### Logpresso App

Based on a high-performance, schema-less big data engine, the Logpresso platform provides many features related to log collection, storage, detection, analysis, and visualization required for security operations. However, it takes a lot of effort to configure an actual operating environment using only the basic features.

Depending on the integration target, you may need to develop a dedicated collector, parse binary packets, or call a REST API to control the integration device. Even if you are able to fully configure your production environment using only basic platform features, you still need to write regular expressions, set up real-time or batch detection scenarios, or create dashboard widgets.

Instead of doing these tasks over and over again, Logpresso partners can develop fully packaged apps to maximize reusability. Logpresso apps provide the following features:

**Logpresso App Features**

|  |  |
| --- | --- |
| Item | Description |
| Log Schema | Define a set of standardized log field names. |
| Parser | Define a parser that parses logs to extract a standardized set of fields. |
| Logger model | Define a combination of ingestion types and normalization rules. |
| Dataset | Define a dataset to use as a data source in a dashboard widget or pivot. |
| Procedure | Define a parameterized query. |
| Report template | Define the report formatting. |
| Threat intelligence feed | Define a feed to automatically sync indicators from threat intelligence services. |
| Real-time detection scenario | Define a real-time detection scenario that detects in milliseconds. |
| Batch detection scenario | Define a batch detection scenario that runs at a specified interval. |
| Subnet group | Define the network subnets referenced by the detection scenario. |
| Port group | Define the port groups referenced by the detection scenario. |
| Pattern group | Define a group of patterns referenced by a detection scenario. |
| Response model | Define a response model that blocks or unblocks specified IP addresses from devices. |
| Widget | Define reusable widgets that visualize information in a dashboard. |
| Dashboard | Define the dashboards you need for threat detection or service monitoring. |
| Connect profile | Define the required connection properties. e.g. REST API endpoint or API key. |
| Query command | Define a custom query command. |
| Playbook | Define reusable playbooks. |

This means that you can install multiple Logpresso apps on the Logpresso platform and configure your production environment with minimal setup. In the following sections, we'll explain how Logpresso apps run on the Logpresso platform.