

Microsoft Sentinel

スケーラブルでクラウドネイティブの

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

Microsoft Sentinelとは？

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。

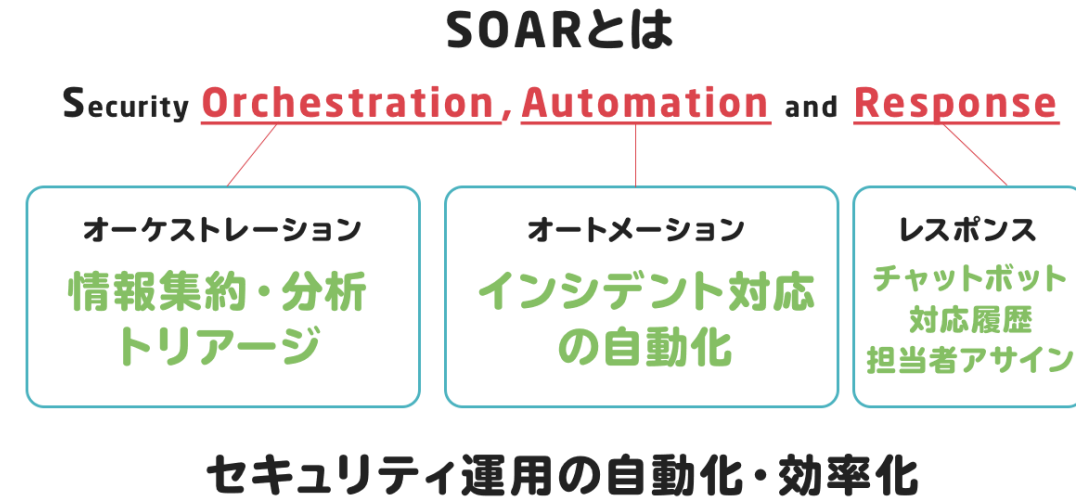
- Microsoft Sentinel は、スケーラブルでクラウドネイティブ型の **セキュリティ情報イベント管理 (SIEM)** および **セキュリティオーケストレーション自動応答 (SOAR)** ソリューションです。
- Microsoft Sentinel は、高度なセキュリティ分析と脅威インテリジェンスを企業全体で実現し、アラートの検出、脅威の可視性、予防的な搜索、および脅威への対応のための 1 つのソリューションを提供します。

