Azure Sentinel を使用したセキュリティ脅威の検出と対応

100 XP

4 分

大規模な環境のセキュリティ管理には、専用のセキュリティ情報およびイベント管理 (SIEM) システムを使用すると便利です。 SIEM システムでは、さまざまなソースから (それらのソースでオープン標準のログ形式がサポートされている場合に) セキュリティ データが集計されます。 脅威の検出と対応に必要な追加機能も提供されます。

Azure Sentinel は、Microsoft のクラウドベースの SIEM システムです。 インテリジェントなセキュリティ分析と脅威分析が使用されます。

Azure Sentinel の機能

Azure Sentinel を使用して、次のことができます。

- **大規模なクラウド データの収集**

  オンプレミスと複数のクラウドの両方から、すべてのユーザー、デバイス、アプリケーション、インフラストラクチャのデータを収集します。

- **以前に検出されなかった脅威の検出**

  Microsoft の包括的な分析と脅威インテリジェンスを使用して、誤検知を最小限に抑えます。

- **人工知能による脅威の調査**

  Microsoft の長年にわたるサイバーセキュリティ経験を活用して、疑わしいアクティビティを大規模に調査します。

- **インシデントへの迅速な対応**

  一般的なタスクの組み込みオーケストレーションと自動化を使用します。

データ ソースを接続する

Tailwind Traders は、Azure Sentinel の機能を調査することにしました。 まず、自社のデータ ソースを識別して接続します。

Azure Sentinel では、セキュリティ イベントの分析に使用できるさまざまなデータ ソースがサポートされています。 これらの接続は、組み込みのコネクタまたは業界標準のログ形式と API によって処理されます。

- **Microsoft ソリューションへの接続**

コネクタによって、Microsoft Threat Protection ソリューション、Microsoft 365 ソース (Office 365 を含む)、Azure Active Directory、Windows Defender ファイアウォールなどのサービスがリアルタイムで統合されます。

- **その他のサービスおよびアプリケーションへの接続**

  コネクタは、AWS CloudTrail、Citrix Analytics (セキュリティ)、Sophos XG Firewall、VMware Carbon Black Cloud、Okta SSO など、Microsoft 以外の一般的なサービスやソリューションに対して用意されています。

- **業界標準のデータ ソースへの接続**

  Azure Sentinel では、Common Event Format (CEF) メッセージング標準、Syslog、または REST API を使用する他のソースからのデータがサポートされています。

脅威を検出する

Tailwind Traders は疑わしいイベントが発生したときに通知を受け取る必要があります。 組み込みの分析とカスタム ルールの両方を使用して脅威を検出することにしました。

