Defensive Security Project
by: Eli Parry-Giles, Joel Castillo Gomez, Abel Woldemichael, Jada Sweetney, Douglass Thompson

Table of Contents

This document contains the following resources:

01 Monitoring Environment

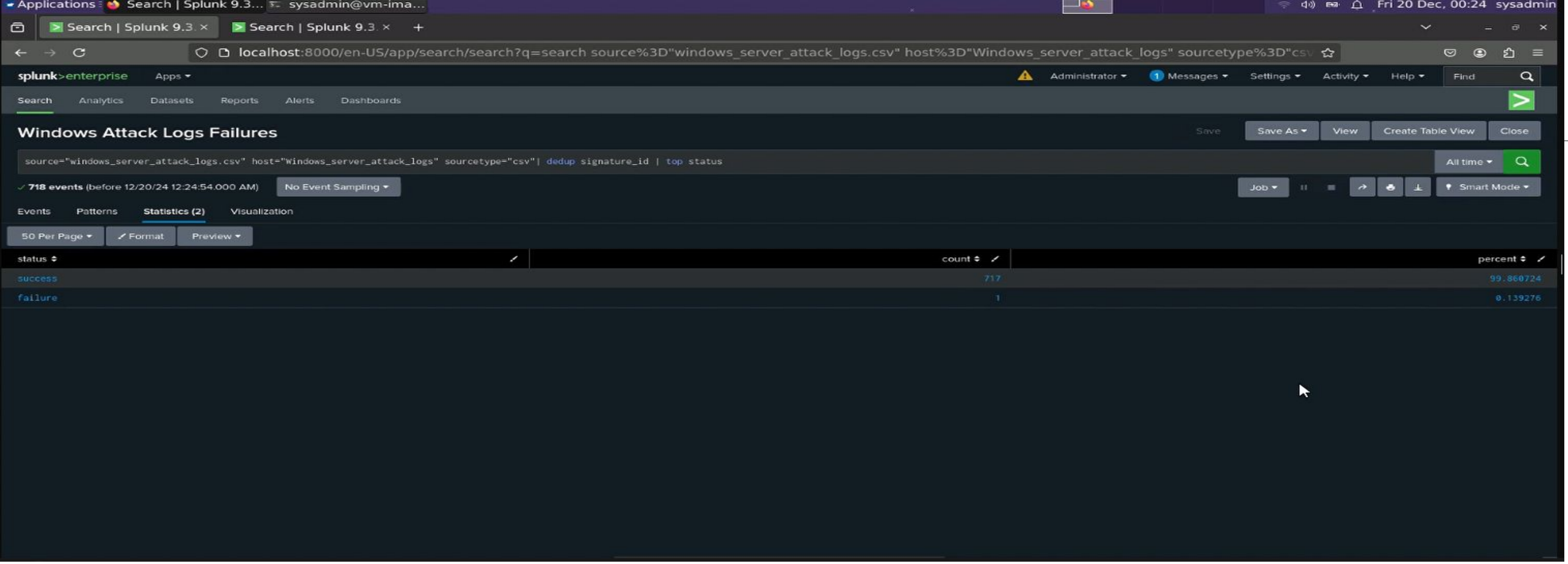
02 Attack Analysis

03 Project Summary & Future Mitigations

Monitoring Environment

Scenario

- We gathered the details of successful and failed login attempts from our users from our organization and located Attacks of the date of when they happened and the time that it happened. We pinpointed the attack through viewing the log in attempts of certain users and seeing which user had the most suspicious activity. we never obtained the users actual name but came down to a conclusion of two users that caused the attack which were Identified as Users A and K. We also located the countries of which these attacks were coming from which was mainly from Ukraine. We installed Alerts into the system to let us know when attempts Failed, when accounts were deleted, when Logins from foreign Countries occurred and when Accounts were logged into.

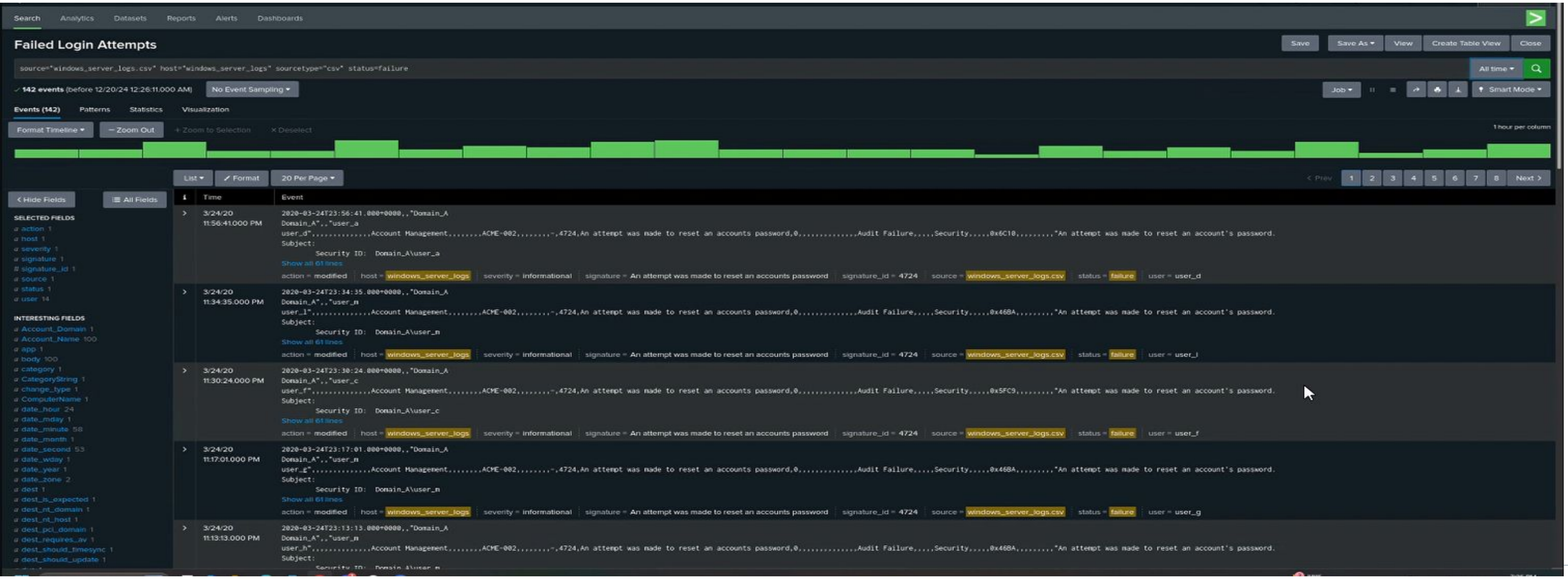


Windows Attack Logs Failures

```
source="windows_server_attack_logs.csv" host="Windows_server_attack_logs" sourcetype="csv"| dedup signature_id | top status
```

✓ **718 events** (before 12/20/24 12:24:54.000 AM)

status	count	percent
success	717	99.860724
failure	1	0.139276



Failed Login Attempts

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" status=failure
```

✓ **142 events** (before 12/20/24 12:26:11.000 AM)

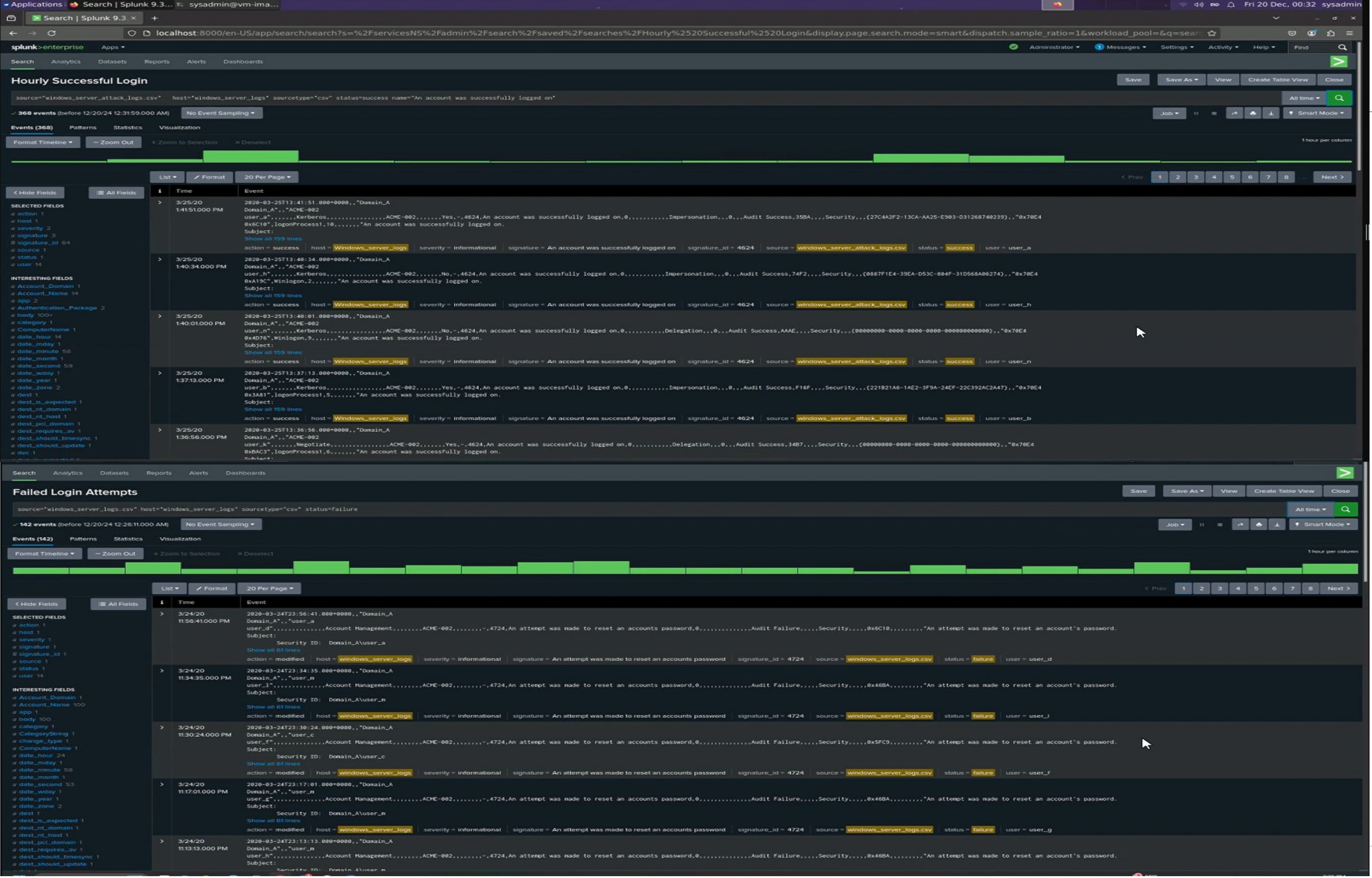
SELECTED FIELDS

a action 1
a host 1
a severity 1
a signature 1
# signature_id 1
a source 1
a status 1
a user 14

INTERESTING FIELDS

a Account_Domain 1
a Account_Name 100
a app 1
a body 100
a category 1
a CategoryString 1
a change_type 1
a ComputerName 1
a date_hour 24
a date_mday 1
a date_minute 58
a date_month 1
a date_second 53
a date_wday 1
a date_year 1
a date_zone 2
a dest 1
a dest_is_expected 1
a dest_nt_domain 1
a dest_nt_host 1
a dest_pci_domain 1
a dest_requires_av 1
a dest_should_timesync 1
a dest_should_update 1

```
i  Time                  Event
>  3/24/20               2020-03-24T23:56:41.000+0000,,"Domain_A
   11:56:41.000 PM       Domain_A",,"user_a
                         user_d",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x6C10,,,,,,,,"An attempt was made to reset an account's password.
                         Subject:
                                 Security ID:  Domain_A\user_a
                         Show all 61 lines
                         action = modified | host = windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_logs.csv | status = failure | user = user_d
>  3/24/20               2020-03-24T23:34:35.000+0000,,"Domain_A
   11:34:35.000 PM       Domain_A",,"user_m
                         user_l",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x46BA,,,,,,,,"An attempt was made to reset an account's password.
                         Subject:
                                 Security ID:  Domain_A\user_m
                         Show all 61 lines
                         action = modified | host = windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_logs.csv | status = failure | user = user_l
>  3/24/20               2020-03-24T23:30:24.000+0000,,"Domain_A
   11:30:24.000 PM       Domain_A",,"user_c
                         user_f",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x5FC9,,,,,,,,"An attempt was made to reset an account's password.
                         Subject:
                                 Security ID:  Domain_A\user_c
                         Show all 61 lines
                         action = modified | host = windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_logs.csv | status = failure | user = user_f
>  3/24/20               2020-03-24T23:17:01.000+0000,,"Domain_A
   11:17:01.000 PM       Domain_A",,"user_m
                         user_g",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x46BA,,,,,,,,"An attempt was made to reset an account's password.
                         Subject:
                                 Security ID:  Domain_A\user_m
                         Show all 61 lines
                         action = modified | host = windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_logs.csv | status = failure | user = user_g
>  3/24/20               2020-03-24T23:13:13.000+0000,,"Domain_A
   11:13:13.000 PM       Domain_A",,"user_m
                         user_h",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x46BA,,,,,,,,"An attempt was made to reset an account's password.
                         Subject:
                                 Security ID:  Domain_A\user_m
```



Hourly Successful Login

```
source="windows_server_attack_logs.csv"   host="windows_server_logs" sourcetype="csv" status=success name="An account was successfully logged on"
```

✓ 368 events (before 12/20/24 12:31:59.000 AM)

Events (368)

