Defensive Security Project
by: Bo, Chris, Connor, Joseph & Seth

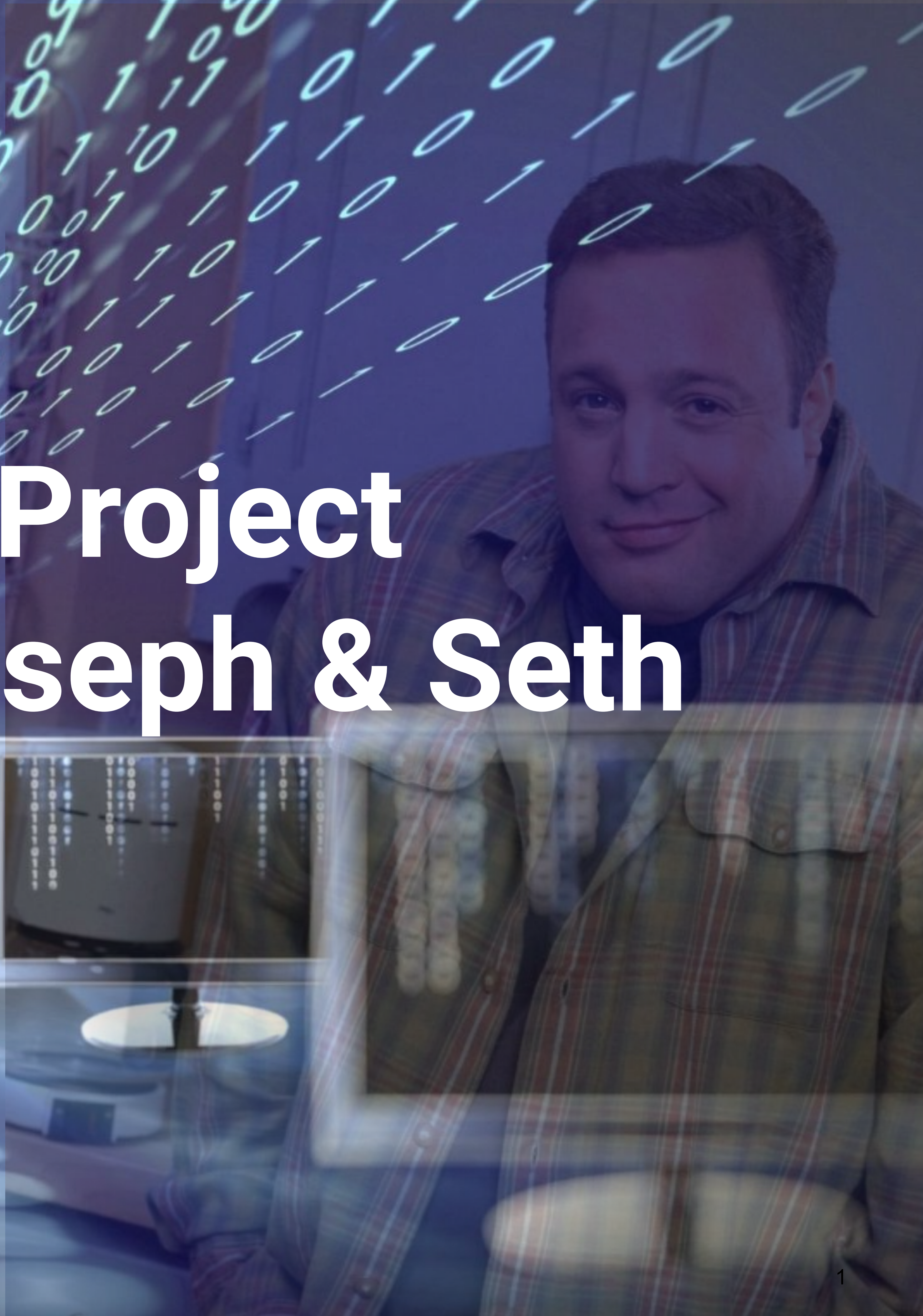


Table of Contents

This document contains the following resources:

01 **Monitoring Environment**

02 **Attack Analysis**

03 **Project Summary & Future Mitigations**

Monitoring Environment

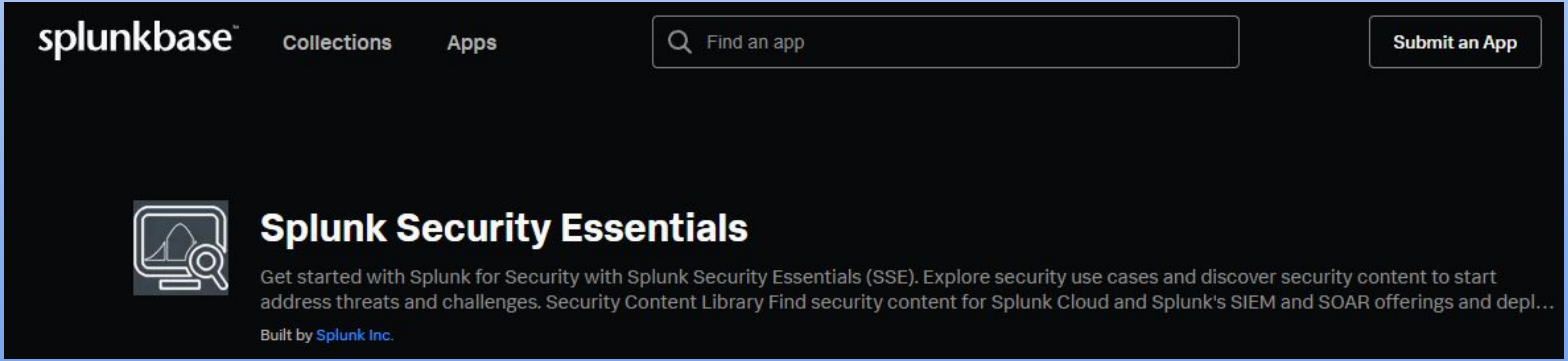
Scenario

- Me and the boiz of Vandalay Corp (VSI) are defensive security specialists who will help mitigate, protect, and investigate the cyber attacks that are frequently happening from JobeCorp, our arch-nemesis. They took down several of our machines, and we need to identify which systems are down and how they did it.
- What this presentation will show the logs of our monitoring systems that were targeted (Windows and Apache) and the reports and alerts that we’ve set up to show the data of what happened while we were under attack.

Splunk Security Essentials Add-on

Splunk Security Essentials Add-on

- This Splunk add-on (SSE) provides a security content library and takes the logs and events we're Splunking to analyze and give us suggestions on what to do to improve our security and shows what we can do to take care of any low to critical issues that would need immediate attention.
- It makes it easier to analyze the events and data in our environment to help detect the fields and tags using the security library.
- It has a public rating of 4 out of 5 stars from 55+ reviews, so we know that there are plenty of users.
- It seems to be easy to understand and use.



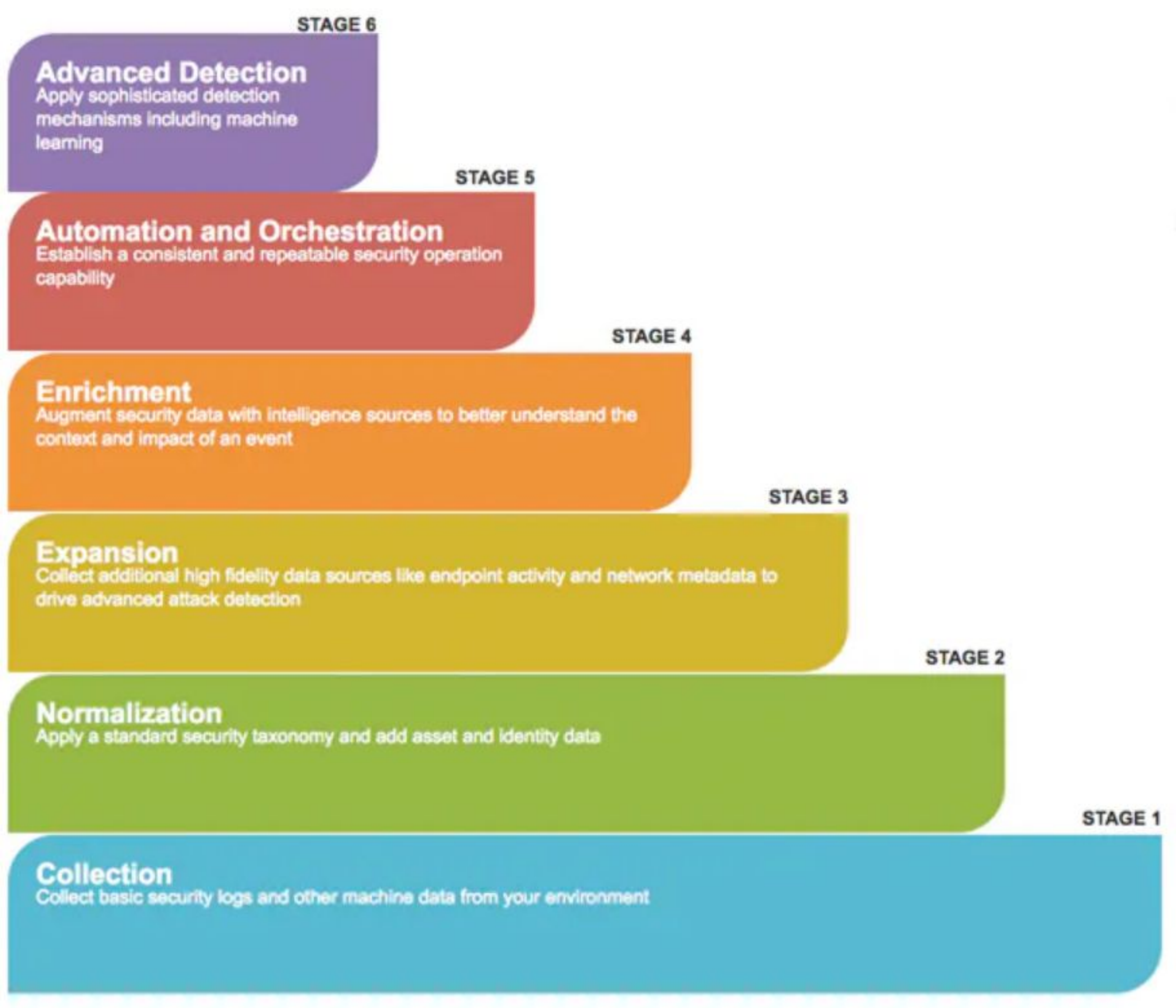
Splunk Security Essentials

Get started with Splunk for Security with Splunk Security Essentials (SSE). Explore security use cases and discover security content to start address threats and challenges. Security Content Library Find security content for Splunk Cloud and Splunk's SIEM and SOAR offerings and depl...

Built by Splunk Inc.

Splunk Security Essentials Add-on

- Add in the report for the Splunk Security Essentials to analyze
- It shows a collection of recommended actions for us to address from brute force detection to a malware ourbreak, and I’m sure it will be able to identify the kinds of attacks that JobeCorp have done.
- As it identifies data, it will expand and collect endpoint activities and network metadata in order to detect more attacks.
- Uses its sources to better understand the impact of the events
- Creates a way that we can use consistently to be more secure
- Finally, it uses its experience and saves it to use for future logs and contexts so that the machine will actually learn how to automatically detect it.



STAGE 6

Advanced Detection
Apply sophisticated detection mechanisms including machine learning

STAGE 5

Automation and Orchestration
Establish a consistent and repeatable security operation capability

STAGE 4

Enrichment
Augment security data with intelligence sources to better understand the context and impact of an event

STAGE 3

Expansion
Collect additional high fidelity data sources like endpoint activity and network metadata to drive advanced attack detection

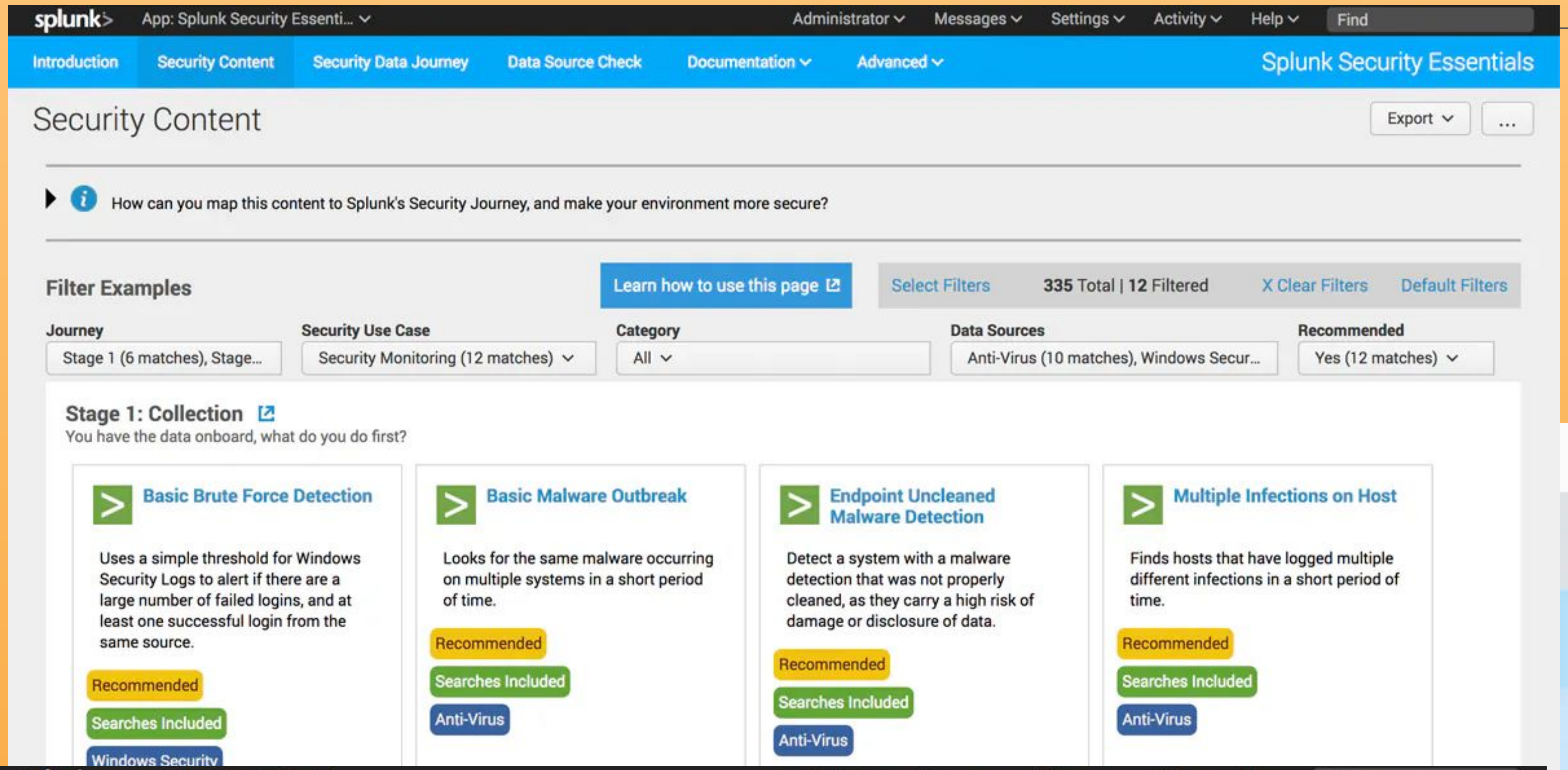
STAGE 2

Normalization
Apply a standard security taxonomy and add asset and identity data

STAGE 1

Collection
Collect basic security logs and other machine data from your environment

Splunk Security Essentials Add-on



Security Content

How can you map this content to Splunk's Security Journey, and make your environment more secure?

