

センチネル (sentinel)

- 歩哨、前哨、監視員、番人、見張り
- 番兵 - コンピュータ用語でデータの終了を示すデータのこともそう呼ぶ。

Azure Sentinelとは？

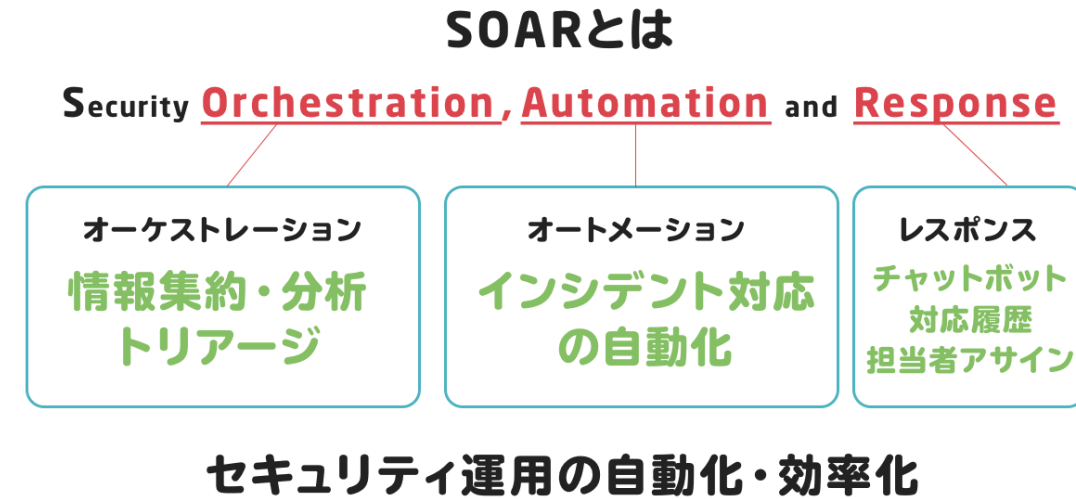
- Microsoft Azure Sentinel は、スケーラブルでクラウドネイティブ型の **セキュリティ情報イベント管理 (SIEM)** および **セキュリティ オークストレーション自動応答 (SOAR)** ソリューションです。
- Azure Sentinel は、高度なセキュリティ分析と脅威インテリジェンスを企業全体で実現し、アラートの検出、脅威の可視性、予防的な搜索、および脅威への対応のための 1 つのソリューションを提供します。