```
i  Time                 Event
>  3/25/20              2020-03-25T13:41:51.000+0000,,"Domain_A
   1:41:51.000 PM       Domain_A",,"ACME-002
                        user_a",,,,,,,Kerberos,,,,,,,,,,,,,,,,ACME-002,,,,,,,Yes,-,4624,An account was successfully logged on,0,,,,,,,,,,,Impersonation,,,0,,,Audit Success,35BA,,,,Security,,,{27C4A2F2-13CA-AA25-E903-D31268740239},,"0x70E4
                        0x6C10",logonProcess1,10,,,,,,,"An account was successfully logged on.
                        Subject:
                        Show all 159 lines
                        action = success | host = Windows_server_logs | severity = informational | signature = An account was successfully logged on | signature_id = 4624 | source = windows_server_attack_logs.csv | status = success | user = user_a
>  3/25/20              2020-03-25T13:40:34.000+0000,,"Domain_A
   1:40:34.000 PM       Domain_A",,"ACME-002
                        user_h",,,,,,,Kerberos,,,,,,,,,,,,,,,,ACME-002,,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,,,Impersonation,,,0,,,Audit Success,74F2,,,,Security,,,{0887F1E4-39EA-D53C-804F-31D568A06274},,"0x70E4
                        0xA19C",Winlogon,2,,,,,,,"An account was successfully logged on.
                        Subject:
                        Show all 159 lines
                        action = success | host = Windows_server_logs | severity = informational | signature = An account was successfully logged on | signature_id = 4624 | source = windows_server_attack_logs.csv | status = success | user = user_h
>  3/25/20              2020-03-25T13:40:01.000+0000,,"Domain_A
   1:40:01.000 PM       Domain_A",,"ACME-002
                        user_n",,,,,,,Kerberos,,,,,,,,,,,,,,,,ACME-002,,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,,,Delegation,,,0,,,Audit Success,AAAE,,,,Security,,,{00000000-0000-0000-0000-000000000000},,"0x70E4
                        0x4D76",Winlogon,9,,,,,,,"An account was successfully logged on.
                        Subject:
                        Show all 159 lines
                        action = success | host = Windows_server_logs | severity = informational | signature = An account was successfully logged on | signature_id = 4624 | source = windows_server_attack_logs.csv | status = success | user = user_n
>  3/25/20              2020-03-25T13:37:13.000+0000,,"Domain_A
   1:37:13.000 PM       Domain_A",,"ACME-002
                        user_b",,,,,,,Kerberos,,,,,,,,,,,,,,,,ACME-002,,,,,,,Yes,-,4624,An account was successfully logged on,0,,,,,,,,,,,Impersonation,,,0,,,Audit Success,F16F,,,,Security,,,{221B21A6-1AE2-3F9A-24EF-22C392AC2A47},,"0x70E4
                        0x3A81",logonProcess1,5,,,,,,,"An account was successfully logged on.
                        Subject:
                        Show all 159 lines
                        action = success | host = Windows_server_logs | severity = informational | signature = An account was successfully logged on | signature_id = 4624 | source = windows_server_attack_logs.csv | status = success | user = user_b
>  3/25/20              2020-03-25T13:36:56.000+0000,,"Domain_A
   1:36:56.000 PM       Domain_A",,"ACME-002
                        user_k",,,,,,,Negotiate,,,,,,,,,,,,,,,,ACME-002,,,,,,,Yes,-,4624,An account was successfully logged on,0,,,,,,,,,,,Delegation,,,0,,,Audit Success,34B7,,,,Security,,,{00000000-0000-0000-0000-000000000000},,"0x70E4
                        0xBAC3",logonProcess1,6,,,,,,,"An account was successfully logged on.
```

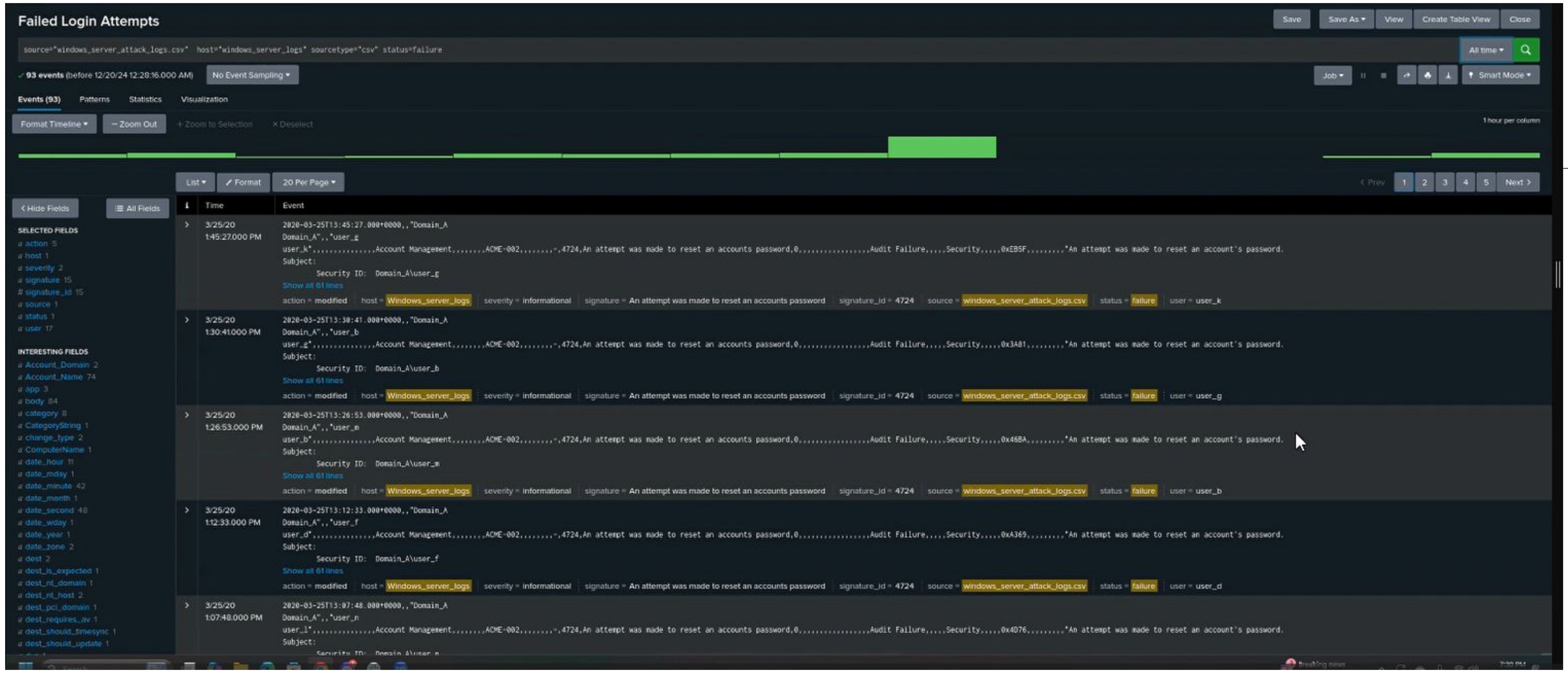
Failed Login Attempts

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" status=failure
```

✓ 142 events (before 12/20/24 12:26:11.000 AM)

Events (142)

```
i  Time                 Event
>  3/24/20              2020-03-24T23:56:41.000+0000,,"Domain_A
   11:56:41.000 PM      Domain_A",,"user_a
                        user_d",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x6C10,,,,,,,,,"An attempt was made to reset an account's password.
                        Subject:
                                Security ID:  Domain_A\user_a
                        Show all 61 lines
                        action = modified | host = windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_logs.csv | status = failure | user = user_d
>  3/24/20              2020-03-24T23:34:35.000+0000,,"Domain_A
   11:34:35.000 PM      Domain_A",,"user_m
                        user_l",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x46BA,,,,,,,,,"An attempt was made to reset an account's password.
                        Subject:
                                Security ID:  Domain_A\user_m
                        Show all 61 lines
                        action = modified | host = windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_logs.csv | status = failure | user = user_l
>  3/24/20              2020-03-24T23:30:24.000+0000,,"Domain_A
   11:30:24.000 PM      Domain_A",,"user_c
                        user_f",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x5FC9,,,,,,,,,"An attempt was made to reset an account's password.
                        Subject:
                                Security ID:  Domain_A\user_c
                        Show all 61 lines
                        action = modified | host = windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_logs.csv | status = failure | user = user_f
>  3/24/20              2020-03-24T23:17:01.000+0000,,"Domain_A
   11:17:01.000 PM      Domain_A",,"user_m
                        user_g",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x46BA,,,,,,,,,"An attempt was made to reset an account's password.
                        Subject:
                                Security ID:  Domain_A\user_m
                        Show all 61 lines
                        action = modified | host = windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_logs.csv | status = failure | user = user_g
>  3/24/20              2020-03-24T23:13:13.000+0000,,"Domain_A
   11:13:13.000 PM      Domain_A",,"user_m
                        user_h",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x46BA,,,,,,,,,"An attempt was made to reset an account's password.
                        Subject:
```



Failed Login Attempts

```
source="windows_server_attack_logs.csv"  host="windows_server_logs" sourcetype="csv" status=failure
```

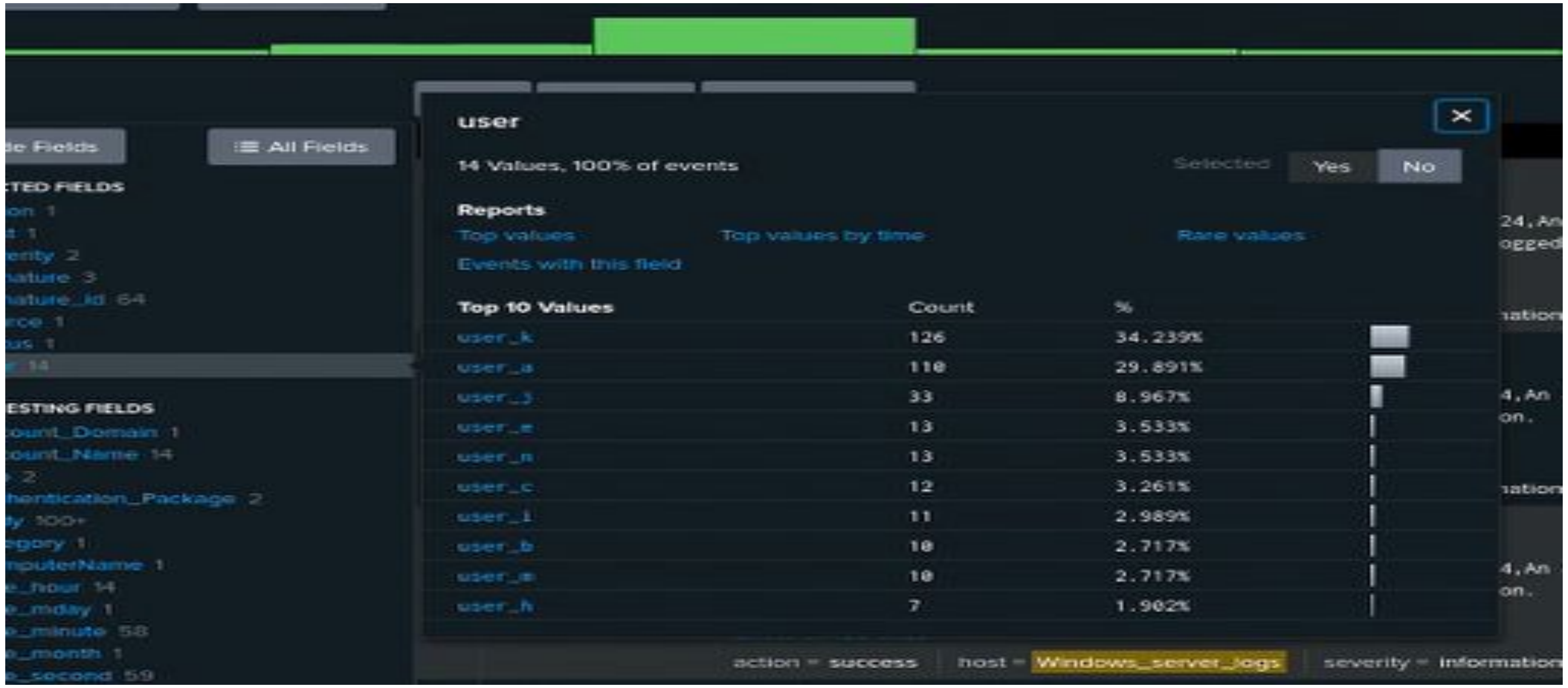
✓ 93 events (before 12/20/24 12:28:16.000 AM) No Event Sampling ▾

Events (93) Patterns Statistics Visualization

SELECTED FIELDS
a action 5
a host 1
a severity 2
a signature 15
# signature_id 15
a source 1
a status 1
a user 17

INTERESTING FIELDS
a Account_Domain 2
a Account_Name 74
a app 3
a body 84
a category 8
a CategoryString 1
a change_type 2
a ComputerName 1
a date_hour 11
a date_mday 1
a date_minute 42
a date_month 1
a date_second 48
a date_wday 1
a date_year 1
a date_zone 2
a dest 2
a dest_is_expected 1
a dest_nt_domain 1
a dest_nt_host 2
a dest_pci_domain 1
a dest_requires_av 1
a dest_should_timesync 1
a dest_should_update 1

```
i  Time            Event
>  3/25/20         2020-03-25T13:45:27.000+0000,,"Domain_A
   1:45:27.000 PM  Domain_A",,"user_g
                   user_k",,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,Security,,,,,0xEB5F,,,,,,,,"An attempt was made to reset an account's password.
                   Subject:
                           Security ID:  Domain_A\user_g
                   Show all 61 lines
                   action = modified | host = Windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_attack_logs.csv | status = failure | user = user_k
>  3/25/20         2020-03-25T13:30:41.000+0000,,"Domain_A
   1:30:41.000 PM  Domain_A",,"user_b
                   user_g",,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,Security,,,,,0x3A81,,,,,,,,"An attempt was made to reset an account's password.
                   Subject:
                           Security ID:  Domain_A\user_b
                   Show all 61 lines
                   action = modified | host = Windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_attack_logs.csv | status = failure | user = user_g
>  3/25/20         2020-03-25T13:26:53.000+0000,,"Domain_A
   1:26:53.000 PM  Domain_A",,"user_m
                   user_b",,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,Security,,,,,0x46BA,,,,,,,,"An attempt was made to reset an account's password.
                   Subject:
                           Security ID:  Domain_A\user_m
                   Show all 61 lines
                   action = modified | host = Windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_attack_logs.csv | status = failure | user = user_b
>  3/25/20         2020-03-25T13:12:33.000+0000,,"Domain_A
   1:12:33.000 PM  Domain_A",,"user_f
                   user_d",,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,Security,,,,,0xA369,,,,,,,,"An attempt was made to reset an account's password.
                   Subject:
                           Security ID:  Domain_A\user_f
                   Show all 61 lines
                   action = modified | host = Windows_server_logs | severity = informational | signature = An attempt was made to reset an accounts password | signature_id = 4724 | source = windows_server_attack_logs.csv | status = failure | user = user_d
>  3/25/20         2020-03-25T13:07:48.000+0000,,"Domain_A
   1:07:48.000 PM  Domain_A",,"user_n
                   user_l",,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,Security,,,,,0x4D76,,,,,,,,"An attempt was made to reset an account's password.
                   Subject:
                           Security ID:  Domain_A\user_n
```