Filter Examples

Learn how to use this page | Select Filters | 335 Total | 12 Filtered | X Clear Filters | Default Filters

Journey	Security Use Case	Category	Data Sources	Recommended
Stage 1 (6 matches), Stage...	Security Monitoring (12 matches)	All	Anti-Virus (10 matches), Windows Secur...	Yes (12 matches)

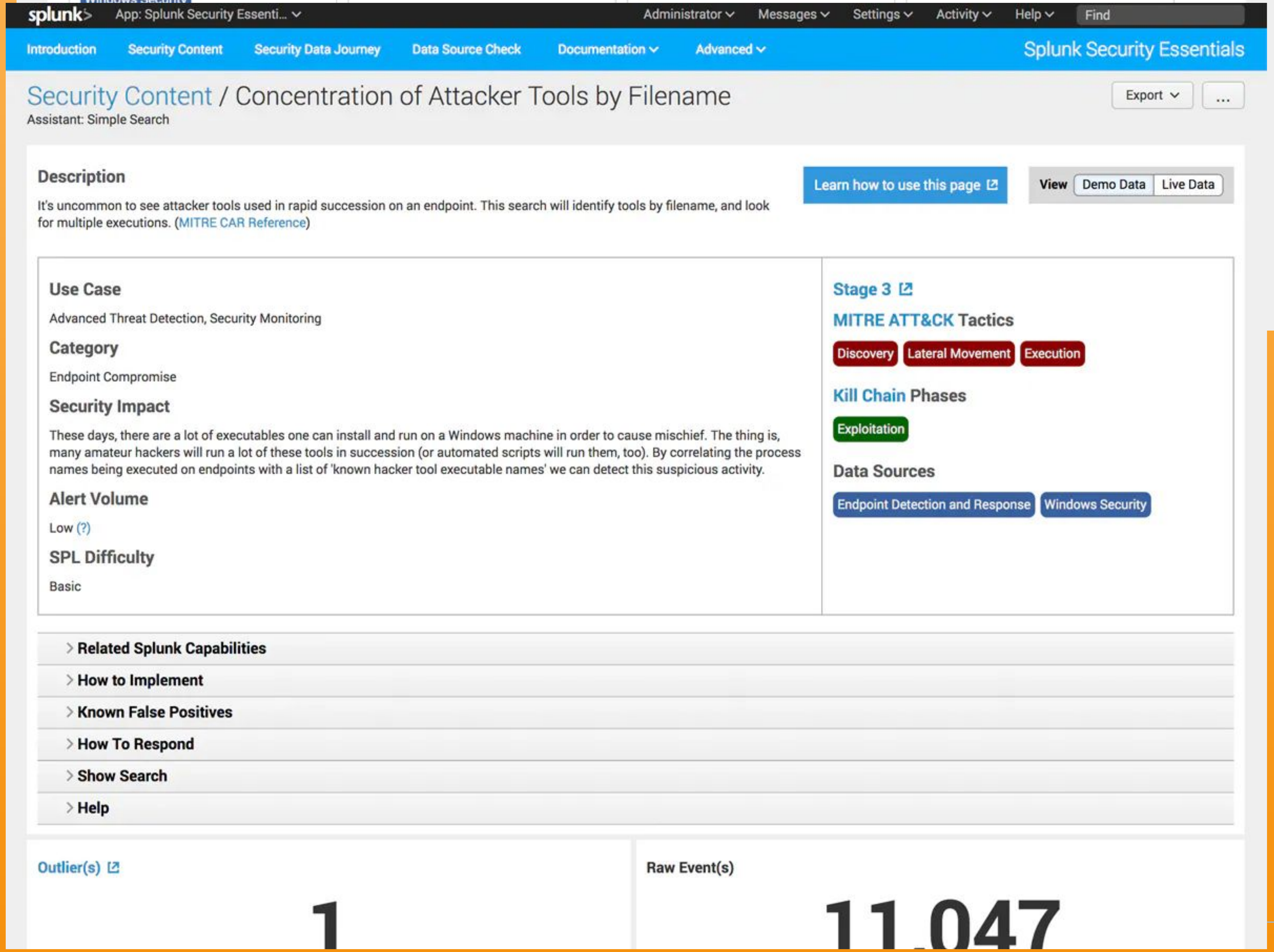
Stage 1: Collection
You have the data onboard, what do you do first?

Basic Brute Force Detection
Uses a simple threshold for Windows Security Logs to alert if there are a large number of failed logins, and at least one successful login from the same source.
Recommended | Searches Included | Windows Security

Basic Malware Outbreak
Looks for the same malware occurring on multiple systems in a short period of time.
Recommended | Searches Included | Anti-Virus

Endpoint Uncleaned Malware Detection
Detect a system with a malware detection that was not properly cleaned, as they carry a high risk of damage or disclosure of data.
Recommended | Searches Included | Anti-Virus

Multiple Infections on Host
Finds hosts that have logged multiple different infections in a short period of time.
Recommended | Searches Included | Anti-Virus



Security Content / Concentration of Attacker Tools by Filename
Assistant: Simple Search

Description
It's uncommon to see attacker tools used in rapid succession on an endpoint. This search will identify tools by filename, and look for multiple executions. (MITRE CAR Reference)

Use Case
Advanced Threat Detection, Security Monitoring

Category
Endpoint Compromise

Security Impact
These days, there are a lot of executables one can install and run on a Windows machine in order to cause mischief. The thing is, many amateur hackers will run a lot of these tools in succession (or automated scripts will run them, too). By correlating the process names being executed on endpoints with a list of 'known hacker tool executable names' we can detect this suspicious activity.

Alert Volume
Low (?)

SPL Difficulty
Basic

Stage 3

MITRE ATT&CK Tactics
Discovery | Lateral Movement | Execution

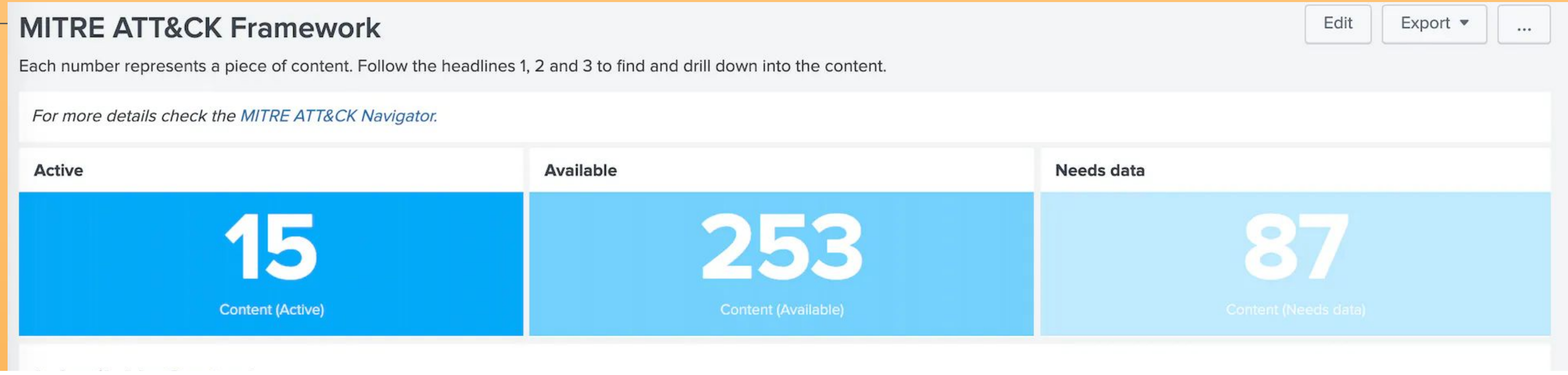
Kill Chain Phases
Exploitation

Data Sources
Endpoint Detection and Response | Windows Security

- Related Splunk Capabilities
- How to Implement
- Known False Positives
- How To Respond
- Show Search
- Help

Outlier(s): 1

Raw Event(s): 11,047

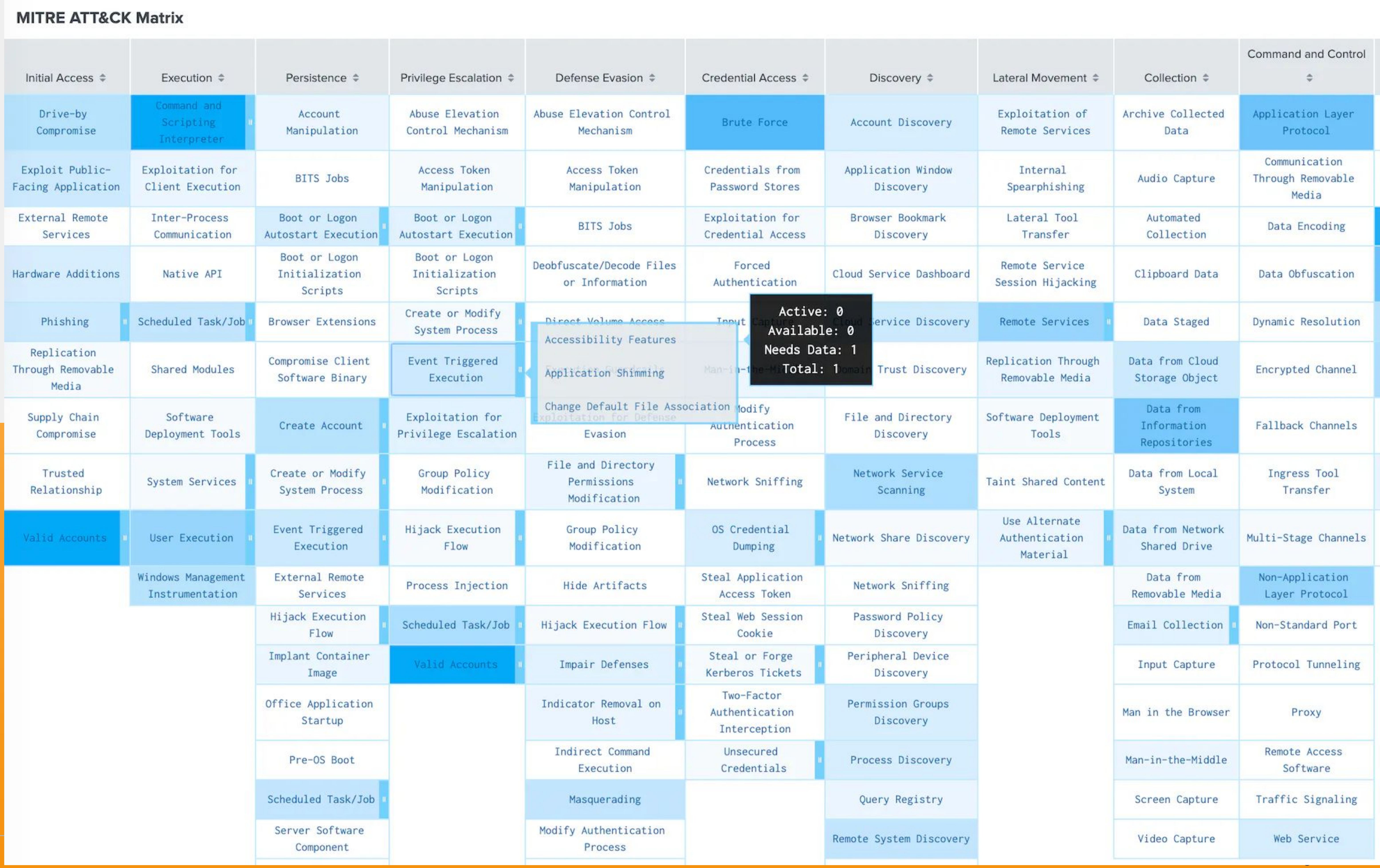


MITRE ATT&CK Framework

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

For more details check the MITRE ATT&CK Navigator.

Active	Available	Needs data
15 Content (Active)	253 Content (Available)	87 Content (Needs data)



MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Input Capture	Cloud Service Discovery	Remote Services	Data Staged	Dynamic Resolution
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	Domain Trust Discovery	Replication Through Removable Media	Data from Cloud Storage Object	Encrypted Channel
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process	File and Directory Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels
Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Local System	Ingress Tool Transfer
Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	OS Credential Dumping	Network Share Discovery	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol
		Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal Web Session Cookie	Password Policy Discovery		Email Collection	Non-Standard Port
		Implant Container Image	Valid Accounts	Impair Defenses	Steal or Forge Kerberos Tickets	Peripheral Device Discovery		Input Capture	Protocol Tunneling
		Office Application Startup		Indicator Removal on Host	Two-Factor Authentication Interception	Permission Groups Discovery		Man in the Browser	Proxy
		Pre-OS Boot		Indirect Command Execution	Unsecured Credentials	Process Discovery		Man-in-the-Middle	Remote Access Software
		Scheduled Task/Job		Masquerading		Query Registry		Screen Capture	Traffic Signaling
		Server Software Component		Modify Authentication Process		Remote System Discovery		Video Capture	Web Service

Accessibility Features
Application Shimming
Change Default File Association

```
Active: 0
Available: 0
Needs Data: 1
Total: 1
```

Logs Analyzed

1 Windows Logs

- Logs of user credential exploitation attempts using brute force attacks; they were able to compromise a user account, delete it, and create a new one to change domain policies.

