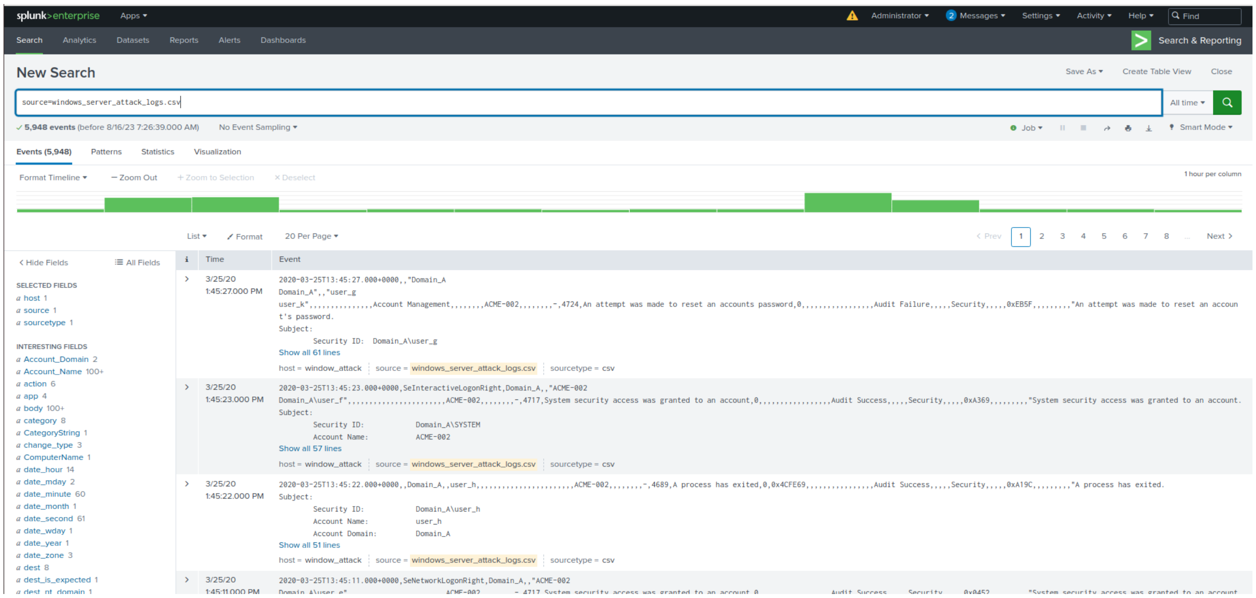
Project 3 Day 2

Part 1: Load Windows Attack Logs

In this first part, you will upload Windows attack logs into your Splunk environment. To do so, complete the following steps:

1. Select the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option.
    - Click “Select File.”
    - Select the `windows_server_attack_logs.csv` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
    - Click the green “Next” button on the top right.
3. You will be brought to the “Set Source Type” page.
    - You don't need to change any configurations on this page.
    - Select “Next” again.
4. You'll be brought to the “Input Settings” page.
    - This page contains optional settings for how the data is input.
    - In the “Host” field value, Splunk uses a random value to name the machine or device that generated the logs.
    - Update the value to “Windows_server_logs” and then select “Review”.
5. On the “Review” page, verify that you've chosen the correct settings.
    - Select “Submit” to proceed with uploading your data into Splunk.
6. Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear.
7. Select “Start Searching.”



```
source=windows_server_attack_logs.csv
```

✓ 5,948 events (before 8/16/23 7:26:39.000 AM) No Event Sampling

SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- Account_Domain 2
- Account_Name 100+
- action 6
- app 4
- body 100+
- category 8
- CategoryString 1
- change_type 3
- ComputerName 1
- date_hour 14
- date_mday 2
- date_minute 60
- date_month 1
- date_second 61
- date_wday 1
- date_year 1
- date_zone 3
- dest 8
- dest_is_expected 1
- dest_nt_domain 1

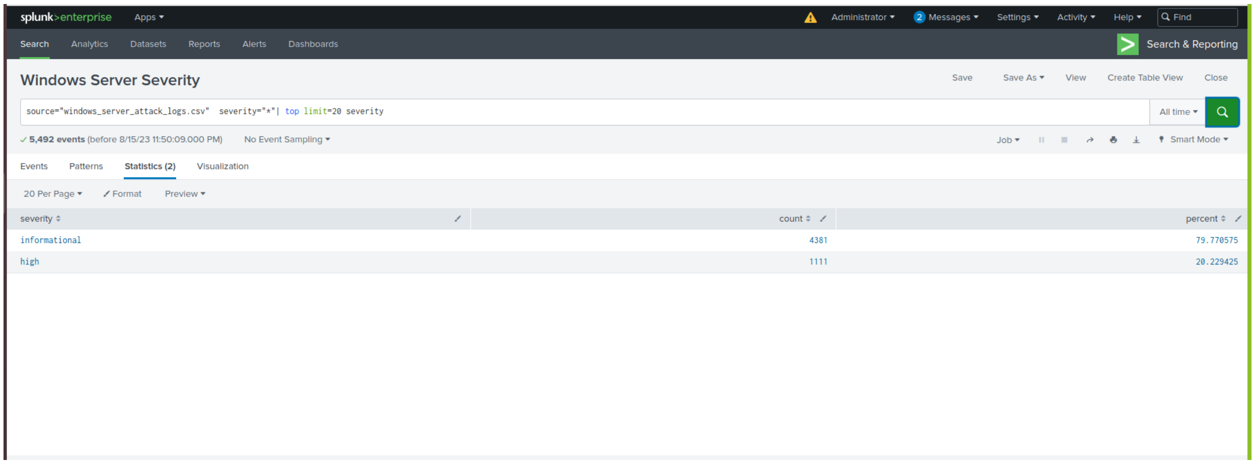
Time	Event
3/25/20 1:45:27.000 PM	2020-03-25T13:45:27.000+0000,,"Domain_A Domain_A",,"user_g user_k",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0xEB5F,,,,,,,,,"An attempt was made to reset an accoun t's password. Subject: Security ID: Domain_A\user_g Show all 61 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
3/25/20 1:45:23.000 PM	2020-03-25T13:45:23.000+0000,SeInteractiveLogonRight,Domain_A,,"ACME-002 Domain_A\user_f",,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4717,System security access was granted to an account,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"System security access was granted to an account. Subject: Security ID: Domain_A\SYSTEM Account Name: ACME-002 Show all 57 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
3/25/20 1:45:22.000 PM	2020-03-25T13:45:22.000+0000,,Domain_A,,user_h,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4689,A process has exited,0,0x4CFE69,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA19C,,,,,,,,,"A process has exited. Subject: Security ID: Domain_A\user_h Account Name: user_h Account Domain: Domain_A Show all 51 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
3/25/20 1:45:11.000 PM	2020-03-25T13:45:11.000+0000,SeNetworkLogonRight,Domain_A,,"ACME-002

Part 2: Analyze Windows Attack Logs

In this part, you will review the reports, alerts, and dashboards that you created in Day 1 and analyze the results. To do so, complete the following steps:

Report Analysis for Severity

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that you created to analyze the different severities.
3. Select “Open in Search.”
4. Take note of the percentages of different severities.
5. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
6. Select “Save.”
7. Review the updated results, and answer the following question in the Project 3 Review Questions document:
    - Did you detect any suspicious changes in severity?

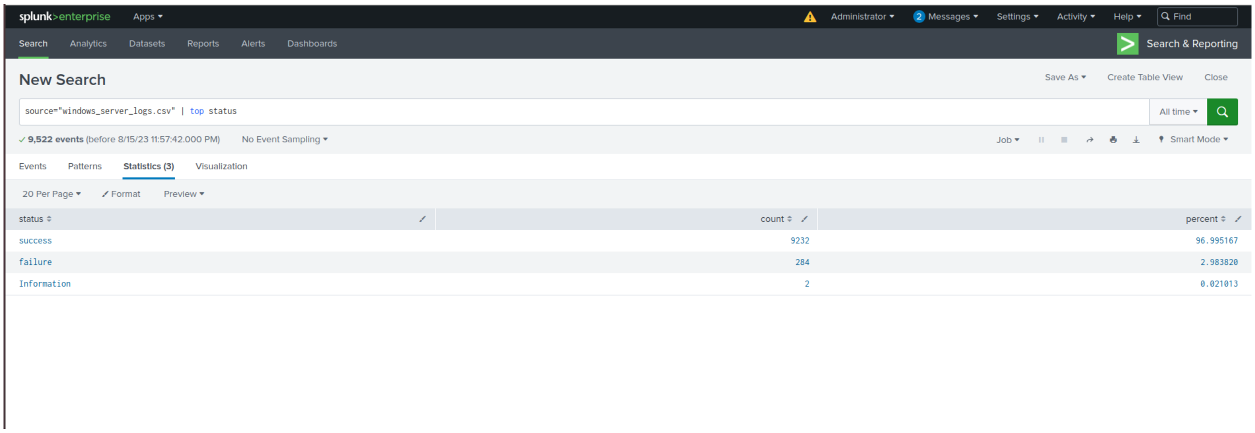


Windows Server Severity

```
source="windows_server_attack_logs.csv"  severity="*"| top limit=20 severity
```

✓ 5,492 events (before 8/15/23 11:50:09.000 PM) No Event Sampling ▾

severity	count	percent
informational	4381	79.770575
high	1111	20.229425

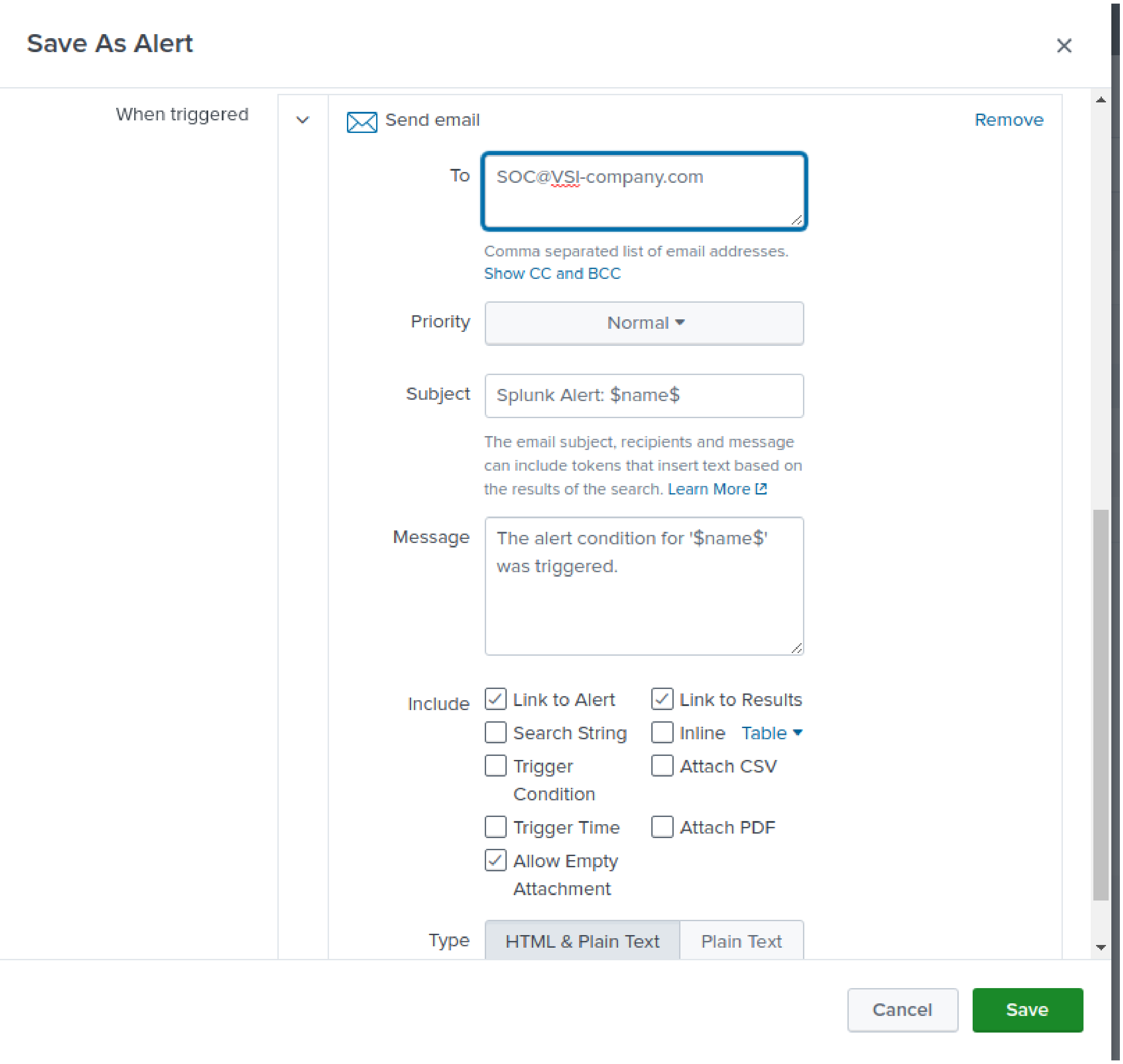


New Search

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

✓ **9,522 events** (before 8/15/23 11:57:42.000 PM) No Event Sampling

status	count	percent
success	9232	96.995167
failure	284	2.983820
Information	2	0.021013



Save As Alert

When triggered

Send email

To: SOC@VSI-company.com

Comma separated list of email addresses.
Show CC and BCC

Priority: Normal

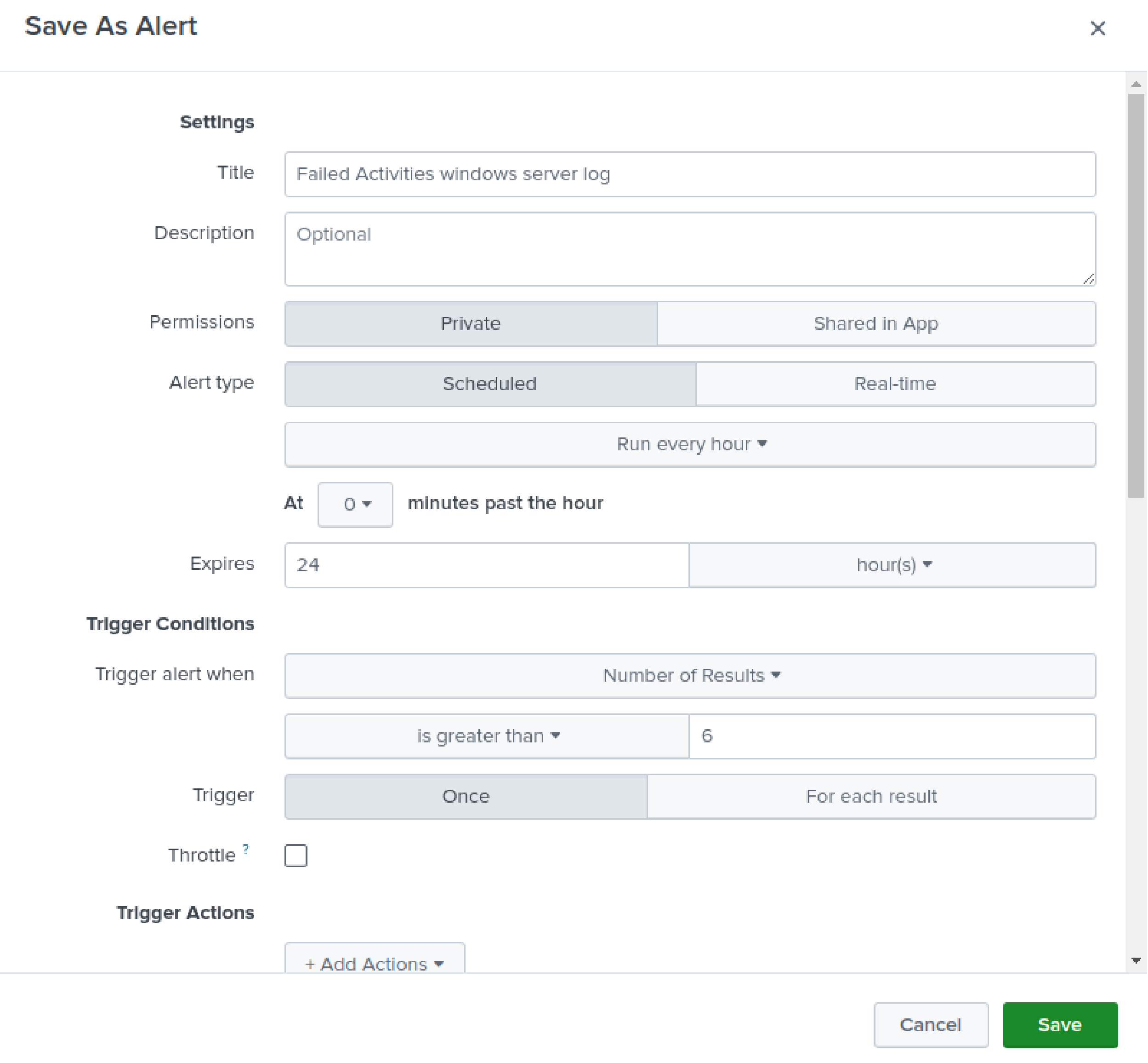
Subject: Splunk Alert: $name$

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Message: The alert condition for '$name$' was triggered.

