

# Splunk - Exploring SPL

27072023Thu

[TryHackMe](#) | [Splunk: Exploring SPL](#)

Learn and explore the basics of the Search Processing Language.

The screenshot shows the TryHackMe dashboard for the 'Splunk: Exploring SPL' lab. The top navigation bar includes links for Dashboard, Learn, Compete, and Other, along with buttons for 'Access Machines', 'Go Premium', and a user profile. The main header features a large green play button icon and the title 'Splunk: Exploring SPL' with the subtitle 'Learn and explore the basics of the Search Processing Language.' Below this, there's a section for 'Active Machine Information' with a table showing the machine title 'Exploring\_\_SPL', IP address '10.10.24.117', and expiration time '57m 41s'. A progress bar indicates 5% completion. The task list shows 'Task 1 Introduction' (completed) and 'Task 2 Connect with the Lab' (in progress). The 'Room Machine' section provides instructions on how to start the machine and access the lab, including a note about the index 'windowslogs'.

Title	IP Address	Expires	
Exploring__SPL	10.10.24.117	57m 41s	<a href="#">?</a> <a href="#">Add 1 hour</a> <a href="#">Terminate</a>

5%

Task 1 ☒ Introduction

Task 2 ☐ Connect with the Lab

**Room Machine** [Start Machine](#)

Before moving forward, deploy the machine. You can access this lab in the AttackBox or click <https://10-10-24-117.p.thmlabs.com/> to start the lab in your browser when the machine is fully started. The machine will take up to 3-5 minutes to start.

**Note:** For this room, we will work on the index `windowslogs`.

The screenshot shows the Splunk Enterprise web interface in a Mozilla Firefox browser. The left sidebar contains the 'Apps' menu with options like 'Search & Reporting', 'Python Upgrade Readiness App', 'Splunk Essentials for Cloud and Enterprise 8.2', and 'Splunk Secure Gateway'. The main content area is titled 'Explore Splunk' and features three cards: 'Add Data' (with a plus icon), 'Splunk Apps' (with a puzzle piece icon), and 'Splunk Docs' (with a book icon). Below these cards, there's a section for 'Forwarders: Instance' with a status indicator and a 'Close' button. A message at the bottom states 'Forwarder Monitoring is disabled. Please go to the setup page to enable it.'