SIEMとは？

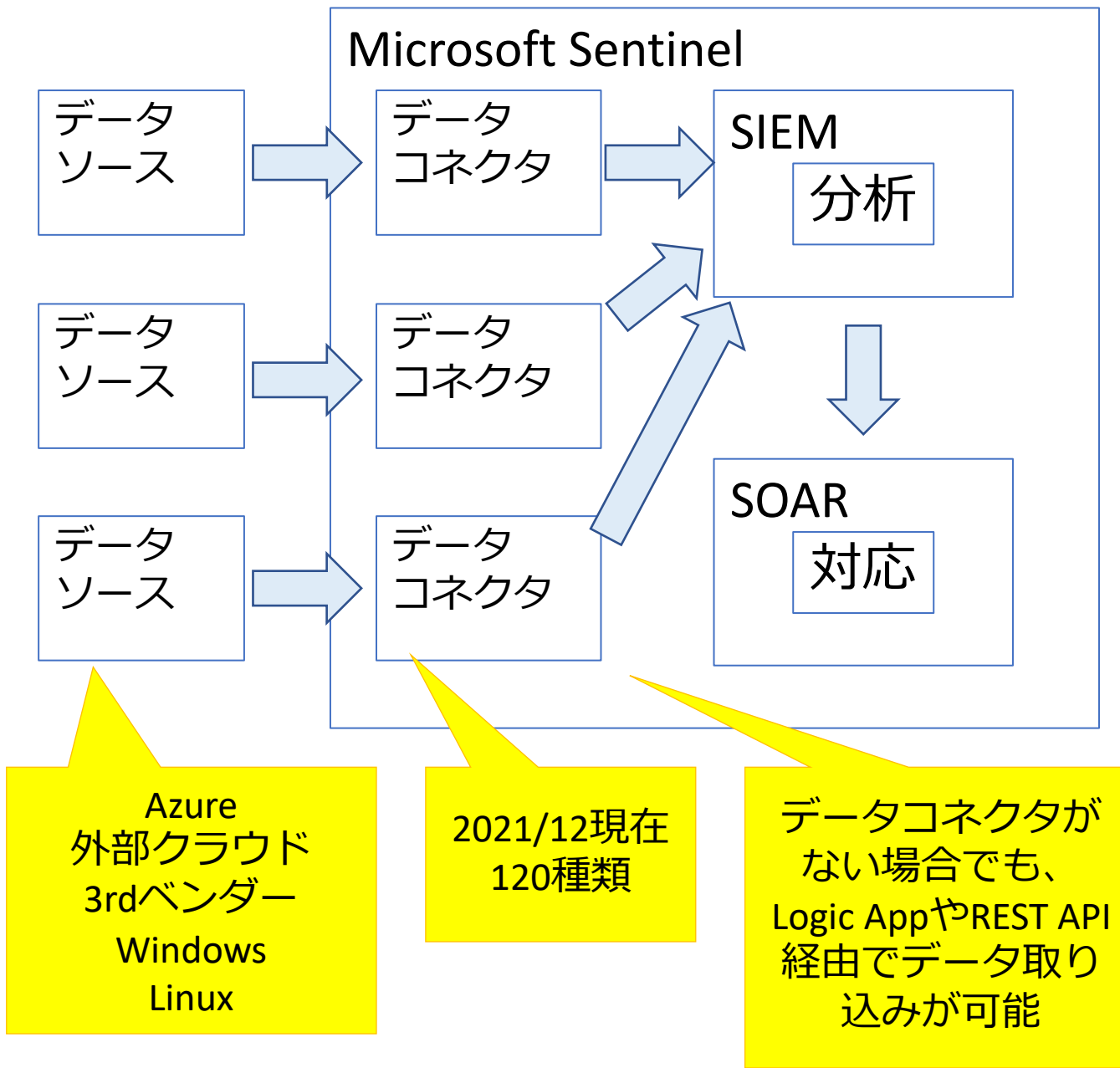
- セキュリティ情報イベント管理 (SIEM)
- セキュリティ機器やネットワーク機器などからログを集めて一元管理し、相関分析によってセキュリティインシデントを自動的に発見するためのソリューション。
- 複数台の機器から集めたログを時系列などで相関分析することで、セキュリティインシデントの予兆や痕跡を見つけ出します。

