



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_id

16 Values, 99.958% of events

Selected

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: 4475.150063051702 **Min:** 1102 **Max:** 4743 **Std Dev:** 880.5020109145164

Top 10 Values	Count	%
4672	342	7.186%
4743	340	7.144%
4648	333	6.997%
4739	329	6.913%
4624	323	6.787%
4718	320	6.724%
4726	318	6.682%
4673	317	6.661%
4720	313	6.577%
4689	309	6.493%

SIGNATURE

STATUS

a src_user 15	Top values	Top values by time	Rare values
a src_user_watchlist 1	Events with this field		
a status 3	Values	Count	%
a subject 16	success	4,616	96.995%
a ta_windows_action 1	failure	142	2.984%
a ta_windows_security_CategoryString 2	Information	1	0.021%
a tag 20			
a tag__action 2			
a tag__eventtype 17			

SEVERITY

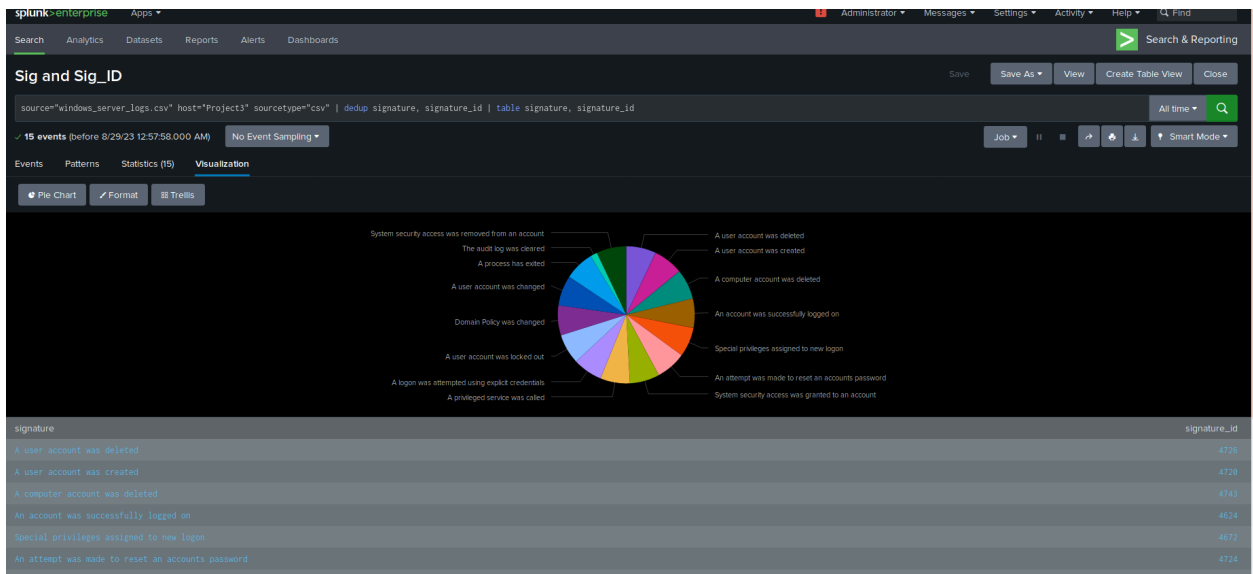
a product 1	severity		
a punct 27	2 Values, 99.937% of events		
a raw 100+	Selected Yes No		
# RecordNumber 100+	Reports		
a Security_ID 100+	Top values	Top values by time	Rare values
a session_id 17	Events with this field		
a severity 2	Values	Count	%
# severity_id 2	informational	4,429	93.085%
a signature 15	high	329	6.915%
# signature_id 16			
a SourceName 2			
a splunk_server 1			
a src_nt_domain 16			
a src_user 15			

