

# *TryHackme: Learning Splunk SPL*

Clay Jones

## Objective:

The objective is to learn SPLs in Splunk, in order to perform SIEM searches more adequately.

## Performing a simple search

The screenshot shows the Splunk Search interface. The search bar contains the query `host=*cyber-host*`. Below the search bar, it indicates 134 events found for the time range 4/15/22 8:05:00.000 AM to 4/15/22 8:06:00.000 AM. The interface includes tabs for Events (134), Patterns, Statistics, and Visualization. A table view is selected, showing a list of events. The first event is highlighted, showing details for a system account named 'SYSTEM'.

Time	Event
4/15/22 8:05:56.000 AM	<pre>{ [-]   @version: 1   AccountName: SYSTEM   AccountType: User }</pre>

Just simply filter logs what contained “cyber-host”

New Search

Save As ▾ Create Table View Close

1 DestAddress="172.18.39.6" AND DestPort=135

All time 🔍

✓ 8 events (before 2/18/25 2:04:16.000 AM) No Event Sampling ▾

Job ▾ || ▮ → 📄 ⬇️ 🔊 Verbose Mode ▾

Events (8) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

1 second per column

List ▾ ✎ Format 50 Per Page ▾

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

Time

Event

>

4/15/22

8:06:17.000 AM

[ - ]

@version: 1

Application: \device\harddiskvolume2\windows\system32\svchost.exe

Category: Filtering Platform Connection

Channel: Security

## Using Boolean operators to filter logs and finding the source ips to the destination address.

## Find cases of a word

The screenshot shows the Splunk Search interface. The search bar at the top contains the query `index=windowslogs (*cyber*)`. Below the search bar, it indicates **12,256 events** found. The interface is divided into several sections:

- Events (12,256)**: A tab for viewing the search results.
- Format Timeline**: A button to format the timeline view.
- Zoom Out**: A button to zoom out the timeline.
- + Zoom to Selection**: A button to zoom to the selected event.
- x Deselect**: A button to deselect the current selection.
- 1 day per column**: A label indicating the time scale for the timeline view.
- List**: A button to view the results in a list format.
- Format**: A button to format the results.
- 50 Per Page**: A label indicating the number of results per page.

The main results area displays a table with the following columns: **Time** and **Event**. The first event is shown with the following details:

- Time**: 7/14/22 11:37:59.000 PM
- Event**:
  - `@version: 1`
  - `AccountName: SYSTEM`
  - `AccountType: User`
  - `CallTrace: C:\windows\SYSTEM32\ntdll.dll+9c534[C:\windows\SYSTEM32\psmserviceexthost.dll+222a3[C:\windows\SYSTEM32\psmserviceexthost.dll+1a172[C:\wind`
  - `Category: Process accessed (rule: ProcessAccess)`
  - `Channel: Microsoft-Windows-Sysmon/Operational`
  - `Domain: NT AUTHORITY`
  - `EventID: 10`
  - `EventReceivedTime: 2022-04-15 08:05:46`
  - `EventTime: 2022-04-15 08:05:44`

This searches for the cases that “cyber\*” shows up.

## Sorting Data

1 index=windowslogs | table EventID User Image Hostname | dedup EventID

✓ 12,256 events (before 2/18/25 2:25:04.000 AM) No Event Sampling

Events (12,256) Patterns **Statistics (55)** Visualization

100 Per Page Format Preview

EventID	User	Image	Hostname
10			Micheal.Beaven
5156			James.browne
5158			James.browne
800			James.browne
4103			James.browne
12		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	James.browne
3	NT AUTHORITY\SYSTEM	C:\Windows\System32\dns.exe	Salena.Adam
22		C:\Windows\System32\svchost.exe	James.browne
4658			James.browne
4663			James.browne

10.10.206.247/en-US/app/search/search?q=search index%3Dwindowslogs | table \_time EventID Hostname SourceName | reverse

1 index=windowslogs | table \_time EventID Hostname SourceName | reverse

2 | dedup Hostname

✓ 12,256 events (before 2/18/25 2:26:45.000 AM) No Event Sampling

Events (12,256) Patterns **Statistics (3)** Visualization

100 Per Page Format Preview

_time	EventID	Hostname	SourceName
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	10	Micheal.Beaven	Microsoft-Windows-Sysmon
2022-04-15 08:05:46	5158	Salena.Adam	Microsoft-Windows-Security-Auditing

splunk>enterprise

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 index=windowslogs | rare limit=8 User

✓ 12,256 events (before 2/18/25 2:48:11.000 AM) No Event Sampling

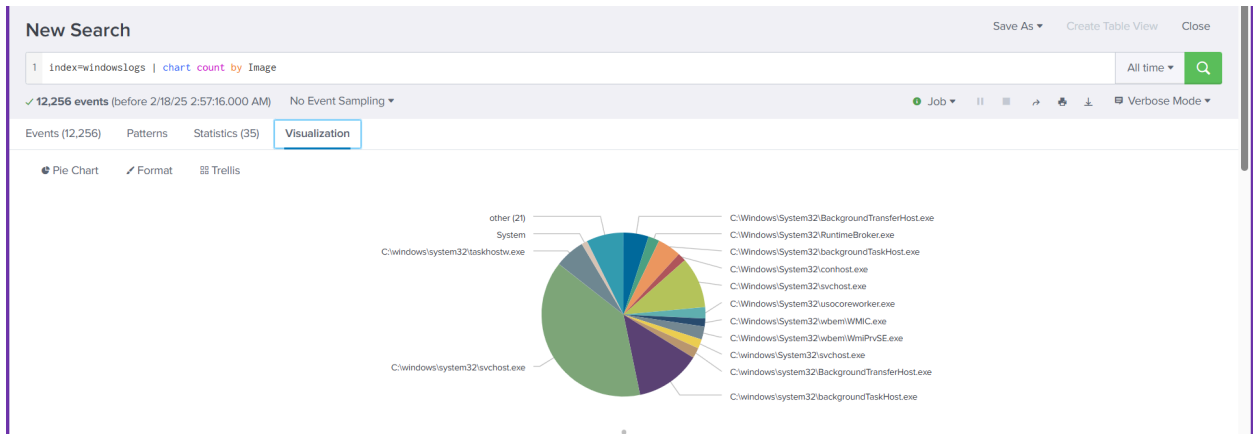
Events (12,256) Patterns **Statistics (4)** Visualization

100 Per Page Format Preview

User	count	percent
Cybertees\James	5	4.201681
NT AUTHORITY\NETWORK SERVICE	20	16.806723
Cybertees\Alberto	24	20.168067
NT AUTHORITY\SYSTEM	70	58.823529

I created tables and sorted the data via the reverse filter. I also used the head and tail commands to show the top and bottom. Depup was used to ignore duplicates.

## Creating a graph



Using a graph to sort the data.

## Important SPL commands