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。

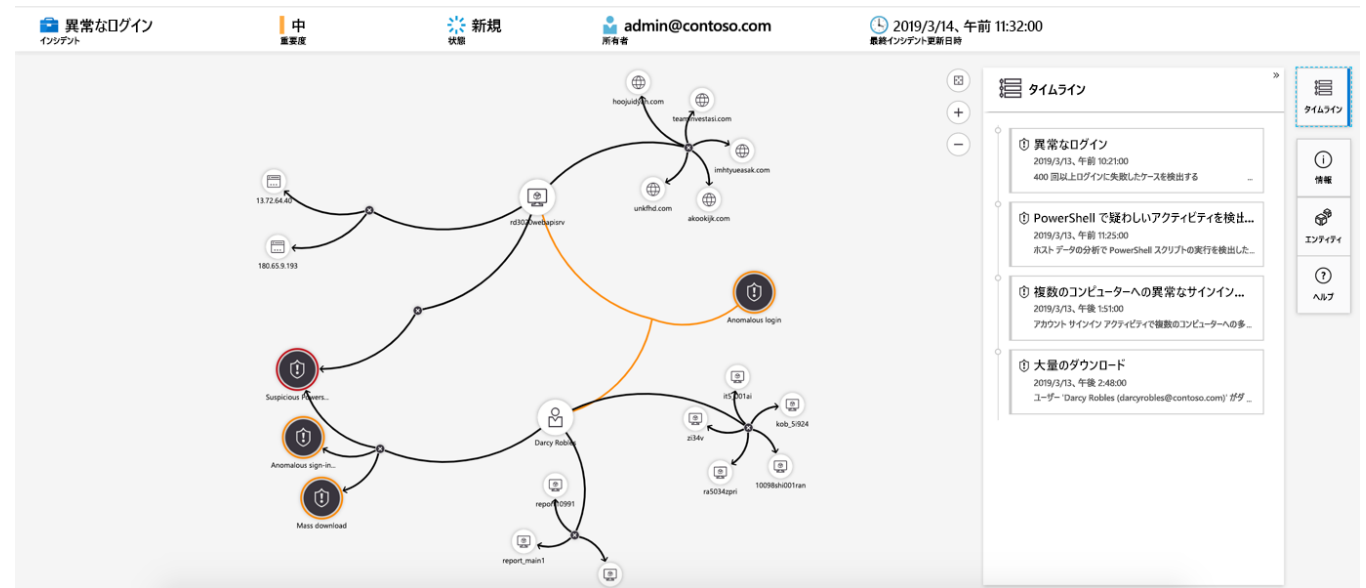
- データソースから取り込まれた各種データから脅威の検出を行います。
- 検出のためのルールセットは、MicrosoftがGitHub上で提供しているものを利用しています。

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。

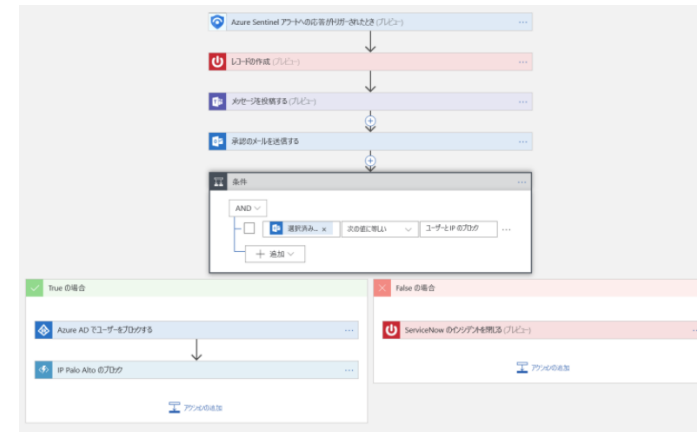


脅威を検出します。Microsoftの分析と脅威インテリジェンスを使用して、誤判定を最小限に抑えます。

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。



Microsoft Defender for Cloudと Azure Sentinelの関係は？



Microsoft Defender for Cloud は、わずか数クリックで Microsoft Sentinel に接続できます。Microsoft Sentinel から Microsoft Defender for Cloud 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。


Microsoft Defender for CloudとMicrosoft Sentinelの関係は？

- 統合セキュリティ管理システムであるMicrosoft Defender for Cloud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、Microsoft Defender for Cloud 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。
- Microsoft Defender for Cloud 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、Microsoft Defender for Cloud 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、Microsoft Sentinel を構築しました。

Microsoft 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）

Microsoft Sentinelの作成

Log Analyticsワークスペースを作成

Microsoft SentinelをLog Analyticsワークスペースに追加

Microsoft Azure



sentinel



Microsoft Sentinel

サービス

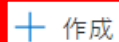


Microsoft Sentinel

[ホーム](#) >

Microsoft Sentinel ☆ ...

既定のディレクトリ



+ 作成



ビューの管理 ▾



更新



CSV にエクスポート



クエリを開く



インシデントの表示



フィードバック

任意のフィールドのフィルター...

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



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



表示する Microsoft 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。Microsoft Sentinel で、エンタープライズ全体を概観できます。

Microsoft Sentinel の作成

[詳細情報](#) ↗

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

既定のディレクトリ

■■■ Microsoft Sentinel を追加しています



Microsoft Sentinel をワークスペース 'loga90182374' に追加しています



Microsoft Sentinel | 概要 ...