SIEMとは？

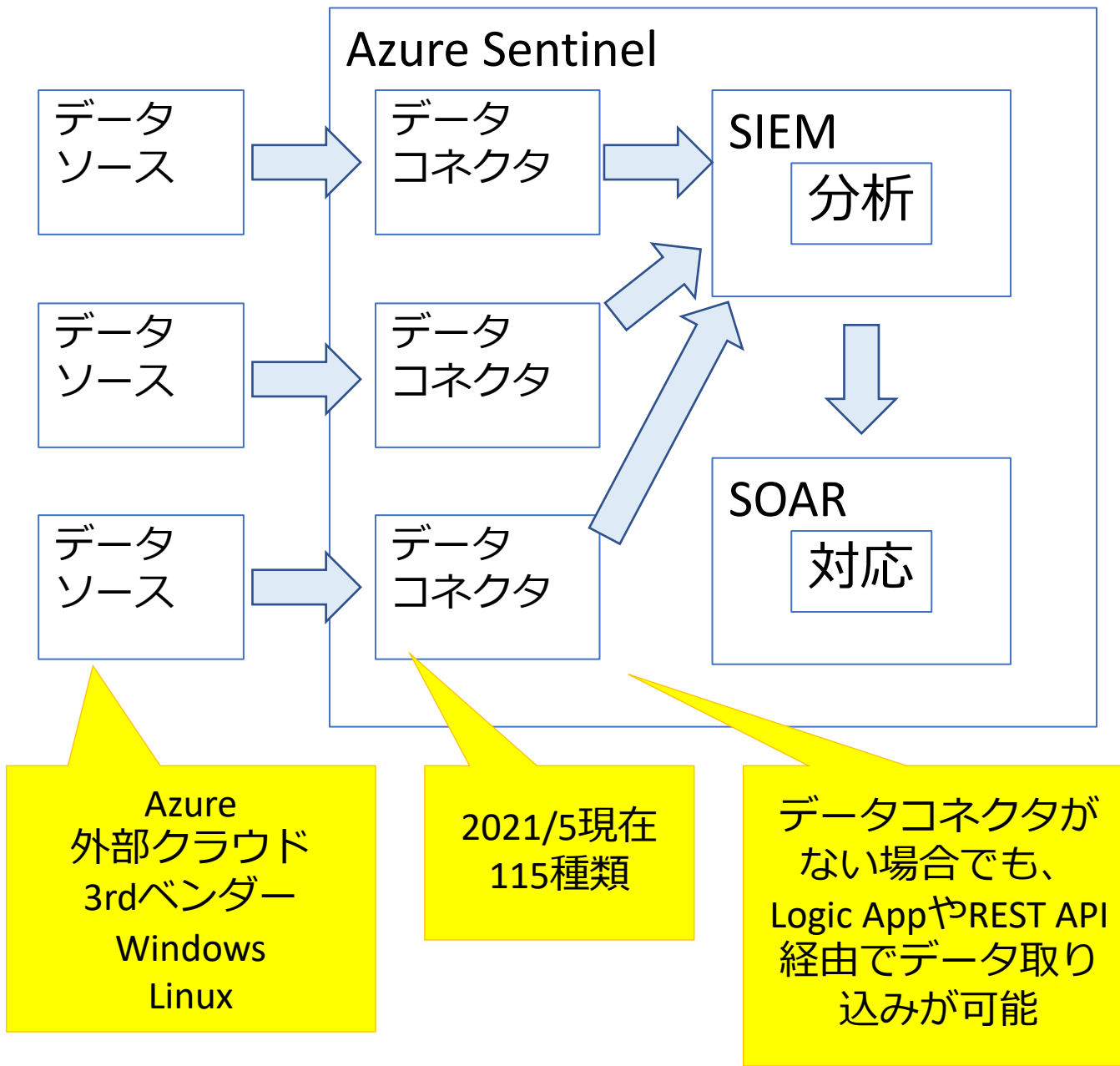
- セキュリティ情報イベント管理 (SIEM)
- セキュリティ機器やネットワーク機器などからログを集めて一元管理し、相関分析によってセキュリティインシデントを自動的に発見するためのソリューション。
- 複数台の機器から集めたログを時系列などで相関分析することで、セキュリティインシデントの予兆や痕跡を見つけ出します。

SOARとは？

- セキュリティ オークストレーション 自動応答 (SOAR)
- インシデントの分析から対応までを自動化・効率化するツールのこと。
- 担当者の負担を減らしてより効率よくセキュリティ部署を運用するためのしくみです。



