## ポリシー

ポリシー機能は、収集されたデータを分析し、定義されたポリシーに従って脅威を検出します。本セクションで説明するポリシー機能は以下の通りです。

* **[ストリームルール](section-stream-rule)**: リアルタイムで収集されたデータに対し、パターンや特定条件に基づく相関分析を行い、脅威を検出する機能です。
* **[バッチルール](section-batch-rule)**: 時間経過とともに発生する異なるイベントを相関させて脅威を検出する機能です。
* **[プレイブック](section-playbook)**: ストリームルールやバッチルールで検出された脅威に対し、自動的に対応を実施する機能です。

以下の機能は、リアルタイムおよびバッチ検出、セキュリティ運用、プレイブック実行に必要な脅威インテリジェンス、関連データ、資産情報の管理を可能にします。

* **[機械学習モデル](section-ml-model)**: ランダムフォレストやアイソレーションフォレストアルゴリズムを用いてデータを分析・学習し、データの予測や異常行動の識別・検出を行う機能です。
* **[脅威インテリジェンス](section-threat-intelligence)**: ログプレッソCTIやアプリケーションを通じて提供される脅威インテリジェンスの管理機能です。
* **[行動プロファイル](section-behavior-profile)**: 過去の行動を定期的にプロファイリングし、行動ベースの検出を可能にする機能です。
* **[学習データセット](section-ml-input)**: 機械学習モデルの学習用データを管理する機能です。
* **[サイト](section-site)**: セキュリティ監視対象となるサイトの管理機能です。
* **[資産IP](section-asset-ip)**: 脅威から保護すべき資産のIPアドレスを管理する機能です。
* **[アドレスグループ](section-address-group)**: ブロックや許可に利用できるIPアドレスグループの管理機能です。
* **[サブネットグループ](section-subnet-group)**: ブロックや許可に利用できるIPネットワークグループの管理機能です。
* **[ポートグループ](section-port-group)**: ブロックや許可に利用できるTCP/UDPサービスのポートグループ管理機能です。
* **[ユーザー定義フィルター](section-udf)**: ストリームルールやバッチルールで利用可能なフィルターの管理機能です。
* **[パターングループ](section-pattern-group)**: データ内で検索対象となるパターングループを定義する管理機能です。
* **[アラームグループ](section-alarm-group)**: ストリームルールやバッチルールによる脅威検出時にアラートを受信するアカウントの管理機能です。
* **[インジケーター](section-indicator)**: ユーザー定義の侵害指標（IoC）を管理する機能です。