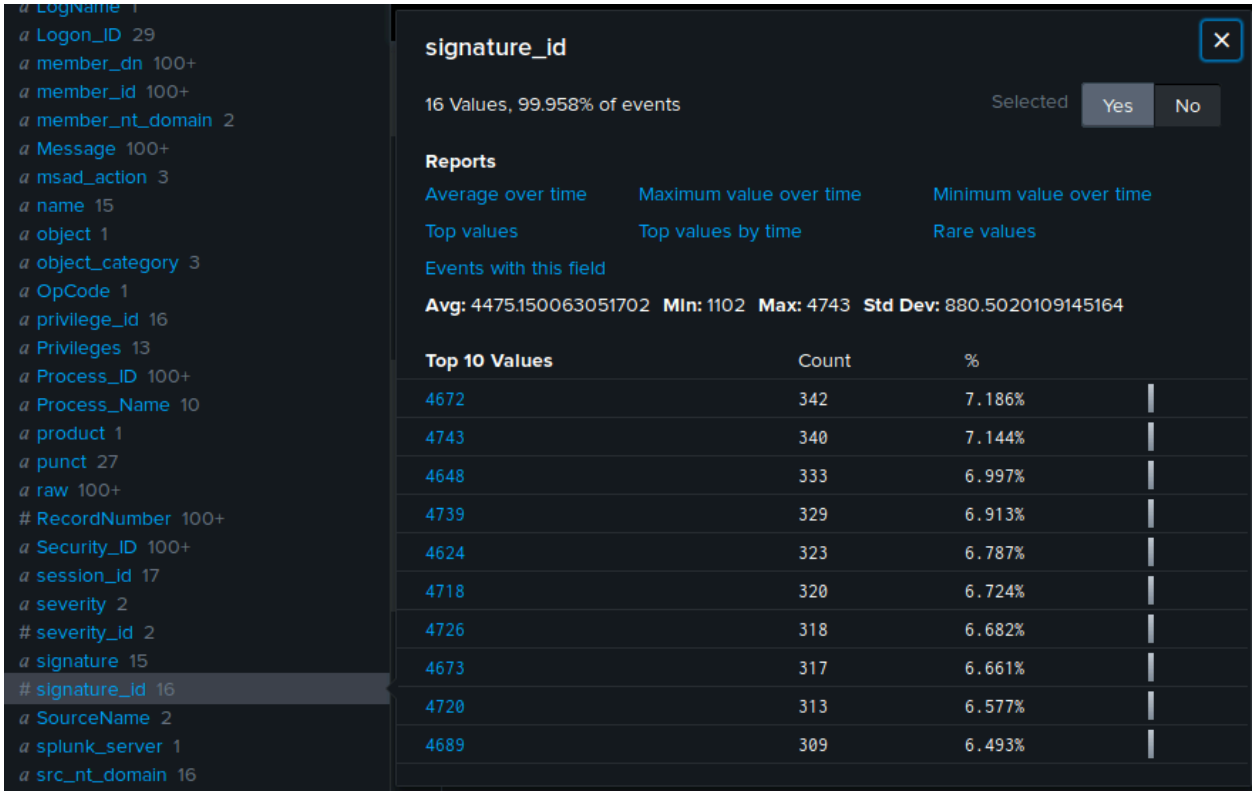
Cybersecurity

Project 3 Splunk Analysis

Make a copy of this document before you begin. Place your answers below each question.

Splunk Analysis File

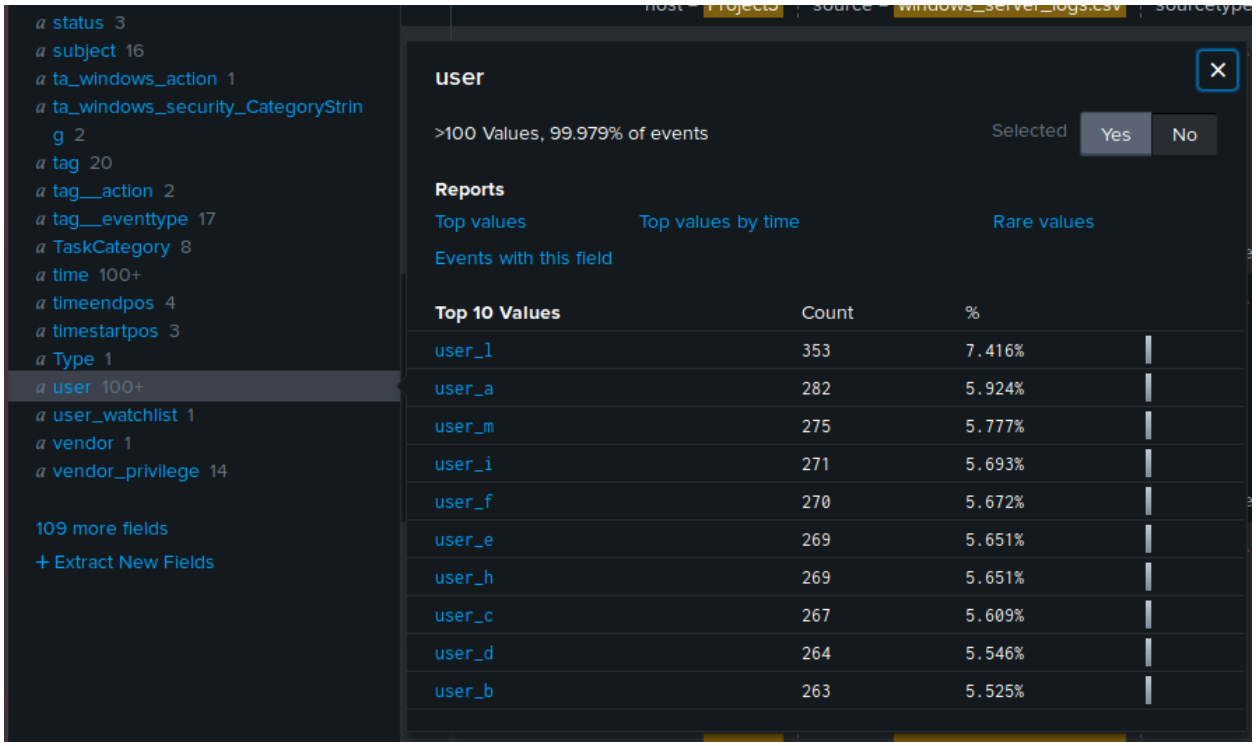
PART 1
SIGNATURE_ID



SIGNATURE


a OpCode 1
a privilege_id 16
a Privileges 13
a Process_ID 100+
a Process_Name 10
a product 1
a punct 27
a raw 100+
RecordNumber 100+
a Security_ID 100+
a session_id 17
a severity 2
severity_id 2
a signature 15
signature_id 16
a SourceName 2
a splunk_server 1
a src_nt_domain 16
a src_user 15
a src_user_watchlist 1
a status 3
a subject 16
a ta_windows_action 1
a ta_windows_security_CategoryStrin g 2
a tag 20
signature
15 Values, 99.937% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
Special privileges assigned to new logon 342 7.188%
A computer account was deleted 340 7.146%
A logon was attempted using explicit credentials 333 6.999%
Domain Policy was changed 329 6.915%
An account was successfully logged on 323 6.788%
System security access was removed from an account 320 6.726%
A user account was deleted 318 6.683%
A privileged service was called 317 6.662%
A user account was created 313 6.578%
A process has exited 309 6.494%

USER


a status 3
a subject 16
a ta_windows_action 1
a ta_windows_security_CategoryStrin g 2
a tag 20
a tag__action 2
a tag__eventtype 17
a TaskCategory 8
a time 100+
a timeendpos 4
a timestartpos 3
a Type 1
a user 100+
a user_watchlist 1
a vendor 1
a vendor_privilege 14
109 more fields
+ Extract New Fields
user
>100 Values, 99.979% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
user_l 353 7.416%
user_a 282 5.924%
user_m 275 5.777%
user_i 271 5.693%
user_f 270 5.672%
user_e 269 5.651%
user_h 269 5.651%
user_c 267 5.609%
user_d 264 5.546%
user_b 263 5.525%

