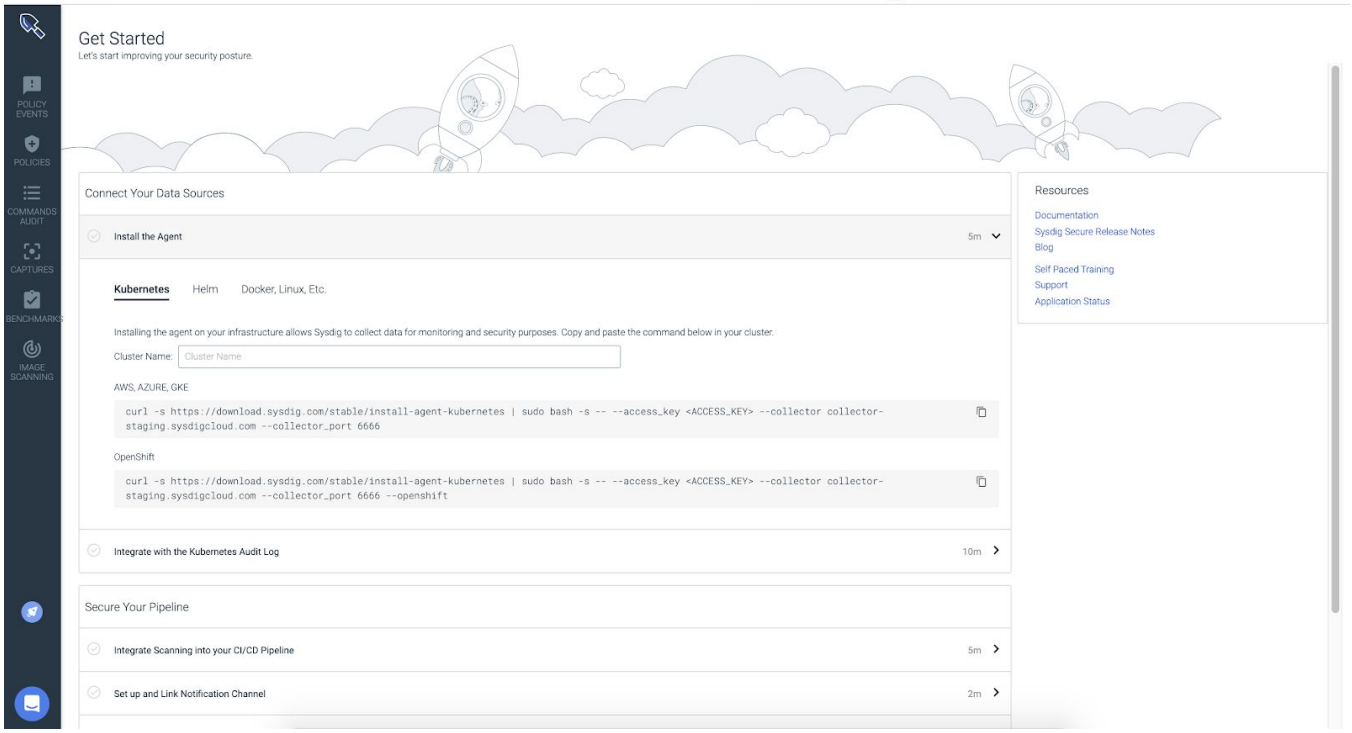
Sysdig Secure を始めましょう

本文の内容は、Sysdig Secureを始めましょうのドキュメント(https://docs.sysdig.com/en/getting-started-with-sysdig-secure.html）を元に日本語に翻訳・再構成した内容となっております。

Sysdig Secureを始めましょう

Get Started ページ（SaaS）

[Get Started]ページは、ユーザーがSysdig Secureを最大限活用できるようするための重要なステップを把握できるようにします。ユーザーがタスクを完了し、Sysdigが製品に新しい機能を追加すると、ページは新しい手順を案内する内容に更新されます。



[Get Started]ページは、各種情報のリンクページとしても活用いただけます。

- ドキュメント
- リリースノート
- Sysdigブログ
- セルフペーストレーニング
- サポート

ユーザーは、サイドメニューのロケットをクリックして、いつでも[Get Started]ページにアクセスできます。

データソースの接続

エージェントをインストールする

- インフラストラクチャにエージェントをインストールすると、Sysdigはモニタイングとセキュリティの目的でデータを収集を始めます

Kubernetes Auditログとの統合

- Kubernetes Auditログは、Kubernetes APIアクティビティを記録したセキュリティ関連の時系列のレコードセットを提供します。Kubernetes Auditログを解析することにより、ユーザーアクティビティ、機密性の高い内容の変更、権限の更新を追跡できます。APIログの処理と監査は、Kubernetes環境内での侵害の指標を追跡し、コンプライアンスコントロールを満たすための鍵となります。

あなたのパイプラインをセキュアにしましょう

あなたのCI/CDパイプラインにスキャニングを統合する

- CI/CDワーカーノード上でローカルでイメージの分析を可能とする、Sysdigセキュアインラインスキャナは、以下の利点を提供します。
    - イメージがレジストリにプッシュされる前に、イメージをスキャンしてシフトレフトを実現する
    - スキャンワークロードを並列化および分散する機能
    - 資格情報をSysdigのSaaSサービスに記録したり、分析のためにSysdigバックエンドにイメージを送信する必要もありません。