選択したワークスペース: 'loga90182374'

🔍 検索 (Ctrl+/)

⌂ 最新の情報に更新

🕒 過去 24 時間 ▾

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

コンテンツ管理

📁 コンテンツ ハブ (プレビュー)

📁 リポジトリ (プレビュー)

👤 コミュニティ

構成

🔗 データ コネクタ

🔍 分析

📁 ウォッチリスト

⚙️ オートメーション

⚙️ 設定

📶 0
イベント

🛡️ 0
警告

👜 0
インシデント

状態別インシデント

🆕 新規 (0)

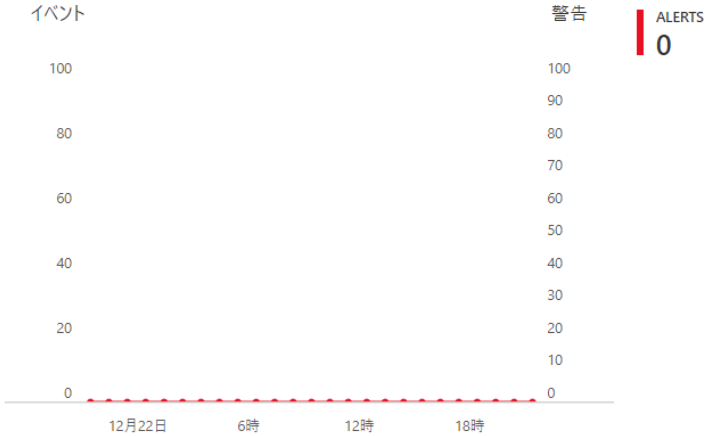
🟡 アクティブ (0)

🟢 終了 (真陽性) (0)

🔴 終了 (誤検知) (0)

📄 詳細情報
🔗 ドキュメント

時間経過に伴うイベントとアラート



悪意のある可能性があるイベント



最近のインシデント

データが見つかりませんでした

データ ソースの異常

データが見つかりませんでした

お客様の SecOps のための ML の民主化



ML に現在どのくらい投資しているかにかかわらず、ML における MS の最先端の研究とベスト プラクティスを活用することにより、セキュリティ専門家は AI の力を最大限活かすことができます。

📄 詳細情報 >

データ コネクタの追加

データコネクタは複数追加することができる。

2つ目のデータコネクタとしてAzure Active Directory Identity Protectionを接続

ホーム > Microsoft Sentinel > ワークスペースへの Microsoft Sentinel の追加 > Microsoft Sentinel

Microsoft Sentinel | データ コネクタ ...
選択したワークスペース: 'loga90182374'

検索 (Ctrl+/)

ガイドとフィードバック 最新の情報に更新

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

ハンディング

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

コンテンツ管理

コンテンツ ハブ (プレビュー)

リポジトリ (プレビュー)

コミュニティ

構成

データ コネクタ

分析

ウォッチリスト

オートメーション

設定

120
コネクタ

0
接続済み

azure

プロバイダー

増やす (2)

状態 ↑↓

コネクタ名 ↑↓



Azure Active Directory

Microsoft



Azure Active Directory Identity Protection

Microsoft



Azure DDoS Protection

Microsoft



Azure Firewall

Microsoft



Azure Information Protection (プレビュー)

Microsoft



Azure Key Vault

Microsoft



Azure Kubernetes Service (AKS)

Microsoft



Azure SQL データベース

Microsoft



Azure Storage アカウント (プレビュー)

Microsoft



Azure Web アプリケーション ファイアウォール (WAF)

Microsoft



Azure アクティビティ

Azure Active Directoryを検索して選択



Azure Active Directory

未接続
状態

Microsoft
プロバイダー

--
最後に受信したログ

説明

監査とサインインのログを Microsoft Sentinel に接続して、Azure Active Directory シナリオに関する分析情報を収集すると、Azure Active Directory の分析情報を取得できます。サインイン ログを使用すると、アプリの使用状況、条件付きアクセス ポリシー、レガシ認証関連の詳細について確認できます。監査ログ テーブルを使用すると、パスワードリセットのセルフサービス (SSPR) の使用状況や、ユーザー、グループ、ロール、アプリ管理などの Azure Active Directory 管理アクティビティに関する情報を取得できます。