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収集します。



脅威を検出します。Microsoft の分析と脅威インテリジェンスを使用して、誤判定を最小限に抑えます。

人工知能を使用して脅威を調査します。疑わしいアクティビティを探索します。

インシデントに迅速に対応します。一般的なタスクの組み込みのオーケストレーションとオートメーションを使用します。

脅威を検出します。Microsoftの分析と脅威インテリジェンスを使用して、誤判定を最小限に抑えます。

人工知能を使用して脅威を調査します。疑わしいアクティビティを検索します。

インシデントに迅速に対応します。一般的なタスクの組み込みのオーケストレーションとオートメーションを使用します。

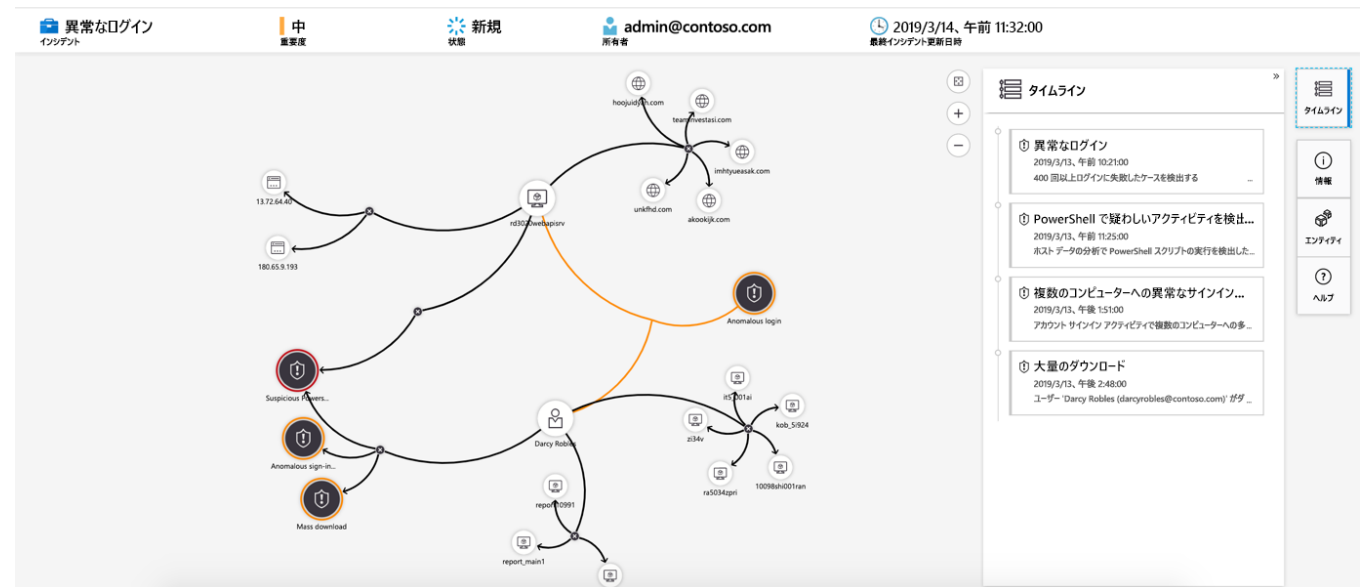
- データソースから取り込まれた各種データから脅威の検出を行います。
- 検出のためのルールセットは、MicrosoftがGitHub上で提供しているものを利用しています。

脅威を検出します。Microsoftの分析と脅威インテリジェンスを使用して、誤判定を最小限に抑えます。

人工知能を使用して脅威を調査します。疑わしいアクティビティを検索します。

インシデントに迅速に対応します。一般的なタスクの組み込みのオーケストレーションとオートメーションを使用します。

- 組み込みのAIも使用して、インテリジェントな脅威の検出を行います。
- 「調査グラフ」を使用して、関連するデータとエンティティを結びつけることができます。

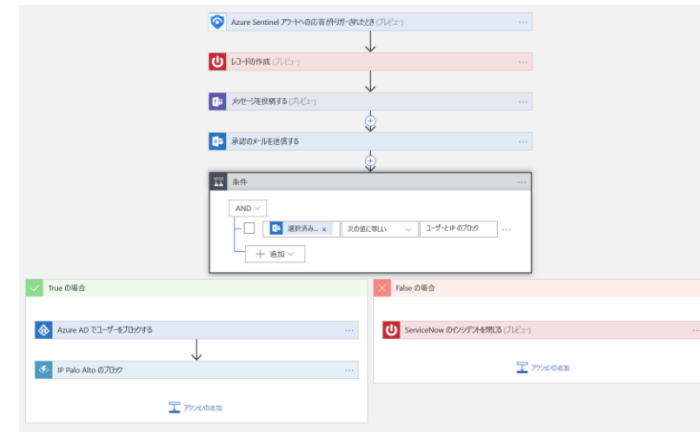


脅威を検出します。Microsoftの分析と脅威インテリジェンスを使用して、誤判定を最小限に抑えます。

人工知能を使用して脅威を調査します。疑わしいアクティビティを検索します。

インシデントに迅速に対応します。一般的なタスクの組み込みのオーケストレーションとオートメーションを使用します。

- 検出されたアラートは「インシデント」として登録されます。
- 各インシデントのオーナー（責任者）、ステータス、重要度などの管理を行うことができます。
- Azure Logic Appをベースにした「セキュリティプレイブック」を使用して、対応を自動化することができます。