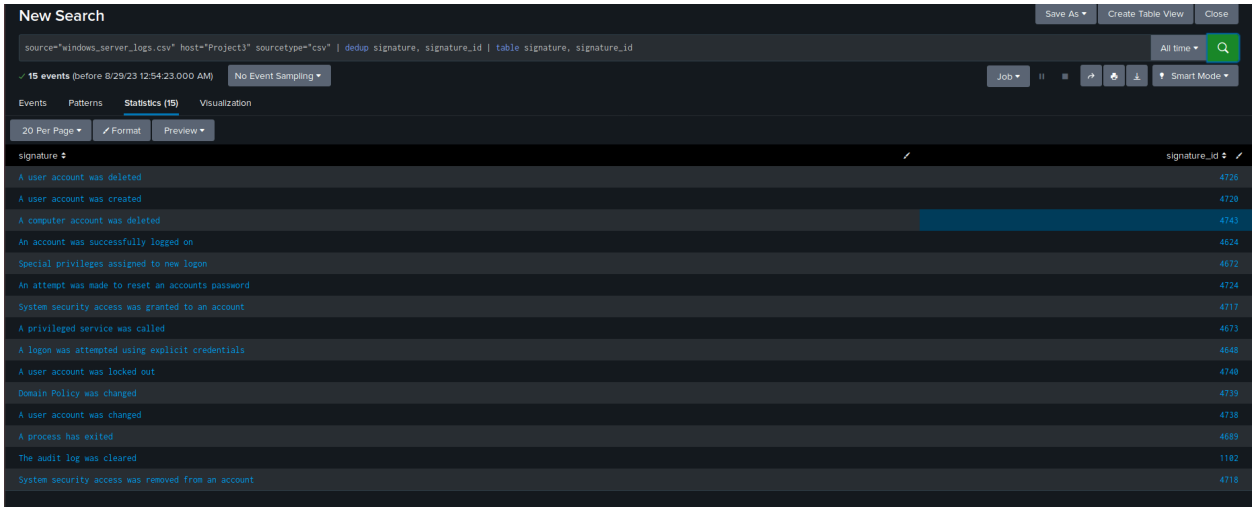
STATUS

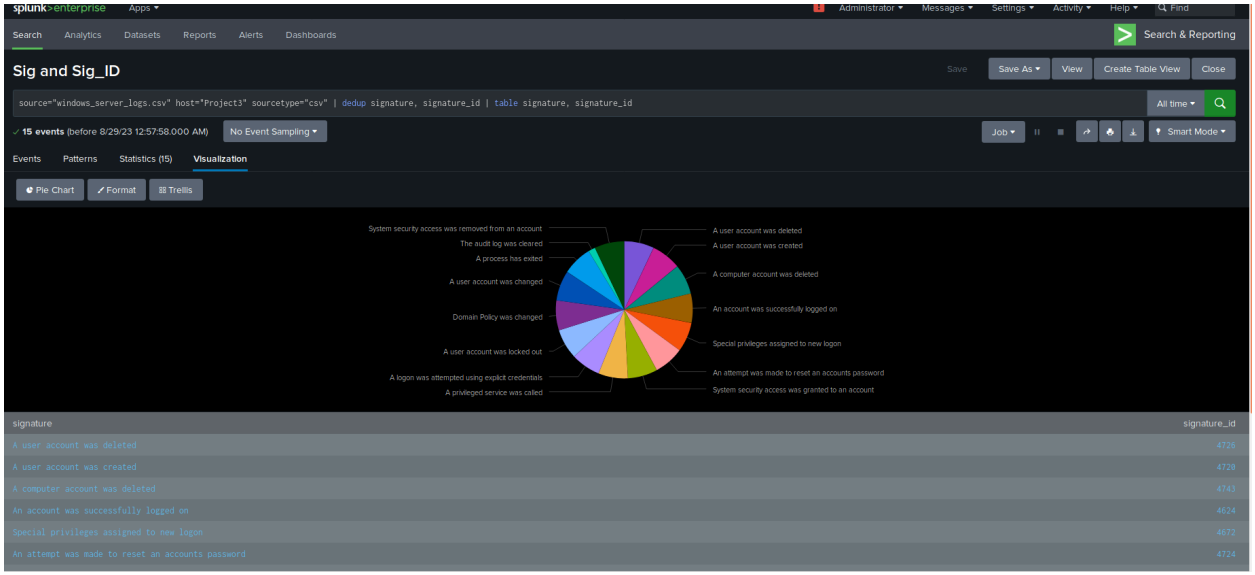
SEVERITY

PART 2

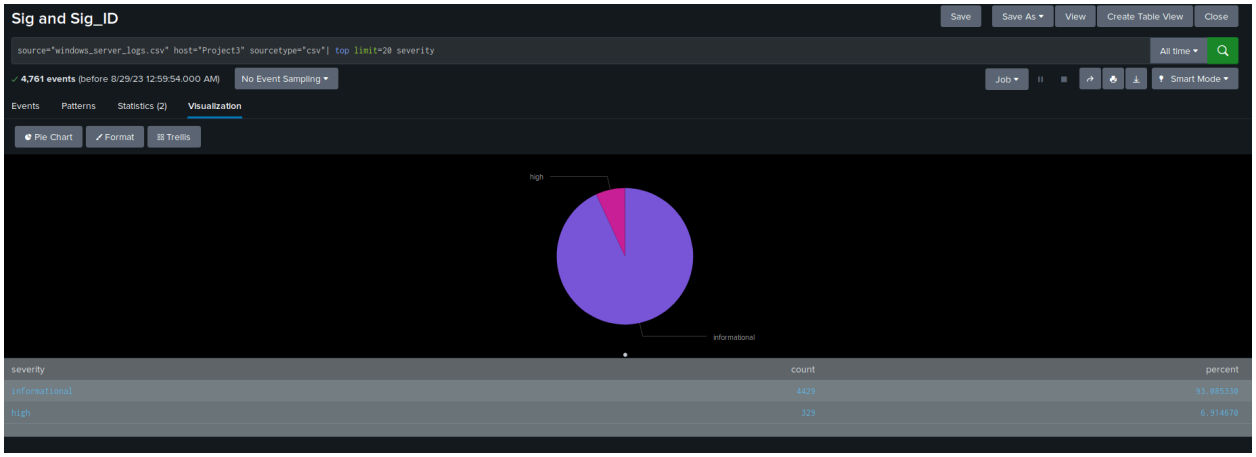
REPORT 1

source="windows_server_attack_logs.csv" host="Linux_Server" sourcetype="csv" | dedup signature, signature_id | table signature, signature_id