PART 2

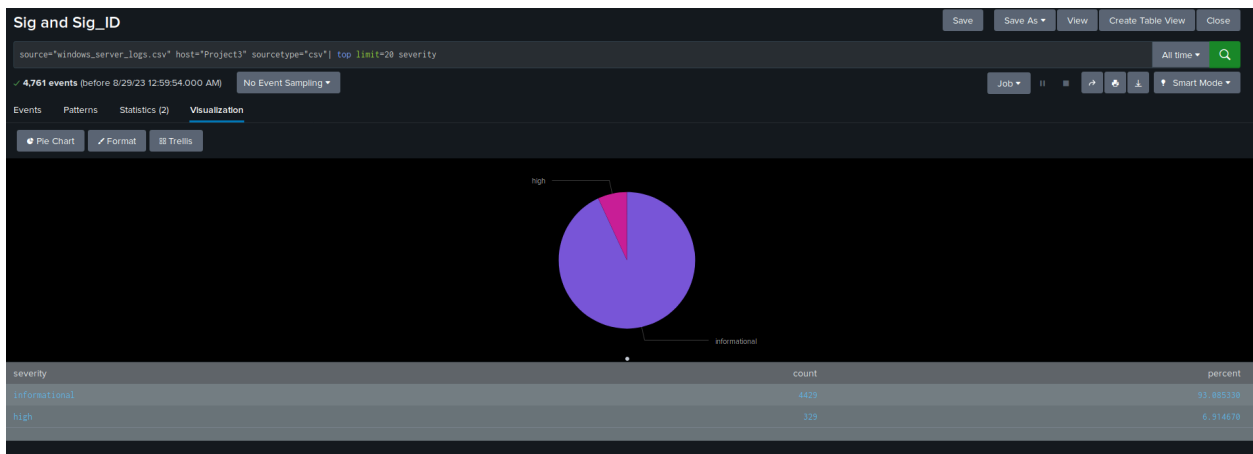
REPORT 1

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

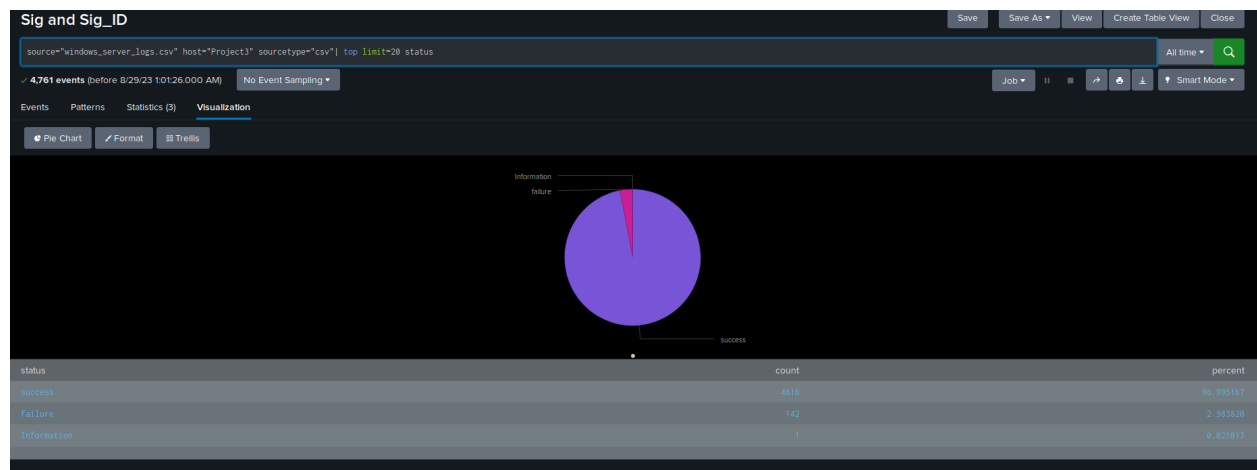
New Search		Save As	Create Table View	Close
source="windows_server_logs.csv" host="Project3" sourcetype="csv" dedup signature, signature_id table signature, signature_id				
15 events (before 8/29/23 12:54:23.000 AM) No Event Sampling				
Events Patterns Statistics (15) Visualization				
20 Per Page Format Preview				
signature				signature_id
A user account was deleted				4726
A user account was created				4728
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
The audit log was cleared				1182
System security access was removed from an account				4718



REPORT 2



REPORT 3



ALERTS

Alert-Fail- Activities

splunk enterprise Apps

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

Alert-Fail-Activities

Edit

Enabled: Yes [Disable](#)

App: search

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

Modified: Aug 29, 2023 1:24:13 AM

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

Trigger Condition: Number of Results is > 18. [Edit](#)

Actions: 1 Action [Edit](#)

[Send email](#)

There are no fired events for this alert.

SECOND ALERT

Successful logins

splunk enterprise Apps

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

Alert-Successful-Login

Edit

Enabled: Yes [Disable](#)

App: search

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

Modified: Aug 29, 2023 1:44:53 AM

Alert Type: Scheduled. Weekly, Monday at 0:00. [Edit](#)

Trigger Condition: Number of Results is > 26. [Edit](#)

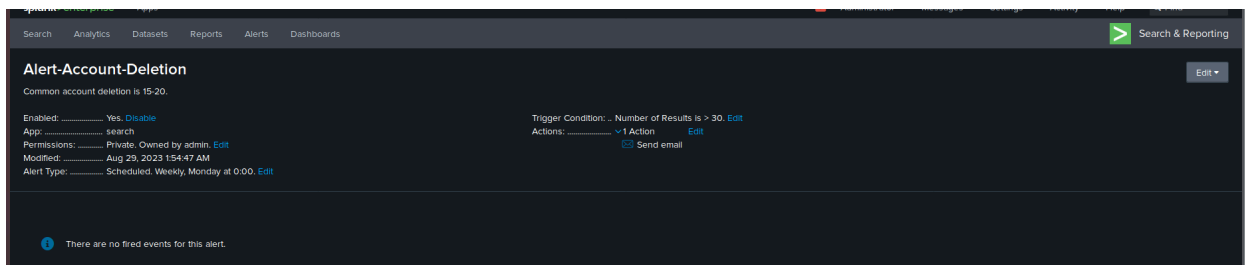
Actions: 1 Action [Edit](#)

[Send email](#)

There are no fired events for this alert.