Include:
☑ Link to Alert ☑ Link to Results
□ Search String □ Inline Table
□ Trigger Condition □ Attach CSV
□ Trigger Time □ Attach PDF
☑ Allow Empty Attachment

Type: HTML & Plain Text | Plain Text



Save As Alert

Settings

Title: Failed Activities windows server log

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

At 0 minutes past the hour

Expires: 24 hour(s)

Trigger Conditions

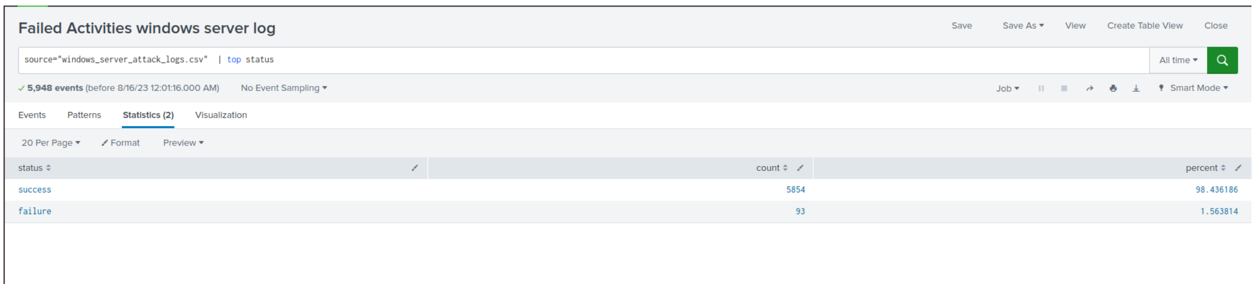
Trigger alert when: Number of Results

is greater than 6

Trigger: Once | For each result

Throttle ? □

Trigger Actions

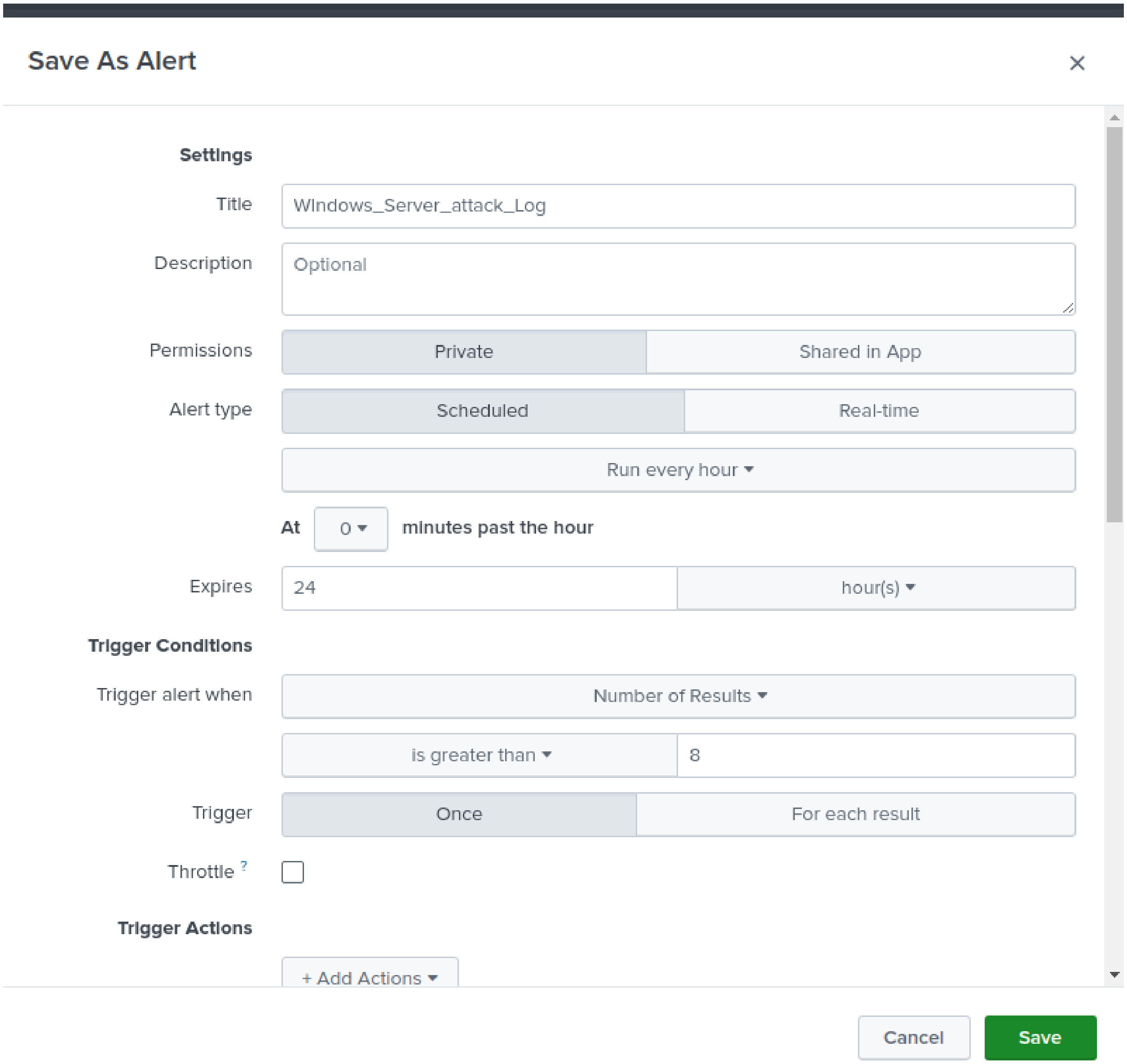


Failed Activities windows server log

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

✓ **5,948 events** (before 8/16/23 12:01:16.000 AM)   No Event Sampling

status	count	percent
success	5854	98.436186
failure	93	1.563814



Save As Alert

Settings

Title: Windows_Server_attack_Log

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour ▾

At 0 ▾ minutes past the hour

Expires: 24 hour(s) ▾

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ 8

Trigger: Once | For each result

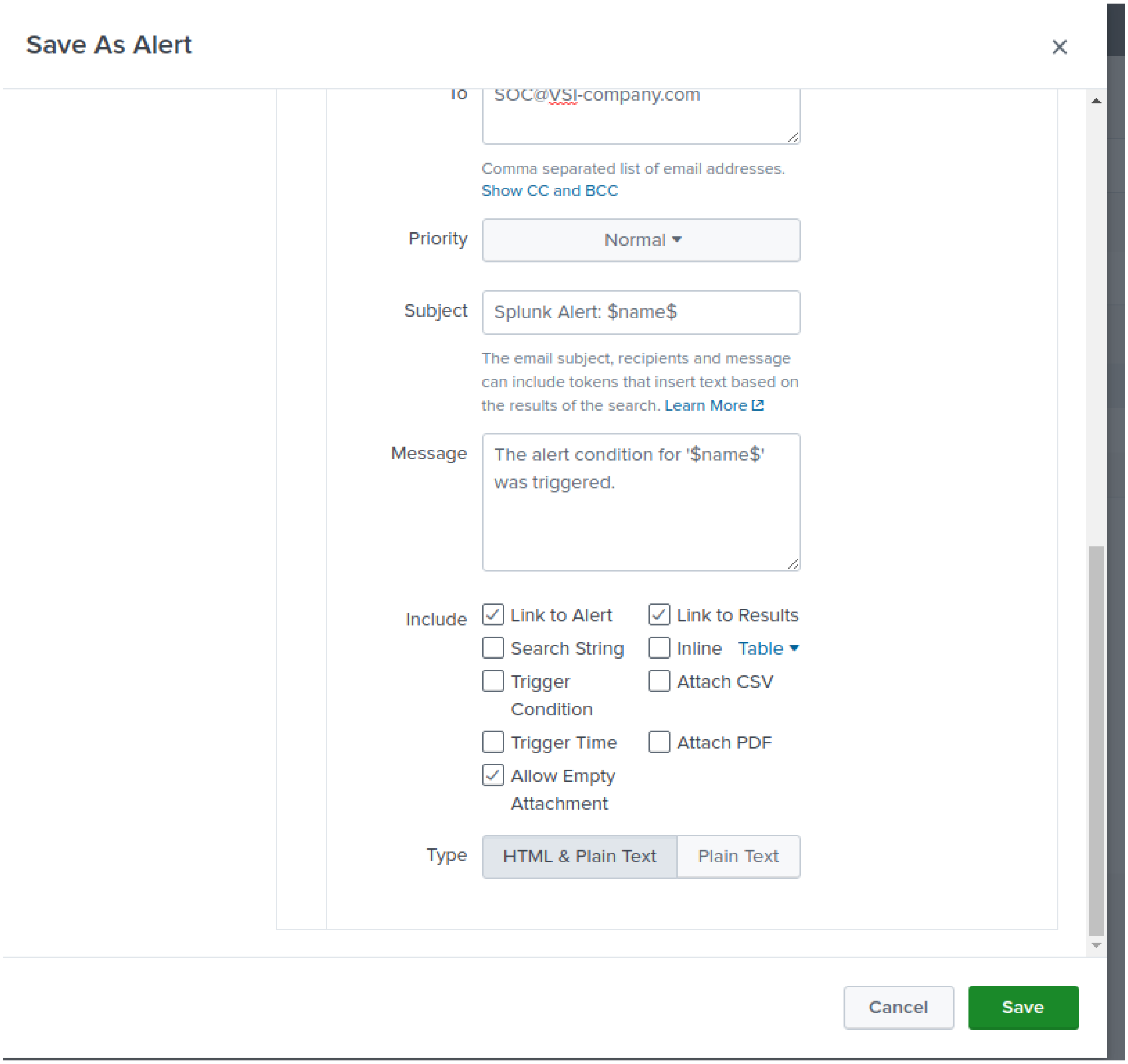
Throttle ? □

Trigger Actions

+ Add Actions ▾

Cancel

Save



Save As Alert

To SOC@VSI-company.com

Comma separated list of email addresses.
Show CC and BCC

Priority: Normal

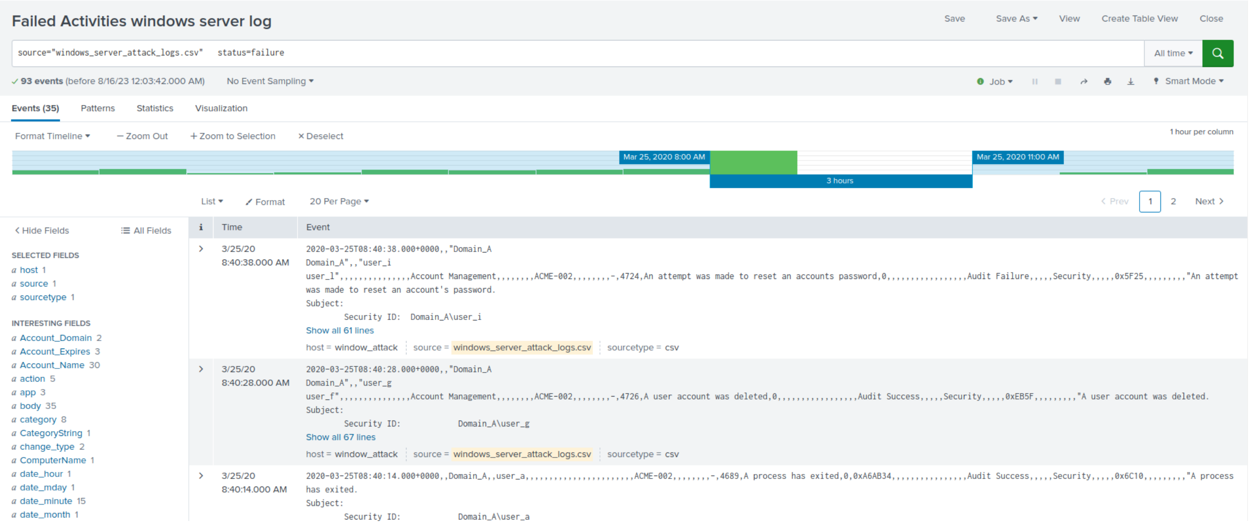
Subject: Splunk Alert: $name$

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Message: The alert condition for '$name$' was triggered.

Include:
☑ Link to Alert
☑ Link to Results
□ Search String
□ Inline Table
□ Trigger Condition
□ Attach CSV
□ Trigger Time
□ Attach PDF
☑ Allow Empty Attachment

Type: [✓ HTML & Plain Text] Plain Text



Failed Activities windows server log

```
source="windows_server_attack_logs.csv"   status=failure
```

✓ 93 events (before 8/16/23 12:03:42.000 AM)   No Event Sampling

All time · Smart Mode

Events (35)   Patterns   Statistics   Visualization

1 hour per column

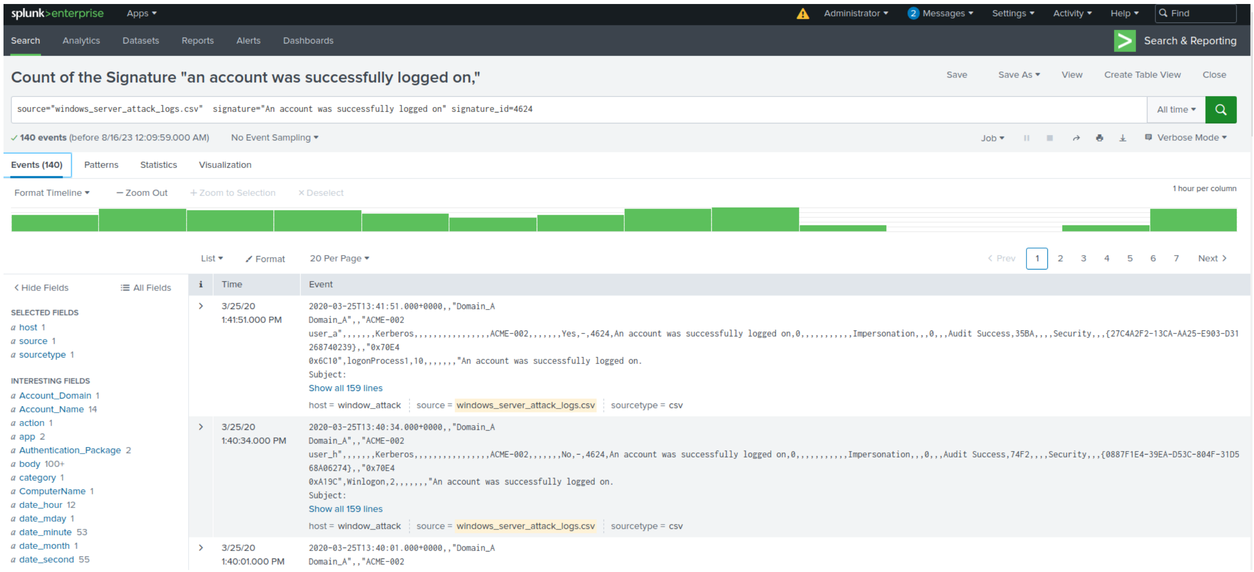
Mar 25, 2020 8:00 AM — 3 hours — Mar 25, 2020 11:00 AM

List · Format · 20 Per Page

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2
a Account_Expires 3
a Account_Name 30
a action 5
a app 3
a body 35
a category 8
a CategoryString 1
a change_type 2
a ComputerName 1
a date_hour 1
a date_mday 1
a date_minute 15
a date_month 1

i	Time	Event
>	3/25/20 8:40:38.000 AM	2020-03-25T08:40:38.000+0000,,"Domain_A Domain_A",,"user_i user_l",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x5F25,,,,,,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_i Show all 61 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
>	3/25/20 8:40:28.000 AM	2020-03-25T08:40:28.000+0000,,"Domain_A Domain_A",,"user_g user_f",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,Audit Success,,,,Security,,,,0xEB5F,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_g Show all 67 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
>	3/25/20 8:40:14.000 AM	2020-03-25T08:40:14.000+0000,,Domain_A,,user_a,,,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4689,A process has exited,0,0xA6AB34,,,,,,,,,,,,,,,Audit Success,,,,Security,,,,0x6C10,,,,,,,,"A process has exited. Subject: Security ID: Domain_A\user_a



