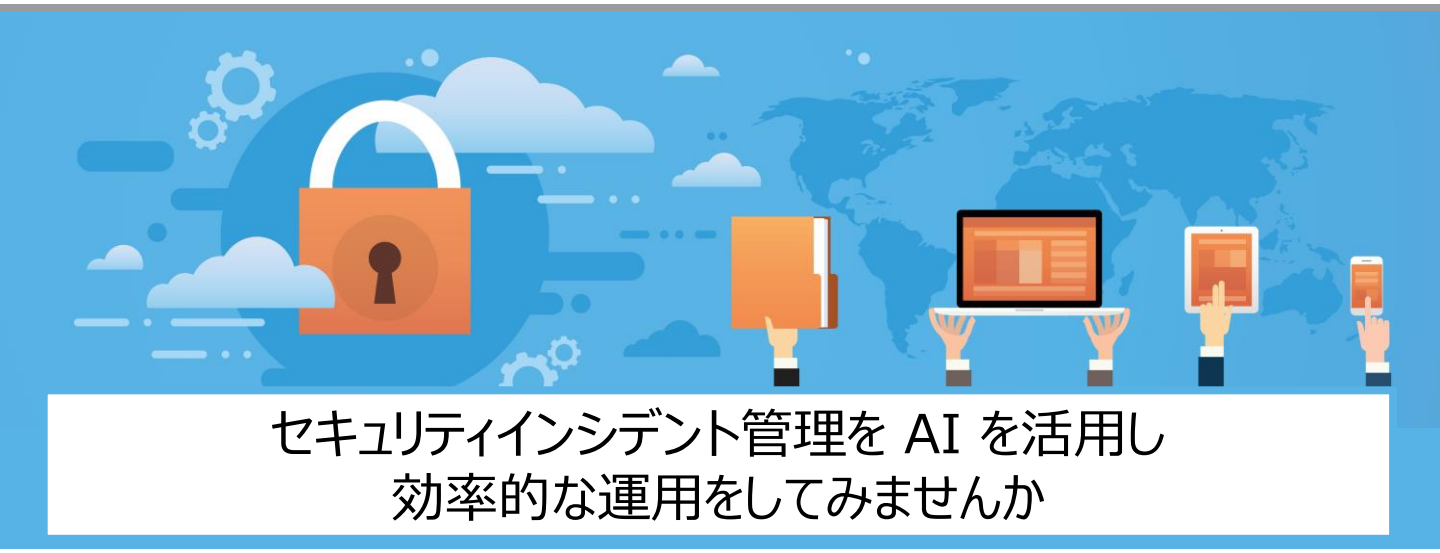
パーソル クロステクノロジー



セキュリティインシデント管理を AI を活用し 効率的な運用をしてみませんか

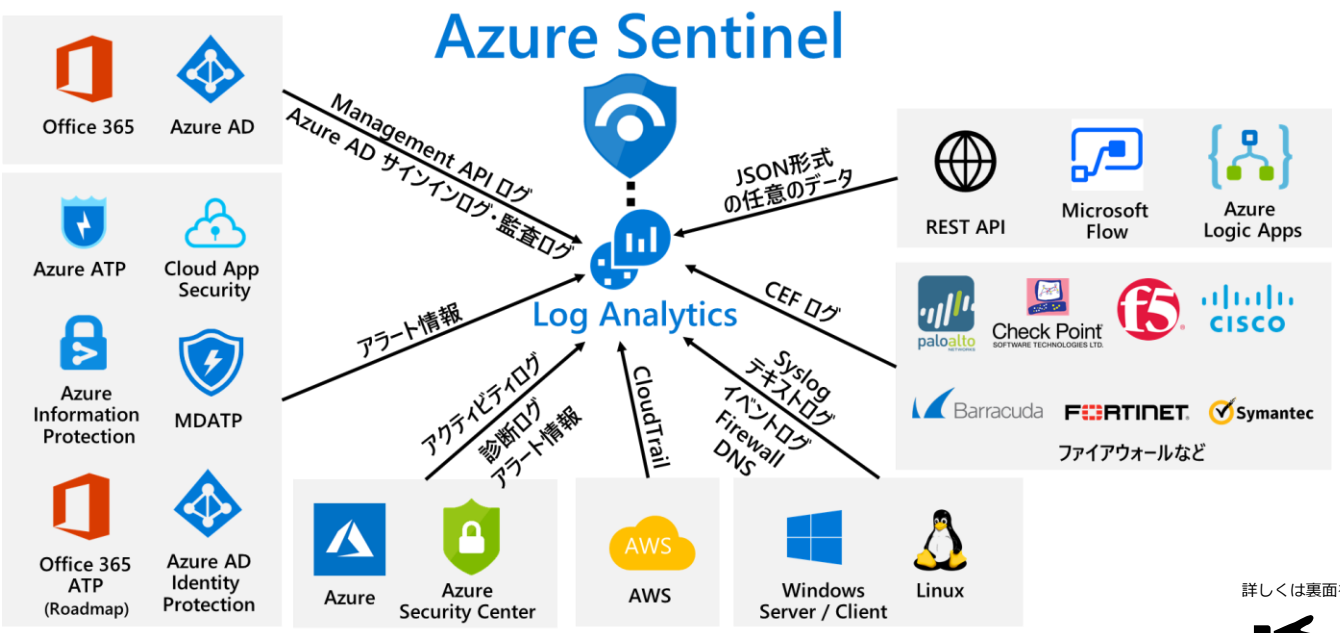
Microsoft Azure Sentinel は、スケーラブルでクラウドネイティブ型の**セキュリティ情報イベント管理 (SIEM)** および**セキュリティ オーケストレーション自動応答 (SOAR)** ソリューションです。Azure Sentinel は、高度なセキュリティ分析と脅威インテリジェンスを企業全体で実現し、アラートの検出、脅威の可視性、予防的な捜索、および脅威への対応のための 1 つのソリューションを提供します。

収集
オンプレミスと複数のクラウド内の両方で、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にわたって、クラウド規模でデータを収集します。

検出
Microsoft の分析と類を見ない脅威インテリジェンスを使用して、以前に発見された脅威を検出し、擬陽性を最小限に抑えます。

調査
Microsoft での数十年にわたるサイバーセキュリティの実績を活用しながら、AI を使用して脅威を調査して、疑わしいアクティビティを大規模に検出します。

応答
一般的なタスクの組み込みのオーケストレーションと自動化を使用して、インシデントに迅速に対応します。



詳しくは裏面を

サービス紹介

Azure Sentinel ワークショップ

Azure Sentinel のご紹介

Azure Sentinel の基本的な機能をご説明し、Sentinel の優位性やできることをはじめにご理解いただきます。

初期設定支援