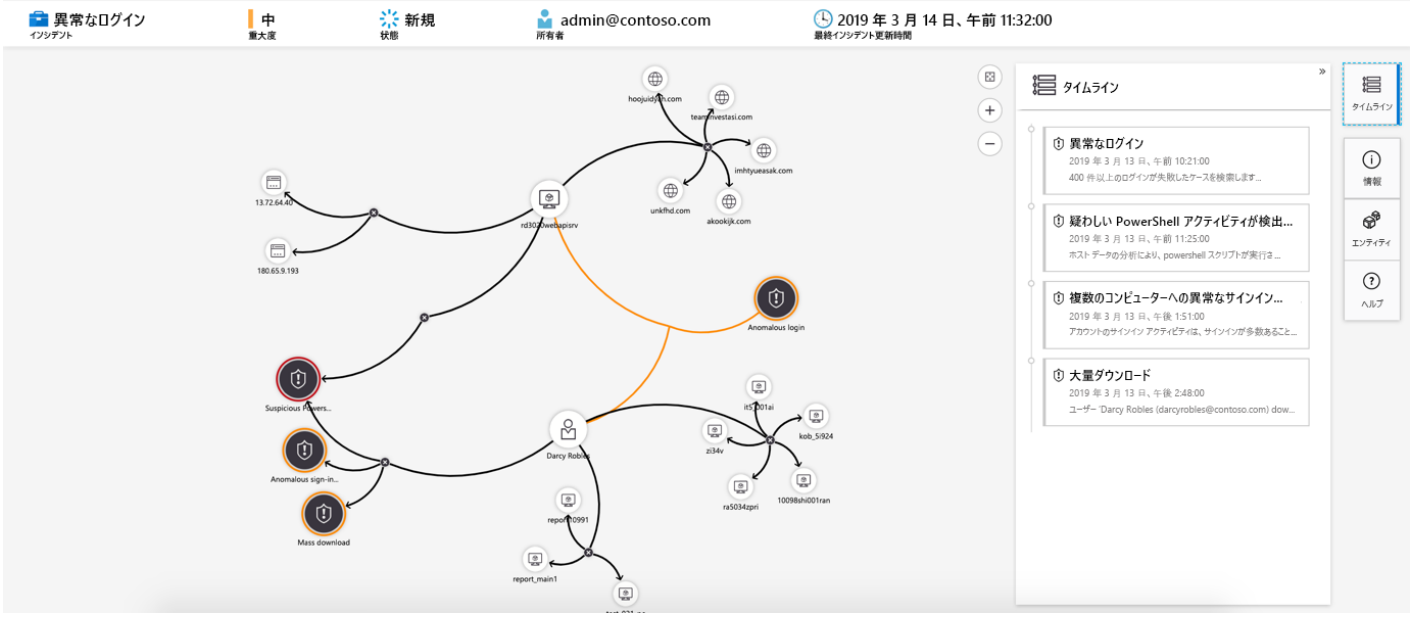
組み込みの分析 では、Microsoft のセキュリティ専門家とアナリストのチームが既知の脅威、一般的な攻撃ベクトル、疑わしいアクティビティのエスカレーション チェーンに基づいて設計したテンプレートが使用されます。 これらのテンプレートをカスタマイズして、環境全体で疑わしいと思われるアクティビティを検索できます。 一部のテンプレートでは、Microsoft の独自のアルゴリズムに基づく機械学習の行動分析が使用されています。

カスタム分析 は、環境内で特定の条件を検索するために作成するルールです。 クエリによって生成される結果の数を (過去のログ イベントに基づいて) プレビューしたり、クエリの実行スケジュールを設定したりできます。 アラートのしきい値も設定できます。

調査と対応

Azure Sentinel で疑わしいイベントが検出されたときに、Tailwind Traders は特定のアラートまたは インシデント (関連するアラートのグループ) を調査できます。 調査グラフを使用して、アラートに直接関係するエンティティの情報を確認したり、調査の指針となる一般的な探索クエリを確認したりできます。

次の例は、Azure Sentinel で調査グラフがどのように表示されるかを示したものです。



さらに、Azure Monitor ブックを使用して脅威への対応を自動化します。 たとえば、ネットワークにアクセスする悪意のある IP アドレスを検出するアラートを設定して、次の手順を実行するブックを作成することができます。

1. アラートがトリガーされたら、IT チケット発行システムでチケットを開きます。
2. セキュリティ アナリストがインシデントを把握していることを確認するため、Microsoft Teams または Slack のセキュリティ操作チャネルにメッセージを送信します。
3. アラートに含まれているすべての情報を、上級ネットワーク管理者とセキュリティ管理者に送信します。メール メッセージには、次の 2 つのユーザー オプション ボタンが含まれています: **[ブロック]** または **[無視]**。

管理者が **[ブロック]** を選択した場合は、ファイアウォールで IP アドレスがブロックされ、Azure Active Directory でそのユーザーが無効になります。 管理者が **[無視]** を選択した場合は、Azure Sentinel でアラートが閉じられ、IT チケット発行システムでインシデントが閉じられます。

管理者からの応答を受信した後、ブックの実行が継続されます。

ブックは、ルールによってアラートがトリガーされたときに、手動または自動で実行できます。