最後に受信したデータ ①

--

関連コンテンツ

6
ブック

2
クエリ

62
分析ルールのテンプレート

受信したデータ

[Log Analytics に移動する](#)

100

80

60

40

20

0

12月17日

12月19日

12月21日

へ 受信したデータの合計

1/5

受信したデータの合計

コネクタ ページを開く

Azure Active Directory ...



Azure Active Directory

未接続
状態

Microsoft
プロバイダー

--
最後に受信したログ

説明

監査とサインインのログを Microsoft Sentinel に接続して、Azure Active Directory シナリオに関する分析情報を収集すると、Azure Active Directory の分析情報を取得できます。サインイン ログを使用すると、アプリの使用状況、条件付きアクセス ポリシー、レガシ認証関連の詳細について確認できます。監査ログ テーブルを使用すると、パスワード リセットのセルフサービス (SSPR) の使用状況や、ユーザー、グループ、ロール、アプリ管理などの Azure Active Directory 管理アクティビティに関する情報を取得できます。

最後に受信したデータ ①

--

関連コンテンツ

6
ブック

2
クエリ

62
分析ルール テンプレート

受信したデータ

Log Analytics に移動する

100

80

60

40

20

0

12月17日

12月19日

12月21日

受信したデータの合計

1/5

0

受信したデータの合計

0

データ型

SigninLogs --

AuditLogs --

AADNonInteractiveUserSignInLogs --

AADServicePrincipalSignInLogs --

手順

次の手順

前提条件

Azure Active Directory と統合するには、次のものがあることを確認してください。

✓ ワークスペース: 読み取りおよび書き込みアクセス許可。

✓ 診断設定: AAD 診断設定に対する読み取りアクセス許可。

✓ テナントのアクセス許可: ワークスペースに読み取りアクセス許可。

構成

Azure Active Directory のログを Microsoft Sentinel に接続する

Azure Active Directory のログの種類を選択:

☒ Sign-In Logs

In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

☐ 監査ログ

☐ Non-Interactive User Sign-In Log (プレビュー)

☐ Service Principal Sign-In Logs (プレビュー)

☐ Managed Identity Sign-In Logs (プレビュー)

☐ Provisioning Logs (プレビュー)

☐ ADFS Sign-In Logs (プレビュー)

☐ User Risk Events (プレビュー)

☐ 危険なユーザー (プレビュー)

変更の適用

Sign-in Logsにチェック

接続完了（実際に接続されるまで15分ほどかかる）

[ホーム](#) > [Microsoft Sentinel](#) > [ワークスペースへの Microsoft Sentinel の追加](#) > [Microsoft Sentinel](#) >

Azure Active Directory ...



Azure Active Directory

未接続
状態

Microsoft
プロバイダー

--
最後に受信したログ

説明

監査とサインインのログを Microsoft Sentinel に接続して、Azure Active Directory シナリオに関する分析情報を収集すると、Azure Active Directory の分析情報を取得できます。サインイン ログを使用すると、アプリの使用状況、条件付きアクセス ポリシー、レガシ認証関連の詳細について確認できます。監査ログ テーブルを使用すると、パスワードリセットのセルフサービス (SSPR) の使用状況や、ユーザー、グループ、ロール、アプリ管理などの Azure Active Directory 管理アクティビティに関する情報を取得できます。

最後に受信したデータ ①

--

関連コンテンツ

6
ブック

2
クエリ

62
分析ルールのテンプレート

受信したデータ

[Log Analytics に移動する](#)

受信したデータの合計

12月17日 12月19日 12月21日

1/5 0 0

データ型

SigninLogs --

AuditLogs --

AADNonInteractiveUserSignInLogs --

AADServicePrincipalSignInLogs --

手順 次の手順

推奨ブック (6 個)