Count of the Signature "an account was successfully logged on,"

```
source="windows_server_attack_logs.csv"  signature="An account was successfully logged on" signature_id=4624
```

✓ 140 events (before 8/16/23 12:09:59.000 AM)   No Event Sampling

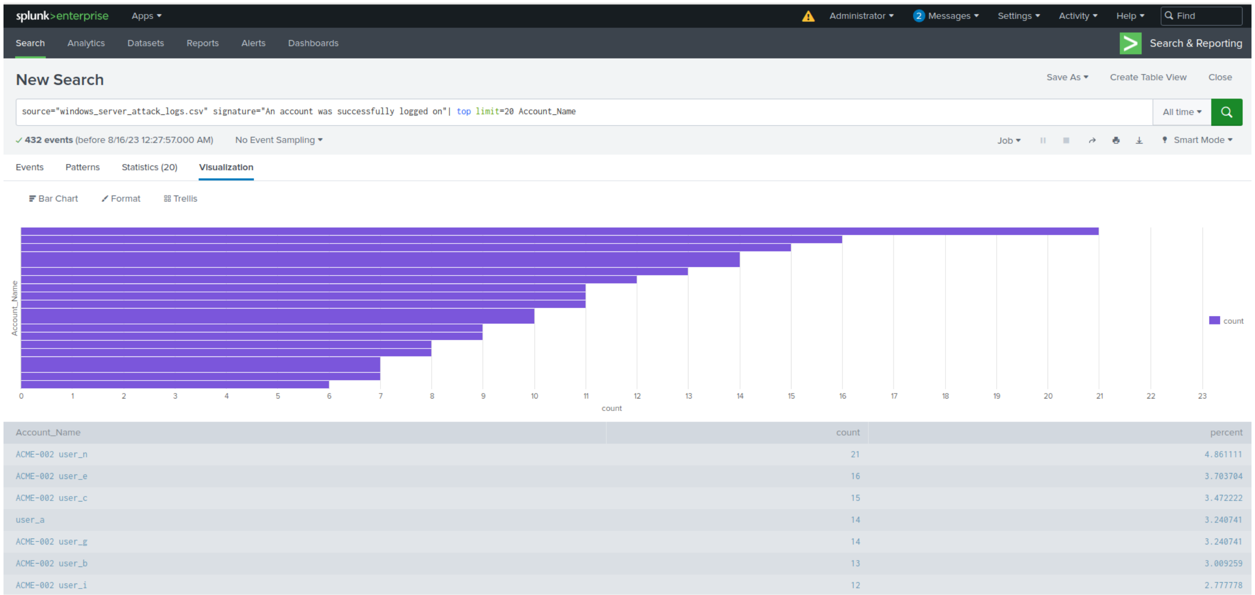
SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Account_Domain 1
- a Account_Name 14
- a action 1
- a app 2
- a Authentication_Package 2
- a body 100+
- a category 1
- a ComputerName 1
- a date_hour 12
- a date_mday 1
- a date_minute 53
- a date_month 1
- a date_second 55

i	Time	Event
›	3/25/20 1:41:51.000 PM	2020-03-25T13:41:51.000+0000,,"Domain_A 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-D31 268740239},,"0x70E4 0x6C10",logonProcess1,10,,,,,,,"An account was successfully logged on. Subject: Show all 159 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
›	3/25/20 1:40:34.000 PM	2020-03-25T13:40:34.000+0000,,"Domain_A 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-31D5 68A06274},,"0x70E4 0xA19C",Winlogon,2,,,,,,,"An account was successfully logged on. Subject: Show all 159 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
›	3/25/20 1:40:01.000 PM	2020-03-25T13:40:01.000+0000,,"Domain_A Domain_A",,"ACME-002

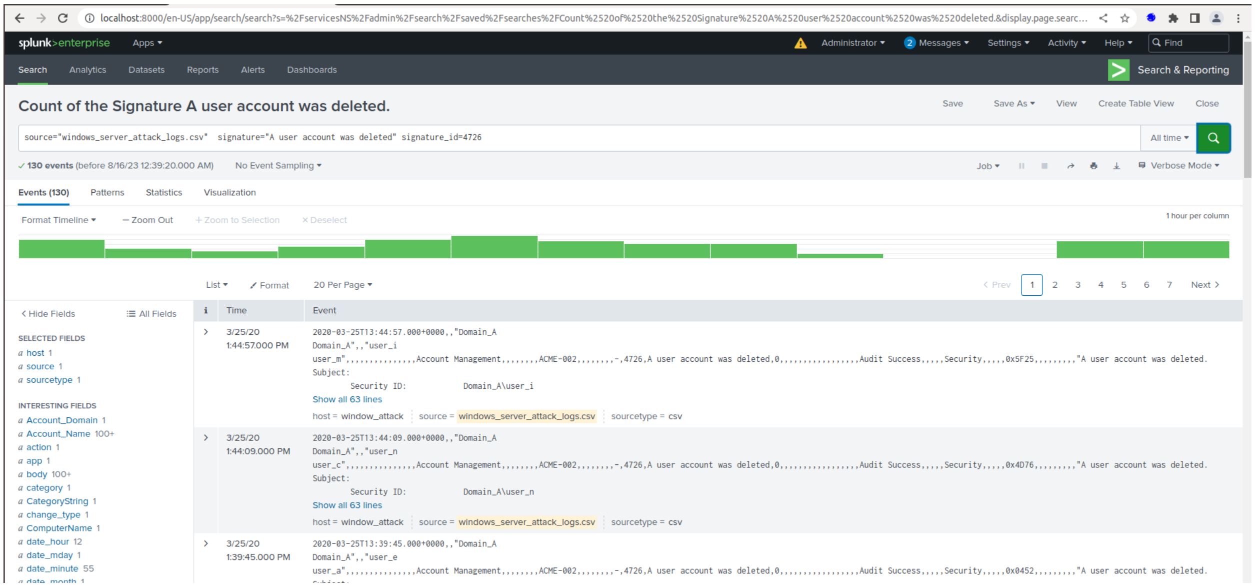


New Search

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on"| top limit=20 Account_Name
```

✓ 432 events (before 8/16/23 12:27:57.000 AM)   No Event Sampling

Account_Name	count	percent
ACME-002 user_n	21	4.861111
ACME-002 user_e	16	3.703704
ACME-002 user_c	15	3.472222
user_a	14	3.240741
ACME-002 user_g	14	3.240741
ACME-002 user_b	13	3.009259
ACME-002 user_i	12	2.777778



Count of the Signature A user account was deleted.

```
source="windows_server_attack_logs.csv"  signature="A user account was deleted" signature_id=4726
```

✓ 130 events (before 8/16/23 12:39:20.000 AM)   No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

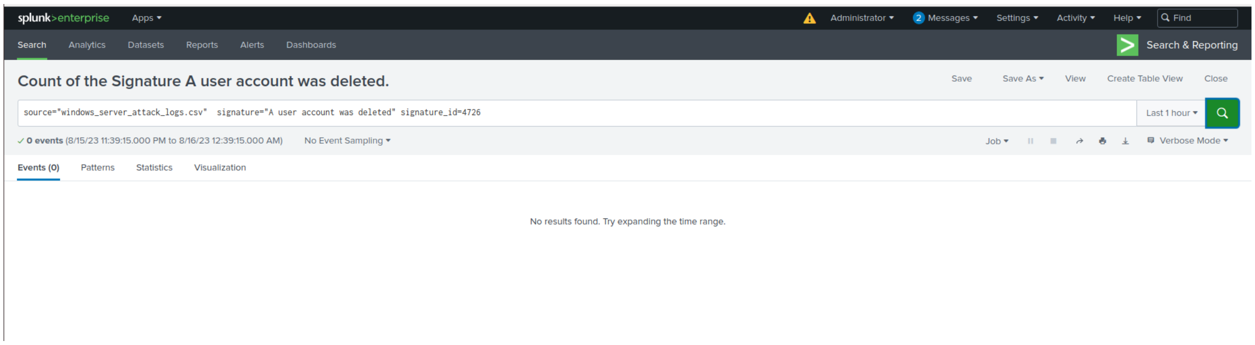
INTERESTING FIELDS
- a Account_Domain 1
- a Account_Name 100+
- a action 1
- a app 1
- a body 100+
- a category 1
- a CategoryString 1
- a change_type 1
- a ComputerName 1
- a date_hour 12
- a date_mday 1
- a date_minute 55
- a date_month 1

i	Time	Event

›	3/25/20
	1:44:57.000 PM
		`2020-03-25T13:44:57.000+0000,,"Domain_A`
		`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`
		Show all 63 lines
		host = window_attack source = windows_server_attack_logs.csv sourcetype = csv

›	3/25/20
	1:44:09.000 PM
		`2020-03-25T13:44:09.000+0000,,"Domain_A`
		`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`
		Show all 63 lines
		host = window_attack source = windows_server_attack_logs.csv sourcetype = csv

›	3/25/20
	1:39:45.000 PM
		`2020-03-25T13:39:45.000+0000,,"Domain_A`
		`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.`

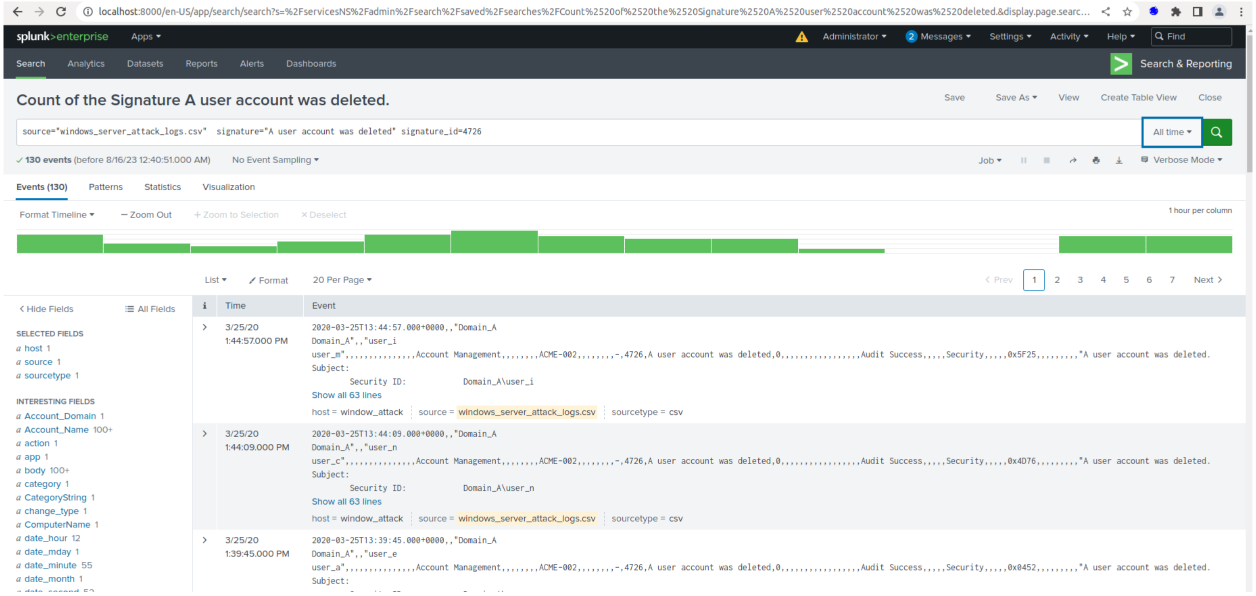


Count of the Signature A user account was deleted.

```
source="windows_server_attack_logs.csv"  signature="A user account was deleted" signature_id=4726
```

✓ 0 events (8/15/23 11:39:15.000 PM to 8/16/23 12:39:15.000 AM)   No Event Sampling ▾

No results found. Try expanding the time range.



Count of the Signature A user account was deleted.

```
source="windows_server_attack_logs.csv"  signature="A user account was deleted" signature_id=4726
```

✓ 130 events (before 8/16/23 12:40:51.000 AM)   No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a Account_Domain 1
- a Account_Name 100+
- a action 1
- a app 1
- a body 100+
- a category 1
- a CategoryString 1
- a change_type 1
- a ComputerName 1
- a date_hour 12
- a date_mday 1
- a date_minute 55
- a date_month 1

i	Time	Event

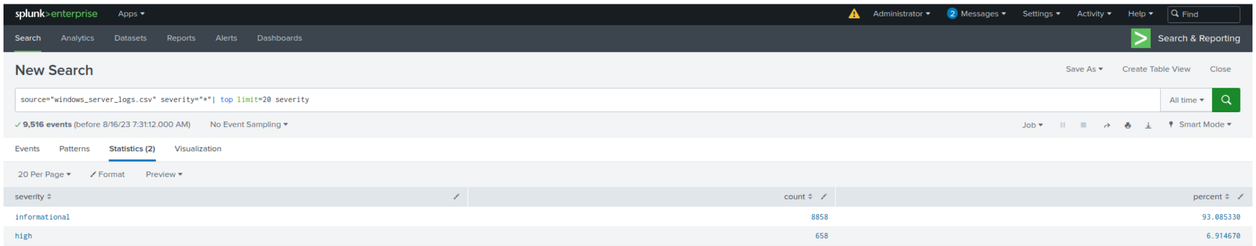
›	3/25/20
	1:44:57.000 PM
		`2020-03-25T13:44:57.000+0000,,"Domain_A`
		`Domain_A",,"user_i`
		`user_m",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x5F25,,,,,,,,,"A user account was deleted.`
		`Subject:`
		`        Security ID:            Domain_A\user_i`
		Show all 63 lines
		host = window_attack source = windows_server_attack_logs.csv sourcetype = csv

›	3/25/20
	1:44:09.000 PM
		`2020-03-25T13:44:09.000+0000,,"Domain_A`
		`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`
		Show all 63 lines
		host = window_attack source = windows_server_attack_logs.csv sourcetype = csv

›	3/25/20
	1:39:45.000 PM
		`2020-03-25T13:39:45.000+0000,,"Domain_A`
		`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:`

New

1. percentages of different severities.

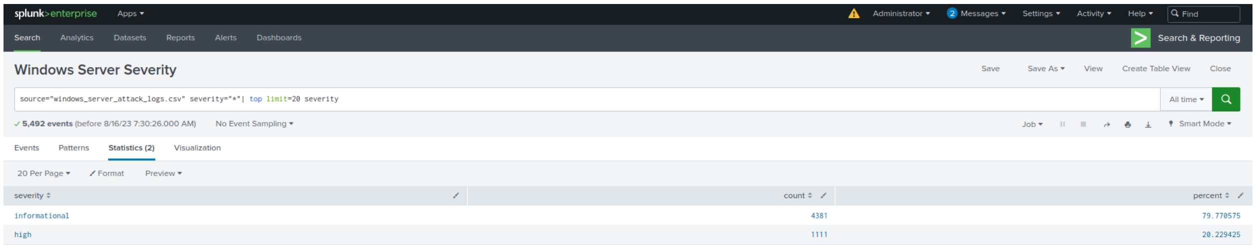


New Search

```
source="windows_server_logs.csv" severity="*"| top limit=20 severity
```

✓ 9,516 events (before 8/16/23 7:31:12.000 AM) No Event Sampling

severity	count	percent
informational	8858	93.085330
high	658	6.914670



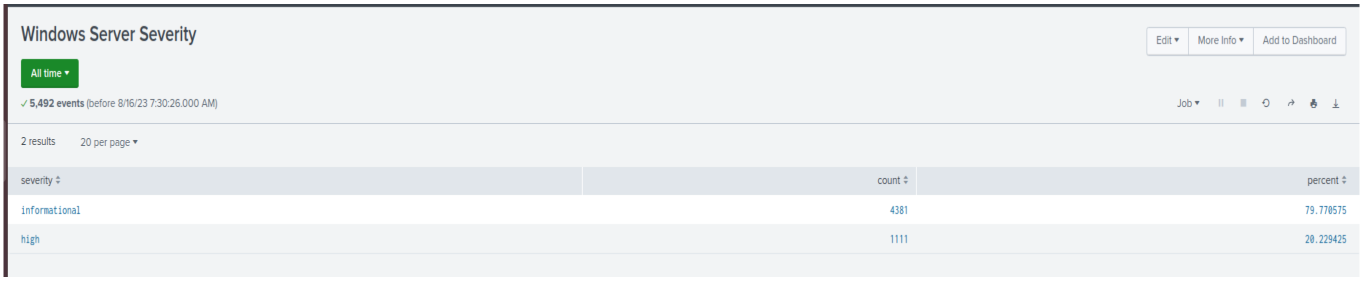
Windows Server Severity