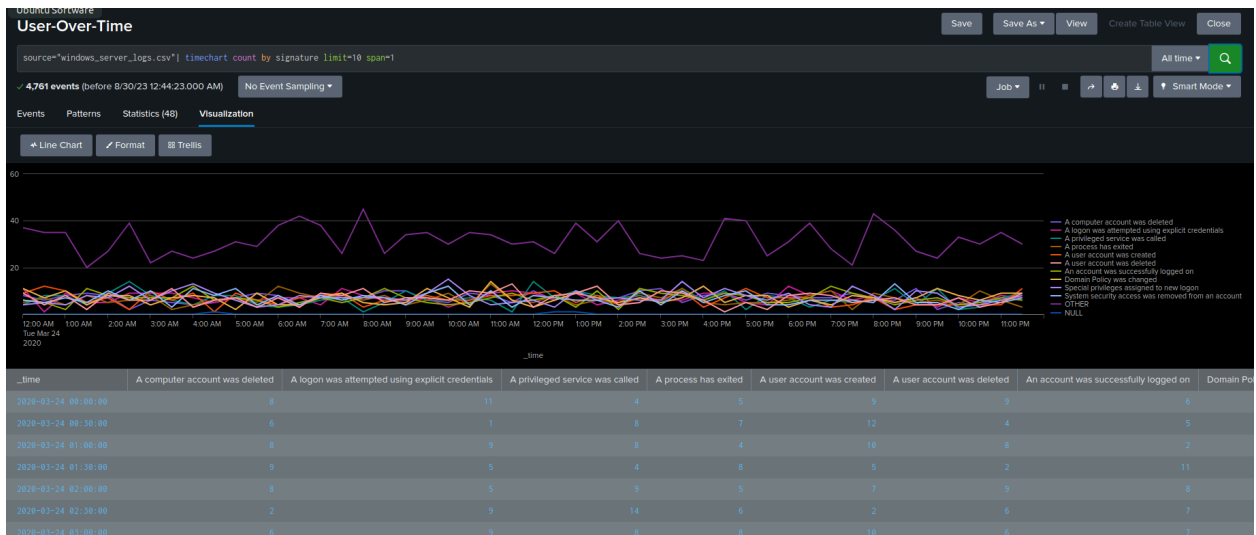
THIRD ALERT

Account deletion

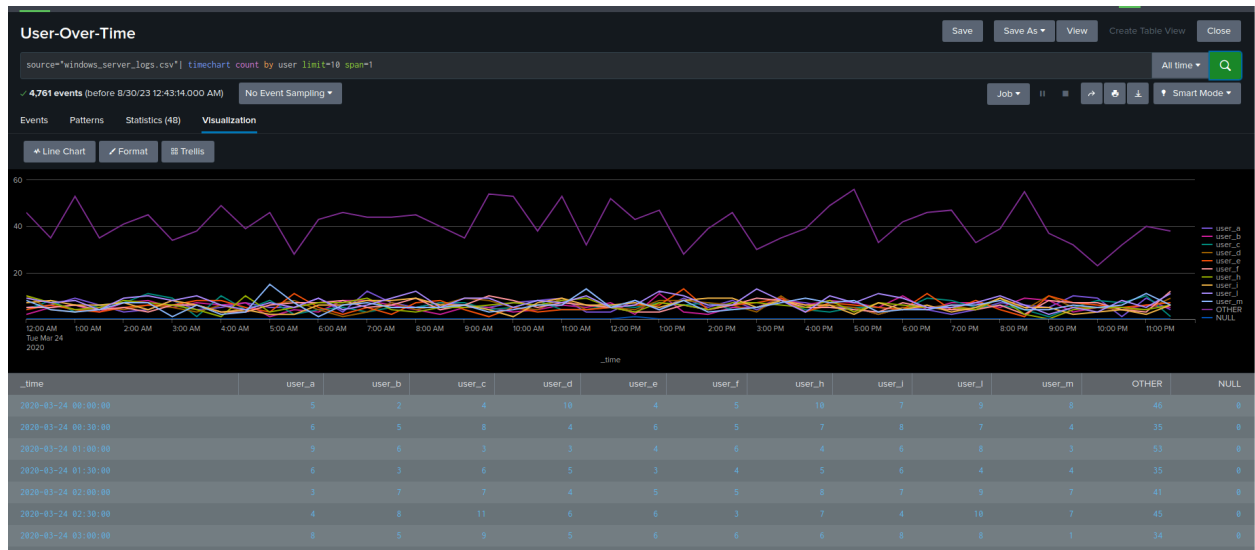


Dashboard

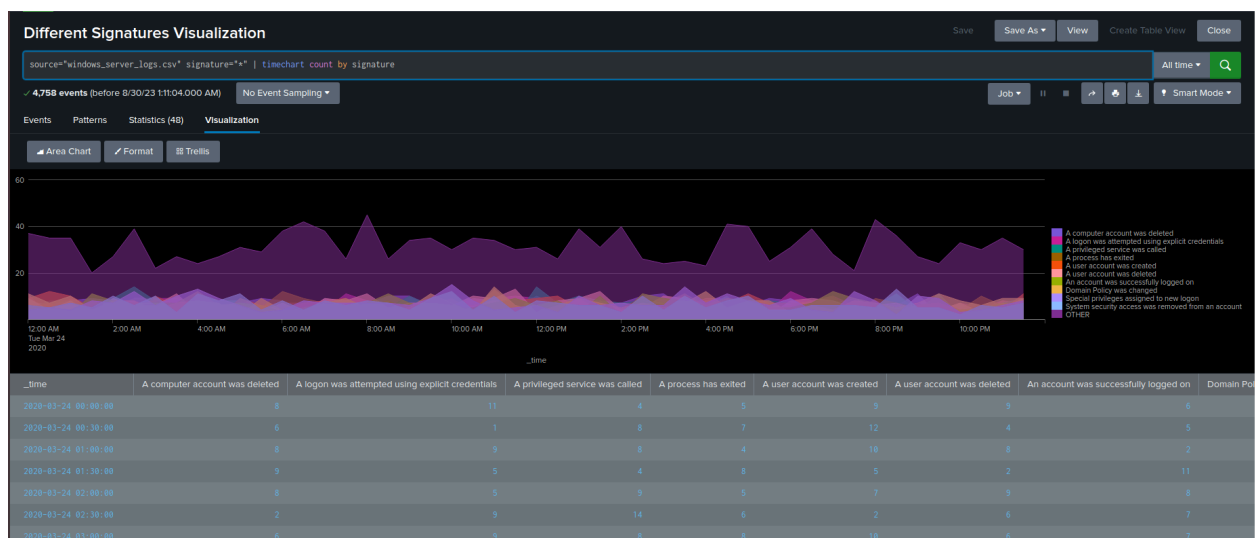
By Signature over time



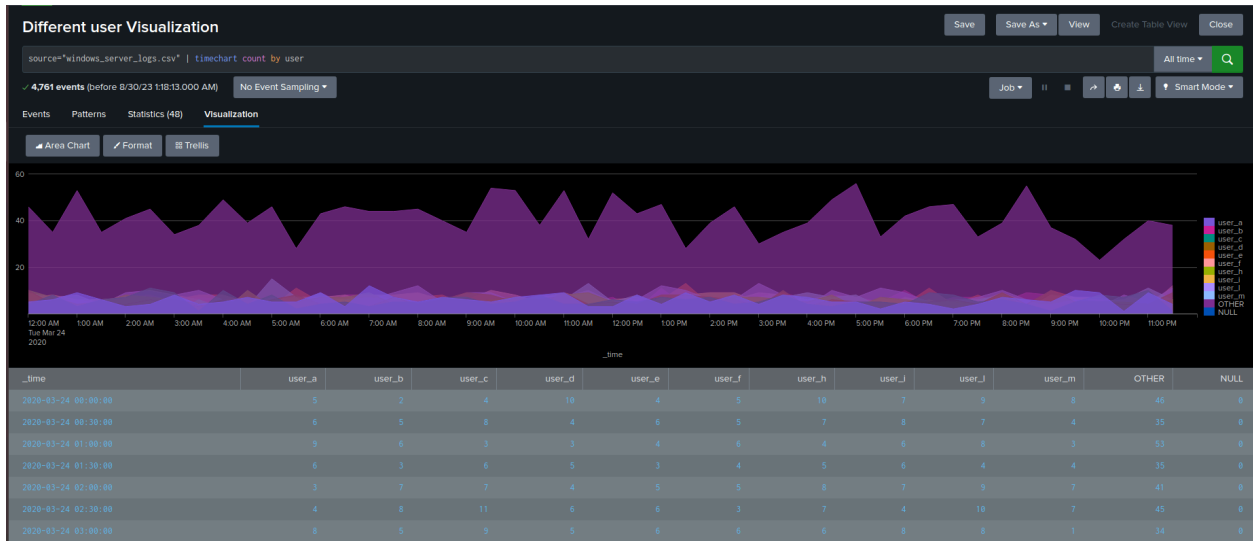
By User over time



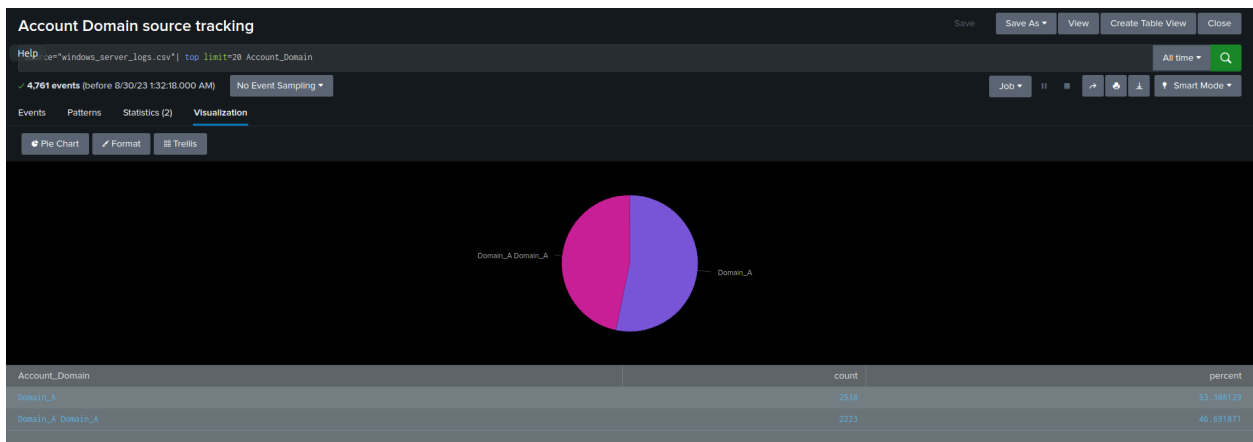
Count by different signatures



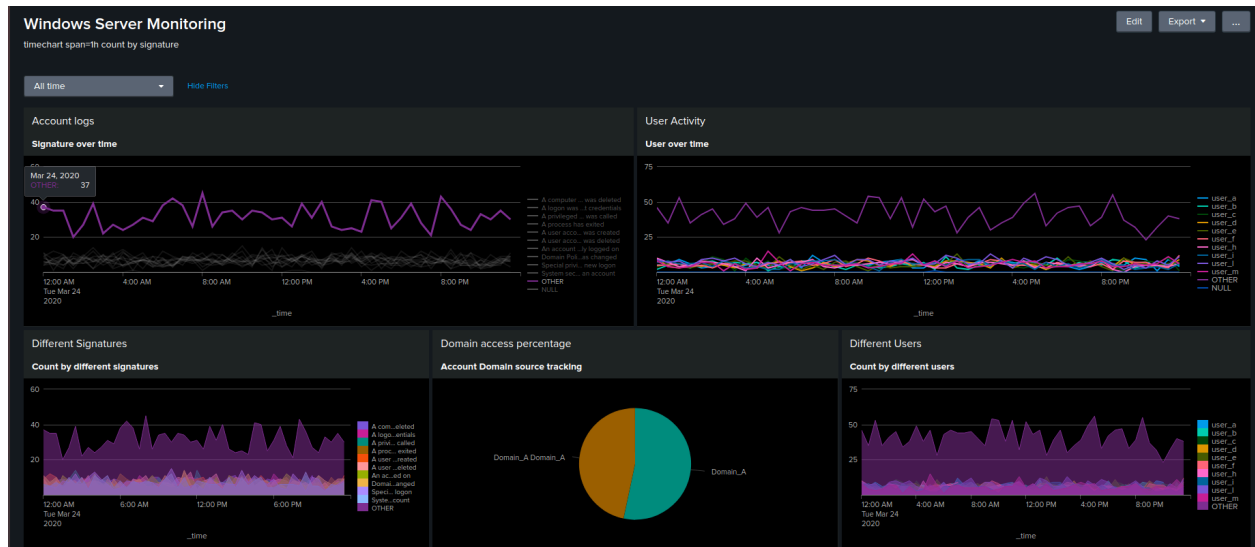
Count by different users



Account Domain source tracking

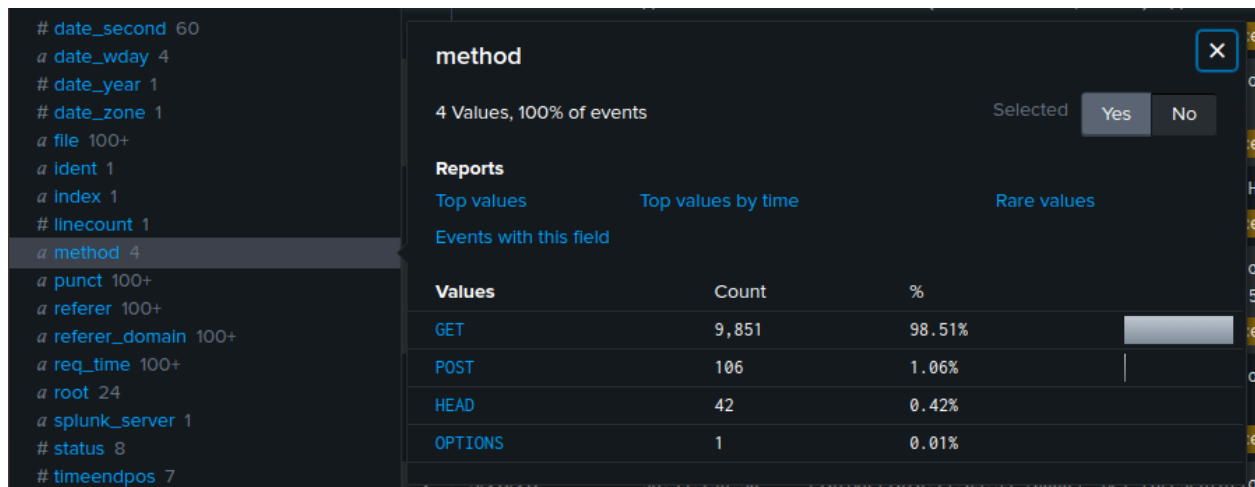


Dashboard



PART 3

Method



Referer_domain

- Clientip

INTERESTING FIELDS # bytes 100+ a clientip 100+ # date_hour 24 # date_mday 4 # date_minute 1 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	clientip			Selected <div>YesNo</div>	
	>100 Values, 100% of events				
	Reports				
	Top values			Top values by time	
	Events with this field			Rare values	
	Top 10 Values			Count	%
	66.249.73.135			482	4.82%
	46.105.14.53			364	3.64%
	130.237.218.86			357	3.57%
	75.97.9.59			273	2.73%

- Useragent

INTERESTING FIELDS

- # bytes 100+
- a clientip 100+
- # date_hour 24
- # date_mday 4
- # date_minute 1
- 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

102 more fields

+ Extract New Fields

useragent

>100 Values, 99.99% of events

Selected

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	1,044	10.441%
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	369	3.69%
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	364	3.64%
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	296	2.96%
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	271	2.71%
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	268	2.68%
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	237	2.37%
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	236	2.36%
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	229	2.29%
Tiny Tiny RSS/1.11 (http://tt-rss.org/)	198	1.98%

PART 4

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

HTTP Methods

Save

Save As

View

Create Table View

Close

source="apache_logs.txt" | top limit=20 method

All time

10,000 events (before 8/30/23 2:24:21.000 AM)

No Event Sampling

Job

Smart Mode

Events

Patterns

Statistics (4)