[ブック ギャラリーへ移動 >](#)

Azure AD サインイン ログ
Microsoft

Azure AD 監査ログ

クエリのサンプル (2 件)

すべてのログ

SigninLogs

| take 1000

| sort by TimeGenerated

[実行](#)

1 時間単位で集計

AuditLogs

| summarize count() by bin(TimeGenerated, 1h)

| sort by TimeGenerated

[実行](#)

関連する分析テンプレート (62)

[分析テンプレートへ移動 >](#)

重大度 ↑↓	名前 ↑↓	ルールの種類 ↑↓	データ ソース
高	Suspicious application consent similar t...	Scheduled	Azure Active Direct...
高	Bulk Changes to Privileged Account Per...	Scheduled	Azure Active Direct...
高	Log4j vulnerability exploit aka Log4She...	Scheduled	Office 365 +13 ①
高	Known Barium IP	Scheduled	Office 365 +13 ①
高	新規 User agent search for log4j explo...	Scheduled	Azure Web ア... +5 ①
高	Authentication Methods Changed for P...	Scheduled	Azure Active Direct...
高	Azure AD Role Management Permissio...	Scheduled	Azure Active Direct...

データコネクタは複数追加することができる。

2つ目のデータコネクタとしてAzure Active Directory Identity Protectionを接続

ホーム > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | データ コネクタ

選択したワークスペース: 'loga90182374'

検索 (Ctrl+/) << ガイドとフィードバック 最新の情報に更新

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

コンテンツ管理

- コンテンツ ハブ (プレビュー)
- リポジトリ (プレビュー)
- コミュニティ

構成

- データ コネクタ**
- 分析
- ウォッチリスト
- オートメーション
- 設定

120 コネクタ 3 接続済み

identity protection x プロバイダー: すべて 増やす (2)

状態 ↑↓ コネクタ名 ↑↓

状態	コネクタ名
	Azure Active Directory Identity Protection Microsoft

Identity Protectionで検索

コネクタページを開き「接続」をクリック

Azure Active Directory Identity Protection

接続済み 状態 Microsoft プロバイダー 9 分前 最後に受信したログ

説明

Azure Active Directory Identity Protection では、リスク ユーザー、リスク イベント、脆弱性の統合ビューが提供され、直ちにリスクを修正する機能があり、将来のイベントを自動修復するポリシーを設定できます。このサービスは、コンシューマー ID を保護する Microsoft のエクスペリエンスに基づいて構築されており、1 日に 130 億回を超えるログインからの信号に基づいて非常に正確な精度を実現しています。Microsoft Azure Active Directory Identity Protection アラートを Microsoft Sentinel に統合すると、ダッシュボードを表示したり、カスタム アラートを作成したり、調査を改善したりできます。

[Azure Active Directory Premium P1/P2 を入手する >](#)

最後に受信したデータ
21/12/22 22:11

関連コンテンツ

0 ブック 2 クエリ 2 分析ルールテンプレート

受信したデータ [Log Analytics に移動する](#)