Home | Splunk 8.2.6 — Mozilla Firefox

10-10-24-117.p.thmlabs.com/en-US/app/launcher/home

splunk>enterprise

Apps

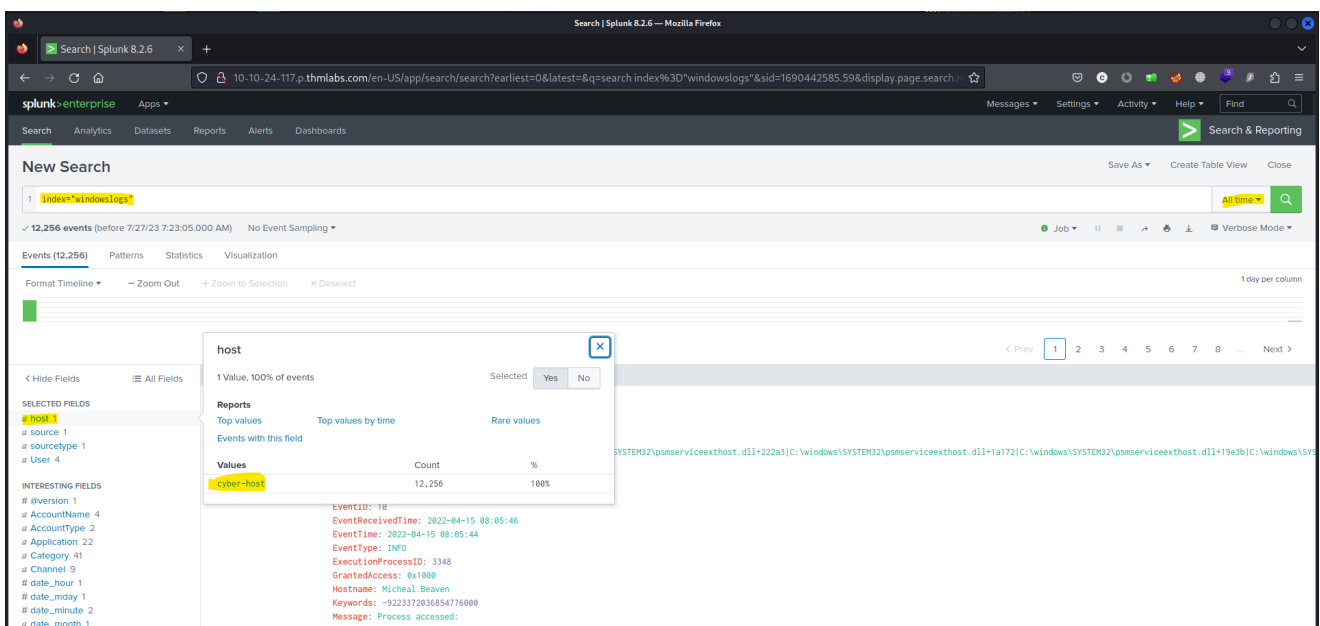
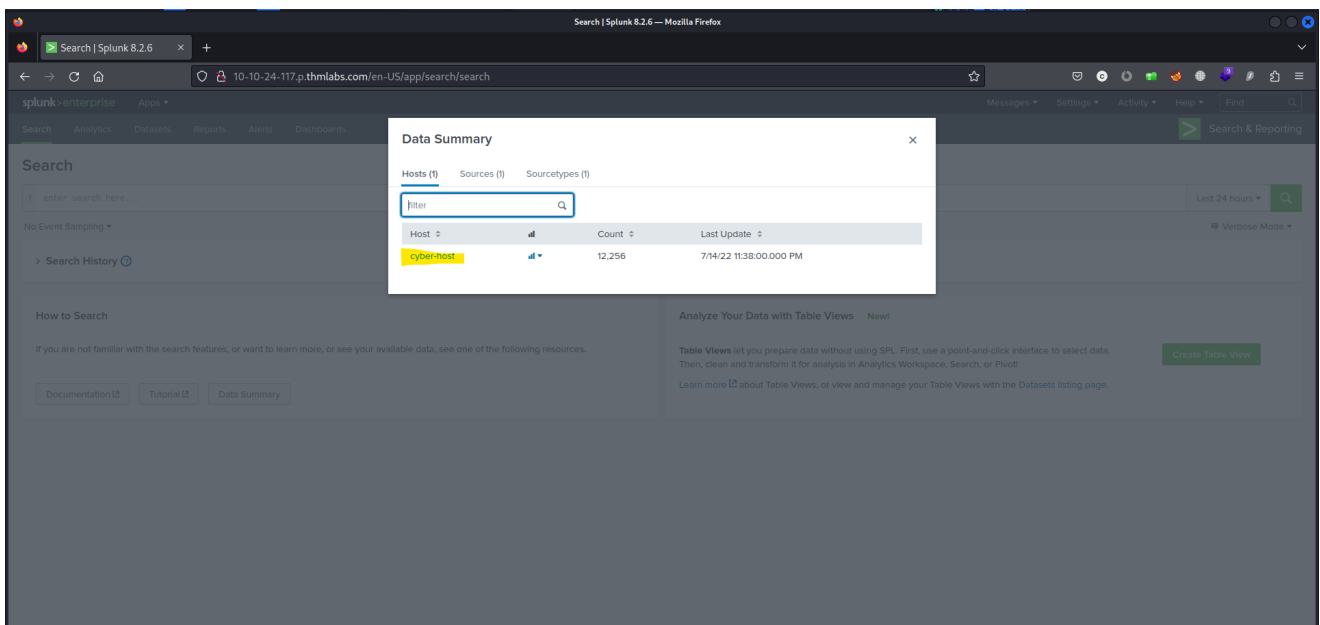
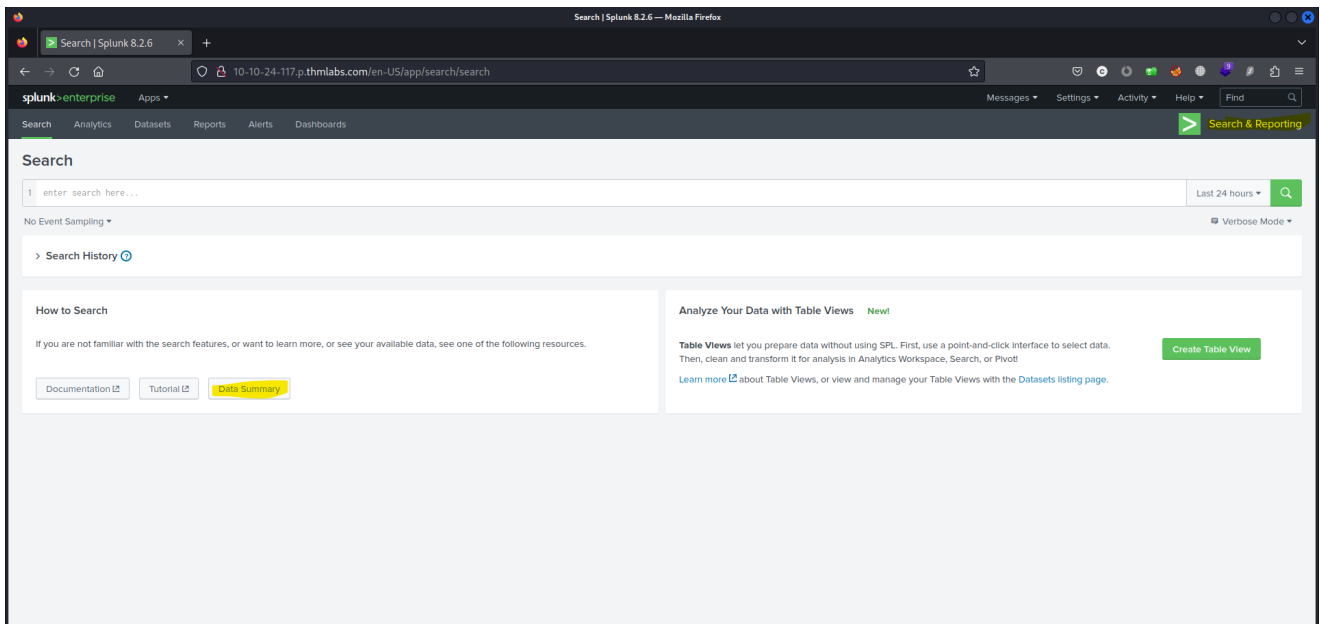
- Search & Reporting
- Python Upgrade Readiness App
- Splunk Essentials for Cloud and Enterprise 8.2
- Splunk Secure Gateway
- + Find More Apps

