Checklist for Extractor Validation

Pre-requisites:

- Linux system

- Dependencies of Extractor SDK

- Knowledge of Log Analysis

- Knowledge of Regular expression

|  |  |
| --- | --- |
| Peer review of <NameOfTheExtractor>.yml |  |
| Maker :                   \_\_\_\_\_\_\_\_\_\_  Checker   :              \_\_\_\_\_\_\_\_\_\_ |  |
| Section 1 - YAML Validation | Tick Mark  / |
| 1. All the basic device-related information populated appropriately |  |
| 1. Regex steps are minimum and the time taken to parse the data is minimum |  |
| 1. For master filter, a strict log source-specific regex is written |  |
| 1. First match is defined appropriately so that it annotates the Streams to the Log |  |
| 1. The Regex of all FMs are different if multiple FMs |  |
| 1. Decoder is regex OR custom OR JSON depending on the log format. |  |
| 1. Suitable decoder regex capturing all the important fields from the log event is written |  |
| 1. Most informative fields under the 'event-key-format' section are selected. (This will help in assigning the Stream properly) |  |
| 1. Check that all the potential events are mapped under the event key mapping section |  |
| 1. Check that all the Streams are mentioned as per Blueprint, and double-check the spelling |  |
| 1. Check that all the available actions can be referred from 'Stream-Action Extractor Mapping' on the Github page |  |
| 1. Check a fallback is defined for every first match section |  |
| 1. Check ‘globals’ defined for every first match section |  |
| 1. Check ‘Fallback’ section exists |  |
| Section 2 - Extractor Debugging | / |
| 1. Redme.txt of Extractor SDK is followed |  |
| 1. Once debugged, check all desired fields are being parsed as expected |  |
| 1. Check for all the Streams, Actions, and Status that are defined |  |
| 1. Check all the potential logs are streamed appropriately and all the non-potential logs are parsed under OTHER Stream |  |
| Section 3 - Console Testing | / |
| 1. Extractor is added on the console. |  |
| 2. 'Collection Status' page indicates successful application of extractor. |  |
| 3. On the 'Find' page, check whether all the logs of that particular extractor are parsing as desired. |  |
| Review Done Date:     \_\_\_\_\_\_\_\_\_\_  Sign off by Reviewer: \_\_\_\_\_\_\_\_\_\_\_ |  |