### ログプレッソ・ソナーアプリ

ログプレッソ・ソナープラットフォームは、高性能なスキーマレスビッグデータエンジンを基盤とし、セキュリティ運用に必要なログの収集、保存、検出、分析、可視化に関する多くの機能を提供します。しかし、基本機能のみを用いて実際の運用環境を構築するには多大な労力が必要となります。

連携対象によっては専用のロガーを開発する必要があり、バイナリパケットのパースが求められる場合や、連携機器を制御するためにREST APIを呼び出す必要がある場合もあります。たとえ基本プラットフォーム機能のみで運用環境を構築できたとしても、正規表現の作成や、ストリーム検出シナリオやバッチ検出シナリオの設定、ダッシュボードウィジェットの作成・配置などの作業が依然として必要です。

ログプレッソ・ソナーパートナーは、エンジニアがこれらの作業を繰り返し行う代わりに、完全にパッケージ化されたアプリを開発し、再利用性を最大化することができます。ログプレッソ・ソナーアプリは、以下の機能を提供します。

**ログプレッソ・ソナーアプリの機能**

|  |  |
| --- | --- |
| 項目 | 説明 |
| ログスキーマ | 標準化されたログフィールド名の集合を定義します。 |
| パーサー | ログをパースし、標準化されたフィールドセットを抽出するパーサーを定義します。 |
| ロガーモデル | 収集タイプと正規化ルールの組み合わせを定義します。 |
| データセット | ダッシュボードウィジェットやピボットでデータソースとして利用するデータセットを定義します。 |
| プロシージャ | パラメータ化されたクエリを定義します。 |
| レポート | レポート書式を定義します。 |
| 脅威インテリジェンスフィード | 外部インテリジェンスサービスのインジケーターを自動収集するフィードを定義します。 |
| ストリーム検出シナリオ | ミリ秒単位で検出を行うストリーム検出シナリオを定義します。 |
| バッチ検出シナリオ | 指定したインターバルで実行されるバッチ検出シナリオを定義します。 |
| サブネットグループ | 検出シナリオで参照するサブネットグループを定義します。 |
| ポートグループ | 検出シナリオで参照するポートグループを定義します。 |
| パターングループ | 検出シナリオで参照するパターングループを定義します。 |
| レスポンスターゲットモデル | 指定したIPアドレスを連携機器でブロックまたはブロック解除するレスポンスターゲットモデルを定義します。 |
| ウィジェット | ダッシュボードで情報を可視化する再利用可能なウィジェットを定義します。 |
| ダッシュボード | 複数のウィジェットを組み合わせ、脅威検出やサービスモニタリングに必要なダッシュボードを定義します。 |
| 接続プロファイル | REST APIアドレス、APIキーなどの接続設定を管理します。 |
| クエリコマンド | ユーザー定義クエリコマンドを拡張します。 |
| プレイブック | 再利用可能なプレイブックを定義します。 |

つまり、ログプレッソ・ソナープラットフォームに複数のログプレッソ・ソナーアプリをインストールすることで、最小限の設定で運用環境を構築することが可能です。次の章では、ログプレッソ・ソナーアプリがどのようにプラットフォーム上で動作するかについて説明します。