Explore Splunk

- Add Data**  
Add or forward data to Splunk. Afterwards, you may [extract fields](#).
- Splunk Apps**  
Apps and add-ons extend the capabilities of Splunk.
- Splunk Docs**  
Comprehensive documentation for Splunk and for all other Splunk products.

Forwarders: Instance [?](#) [Close](#)

Forwarder Monitoring is disabled. Please go to the [setup](#) page to enable it.



## Task 2 Connect with the Lab

What is the name of the host in the Data Summary tab?

cyber-host

The screenshot shows the Splunk Search & Reporting app interface. The Search History panel on the left lists several search queries. The 7th query is highlighted in yellow and marked with a red '7'. The query is: `index=windowslogs | chart count(EventCode) by Image`. The right panel shows the results of the selected search, including a table of event counts by image.

## Task 3 Search & Reporting App Overview

In the search History, what is the 7th search query in the list? (excluding your searches from today)

index=windowslogs | chart count(EventCode) by Image

The screenshot shows the Splunk Search & Reporting app interface. The left panel shows the field list, with `SourceAddress` highlighted. The right panel shows the Data Summary tab for the selected search query. The `SourceAddress` field is selected, and a table of event counts by source address is displayed. The table shows that the source address `172.90.12.11` has the highest count of events.

In the left field panel, which Source IP has recorded max events?

172.90.12.11

The screenshot shows the Splunk Search interface. The search bar contains the query: `host="cyber-host" index="windowslogs" | eventcount summarize=false index="1" dedup index | rename index as name | fields name source="Event_logs.json" host="cyber-host" index="windowslogs" sourcetype="json" index="*" | *`. The date and time range filter is set to `04/15/2022` from `08:05:00.000` to `08:06:00.000`. The search results show 134 events.

The screenshot shows the Splunk Search interface with the search results for the query `index=windowslogs | chart count(EventCode) by Image`. The results are displayed in a table with columns for Image and count(EventCode). The table shows 6 results, with the first row being `C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe` and a count of 0.

