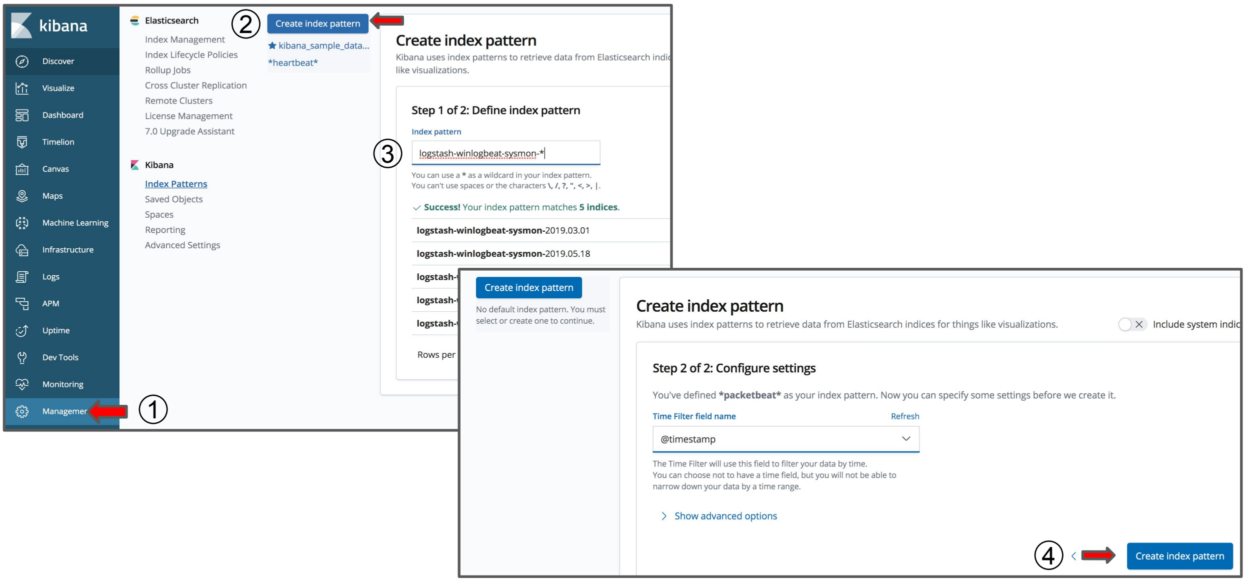
Create Index Pattern for Sysmon



Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indic like visualizations.

Step 1 of 2: Define index pattern

Index pattern: logstash-winlogbeat-sysmon-*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ Success! Your index pattern matches 5 indices.

logstash-winlogbeat-sysmon-2019.03.01
logstash-winlogbeat-sysmon-2019.05.18
logstash-
logstash-
logstash-

Rows per

No default index pattern. You must select or create one to continue.

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Include system indic

Step 2 of 2: Configure settings

You've defined *packetbeat* as your index pattern. Now you can specify some settings before we create it.

Time Filter field name: @timestamp

Refresh

The Time Filter will use this field to filter your data by time.
You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

Show advanced options

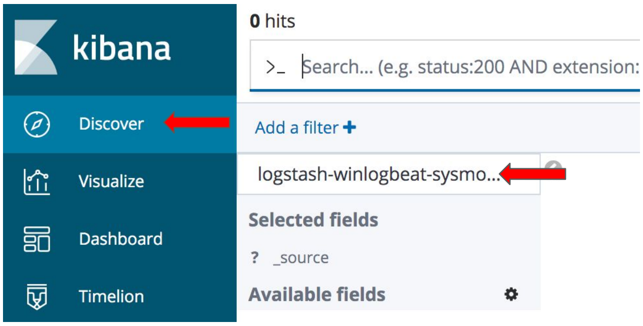
In this lab we will add a Logstash filter that will count the length of the command line from the process create event in Sysmon.

First we need to create an index pattern for the Sysmon index.