Azure Security Center (ASC) と Azure Sentinel の関係は？



Azure Security Center は、わずか数クリックで Azure Sentinel に接続できます。Azure Sentinel から Security Center のデータにアクセスできるようになったら、ファイアウォール、ユーザー、デバイスなどの他のソースと組み合わせて、高度なクエリや人工知能によるプロアクティブな検索や脅威の軽減が可能になります。

Azure Security Center (ASC) と Azure Sentinelの関係は？


- 統合セキュリティ管理システムであるSecurity Center の利用は急速に拡大しており、機能も増えて、セキュリティ情報イベント管理 (SIEM) に似た「調査」機能を展開しています。
- この調査機能は高い評価を得ていますが、お客様からはより多くの機能を求める声が寄せられています。
- 同時に、Security Center の従来のビジネス モデルは、仮想マシン (VM) などのリソース単位で価格が設定されており、必ずしも SIEM に適してはいません。
- Security Center は、高度なセキュリティ運用 (SecOps) での検索シナリオや SIEM ツールとしての使用を意図したものではありません。
- そこで、Security Center とは別の、連携が可能な洗練されたスタンドアロン SIEM ソリューションを必要としているお客様に向けて、Azure Sentinel を構築しました。

Azure Sentinelの価格

Azure Sentinel の価格

Azure Sentinel では、Azure Sentinel での分析用に取り込まれたデータ量に基づいて請求されます。Azure Sentinel では、柔軟で予測可能な価格モデルが提供されています。

Azure Sentinel サービスのお支払いには、容量予約と従量課金制の 2 つの方法があります。Azure Sentinel のコストは、選択した価格レベルによって異なります。詳細については、[Azure Sentinel の価格](#)をご覧ください。

 これには、Azure Log Analytics のデータ取り込みの価格は含まれません。Log Analytics の価格に関する詳細をご確認ください。

▽ 100 GB/日
従量課金制の価格と比較して 50% 割引


▽ 200 GB/日
従量課金制の価格と比較して 55% 割引

▽ 300 GB/日
従量課金制の価格と比較して 57% 割引


▽ 400 GB/日
従量課金制の価格と比較して 58% 割引

▽ 500 GB 以上/日
従量課金制の価格と比較して 60% 割引

△ 従量課金制の
1 GB あたり

現在の階層 

従量課金制の価格では、Azure Sentinel によって分析されるデータがギガバイト (GB) 単位で課金されます。付属の 90 日間の保有期間を超えて、データ保有期間を延長した場合は、追加料金が発生します。[Azure Sentinel の価格](#)に関する詳細をご確認ください。

 これには、Azure Log Analytics のデータ取り込みの価格は含まれません。Log Analytics の価格に関する詳細をご確認ください。

適用

デフォルトは「従量課金制」、分析されたデータのGBあたり275円

1日のデータ量が多くなってきた場合は、「予約容量」に切り替えるとお得（50%～60%の割引）



サービス



Azure Sentinel

リソース

該当結果が見つかりませんでした。

Marketplace



vArmour Application Con



Light Azure Sentinel MSS



Managed Azure Sentinel



Azure Managed Services

ドキュメント

[Azure Sentinel とは | Microso](#)

[Azure Sentinel のドキュメント |](#)

>>

[ホーム](#) >

Azure Sentinel

☆ ...

既定のディレクトリ



+

作成



クラシック ビューを開く



ビューの管理



更新



CSV にエクスポート



クエリを開く



フィードバック



インシデントの表示

任意のフィールドのフィルタ...