Visualization

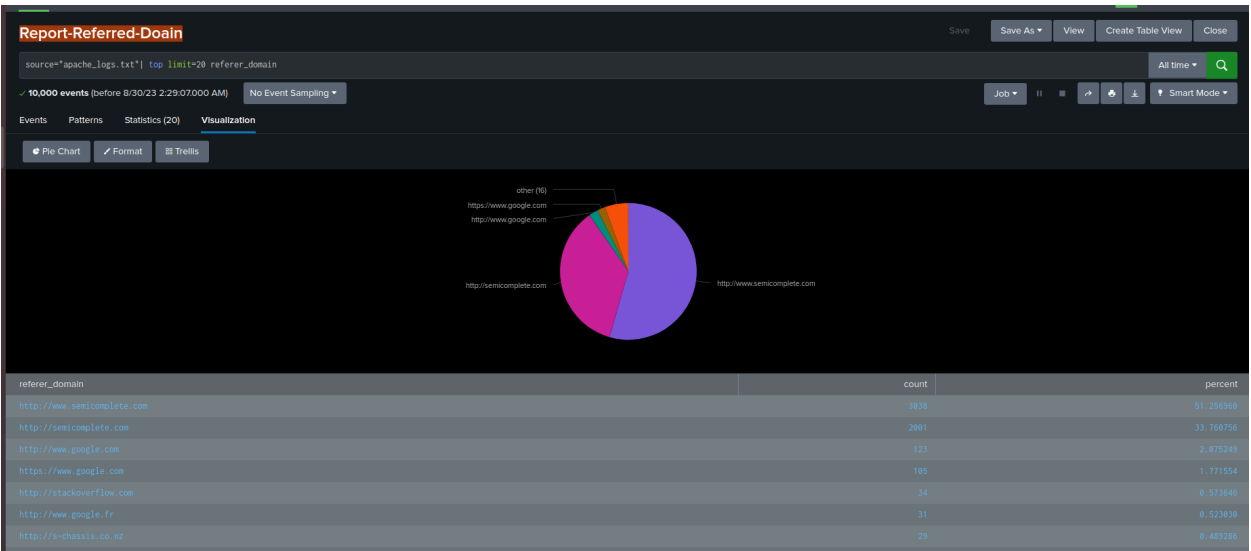
20 Per Page

Format

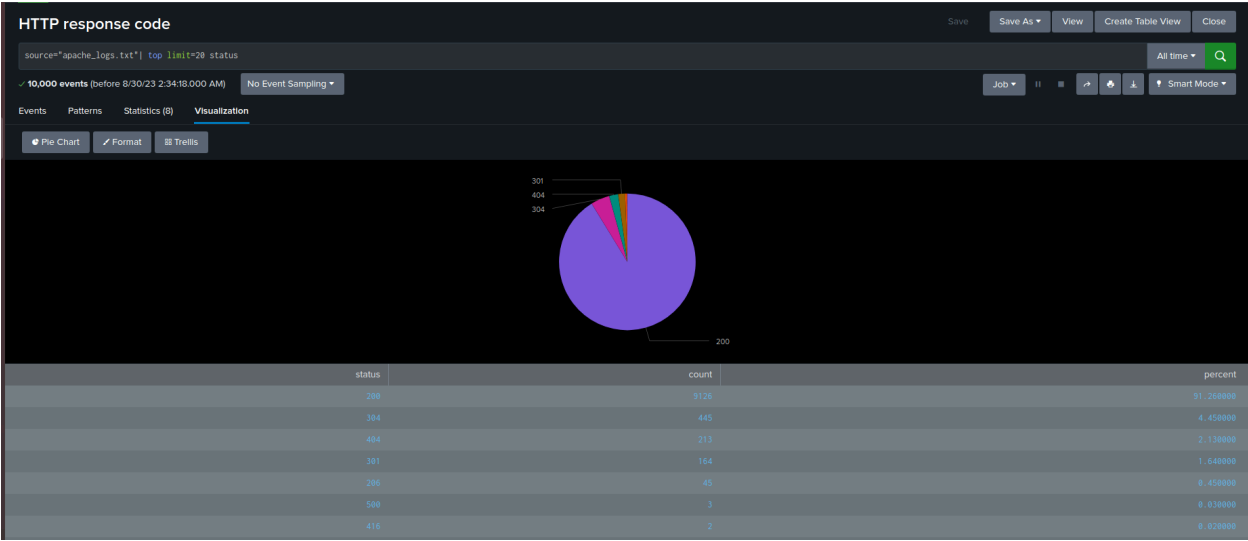
Preview

method	count	percent
GET	9851	98.510000
POST	100	1.000000
HEAD	42	0.420000
OPTIONS	1	0.010000

Report-Referred-DOMAIN



a. HTTP response code



ALERTS

France-IP-Access

France-IP-Access

Enabled: Yes. [Disable](#)

App: search

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

Modified: Aug 30, 2023 3:33:14 AM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: Number of Results is > 2. [Edit](#)

Actions: 1 Action [Edit](#)

[Send email](#)

There are no fired events for this alert.

Alert-POST-Method

Alert-POST-Method

Enabled: Yes. [Disable](#)

App: search

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

Modified: Aug 30, 2023 3:37:18 AM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: Number of Results is > 10. [Edit](#)

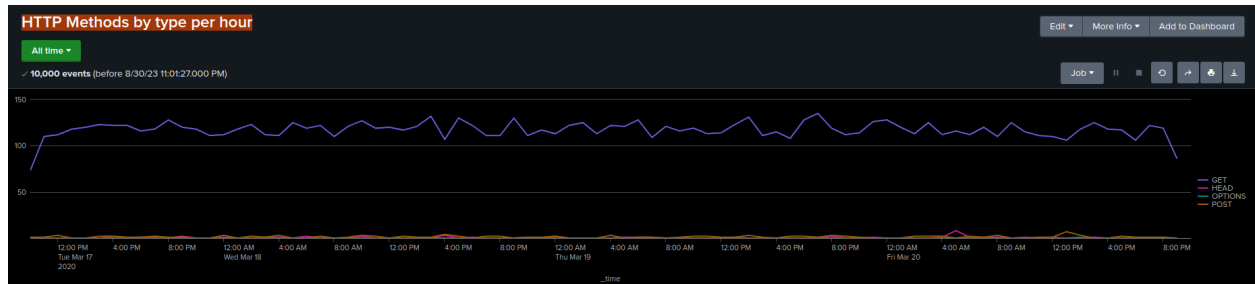
Actions: 1 Action [Edit](#)

[Send email](#)

There are no fired events for this alert.

- Visualizations and dashboards

2. HTTP Methods by type per hour



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

HTTP Methods by type per hour

source="apache_logs.txt" | **iplocation** clientip | **geostats** latfield=lat longfield=lon count

✓ 10,000 events (before 8/30/23 3:53:20.000 AM)

No Event Sampling ▾

Terminal

Events Patterns

Select visualization

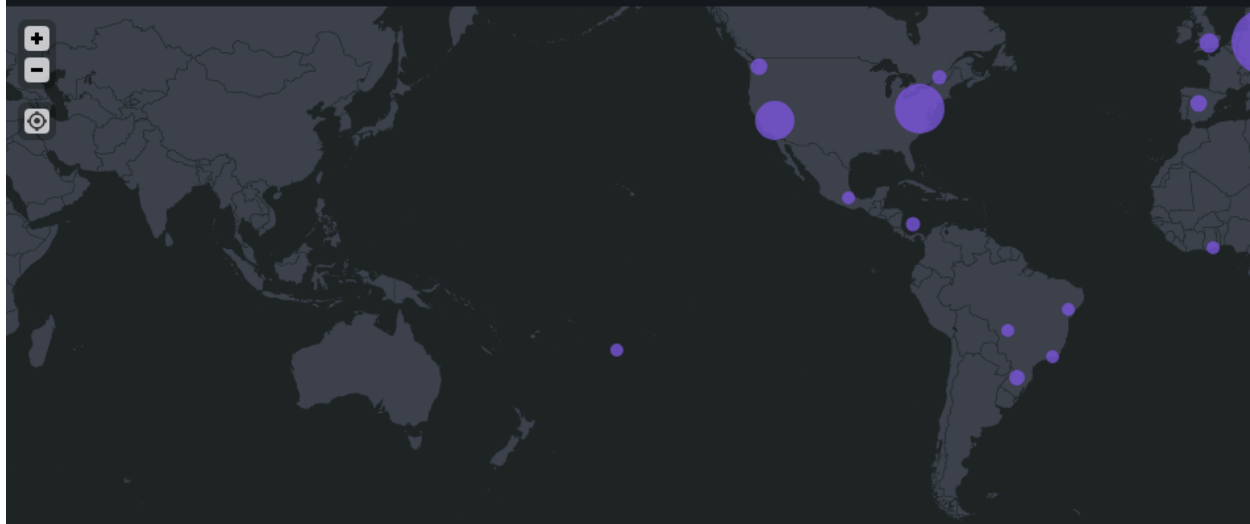
Statistics (3,806)