通知チャネルの設定とリンク

- Sysdig Secureはアラートを発行して、イベント、異常、または注意が必要なセキュリティインシデントのプロアクティブな通知を行います。アラートシステムは、通常の電子メール、Slack、クラウドプロバイダーの通知キュー、カスタムWebhookなど様々なプッシュゲートウェイを提供します。

リポジトリスキャンアラートのセットアップ

- スキャン結果をSysdigが提供する通知チャネルのいずれかと統合することにより、ユーザーはイメージ分析プロセスの出力に関するレポートをすぐに実行できます。リポジトリアラートは、レジストリ/リポジトリスコープに応じて異なるトリガー条件を使用してカスタマイズできます。

ランタイム環境の保護

ランタイムスキャンアラートのセットアップ

- ユーザーがセットアップできる最も実用的なアラートの1つは、既存のランタイムイメージが新しく発見された脆弱性の影響を受けているかどうかを検出することです。これらのアラートは、コンテナおよびKubernetesメタデータを使用して範囲を設定できるため、イメージがコンプライアンスから外れるとすぐに適切なチームに通知されます。

検出ルールの作成

- Sysdig Secureは、オープンソースプロジェクトであるFalcoの上に構築されたビヘイビア検出エンジンを活用して、異常なランタイムアクティビティを検出して対応できます。さらに、ユーザーは、基本ポリシーエンジンを使用して、プロセス実行、ファイルアクセス、およびネットワークアクティビティのホワイトリストベースのセキュリティルールを簡単に作成できます。

基本的なオンボーディング

このセクションでは、Sysdig Secure（オンプレミス）のオンボーディングの秘訣について説明します。

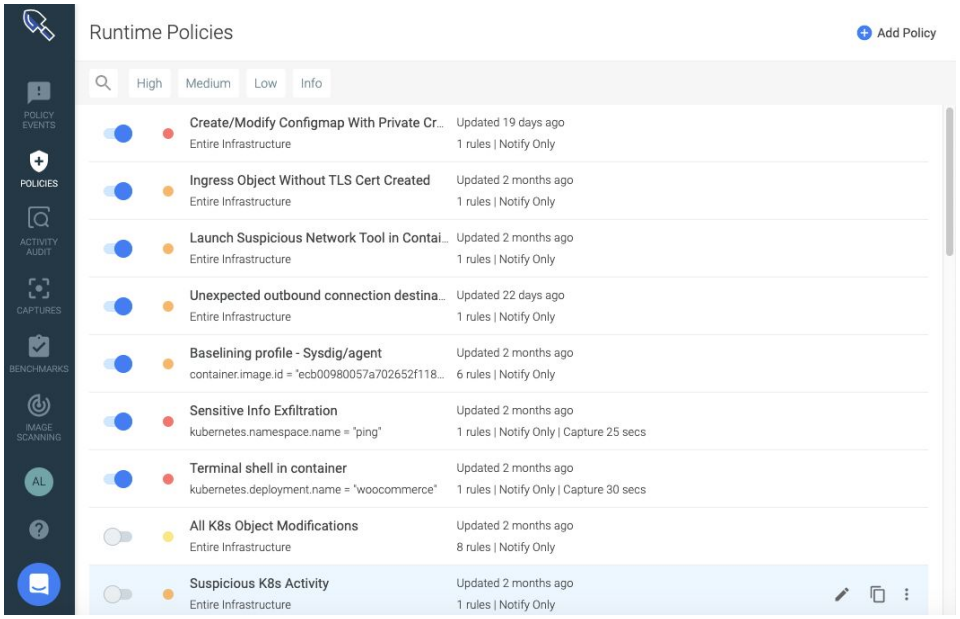
Sysdig Secureインターフェースへのアクセス

Sysdig Secureインターフェースにアクセスするには、 Welcome Wizardで、Sysdigエージェントをインストールし、コア管理ユーザーを作成する必要があります。インストール手順については、 エージェントインストールドキュメントをご参照ください。

注記
ユーザーを追加するには、Sysdig Secureまたは統合認証ツールのいずれかを使用して、ユーザー資格情報も定義する必要があります。ユーザー作成の詳細については、 ユーザーおよびチーム管理ドキュメントをご参照ください。

Sysdig Secureインターフェースの詳細

Sysdig Secure UIは、以下のモジュールで構成されています。



- ポリシーイベント
- ポリシー
- [ベータ]アクティビティ監査
- キャプチャ
- イメージスキャン
- ベンチマーク

ワークフローの好みや、Sysdig Secureの実装、もしくは、新規ユーザかの状況に応じていくつかのスタートポイントがあります。

- 新しいSysdig Secure環境の場合は、ポリシーモジュールに移動して、環境に必要なポリシーとルールの構成を開始します。
- 新しいSysdig Secureユーザーの場合、ポリシーイベントモジュールに移動して、環境の現在の状態を確認します。