サブスクリプション == すべて

リソース グループ == すべて



場所 == すべて



+ フィルターの追加

0 件中 0 ~ 0 件のレコードを表示しています。

グループ化なし

リ

名前 ↑↓

リソース グループ ↑↓

場所 ↑↓

サブスクリプション ↑↓

ディレクトリ



表示する Azure Sentinel がありません

今の時代に適応するよう作り直された SIEM を使用すると、被害が発生する前に脅威を検出し、防ぐことができます。Azure Sentinel で、エンタープライズ全体を概観できます。

[詳細情報](#)[Azure Sentinel の作成](#)

ワークスペースへの Azure Sentinel の追加 ...

[+ 新しいワークスペースの作成](#) [🔄 最新の情報に更新](#)

名前でフィルター処理...



ワークスペースが見つかりません



[新しいワークスペースの作成](#)

追加

取り消し

Log Analytics ワークスペースの作成 ...

基本 価格レベル タグ 確認および作成

 Log Analytics ワークスペースは、Azure Monitor ログの基本的な管理ユニットです。新しい Log Analytics ワークスペースを作成する場合は、特定の考慮事項があります。[詳細情報](#) 

Azure Monitor ログを使用すると、Azure とその他の環境内の監視対象のリソースから収集したデータを簡単に保存、保持、クエリ処理して、価値ある分析情報を入手できます。Log Analytics ワークスペースは、ログデータの収集と保存が行われる論理ストレージ ユニットです。

プロジェクトの詳細

デプロイされているリソースとコストを管理するサブスクリプションを選択します。フォルダーのようなリソース グループを使用して、すべてのリソースを整理し、管理します。

サブスクリプション * ⓘ

Azure Pass - スポンサー プラン 

リソース グループ * ⓘ

test 

[新規作成](#)

インスタンスの詳細

名前 * ⓘ

sentinelworkspace1 

地域 * ⓘ

米国東部 

確認および作成

« 前へ

次: 価格レベル >

ワークスペースへの Azure Sentinel の追加 ...



[+ 新しいワークスペースの作成](#) [🔄 最新の情報に更新](#)

名前ですフィルター処理...				
ワークスペース ↑↓	場所 ↑↓	ResourceGroup ↑↓	サブスクリプション ↑↓	ディレクトリ ↑↓
 sentinelworkspace1	eastus	test	Azure Pass - スポンサー プラン	既定のディレクトリ

3  ?  test2021-0518@outlook...
既定のディレクトリ 

*** Azure Sentinel を追加しています

1:23



Azure Sentinel をワークスペース 'sentinelworkspace1' に追加しています

[ホーム](#) > [Azure Sentinel](#) > [Azure Sentinel](#)

Azure Sentinel | ニュースとガイド

選択したワークスペース: 'sentinelworkspace1'



新機能

始める

全般

概要

ログ

ニュースとガイド

脅威管理

インシデント

ブック

ハンティング

ノートブック

エンティティの動作

脅威インテリジェンス (プレビュー)

構成

データ コネクタ

分析

ウォッチリスト (プレビュー)

オートメーション

ソリューション (プレビュー)

コミュニティ

設定

Azure Sentinel

最も重要な事項に集中できるようにするクラウドネイティブの SIEM

クラウドのスケールで、クラウドまたはオンプレミスから任意の形式のデータを収集し、分析できます。AI を味方に付け、セキュリティに関する数十年に及ぶ Microsoft の経験から得て組み込まれたナレッジとインテリジェンスを利用して、実際の脅威を数分で検出し、調査し、それに対処することができます。



1. データの収集

クラウドのスケールで、オンプレミスと複数のクラウドの両方 について、エンタープライズ全体からデータを収集します

接続



2. セキュリティ アラートの作成

分析を使用してアラートを作成することにより、重要なことに注意を集中します

作成



3. 自動化と調整

組み込みのブレイックを使用またはカスタマイズして一般的なタスクを自動化します

作成



続きは以下をご覧ください
(MS社員による解説)

[Azure] クラウドネイティブな SIEM である Azure Sentinel を触ってみた

<https://qiita.com/Yoshifumi/items/0d38e7f9de293d6490df>