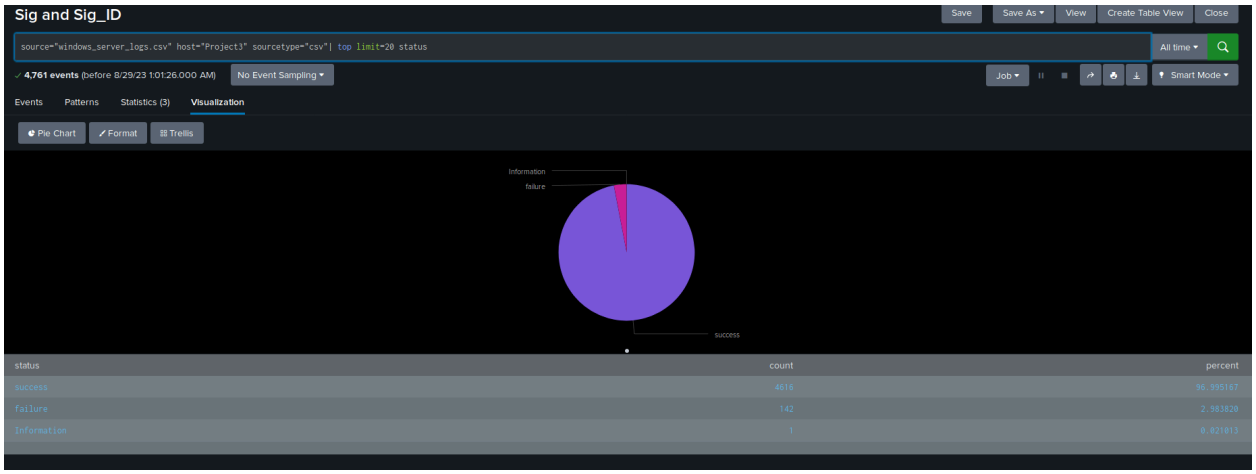




REPORT 2

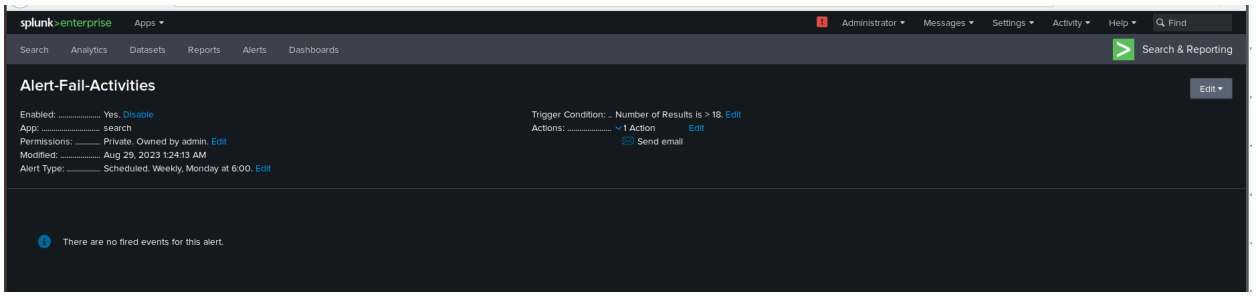


REPORT 3

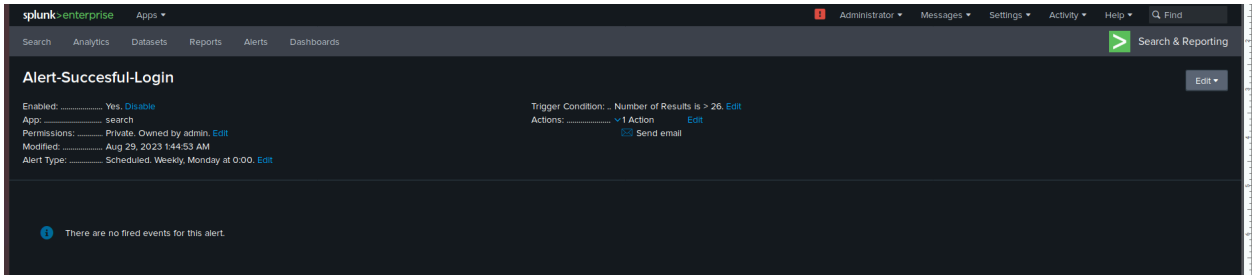


ALERTS

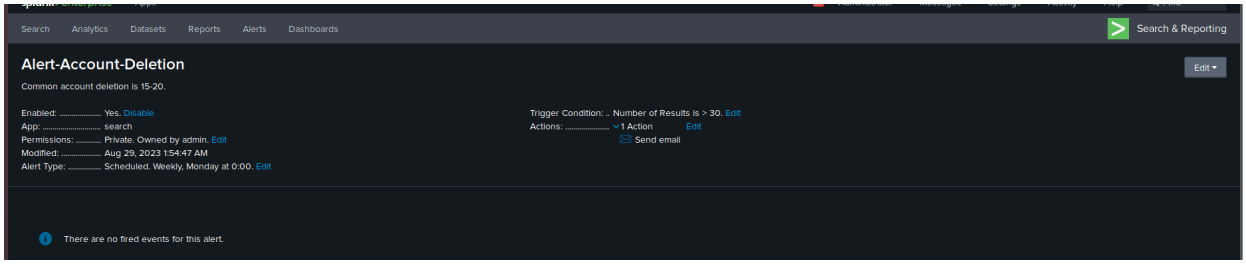
Alert-Fail- Activities



SECOND ALERT
Successful logins

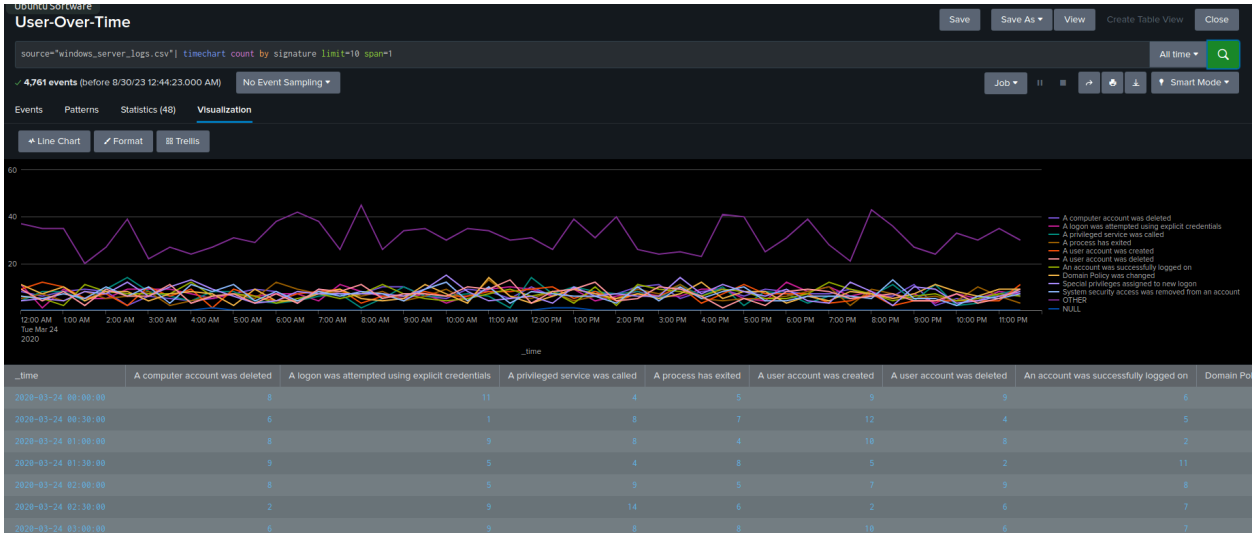


THIRD ALERT
Account deletion

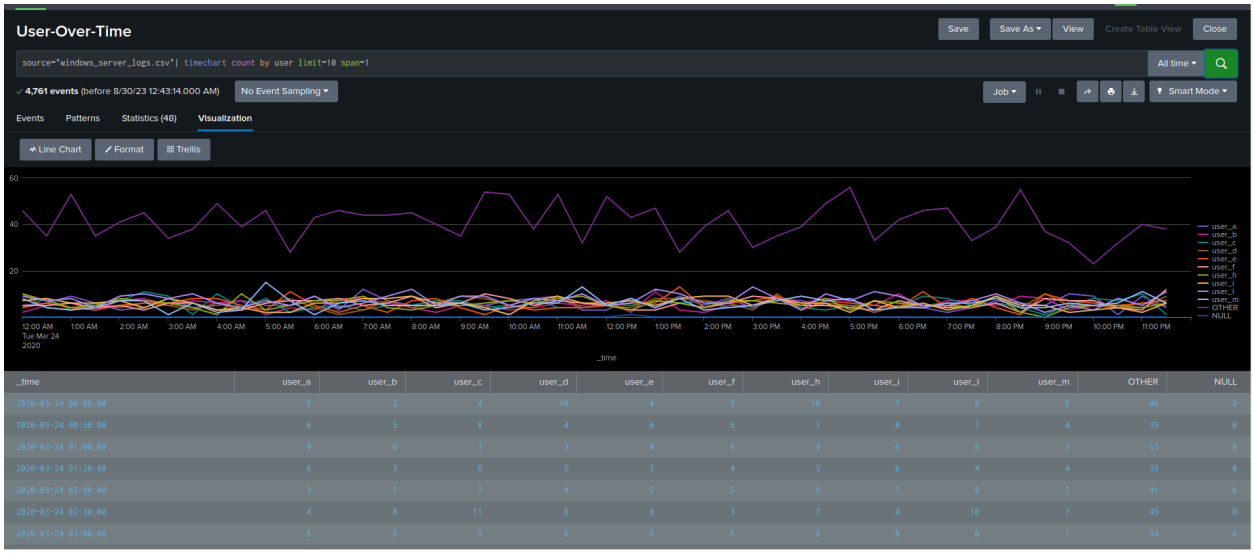


Dashboard

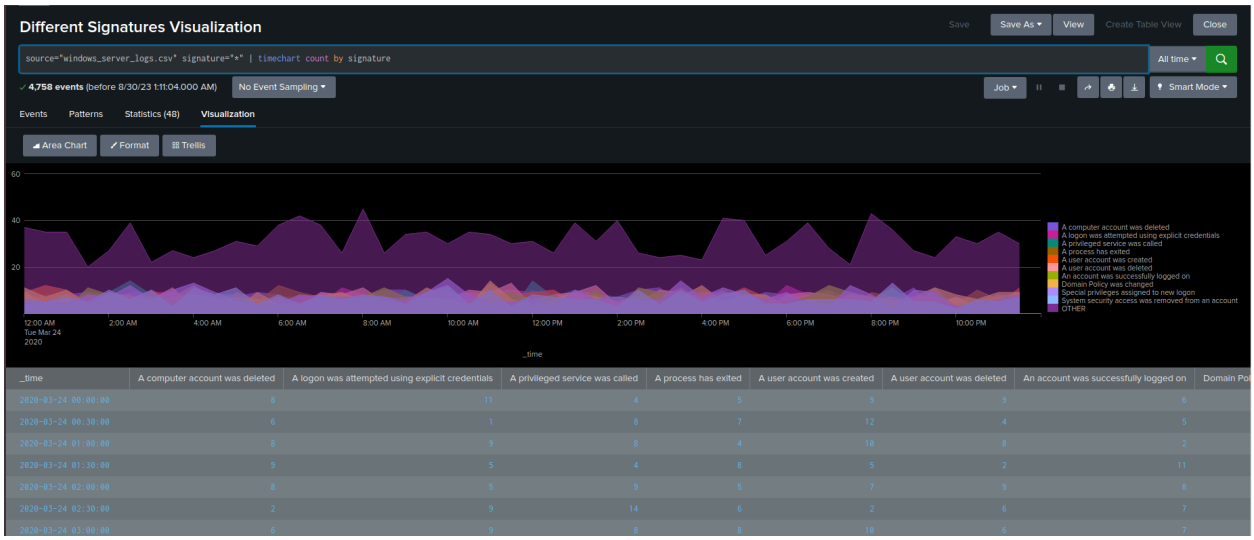
By Signature over time



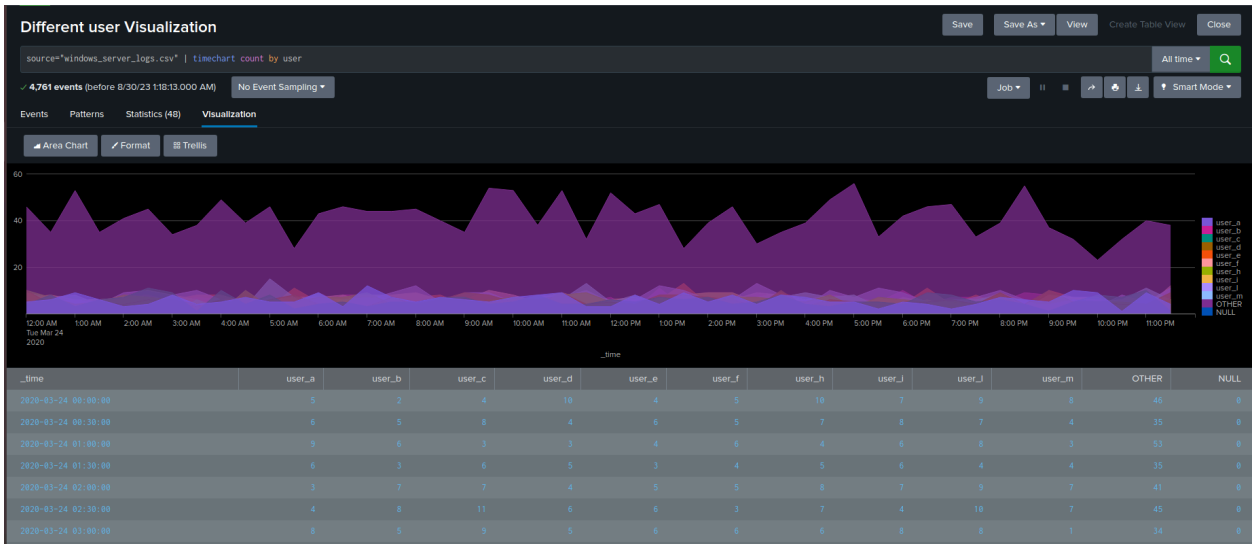
By User over time



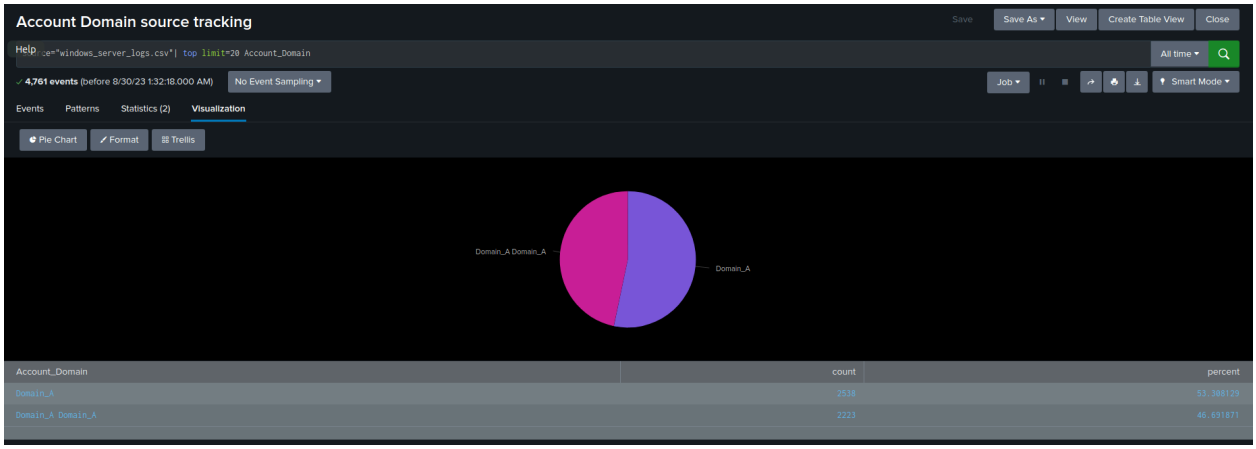
Count by different signatures



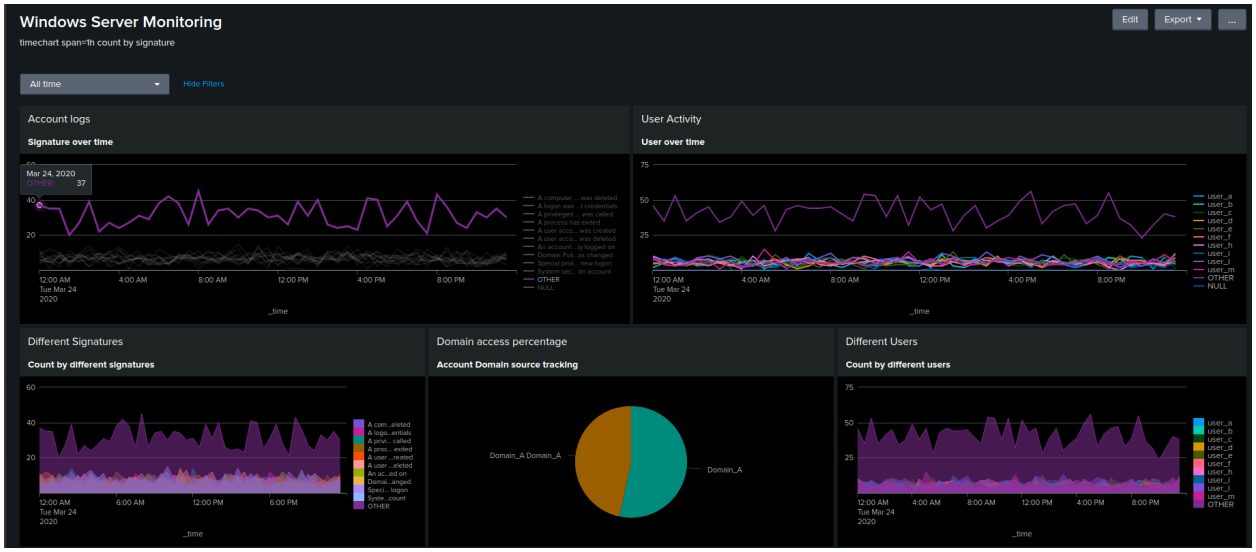
Count by different users



Account Domain source tracking

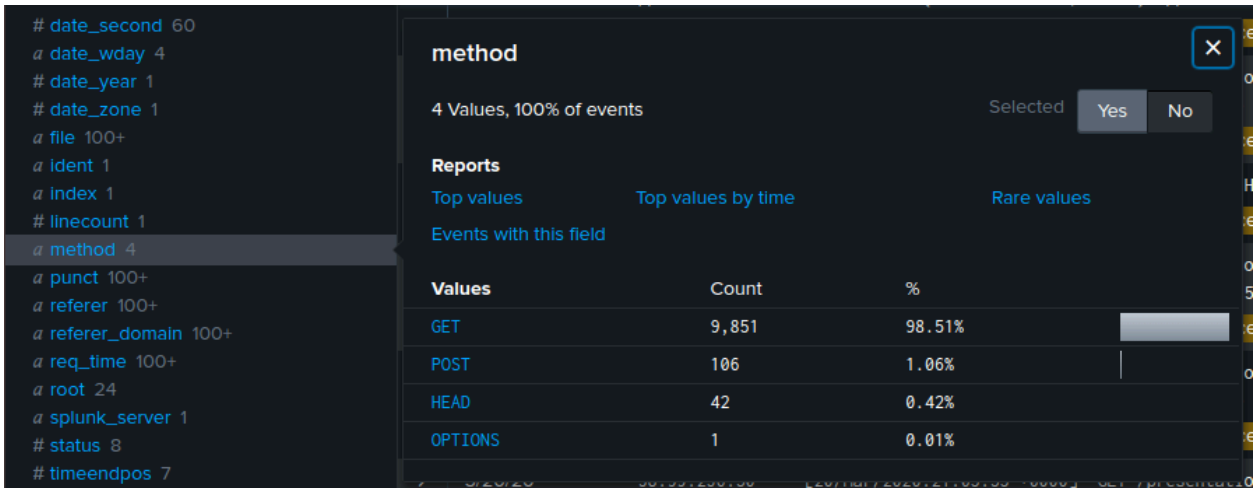


Dashboard



PART 3

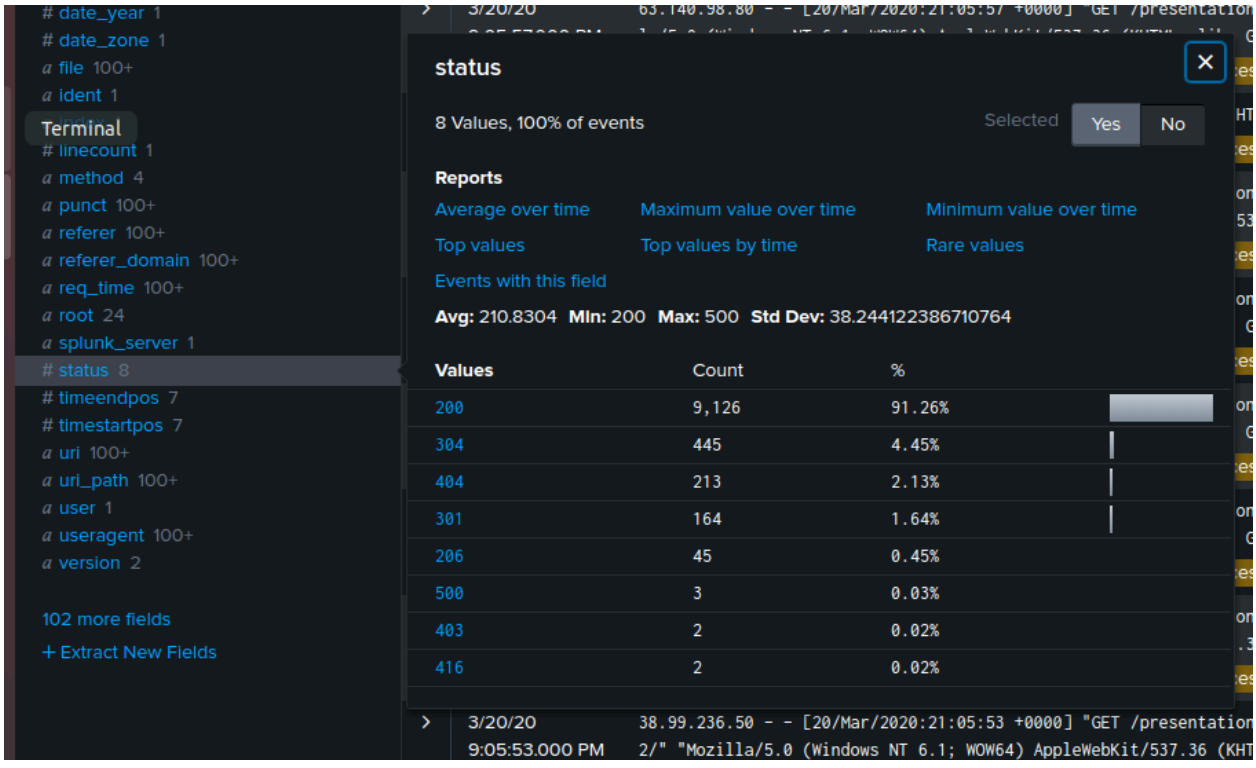
- Method