*We analyzed both the server logs and attack logs in order to find the differences between “normal” and compromised.

2 Apache Logs

- Logs of HTTP POST activity coming from all around the world, and there was more suspicious HTTP POST activity from Ukraine specifically.
- The POST alerts skyrocketed and that was what we were able to track down with.
- They were most likely trying to brute force the VSI login page to see if they can exploit our credentials.

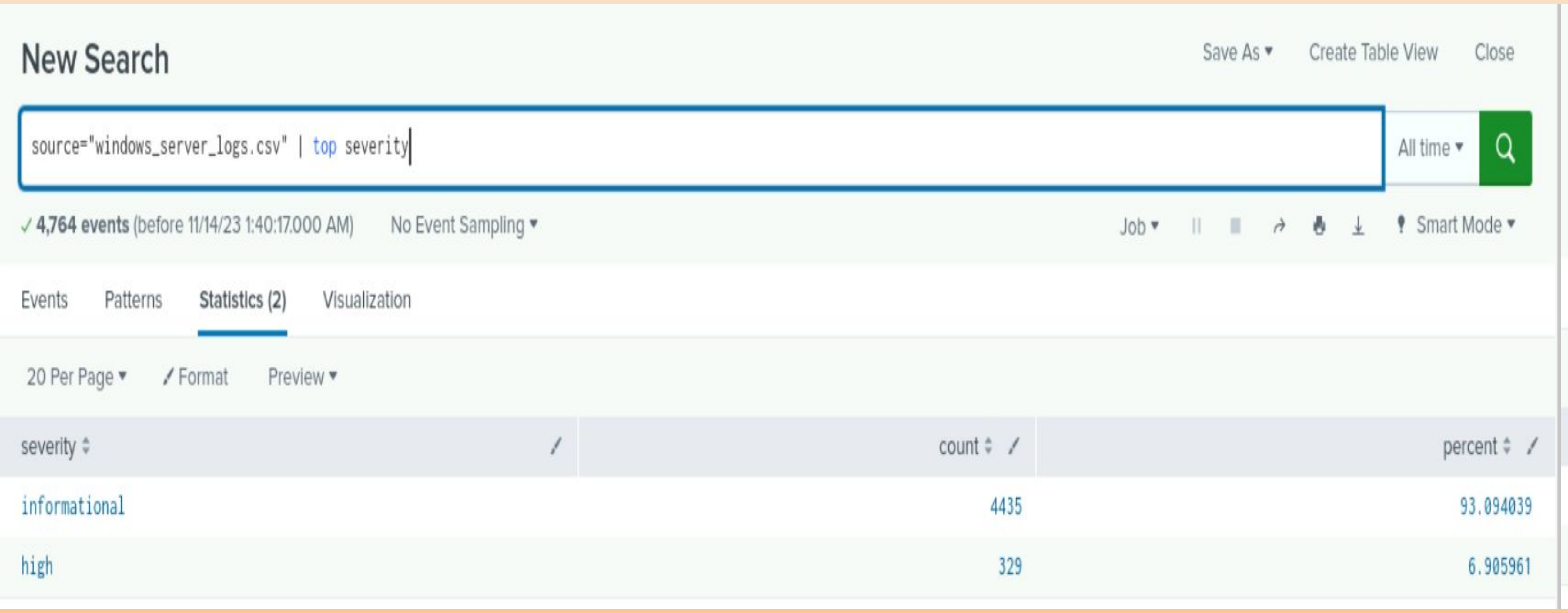
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Report Analysis for Severity	High severity increased from 6.9 to 20
Report Analysis for Failed Activities	Success rate for activities increased by 1.4%

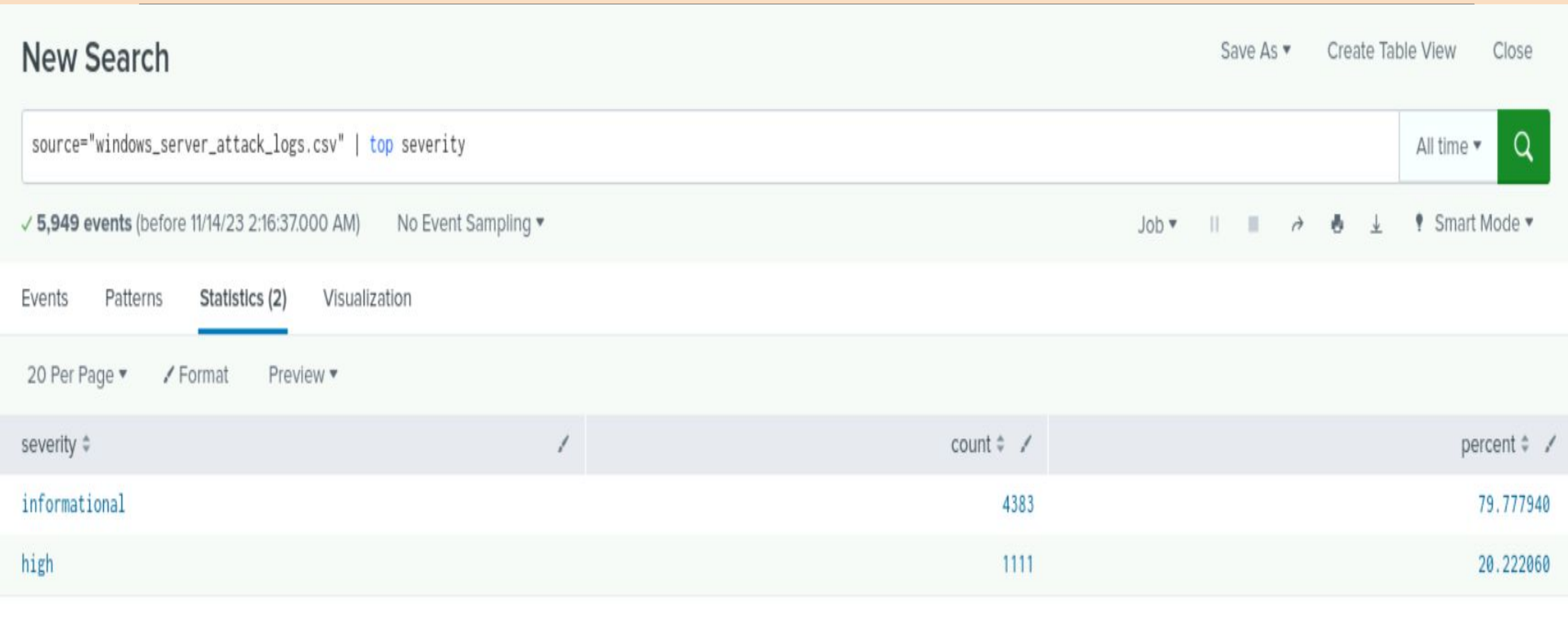
Images of Reports—Windows



```
source="windows_server_logs.csv" | top severity
```

✓ 4,764 events (before 11/14/23 1:40:17.000 AM)

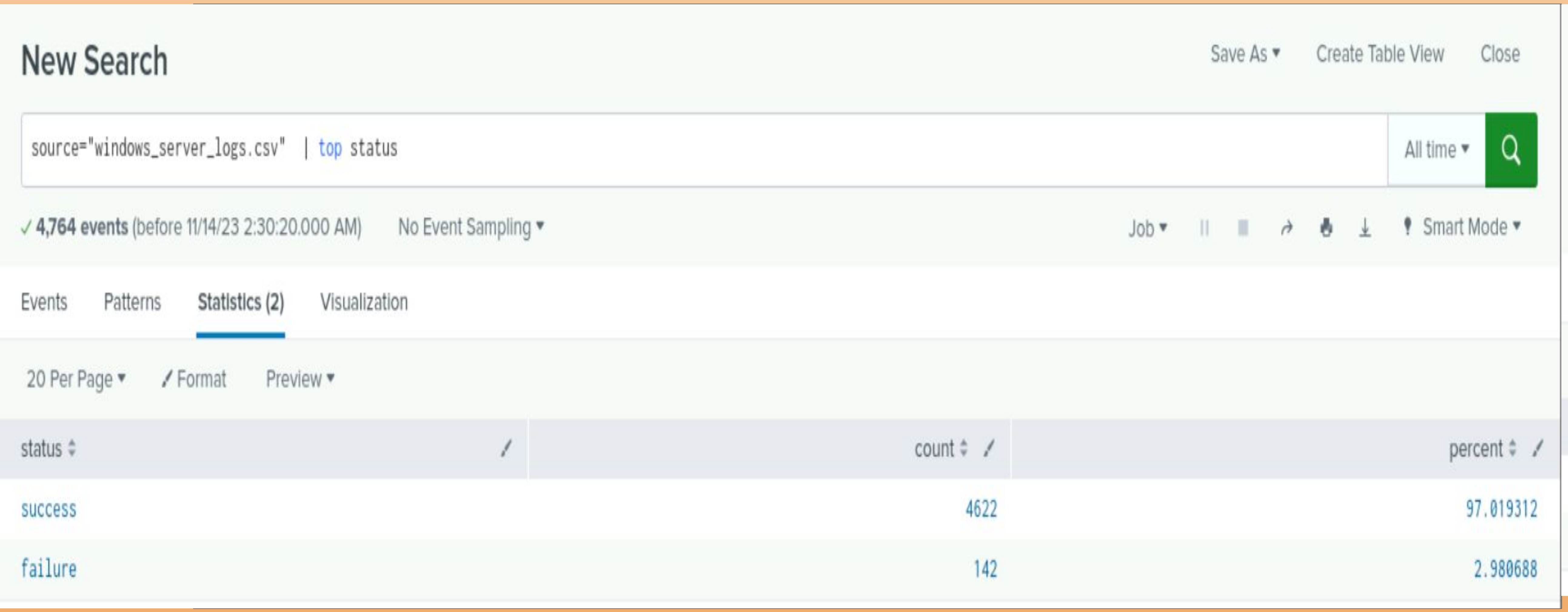
severity	count	percent
informational	4435	93.094039
high	329	6.905961



```
source="windows_server_attack_logs.csv" | top severity
```

✓ 5,949 events (before 11/14/23 2:16:37.000 AM)

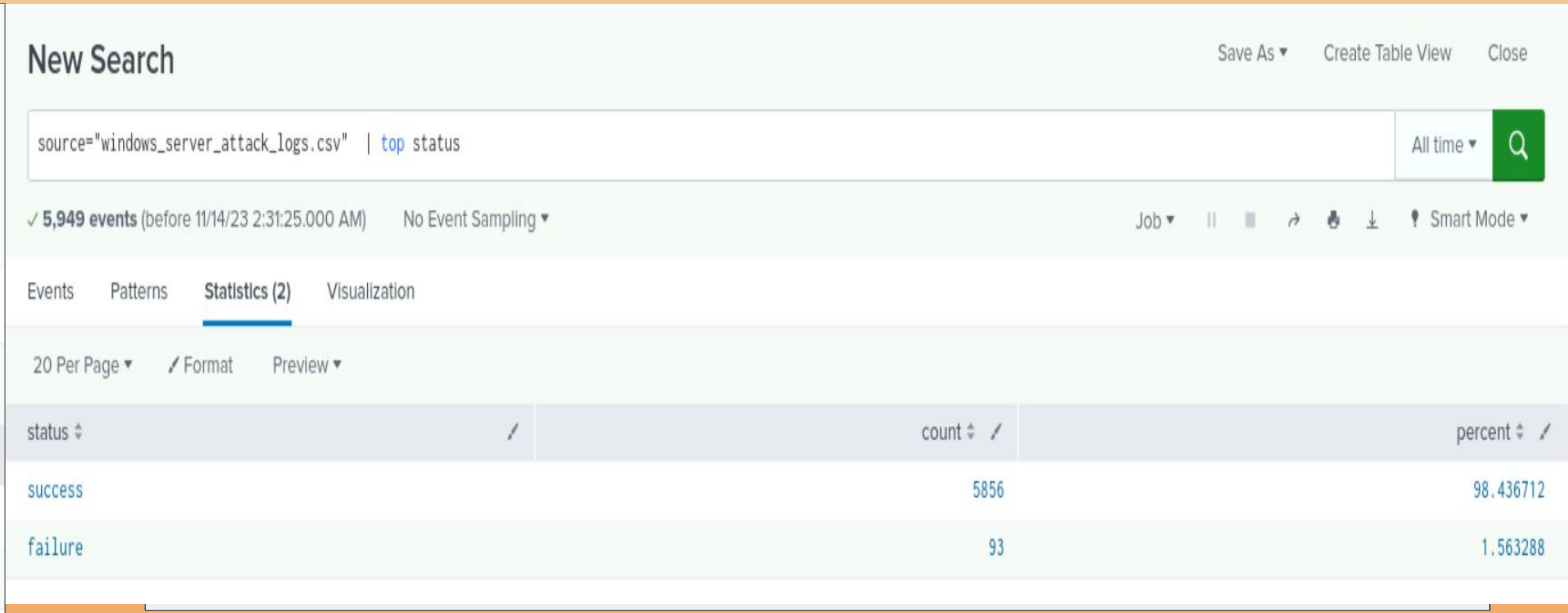
severity	count	percent
informational	4383	79.777940
high	1111	20.222060



```
source="windows_server_logs.csv"  | top status
```

