted	4726	318	6.675063
A privileged service was called	4673	317	6.654072
A user account was created	4720	313	6.570109
System security access was granted to an account	4717	309	6.486146

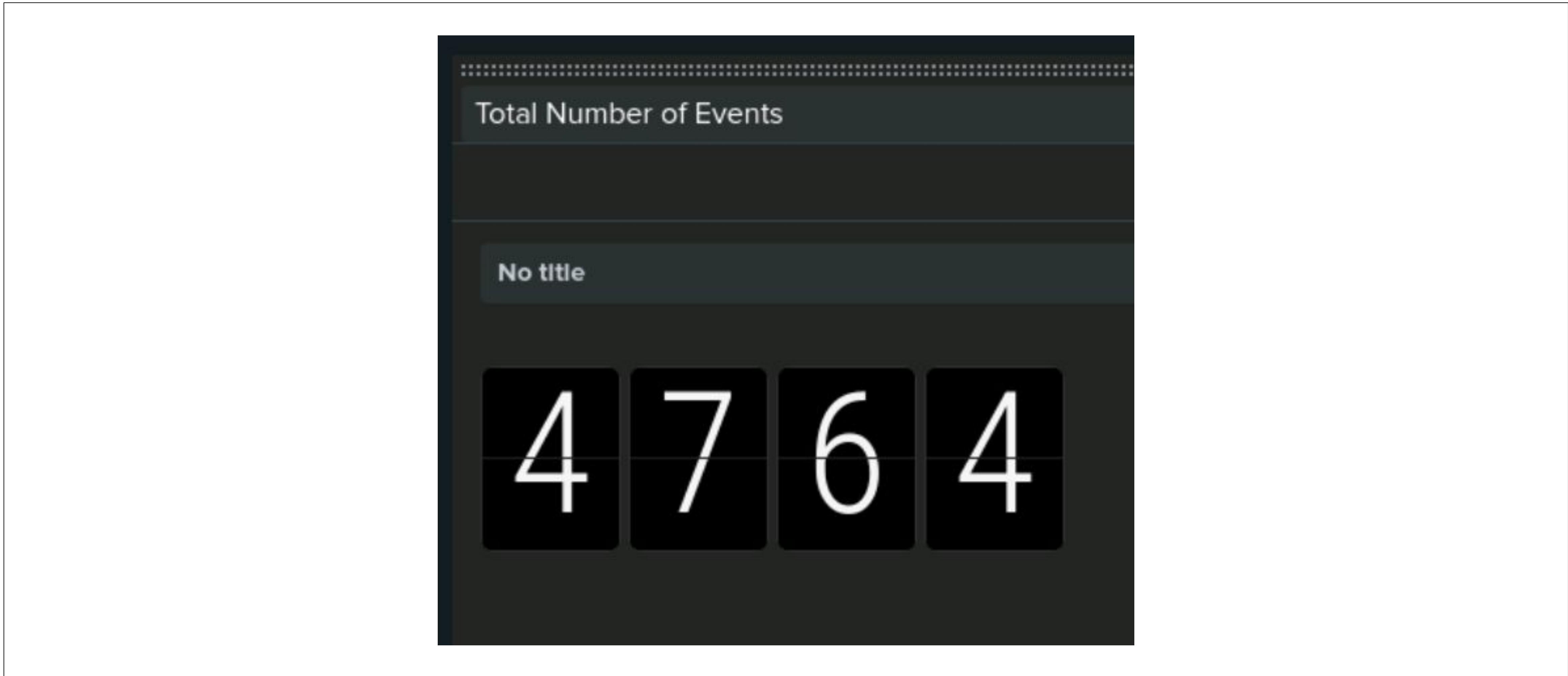
Dashboards—Windows

31



Dashboards—Windows

32



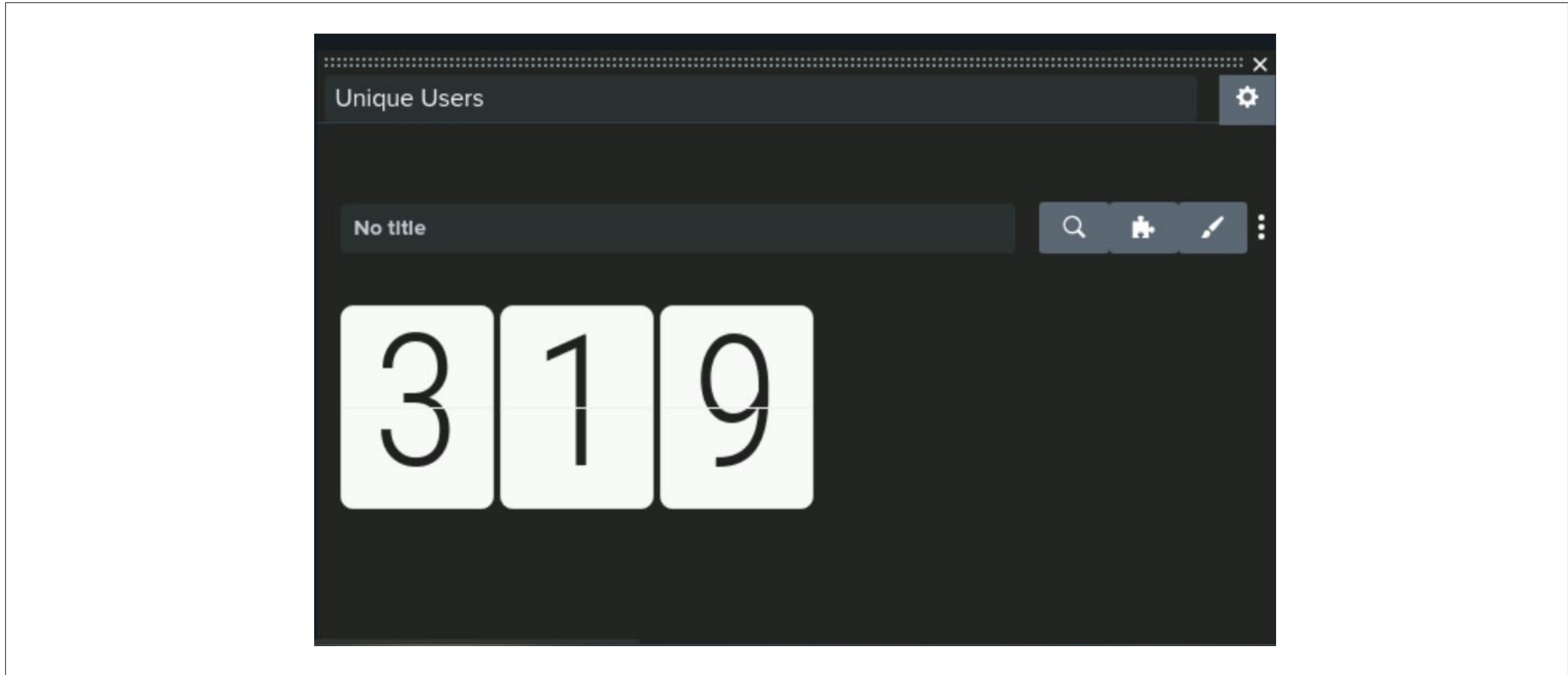
Dashboards—Windows

33



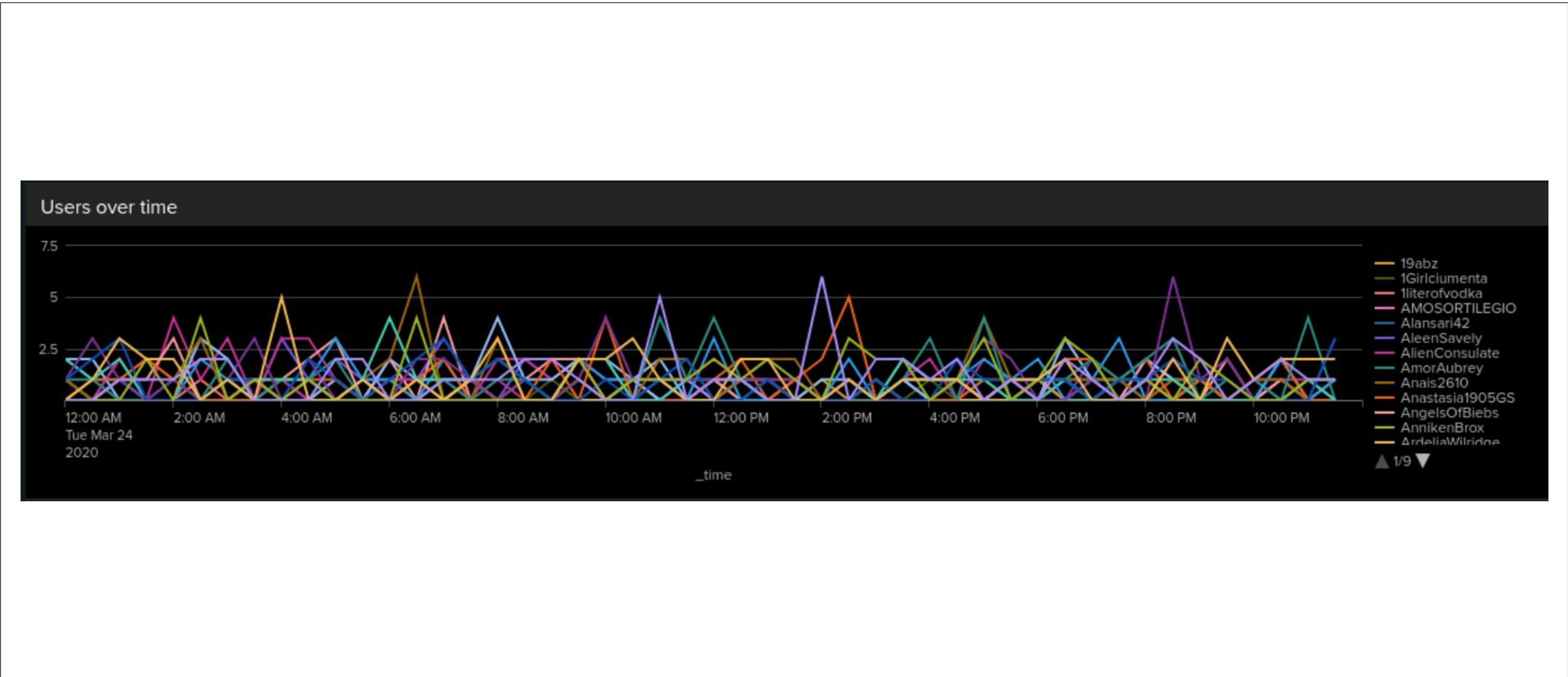
Dashboards—Windows

34



Dashboards—Windows

35



Apache Logs



Reports—Apache

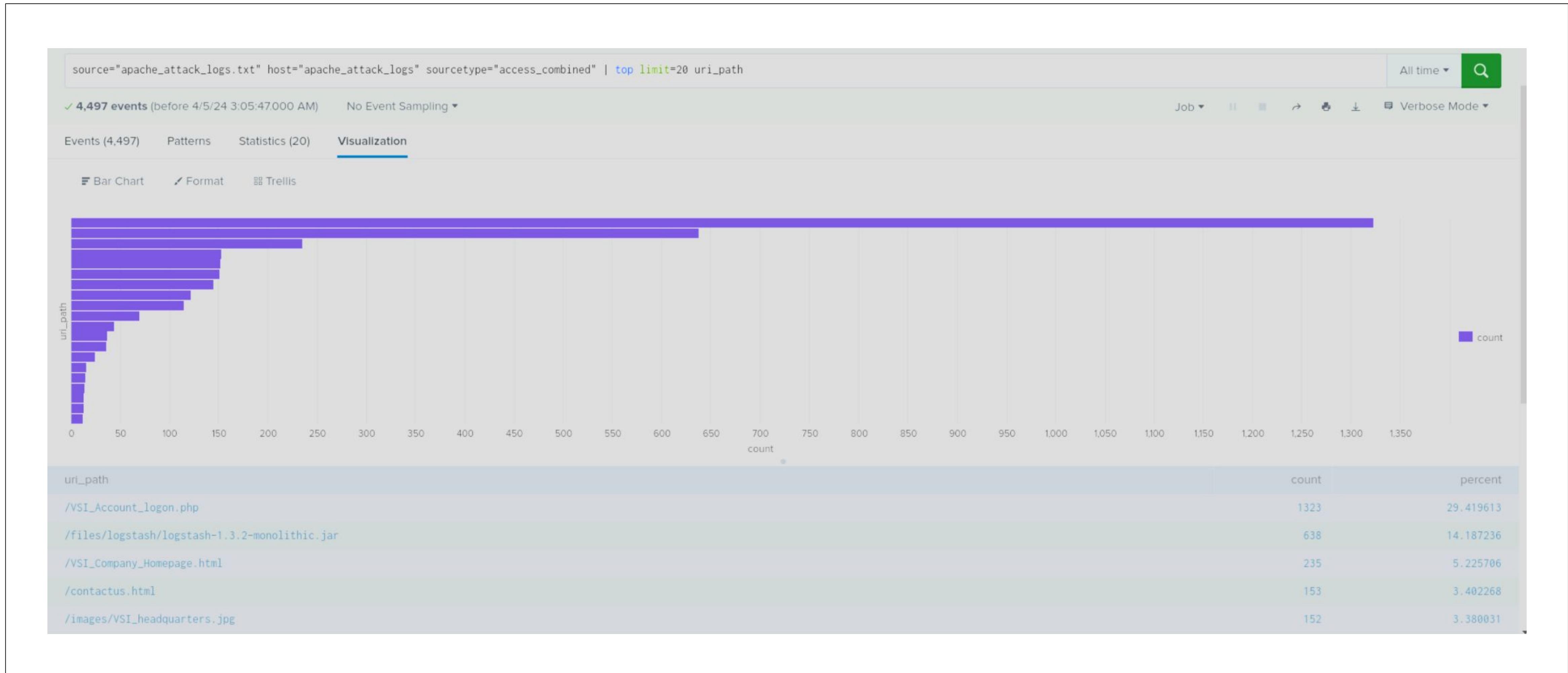
37

Designed the following reports:

Report Name	Report Description
Unique URI REPORT	Bar Chart showing the count and percentage of each URI visitations.
Top 10 Countries REPORT	Bar Chart showing the top 10 countries with the highest login counts to the server.
IP By Location REPORT	A map visualization which illustrates the geographical sources of the IP logins.
HTTP Methods Over One Hour REPORT	Column Chart showing the most commonly used HTTP Methods over the span of an hour.
HTTP Response Code REPORT	BarChart illustrating the most common response code response for various HTTP methods.
HTTP Methods Pie Chart REPORT	A Pie chart illustrating the most common HTTP Methods.
Top Ten Referrer By Domain REPORT	Barchart that shows the 10 referrer domains.
Unique Referrers REPORT	Departures Board Visualization of the unique Referrers.