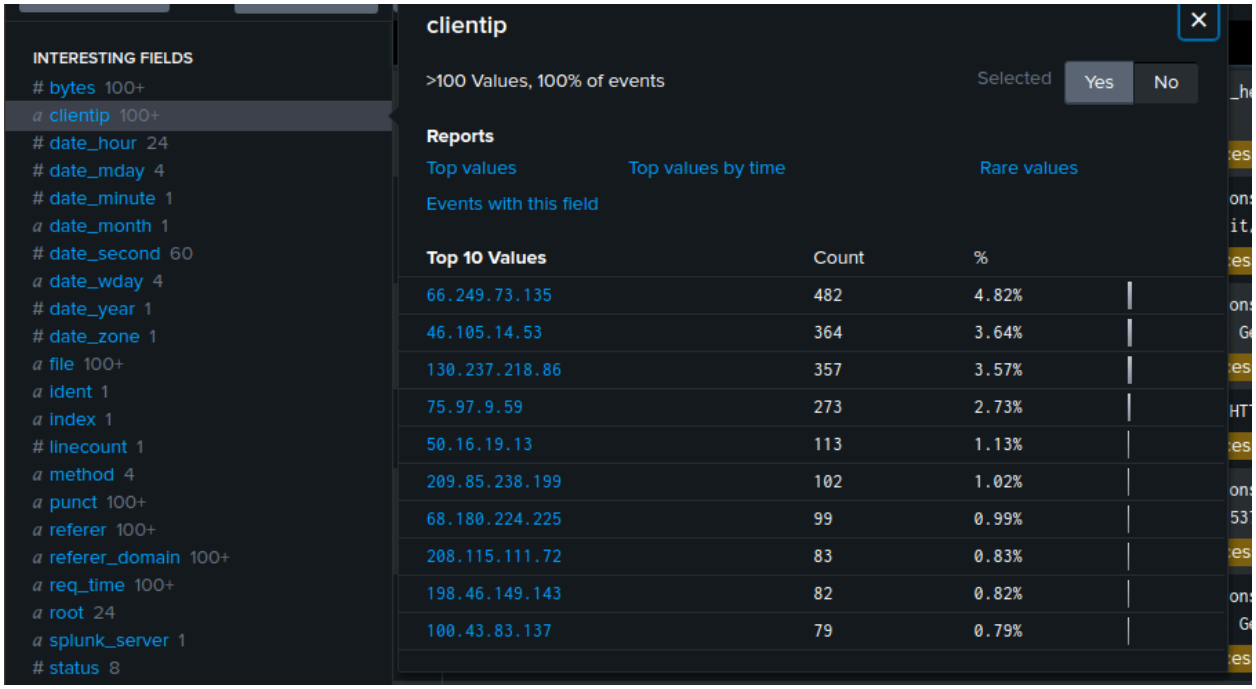
- Referer_domain


a date_month 1
date_second 60
a date_wday 4
date_year 1
date_zone 1
a file 100+
a ident 1
a index 1
linecount 1
a method 4
a punct 100+
a referer 100+
a referer_domain 100+
a req_time 100+
a root 24
a splunk_server 1
status 8
timeendpos 7
timestartpos 7
a uri 100+
a uri_path 100+
a user 1
a useragent 100+
a version 2
referer_domain
>100 Values, 59.27% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
http://www.semicomplete.com 3,038 51.257%
http://semicomplete.com 2,001 33.761%
http://www.google.com 123 2.075%
https://www.google.com 105 1.772%
http://stackoverflow.com 34 0.574%
http://www.google.fr 31 0.523%
http://s-chassis.co.nz 29 0.489%
http://logstash.net 28 0.472%
http://www.google.es 25 0.422%
https://www.google.co.uk 23 0.388%

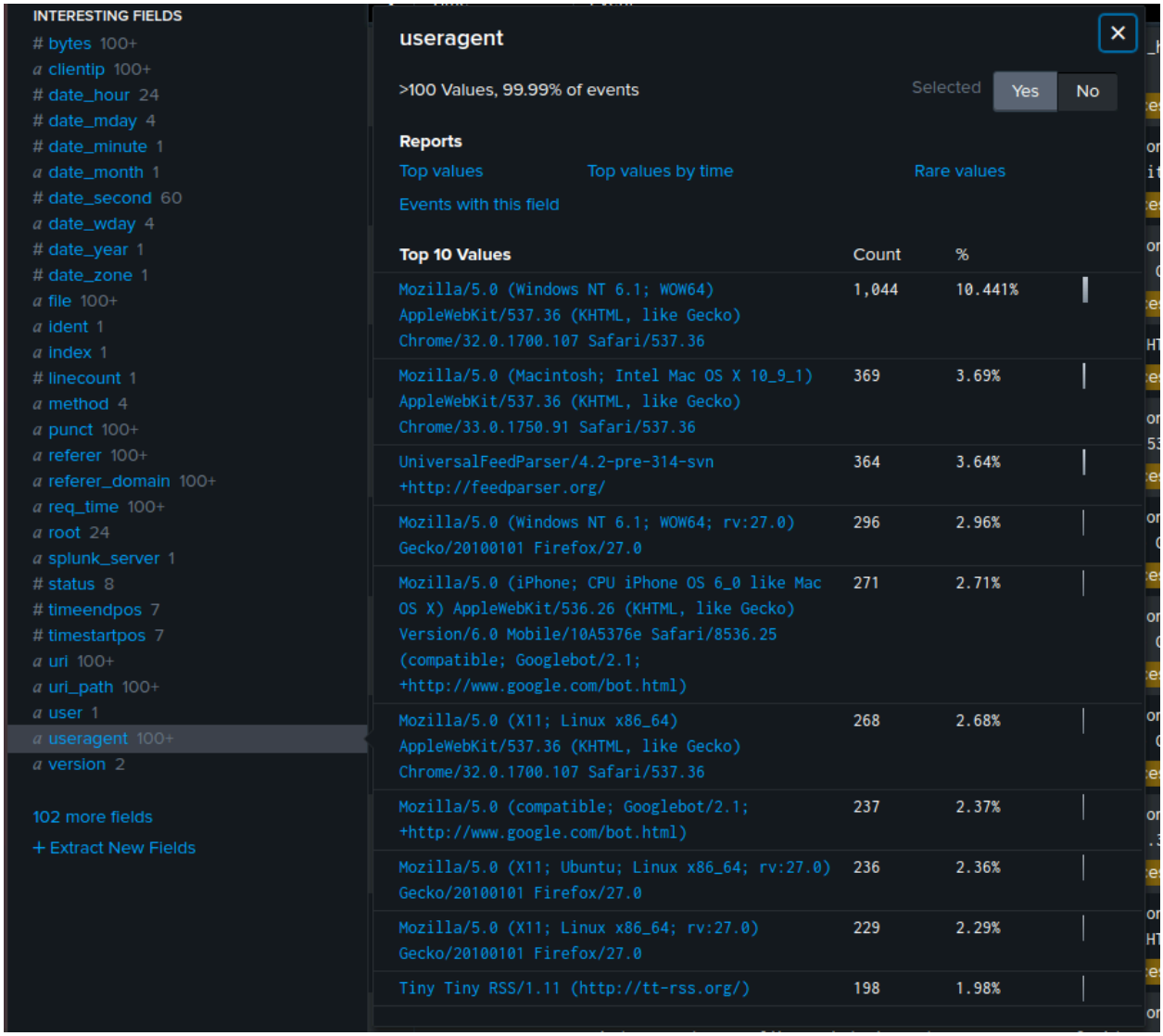
- Status


a file 100+
a ident 1
Terminal
linecount 1
a method 4
a punct 100+
a referer 100+
a referer_domain 100+
a req_time 100+
a root 24
a splunk_server 1
status 8
timeendpos 7
timestartpos 7
a uri 100+
a uri_path 100+
a user 1
a useragent 100+
a version 2
102 more fields
+ Extract New Fields
status
8 Values, 100% of events
Selected
Yes
No
Reports
Average over time
Maximum value over time
Minimum value over time
Top values
Top values by time
Rare values
Events with this field
Avg: 210.8304 Min: 200 Max: 500 Std Dev: 38.244122386710764
Values
Count
%
200 9,126 91.26%
304 445 4.45%
404 213 2.13%
301 164 1.64%
206 45 0.45%
500 3 0.03%
403 2 0.02%
416 2 0.02%
3/20/20 9:05:53.000 PM
38.99.236.50 - - [20/Mar/2020:21:05:53 +0000] "GET /presentation
2/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHT

- Clientip

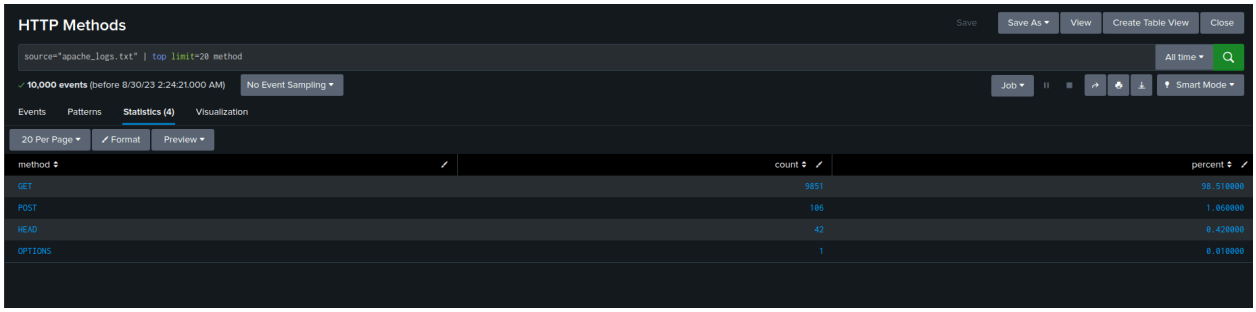


- Useragent

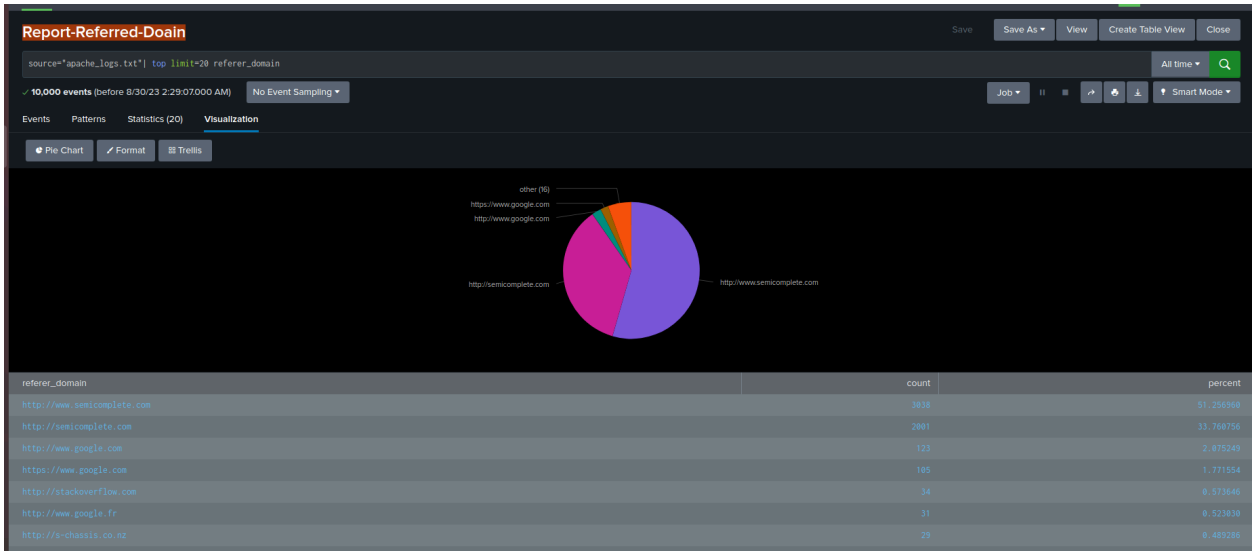


PART 4

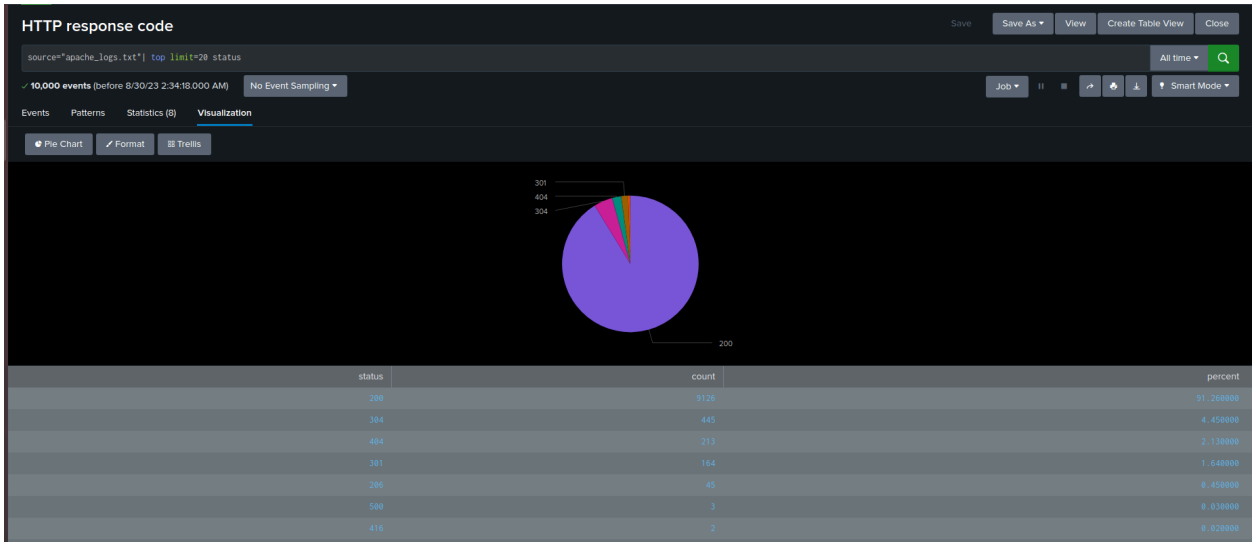
a. HTTP methods (GET, POST, HEAD, etc.).



