Azure Security Center を使用してセキュリティ脅威から保護する

100 XP

6 分

Tailwind Traders は、Azure サービスの使用範囲を広げています。 現在もオンプレミスのワークロードがあり、セキュリティ関連の構成に関する最新のベスト プラクティスと業務手続きを適用しています。 自社のすべてのシステムが最小限のセキュリティ レベルを満たし、自社の情報が攻撃から保護されるようにするには、どうすればよいでしょうか。

多くの Azure サービスにはセキュリティ機能が組み込まれています。 また、Azure には、Tailwind Traders がこの要件に対応するために使用できるツールも用意されています。 まず、Azure Security Center について説明します。

Azure Security Center とは

Azure Security Center は、Azure とオンプレミスの両方ですべてのサービスにわたってセキュリティ体制を可視化できる監視サービスです。 セキュリティ体制 という用語は、サイバーセキュリティのポリシーと制御、およびセキュリティ脅威の予測、回避、対応方法を指しています。

Security Center には次の機能があります。

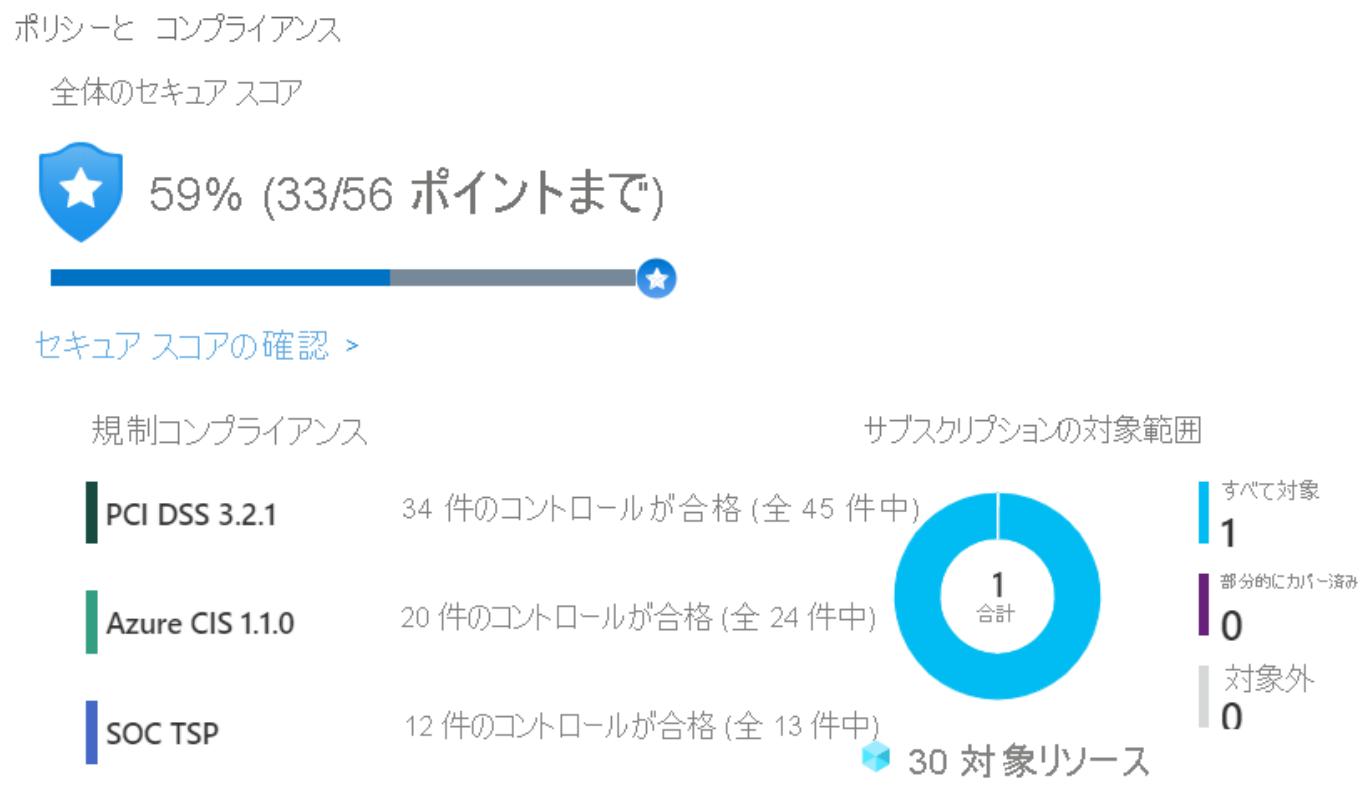
- オンプレミスおよびクラウドのワークロード全体のセキュリティ設定を監視する。
- 新しいリソースがオンラインになったときに必要なセキュリティ設定を自動的に適用する。
- 現在の構成、リソース、ネットワークに基づいてセキュリティの推奨事項を提供する。
- リソースを継続的に監視し、自動的なセキュリティ評価を実行して、潜在的な脆弱性を悪用される前に特定する。
- 機械学習を使用して、マルウェアが仮想マシン (VM) やその他のリソースにインストールされる前に検出してブロックする。 また、適応型アプリケーション制御 を使用して、許可されたアプリケーションを列挙するルールを定義し、許可するアプリケーションのみを実行できるようにすることもできる。
- 受信攻撃の可能性を検出して分析し、脅威および発生した可能性がある侵害後のアクティビティを調査する。
- ネットワーク ポートの Just-In-Time アクセス制御を提供する。 これにより、必要な場合に必要なトラフィックのみがネットワークで許可されるようになり、攻撃対象の領域が減る。

この短いビデオでは、Security Center が、ネットワークの強化、クラウド リソースのセキュリティ保護と監視、および全体的なセキュリティ体制の向上にどのように役立つかについて説明します。