```
source="windows_server_attack_logs.csv" severity="*"| top limit=20 severity
```

✓ 5,492 events (before 8/16/23 7:30:26.000 AM) No Event Sampling

severity	count	percent
informational	4381	79.770575
high	1111	20.229425

Saved New changes with `source="windows_server_attack_logs.csv"`.



Windows Server Severity

✓ 5,492 events (before 8/16/23 7:30:26.000 AM)

2 results 20 per page

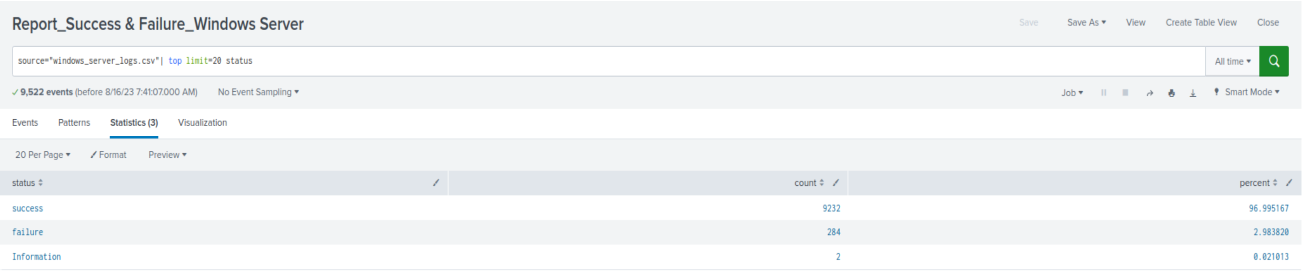
severity	count	percent
informational	4381	79.770575
high	1111	20.229425

Report Analysis for Failed Activities

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that you created to analyze the different activities.
3. Select “Open in Search.”
4. Take note of the failed activities percentage.

5. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
6. Select “Save.”
7. Review the updated results, and answer the following question in the review document:
    - ○ Did you detect any suspicious changes in failed activities?

Now, you will review the alerts that you created on Day 1 and analyze the results.



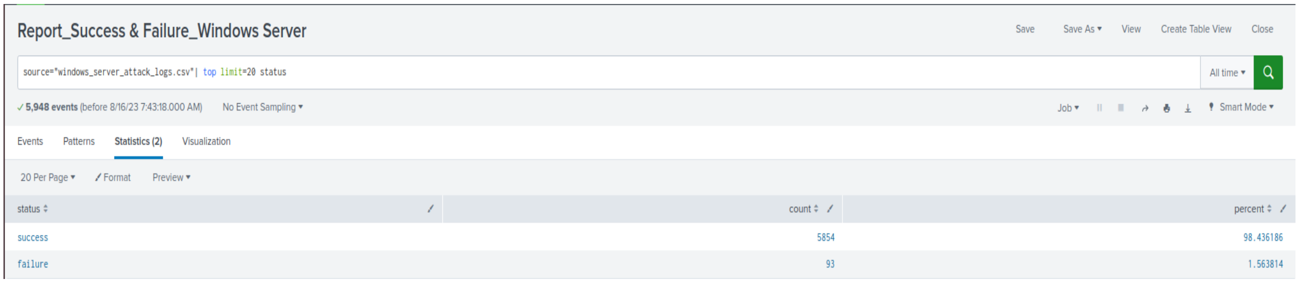
Report_Success & Failure_Windows Server

```
source="windows_server_logs.csv"| top limit=20 status
```

✓ **9,522 events** (before 8/16/23 7:41:07.000 AM) No Event Sampling ▾

Events Patterns **Statistics (3)** Visualization

status	count	percent
success	9232	96.995167
failure	284	2.983820
Information	2	0.021013



Report_Success & Failure_Windows Server

```
source="windows_server_attack_logs.csv"| top limit=20 status
```

✓ **5,948 events** (before 8/16/23 7:43:18.000 AM) No Event Sampling ▾

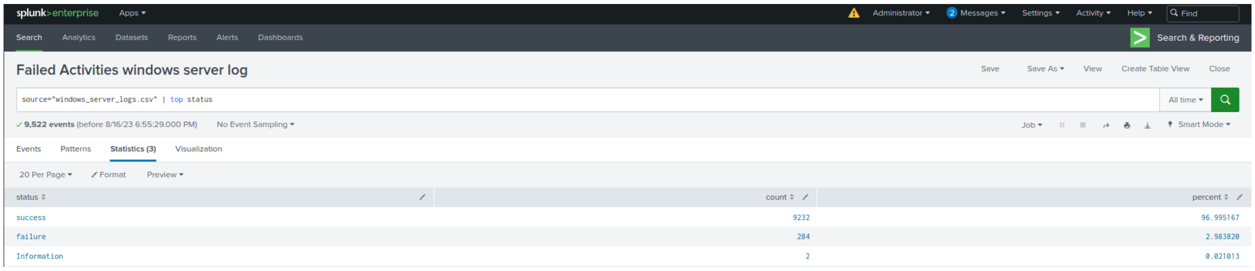
Events Patterns **Statistics (2)** Visualization

status	count	percent
success	5854	98.436186
failure	93	1.563814

Alert Analysis for Failed Windows Activity

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of failed activities.
3. Select “Open in Search.”
4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
5. Review the updated results, and answer the following questions in the review document (*note that your alerts will not trigger; this is a theoretical exercise*):
    - ○ Did you detect a suspicious volume of failed activity?

- If so, what was the count of events in the hour(s) it occurred?
- When did it occur?
- Would your alert be triggered for this activity?
- After reviewing, would you change your threshold from what you previously selected?

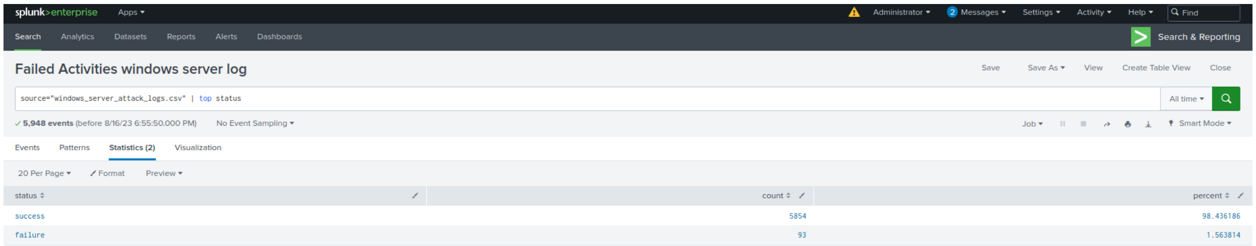


Failed Activities windows server log

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

✓ 9,522 events (before 8/16/23 6:55:29.000 PM) No Event Sampling

status	count	percent
success	9232	96.995167
failure	284	2.983820
Information	2	0.021013

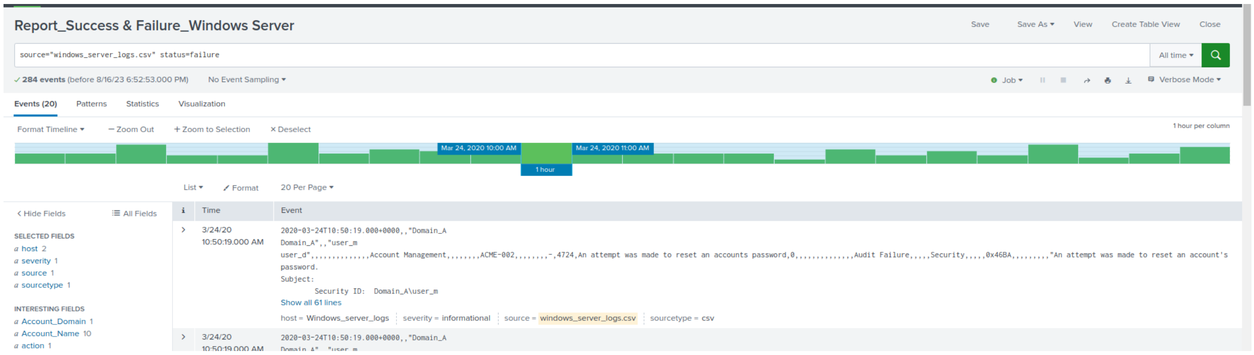


Failed Activities windows server log

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

✓ 5,948 events (before 8/16/23 6:55:50.000 PM) No Event Sampling

status	count	percent
success	5854	98.436186
failure	93	1.563814



Report_Success & Failure_Windows Server

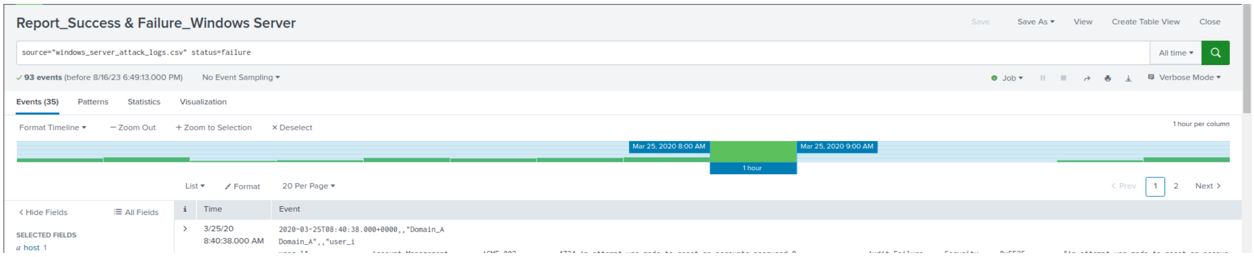
```
source="windows_server_logs.csv" status=failure
```

✓ 284 events (before 8/16/23 6:52:53.000 PM) No Event Sampling

SELECTED FIELDS
a host 2
a severity 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 1
a Account_Name 10
a action 1

i	Time	Event
>	3/24/20 10:50:19.000 AM	2020-03-24T10:50:19.000+0000,,"Domain_A Domain_A",,"user_m user_d",,,,,,,,,,,,,,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 host = Windows_server_logs severity = informational source = windows_server_logs.csv sourcetype = csv
>	3/24/20 10:50:19.000 AM	2020-03-24T10:50:19.000+0000,,"Domain_A Domain_A",,"user_m



Report_Success & Failure_Windows Server

```
source="windows_server_attack_logs.csv" status=failure
```

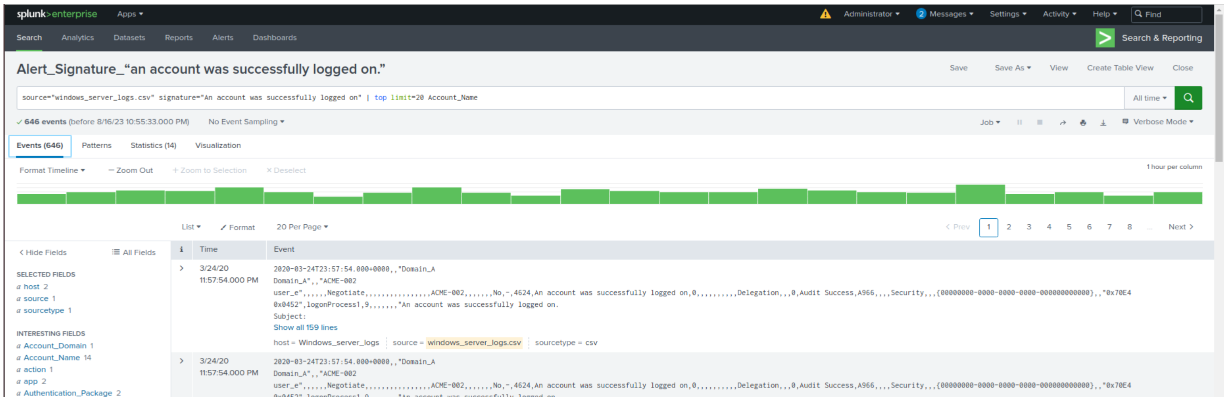
✓ 93 events (before 8/16/23 6:49:13.000 PM) No Event Sampling

SELECTED FIELDS
a host 1

i	Time	Event
>	3/25/20 8:40:38.000 AM	2020-03-25T08:40:38.000+0000,,"Domain_A Domain_A",,"user_i

Alert Analysis for Successful Logins

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of successful logins.
3. Select “Open in Search.”
4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
5. Review the updated results, and answer the following questions in the review document:
   - Did you detect a suspicious volume of successful logins?
   - If so, what was the count of events in the hour(s) it occurred?
   - Who is the primary user logging in?
   - When did it occur?
   - Would your alert be triggered for this activity?
   - After reviewing, would you change your threshold from what you previously selected?



Alert_Signature_“an account was successfully logged on.”

```
source="windows_server_logs.csv" signature="An account was successfully logged on" | top limit=20 Account_Name
```

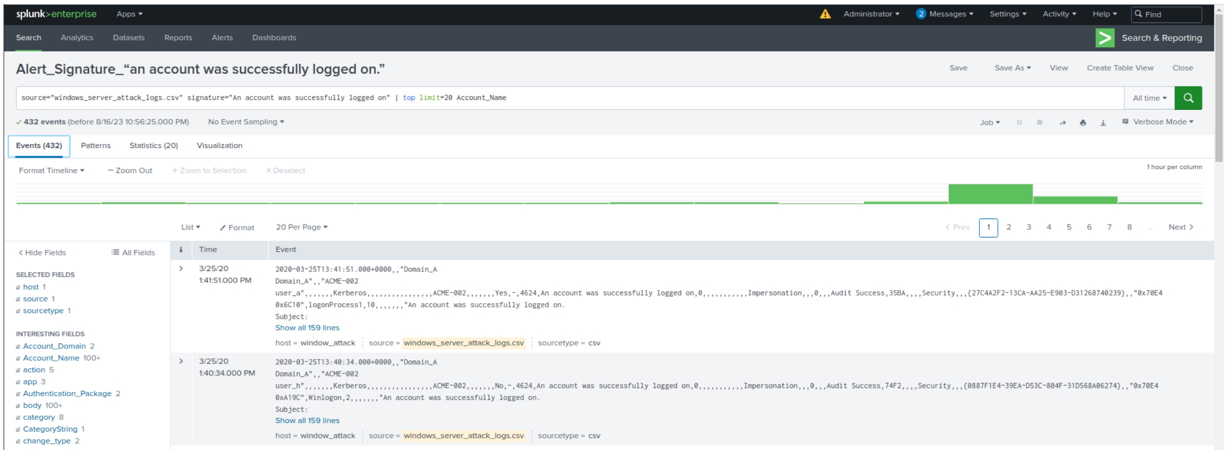
✓ 646 events (before 8/16/23 10:55:33.000 PM)   No Event Sampling

Events (646)   Patterns   Statistics (14)   Visualization

SELECTED FIELDS
- a host 2
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a Account_Domain 1
- a Account_Name 14
- a action 1
- a app 2
- a Authentication_Package 2

i	Time	Event
>	3/24/20 11:57:54.000 PM	2020-03-24T23:57:54.000+0000,,"Domain_A 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 host = Windows_server_logs source = windows_server_logs.csv sourcetype = csv
>	3/24/20 11:57:54.000 PM	2020-03-24T23:57:54.000+0000,,"Domain_A 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



Alert_Signature_"an account was successfully logged on."

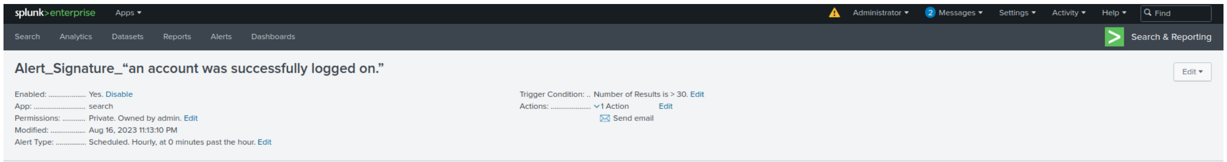
```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on" | top limit=20 Account_Name
```

✓ 432 events (before 8/16/23 10:56:25.000 PM) No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2
a Account_Name 100+
a action 5
a app 3
a Authentication_Package 2
a body 100+
a category 8
a CategoryString 1
a change_type 2

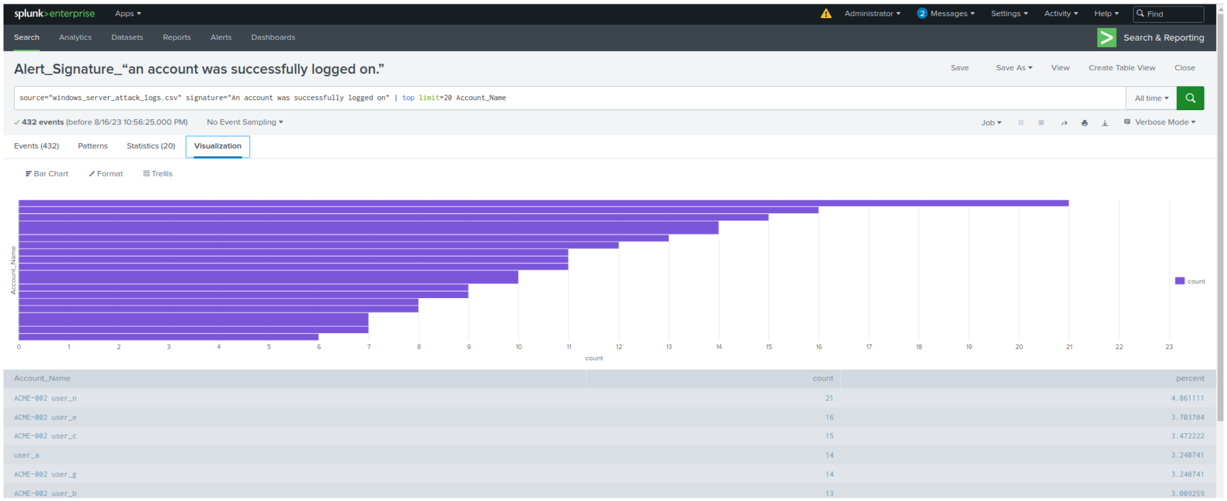
i	Time	Event
>	3/25/20 1:41:51.000 PM	2020-03-25T13:41:51.000+0000,,"Domain_A Domain_A",,"ACME-002 user_a",,,,,,,Kerberos,,,,,,,,,,,,,,,ACME-002,,,,,,Yes,-,4624,An account was successfully logged on,0,,,,,,,,,,Impersonation,,,0,,,Audit Success,35BA,,,,Security,,,{27C4A2F2-13CA-AA25-E903-D31268740239},,"0x70E4 0x6C10",logonProcess1,10,,,,,,"An account was successfully logged on. Subject: Show all 159 lines host = window_attack source = windows_server_attack_logs.csv sourcetype = csv
>	3/25/20 1:40:34.000 PM	2020-03-25T13:40:34.000+0000,,"Domain_A 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 host = window_attack source = windows_server_attack_logs.csv sourcetype = csv



Alert_Signature_"an account was successfully logged on."

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 16, 2023 11:13:10 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

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



Alert_Signature_"an account was successfully logged on."

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on" | top limit=20 Account_Name
```