Report-Referred-DOMAIN

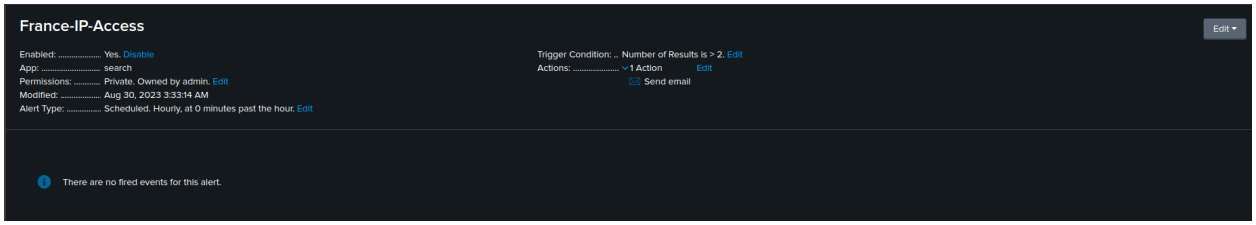


a. HTTP response code

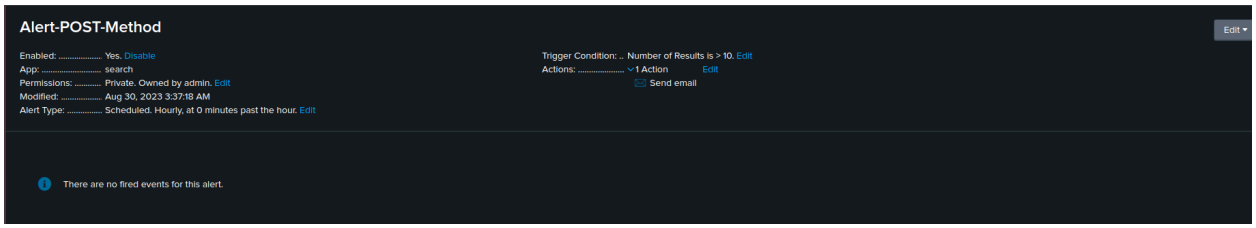


ALERTS

France-IP-Access

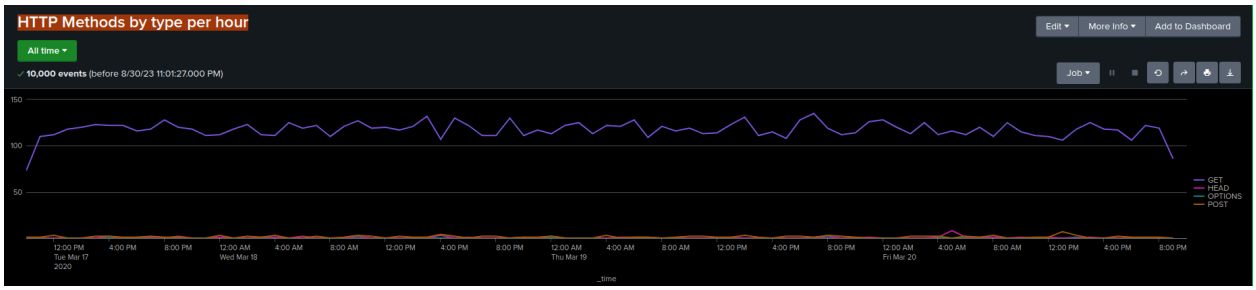


Alert-POST-Method

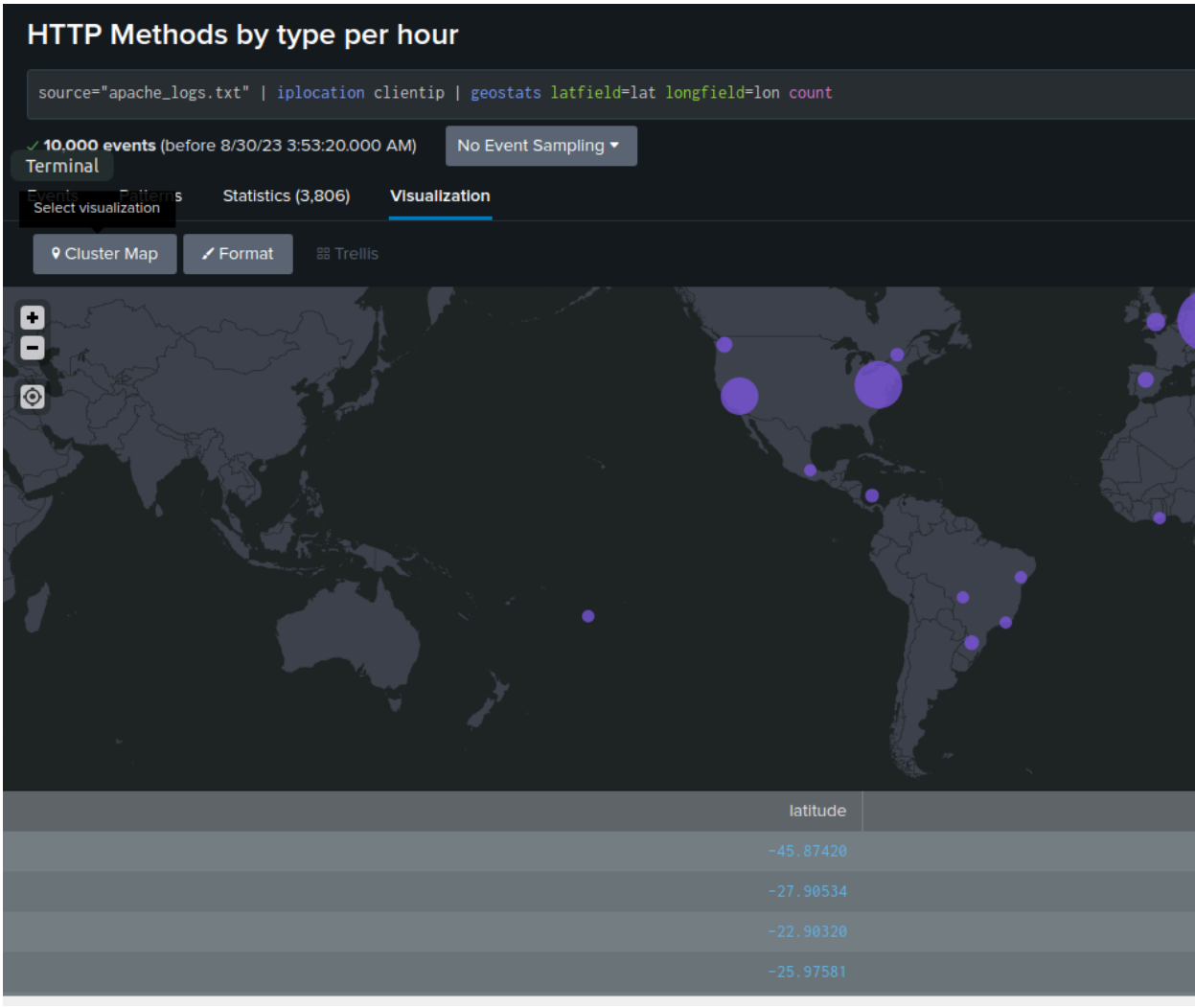


- **Visualizations and dashboards**

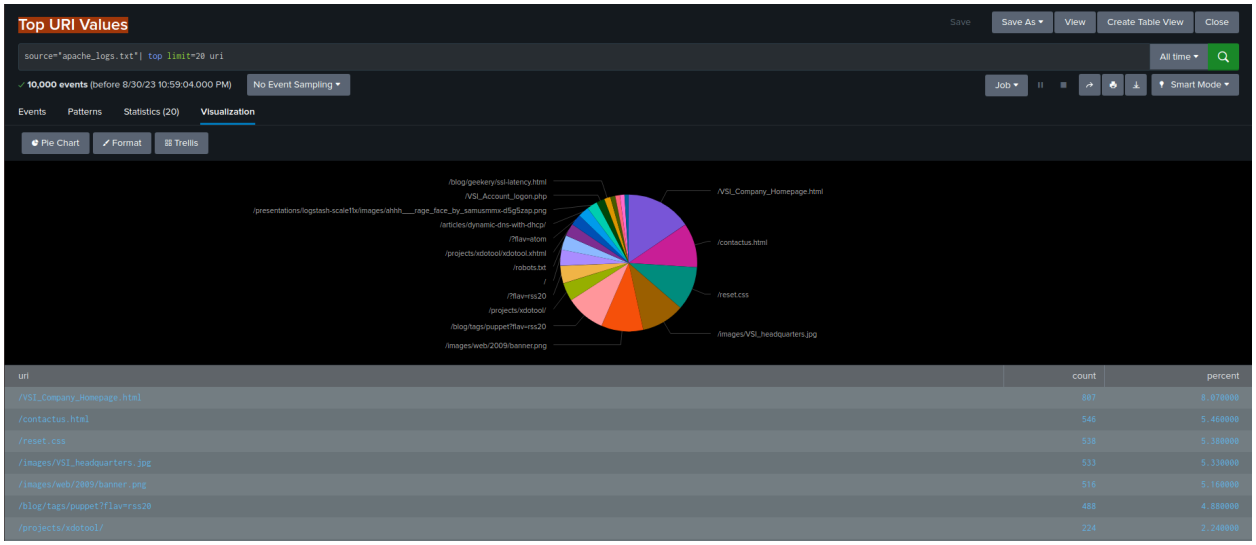
2. HTTP Methods by type per hour



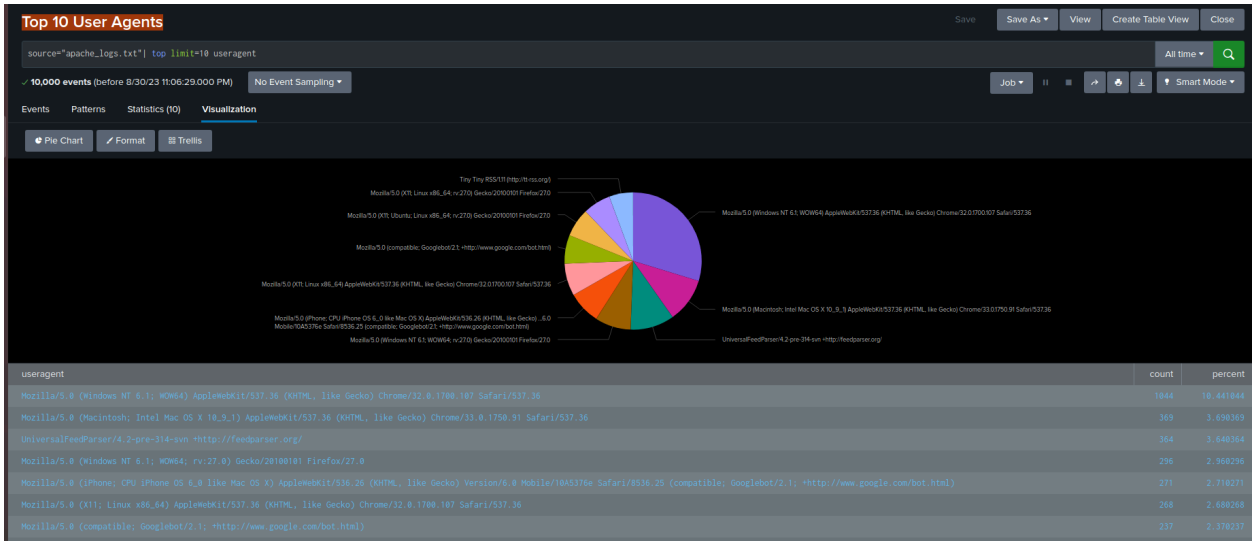
a. geographical map showing the location based on the “clientip” field



2. Top URI Values



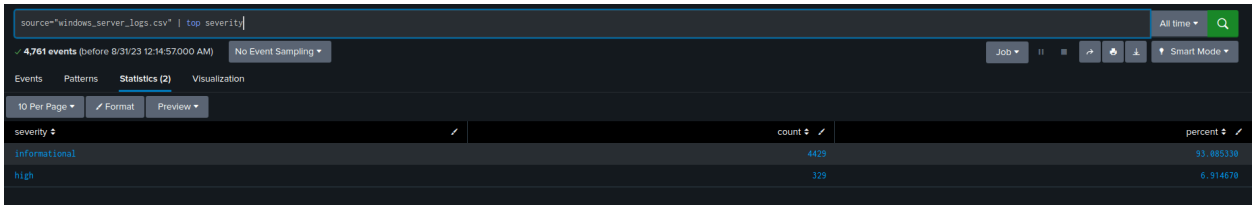
Top 10 User Agents



SPLUNK DAY 2

—

TOP SEVERITY- LOGS



TOP SEVERITY- ATTACKS

Did you detect any suspicious changes in severity?