user

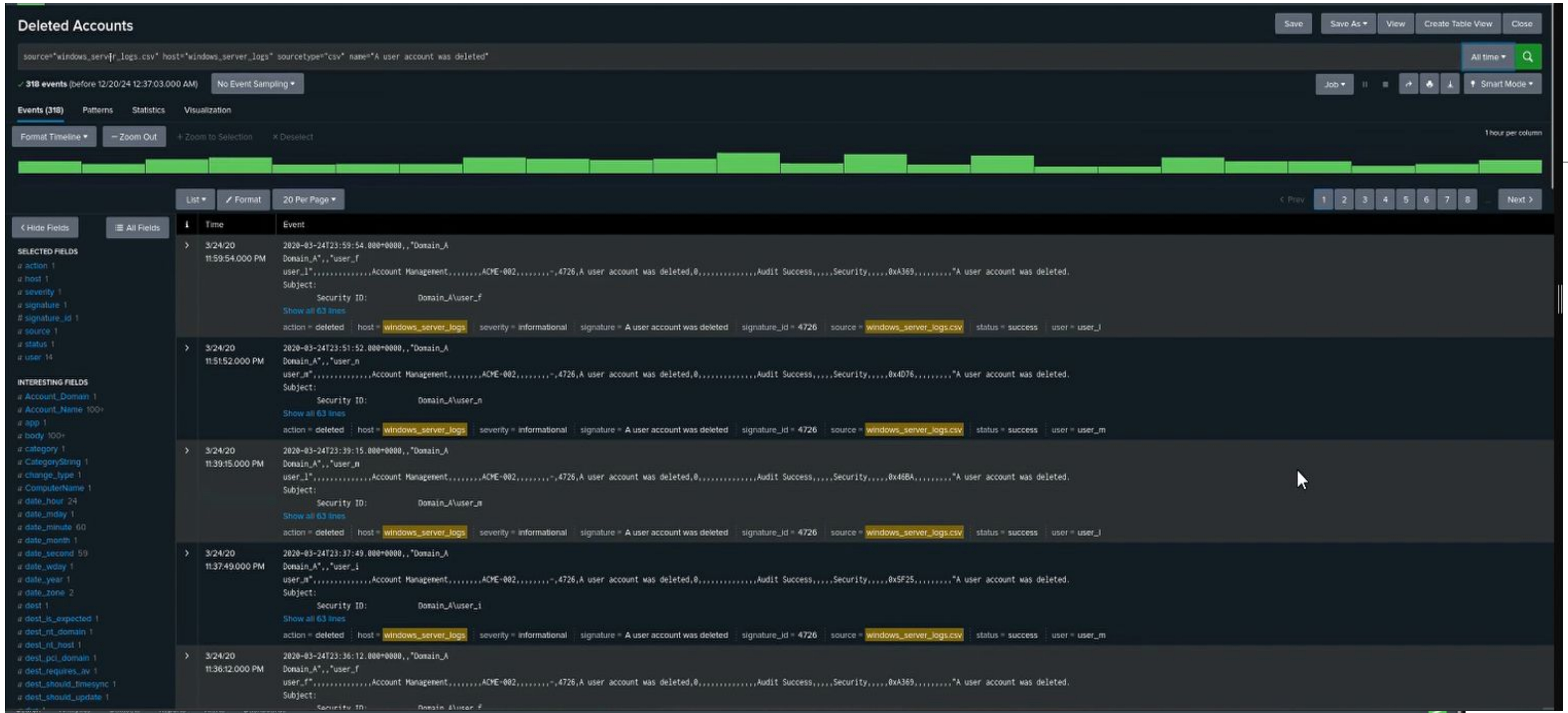
14 Values, 100% of events

Reports

Top values Top values by time Rare values

Events with this field

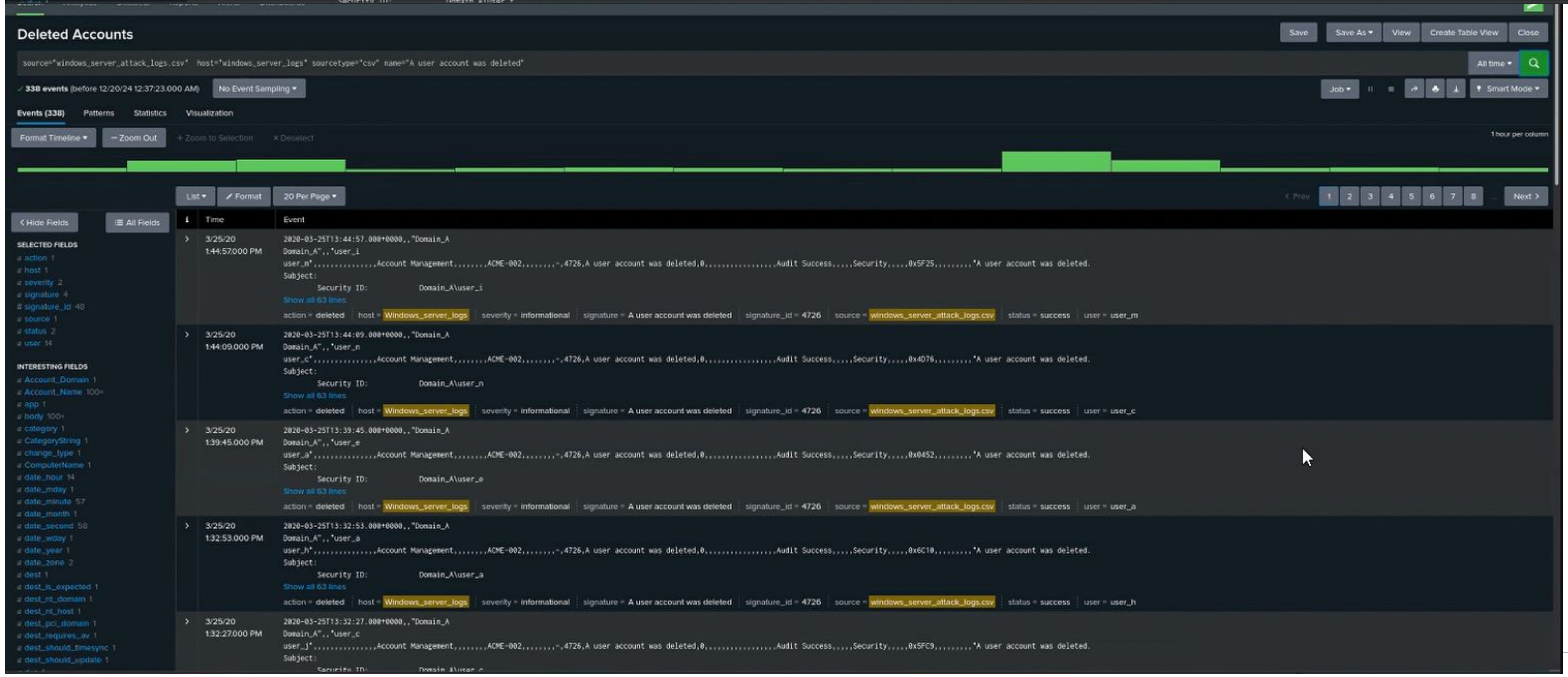
Top 10 Values	Count	%
user_k	126	34.239%
user_a	110	29.891%
user_j	33	8.967%
user_e	13	3.533%
user_n	13	3.533%
user_c	12	3.261%
user_i	11	2.989%
user_b	10	2.717%
user_m	10	2.717%
user_h	7	1.902%



```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" name="A user account was deleted"
```

✓ 318 events (before 12/20/24 12:37:03.000 AM)

```
3/24/20          2020-03-24T23:59:54.000+0000,,"Domain_A
11:59:54.000 PM  Domain_A",,"user_f
                 user_l",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_f
                 action = deleted  host = windows_server_logs  severity = informational  signature = A user account was deleted  signature_id = 4726  source = windows_server_logs.csv  status = success  user = user_l

3/24/20          2020-03-24T23:51:52.000+0000,,"Domain_A
11:51:52.000 PM  Domain_A",,"user_n
                 user_m",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x4D76,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_n
                 action = deleted  host = windows_server_logs  severity = informational  signature = A user account was deleted  signature_id = 4726  source = windows_server_logs.csv  status = success  user = user_m

3/24/20          2020-03-24T23:39:15.000+0000,,"Domain_A
11:39:15.000 PM  Domain_A",,"user_m
                 user_l",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x46BA,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_m
                 action = deleted  host = windows_server_logs  severity = informational  signature = A user account was deleted  signature_id = 4726  source = windows_server_logs.csv  status = success  user = user_l

3/24/20          2020-03-24T23:37:49.000+0000,,"Domain_A
11:37:49.000 PM  Domain_A",,"user_i
                 user_m",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x5F25,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_i
                 action = deleted  host = windows_server_logs  severity = informational  signature = A user account was deleted  signature_id = 4726  source = windows_server_logs.csv  status = success  user = user_m

3/24/20          2020-03-24T23:36:12.000+0000,,"Domain_A
11:36:12.000 PM  Domain_A",,"user_f
                 user_f",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_f
```



```
source="windows_server_attack_logs.csv"  host="windows_server_logs" sourcetype="csv" name="A user account was deleted"
```

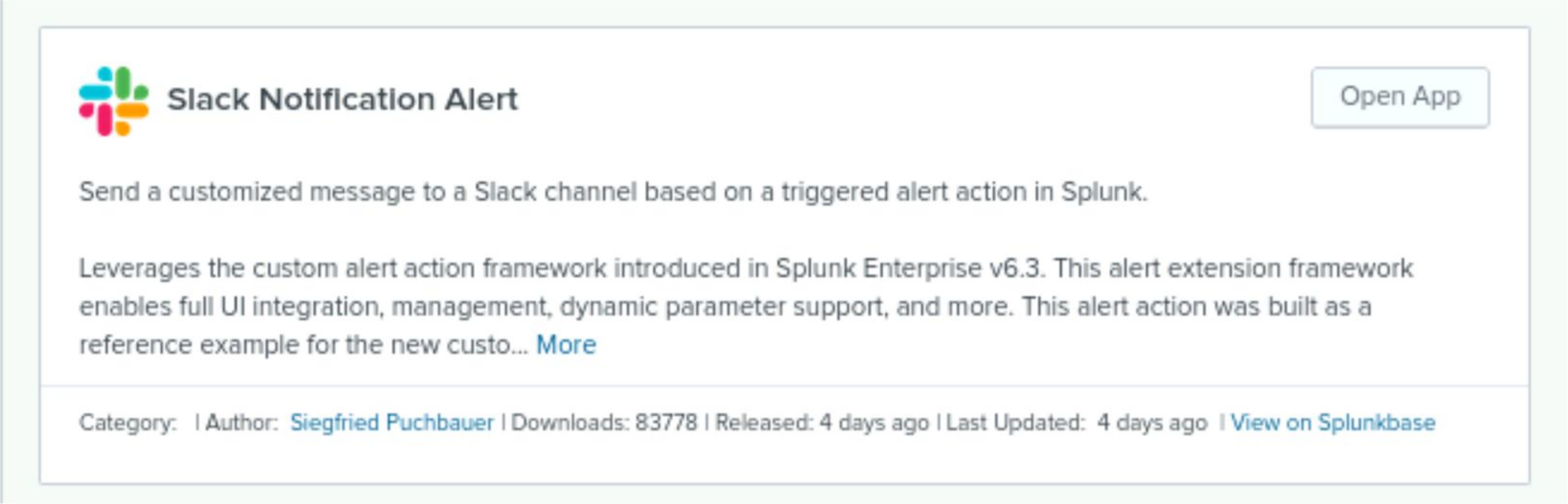
✓ 338 events (before 12/20/24 12:37:23.000 AM)

```
3/25/20          2020-03-25T13:44:57.000+0000,,"Domain_A
1:44:57.000 PM   Domain_A",,"user_i
                 user_m",,,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x5F25,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_i
                 action = deleted  host = Windows_server_logs  severity = informational  signature = A user account was deleted  signature_id = 4726  source = windows_server_attack_logs.csv  status = success  user = user_m

3/25/20          2020-03-25T13:44:09.000+0000,,"Domain_A
1:44:09.000 PM   Domain_A",,"user_n
                 user_c",,,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x4D76,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_n
                 action = deleted  host = Windows_server_logs  severity = informational  signature = A user account was deleted  signature_id = 4726  source = windows_server_attack_logs.csv  status = success  user = user_c

3/25/20          2020-03-25T13:39:45.000+0000,,"Domain_A
1:39:45.000 PM   Domain_A",,"user_e
                 user_a",,,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x0452,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_e
                 action = deleted  host = Windows_server_logs  severity = informational  signature = A user account was deleted  signature_id = 4726  source = windows_server_attack_logs.csv  status = success  user = user_a

3/25/20          2020-03-25T13:32:53.000+0000,,"Domain_A
1:32:53.000 PM   Domain_A",,"user_a
                 user_h",,,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x6C10,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_a
                 action = deleted  host = Windows_server_logs  severity = informational  signature = A user account was deleted  signature_id = 4726  source = windows_server_attack_logs.csv  status = success  user = user_h

3/25/20          2020-03-25T13:32:27.000+0000,,"Domain_A
1:32:27.000 PM   Domain_A",,"user_c
                 user_j",,,,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x5FC9,,,,,,,,,"A user account was deleted.
                 Subject:
                         Security ID:          Domain_A\user_c
```

Slack Notification Alerts “Add-On” App

Slack Notification Alerts

We have chosen Slack Notification Alerts as our add-on app. This app enables alerts to be sent to Slack via message. Alerts must be set up to go to the created bot and the chosen alert will be sent to a chosen channel in Slack.



Slack Notification Alert

Send a customized message to a Slack channel based on a triggered alert action in Splunk.

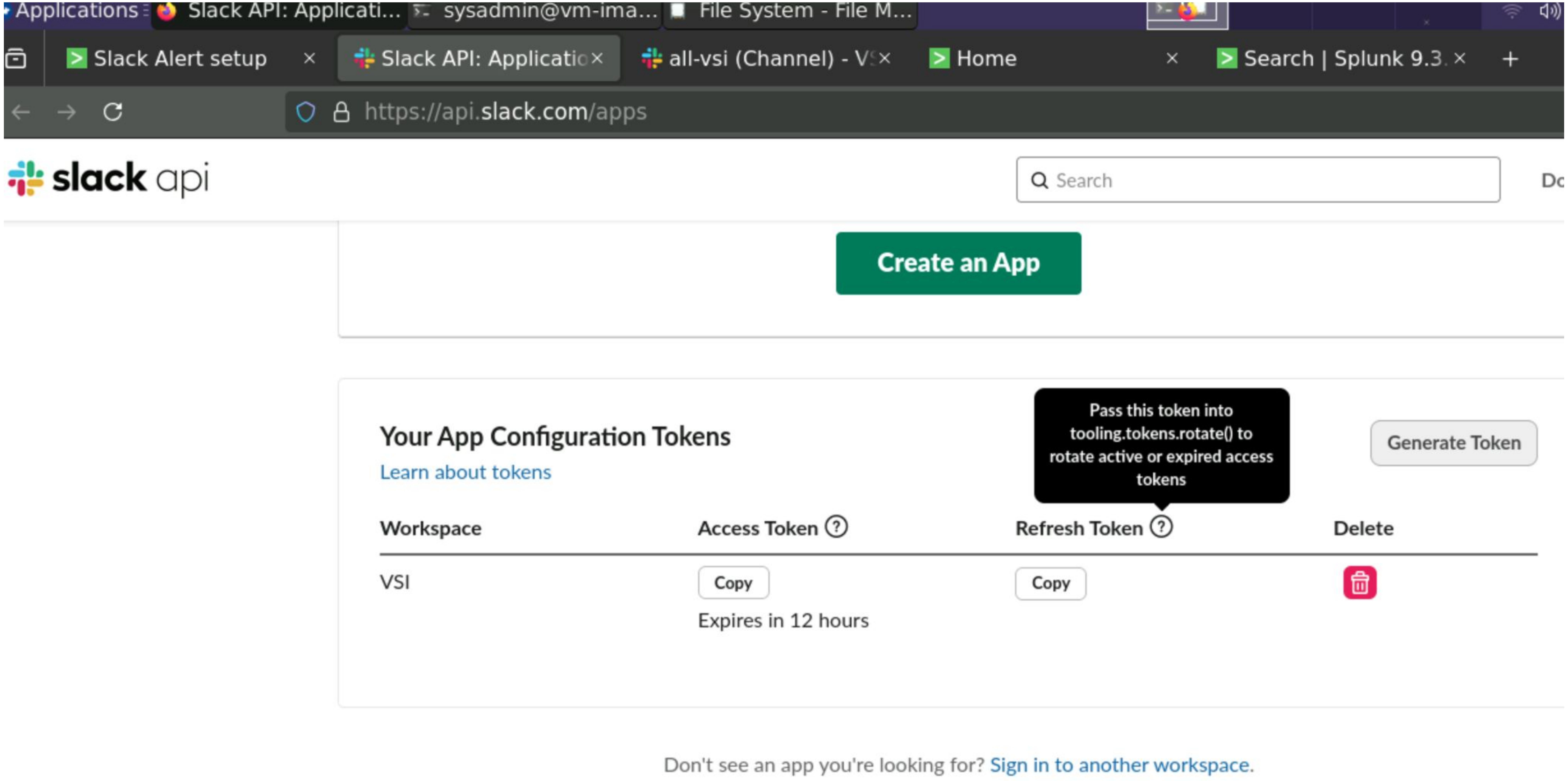
Leverages the custom alert action framework introduced in Splunk Enterprise v6.3. This alert extension framework enables full UI integration, management, dynamic parameter support, and more. This alert action was built as a reference example for the new custo... More

Category: | Author: Siegfried Puchbauer | Downloads: 83778 | Released: 4 days ago | Last Updated: 4 days ago | View on Splunkbase

Slack Notification Alerts

This app is very versatile and can be used as a way to communicate to many people in a department at once. Setting up this app could reach the SOC analyst team at the same time and could prove useful when VSI is getting attacked.

Slack Notification Alerts



Your App Configuration Tokens

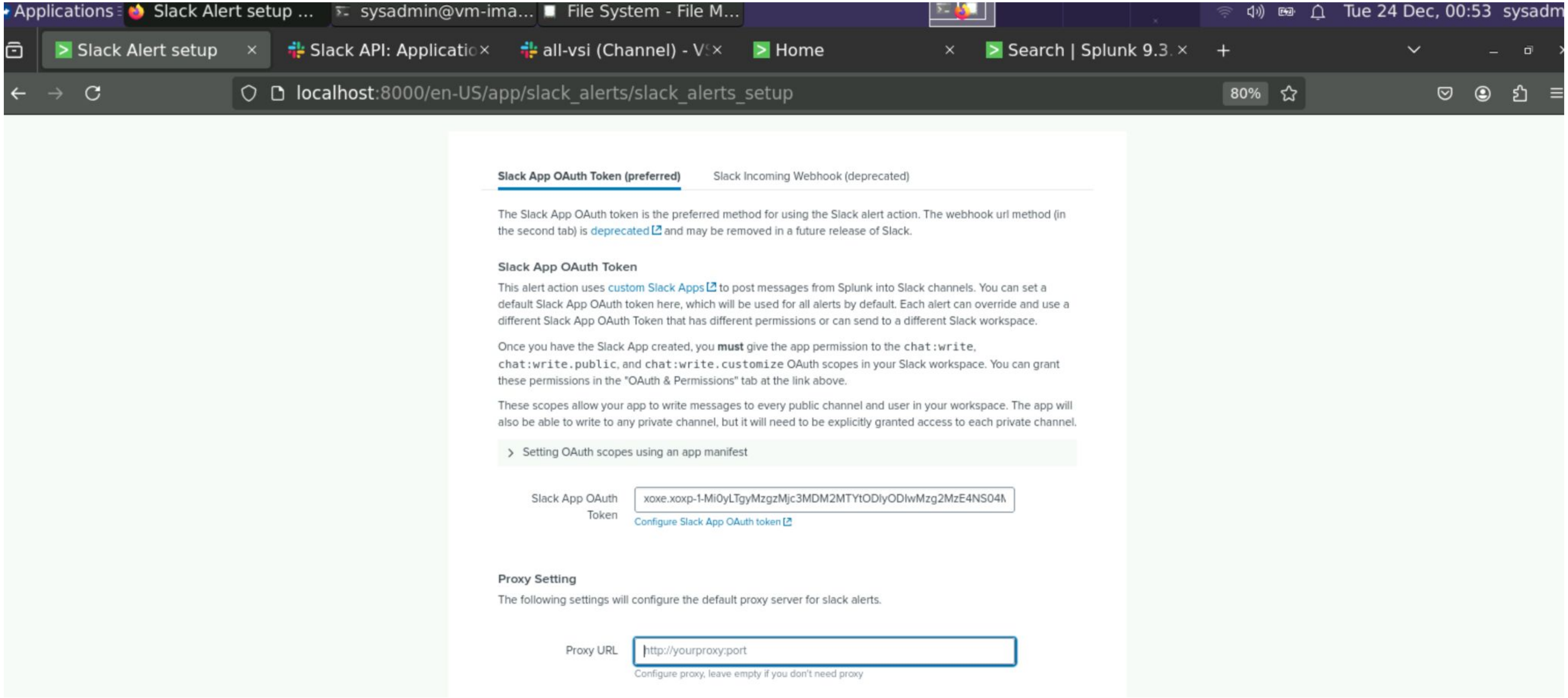
Learn about tokens

Pass this token into tooling.tokens.rotate() to rotate active or expired access tokens

Workspace	Access Token	Refresh Token	Delete
VSI	Copy Expires in 12 hours	Copy	

Don't see an app you're looking for? Sign in to another workspace.