✓ 4,764 events (before 11/14/23 2:30:20.000 AM)

status	count	percent
success	4622	97.019312
failure	142	2.980688

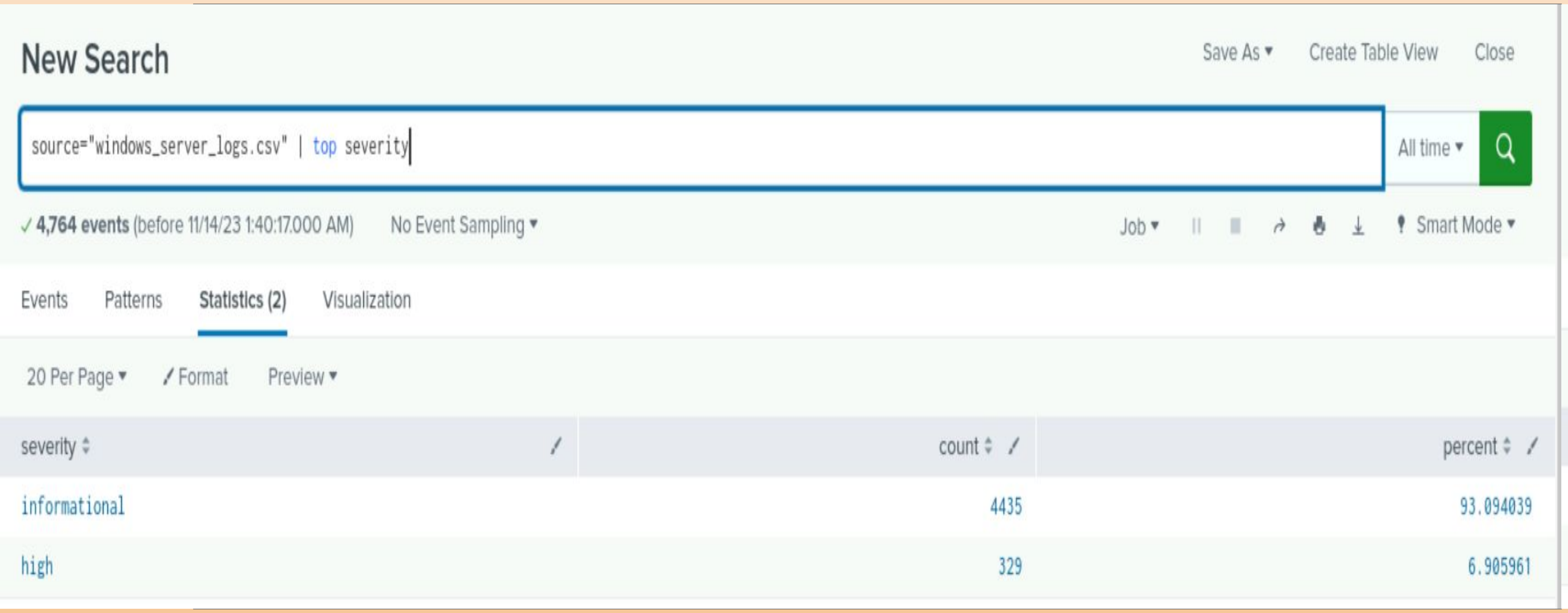


```
source="windows_server_attack_logs.csv"  | top status
```

✓ 5,949 events (before 11/14/23 2:31:25.000 AM)

status	count	percent
success	5856	98.436712
failure	93	1.563288

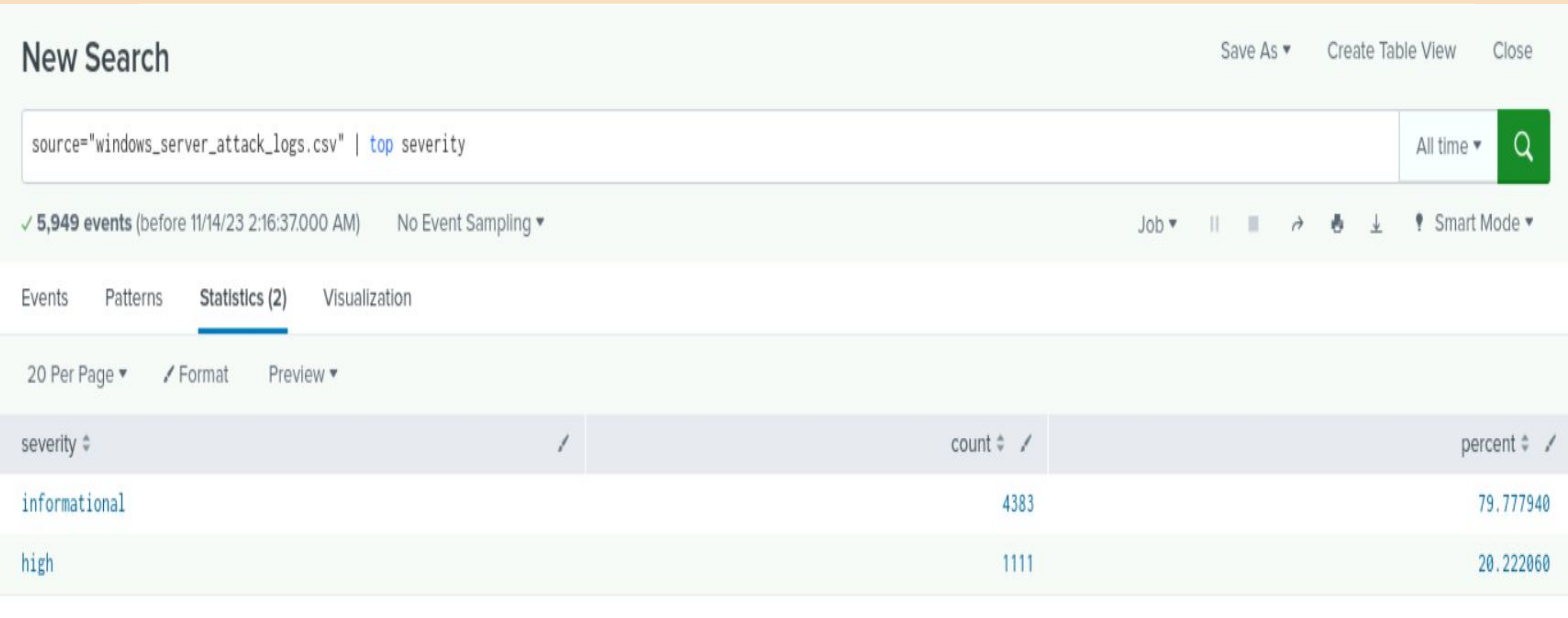
Images of Reports—Windows



```
source="windows_server_logs.csv" | top severity
```

✓ 4,764 events (before 11/14/23 1:40:17.000 AM) No Event Sampling ▾

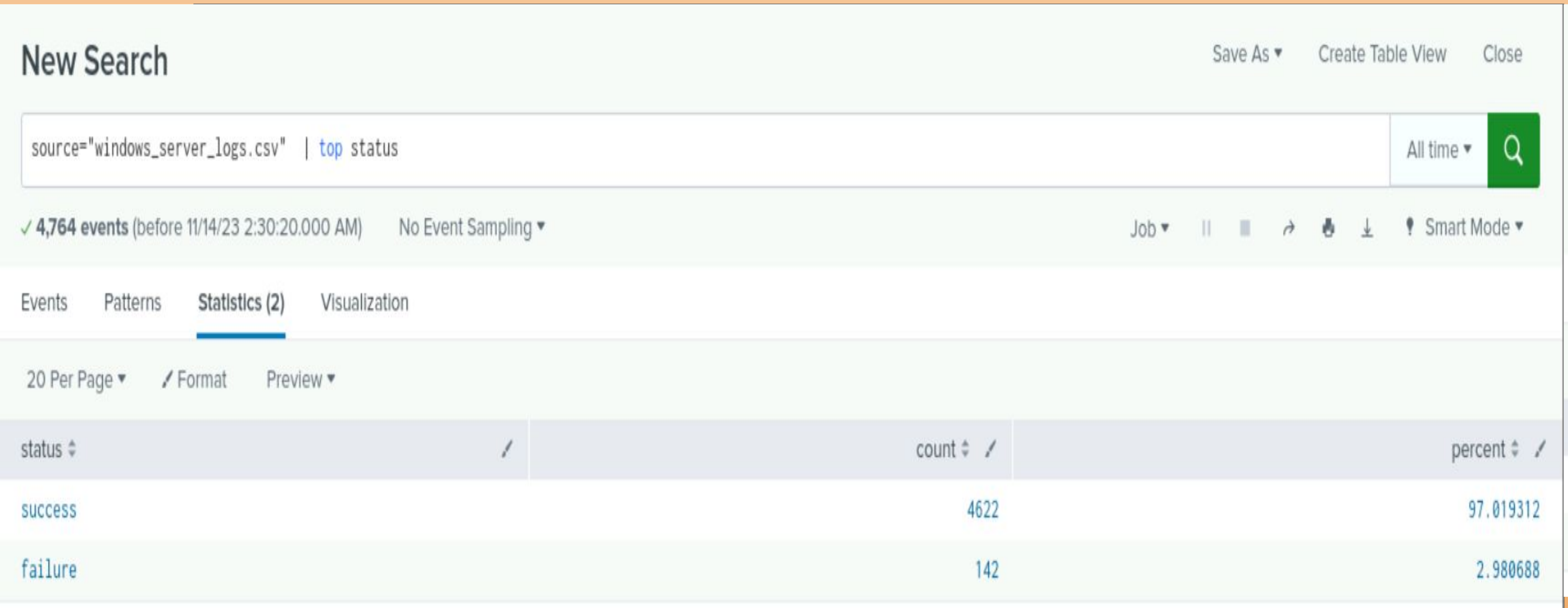
severity	count	percent
informational	4435	93.094039
high	329	6.905961



```
source="windows_server_attack_logs.csv" | top severity
```

✓ 5,949 events (before 11/14/23 2:16:37.000 AM) No Event Sampling ▾

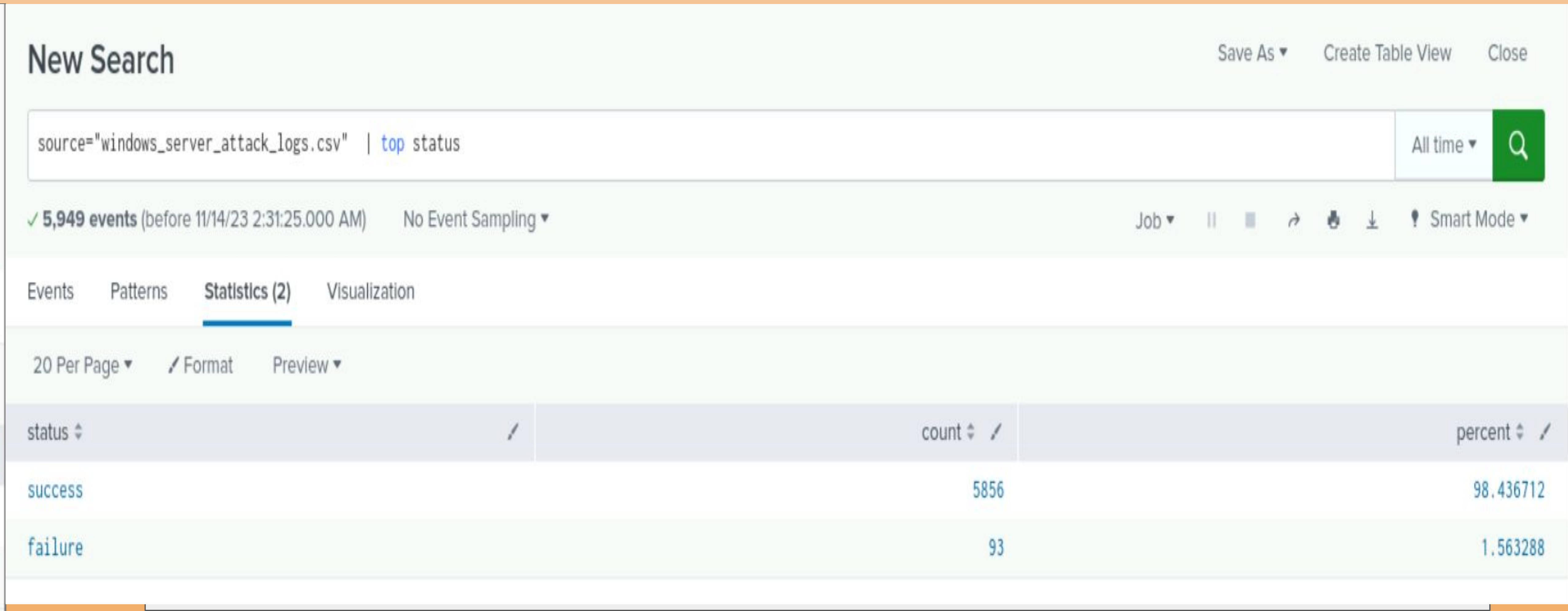
severity	count	percent
informational	4383	79.777940
high	1111	20.222060



```
source="windows_server_logs.csv"  | top status
```

✓ 4,764 events (before 11/14/23 2:30:20.000 AM) No Event Sampling ▾

status	count	percent
success	4622	97.019312
failure	142	2.980688



```
source="windows_server_attack_logs.csv"  | top status
```

✓ 5,949 events (before 11/14/23 2:31:25.000 AM) No Event Sampling ▾

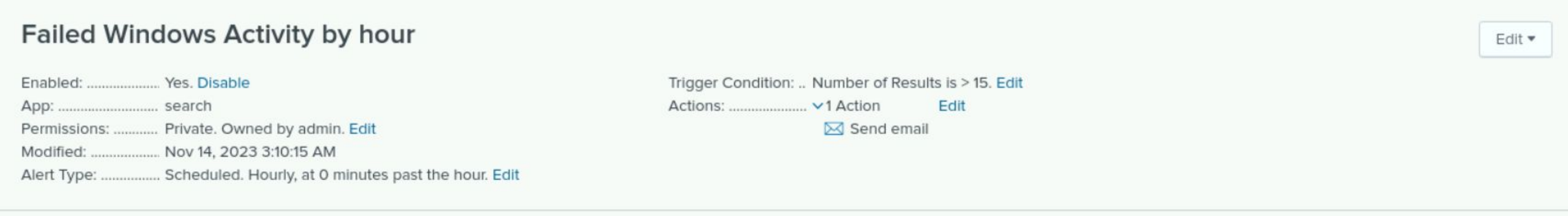
status	count	percent
success	5856	98.436712
failure	93	1.563288

