sysdig

【ベータ版】
コンプライアンス

本文の内容は、【ベータ版】コンプライアンスのドキュメント(https://docs.sysdig.com/en/compliance--beta-.html）2020年11月25日時点を元に日本語に翻訳・再構成した内容となっております。

[ベータ版]コンプライアンス

Sysdig Secure の コンプライアンス モジュールは、様々なコンプライアンス基準から選択されたコントロールをチェックするバリデータツールと、レポートを生成するツールで構成されています。最初のリリースでは、PCI 3.2の特定のコントロールに対するチェックを提供しています。今後のリリースでは、SOC2、NIST-800-53などが含まれる予定です。

バリデータは、イメージスキャンポリシー、Falcoランタイムポリシーとルール、スケジュールされたベンチマークテストなど、Sysdig Secureの多くの機能をチェックします。時間の経過とともに、新たなコンプライアンスカバレッジが追加されます。

免責事項：Sysdig は、物理的なセキュリティに関連するものなど、フレームワーク内のすべてのコントロールをチェックすることはできません。

注意事項

この機能はベータリリースです。Sysdig Secure 管理者は、Sysdig Labs インターフェースの [設定] からこの機能を有効にする必要があります。

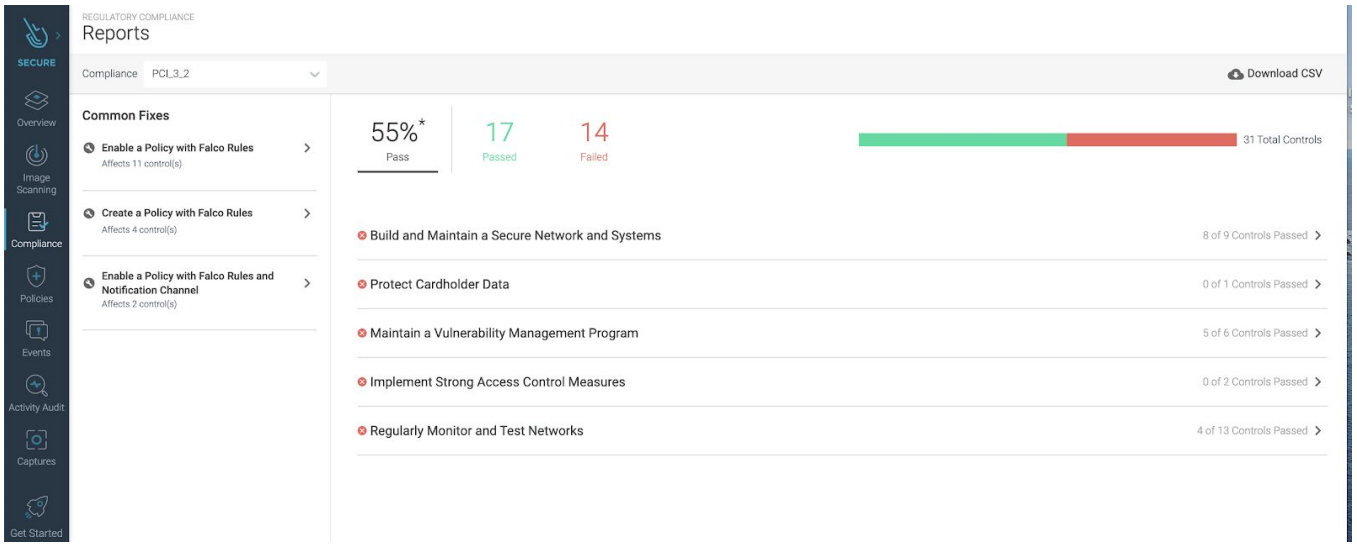
コンプライアンスレポートの使用

コンプライアンスモジュールにアクセスする

1. Sysdig Secure admin： `Settings > Sysdig Labs` で機能を有効にします。
2. 左側のナビゲーションにあるコンプライアンスアイコンをクリックします。

レポートのレビュー

コンプライアンスのページにアクセスすると、それぞれの標準コントロールがチェックされ、環境の現在の状態が常に表示されます。



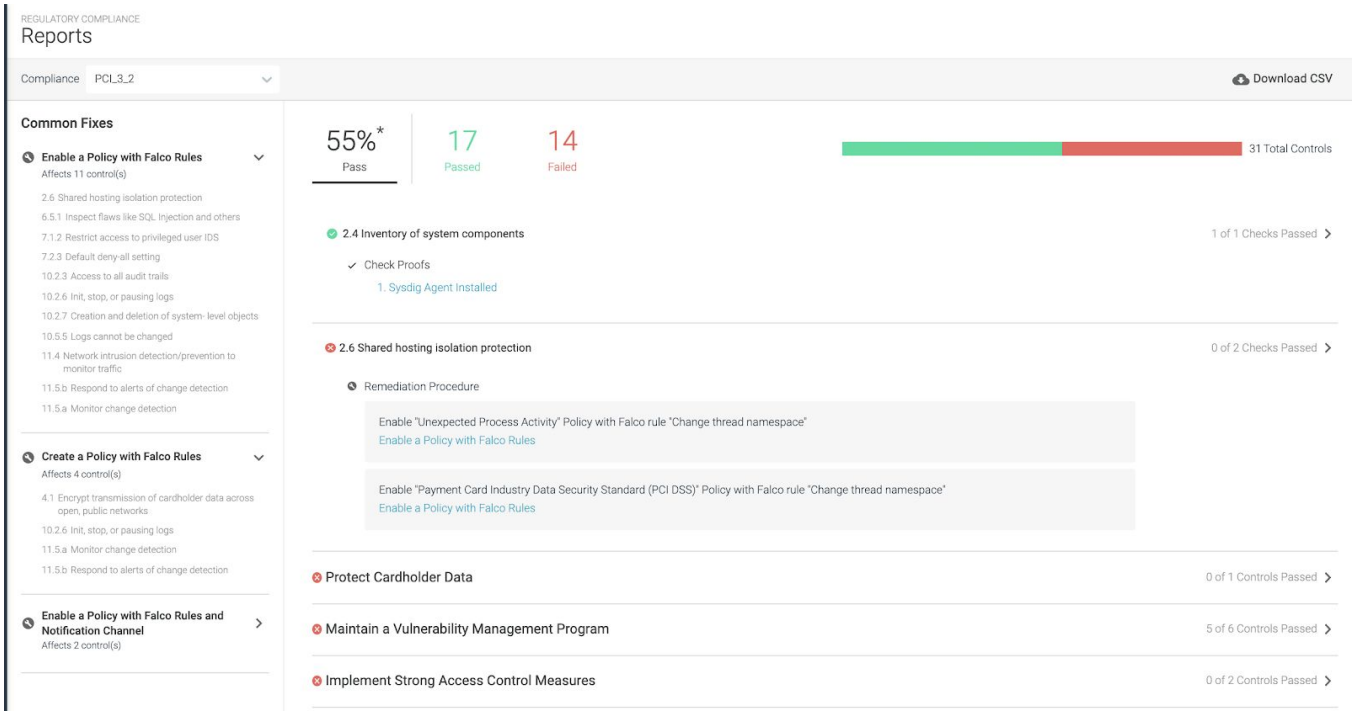
コンプライアンスレポートの概要

ページの一番上のセクションでは、Pass|Failのサマリーデータを使って、コンプライアンスレポートのサマリーを表示しています。

- **Pass %**：利用可能なすべてのチェックのうち、合格したチェックの総パーセンテージ
- **Passed**：Sysdigが検証できた実装されたコントロールの総数
- **Failed**：Sysdig が検証できなかったコントロールの総数
- **Unchecked**：Sysdigがチェックするように設定されているが、検証できないコントロールの総数（つまり、検証時にAPIが利用できない）。
- **Total Controles**：Sysdigがチェックするように設定されているコントロールの総数