✓ 432 events (before 8/16/23 10:56:25.000 PM) No Event Sampling

Account_Name	count	percent
ACME-002 user_n	21	4.861111
ACME-002 user_e	16	3.703704
ACME-002 user_c	15	3.472222
user_a	14	3.240741
ACME-002 user_g	14	3.240741
ACME-002 user_b	13	3.009259

Alert Analysis for Deleted Accounts

1. Access the "Alerts" tab, and select "Yours" to view the alerts that you created on Day 1.

2. Select the alert for suspicious volume of deleted accounts.

3. Select "Open in Search."

4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.

5. Review the updated results, and answer the following question in the review document:
    - Did you detect a suspicious volume of deleted accounts?

Next, you will view your dashboard and analyze the results.

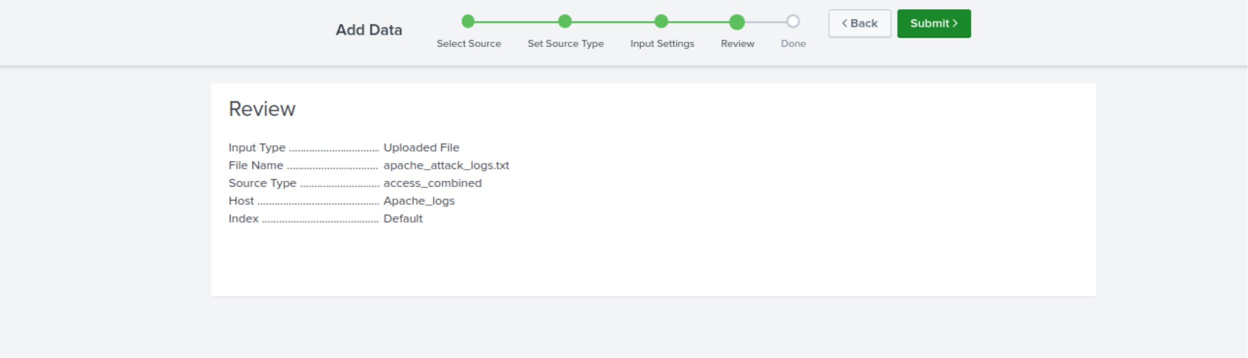
Part 3: Load Apache Attack Logs

In this part, you will upload Apache attack logs into your Splunk environment. To do so, complete the following steps:

1. Return to the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option.
    - Click “Select File.”
    - Select the `apache_attack_logs.txt` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
    - Click the green “Next” button on the top right.
3. You will be brought to the “Set Source Type” page.
    - You don’t need to change any configurations on this page.
    - Select “Next” again.
4. You'll be brought to a page called “Input Settings.”
    - This page contains optional settings for how the data is input.
    - In the “Host” field value, Splunk uses a random value to name the machine or device that generated the logs.
    - Update the value to “Apache_logs” and then select “Review.”
5. At the “Review” page, verify that you've chosen the correct settings.
    - Select “Submit” to proceed with uploading your data into Splunk.
6. Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear.

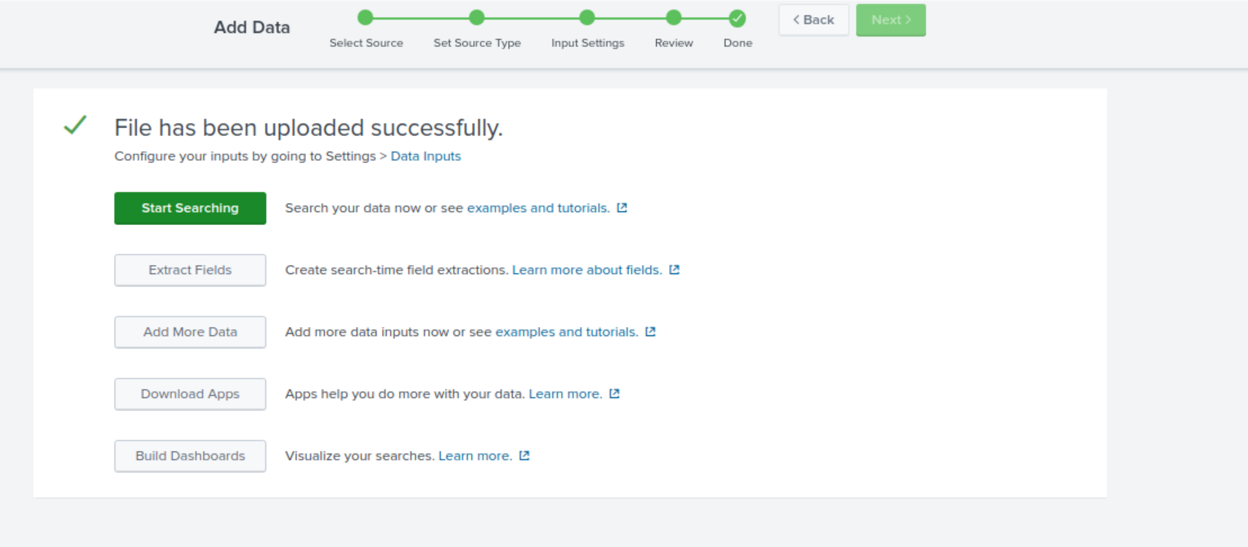
7. Select “Start Searching.”

8. ⚠️ **Important**: After the data populates on the search, select “All Time” for the time range.



Review

Input Type .... Uploaded File
File Name .... apache_attack_logs.txt
Source Type .... access_combined
Host .... Apache_logs
Index .... Default



✓ File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

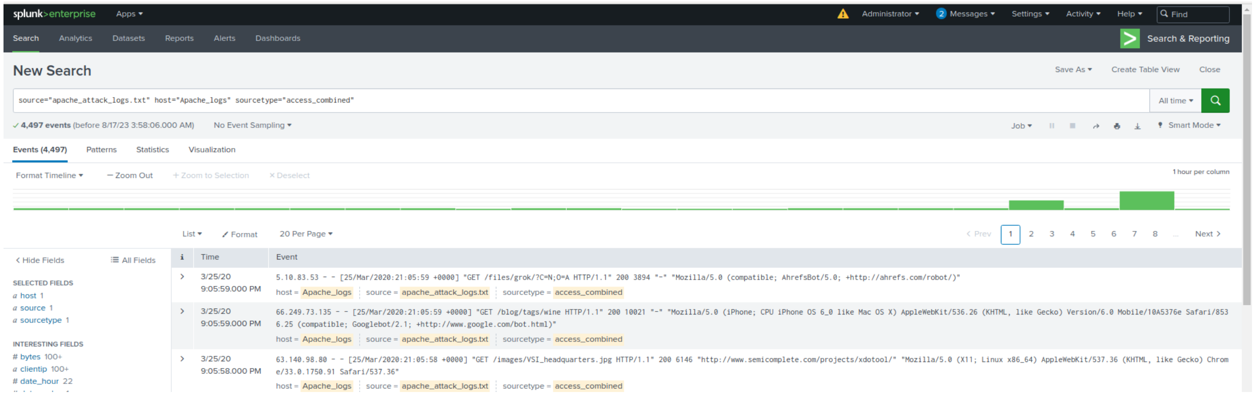
Search your data now or see examples and tutorials.

Create search-time field extractions. Learn more about fields.

Add more data inputs now or see examples and tutorials.

Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.



New Search

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined"
```

All time ▾

✓ **4,497 events** (before 8/17/23 3:58:06.000 AM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bytes 100+
a clientip 100+
# date_hour 22

i	Time	Event

›	3/25/20
	9:05:59.000 PM
		`5.10.83.53 - - [25/Mar/2020:21:05:59 +0000] "GET /files/grok/?C=N;O=A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)"`
		host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined

›	3/25/20
	9:05:59.000 PM
		`66.249.73.135 - - [25/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)"`
		host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined

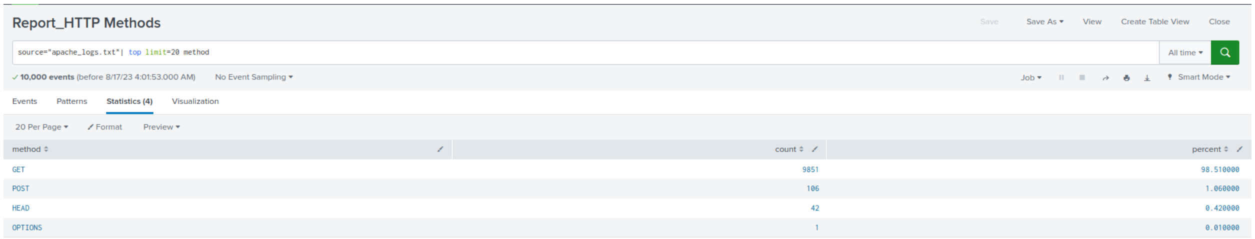
›	3/25/20
	9:05:58.000 PM
		`63.140.98.80 - - [25/Mar/2020:21:05:58 +0000] "GET /images/VSI_headquarters.jpg HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36"`
		host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined

Part 4: Analyze Apache Attack Logs

In this part, you will review the reports, alerts, and dashboards that you created on Day 1 and analyze the results. To do so, complete the following steps:

Report Analysis for Methods

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that analyzes the different HTTP methods.
3. Select “Edit” > “Open in Search.”
4. Take note of the percent and count of the various methods.
5. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt`.
6. Select “Save.”
7. Review the updated results, and answer the following questions in the review document:
    - Did you detect any suspicious changes in HTTP methods? If so, which one?
    - What is that method used for?

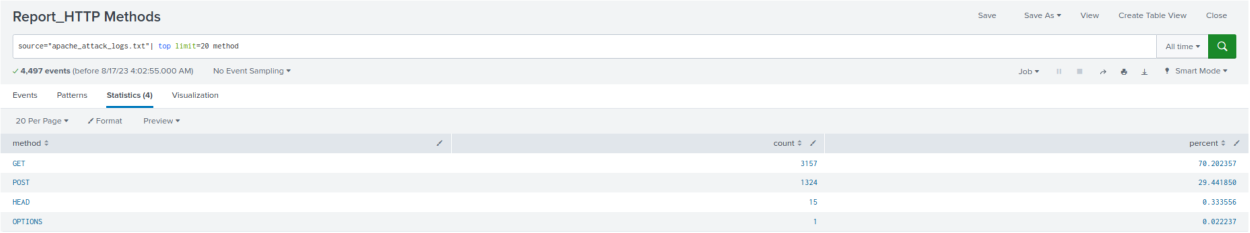


Report_HTTP Methods

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

✓ **10,000 events** (before 8/17/23 4:01:53.000 AM) No Event Sampling ▾

method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000



Report_HTTP Methods

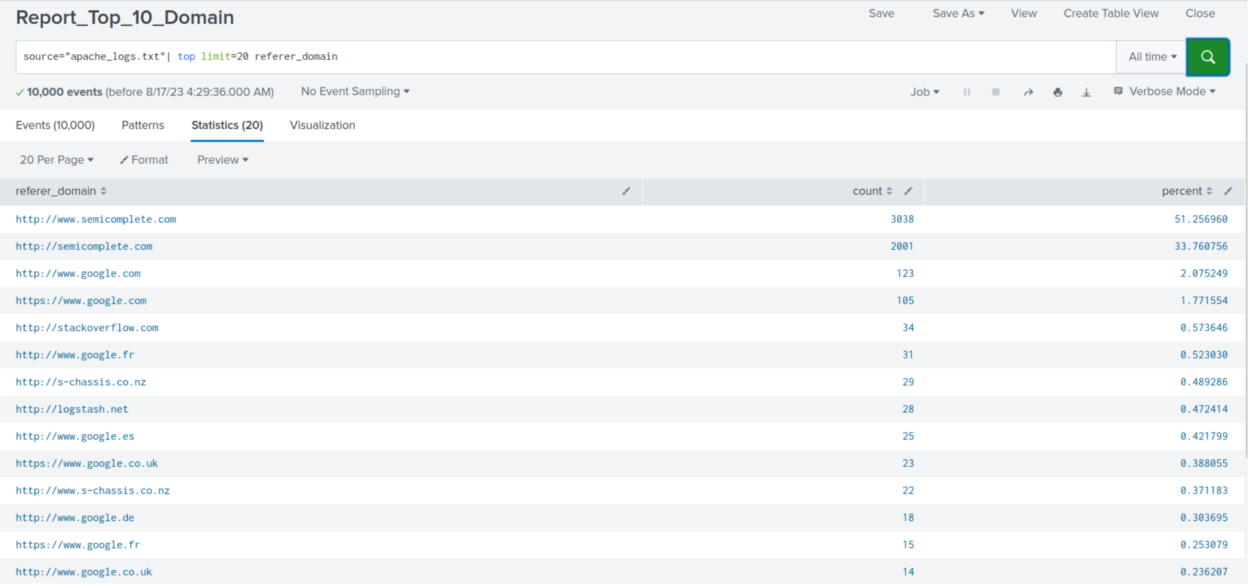
```
source="apache_attack_logs.txt"| top limit=20 method
```

✓ **4,497 events** (before 8/17/23 4:02:55.000 AM) No Event Sampling ▾

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

Report Analysis for Referrer Domains

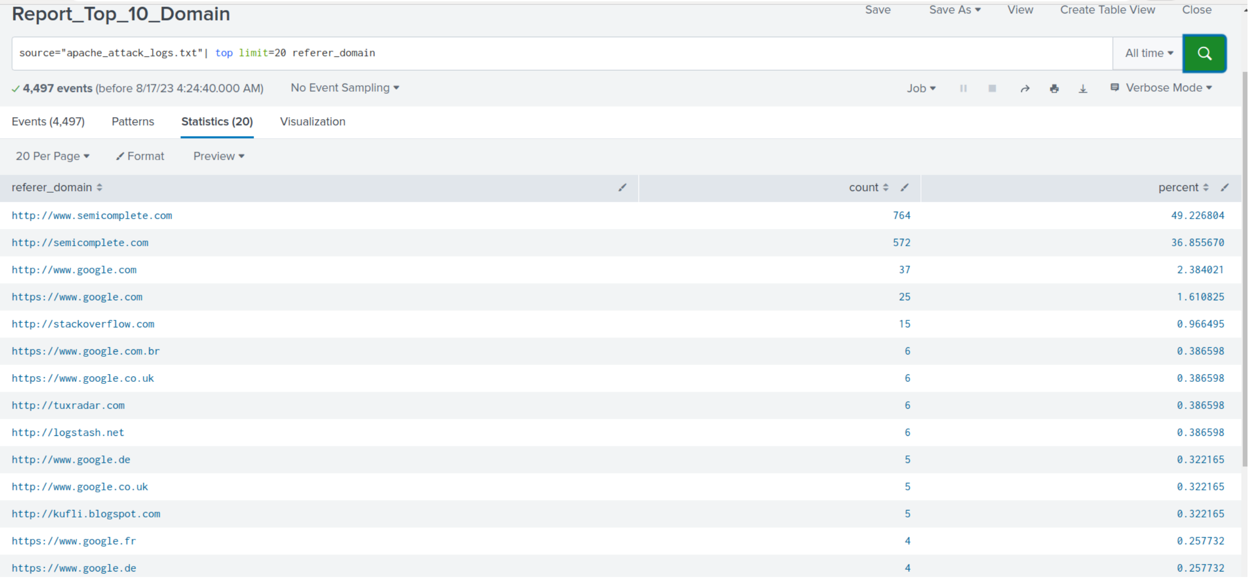
1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that analyzes the different referrer domains.
3. Select “Edit” > “Open in Search.”
4. Take note of the different referrer domains.
5. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt`.
6. Select “Save.”
7. Review the updated results, and answer the following question in the review document:
    - Did you detect any suspicious changes in referrer domains?