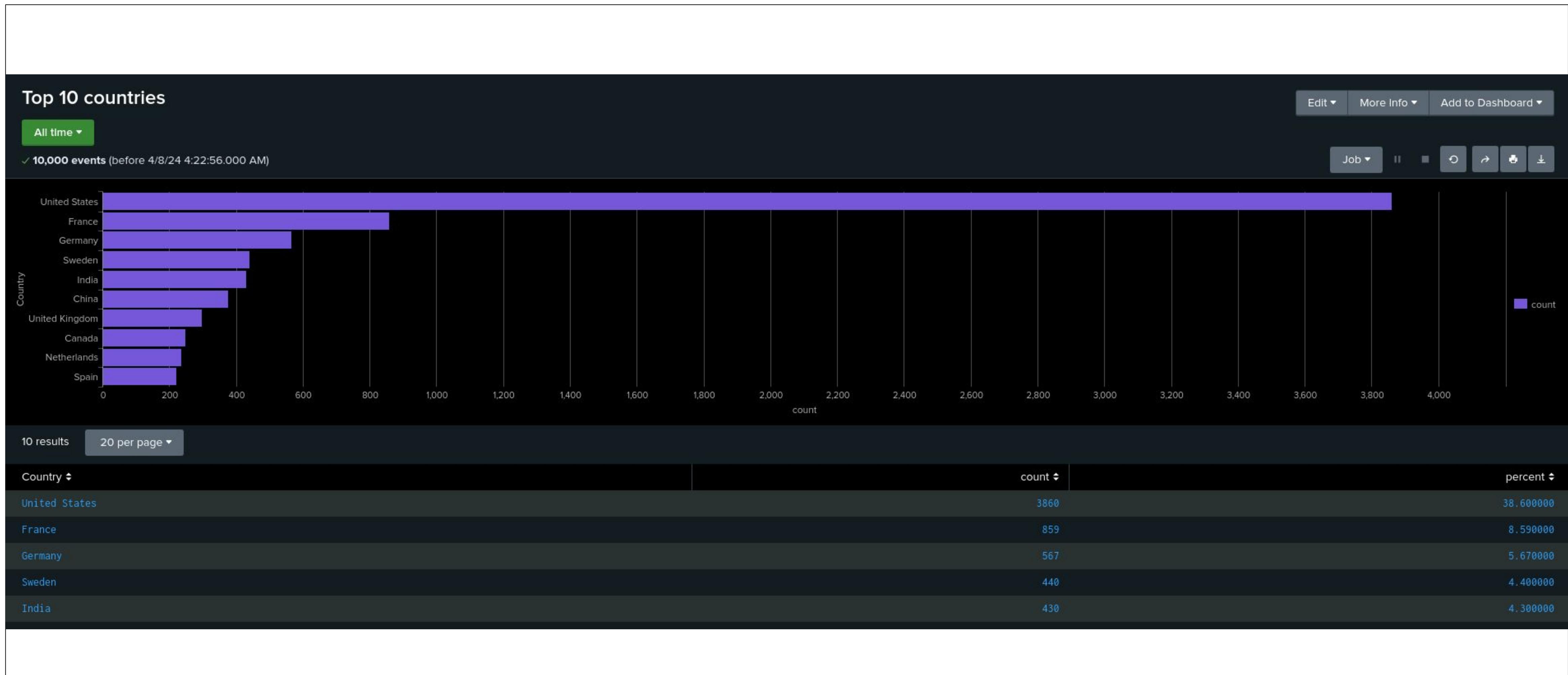
Images of Reports—Apache

38



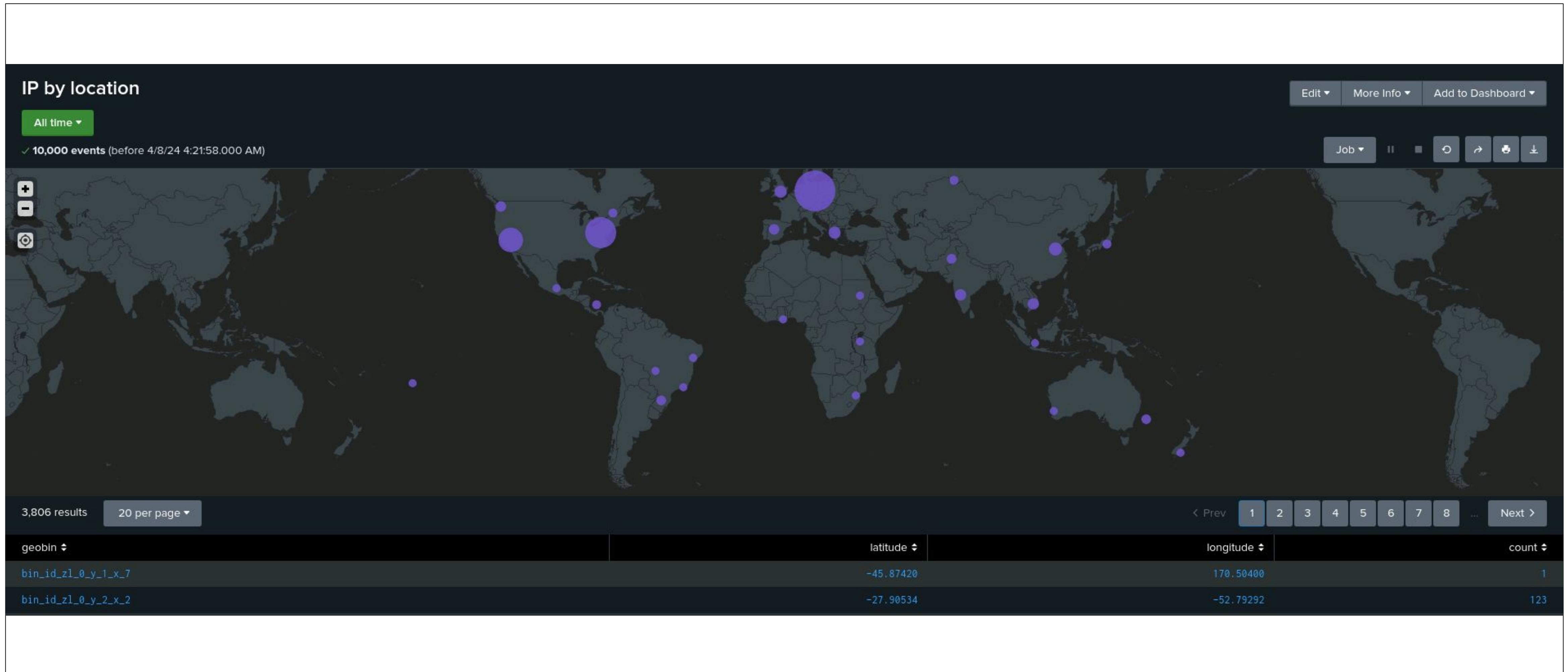
Images of Reports—Apache

39



Images of Reports—Apache

40



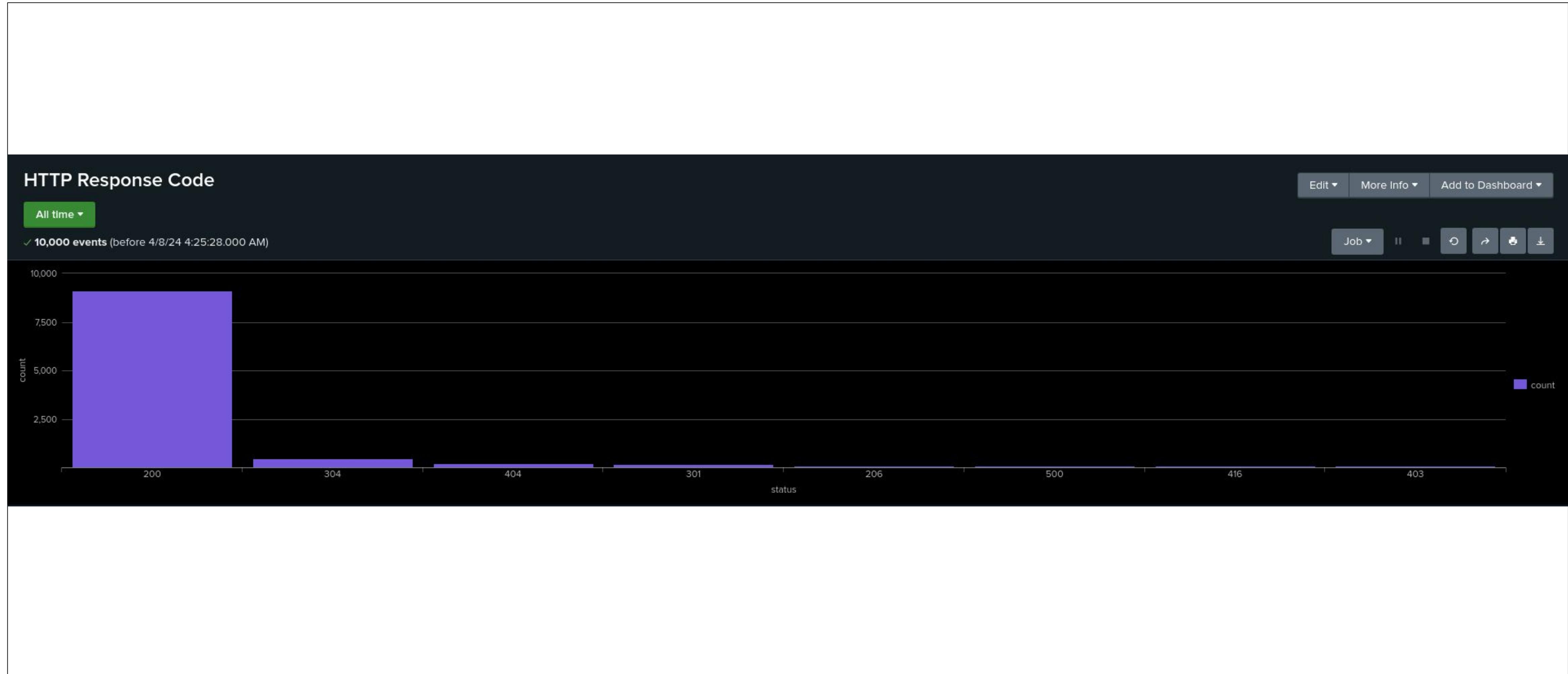
Images of Reports—Apache

41



Images of Reports—Apache

42



Images of Reports—Apache

43



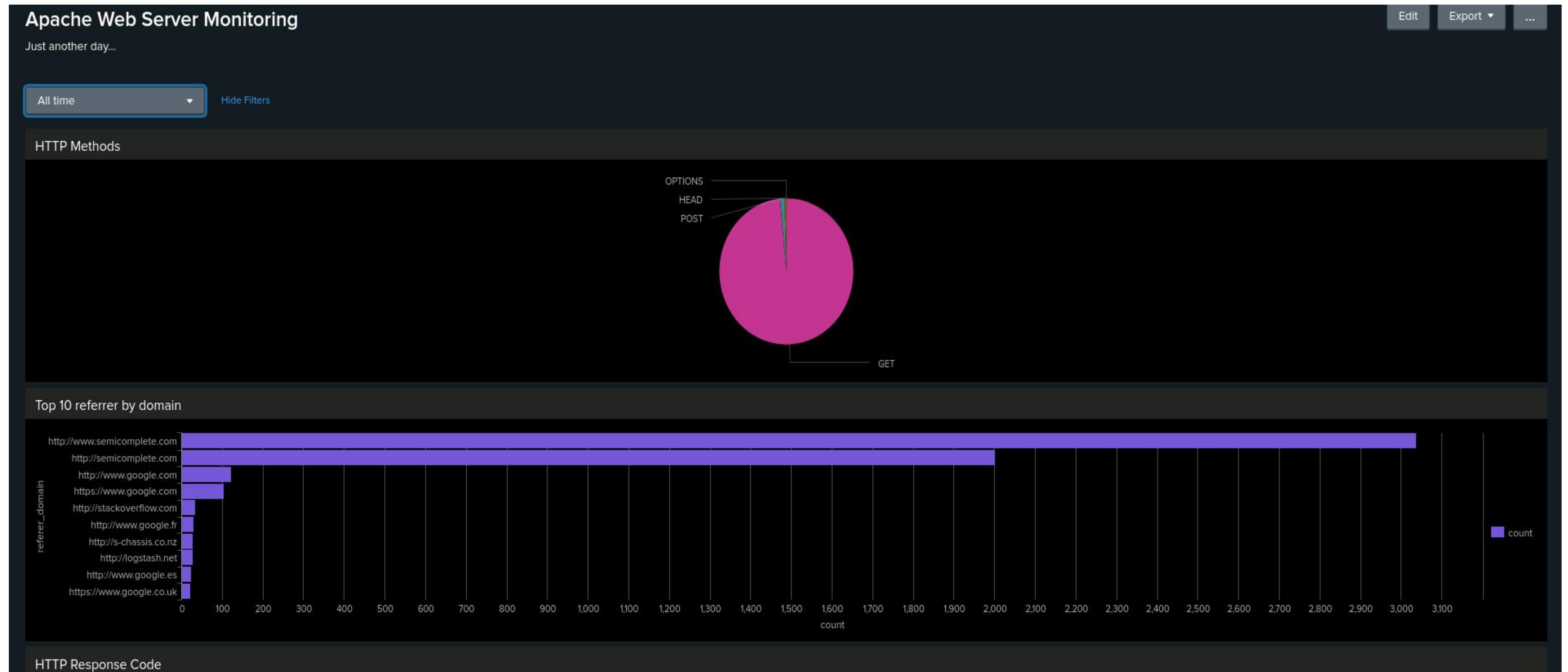
Images of Reports—Apache

44



Dashboards—Apache

45



Images of Reports—Apache

46

The screenshot shows a search interface with the following elements:

- Section Title:** Unique Referrers
- Time Filter:** All time ▾
- Event Count:** ✓ 10,000 events (before 4/8/24 4:26:12.000 AM)
- Result Count:** 1 result
- Items per Page:** 20 per page ▾
- Sort Column:** dc(referer) ▾
- Result Row:** 628

Alerts—Apache

47

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[Hourly POST Requests]	[Send e-mail to: SOC@VSI-company.com]	[~7]	[>12]



Hourly POST requests threshold exceeded

the threshold for post requests has been exceeded (>12/hour)

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Apr 3, 2024 5:13:40 AM

Alert Type: Scheduled. Weekly, Monday at 6:00. [Edit](#)

Trigger Condition: .. Number of Results is > 12. [Edit](#)

Actions: 1 Action [Edit](#)

Send email

JUSTIFICATION: [Highest number of POST requests was 7/hour over 24 hours.]

Alerts—Apache

48

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[Hourly Traffic From Outside US]	[Send e-mail to: SOC@VSI-company.com]	[120]	[>200 in 60 min.]



Hourly Traffic from Outside US Exceeding Threshold

the traffic from outside the US has exceeded the alert threshold (>200/hour)

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Apr 3, 2024 5:09:17 AM

Alert Type: Real-time. [Edit](#)

Trigger Condition: .. Number of Results is > 200 in 60 minutes. [Edit](#)