*How many events are returned when we apply the time filter to display events on 04/15/2022 and Time from 08:05 AM to 08:06 AM?*

134

## Task 4 Splunk Processing Language Overview

User="\*James\*" AND EventID="1"

The screenshot shows a Splunk search interface with the query `User=*James* AND EventID=1`. The search results show 4 events. The first event is expanded, showing details for a process creation event.

Time	Event
4/15/22 8:06:02.000 AM	<pre>{   @version: 1   AccountName: SYSTEM   AccountType: User   Category: Process Create (rule: ProcessCreate)   Channel: Microsoft-Windows-Sysmon/Operational   CommandLine: C:\windows\system32\net1 user /add Alberto.paw@rd1   Company: Microsoft Corporation   CurrentDirectory: C:\windows\system32\   Description: Net Command   Domain: NT AUTHORITY   EventID: 1   EventReceivedTime: 2022-04-15 08:06:02   EventTime: 2022-04-15 08:06:02   EventType: INFO   ExecutionProcessID: 3348   FileVersion: 10.0.18362.997 (WinBuild.160101.0800)   HostName: SAL-01-2022-04-15 08:06:02.000 AM }</pre>

How many Events are returned when searching for Event ID 1 AND User as James?

4

`index="windowslogs" AND DestinationIp="172.18.39.6" AND DestinationPort="135"`

The screenshot shows a Splunk search interface with the query `index="windowslogs" AND DestinationIp="172.18.39.6" AND DestinationPort="135"`. The search results show 4 events. The first event is expanded, showing details for a network connection event.

Time	Event
4/15/22 8:06:02.000 AM	<pre>{   @version: 1   AccountName: SYSTEM   AccountType: User   Category: Network connection detected (rule: NetworkConnect)   Channel: Microsoft-Windows-Sysmon/Operational   DestinationHostname: -   DestinationIp: 172.18.39.6   DestinationIpV6: false   DestinationPort: 135   DestinationPortName: -   Domain: NT AUTHORITY   EventID: 3   EventReceivedTime: 2022-04-15 08:06:05   EventTime: 2022-04-15 08:06:03   EventType: INFO   ExecutionProcessID: 3348   HostName: Michael3-Benson }</pre>

How many events are observed with Destination IP 172.18.39.6 AND destination Port 135?

4

`index=windowslogs Hostname="Salena.Adam" DestinationIp="172.18.38.5"`

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=windowslogs Hostname="Salena.Adam" DestinationIp="172.18.38.5"`. The search results show 19 events. A dialog box titled "Sourcetype" is open, showing a table of values for the field "SourceIP".

Values	Count	%
172.90.12.11	17	89.474%
172.18.38.5	2	10.526%

What is the Source IP with highest count returned with this Search query?

Search Query: `index=windowslogs Hostname="Salena.Adam" DestinationIp="172.18.38.5"`

172.90.12.11

`index=windowslogs Hostname="cyber"`

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=windowslogs Hostname="cyber"`. The search results show 0 events. The message "No results found." is displayed in the center of the results area.

In the index windowslogs, search for all the events that contain the term **cyber** how many events returned?

0

`index="windowslogs" OR Hostname="cyber*"`

A screenshot of a web browser displaying the Splunk search interface. The address bar shows a URL from thmlabs.com. The page title is "Search | Splunk 8.2.6". The navigation bar includes links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. A search bar at the top contains the query "index='windowslogs' OR Hostname%'cybera'". Below the search bar, it indicates "12,256 events" were found. The main content area displays a table of search results. The first result is expanded, showing fields like @version, AccountName, AccountType, CallTrace, Category, Channel, Domain, EventID, EventReceivedTime, EventType, ExecutionProcessID, GrantedAccess, Hostname, Keywords, and Message. The host information on the left lists selected fields such as host, source, sourcetype, and user.

Now search for the term `cyber` , how many events are returned?\*

12256

## Task 5 Filtering the Results in SPL

```
index=windowslogs | table _time EventID Hostname SourceName | reverse
```

The screenshot displays the Splunk Search interface. At the top, the search bar contains the query: `index=windowslogs | table _time EventID Hostname SourceName | reverse`. Below the search bar, the results are summarized as 12,256 events. The 'Statistics (12,256)' tab is selected, showing a table of results. The table has four columns: `_time`, `EventID`, `Hostname`, and `SourceName`. The first three rows are highlighted with red numbers 1, 2, and 3. Row 1 shows EventID 800, Hostname James.browne, SourceName PowerShell. Row 2 shows EventID 800, Hostname James.browne, SourceName PowerShell. Row 3 shows EventID 4103, Hostname James.browne, SourceName Microsoft-Windows-PowerShell.