Slack Notification Alerts



Slack App OAuth Token (preferred) | Slack Incoming Webhook (deprecated)

The Slack App OAuth token is the preferred method for using the Slack alert action. The webhook url method (in the second tab) is deprecated and may be removed in a future release of Slack.

Slack App OAuth Token

This alert action uses custom Slack Apps to post messages from Splunk into Slack channels. You can set a default Slack App OAuth token here, which will be used for all alerts by default. Each alert can override and use a different Slack App OAuth Token that has different permissions or can send to a different Slack workspace.

Once you have the Slack App created, you **must** give the app permission to the `chat:write`, `chat:write.public`, and `chat:write.customize` OAuth scopes in your Slack workspace. You can grant these permissions in the "OAuth & Permissions" tab at the link above.

These scopes allow your app to write messages to every public channel and user in your workspace. The app will also be able to write to any private channel, but it will need to be explicitly granted access to each private channel.

› Setting OAuth scopes using an app manifest

Slack App OAuth Token: xoxe.xoxp-1-Mi0yLTgyMzgzMjc3MDM2MTYtODlyODIwMzg2MzE4NS04N

Configure Slack App OAuth token

Proxy Setting

The following settings will configure the default proxy server for slack alerts.

Proxy URL: http://yourproxy:port

Configure proxy, leave empty if you don't need proxy

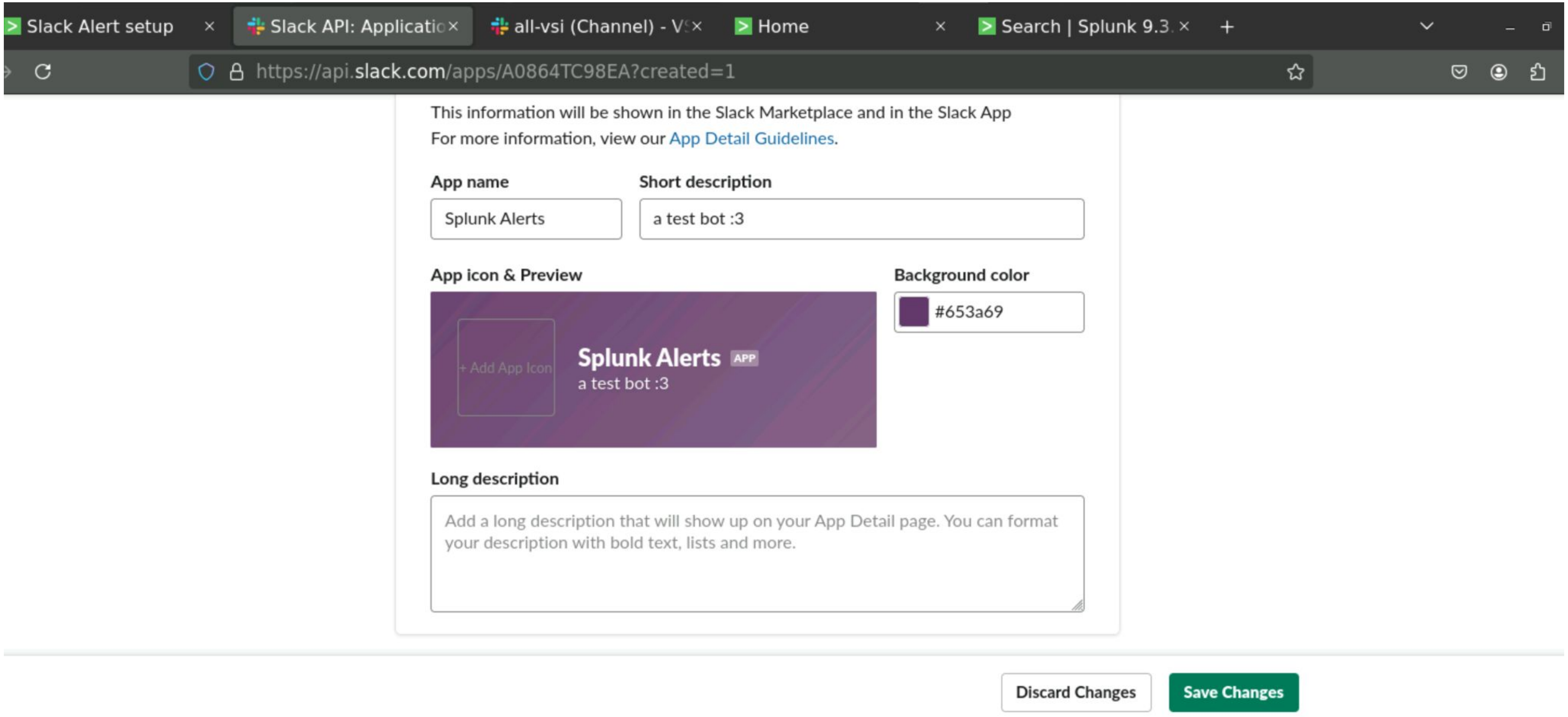
Slack Notification Alerts

slack api
Search
Docun
Create New App
Filter apps by name or workspace

Your Apps

App Name	Workspace	App Type	Distribution Status
Splunk Alerts	VSI	Modern	Not distributed

Slack Notification Alerts



This information will be shown in the Slack Marketplace and in the Slack App
For more information, view our App Detail Guidelines.

App name: Splunk Alerts

Short description: a test bot :3

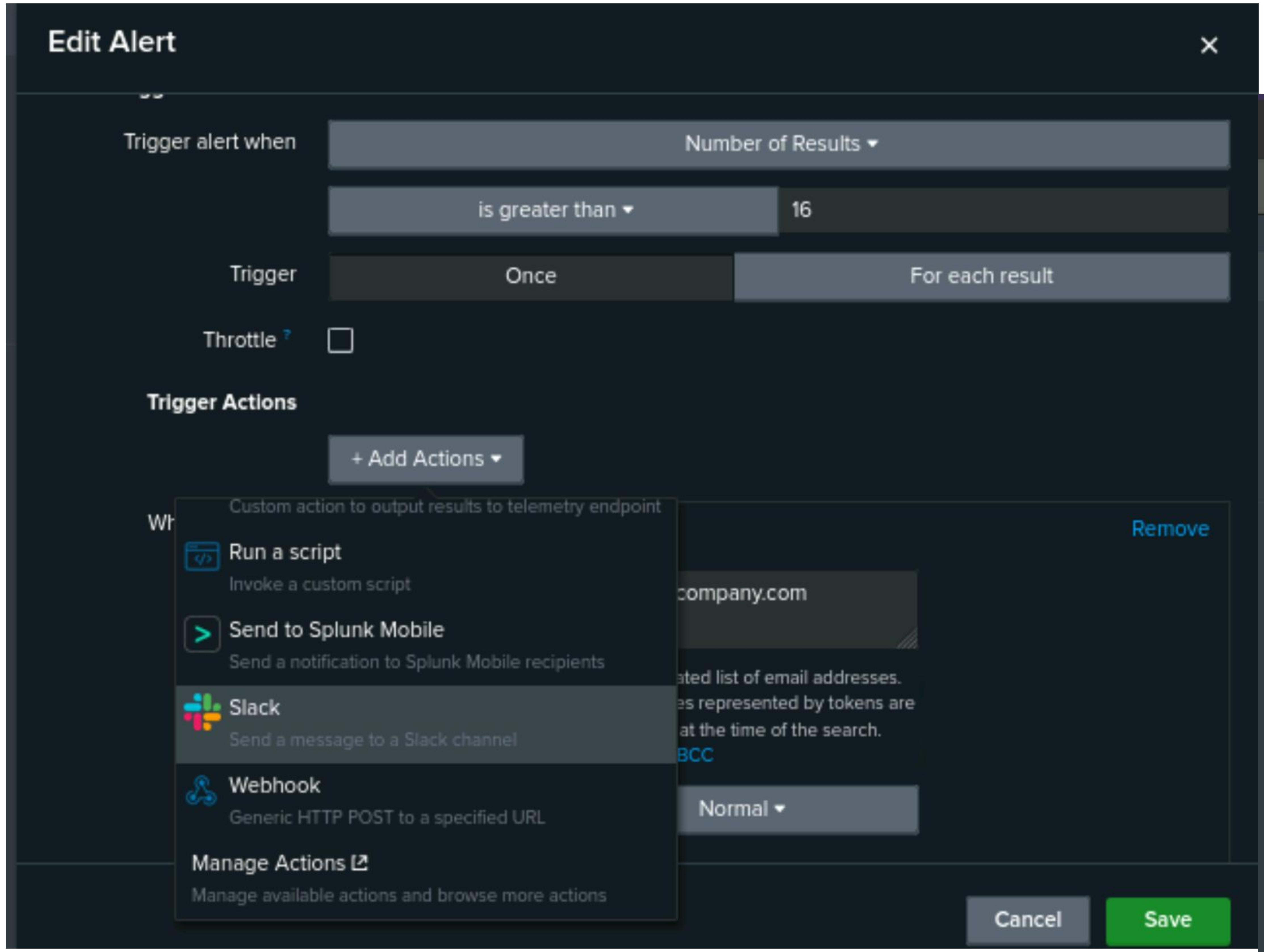
App icon & Preview

Background color: #653a69

Long description

Add a long description that will show up on your App Detail page. You can format your description with bold text, lists and more.

Slack Notification Alerts



Edit Alert

Trigger alert when: Number of Results

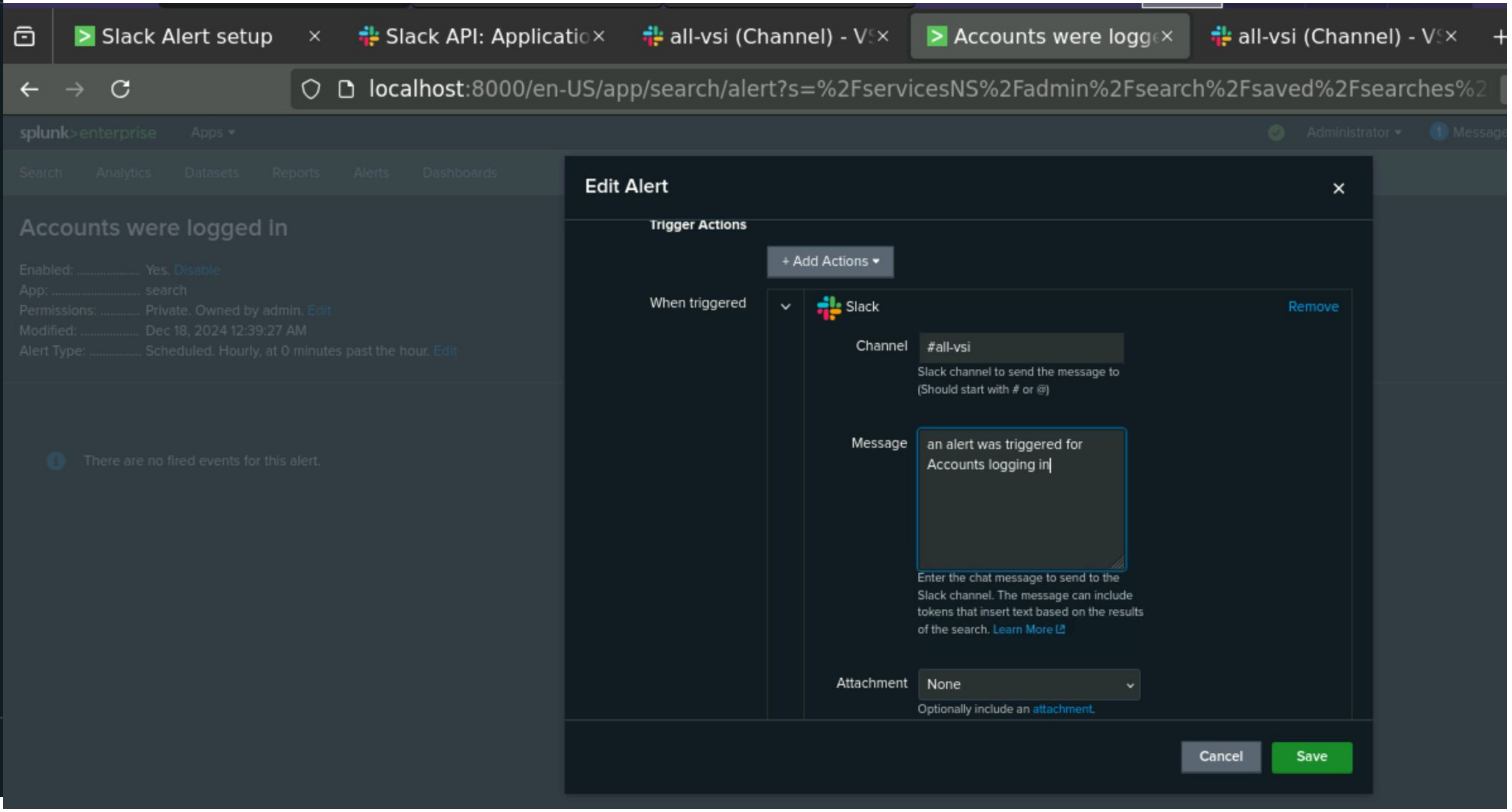
is greater than: 16

Trigger: Once | For each result

Throttle: □

Trigger Actions

+ Add Actions
Custom action to output results to telemetry endpoint
Run a script
Invoke a custom script
Send to Splunk Mobile
Send a notification to Splunk Mobile recipients
Slack
Send a message to a Slack channel
Webhook
Generic HTTP POST to a specified URL
Manage Actions
Manage available actions and browse more actions
Wh
Remove
company.com
ated list of email addresses.
es represented by tokens are
at the time of the search.
BCC
Normal
Cancel
Save



Accounts were logged in

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Dec 18, 2024 12:39:27 AM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit

There are no fired events for this alert.