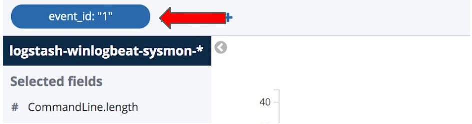
1) Open Kibana either from the shortcut on the CentOS machine or by visiting http://<CentOS IP>:5601/ from your host machine.
2) Verify there is a sysmon index pattern, if not create one like the screenshot above
3) Type logstash-winlogbeat-sysmon-* then click Next Step
4) Select @timestamp from the dropdown, then click Create index pattern

Get command line field name from Sysmon

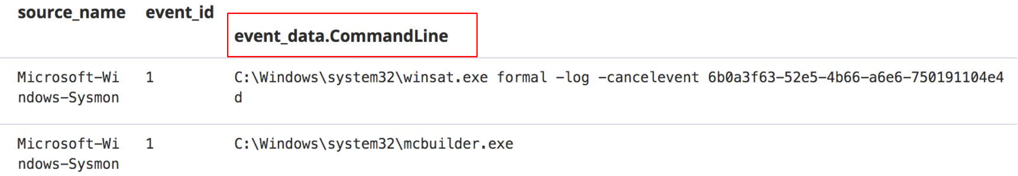
1



2



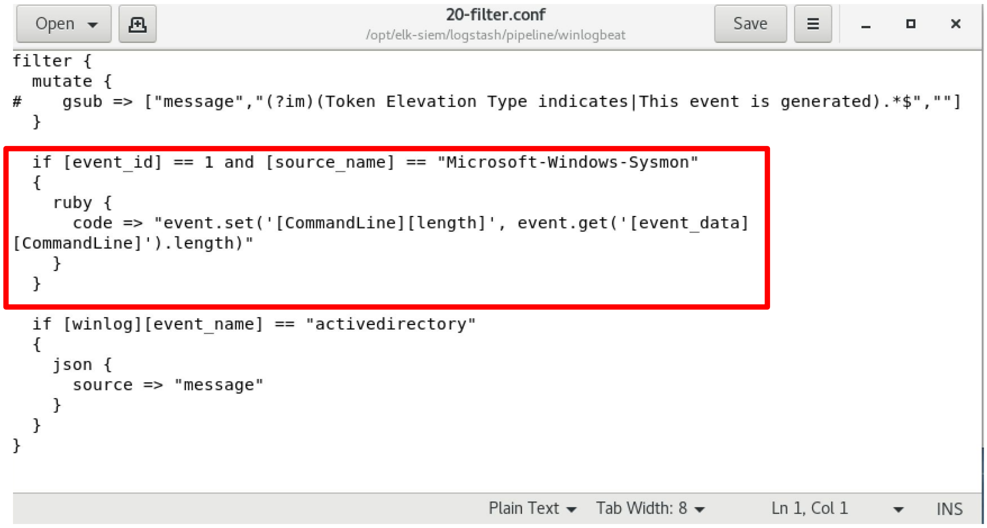
3



source_name	event_id	event_data.CommandLine
Microsoft-Windows-Sysmon	1	C:\Windows\system32\winsat.exe formal -log -cancelevent 6b0a3f63-52e5-4b66-a6e6-750191104e4d
Microsoft-Windows-Sysmon	1	C:\Windows\system32\mcbuilder.exe

1) Using the discover tab, find the event_data.CommandLine field in the sysmon index pattern.
2) Add a filter for event_id 1, which is sysmon process create event
3) Take note of the name of the field that contains the full command line, this will be used in our Logstash filter.

Add Ruby filter to winlogbeat pipeline in Logstash



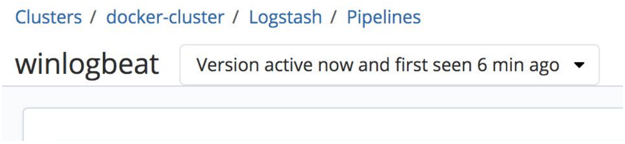
```
filter {
  mutate {
#    gsub => ["message","(?im)(Token Elevation Type indicates|This event is generated).*$",""]
  }

  if [event_id] == 1 and [source_name] == "Microsoft-Windows-Sysmon"
  {
    ruby {
      code => "event.set('[CommandLine][length]', event.get('[event_data]
[CommandLine]').length)"
    }
  }
  if [winlog][event_name] == "activedirectory"
  {
    json {
      source => "message"
    }
  }
}
```