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	Alert set to run a report looking for high numbers of failed attempts that could indicate an attack	10	15

JUSTIFICATION: 15 is a satisfactory threshold as it is high enough that it reduces chances of causing alert fatigue with false positive reports, but not being to high above the baseline that suspicious failed activities do not set off the trigger



Failed Windows Activity by hour

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Nov 14, 2023 3:10:15 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

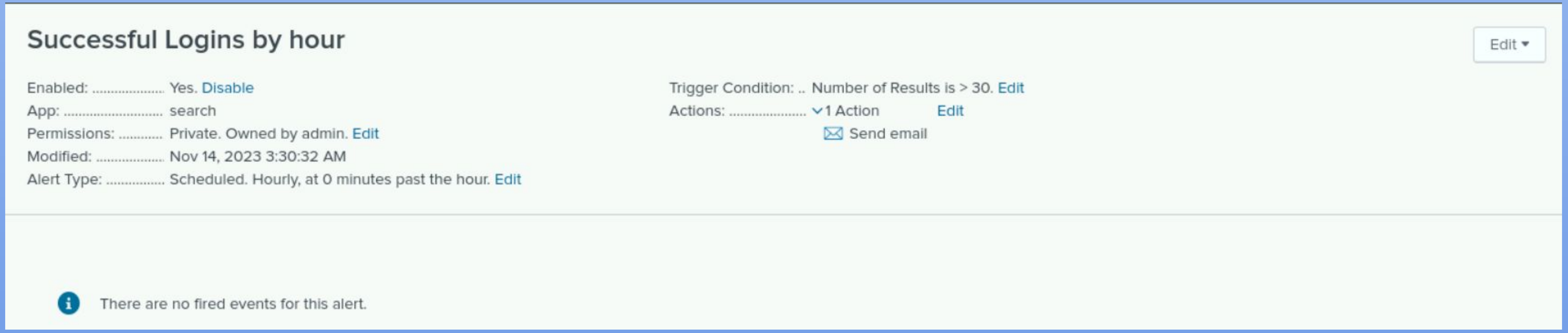
Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... 1 Action Edit
Send email

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins	Alert set to notify if successful logins exceed normal amounts	12	30

JUSTIFICATION: 30 is a suitable threshold as it is above baseline and will not trigger alerts for normal user successful logins, but will report and capture suspicious volumes of successful logins.



Successful Logins by hour

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Nov 14, 2023 3:30:32 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 30. Edit
Actions: .... 1 Action Edit
Send email

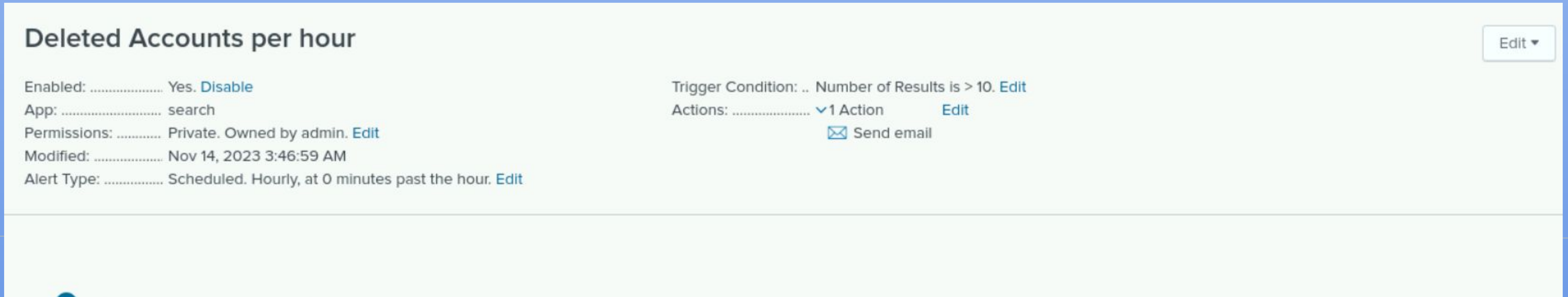
There are no fired events for this alert.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Deleted Accounts	Alert designed to notify SOC Analyst if there is a suspicious volume of deleted accounts	7	10

JUSTIFICATION: With the baseline of 13, 30 is a good threshold as it will catch high volumes of deleted accounts and stays above normal levels of account deletion.

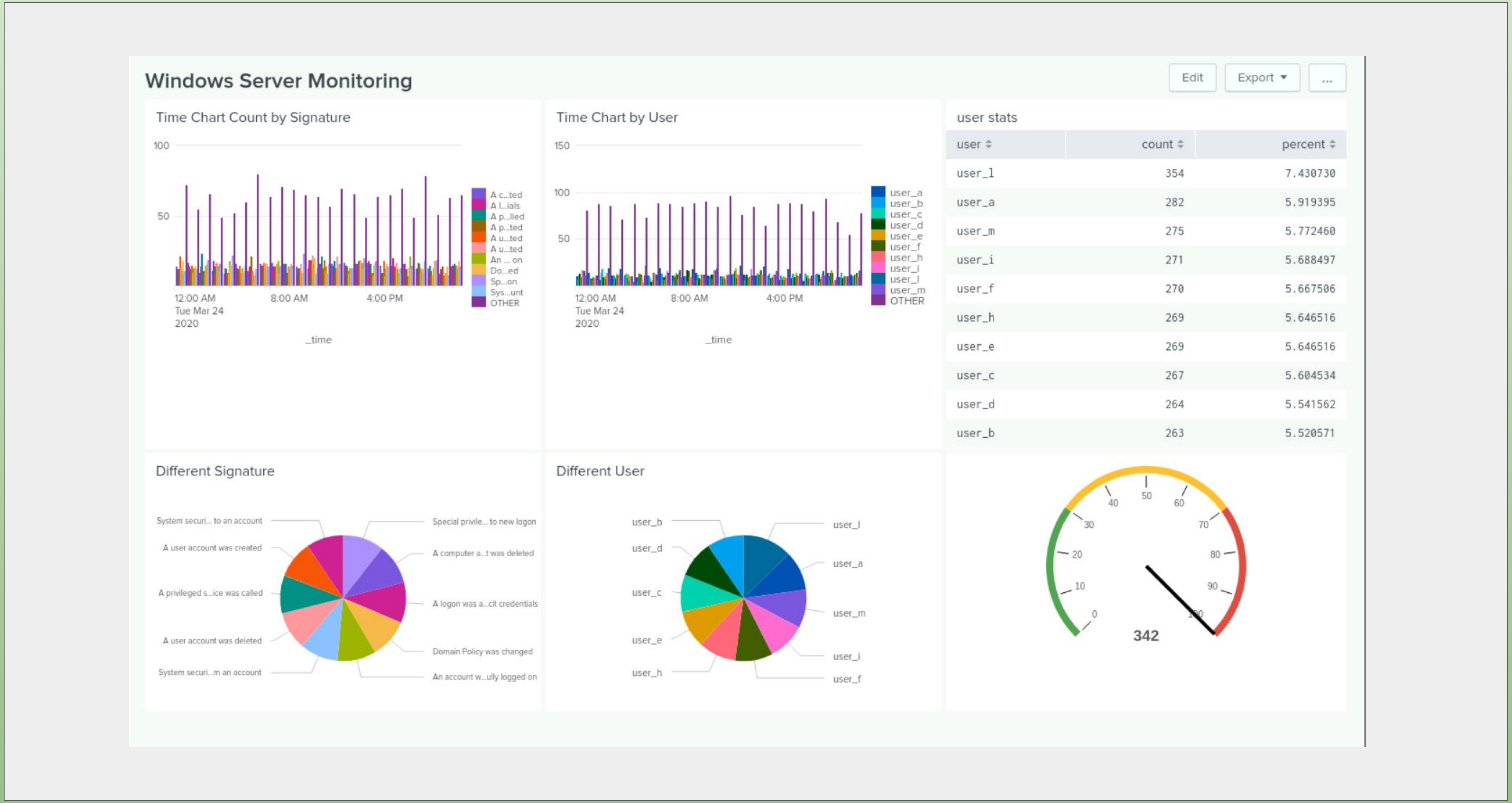


Deleted Accounts per hour

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Nov 14, 2023 3:46:59 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 10. Edit
Actions: .... ⌄1 Action Edit
✉ Send email

Dashboards—Windows



Windows Server Monitoring

Time Chart Count by Signature

Time Chart by User

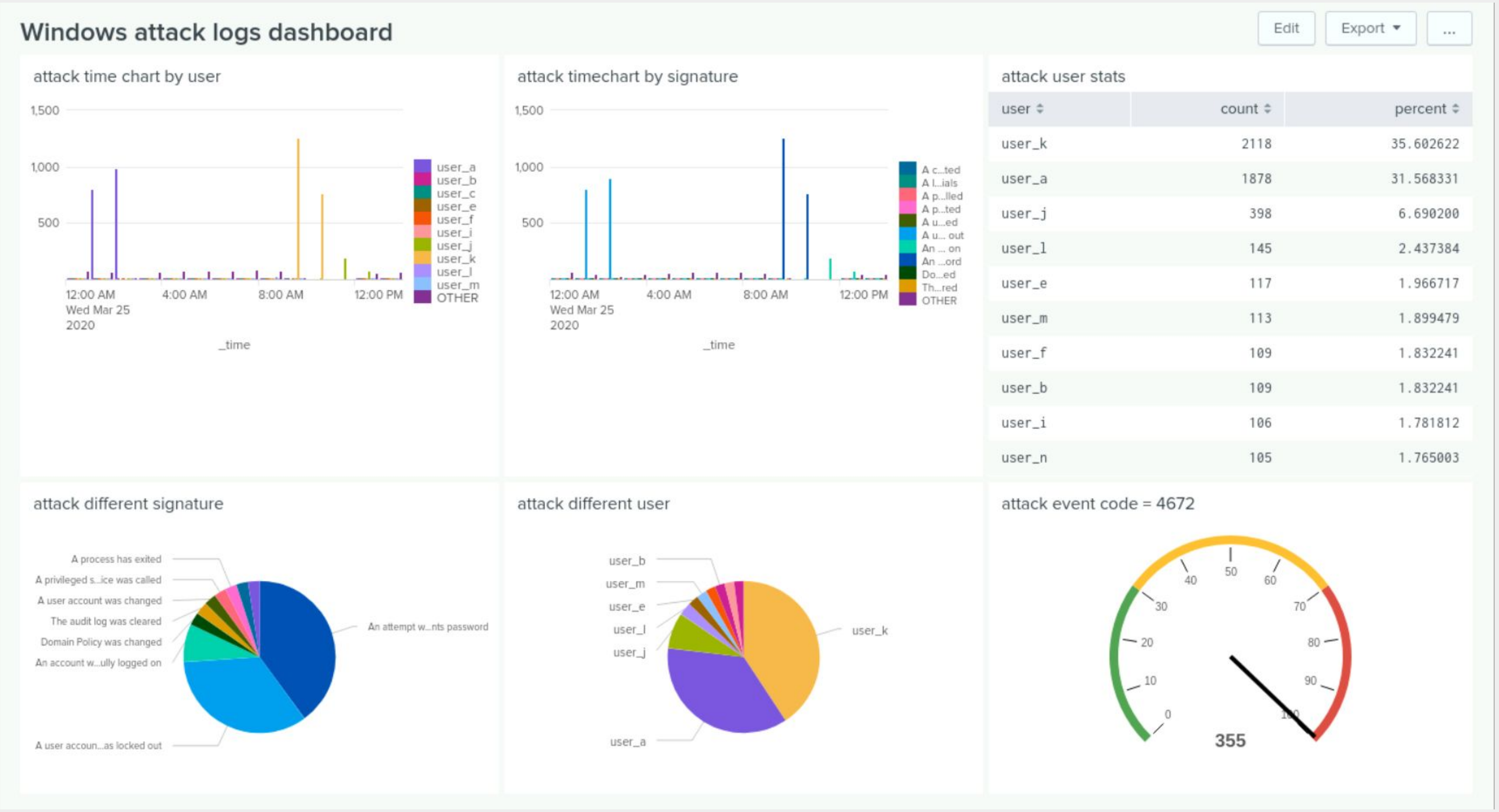
user stats

user ⇕	count ⇕	percent ⇕
user_l	354	7.430730
user_a	282	5.919395
user_m	275	5.772460
user_i	271	5.688497
user_f	270	5.667506
user_h	269	5.646516
user_e	269	5.646516
user_c	267	5.604534
user_d	264	5.541562
user_b	263	5.520571