Edit Alert

Trigger Actions

+ Add Actions

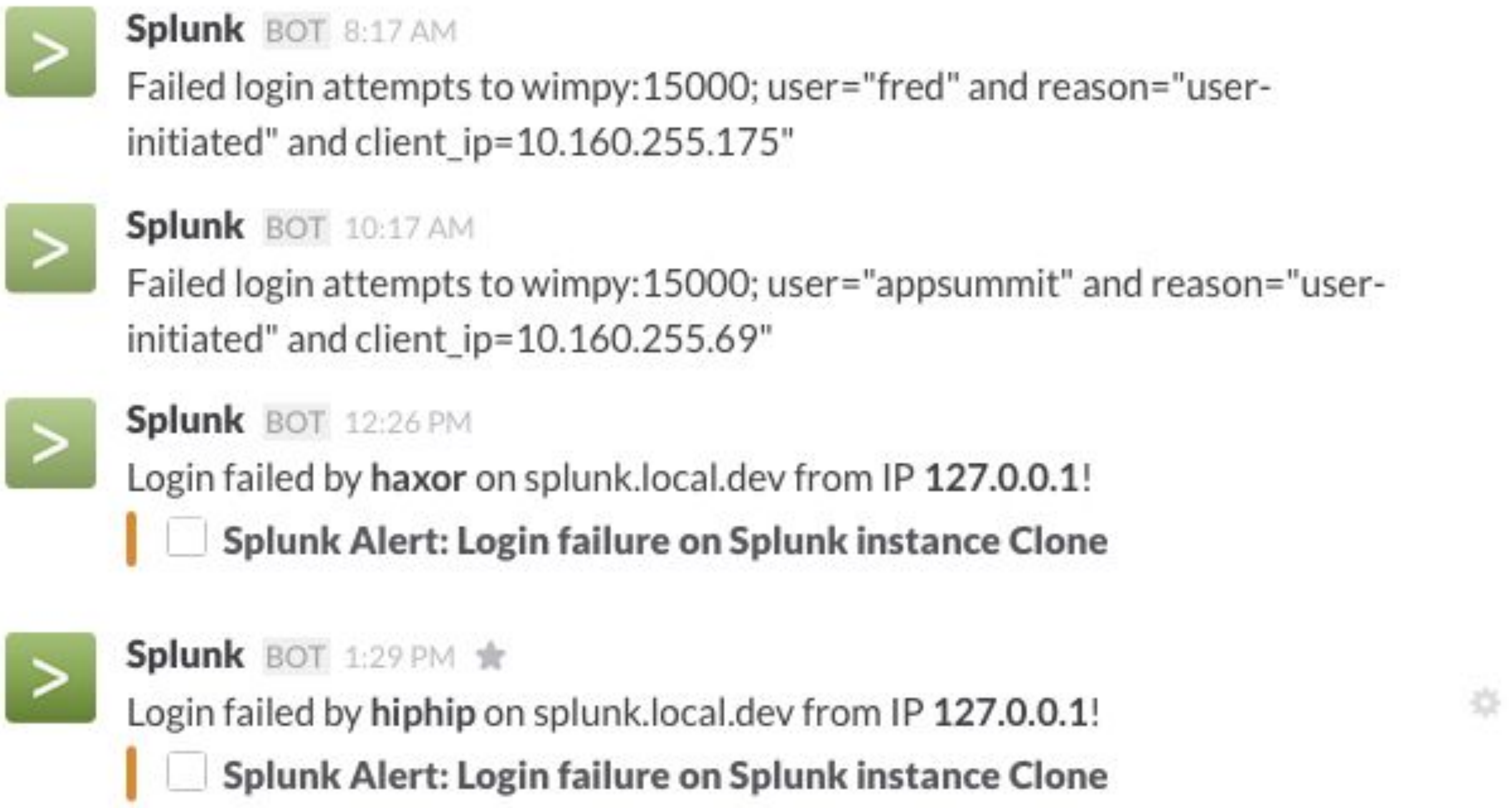
When triggered: Slack — Remove

Channel: #all-vsi
Slack channel to send the message to (Should start with # or @)

Message: an alert was triggered for Accounts logging in
Enter the chat message to send to the Slack channel. The message can include tokens that insert text based on the results of the search. Learn More

Attachment: None
Optionally include an attachment.

Slack Notification Alerts



Splunk BOT 8:17 AM
Failed login attempts to wimpy:15000; user="fred" and reason="user-initiated" and client_ip=10.160.255.175"

Splunk BOT 10:17 AM
Failed login attempts to wimpy:15000; user="appsummit" and reason="user-initiated" and client_ip=10.160.255.69"

Splunk BOT 12:26 PM
Login failed by **haxor** on splunk.local.dev from IP **127.0.0.1**!
□ **Splunk Alert: Login failure on Splunk instance Clone**

Splunk BOT 1:29 PM
Login failed by **hiphip** on splunk.local.dev from IP **127.0.0.1**!
□ **Splunk Alert: Login failure on Splunk instance Clone**

(Example of Splunk sending Alerts)

Logs Analyzed

1 Windows Logs

- User account activities (deleted, created, successful login, user locked out, etc.)
- Success and failure activities

2 Apache Logs

- Different HTTP methods
- Domains that referred/directed traffic to VSI's website
- HTTP response codes
- Activity from different countries

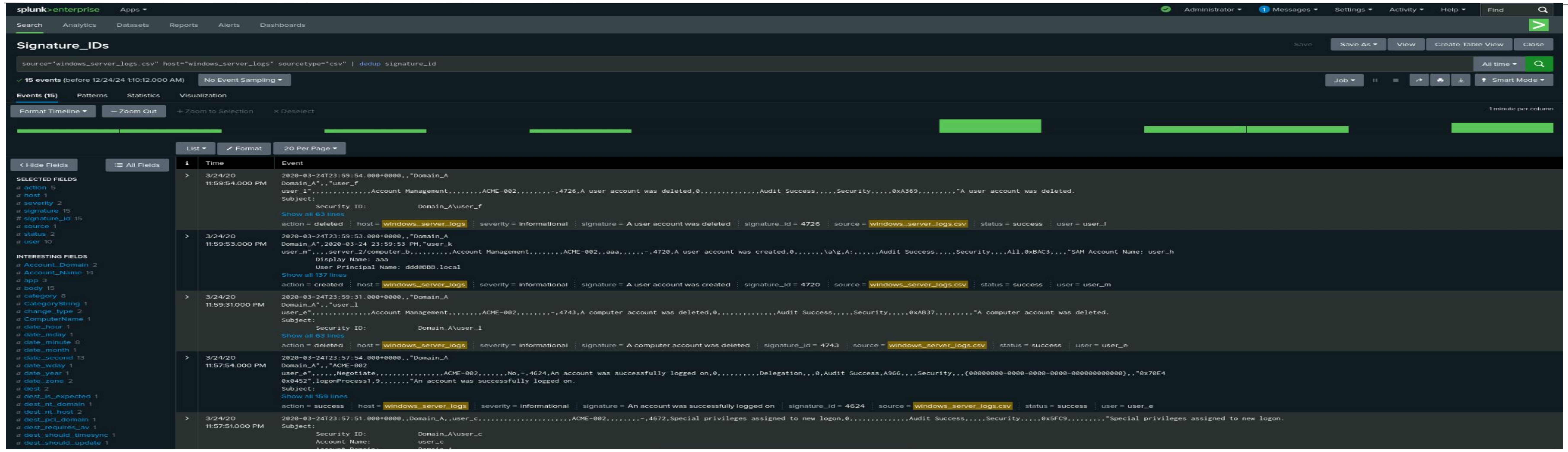
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signature IDs	Shows the ID number associated with the specific signature for Windows activity
Severity	Will show us the severity levels of the Window logs.
Success and Failure	Will report on and show us any suspicious levels of failed activity on the server.

Images of Reports—Windows



Signature_IDs

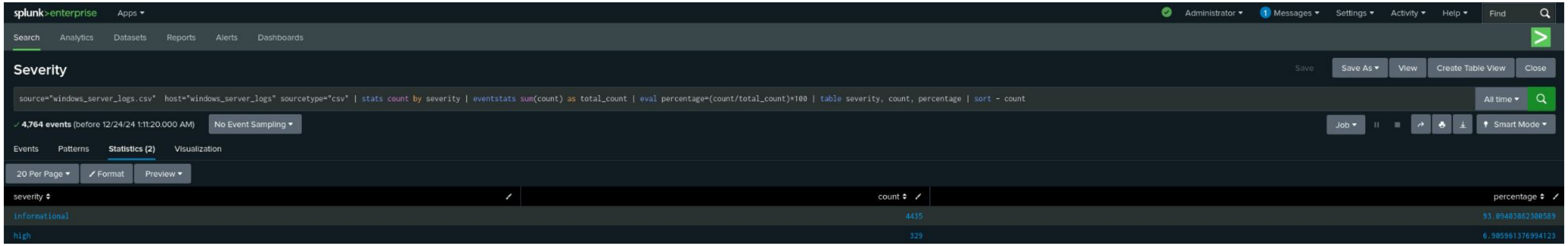
```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" | dedup signature_id
```

✓ **15 events** (before 12/24/24 1:10:12.000 AM)

SELECTED FIELDS
- action 5
- host 1
- severity 2
- signature 15
- signature_id 15
- source 1
- status 2
- user 10

INTERESTING FIELDS
- Account_Domain 2
- Account_Name 14
- app 3
- body 15
- category 8
- CategoryString 1
- change_type 2
- ComputerName 1
- date_hour 1
- date_mday 1
- date_minute 8
- date_month 1
- date_second 13
- date_wday 1
- date_year 1
- date_zone 2
- dest 2
- dest_is_expected 1
- dest_nt_domain 1
- dest_nt_host 2
- dest_pci_domain 1
- dest_requires_av 1
- dest_should_timesync 1
- dest_should_update 1

```
i  Time                Event
>  3/24/20             2020-03-24T23:59:54.000+0000,,"Domain_A
   11:59:54.000 PM     Domain_A",,"user_f
                       user_l",,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A user account was deleted.
                       Subject:
                               Security ID:           Domain_A\user_f
                       Show all 63 lines
                       action = deleted | host = windows_server_logs | severity = informational | signature = A user account was deleted | signature_id = 4726 | source = windows_server_logs.csv | status = success | user = user_l
>  3/24/20             2020-03-24T23:59:53.000+0000,,"Domain_A
   11:59:53.000 PM     Domain_A",2020-03-24 23:59:53 PM,"user_k
                       user_m",,,,server_2/computer_b,,,,,,,,,Account Management,,,,,,,ACME-002,,aaa,,,,,,-,4720,A user account was created,0,,,,,,,\a\g,A:,,,,,,Audit Success,,,,,Security,,,,All,0xBAC3,,,,"SAM Account Name: user_h
                               Display Name: aaa
                               User Principal Name: ddd@BBB.local
                       Show all 137 lines
                       action = created | host = windows_server_logs | severity = informational | signature = A user account was created | signature_id = 4720 | source = windows_server_logs.csv | status = success | user = user_m
>  3/24/20             2020-03-24T23:59:31.000+0000,,"Domain_A
   11:59:31.000 PM     Domain_A",,"user_l
                       user_e",,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,-,4743,A computer account was deleted,0,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xAB37,,,,,,,,,"A computer account was deleted.
                       Subject:
                               Security ID:           Domain_A\user_l
                       Show all 63 lines
                       action = deleted | host = windows_server_logs | severity = informational | signature = A computer account was deleted | signature_id = 4743 | source = windows_server_logs.csv | status = success | user = user_e
>  3/24/20             2020-03-24T23:57:54.000+0000,,"Domain_A
   11:57:54.000 PM     Domain_A",,"ACME-002
                       user_e",,,,,,Negotiate,,,,,,,,,,,,,,,ACME-002,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,,Delegation,,,0,Audit Success,A966,,,,Security,,,{00000000-0000-0000-0000-000000000000},,"0x70E4
                       0x0452",logonProcess1,9,,,,,,,"An account was successfully logged on.
                       Subject:
                       Show all 159 lines
                       action = success | host = windows_server_logs | severity = informational | signature = An account was successfully logged on | signature_id = 4624 | source = windows_server_logs.csv | status = success | user = user_e
>  3/24/20             2020-03-24T23:57:51.000+0000,,Domain_A,,user_c,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,-,4672,Special privileges assigned to new logon,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x5FC9,,,,,,,,,"Special privileges assigned to new logon.
   11:57:51.000 PM     Subject:
                               Security ID:           Domain_A\user_c
                               Account Name:          user_c
```

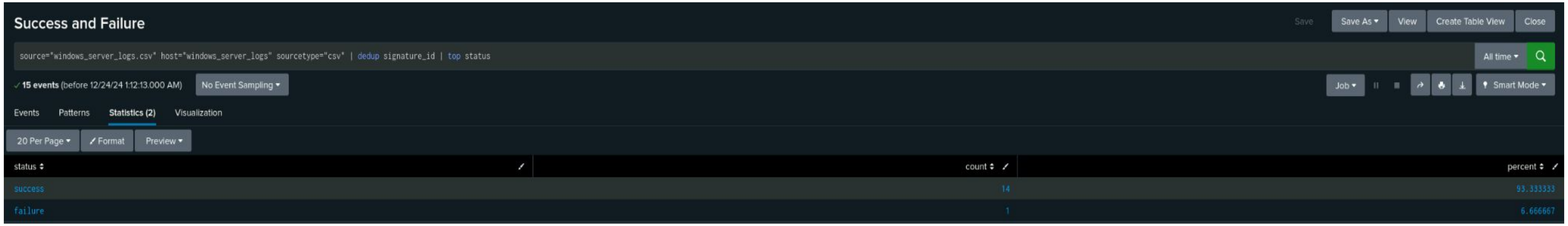


Severity

```
source="windows_server_logs.csv"  host="windows_server_logs" sourcetype="csv" | stats count by severity | eventstats sum(count) as total_count | eval percentage=(count/total_count)*100 | table severity, count, percentage | sort - count
```

✓ **4,764 events** (before 12/24/24 1:11:20.000 AM)

severity	count	percentage
informational	4435	93.09403862300589
high	329	6.905961376994123