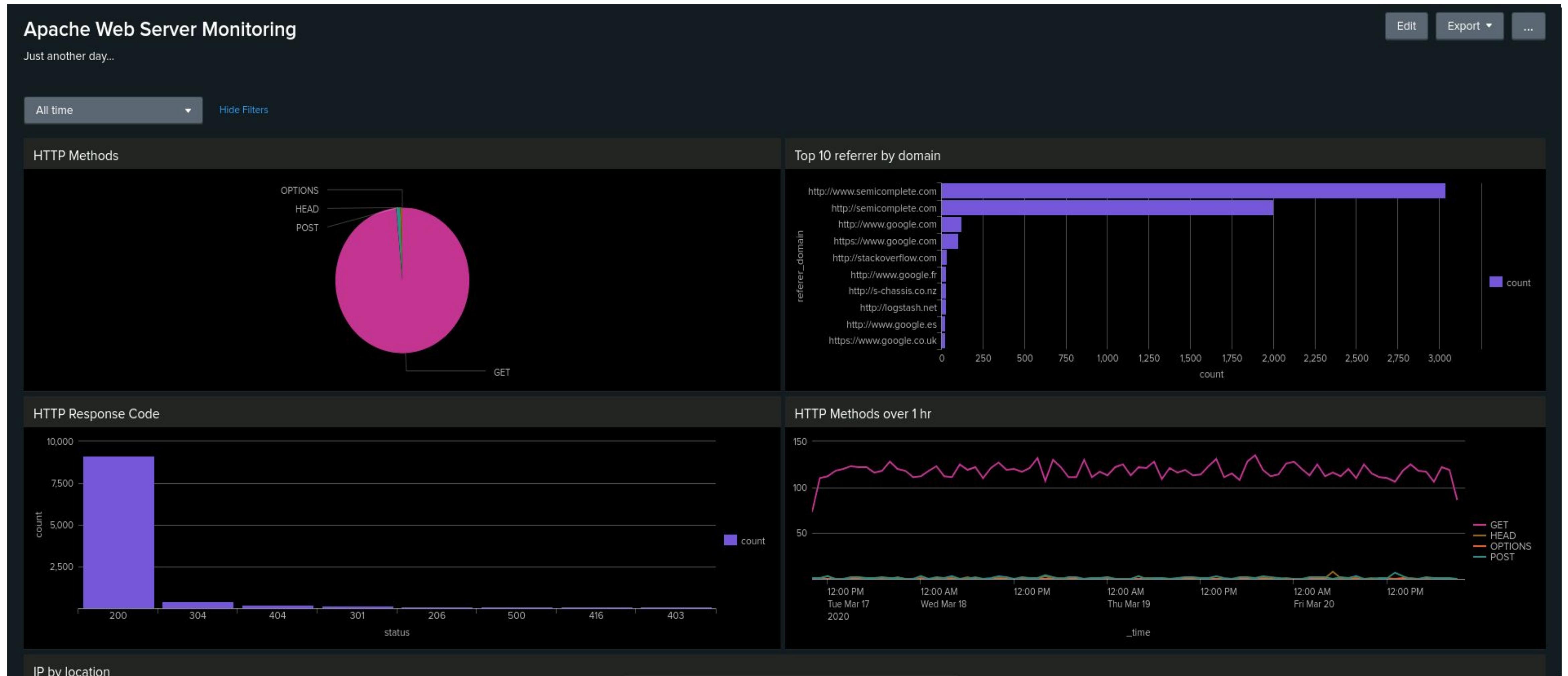
Actions: [1 Action](#) [Edit](#)

Send email

JUSTIFICATION: [Traffic from outside the US peaked at 120/hour over 24 hours.]