Visualization

📍 Cluster Map

✍ Format

🔧 Trellis



latitude

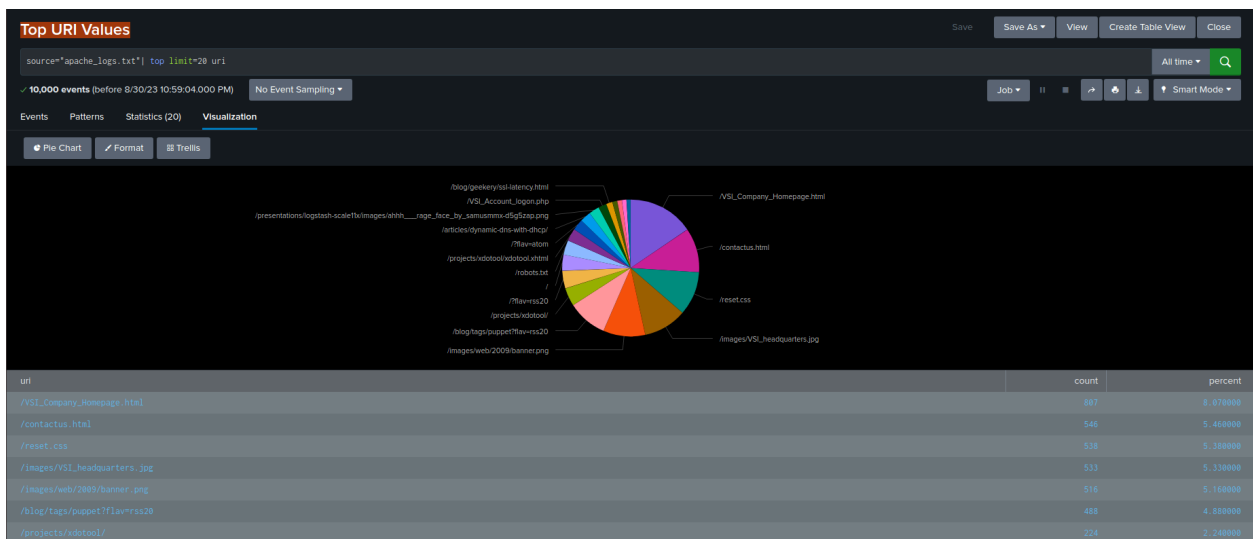
-45.87420

-27.90534

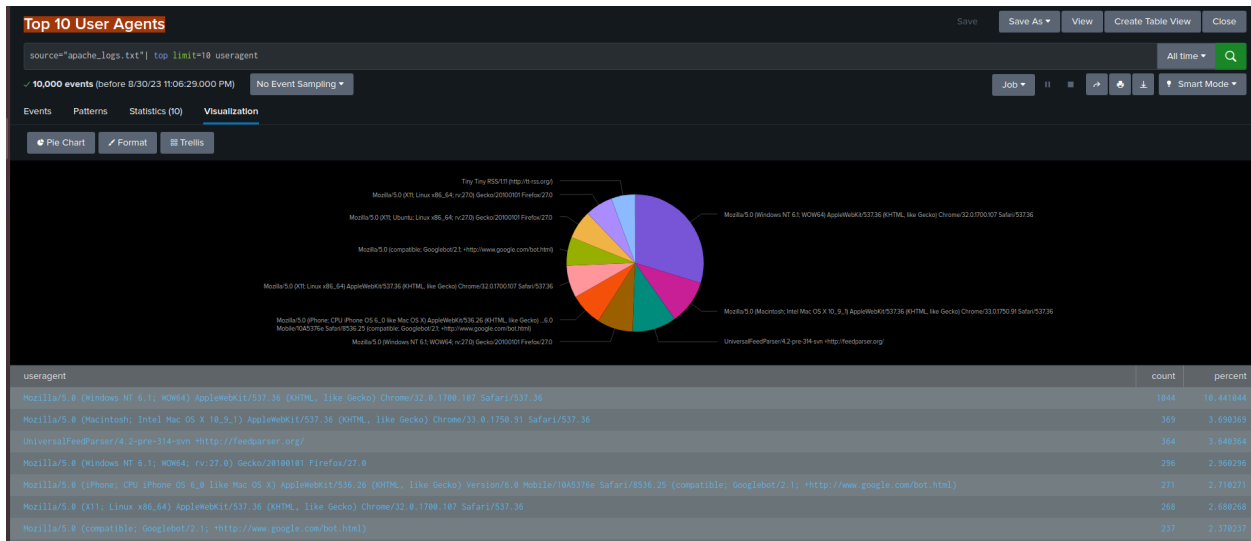
-22.90320

-25.97581

2. Top URI Values



Top 10 User Agents



SPLUNK DAY 2

TOP SEVERITY- LOGS

source="windows_server_logs.csv" | top severity

4,761 events (before 8/31/23 12:14:57.000 AM) No Event Sampling

Events Patterns Statistics (2) Visualization

10 Per Page Format Preview

severity	count	percent
informational	4429	93.885130
high	329	6.914670

TOP SEVERITY- ATTACKS

New Search Save As Create Table View Close

source="windows_server_attack_logs.csv" | top severity All time Q

5,948 events (before 8/31/23 12:09:00 AM) No Event Sampling Job || ↗ ↘ Smart Mode

Events Patterns **Statistics (2)** Visualization

10 Per Page Format Preview

severity	count	percent
informational	4381	73.770575
high	1111	20.229425

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

source="windows_server_logs.csv" | top status All time Q

4,761 events (before 8/31/23 13:02:00 AM) No Event Sampling Job || ↗ ↘ Smart Mode

Events Patterns **Statistics (3)** Visualization

10 Per Page Format Preview

status	count	percent
success	4616	96.995167
failure	142	2.983820
Information	1	0.021013

Attack logs

source="windows_server_attack_logs.csv" | top status All time Q

5,948 events (before 8/31/23 13:15:00 AM) No Event Sampling Job || ↗ ↘ Smart Mode