利用開始に必要なオンボーディングの設定をご支援いたします。オンボーディングの後は分析方法のご紹介などを行います。

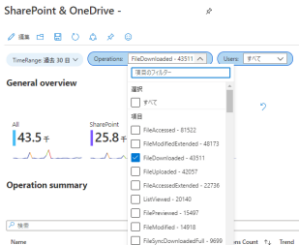
ワークショップシナリオ例

サーバーログのセキュリティイベント分析

サービス内容	セキュリティイベント分析
想定シナリオ	1. VM 内のセキュリティイベントの可視化や調査 2. インシデントの可視化と分析

不審なアクティビティの分析

サービス内容	Microsoft365 ユーザーアクティビティ分析
想定シナリオ	1. Microsoft 365 利用状況の可視化（MCASにて異常振る舞い検出[短時間での大量DL]） 2. 特定のアクティビティを分析



[諸条件・注意事項]

1. 本ワークショップには Microsoft Azure の環境が必要となります。実施の際は、お客様に Azure 環境をご用意いただくことになります。Azure 環境をお持ちでない場合は別途ご相談ください。
2. サーバー OS およびネットワーク機器のログ分析を希望される場合、お客様環境にログ転送用のサーバをご用意いただく必要がございます。また、分析対象のサーバ OS に Agent のインストールが必要となります。

当社の特徴

アワード受賞パートナー

2020 年 7 月に MS パートナーの中より Security & Compliance アワードを受賞したクラウド セキュリティ トップ パートナーです。Microsoft 365 を中心にクラウドセキュリティ対策にコミットしたチームが対応を行っております。

お問い合わせはこちら ～お気軽にお問い合わせください～

パーソルクロステクノロジー株式会社
本社：〒135-0061 東京都江東区豊洲3-2-20 豊洲フロント7F
Mail: cloud-sales@cloudsteady.jp Web: https://cloudsteady.jp/