セキュリティ態勢を理解する

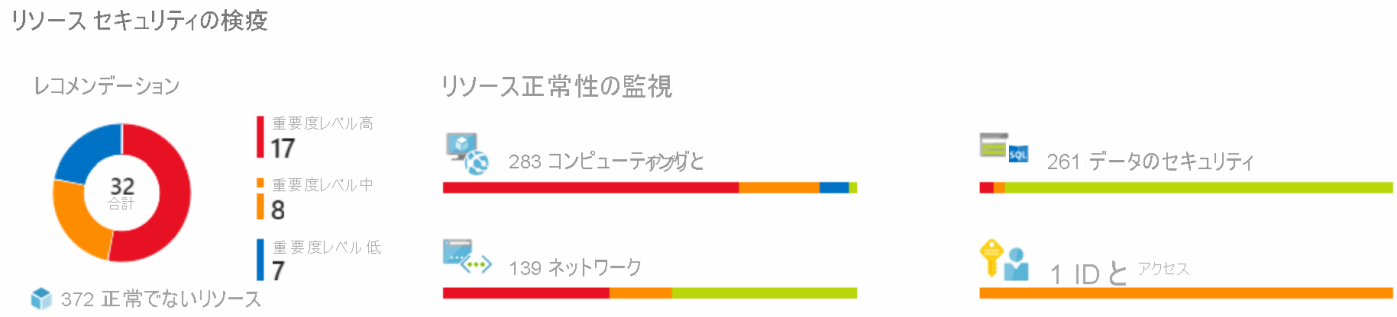
Tailwind Traders は、Security Center を使用して環境内のさまざまなコンポーネントの詳しい分析を取得できます。 割り当てられているすべてのガバナンス ポリシーのセキュリティ制御に照らして自社のリソースが分析されるため、規制コンプライアンス全体をセキュリティの観点からすべて 1 か所で確認できます。

次に示す Azure Security Center に表示される内容の例をご覧ください。



たとえば、Tailwind Traders は Payment Card Industry Data Security Standard (PCI DSS) に準拠している必要があります。 このレポートは、修復が必要な自社のリソースがあることを示しています。

[リソース セキュリティの検疫] セクションでは、Tailwind Traders はセキュリティの観点から自社のリソースの正常性を確認できます。 修復アクションの優先順位を付けやすくするため、推奨事項が低、中、高に分類されています。 次に例を示します。



セキュリティ スコアとは

セキュリティ スコアは、組織のセキュリティ体制の測定値です。

セキュリティ スコアは、セキュリティ制御 (関連するセキュリティの推奨事項のグループ) に基づいています。 スコアは、適用しているセキュリティ制御の割合に基づいて計算されます。 適用するセキュリティ制御が多いほど、受け取るスコアが大きくなります。 制御内の 1 つのリソースに対するすべての推奨事項を修復すると、スコアが向上します。

57% のスコア (60 ポイント中 34 ポイント) が表示された Azure portal の例を次に示します。

セキュリティ スコアの推奨事項に従うことは、組織を脅威から保護するのに役立ちます。 組織は、Azure Security Center の集中型ダッシュボードから ID、データ、アプリ、デバイス、インフラストラクチャなどの自社の Azure リソースのセキュリティを監視し、操作できます。

セキュリティ スコアを使用して、次のことができます。

- 組織のセキュリティ体制の現状について報告する。
- 検出可能性、可視性、ガイダンス、制御の提供によってセキュリティ体制を向上させる。
- ベンチマークと比較して主要業績評価指標 (KPI) を確立する。

脅威からの保護

Security Center には、VM、ネットワーク セキュリティ、ファイルの整合性に対応する高度なクラウド防御機能が含まれています。 これらの機能が Tailwind Traders にどのように適用されるかを見てみましょう。

- **Just In Time VM アクセス**

  Tailwind Traders は、VM への Just-In-Time アクセスを構成します。 このアクセスにより、VM の特定のネットワーク ポートへのトラフィックは既定でブロックされますが、管理者が要求および承認したときに指定された期間だけ許可されます。

- **アダプティブ アプリケーション制御**

  Tailwind Traders は、自社の VM で実行できるアプリケーションを制御することができます。 Security Center では、バックグラウンドで機械学習を使用して、VM で実行されているプロセスを確認します。 VM を保持するリソース グループごとに例外規則が作成され、推奨事項が示されます。 このプロセスでは、自社の VM 上で実行されている未承認のアプリケーションに関して通知するアラートが提供されます。

- **アダプティブ ネットワークのセキュリティ強化機能**

  Security Center では、VM のインターネット トラフィック パターンを監視し、それらのパターンを自社の現在のネットワーク セキュリティ グループ (NSG) 設定と比較することができ

ます。 その後、Security Center を使用して、NSG をさらにロック ダウンするかどうかについての推奨事項と、修復の手順を提供できます。

- **ファイルの整合性の監視**

  Tailwind Traders は、Windows および Linux の重要なファイル、レジストリ設定、アプリケーションへの変更、およびセキュリティ攻撃の兆候となるその他の側面の監視を構成することもできます。

セキュリティの警告への対応

Tailwind Traders は、Security Center を使用してすべてのセキュリティ アラートを一元的に表示できます。 その後、間違ったアラートの破棄、アラートの詳しい調査、アラートの手動修復、または ワークフローの自動化 による自動応答を行うことができます。

ワークフローの自動化では、Azure Logic Apps と Security Center コネクタが使用されます。 ロジック アプリは、脅威検出アラート、または名前や重大度によってフィルター処理された Security Center の推奨事項によってトリガーできます。 その後、メールの送信や Microsoft Teams チャネルへのメッセージ投稿などのアクションを実行するようにロジック アプリを構成できます。