Source types available

Your Splunk deployment has hundreds of data sources stretching over days, weeks, months or years. You need to know which ones are relevant to a certain investigation.

Required data

The data needed in this procedure depends on the types of events you are investigating. The data descriptors can help you decide what data is appropriate for your goal.

Procedure

1. Set the search time range to the time relevant to the investigation, if known.
2. Run the following search. You can optimize it by specifying an index and adjusting the time range.
   
   \[
   \begin{align*}
   \text{| metadata type=sourcetypes} \\
   \text{| sort - totalCount}
   \end{align*}
   \]

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>\text{</td>
<td>metadata type=sourcetypes}</td>
</tr>
<tr>
<td></td>
<td>The metadata command can also be used to see the sources and hosts on your network.</td>
</tr>
<tr>
<td></td>
<td>You can only use the metadata command if you have the get_metadata capability added to your role.</td>
</tr>
<tr>
<td>\text{</td>
<td>sort - totalCount}</td>
</tr>
</tbody>
</table>
Next steps

The result shows all the source types available to you. The source type you focus on depends on the nature of the investigation. For example, if you’re hunting in PowerShell, you probably want to focus on host-based data sources like Microsoft event logs and Microsoft Sysmon. You might later also look at network data sources, but host-based sources are a good start.

Finally, you might be interested in other processes associated with the Creating a timebound picture of network activity use case.