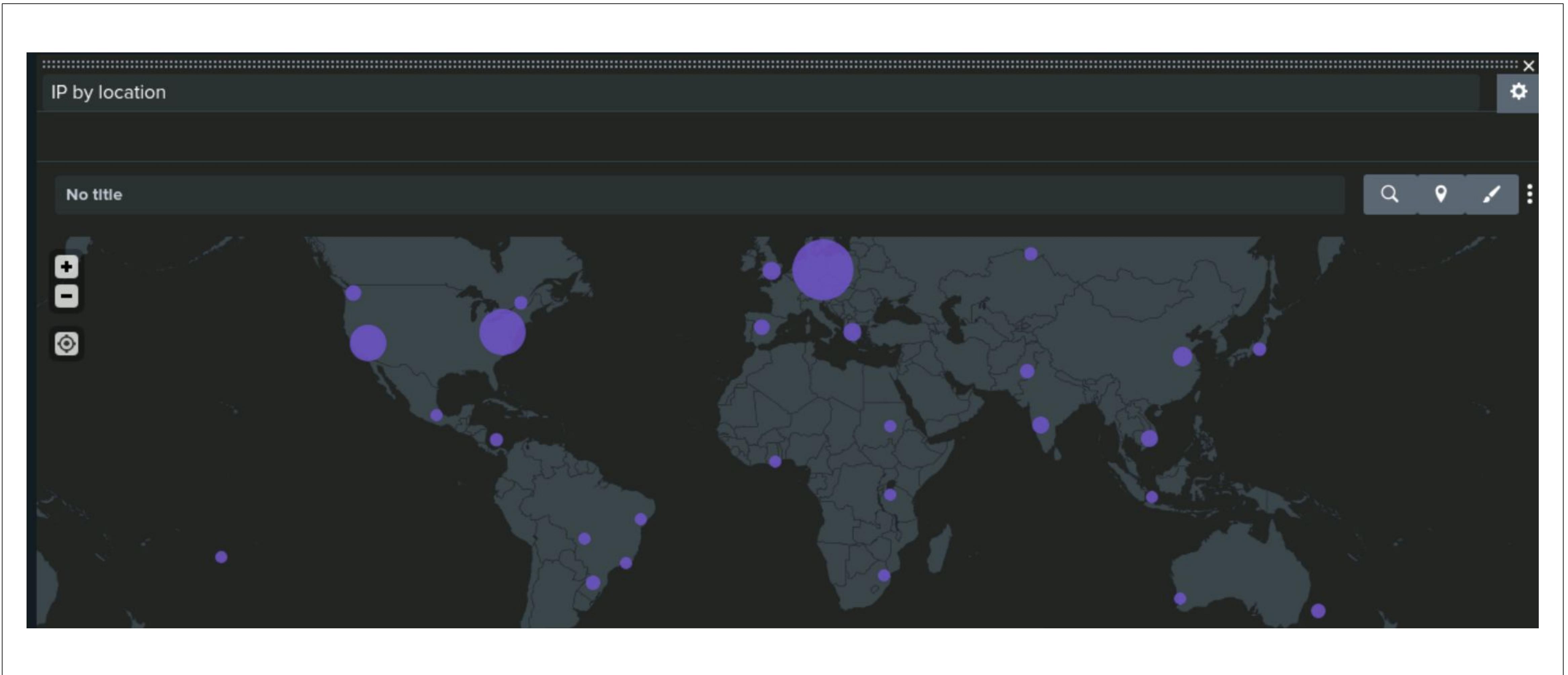
Dashboards—Apache

49



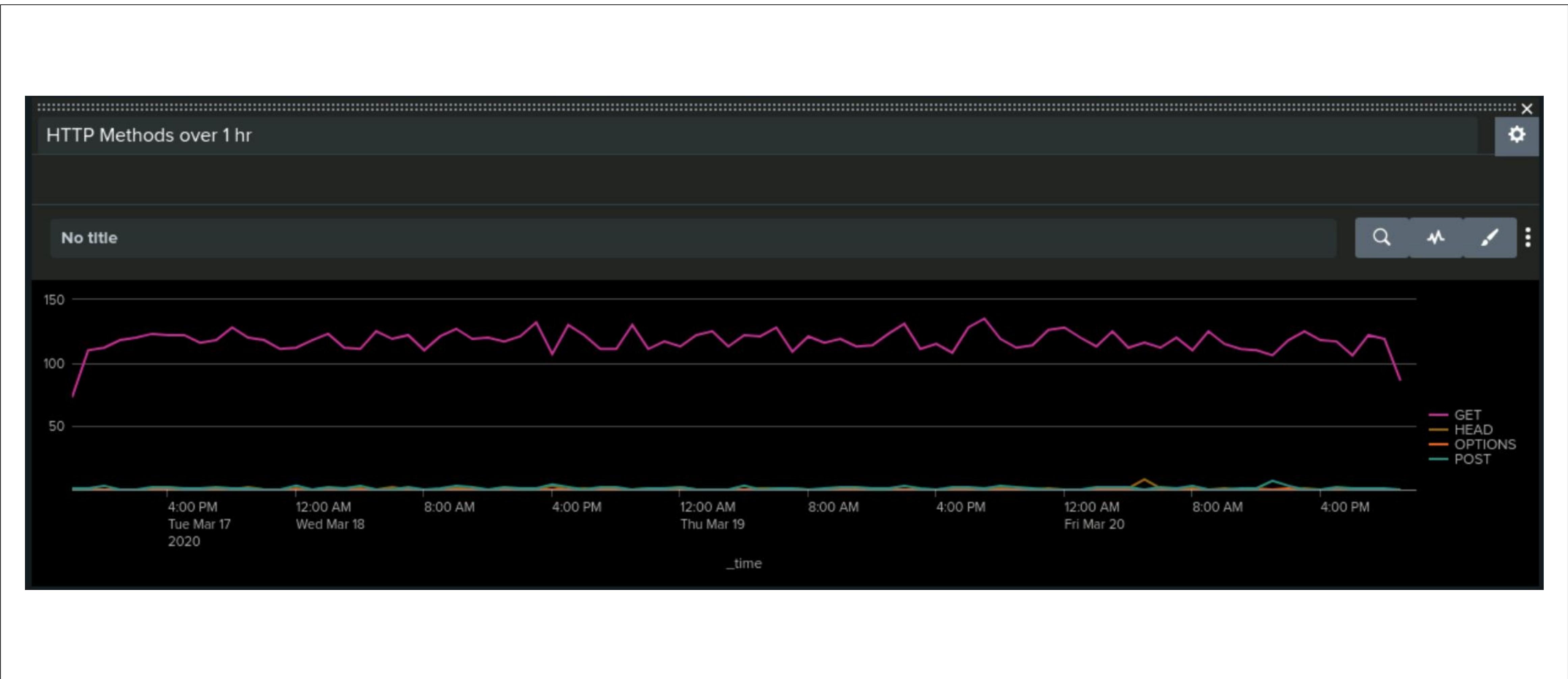
Dashboards—Apache

50



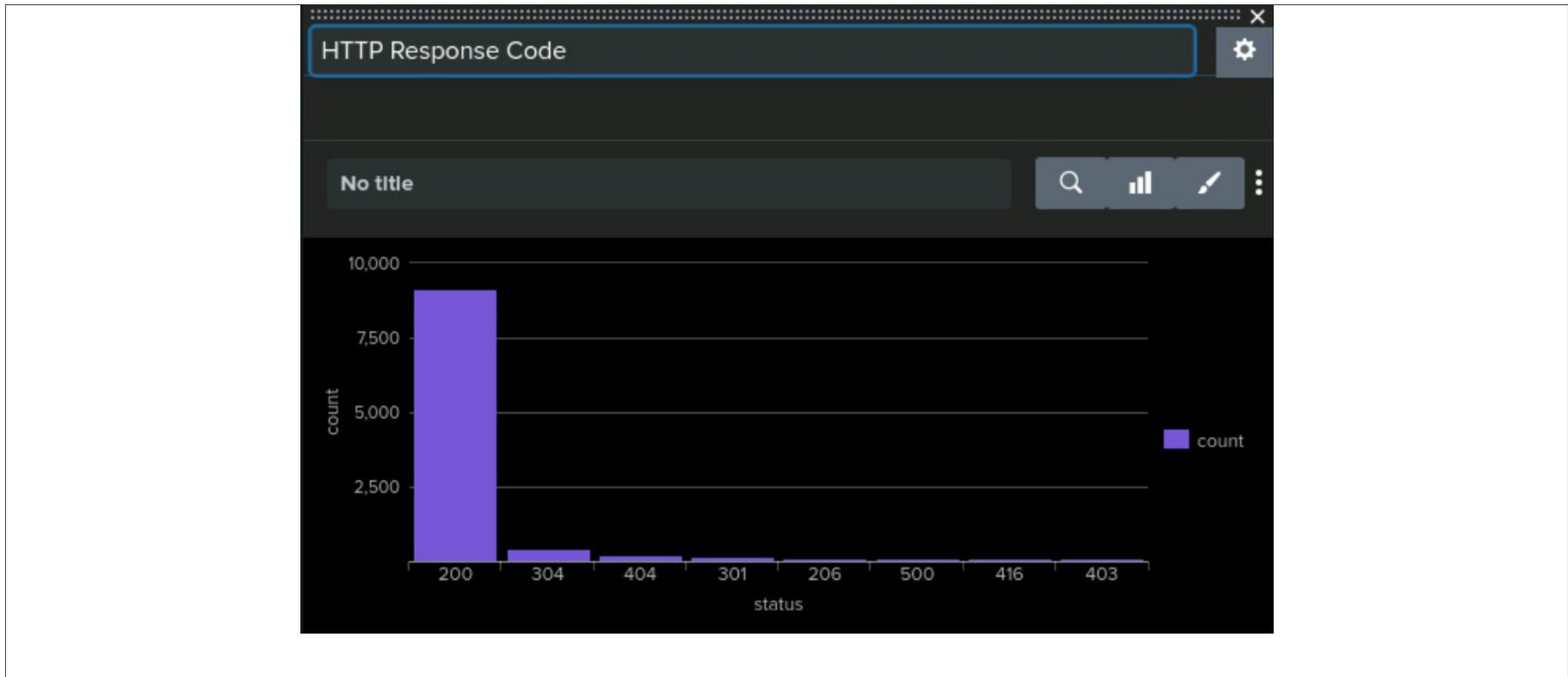
Dashboards—Apache

51



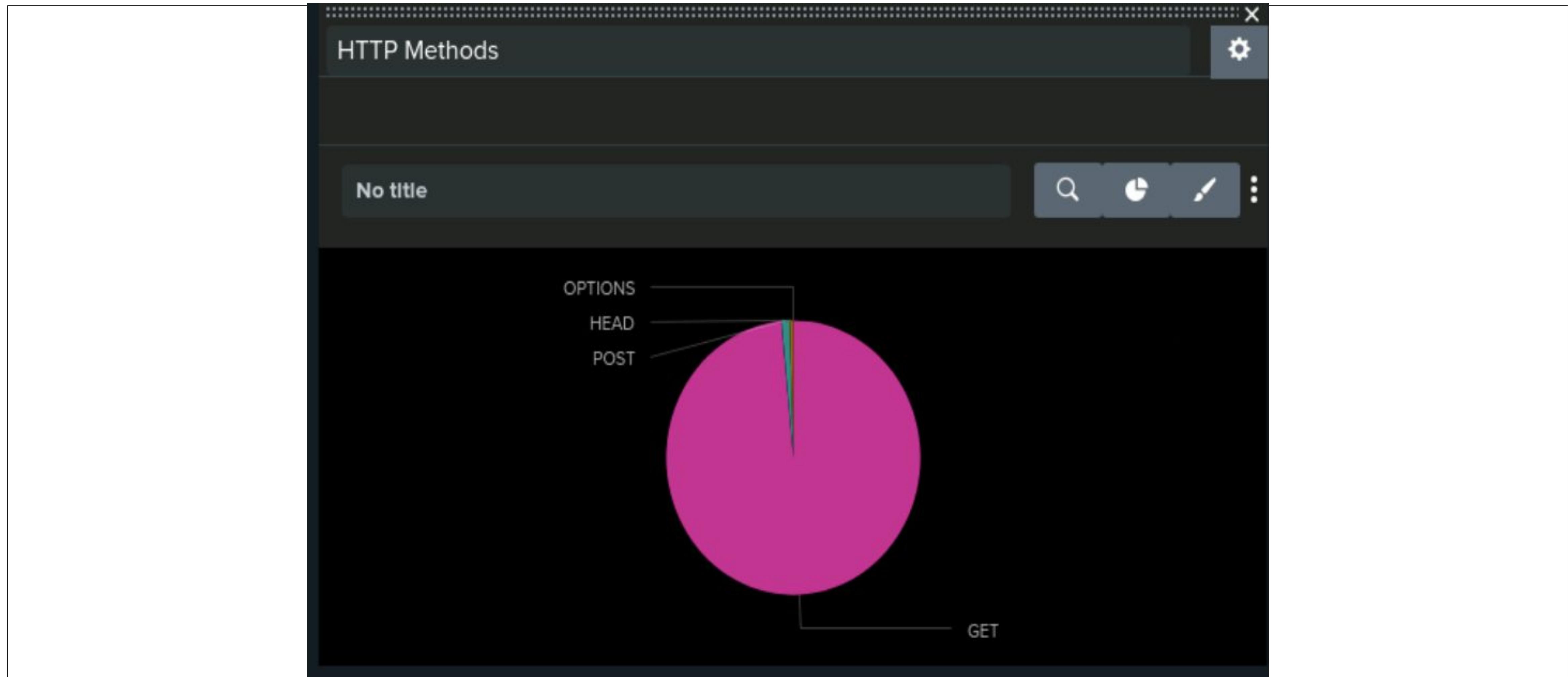
Dashboards—Apache

52



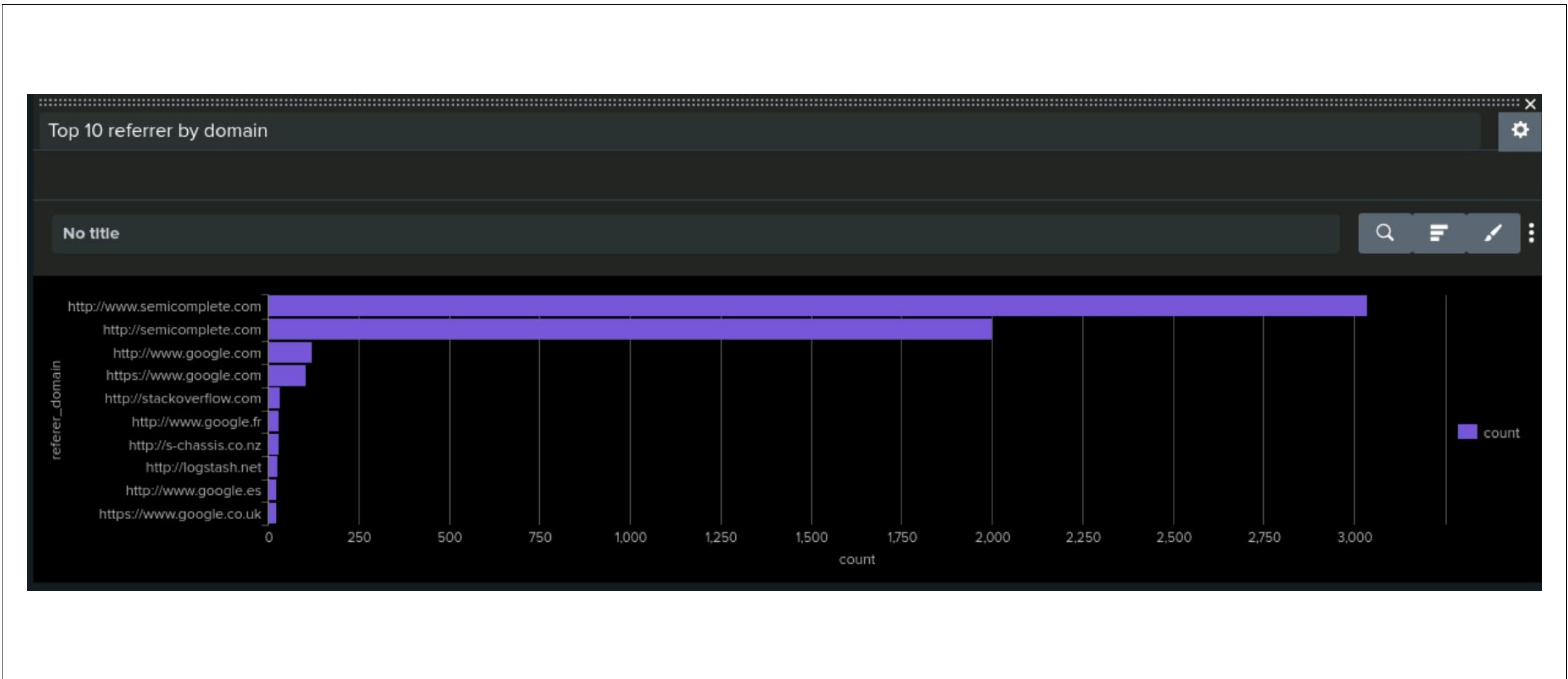
Dashboards—Apache

53



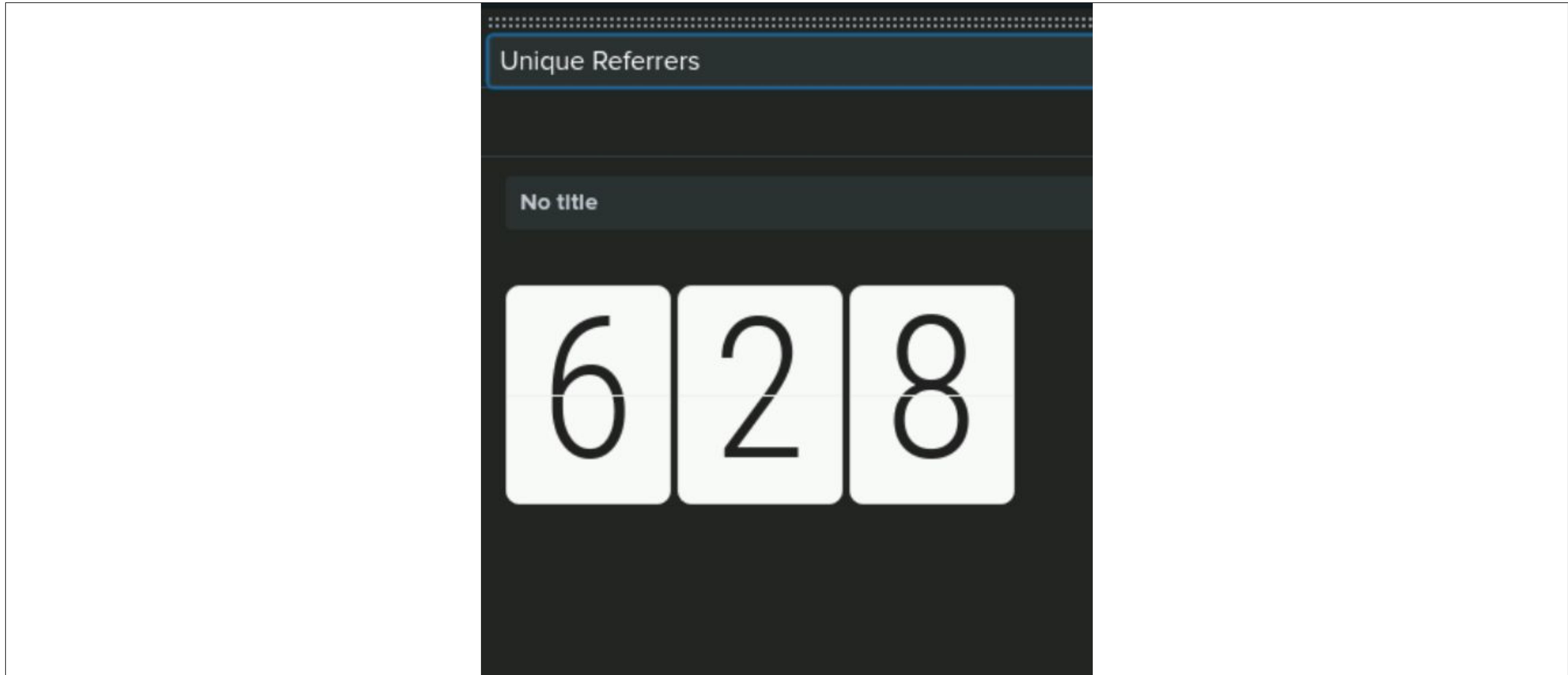
Dashboards—Apache

54



Dashboards—Apache

55





Attack Analysis

Attack Summary—Windows

57

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

- At 12:00:06 AM splunk reported computer account “user_l” deleting computer account “user_i”.
- By 2:00:00 AM these “alphabet users” would continue to self propagate and follow a series of repetitious actions involving resetting account passwords, changing domain password policy (changed to be between 6-8 characters), changing user accounts, clearing audit logs before deleting itself.
- These users were seemingly executed by a piece of malware “example_*.exe” following this same alphabet naming convention.
- The final event took place at 1:45:27 PM when the attack stopped.