1) On your CentOS machine open the Logstash winlogbeat filter in a text editor
   sudo vi /opt/elk-siem/logstash/pipeline/winlogbeat/20-filter.conf or
   sudo gedit /opt/elk-siem/logstash/pipeline/winlogbeat/20-filter.conf
2) Add the lines to the filter block to the file and save it. This uses Ruby in Logstash to measure the length of the event_data.CommandLine field from the Sysmon logs

```
if [event_id] == 1 and [source_name] == "Microsoft-Windows-Sysmon"
{
  ruby {
    code => "event.set('[CommandLine][length]',
event.get('[event_data][CommandLine]').length)"
   }
}
```

Verify the pipeline reloaded in Kibana

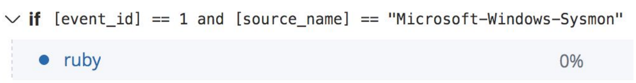
1



Clusters / docker-cluster / Logstash / Pipelines

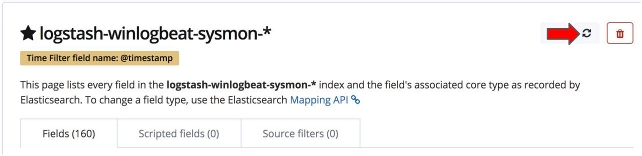
winlogbeat — Version active now and first seen 6 min ago

2



```
if [event_id] == 1 and [source_name] == "Microsoft-Windows-Sysmon"
  ● ruby                                                        0%
```

3



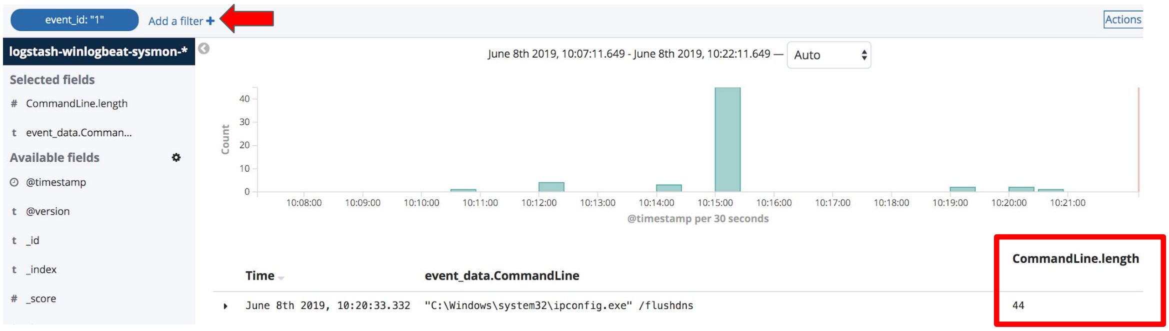
★ logstash-winlogbeat-sysmon-*

Time Filter field name: @timestamp

This page lists every field in the **logstash-winlogbeat-sysmon-*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API

1) In Kibana, verify the winlogbeat pipeline reloads and you can see the new filter
Click Monitoring > Pipelines under Logstash section > Click on the winlogbeat
2) The new Ruby filter should be visible in the pipeline. If the filter does not show up, check the syntax of the filter in the conf file /opt/elk-siem/logstash/pipeline/winlogbeat/20-filter.conf
3) Refresh the index pattern for the new field
Click Management > Index Patterns > refresh logstash-winlogbeat-sysmon-*

View the new field in Kibana



Time	event_data.CommandLine	CommandLine.length
June 8th 2019, 10:20:33.332	"C:\Windows\system32\ipconfig.exe" /flushdns	44

1) On the Discover tab add a filter for suspicious long command lines
   Add Filter > CommandLine.length > is > between 500
2) You can also use the Window DC to run commands to test the new field