Success and Failure

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" | dedup signature_id | top status
```

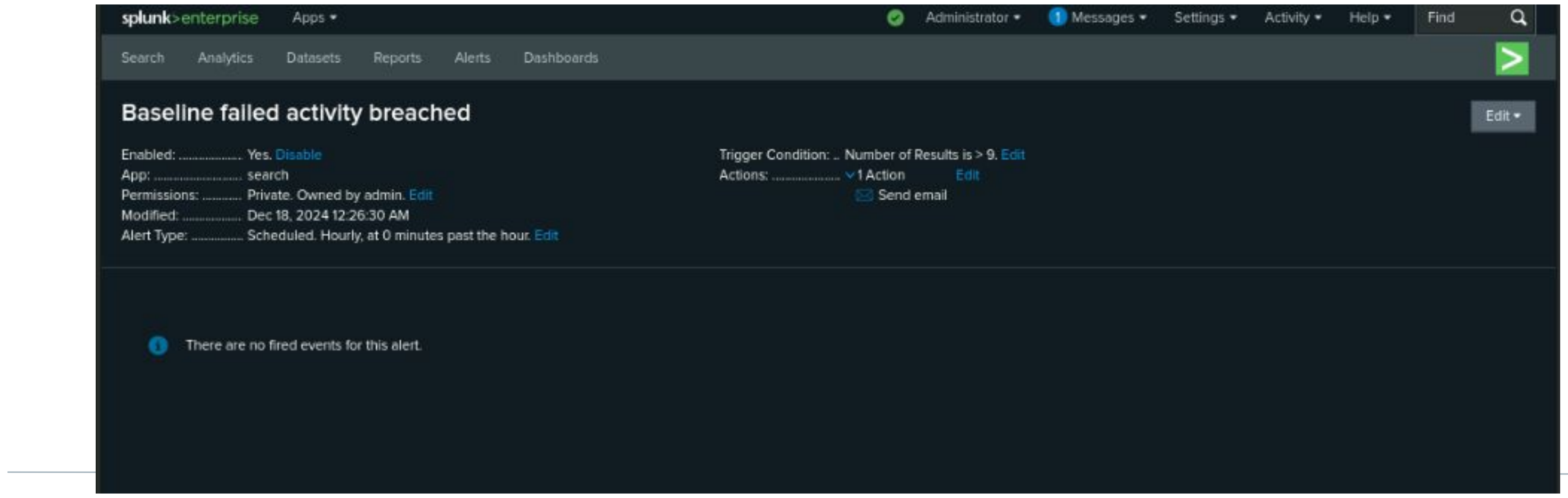
✓ **15 events** (before 12/24/24 1:12:13.000 AM)

status	count	percent
success	14	93.333333
failure	1	6.666667

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Baseline failed activity breached	Threshold of hourly level of failed has been reacherd	6	9
Successful login baseline breached	Threshold of hourly level of successful login has been reacherd	12	15

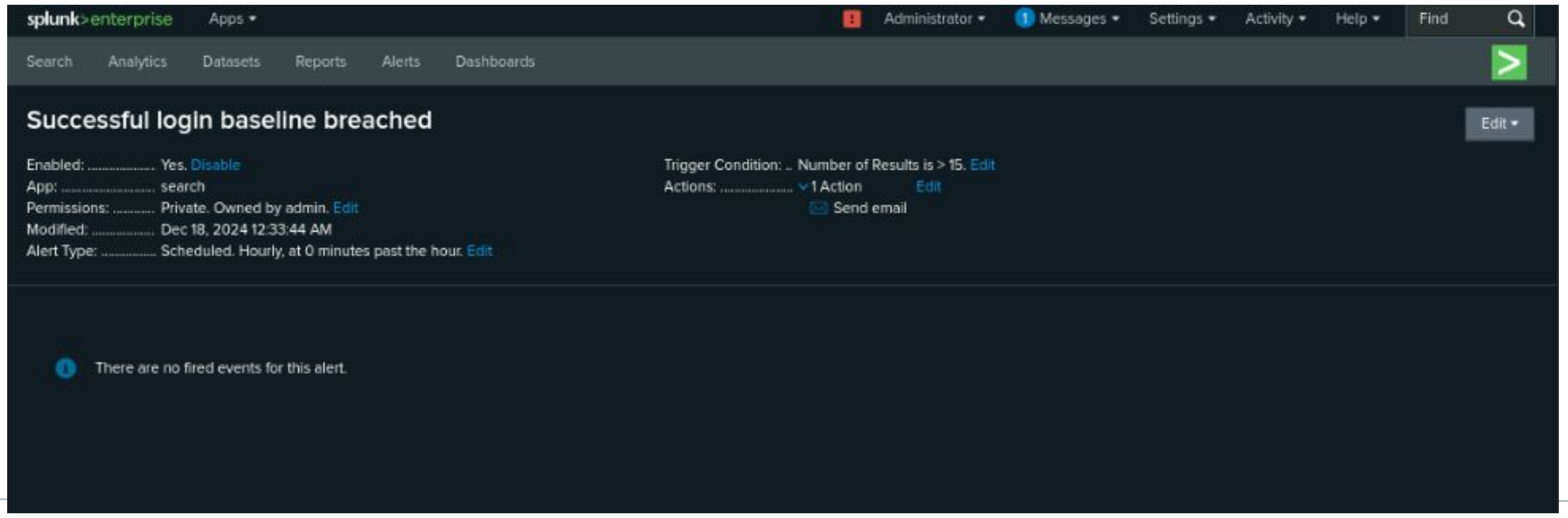


Baseline failed activity breached

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Dec 18, 2024 12:26:30 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 9. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.



Successful login baseline breached

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Dec 18, 2024 12:33:44 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

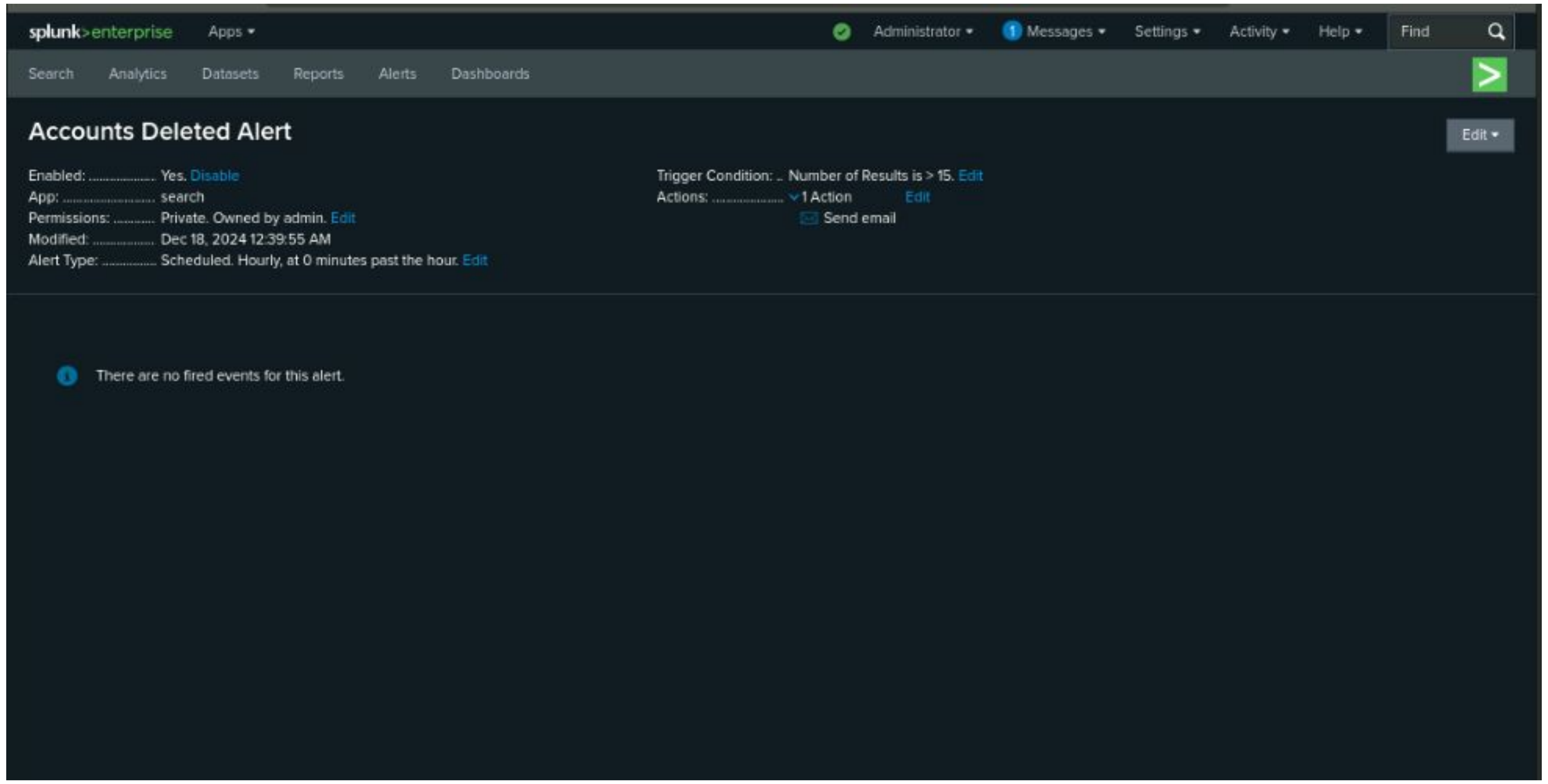
Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Accounts Deleted	Hourly count of user accounts deleted	13	15



Accounts Deleted Alert

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Dec 18, 2024 12:39:55 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

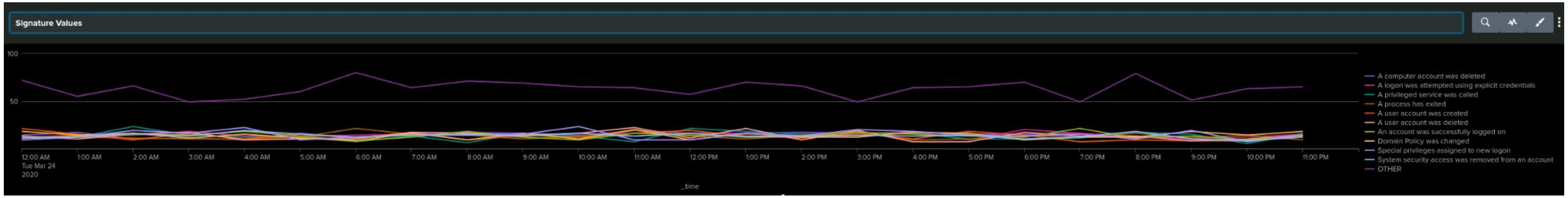
Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... 1 Action Edit
Send email

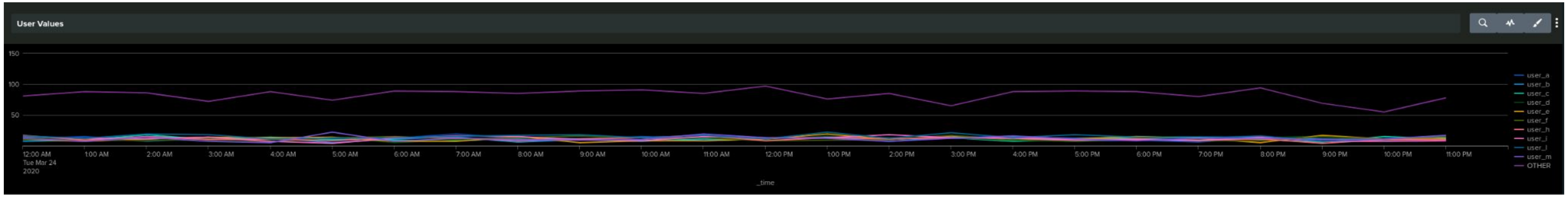
There are no fired events for this alert.

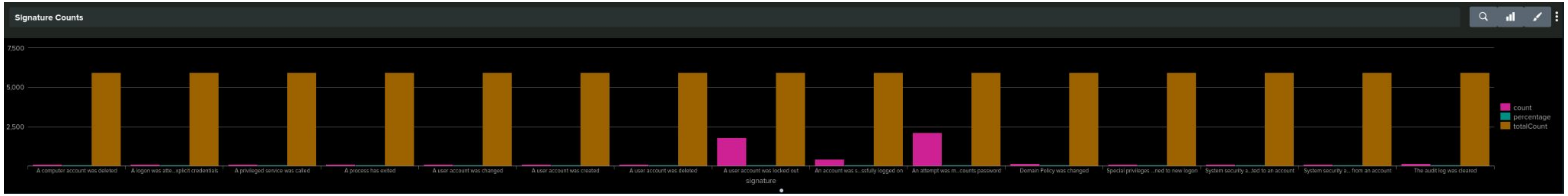
Alerts—Windows

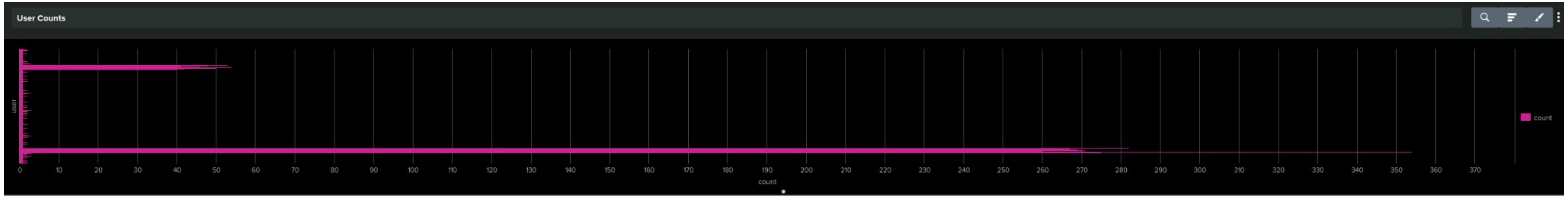
JUSTIFICATION: These thresholds were set based on the baselines analyzed, to avoid an influx of unnecessary alerts for normal activity

Dashboards—Windows









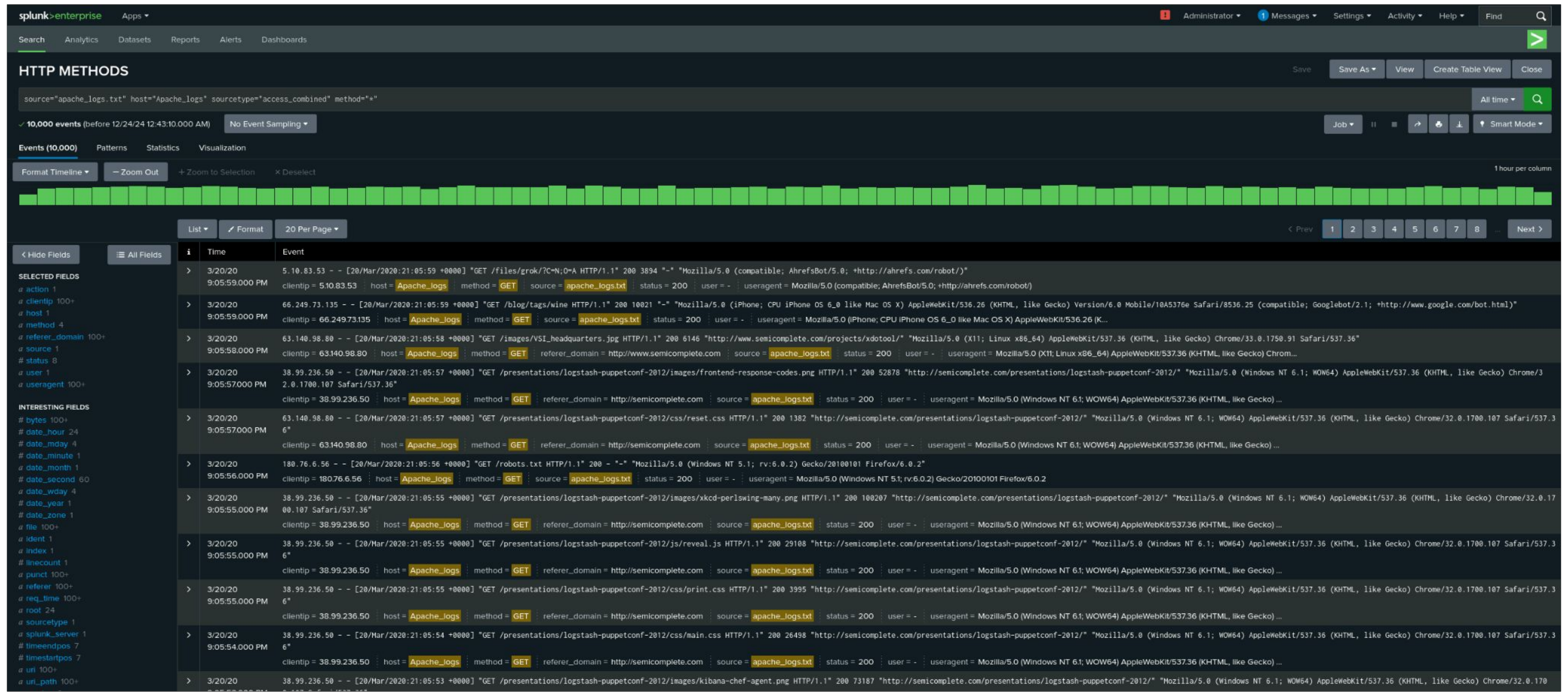
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP METHODS	Provides insight into the type of HTTP activity being requested against VSI’s web server.
HTTP POST	Report to help provide insight into any suspicious levels of HTTP responses
Top 10 Referrer Domains	Will help in assisting VSI with identifying any suspicious referrers

Images of Reports—Apache



HTTP METHODS

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" method="*"
```

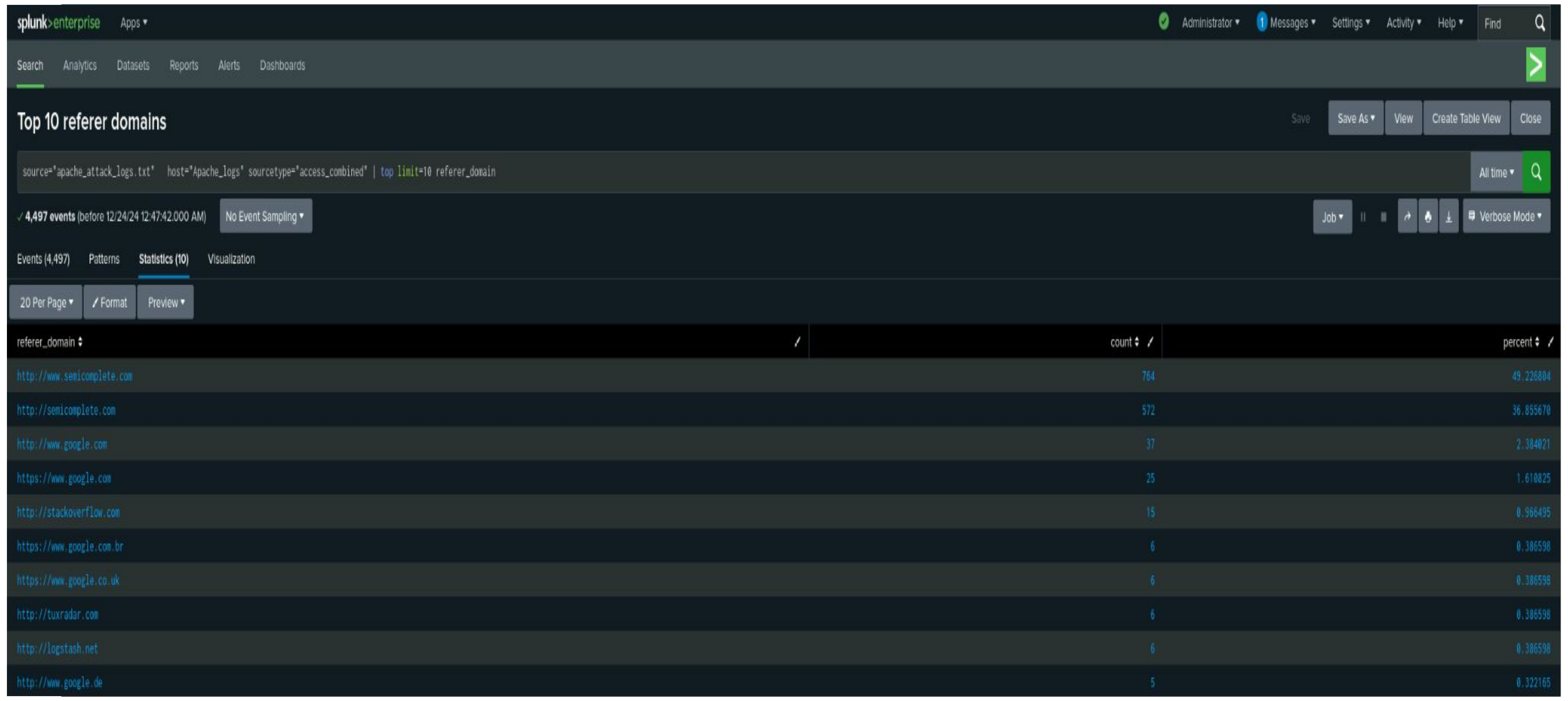
✓ **10,000 events** (before 12/24/24 12:43:10.000 AM)