Different Signature

Different User

Dashboards—Windows



attack user stats

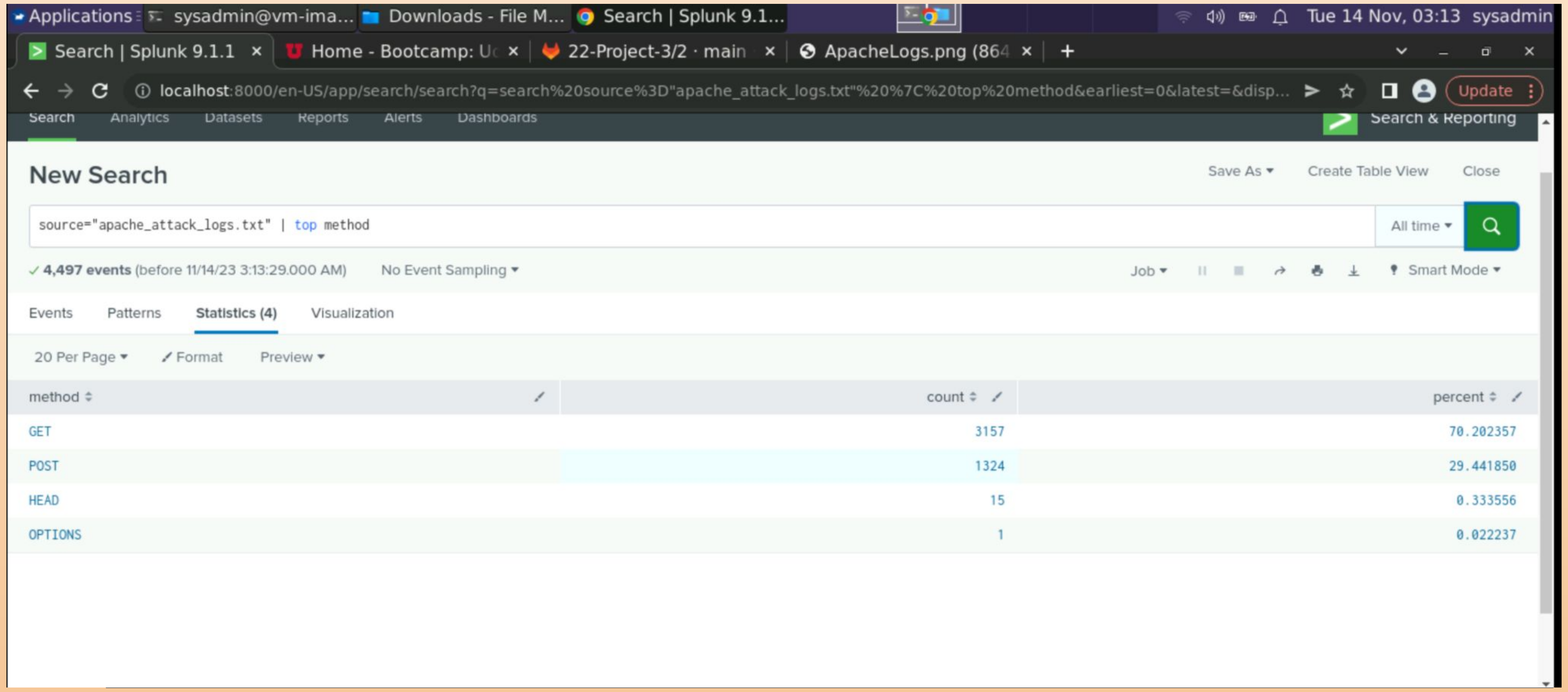
user ⇕	count ⇕	percent ⇕
user_k	2118	35.602622
user_a	1878	31.568331
user_j	398	6.690200
user_l	145	2.437384
user_e	117	1.966717
user_m	113	1.899479
user_f	109	1.832241
user_b	109	1.832241
user_i	106	1.781812
user_n	105	1.765003

Apache Logs

Reports—Apache

Report Name	**Report Description**
Report analysis for methods	Detection of changes in POST and GET methods
Report Analysis for Referrer Domains	Any sus alterations in domains
Report Analysis for HTTP Response Codes	Increased in 404 from 2% to 15% and decreased in 200 code from 91%-83%

Images of Reports—Apache

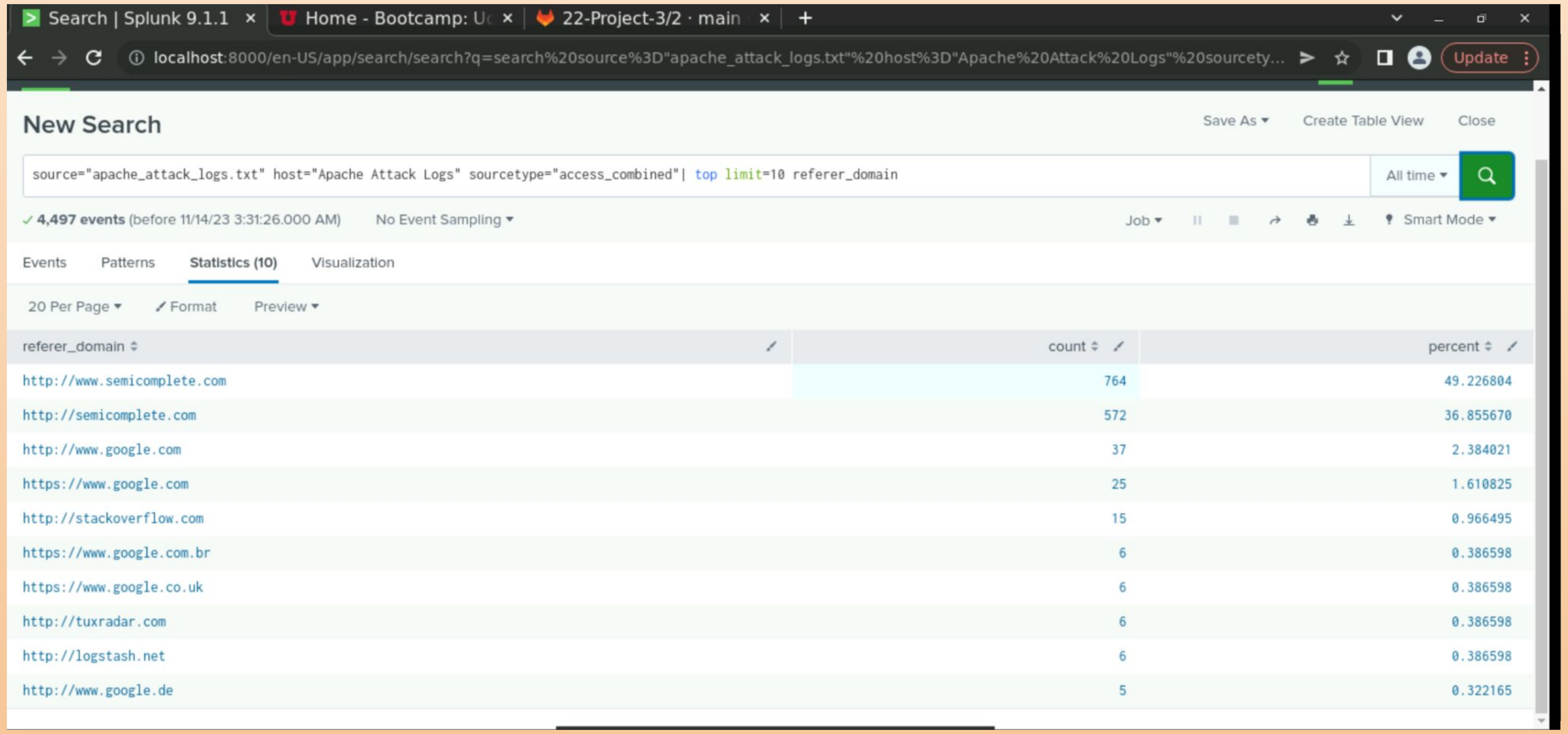

Applications
sysadmin@vm-ima...
Downloads - File M...
Search | Splunk 9.1...
Tue 14 Nov, 03:13 sysadmin
Search | Splunk 9.1.1
Home - Bootcamp: U
22-Project-3/2 · main
ApacheLogs.png (864
localhost:8000/en-US/app/search/search?q=search%20source%3D"apache_attack_logs.txt"%20%7C%20top%20method&earliest=0&latest=&disp...
Update
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
Save As ▾ Create Table View Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events Patterns Statistics (4) Visualization
20 Per Page ▾ Format Preview ▾

New Search

```
source="apache_attack_logs.txt" | top method
```

✓ 4,497 events (before 11/14/23 3:13:29.000 AM)

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

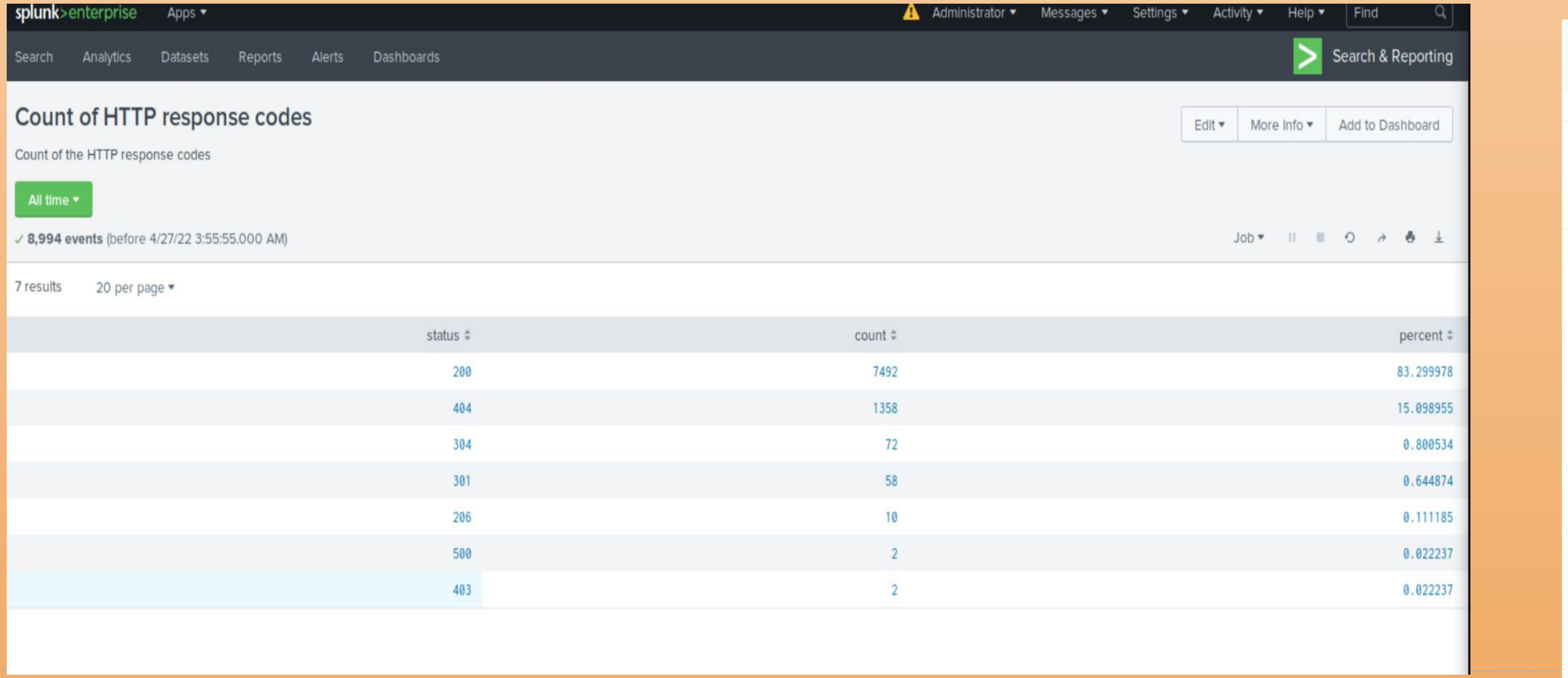

Search | Splunk 9.1.1
Home - Bootcamp: U
22-Project-3/2 · main
localhost:8000/en-US/app/search/search?q=search%20source%3D"apache_attack_logs.txt"%20host%3D"Apache%20Attack%20Logs"%20sourcety...
Update
Save As ▾ Create Table View Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events Patterns Statistics (10) Visualization
20 Per Page ▾ Format Preview ▾

New Search

```
source="apache_attack_logs.txt" host="Apache Attack Logs" sourcetype="access_combined"| top limit=10 referer_domain
```

✓ 4,497 events (before 11/14/23 3:31:26.000 AM)

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


splunk>enterprise Apps ▾
Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
Edit ▾ More Info ▾ Add to Dashboard
All time ▾
Job ▾
20 per page ▾

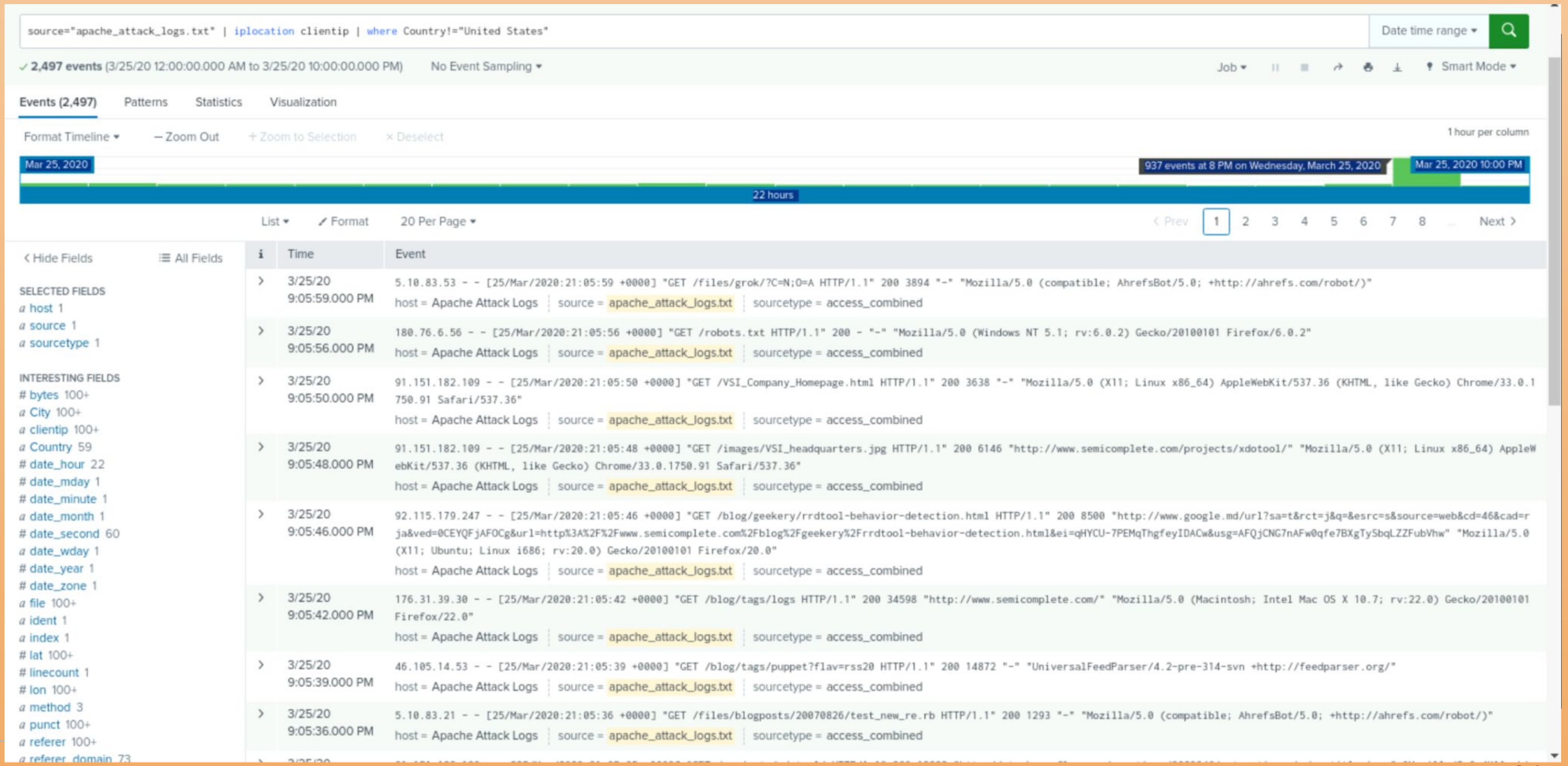
Count of HTTP response codes

Count of the HTTP response codes

✓ 8,994 events (before 4/27/22 3:55:55.000 AM)