Events Patterns **Statistics (2)** Visualization

10 Per Page Format Preview

status	count	percent
success	5854	98.436186
failure	93	1.563814

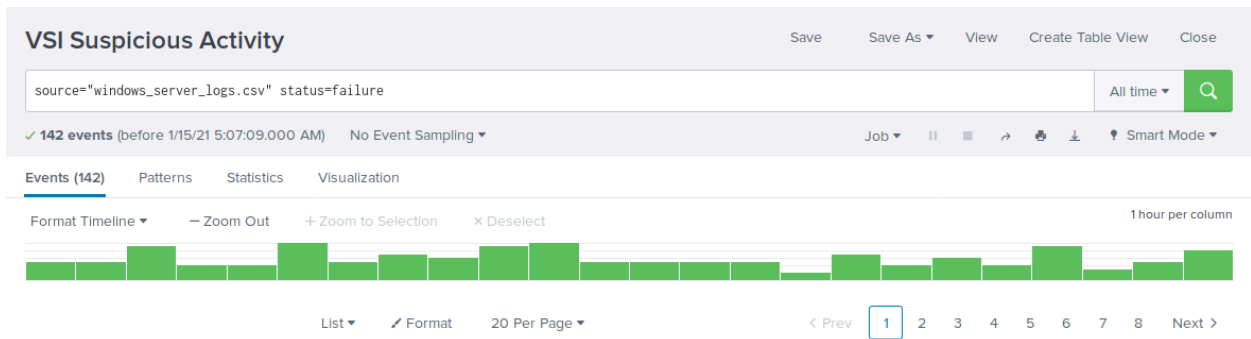
Did you detect any suspicious changes in failed activities?

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

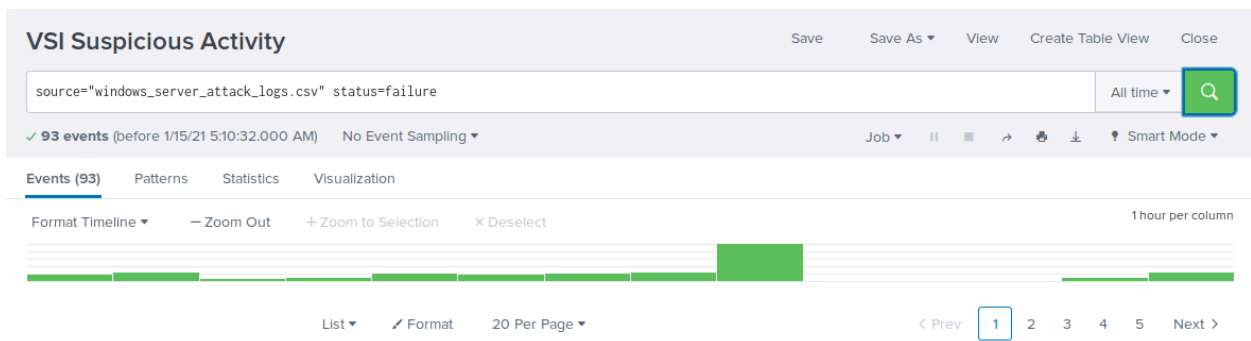
Failure: Notice a decrease of 1% from 3% to 2%.

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?

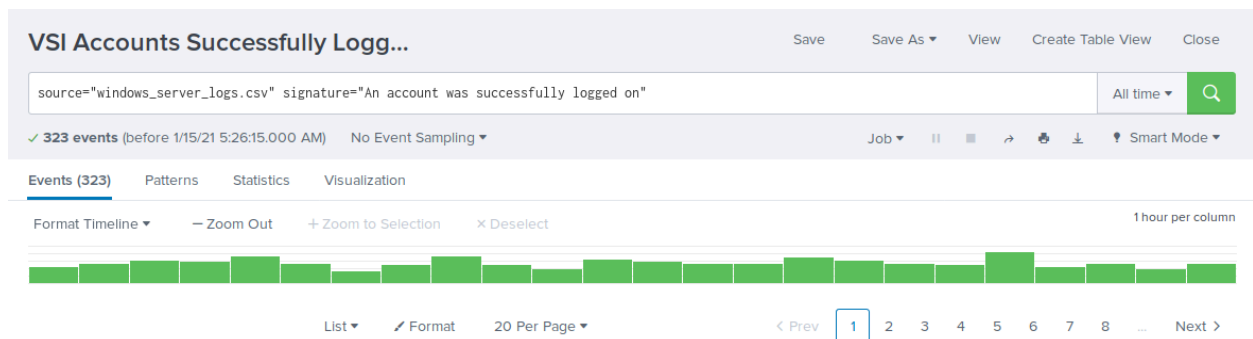
Yes, the alert is within the trigger threshold.

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

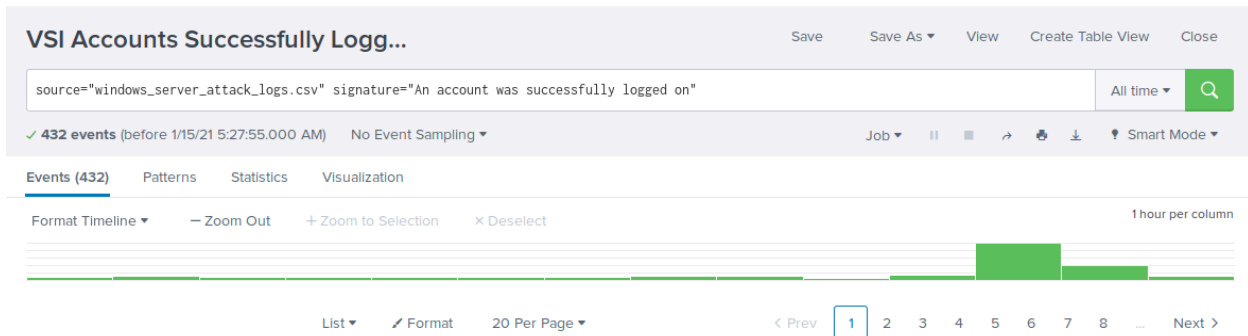
No change in threshold necessary.

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](#)