_time	EventID	Hostname	SourceName
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	10	Michael.Beaven	Microsoft-Windows-Sysmon
2022-04-15 08:05:46	10	Michael.Beaven	Microsoft-Windows-Sysmon
2022-04-15 08:05:46	10	Michael.Beaven	Microsoft-Windows-Sysmon

*What is the third EventID returned against this search query?*

4103

```
index=windowslogs | table _time EventID Hostname SourceName | dedup Hostname |
reverse
```

**New Search**

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

✓ 12,256 events (before 7/27/23 2:12:10.000 PM) No Event Sampling

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

100 Per Page ✓ Format Preview

_time	EventID	Hostname	SourceName
2022-04-15 08:06:38	3	Salena.Adam	Microsoft-Windows-Sysmon
2022-07-14 23:37:59	5156	James.browne	Microsoft-Windows-Security-Auditing
2022-07-14 23:37:59	10	Micheal.Beaven	Microsoft-Windows-Sysmon

Use the dedup command against the Hostname field before the reverse command in the query mentioned in Question 1. What is the first username returned in the Hostname field?

Salena.Adam

## Task 6 SPL - Structuring the Search Results

```
index=windowslogs | table _time EventID Hostname SourceName
| reverse
```

**New Search**

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

✓ 12,256 events (before 7/27/23 2:16:35.000 PM) No Event Sampling

Events (12,256) Patterns **Statistics (12,256)** 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	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
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	10	Micheal.Beaven	Microsoft-Windows-Sysmon
2022-04-15 08:05:46	10	Micheal.Beaven	Microsoft-Windows-Sysmon

Using the Reverse command with the search query index=windowslogs | table \_time EventID Hostname SourceName - what is the HostName that comes on top?

James.browne

```
index=windowslogs | table _time EventID Hostname SourceName | tail
```



**New Search**

1 index=windowslogs | table \_time EventID Hostname SourceName  
2 | tail

✓ 12,256 events (before 7/27/23 2:20:01.000 PM) No Event Sampling

Events (12,256) Patterns **Statistics (10)** 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	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	800	James.browne	PowerShell
2022-04-15 08:05:46	4103	James.browne	Microsoft-Windows-PowerShell

What is the last EventID returned when the query in question 1 is updated with the **tail** command?

4103

index=windowslogs | table \_time EventID Hostname SourceName | sort SourceName

**New Search**

1 index=windowslogs | table \_time EventID Hostname SourceName  
2 | sort SourceName

✓ 12,256 events (before 7/27/23 2:22:55.000 PM) No Event Sampling

Events (12,256) Patterns **Statistics (10,000)** Visualization

100 Per Page ✓ Format Preview

_time	EventID	Hostname	SourceName
2022-04-15 08:06:07	16977	James.browne	Microsoft-Windows-Directory-Services-SAM
2022-04-15 08:06:07	1502	James.browne	Microsoft-Windows-GroupPolicy
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:48	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:43	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:38	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:38	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:38	4103	James.browne	Microsoft-Windows-PowerShell
2022-04-15 08:06:38	4103	James.browne	Microsoft-Windows-PowerShell

Sort the above query against the SourceName. What is the top SourceName returned?

Microsoft-Windows-Directory-Services-SAM

## Task 7 Transformational Commands in SPL

index=windowslogs | top limit=8 Image

Image	count	percent
C:\windows\system32\svchost.exe	1642	38.836329
C:\windows\system32\backgroundTaskHost.exe	547	12.937559
C:\Windows\System32\svchost.exe	426	10.075686
C:\windows\system32\taskhostw.exe	250	5.912961
C:\Windows\System32\backgroundTransferHost.exe	210	4.966887
C:\Windows\System32\backgroundTaskHost.exe	196	4.635762
C:\Windows\System32\wbem\WmiPrivSE.exe	188	2.554399
C:\Windows\System32\usocoreworker.exe	95	2.246925

List the top 8 Image processes using the top command - what is the total count of the 6th Image?

196

index=windowslogs | rare User

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

Using the rare command, identify the user with the least number of activities captured?

James

index=windowslogs | chart count by Image