7 results

status	count	percent
200	7492	83.299978
404	1358	15.098955
304	72	0.800534
301	58	0.644874
206	10	0.111185
500	2	0.022237
403	2	0.022237


Date time range ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events (2,497) Patterns Statistics Visualization
Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect
1 hour per column
Mar 25, 2020
937 events at 8 PM on Wednesday, March 25, 2020
Mar 25, 2020 10:00 PM
22 hours
List ▾ Format 20 Per Page ▾
‹ Prev 1 2 3 4 5 6 7 8 ... Next ›
‹ Hide Fields ☰ All Fields

```
source="apache_attack_logs.txt" | iplocation clientip | where Country!="United States"
```

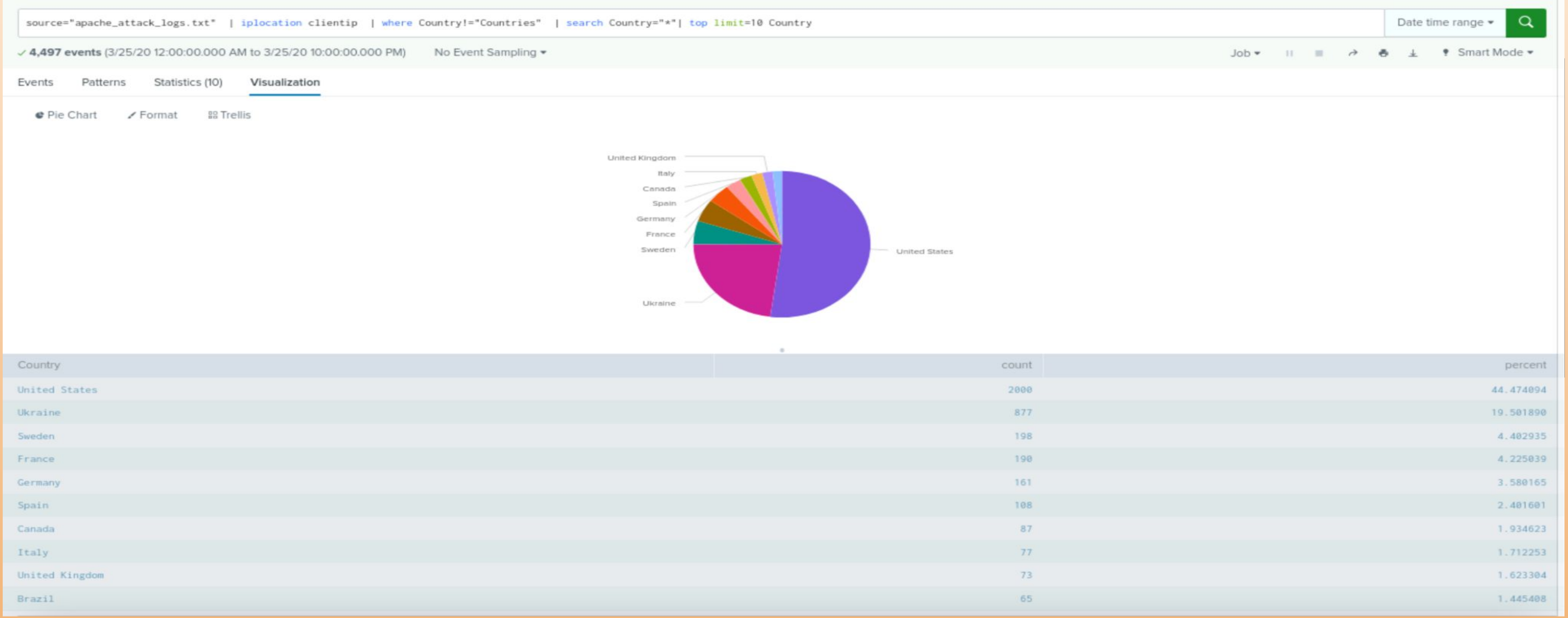
✓ 2,497 events (3/25/20 12:00:00.000 AM to 3/25/20 10:00:00.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bytes 100+
a City 100+
a clientip 100+
a Country 59
# date_hour 22
# date_mday 1
# date_minute 1
a date_month 1
# date_second 60
a date_wday 1
# date_year 1
# date_zone 1
a file 100+
a ident 1
a index 1
# lat 100+
# linecount 1
# lon 100+
a method 3
a punct 100+
a referer 100+
a referer_domain 73

```
i  Time                    Event
>  3/25/20 9:05:59.000 PM  5.10.83.53 - - [25/Mar/2020:21:05:59 +0000] "GET /files/grok/?C=N;O=A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)"
                           host = Apache Attack Logs | source = apache_attack_logs.txt | sourcetype = access_combined
>  3/25/20 9:05:56.000 PM  180.76.6.56 - - [25/Mar/2020:21:05:56 +0000] "GET /robots.txt HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"
                           host = Apache Attack Logs | source = apache_attack_logs.txt | sourcetype = access_combined
>  3/25/20 9:05:50.000 PM  91.151.182.109 - - [25/Mar/2020:21:05:50 +0000] "GET /VSI_Company_Homepage.html HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36"
                           host = Apache Attack Logs | source = apache_attack_logs.txt | sourcetype = access_combined
>  3/25/20 9:05:48.000 PM  91.151.182.109 - - [25/Mar/2020:21:05:48 +0000] "GET /images/VSI_headquarters.jpg HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36"
                           host = Apache Attack Logs | source = apache_attack_logs.txt | sourcetype = access_combined
>  3/25/20 9:05:46.000 PM  92.115.179.247 - - [25/Mar/2020:21:05:46 +0000] "GET /blog/geekery/rrdtool-behavior-detection.html HTTP/1.1" 200 8500 "http://www.google.md/url?sa=t&rct=j&q=&esrc=s&source=web&cd=46&cad=rja&ved=0CEYQFjAFOCg&url=http%3A%2F%2Fwww.semicomplete.com%2Fblog%2Fgeekery%2Frrdtool-behavior-detection.html&ei=qHYCU-7PEMqThgfeyIDACw&usg=AFQjCNG7nAFw0qfe7BXgTySbqLZZFubVhw" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:20.0) Gecko/20100101 Firefox/20.0"
                           host = Apache Attack Logs | source = apache_attack_logs.txt | sourcetype = access_combined
>  3/25/20 9:05:42.000 PM  176.31.39.30 - - [25/Mar/2020:21:05:42 +0000] "GET /blog/tags/logs HTTP/1.1" 200 34598 "http://www.semicomplete.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:22.0) Gecko/20100101 Firefox/22.0"
                           host = Apache Attack Logs | source = apache_attack_logs.txt | sourcetype = access_combined
>  3/25/20 9:05:39.000 PM  46.105.14.53 - - [25/Mar/2020:21:05:39 +0000] "GET /blog/tags/puppet?flav=rss20 HTTP/1.1" 200 14872 "-" "UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/"
                           host = Apache Attack Logs | source = apache_attack_logs.txt | sourcetype = access_combined
>  3/25/20 9:05:36.000 PM  5.10.83.21 - - [25/Mar/2020:21:05:36 +0000] "GET /files/blogposts/20070826/test_new_re.rb HTTP/1.1" 200 1293 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)"
                           host = Apache Attack Logs | source = apache_attack_logs.txt | sourcetype = access_combined
```

Images of Reports—Apache



```
source="apache_attack_logs.txt"  | iplocation clientip  | where Country!="Countries"  | search Country="*"| top limit=10 Country
```

✓ **4,497 events** (3/25/20 12:00:00.000 AM to 3/25/20 10:00:00.000 PM)

Country	count	percent
United States	2000	44.474094
Ukraine	877	19.501890
Sweden	198	4.402935
France	190	4.225039
Germany	161	3.580165
Spain	108	2.401601
Canada	87	1.934623
Italy	77	1.712253
United Kingdom	73	1.623304
Brazil	65	1.445408

There was a spike in POST method activity between 8 p.m. and 9 p.m. on Weds, March 25th, and had a count of 1,296 events. Yes the threshold was set at 200 counts and this would trigger it.
The United is leading cause of these events with a number of 2,000.

Alerts—Apache

Apache attacks from
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FApache%2520attacks%2520from%252...
Update
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit

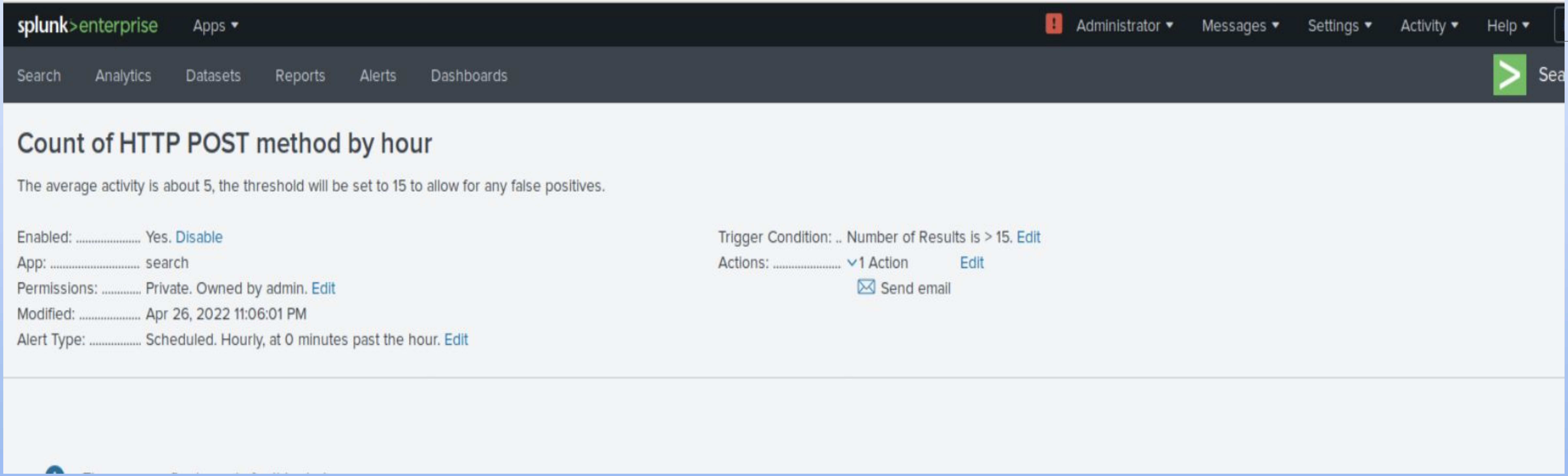
Apache attacks from not the US

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Nov 17, 2023 5:33:01 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 200. Edit
Actions: .... 1 Action Edit
Send email

* The average activity per hour was about 75.
* We concluded the threshold should be set for 200.
* We created an alert to change the search to one hour.
* Then we set it to run every hour.
* Our alert was to trigger when the count is greater than the agreed threshold of 200

Alerts—Apache



Count of HTTP POST method by hour

The average activity is about 5, the threshold will be set to 15 to allow for any false positives.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Apr 26, 2022 11:06:01 PM
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

* The average activity per hour is approximately 5.
* Therefore the threshold is set for 15.
* We created an alert and changed the search to one hour.
* We set it to run every hour.
* The alert was to trigger when the count is greater than the chosen threshold of 15.

Dashboards—Apache

HTTP methods
3,000
2,000
1,000
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
2:00 PM
3:00 PM
4:00 PM
5:00 PM
6:00 PM
7:00 PM
8:00 PM
9:00 PM
_time
GET
HEAD
OPTIONS
POST

```
source="apache_attack_logs.txt" | top limit=10 uri
```

✓ **4,497 events** (before 11/15/23 3:40:09.000 AM) No Event Sampling ▾

All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (10)
Visualization
Column Chart
Format
Trellis
1,500
1,000
500
count
/VSI_Account_logon.php
/files/logstash...-monolithic.jar
/VSI_Compan...mepage.html
/contactus.html
/images/VSI_...dquarters.jpg
/reset.css
/images/web/...9/banner.png
/blog/tags/puppet?flav=rss20
/projects/xdotool/
/?flav=rss20
uri
count

uri	count	percent
/VSI_Account_logon.php	1323	29.419613
/files/logstash/logstash-1.3.2-monolithic.jar	638	14.187236
/VSI_Company_Homepage.html	235	5.225706
/contactus.html	153	3.402268
/images/VSI_headquarters.jpg	152	3.380031

Attack Analysis

Attack Summary—Windows

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

- There was a drastic increase in severity with the high of 6.9 to a 20.22 and a decrease in information from 93 to 79.
- The cause of this change in severity came from higher success rates in activities like gaining privileges to the Windows server from 97 to 98.4; subtle, but any weak spot is enough for a company to go down.