```
source="apache_logs.txt"| top limit=20 referer_domain
```

✓ 10,000 events (before 8/17/23 4:29:36.000 AM) No Event Sampling ▾

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055
http://www.s-chassis.co.nz	22	0.371183
http://www.google.de	18	0.303695
https://www.google.fr	15	0.253079
http://www.google.co.uk	14	0.236207



```
source="apache_attack_logs.txt"| top limit=20 referer_domain
```

✓ 4,497 events (before 8/17/23 4:24:40.000 AM) No Event Sampling ▾

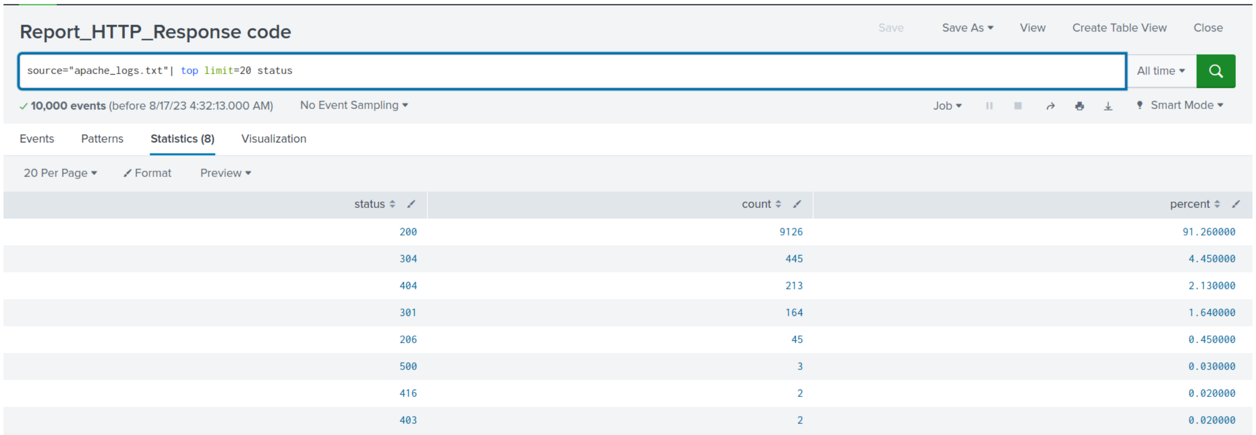
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165
http://www.google.co.uk	5	0.322165
http://kufli.blogspot.com	5	0.322165
https://www.google.fr	4	0.257732
https://www.google.de	4	0.257732

Report Analysis for HTTP Response Codes

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that analyzes the different HTTP response codes.
3. Select “Edit” > “Open in Search.”
4. Take note of the different HTTP response codes.

5. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt`.
6. Select “Save.”
7. Review the updated results and answer the following question in the review document:
   - Did you detect any suspicious changes in HTTP response codes?

Now, you will review the alerts that you created on Day 1 and analyze the results.

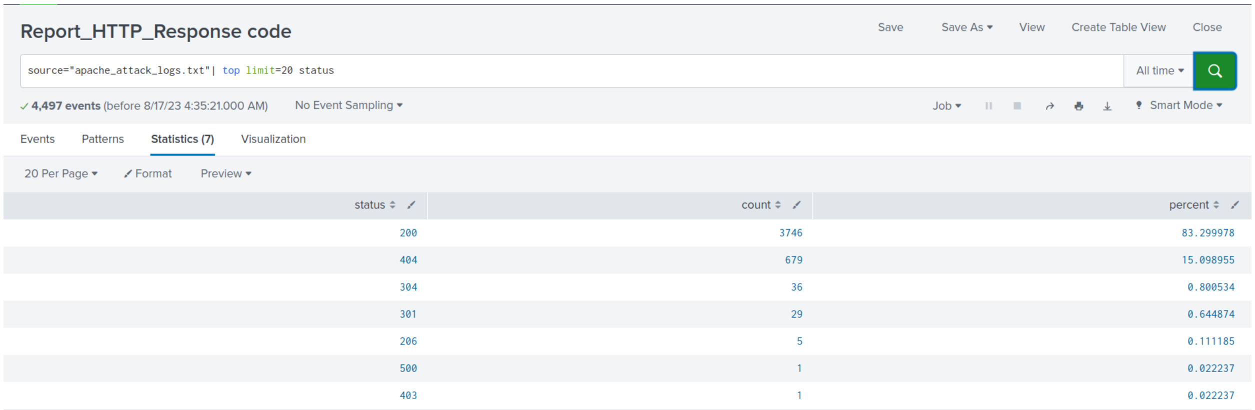


Report_HTTP_Response code

```
source="apache_logs.txt"| top limit=20 status
```

✓ 10,000 events (before 8/17/23 4:32:13.000 AM)

status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000



Report_HTTP_Response code

```
source="apache_attack_logs.txt"| top limit=20 status
```

✓ 4,497 events (before 8/17/23 4:35:21.000 AM)

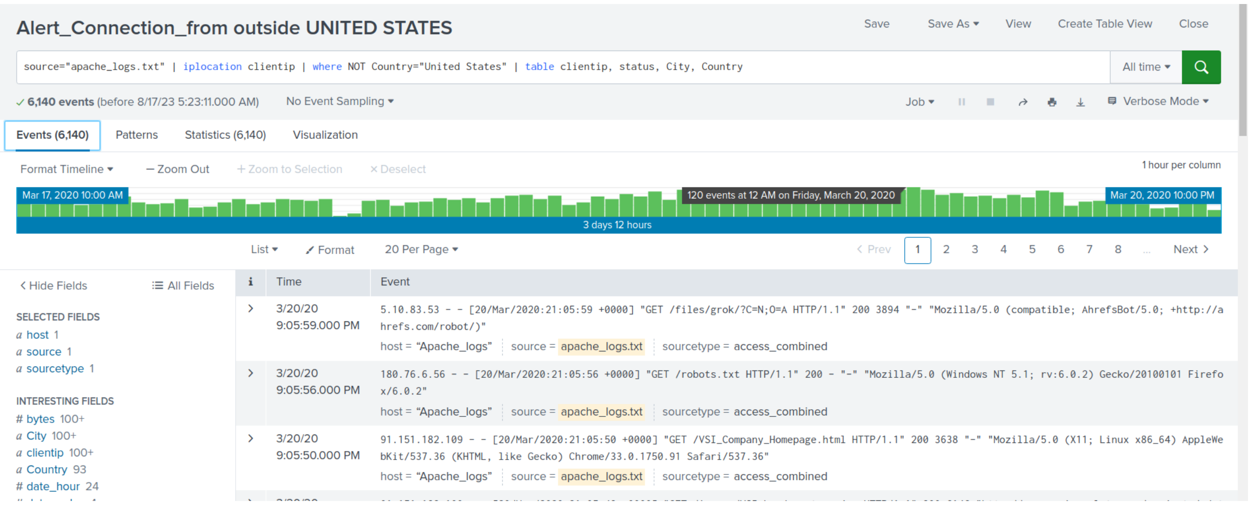
status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Alert Analysis for International Activity

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of international activity.
3. Select “Open in Search.”

4. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt`.

5. Review the updated results, and answer the following questions in the review document:
   - Did you detect a suspicious volume of international activity?
   - If so, what was the count of events in the hour(s) it occurred?
   - Would your alert be triggered for this activity?
   - After reviewing, would you change the threshold you previously selected?



Alert_Connection_from outside UNITED STATES

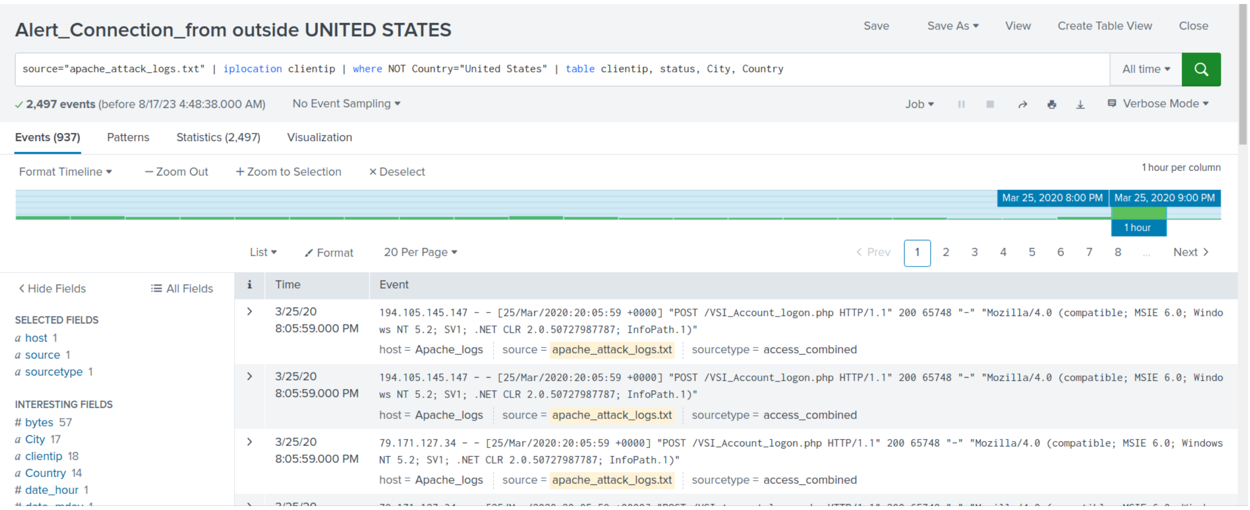
```
source="apache_logs.txt" | iplocation clientip | where NOT Country="United States" | table clientip, status, City, Country
```

✓ 6,140 events (before 8/17/23 5:23:11.000 AM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bytes 100+
a City 100+
a clientip 100+
a Country 93
# date_hour 24

Time	Event
3/20/20 9:05:59.000 PM	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/)" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:56.000 PM	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" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:50.000 PM	91.151.182.109 - - [20/Mar/2020:21:05:50 +0000] "GET /VSI_Company_Homepage.html HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined



Alert_Connection_from outside UNITED STATES

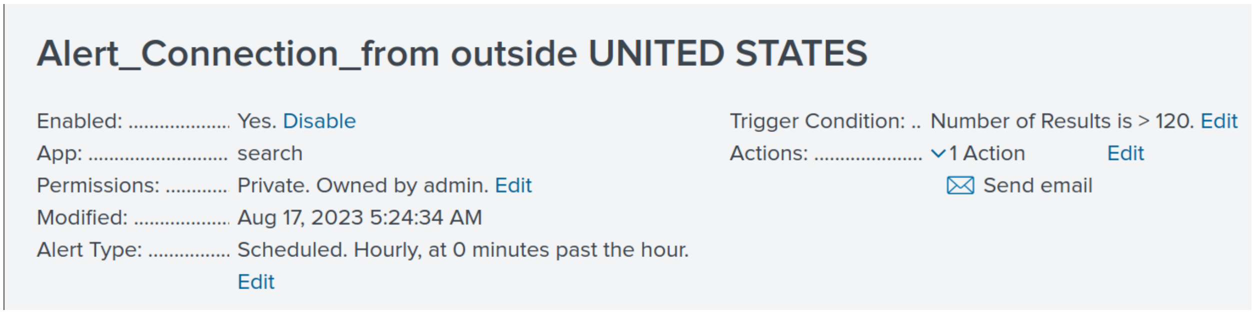
```
source="apache_attack_logs.txt" | iplocation clientip | where NOT Country="United States" | table clientip, status, City, Country
```

✓ 2,497 events (before 8/17/23 4:48:38.000 AM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bytes 57
a City 17
a clientip 18
a Country 14
# date_hour 1

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



Alert_Connection_from outside UNITED STATES

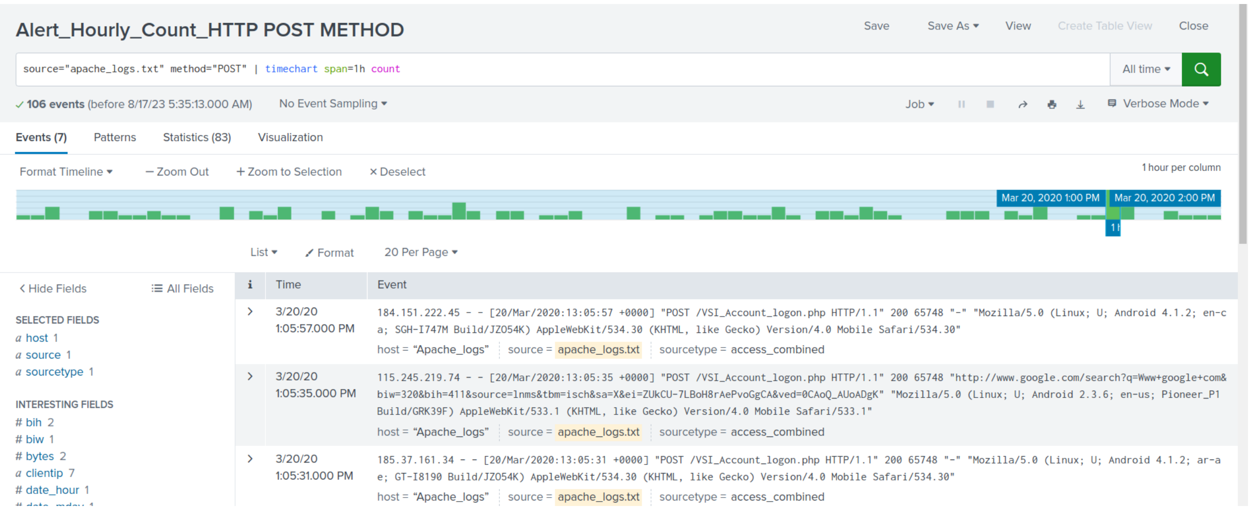
Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 17, 2023 5:24:34 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour.
Edit

Trigger Condition: .. Number of Results is > 120. Edit
Actions: .... ⌄1 Action Edit
✉ Send email

Alert Analysis for HTTP POST Activity

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of HTTP POST activity.
3. Select “Open in Search.”
4. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt`.
5. Review the updated results, and answer the following questions in the review document:
   - Did you detect any suspicious volume of HTTP POST activity?
   - If so, what was the count of events in the hour(s) it occurred?
   - When did it occur?
   - After reviewing, would you change the threshold that you previously selected?

Now, you will set up a dashboard and analyze the results.



Alert_Hourly_Count_HTTP POST METHOD