Events (10,000)

SELECTED FIELDS
- a action 1
- a clientip 100+
- a host 1
- a method 4
- a referer_domain 100+
- a source 1
- # status 8
- a user 1
- a useragent 100+

INTERESTING FIELDS
- # bytes 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 punct 100+
- a referer 100+
- a req_time 100+
- a root 24
- a sourcetype 1
- a splunk_server 1
- # timeendpos 7
- # timestartpos 7
- a uri 100+
- a uri_path 100+

```
i  Time                  Event
>  3/20/20               5.10.83.53 - - [20/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/)"
   9:05:59.000 PM        clientip = 5.10.83.53 | host = Apache_logs | method = GET | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)
>  3/20/20               66.249.73.135 - - [20/Mar/2020:21:05:59 +0000] "GET /blog/tags/wine HTTP/1.1" 200 10021 "-" "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)"
   9:05:59.000 PM        clientip = 66.249.73.135 | host = Apache_logs | method = GET | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (K...
>  3/20/20               63.140.98.80 - - [20/Mar/2020:21:05:58 +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"
   9:05:58.000 PM        clientip = 63.140.98.80 | host = Apache_logs | method = GET | referer_domain = http://www.semicomplete.com | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom...
>  3/20/20               38.99.236.50 - - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/3
   9:05:57.000 PM        2.0.1700.107 Safari/537.36"
                         clientip = 38.99.236.50 | host = Apache_logs | method = GET | referer_domain = http://semicomplete.com | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) ...
>  3/20/20               63.140.98.80 - - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/css/reset.css HTTP/1.1" 200 1382 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.3
   9:05:57.000 PM        6"
                         clientip = 63.140.98.80 | host = Apache_logs | method = GET | referer_domain = http://semicomplete.com | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) ...
>  3/20/20               180.76.6.56 - - [20/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"
   9:05:56.000 PM        clientip = 180.76.6.56 | host = Apache_logs | method = GET | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2
>  3/20/20               38.99.236.50 - - [20/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/images/xkcd-perlswing-many.png HTTP/1.1" 200 100207 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.17
   9:05:55.000 PM        00.107 Safari/537.36"
                         clientip = 38.99.236.50 | host = Apache_logs | method = GET | referer_domain = http://semicomplete.com | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) ...
>  3/20/20               38.99.236.50 - - [20/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/js/reveal.js HTTP/1.1" 200 29108 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.3
   9:05:55.000 PM        6"
                         clientip = 38.99.236.50 | host = Apache_logs | method = GET | referer_domain = http://semicomplete.com | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) ...
>  3/20/20               38.99.236.50 - - [20/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/css/print.css HTTP/1.1" 200 3995 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.3
   9:05:55.000 PM        6"
                         clientip = 38.99.236.50 | host = Apache_logs | method = GET | referer_domain = http://semicomplete.com | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) ...
>  3/20/20               38.99.236.50 - - [20/Mar/2020:21:05:54 +0000] "GET /presentations/logstash-puppetconf-2012/css/main.css HTTP/1.1" 200 26498 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.3
   9:05:54.000 PM        6"
                         clientip = 38.99.236.50 | host = Apache_logs | method = GET | referer_domain = http://semicomplete.com | source = apache_logs.txt | status = 200 | user = - | useragent = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) ...
>  3/20/20               38.99.236.50 - - [20/Mar/2020:21:05:53 +0000] "GET /presentations/logstash-puppetconf-2012/images/kibana-chef-agent.png HTTP/1.1" 200 73187 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.170
```



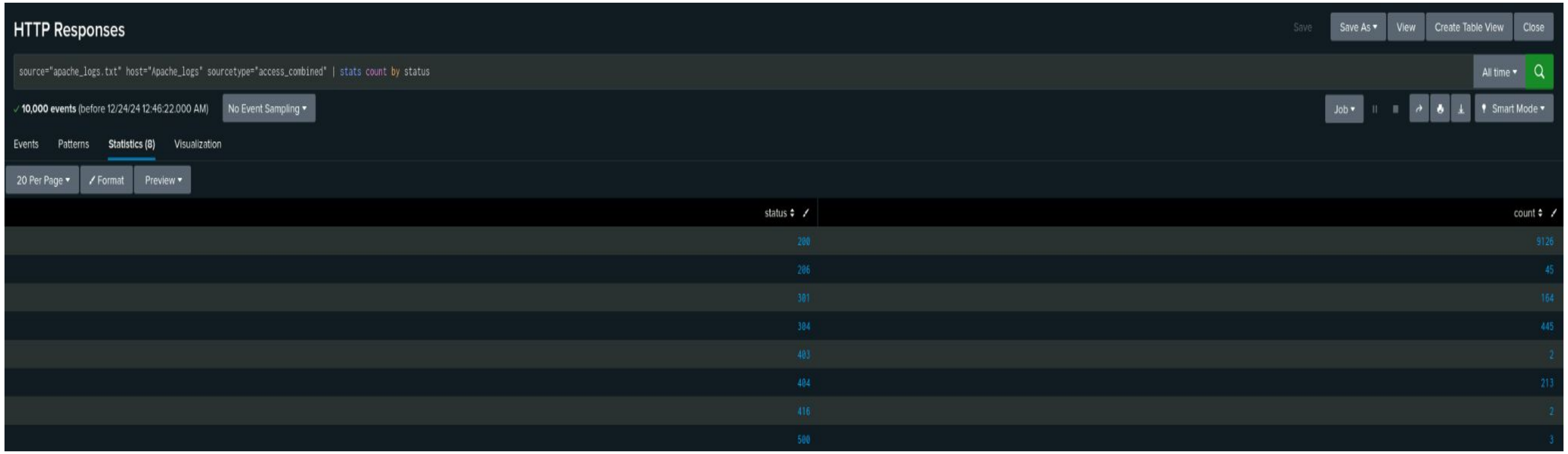
Top 10 referer domains

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | top limit=10 referer_domain
```

✓ **4,497 events** (before 12/24/24 12:47:42.000 AM)

Statistics (10)

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



HTTP Responses

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | stats count by status
```

✓ **10,000 events** (before 12/24/24 12:46:22.000 AM)

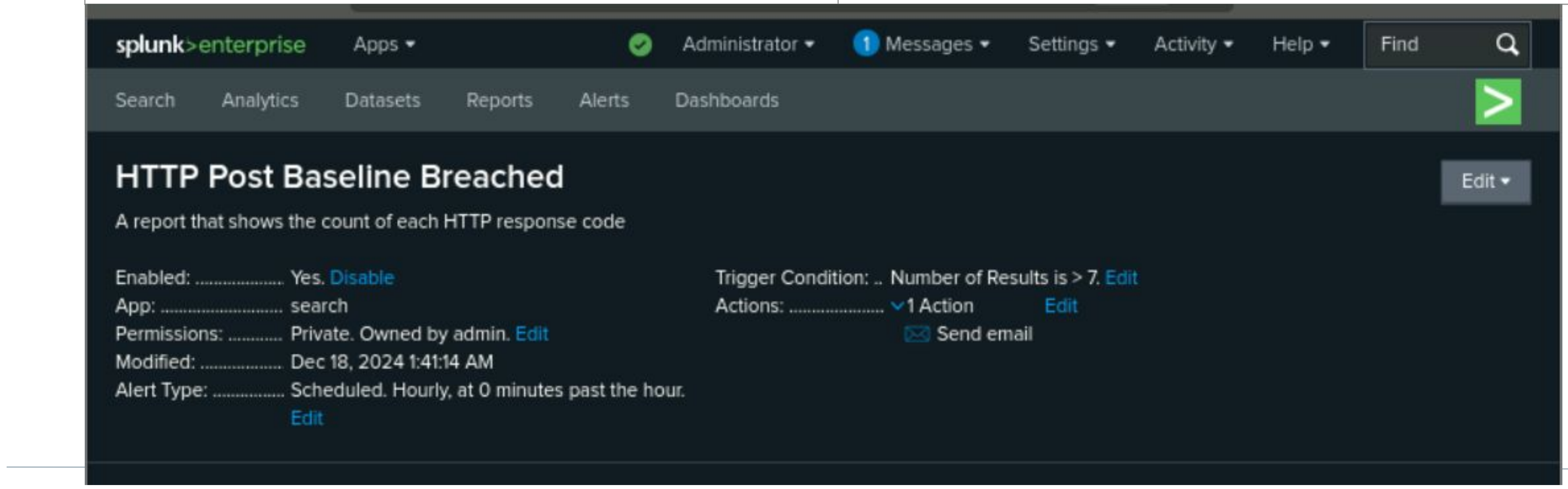
Statistics (8)

status	count
200	9126
206	45
301	164
304	445
403	2
404	213
416	2
500	3

Alerts—Apache

Designed the following alerts:

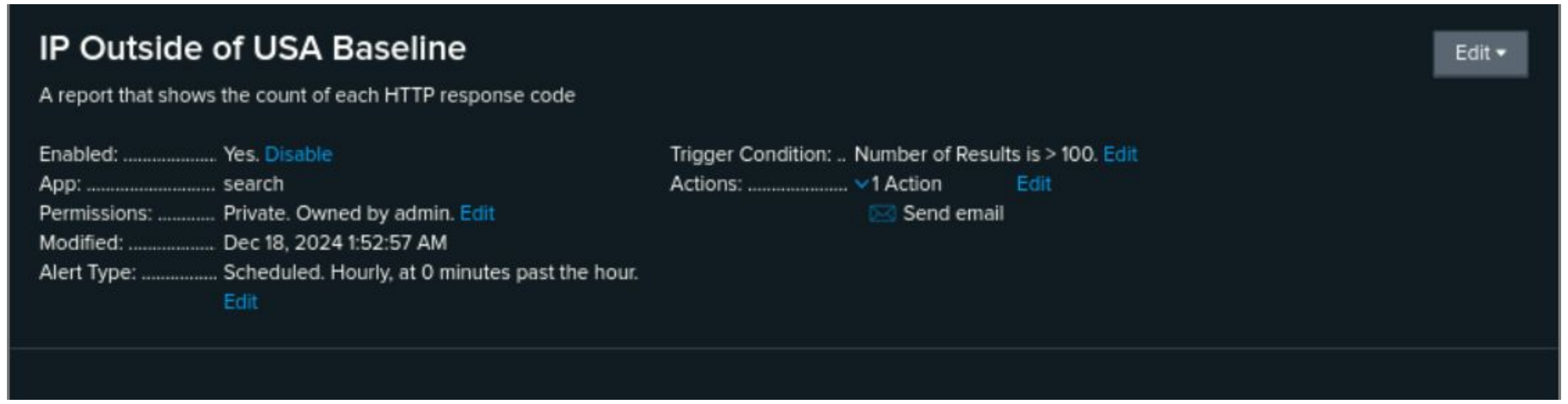
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP Post Baseline Breached	Monitors the hourly count of the HTTP POST method	2	7
IP Outside of USA Baseline	Monitors hourly activity from countries other than USA	80	100



HTTP Post Baseline Breached

A report that shows the count of each HTTP response code

```
Enabled: .................. Yes. Disable            Trigger Condition: .. Number of Results is > 7. Edit
App: ........................ search                 Actions: .................... 1 Action        Edit
Permissions: ........... Private. Owned by admin. Edit                        Send email
Modified: ................. Dec 18, 2024 1:41:14 AM
Alert Type: ............... Scheduled. Hourly, at 0 minutes past the hour.
                            Edit
```

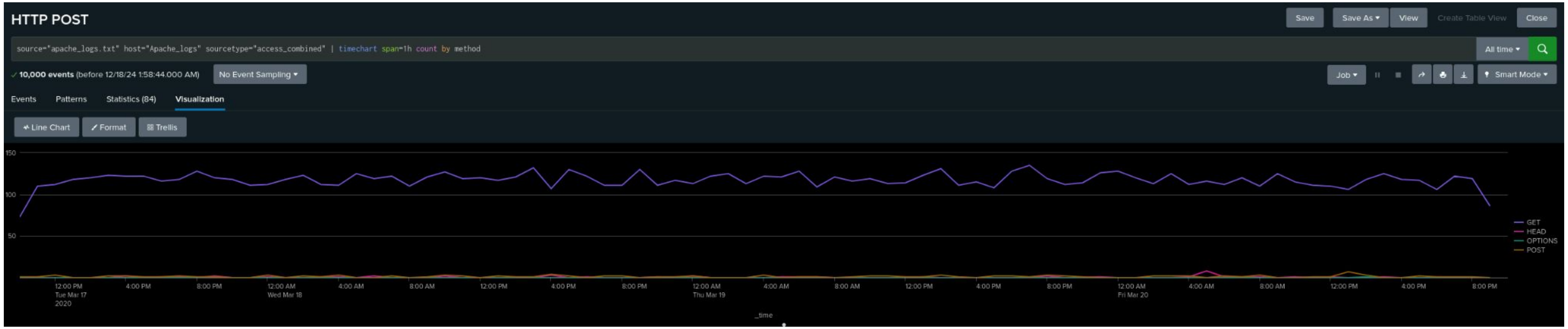


IP Outside of USA Baseline

A report that shows the count of each HTTP response code

```
Enabled: .................. Yes. Disable            Trigger Condition: .. Number of Results is > 100. Edit
App: ........................ search                 Actions: .................... 1 Action        Edit
Permissions: ........... Private. Owned by admin. Edit                        Send email
Modified: ................. Dec 18, 2024 1:52:57 AM
Alert Type: ............... Scheduled. Hourly, at 0 minutes past the hour.
                            Edit
```

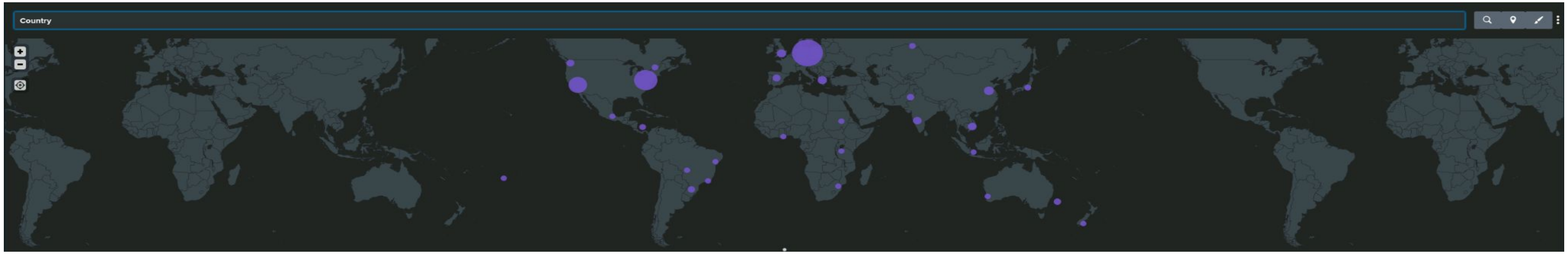
Dashboards—Apache

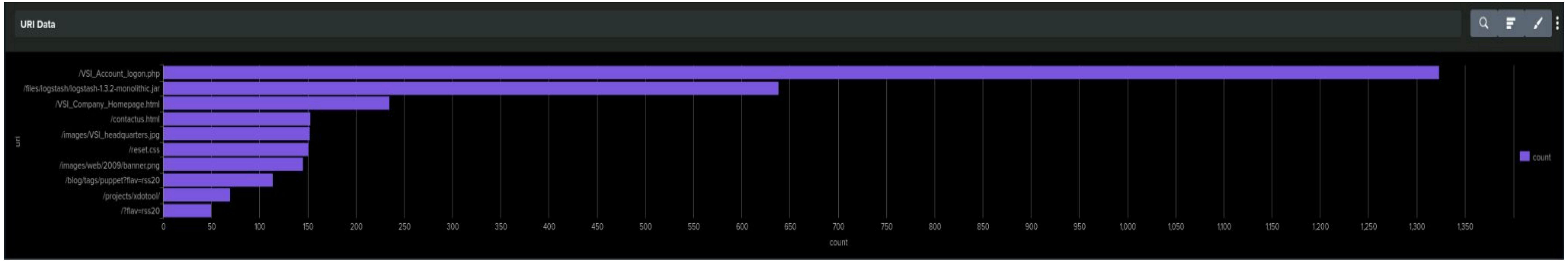


HTTP POST

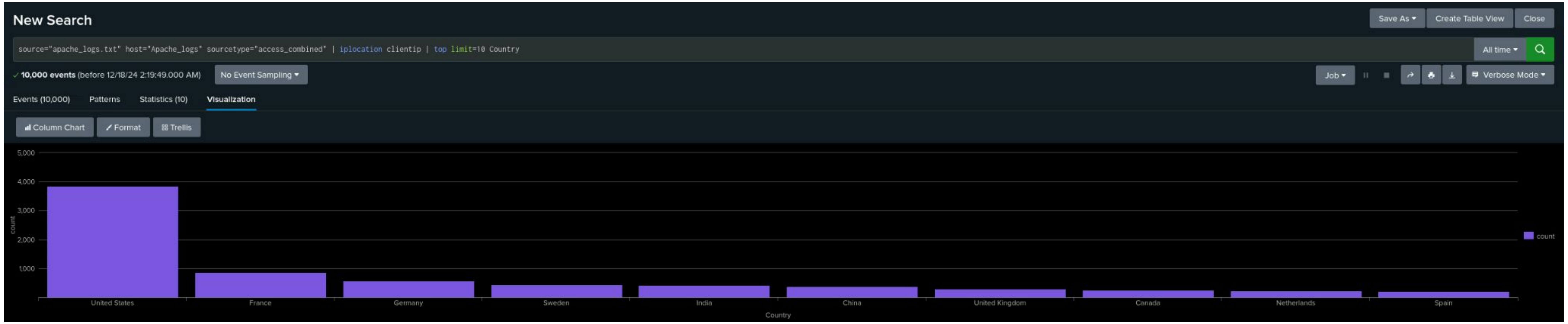
```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | timechart span=1h count by method
```