Info- We see a change of 13 percent in decrease from 93% to 80%

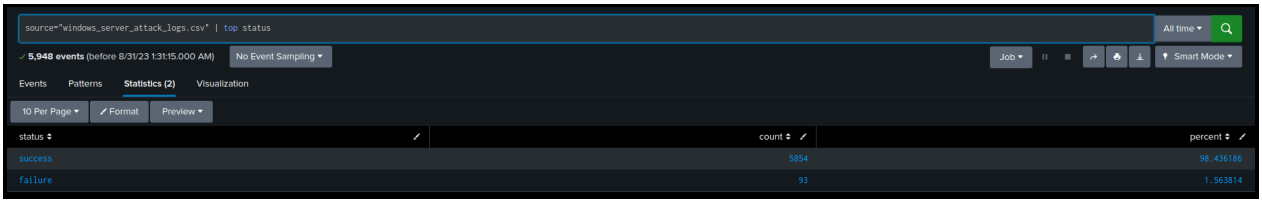
Level High- We see a change of 13 percent increase from 7% to 20%

Based on this information it suggests there are suspicious changes in severity.

Alert Analysis for Failed Windows Activity

LOGS

Attack logs



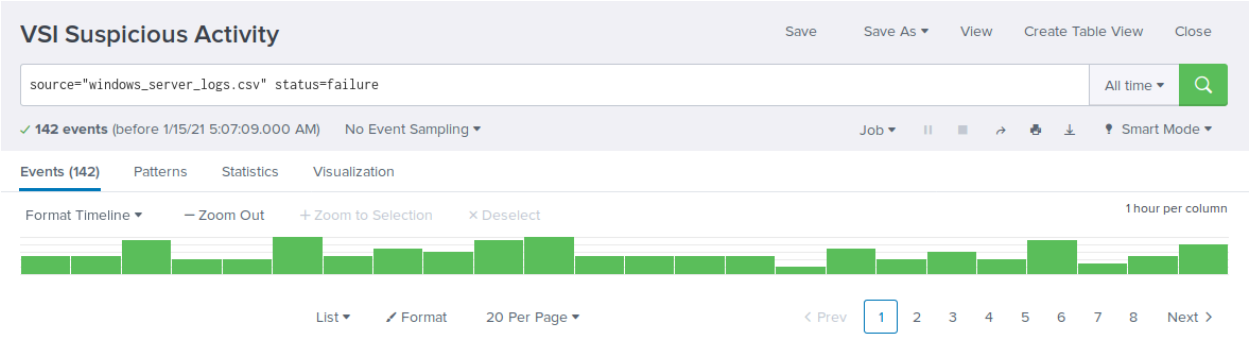
Did you detect any suspicious changes in failed activities?

Success: Notice a 1% increase from 97% to 98%.

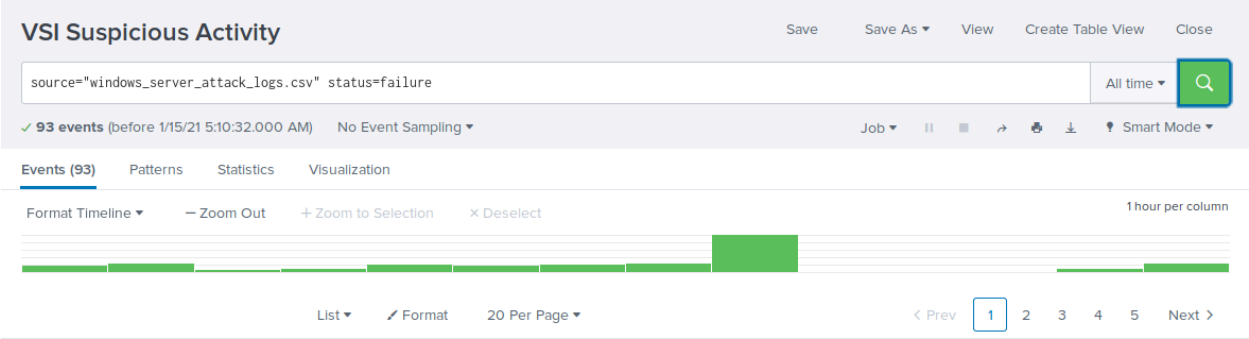
Failure: Notice a decrease of 1% from 3% to 2%.

Based on these results we see no major changes in failed activities.

Log Failures



Attack logs



S

Did you detect a suspicious volume of failed activity?

There was potential for a suspicious volume of failed activity at 8:00 a.m. on Wednesday, March 25th.

If so, what was the count of events in the hour(s) it occurred?

The count of activity was 35 events during this hour.

When did it occur?

8:00 a.m. on Wednesday, March 25th.

Would your alert be triggered for this activity?

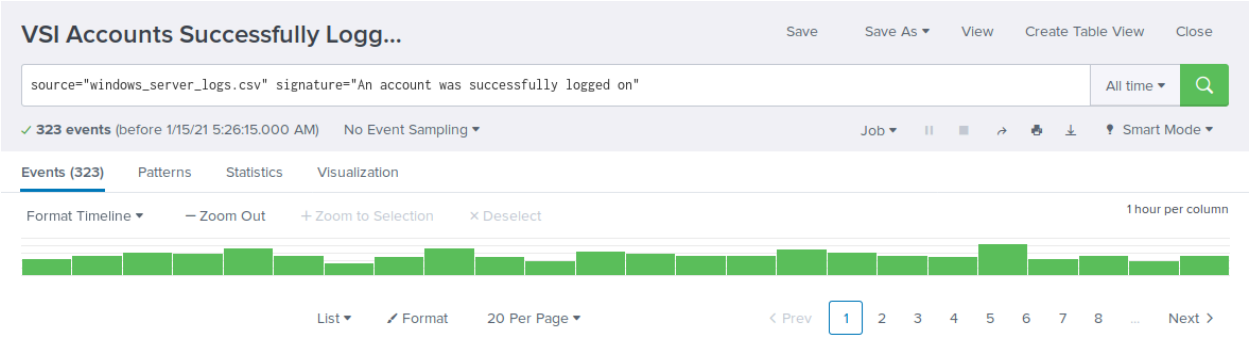
Yes, the alert is within the trigger threshold.

After reviewing, would you change your threshold from what you previously selected?

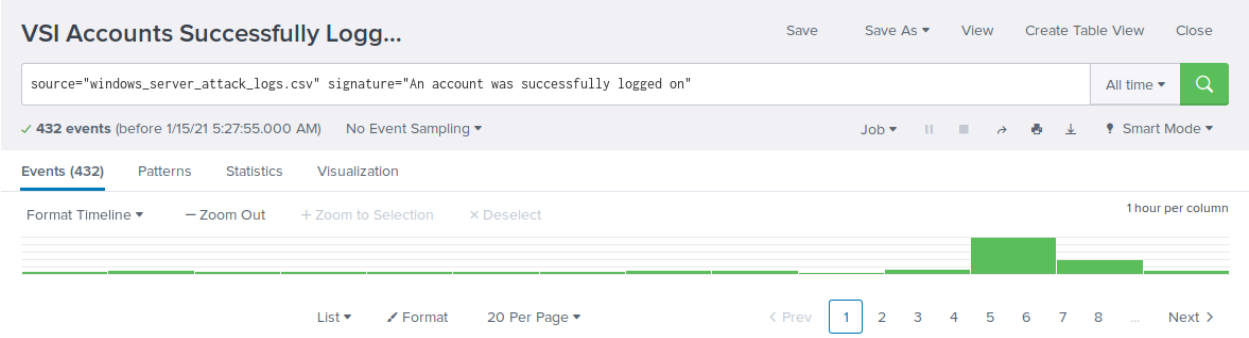
No change in threshold necessary.

Alert Analysis Successful logins

Logs



Attack Logs



Did you detect a suspicious volume of successful logons?

There was potential for suspicious activity at 11:00 a.m. and 12:00 p.m. on Wednesday, March 25th.

If so, what was the count of events in the hour(s) it occurred?

The count of activity is 196 events at 11:00 a.m. and 77 events at 12:00 p.m.

Who is the primary user logging in?

The primary user logging in was user_j.

When did it occur?

The suspicious activities occurred at 11:00 a.m. and 12:00 p.m. on Wednesday, March 25th.

Would your alert be triggered for this activity?

Yes, the alert is within the trigger threshold.

After reviewing, would you change your threshold from what you previously selected?

No change in threshold necessary.

Alert Analysis for Deleted Accounts.

Splunk: Building a Secure Monitoring Solution (Part 1) - DEV Community

Splunk: Building a Secure Monitoring Solution (Part 2) - DEV Community