コントロールレポートと一般的な修正

コントロールは、"コントロール・ファミリー"の折りたたみ可能なセクションの下にグループ化されています。



それらを開くと、それぞれのコントロールの説明とリンクが表示されます。

- **Proof**：コントロールの通過を許可した実装されたSysdig機能へのリンク、または
- **Remediation**：コントロール内のチェックを通過するために実装しなければならないSysdig機能へのリンク

Rationaleは、実装されたSysdig機能がコントロール内のチェックを通過する理由です。

左側の Common Fixes セクションでは、コントロールのチェックを通過するために Sysdig 機能を有効にするためのリンクをまとめています。

リファレンス：PCIコントロールの実装

PCIクイックリファレンスでは、PCI 3.2監査に合格するために必要なコントロールの全範囲について説明しています。このリリースでは、Sysdig Secure は以下のサブセットをチェックします。

1.1.2　現在のネットワーク図
1.1.3　ダイアグラムデータフロー
1.1.6.b 安全でないサービス、プロトコル、および許可されたポートを特定する
2.2　構成標準：CIS、ISO、SANS、NIST
2.2.1　サーバーごとに1つの機能を分離
2.2.2　必要なサービス、プロトコル、デーモンのみを有効にする
2.2.a　システム構成標準
2.4　システムコンポーネントのインベントリ
2.6　共有ホスティングの分離保護
4.1　オープンでパブリックなネットワークを介したカード会員データの暗号化送信
6.1　ランク付けでセキュリティ脆弱性を特定する
6.2　ベンダーセキュリティパッチのインストール
6.4.2　開発・テスト・プロダクションの分離
6.5.1　SQLインジェクションなどの欠陥を検査する
6.5.6　高リスクの脆弱性
6.5.8　不適切なアクセス制御

7.1.2　特権ユーザー IDS へのアクセスを制限する
7.2.3　デフォルトの全否定設定
10.1　個々のユーザーへのアクセスをリンクさせるための監査証跡の導入
10.2　イベントを再構築するための自動監査証跡の実装
10.2.1 カード会員データへのすべての個人ユーザーのアクセス
10.2.2 ルート権限または管理者権限を持つ個人によって行われたすべてのアクション
10.2.3 すべての監査証跡へのアクセス
10.2.6 ログの起動、停止、一時停止
10.2.7 システムレベルのオブジェクトの作成と削除
10.3　イベントの監査証跡を記録する
10.5.5 ログの変更ができない
10.6.1 すべてのセキュリティイベントの毎日のレビュー
11.4　トラフィックを監視するためのネットワーク侵入検知/予防
11.5.a 変更検出を監視
11.5.b　変更検出のアラートへの対応