Screenshots of Attack Logs

58

Initial anomalous event:

The screenshot shows a log viewer interface with the following details:

Time Range: Mar 25, 2020 12:00:06 AM to Mar 25, 2020 12:00:07 AM (1 sec)

Event Details:

Time	Event
3/25/20 12:00:06.000 AM	2020-03-25T00:06.000+0000,,,"Domain_A Domain_A","user_i user_l",,,,,"Account Management",,,,,"ACME-002",,,,,-,4743,A computer account was deleted,0,,,,"Audit Success",,,,"Security",,,,"0x5F25",,,,,"A computer account was deleted. Subject: Security ID: Domain_A\user_i Account Name: user_i Account Domain: Domain_A Logon ID: 0x5F25 Target Computer: Security ID: Domain_A\user_l Account Name: user_l Account Domain: Domain_A Additional Information: Privileges: SeLoadDriverPrivilege",,,,,"Info",,,,,"SeLoadDriverPrivilege",,,,,"216764501",,,,,"Domain_A\user_i Domain_A\user_l",,,,"Microsoft Windows security auditing",,,,,"Computer Account Management",,,,"Information",,,,,"03/25/2020 12:00:06 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4743 EventType=0

Selected Fields:

- host 1
- index 1
- #linecount 1
- source 1
- sourcetype 1
- splunk_server 1

Interesting Fields:

- Account_Domain 1
- Account_Name 1
- action 1
- app 1
- body 1
- category 1
- CategoryString 1
- change_type 1
- ComputerName 1
- date_hour 1
- date_mday 1
- date_minute 1
- date_month 1

Attack Summary—Windows

59

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

- [OH YEAH]

Attack Summary—Windows

60

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

- [Dashboards were very helpful when trying to correlate data to understand the timing and methods of attack.]

Attack Summary—Apache

61

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

- at 6PM a suspicious amount of GET requests for /files/logstash/logstash-1.3.2-monolithic.jar from a Chef Client executing a ruby script via ohai based from of opscode.com
- at 8PM a suspicious amount of POST requests hit /VSI_Account_logon.php, indicative of a brute force log on attack.

Screenshots of Attack Logs

62

The screenshot shows a log analysis interface with the following details:

- Search Bar:** source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined" method=GET "/files/logstash/logstash-1.3.2-monolithic.jar"
- Event Count:** 638 events (before 4/8/24 5:29:15.000 AM)
- Sampling:** No Event Sampling
- Time Range:** Mar 25, 2020 1:00 AM to Mar 25, 2020 10:00 PM (21 hours)
- Format:** 1 hour per column
- Event List:** The list displays 638 events, each containing the following fields:
 - Time: 3/25/20 9:05:11.000 PM
 - Event: 63.140.98.80 - - [25/Mar/2020:21:05:11 +0000] "GET /files/logstash/logstash-1.3.2-monolithic.jar HTTP/1.1" 404 324 "-" "Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.co m)"
 - host = apache_attack_logs | index = main | linecount = 1 | source = apache_attack_logs.txt | sourcetype = access_combined | splunk_server = 3c3213ab153c
- Selected Fields:** host, index, #linecount, source, sourcetype, splunk_server
- Interesting Fields:** bytes, clientip, date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year, date_zone, file, ident, method

Screenshots of Attack Logs

63

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined" method=POST "/VSI_Account_logon.php"
- Results Summary:** ✓ 1,323 events (before 4/8/24 5:47:29.000 AM) No Event Sampling ▾
- Time Range:** All time ▾ (Mar 25, 2020 2:00 AM to 1,296 events at 8 PM on Wednesday, March 25, 2020)
- Event Count:** 1 hour per column
- Event View:** Events (1,323) Patterns Statistics Visualization
- Formatting:** Format Timeline ▾, - Zoom Out, + Zoom to Selection, X Deselect
- Table Headers:** List ▾, Format, 50 Per Page ▾
- Selected Fields:** host, index, source, sourcetype, splunk_server
- Interesting Fields:** bytes, clientip, date_hour, date_mday, date_minute, date_month, date_second
- Table Data:** The table lists 1,323 events. The first few rows show:

Time	Event
3/25/20 8:05:59.000 PM	194.146.132.138 -- [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = apache_attack_logs index = main linecount = 1 source = apache_attack_logs.txt sourcetype = access_combined splunk_server = 3c3213ab153c
3/25/20 8:05:59.000 PM	194.146.132.138 -- [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = apache_attack_logs index = main linecount = 1 source = apache_attack_logs.txt sourcetype = access_combined splunk_server = 3c3213ab153c
3/25/20 8:05:59.000 PM	194.105.145.147 -- [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = apache_attack_logs index = main linecount = 1 source = apache_attack_logs.txt sourcetype = access_combined splunk_server = 3c3213ab153c
3/25/20 8:05:59.000 PM	194.105.145.147 -- [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = apache_attack_logs index = main linecount = 1 source = apache_attack_logs.txt sourcetype = access_combined splunk_server = 3c3213ab153c
3/25/20 8:05:59.000 PM	79.171.127.34 -- [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = apache_attack_logs index = main linecount = 1 source = apache_attack_logs.txt sourcetype = access_combined splunk_server = 3c3213ab153c
3/25/20 8:05:59.000 PM	79.171.127.34 -- [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)" host = apache_attack_logs index = main linecount = 1 source = apache_attack_logs.txt sourcetype = access_combined splunk_server = 3c3213ab153c

Attack Summary—Apache

64

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

- [OH YEAH]

Attack Summary—Apache

65

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

- The dashboards were very helpful in identifying not only the times and potential types of attacks taking place, but the geolocate function of splunk allowed us to see where the attacks were coming from.

Summary and Future Mitigations



Project 3 Summary

67

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

On Wednesday March 25th 2020, from 12am to 9pm an attack originating from Ukraine hit first VSI's Windows server, and later that same day VSI's Apache web servers. The attackers leveraged malware and botnets to manipulate logs and change domain policy for passwords, reset passwords, create new accounts, delete accounts and assign special privileges to new users. The attacks then pivoted to the the Apache web server where a very large number of GET requests pulling logs from the web server, followed by a large number of POST requests allowing the login page to be easily brute forced due to the policy password changes (6-8 characters) and resets. Due to the logs being pulled from the Apache server and the log in being brute forced, these systems should be considered compromised. Similarly, due to log erasure and an unknown executable being present on the windows server, these machines should also be considered compromised.

- To protect VSI from future attacks, what future mitigations would you recommend?
 - The attack seemingly started from a piece of malware that was present on the windows servers, all staff should be trained against phishing attempts and on site security should be reviewed to discover where the malware originated.
 - Firewalls should be in place and updated to stop brute force attempts.
 - Firewalls should be in place to screen potentially malicious IPs.
 - Lock out on too many password attempts in X amount of time to stop brute force.
 - Logs should not be accessible from the web API.

Project 3 (Q&A)

68



Project 3 Ending

The graphic consists of several large, bold, black words arranged in a grid-like pattern. From left to right, the words are:

- GRACIAS**: SPASSIBO, MUHUN, CHALTU, DANKSCHEEN
- ARIGATO**: SHACHALHYA, TASHAKKUR ATU, YAQHANYELAY, SUKSAMA, EKHMET
- SHUKURIA**: HABEEJA, MAITEKA, YUSPAGARATAN
- JUSPAXAR**: TAVTAPUCH, MEDAHAGSE, BAIKA
- TASHAKKUR ATU**: DHAYABAAD, ABIA, MAITIKA, HUI
- YAQHANYELAY**: SPASSIBO, SHACHALHYA, DHAHABAAD, ABIA, MAITIKA, HUI
- SUKSAMA**: EKHMET, SPASSIBO, DENKAUJA, NENACHALHYA
- EKHMET**: SPASSIBO, DENKAUJA, NENACHALHYA
- GRAZIE**: MAAKE, ATTO, LAH
- MEHRBANI**: PALKIES
- PALDIES**: SPASSIBO, DENKAUJA, NENACHALHYA
- THANK**: TINGKI, HATUR S, EKOJU, SIKOMO, MAKETAJ
- YOU**: BOLZİN, MERCI
- BOLZİN**: MINMONCHAB
- MERCI**: MINMONCHAB