```
source="apache_logs.txt" method="POST" | timechart span=1h count
```

✓ **106 events** (before 8/17/23 5:35:13.000 AM)

SELECTED FIELDS
- *a* host 1
- *a* source 1
- *a* sourcetype 1

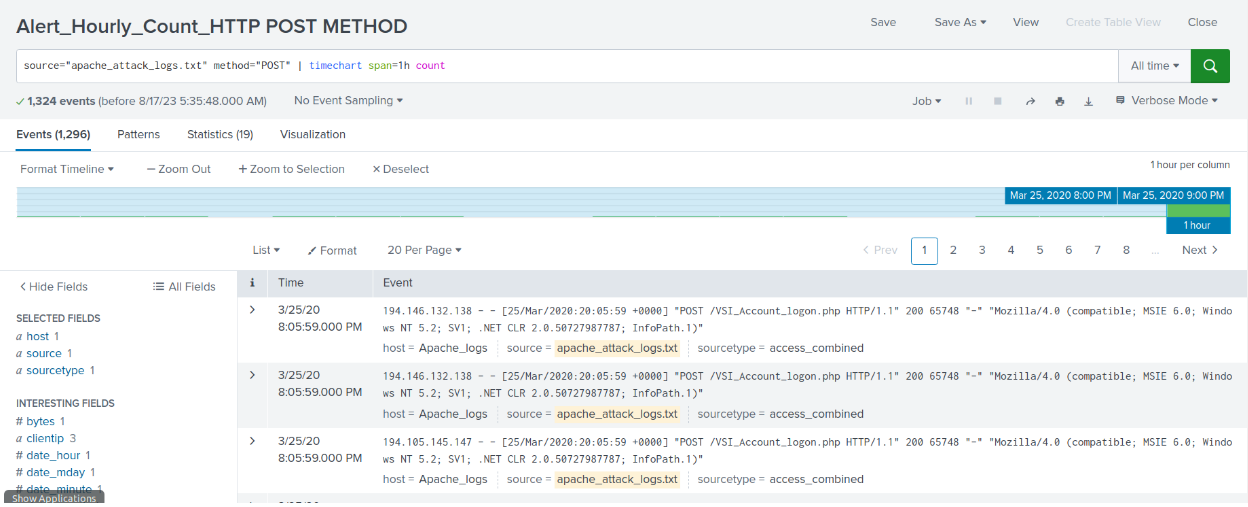
INTERESTING FIELDS
- # bih 2
- # biw 1
- # bytes 2
- *a* clientip 7
- # date_hour 1

i	Time	Event

>	3/20/20 1:05:57.000 PM	`184.151.222.45 - - [20/Mar/2020:13:05:57 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-ca; SGH-I747M Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30"`
		host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined

>	3/20/20 1:05:35.000 PM	`115.245.219.74 - - [20/Mar/2020:13:05:35 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "http://www.google.com/search?q=Www+google+com&biw=320&bih=411&source=lnms&tbm=isch&sa=X&ei=ZUkCU-7LBoH8rAePvoGgCA&ved=0CAoQ_AUoADgK" "Mozilla/5.0 (Linux; U; Android 2.3.6; en-us; Pioneer_P1 Build/GRK39F) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1"`
		host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined

>	3/20/20 1:05:31.000 PM	`185.37.161.34 - - [20/Mar/2020:13:05:31 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/5.0 (Linux; U; Android 4.1.2; ar-ae; GT-I8190 Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30"`
		host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined



Alert_Hourly_Count_HTTP POST METHOD

```
source="apache_attack_logs.txt" method="POST" | timechart span=1h count
```

✓ **1,324 events** (before 8/17/23 5:35:48.000 AM)

SELECTED FIELDS
- *a* host 1
- *a* source 1
- *a* sourcetype 1

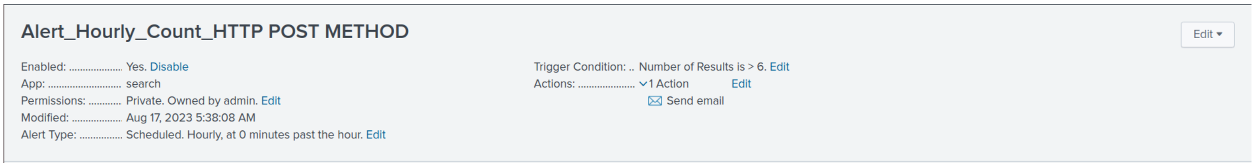
INTERESTING FIELDS
- # bytes 1
- *a* clientip 3
- # date_hour 1
- # date_mday 1
- # date_minute 1

i	Time	Event

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

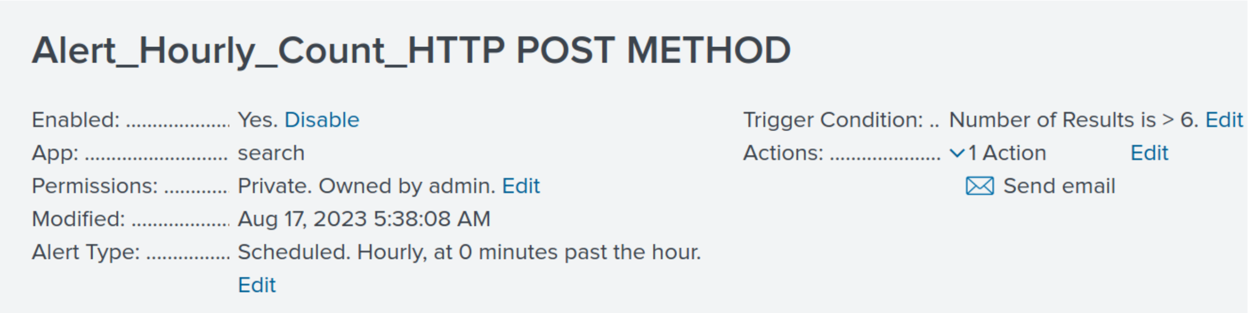
>	3/25/20 8:05:59.000 PM	`194.146.132.138 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)"`
		host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined

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



Alert_Hourly_Count_HTTP POST METHOD

Enabled:	Yes. Disable	Trigger Condition:	Number of Results is > 6. Edit
App:	search	Actions:	✓ 1 Action Edit ✉ Send email
Permissions:	Private. Owned by admin. Edit		
Modified:	Aug 17, 2023 5:38:08 AM		
Alert Type:	Scheduled. Hourly, at 0 minutes past the hour. Edit		



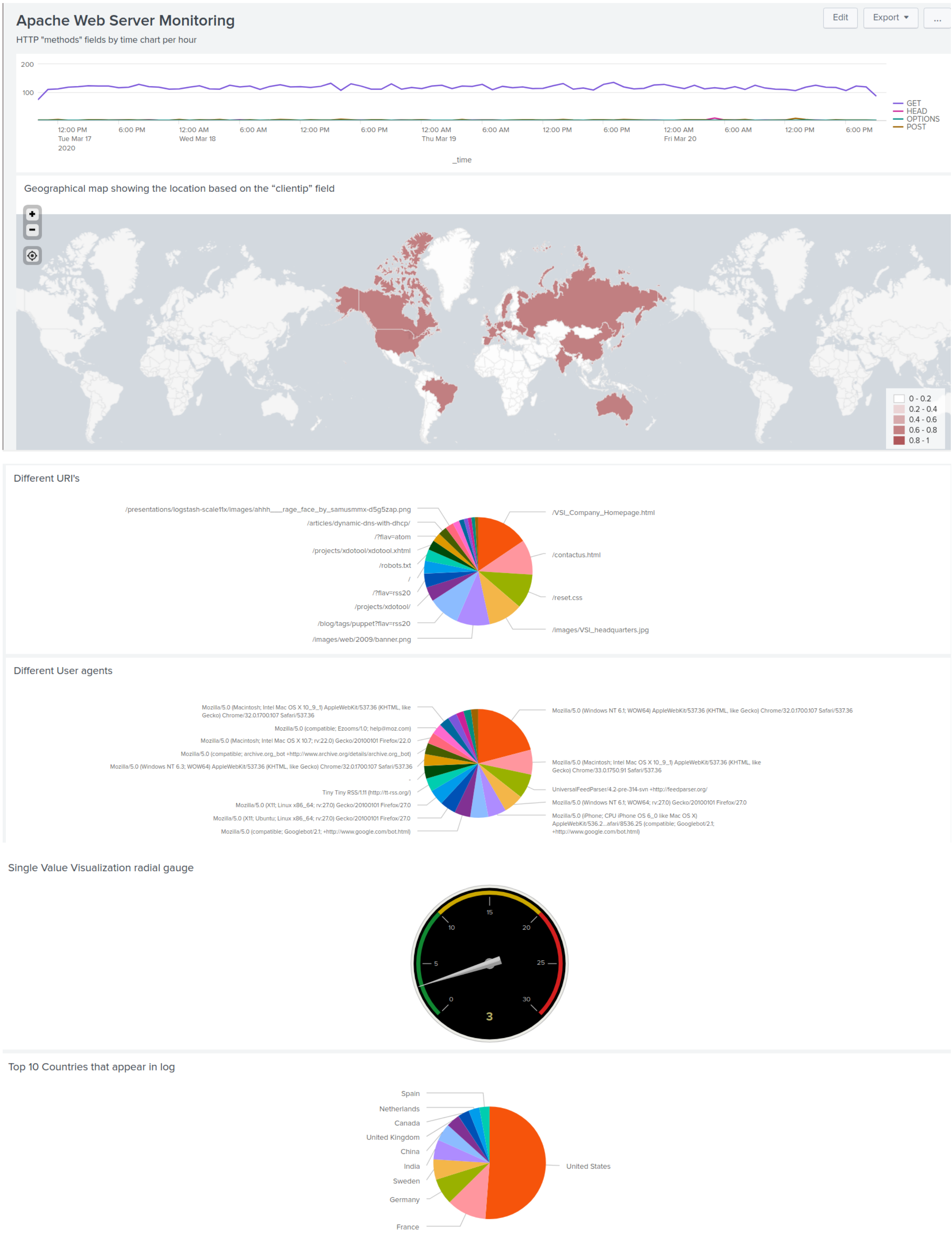
Alert_Hourly_Count_HTTP POST METHOD

Enabled:	Yes. Disable	Trigger Condition:	Number of Results is > 6. Edit
App:	search	Actions:	✓ 1 Action Edit ✉ Send email
Permissions:	Private. Owned by admin. Edit		
Modified:	Aug 17, 2023 5:38:08 AM		
Alert Type:	Scheduled. Hourly, at 0 minutes past the hour. Edit		

Dashboard Setup

1. Access the Apache Web Server Monitoring dashboard.
2. Select “Edit.”
3. For each panel that you created, access the panel and complete the following steps:
    - Select “Edit Search.”
    - Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt`.
    - Select “Apply.”
4. Save the whole dashboard.
5. Change the time on the whole dashboard to “All Time.”

(Before attack)



Apache Web Server Monitoring

HTTP "methods" fields by time chart per hour

200
100
12:00 PM
Tue Mar 17
2020
6:00 PM
12:00 AM
Wed Mar 18
6:00 AM
12:00 PM
6:00 PM
12:00 AM
Thu Mar 19
6:00 AM
12:00 PM
6:00 PM
12:00 AM
Fri Mar 20
6:00 AM
12:00 PM
6:00 PM
_time
GET
HEAD
OPTIONS
POST

Geographical map showing the location based on the “clientip” field

0 - 0.2
0.2 - 0.4
0.4 - 0.6
0.6 - 0.8
0.8 - 1

Different URI's

/presentations/logstash-scale11x/images/ahhh___rage_face_by_samusmmx-d5g5zap.png
/articles/dynamic-dns-with-dhcp/
/?flav=atom
/projects/xdotool/xdotool.xhtml
/robots.txt
/
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/VSI_Company_Homepage.html
/contactus.html
/reset.css
/images/VSI_headquarters.jpg

Different User agents

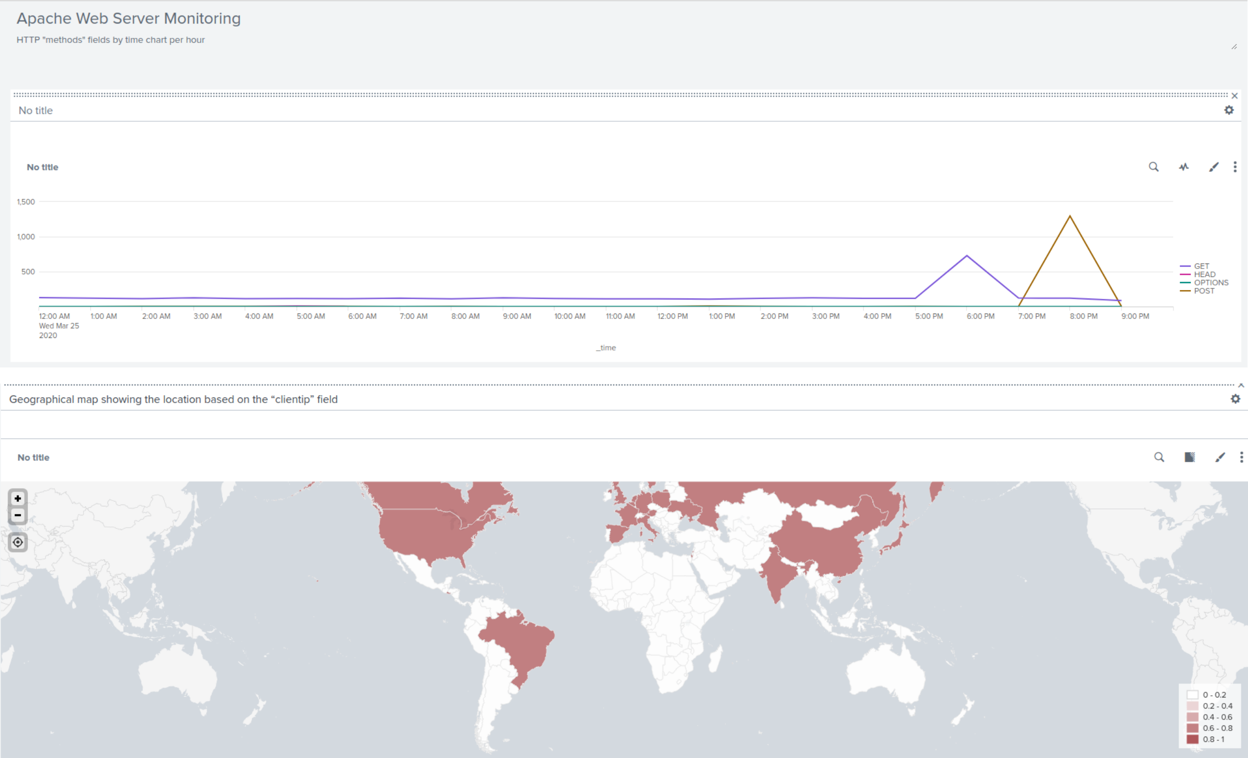
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:22.0) Gecko/20100101 Firefox/22.0
Mozilla/5.0 (compatible; archive.org_bot +http://www.archive.org/details/archive.org_bot)
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
-
Tiny Tiny RSS/1.11 (http://tt-rss.org/)
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)
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 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.2...afari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Single Value Visualization radial gauge

Top 10 Countries that appear in log

Spain
Netherlands
Canada
United Kingdom
China
India
Sweden
Germany
France
United States

(After attack)



Apache Web Server Monitoring

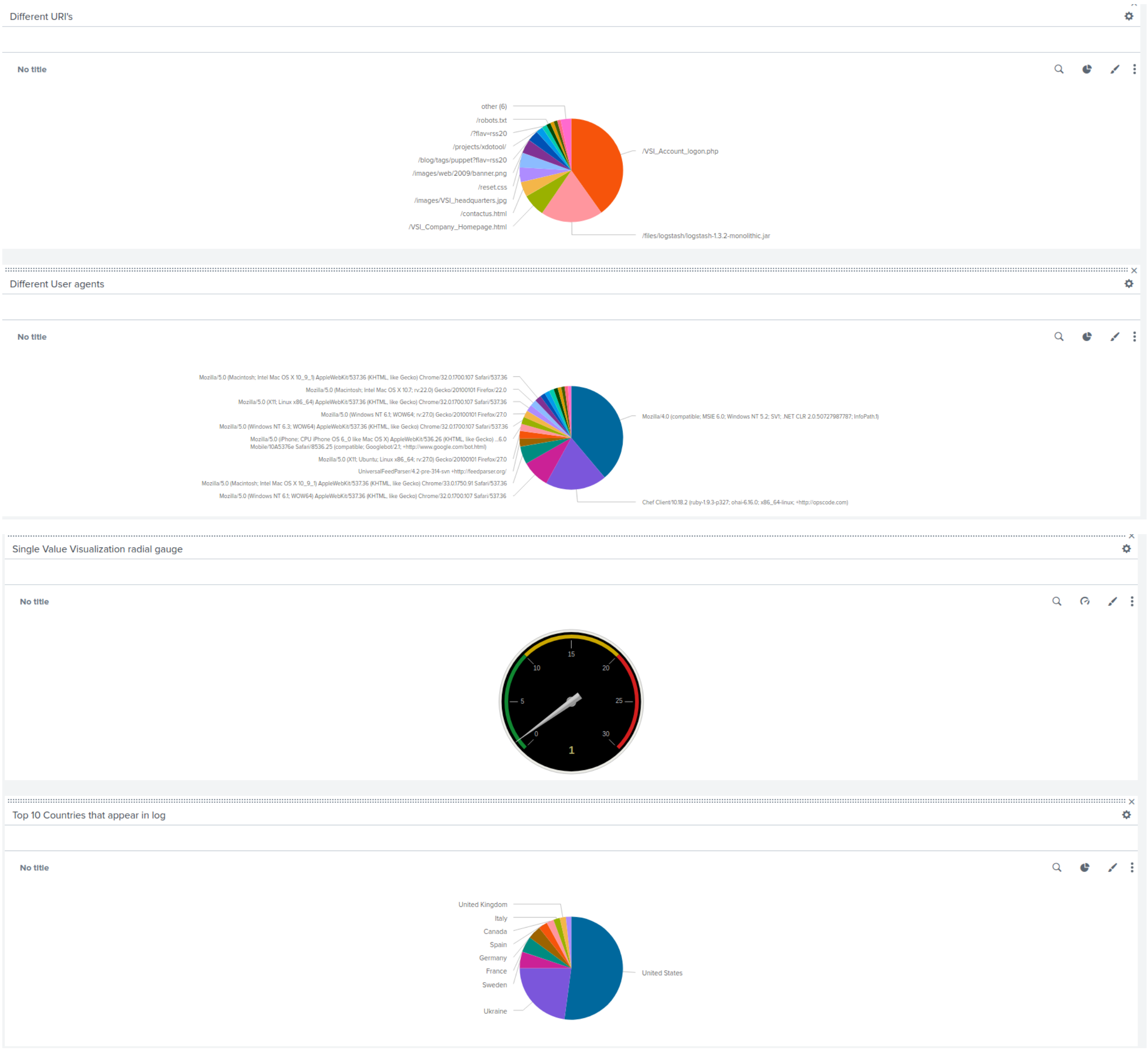
HTTP "methods" fields by time chart per hour

No title

No title

Geographical map showing the location based on the “clientip” field

No title


Different URI's

No title

other (6)
/robots.txt
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/reset.css
/images/VSI_headquarters.jpg
/contactus.html
/VSI_Company_Homepage.html
/VSI_Account_logon.php
/files/logstash/logstash-1.3.2-monolithic.jar

Different User agents

No title

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:22.0) Gecko/20100101 Firefox/22.0
Mozilla/5.0 (X11; Linux x86_64) 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 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) ...6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
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/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)

Single Value Visualization radial gauge

No title

Top 10 Countries that appear in log

No title

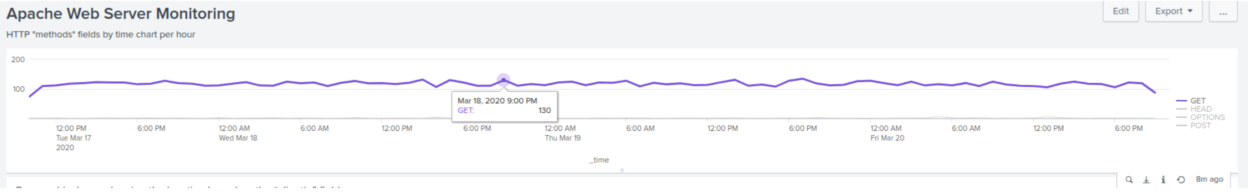
United Kingdom
Italy
Canada
Spain
Germany
France
Sweden
Ukraine
United States

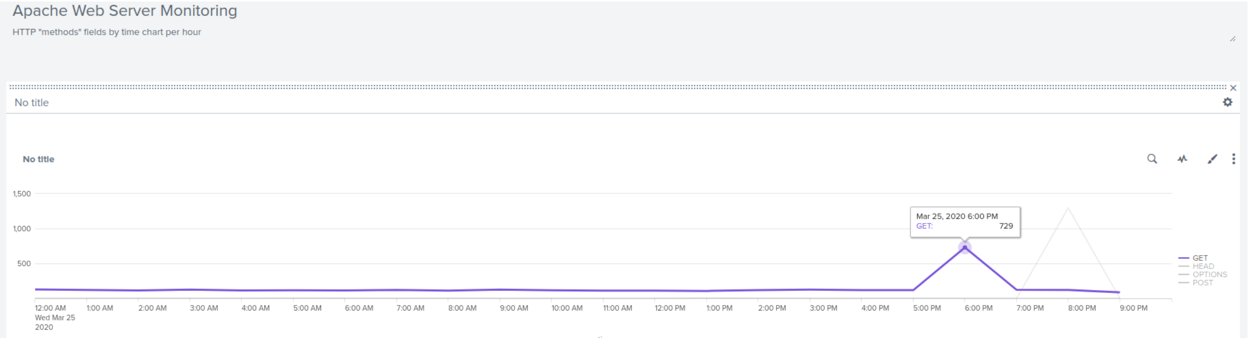
Dashboard Analysis for Time Chart of HTTP Methods

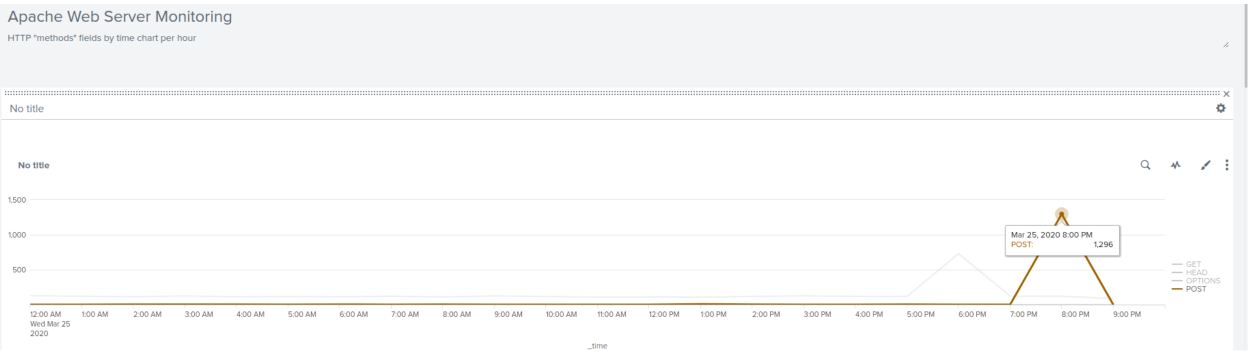
Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?
- Which method seems to be used in the attack?
- At what times did the attack start and stop?

- What is the peak count of the top method during the attack?



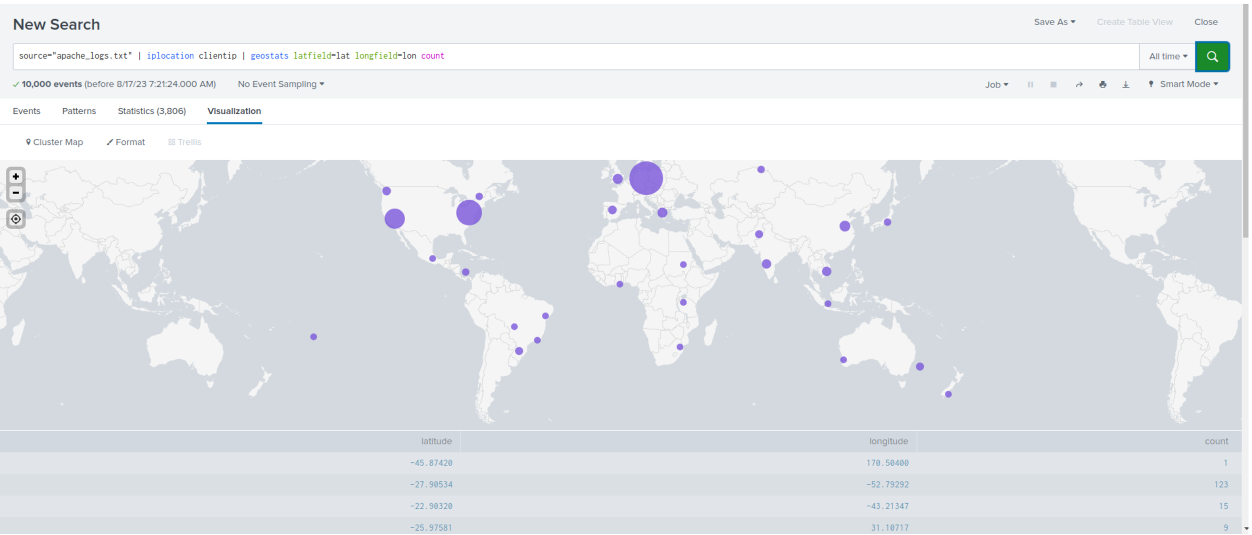




Dashboard Analysis for Cluster Map

Analyze your new cluster map results, and answer the following questions in the review document:

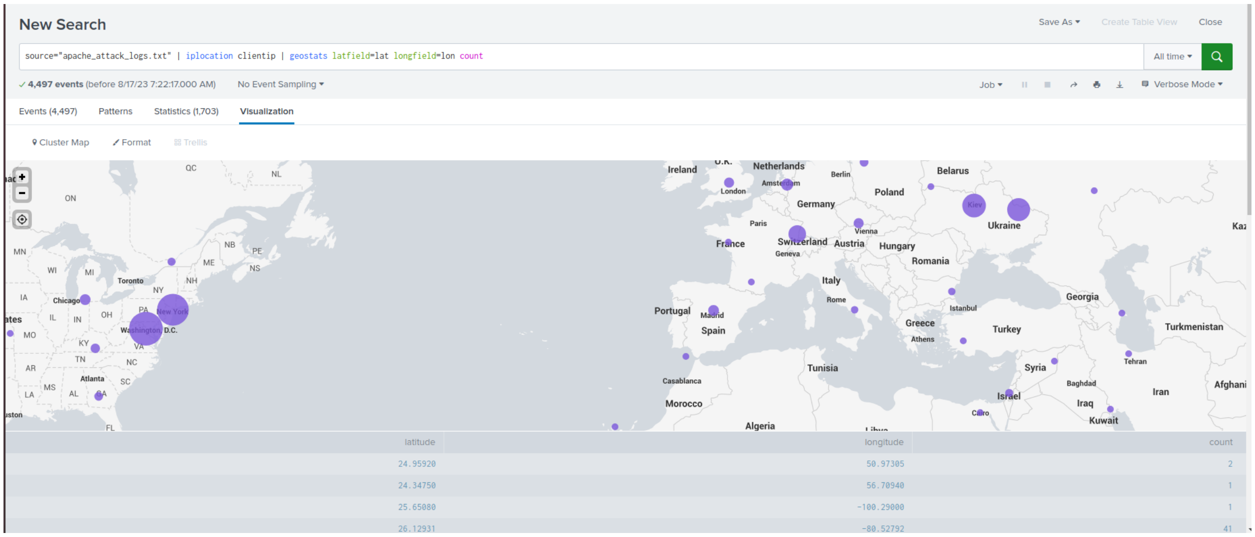
- Does anything stand out as suspicious?
- Which new location (city, country) on the map has a high volume of activity?
  - **Hint**: Zoom in on the map.
- What is the count of that city?



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

✓ 10,000 events (before 8/17/23 7:21:24.000 AM)

latitude	longitude	count
-45.87420	170.50400	1
-27.90534	-52.79292	123
-22.90320	-43.21347	15
-25.97581	31.10717	9



