

Microsoftインテリジェントセキュリティアソシエーションメンバー

**SynackのMicrosoft Sentinelとのインテグレーションで脆弱性への対応が加速する**

# 概要

Microsoft Sentinelは、インテリジェント脅威アナリティクス、イベント管理、脅威の検出、脅威の可視化、プロアクティブハンティング、および脅威への対応を実施するための、クラウドネイティブでスケーラブルな単一ソリューションです。このソリューションによって、早期に脅威を検出し、高度な攻撃に対する迅速な対応が可能になり、その結果、問題解決までの時間が短縮され、Microsoft Azureのセキュリティインシデントを減らすことができます。また、SynackはMicrosoft Sentinelと直接連携し、Synackの脆弱性テストのデータからMicrosoft Sentinelのインシデントを自動的に作成する事で、修復及び解決時間の更なる短縮を支援します。

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | • Synackの脆弱性テスト結果をMicrosoft Sentinelに同期させてMicrosoft Azureの保護を支援する• 新たに発見した脆弱性から自動的にMicrosoft Sentinelインシデントが作成されるので、迅速な分析と修復を可能にする | • インテグレーションと構成が簡単なので迅速に利用を開始できる• 見慣れたMicrosoft Sentinel画面にインシデントを表示して管理する |
|  |  |  |

# SynackとMicrosoft Sentinelが連携して解決までの時間を短縮する

Microsoft Sentinelには、SEIM（Security Information and Event Management：セキュリティ情報とイベントの管理）とSOAR（Security Orchestration Automated Response：セキュリティ統合自動対応）の2つのセキュリティ技術が1つのソリューションに統合されています。Microsoft Sentinelは、インテリジェントセキュリティアナリティクスと脅威インテリジェンスを使用して、全社のさまざまのデータを取り込んで関連付けます。全社からさまざまなデータを取り込み、データの相関関係を明らかにして、高度なセキュリティ分析と脅威インテリジェンスに活用する事ができます。

• リアルタイムでアラートを受信する

• 機械学習とAIで脅威を検出、分析、特定し、インシデントを解決する

• プロアクティブハンティングを実施する

これにより、セキュリティチームはセキュリティ関連イベントをエンドツーエンドで確認できるようになります。また、セキュリティチームが直接的な洞察を得て一か所ですべての機能の分析が可能になります。Microsoft Sentinelはそれ自身でクラウドに発生し得る脅威を探索して対処することができますが、ユーザーにアラートで通知することもできます。

 悪用可能な脆弱性を迅速に管理して修復することは、クラウドへの脅威を最小化するための重要な要素です。Synackは世界で最も高い技術力と信頼のあるクラウドソースペネトレーションテストチームと独自のAI技術を保有し、継続的あるいはポイントインタイムでの脆弱性探査を実施します。SynackのMicrosoft Sentinelソリューションは、これらの探査結果をMicrosoft Sentinelに同期することによって、解決までに要する時間を短縮します。

SynackのMicrosoft Sentinelソリューションは、脆弱性データをSynackアカウントからMicrosoft Sentinelへ同期するデータコネクターを提供します。データコネクターは各脆弱性についてMicrosoft Sentinel内にインシデントを作成し、脆弱性の直近の変化に応じてインシデントデータを最新の状態に保ちます。Microsoft Sentinelに脆弱性情報を送るために、人を介在させる必要はありません。Microsoft SentinelはSynackの情報を利用してインシデントの脅威分析と処理を実施します。さらに、これらすべてを使い慣れたMicrosoft Sentinel環境で管理できます。

|  |  |
| --- | --- |
| 簡単なインテグレーションデータの同期は、Microsoft Azure FunctionがSynackとMicrosoft SentinelのAPIを使用してSynackデータをMicrosoft Sentinelに転送することによって実施されます。SynackのMicrosoft SentinelソリューションはVisual StudioマーケットプレースのMicrosoft Azureポータルから入手できます。Microsoft Sentinelデータコレクターをインストールすると、すぐに同期が開始します。Microsoft AzureやSynackポータルでの設定は必要ありません。データコネクターのデプロイの過程ですべてのパラメーターを正しく入力すると、Synackの脆弱性からの新しいインシデントの作成が開始している様子がMicrosoft Sentinel上で確認できます。デプロイされたMicrosoft Azure Function機能のログを確認することもできます。 | 顧客資産 - Azure顧客資産 - WorldMicrosoft Defender for CloudSynack脆弱性ブックSYNACKSmartScanRead Teamカスタムエンドポイント脆弱性データSynack脆弱性を表示しているMicrosoft Sentinelインシデント画面 |
| 各Synack脆弱性からMicrosoft Sentinelで新しいインシデントが作成されます。各Synackフィールドの値がMicrosoft Azureインシデントのフィールド記述として書き込まれます。Synack脆弱性の状態が変化すると、対応するMicrosoft Sentinelインシデントの状態が次の同期で更新されます。Microsoft Sentinelのインシデントには3つの状態（New（新規）、Active（アクティブ）、Closed（クローズド））があります。Microsoft Sentinelのこれら3つの状態は固定されていて設定変更はできません。Synackでは任意の数の状態を持たせることができます。ただし、それぞれの状態は3つのメジャーカテゴリー（New（新規）、Active（アクティブ）、Closed（クローズド））に属します。 |