✓ **10,000 events** (before 12/18/24 1:58:44.000 AM)



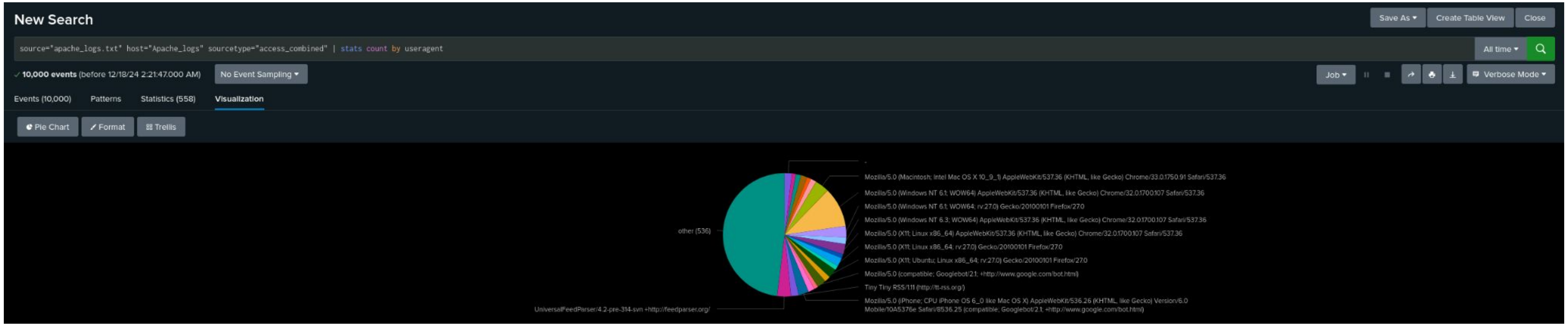


Dashboards—Apache Cont.



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | top limit=10 Country
```

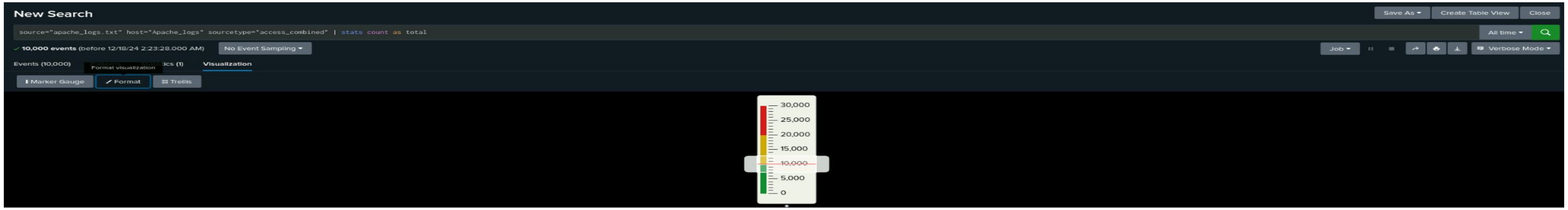
✓ **10,000 events** (before 12/18/24 2:19:49.000 AM)



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | stats count by useragent
```

✓ **10,000 events** (before 12/18/24 2:21:47.000 AM)

New Search
Save As
Create Table View
Close
All time
No Event Sampling
Job
Verbose Mode
Events (10,000)
Patterns
Statistics (558)
Visualization
Pie Chart
Format
Trellis
-
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
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Tiny Tiny RSS/1.11 (http://tt-rss.org/)
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)
other (536)
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | stats count as total
```

✓ **10,000 events** (before 12/18/24 2:23:28.000 AM)

Attack Analysis

Attack Summary—Windows

- The Windows attack system showed a significant rise in high severity levels after the attack, compared to the mostly informational levels seen earlier. There were also more successful events recorded than failures. The alert analysis noted an unusual number of failed activities.

- Failed Logins: On March 25, 2020, at 8 AM, there were 35 failed login attempts, which exceeded the threshold. No changes are suggested.

- Successful Logins: There was an unusual spike in successful logins, with 196 events happening within one hour. Most of these involved the user "user_J" at 11 AM on March 25, 2020. Which exceeded the threshold and no changes were made.

Attack Summary—Windows

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

Alert Analysis:

- The analysis revealed a suspicious volume of failed activities, indicating potential unauthorized access attempts or misconfigurations.

Deleted Account:

-
- The threshold for alerts was set to trigger when the number of deleted accounts exceeded.

Signatures:

- **"A user account was locked out"**:
  - This signature indicates that an account was repeatedly accessed with incorrect credentials, leading to it being locked out.
  - The events for this signature occurred between 1:40 AM and 2:40 AM.
  - The peak count of these events reached 785, suggesting a significant number of lockout attempts during this period.
- **"An attempt was made to reset an account's password"**:
  - This signature points to attempts made to reset the password of an account, which could be a sign of an attack aimed at gaining unauthorized access.
  - These events were recorded between 9:10 AM and 11:00 AM.
  - The peak count of these events was 397, indicating a notable volume of password reset attempts.

Attack Summary—Windows

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

Suspicious Activity Analysis:

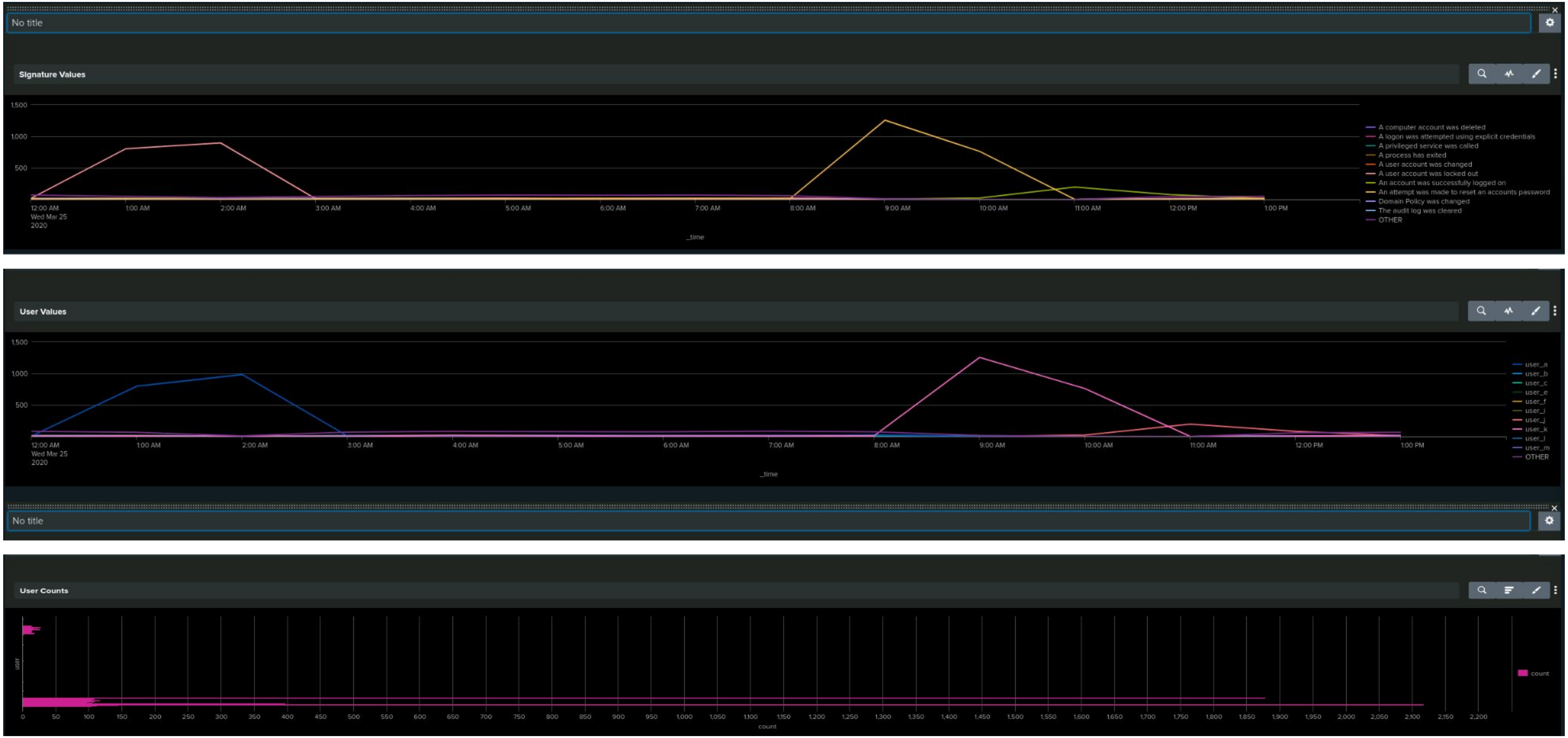
Two users, User_A and User_K, exhibited suspicious activity.

- **User_A:** Activity was noted between 1:40 am and 2:40 am, with a peak count of 785 users.
- **User_K:** Activity was noted between 9:10 am and 11:00 am, with a peak count of 397 users.

Suspicious signatures observed included:

1. “A user account was locked out” peaking at a count of 785 between 1:40 am and 2:40 am.
2. “An attempt was made to reset an account's password” peaking at a count of 397 between 9:10 am and 11:00 am.

Screenshots of Attack Logs



Attack Summary—Apache

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

Upon reviewing the reports, we identified malicious activities where attackers utilized HTTP POST and GET methods to brute force the VSI logon page.

- We observed significant fluctuations in HTTP response codes, particularly "404" (Not Found) and "200" (OK). These variations are indicative of unauthorized attempts to access resources.
- Our analysis highlighted high volumes of suspicious activities originating from international locations, with a notable concentration from Ukraine.
- Alerts were triggered for POST method activities between 8 PM and 9 PM, showing approximately 1,296 events. This is a substantial increase from the typical event count in the 100s, strongly suggesting that these activities are indeed suspicious and likely perpetrated by attackers.

Attack Summary—Apache

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

- On March 25th, we observed a suspicious volume of international activity between 8 PM and 9 PM. This activity fell within our defined thresholds, and an alert would have been triggered accordingly.

- Additionally, there was a significant volume of HTTP POST activity during the same period, peaking at 1,296 events. Our established thresholds were accurate, and an alert would have been triggered for this as well.

Attack Summary—Apache

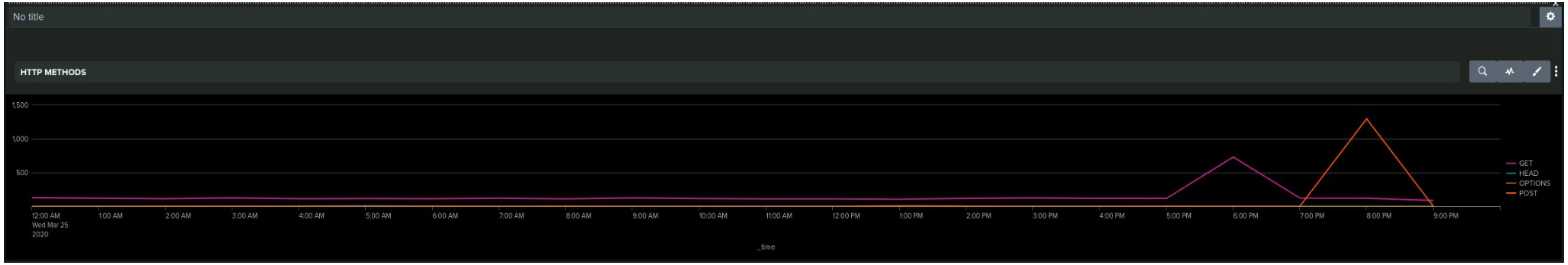
Summarize your findings from your dashboards when analyzing the attack logs.

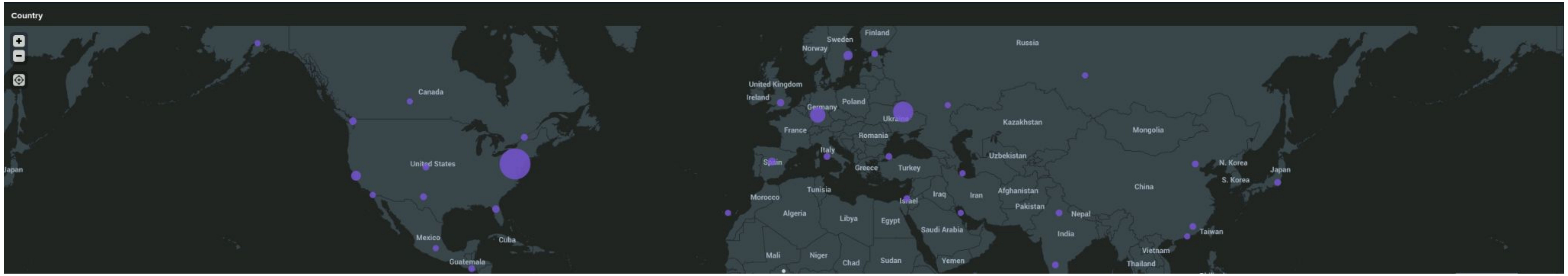
- Our Time Chart of HTTP methods revealed suspicious volumes of GET and POST methods.
  - The GET attack went from 5pm to 7pm and peaked with a count of 729.
  - The POST attack went from 7pm to 9pm and peaked with a count of 1,296.

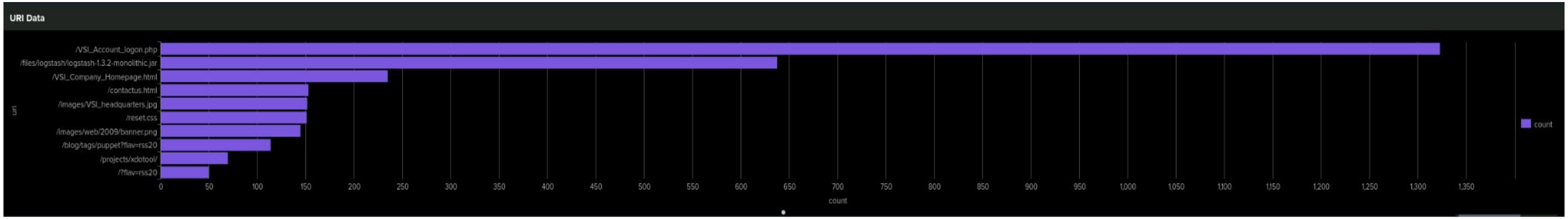
- Our Cluster Map revealed suspicious activity from a couple cities.
  - Kiev (439), Kharkiv (433), D.C. (714), and NYC(549)

- Our URI Data flagged *VSI_Account_logon.php* as having suspiciously high volume.

Screenshots of Attack Logs







Summary and Future Mitigations

Project 3 Summary

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

  The attackers in the Windows logs were attempting to perform mass Password Reset Attacks and logging into multiple accounts to reset their passwords.

  The attackers in the Apache logs were from Ukraine and were attempting to log into accounts using Brute Force attacks.

Project 3 Summary

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

- Multi-factor authentication - MFA mitigates security risks by requiring a second login. This ensures that even if one login is compromised, the unauthorized user may not have access to the second login, especially if they are on a new device.
- Block all HTTP traffic from suspicious countries - This mitigates attackers from other countries VSI may not have business to access their accounts, although with the use of VPNs this may not mitigate it completely.
- Account Lockouts - This mitigates Brute Force attacks by locking out the user completely until they get help, it prevents attackers from entering passwords multiple times in a short duration.