```
source="apache_attack_logs.txt" | iplocation clientip | geostats latfield=lat longfield=lon count
```

✓ 4,497 events (before 8/17/23 7:22:17.000 AM)

latitude	longitude	count
24.95920	50.97305	2
24.34750	56.70940	1
25.65080	-100.29000	1
26.12931	-80.52792	41

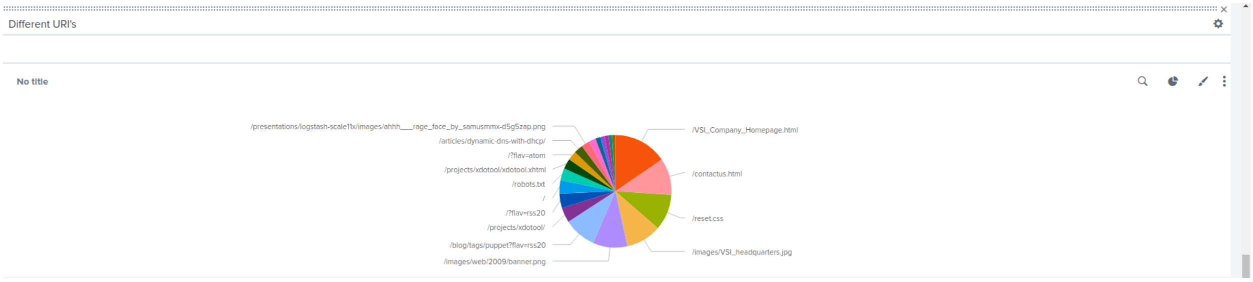
Dashboard Analysis for URI Data

Analyze your dashboard panel of the URI data, and answer the following questions in the review document:

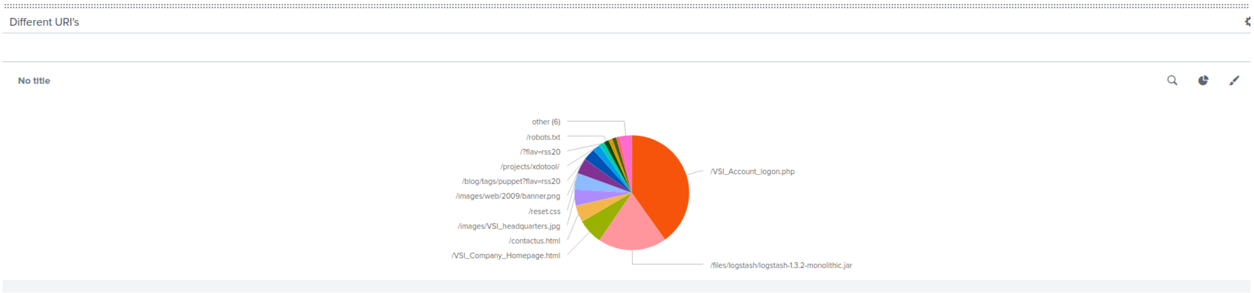
- Does anything stand out as suspicious?
- What URI is hit the most?

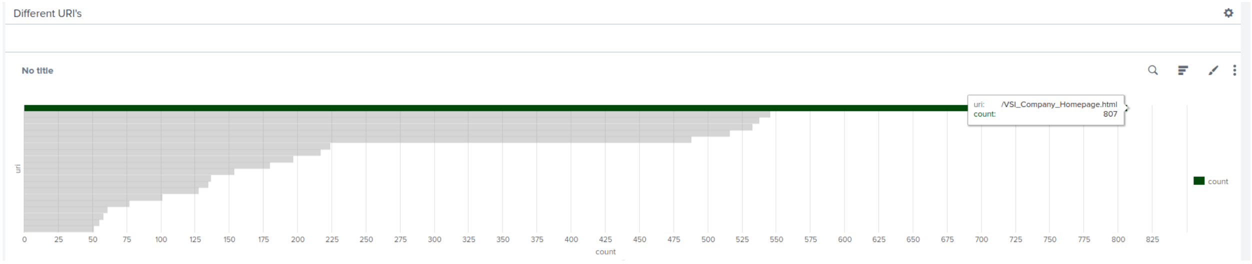
- Based on the URI being accessed, what could the attacker potentially be doing?

(Before attack)

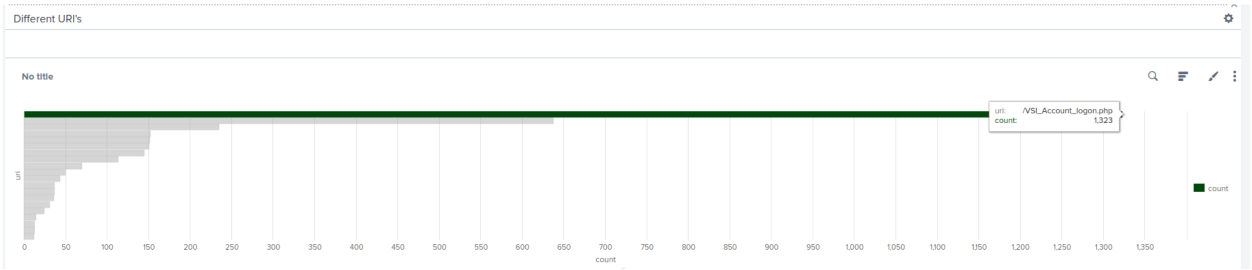

Different URI's
No title
/presentations/logstash-scale11x/images/ahhh___rage_face_by_samusmmx-d5g5zap.png
/articles/dynamic-dns-with-dhcp/
/?flav=atom
/projects/xdotool/xdotool.xhtml
/robots.txt
/
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/VSI_Company_Homepage.html
/contactus.html
/reset.css
/images/VSI_headquarters.jpg

(After attack)


Different URI's
No title
other (6)
/robots.txt
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/reset.css
/images/VSI_headquarters.jpg
/contactus.html
/VSI_Company_Homepage.html
/VSI_Account_logon.php
/files/logstash/logstash-1.3.2-monolithic.jar



uri: /VSI_Company_Homepage.html
count: 807



uri: /VSI_Account_logon.php
count: 1,323