sysdig

Sysdig Secure

本文の内容は、Sysdig Secure のドキュメント(https://docs.sysdig.com/en/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

Sysdig Secureは、Sysdigのコンテナインテリジェンスプラットフォームの一部です。Sysdigは、統合プラットフォームを使用して、コンテナおよびマイクロサービスに適したアーキテクチャでセキュリティ、監視、およびフォレンジックを提供します。Sysdig Secureは、ランタイムセキュリティとフォレンジックに対するサービス対応のアプローチを採用し、DockerとKubernetesの統合によりコンテナの詳細な可視性を統合して、脅威をより効果的にブロックします。

バックグラウンドでは、Sysdigエージェントは監視対象のホスト上に存在し、適切なデータとイベントを収集します。詳細については、Sysdig Agentのドキュメントを参照してください。

主な機能

- 関連するパフォーマンスとセキュリティデータを一緒に提示します。
- イメージスキャン、監査、およびランタイム脆弱性管理機能を提供します。
    - イメージ、クラスター、ネームスペース、ホスト、またはその他のラベルに対する脆弱性をフィルターおよび表面化します
    - スキャンされていないイメージまたは新しい脆弱性から評価ステータスが変更されたイメージに関するアラート
    - ユーザーアクション、コンテナアクティビティ、およびコマンドライン引数を記録する
    - セキュリティポリシーを適用し、攻撃をブロックする
- 分散環境のコンプライアンステストを提供します。
    - ホスト、サービス、またはクラスター全体で実行するカスタマイズされたベンチマークテストを簡単にスケジュール
    - 結果をSIEM、ロギングクラスター、または組織が使用するその他のツールにエクスポートします。
- ランタイム検出とデータ強化を提供します。
    - アプリケーション、コンテナ、ネットワークのアクティビティに基づいて、脅威をリアルタイムで特定してブロック
    - すべてのアプリ、コンテナ、ホスト、およびネットワークシステムコールを追跡するインストルメントカーネル

    - 組織化されたサービスに基づくセキュリティポリシー違反の表示
- インシデント対応とフォレンジックをサポートします。
    - 手動で設定を伴わない単一サービスポリシーで、分散サービス、動的サービス、エフェメラルなサービスを保護
    - ポリシー違反や悪意のある活動に対してアクションが取れるインシデント対応ができるように詳細なシステムキャプチャーを作成します。
    - ポリシー違反から攻撃前および攻撃後のアクティビティの100%粒度のキャプチャにドリルダウンできます。
    - SCAPファイルを表示して、セキュリティイベントの前、最中、後のすべてのシステムアクティビティを確認します。
    - アラートとインシデント対応を統合する