Attack Summary—Windows

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

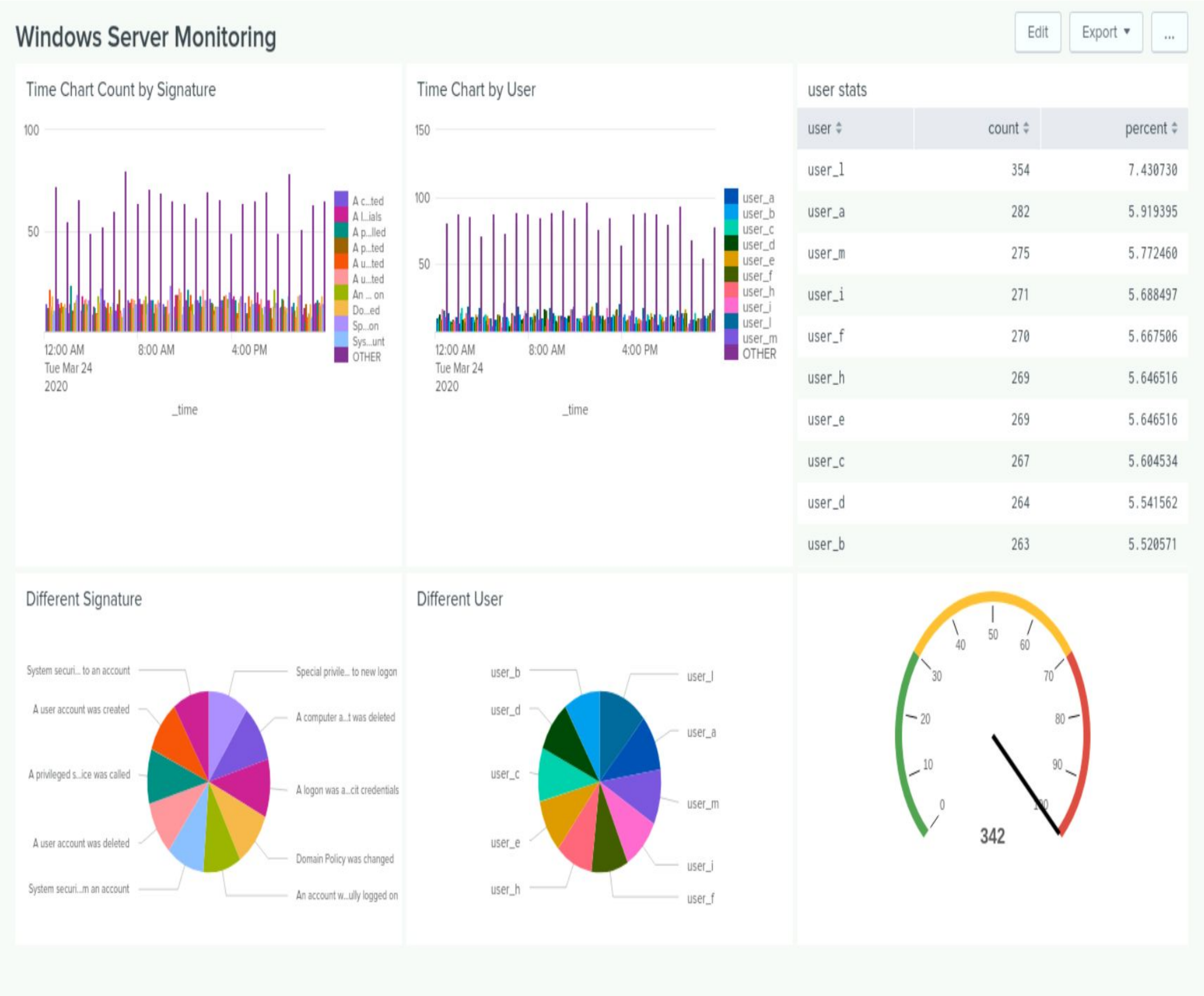
- There were three alerts we set up that notified us if specific conditions were met from those alerts we were able to be notified of suspicious number of,
  - Failed Windows Activities: there was a spike of 35 events occurring at from 8 a.m. and 9 a.m. on 03/25
  - Successful Logins: Average logins were typical around 10-25 per hour but at 11 a.m. there was 196 events and at 12 p.m. there was 77 events
  - Deleted Accounts: There was not a significant number of Deleted Accounts

Attack Summary—Windows

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

- Using the radial gauge, we were able to visualize the stats of each user of the Windows Server Monitoring as well as the user attack stats of how many events they are in in number form and percentage form.
- We used pie charts to narrow down what users were the most active in the sus activities.
- We used time charts for count by signature and by user. According to the signatures, the kind of activities were logging into the server or resetting passwords, changing computer user accounts or deleting them, and creating new users.

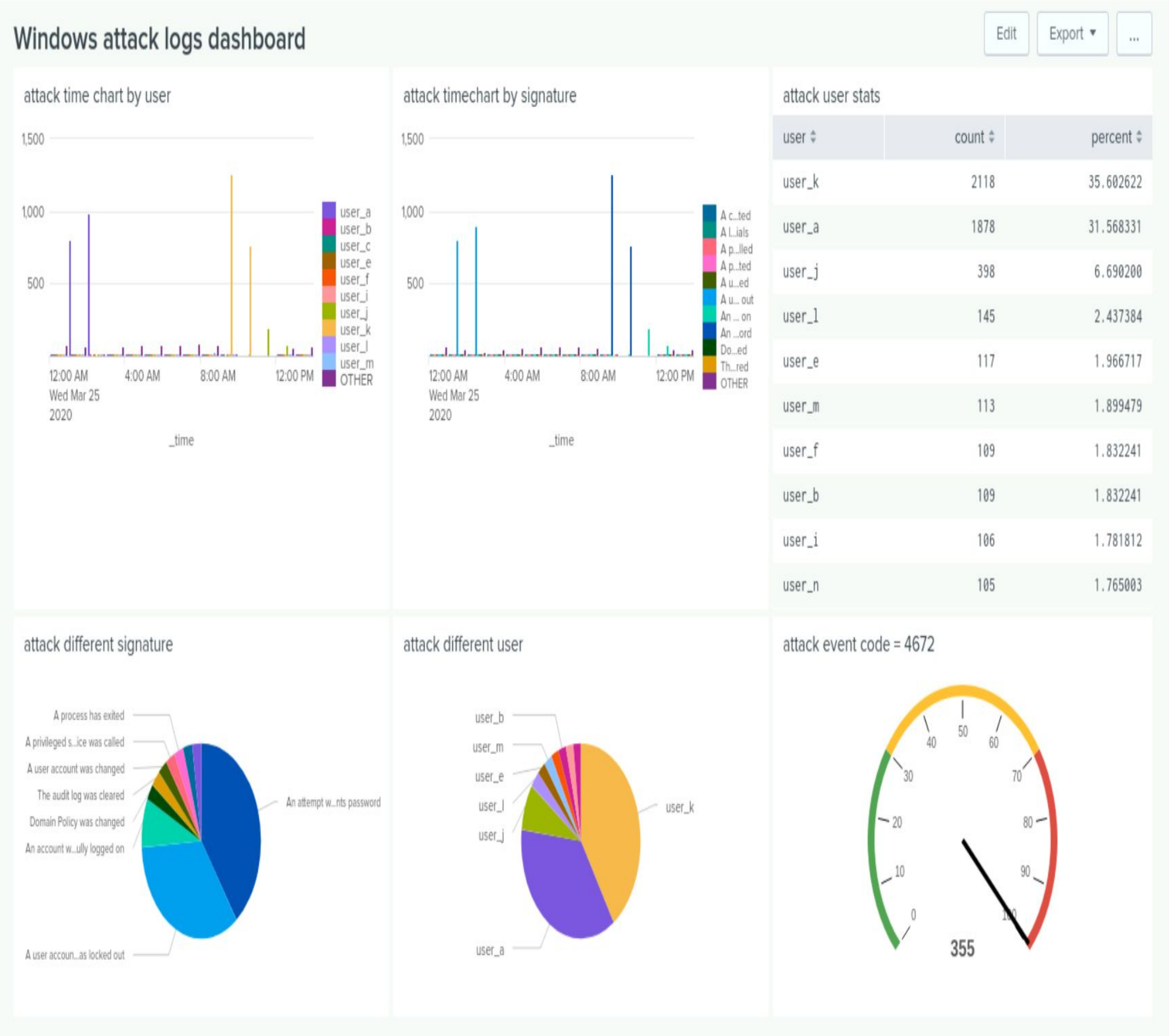
Screenshots of Attack Logs



Windows Server Monitoring

user stats

user ⇕	count ⇕	percent ⇕
user_l	354	7.430730
user_a	282	5.919395
user_m	275	5.772460
user_i	271	5.688497
user_f	270	5.667506
user_h	269	5.646516
user_e	269	5.646516
user_c	267	5.604534
user_d	264	5.541562
user_b	263	5.520571



Windows attack logs dashboard

attack user stats

user ⇕	count ⇕	percent ⇕
user_k	2118	35.602622
user_a	1878	31.568331
user_j	398	6.690200
user_l	145	2.437384
user_e	117	1.966717
user_m	113	1.899479
user_f	109	1.832241
user_b	109	1.832241
user_i	106	1.781812
user_n	105	1.765003

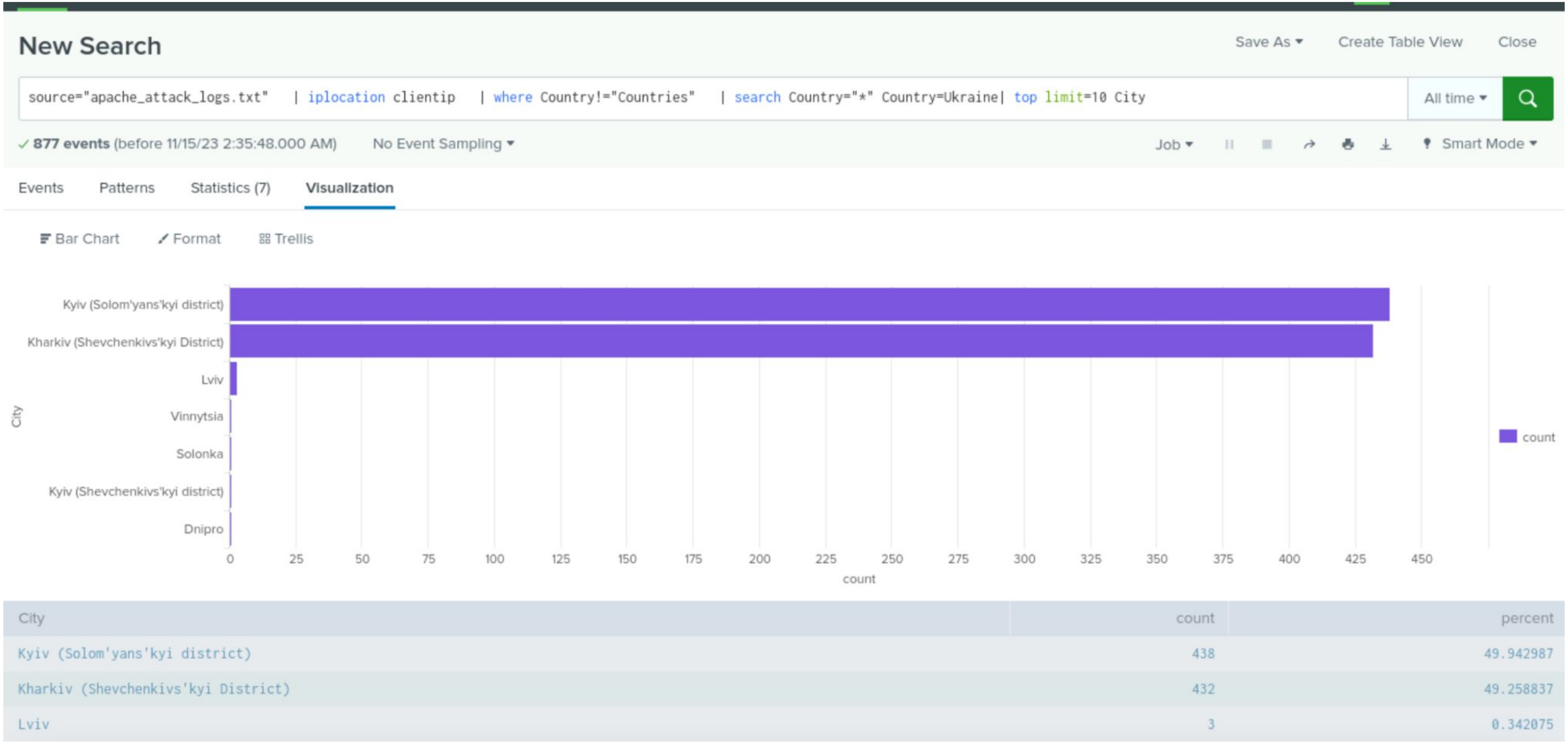
Attack Summary—Apache

- We reviewed the reports that show activity where the attackers were using HTTP POST and GET methods to brute force the VSI logon page.
- Detecting the increased/decrease in http response code such as 404 and 200.
- Analyzing High volumes of international countries of suspicious activity such as Ukraine.
- There were alerts for the POST method activity between 8PM and 9PM with around 1,296 events, which was raised from the normal event counts in the 100s, so we can summarize that this change is definitely suspicious and from attackers.

Attack Summary—Apache

- We made a pie chart for the top 10 countries that have a high volume in activity, and the visual shows that Ukraine came just behind the United States for unusual activity by attackers.
- Images of Count of Top HTTP Response Codes, illustrating which response codes are suspicious rising and decreasing rapidly out of the blue.
- The peak count of the top get method was 3,157 and the peak count for the POST method was 1,324.
- POST Method commenced at 8 p.m. and finished at 9 p.m. Get method began at 6 p.m. and ended at 7 p.m.

Screenshots of Attack Logs



```
source="apache_attack_logs.txt"   | iplocation clientip   | where Country!="Countries"   | search Country="*" Country=Ukraine| top limit=10 City
```

✓ 877 events (before 11/15/23 2:35:48.000 AM)

City	count	percent
Kyiv (Solom'yans'kyi district)	438	49.942987
Kharkiv (Shevchenkivs'kyi District)	432	49.258837
Lviv	3	0.342075

Summary and Future Mitigations

Project 3 Summary

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

Our findings indicate that VSI suffered multiple Brute force attacks from various regions resulting in compromised machines. The threat actors were able to escalate their privileges, delete accounts, passwords and view company data.

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

  As stated at the beginning of our slide show the add on Splunk Security Essentials for its user friendly design and tools to help with spotting and mitigating future attacks. We also recommend that employees use stronger passwords and have a login fail limit of no more than 3. We would also recommend IP blocking so that certain areas cannot access the companies web servers, or the use of a company VPN for remote employees.

THE END