2

1.5

1

0.5

0

12月17日 12月19日 12月21日

受信したデータの合計

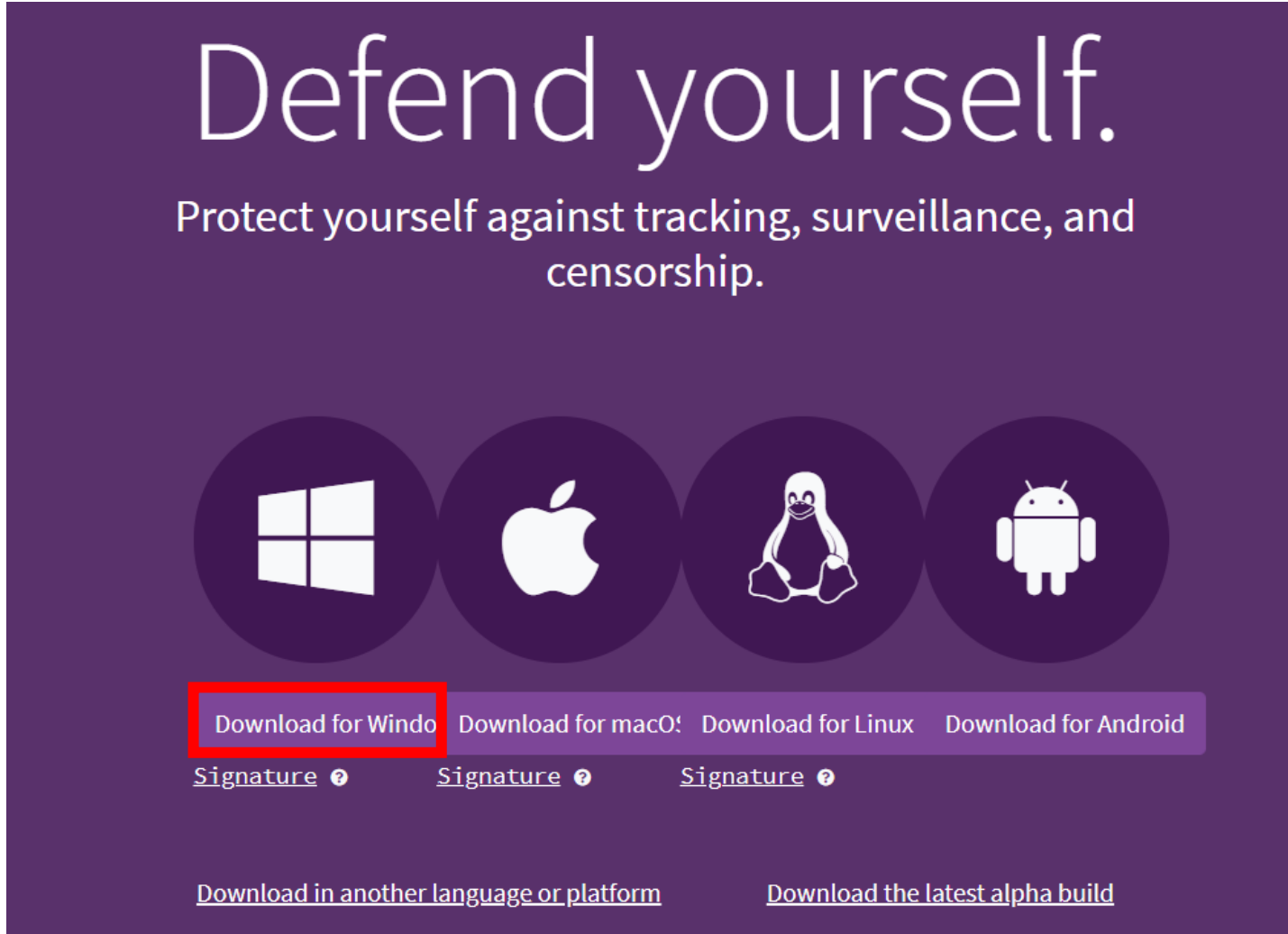
コネクタ ページを開く

検証用の インシデントを発生させる

Torブラウザを使用して、Azure portalに匿名IPアドレスからサインイン

Torブラウザをダウンロードしてインストール

<https://www.torproject.org/download/>

The image shows the Tor Project's download page. It has a dark purple background. At the top, the text "Defend yourself." is written in a large, white, serif font. Below it, in a smaller white sans-serif font, is the text "Protect yourself against tracking, surveillance, and censorship." In the center, there are four white circular icons: the Windows logo, the Apple logo, the Tux penguin (Linux), and the Android robot. Below these icons is a horizontal bar with four buttons: "Download for Windows", "Download for macOS", "Download for Linux", and "Download for Android". The "Download for Windows" button is highlighted with a red rectangular border. Below each button is a link that says "Signature" followed by a question mark icon. At the bottom of the page, there are two more links: "Download in another language or platform" and "Download the latest alpha build".

Defend yourself.

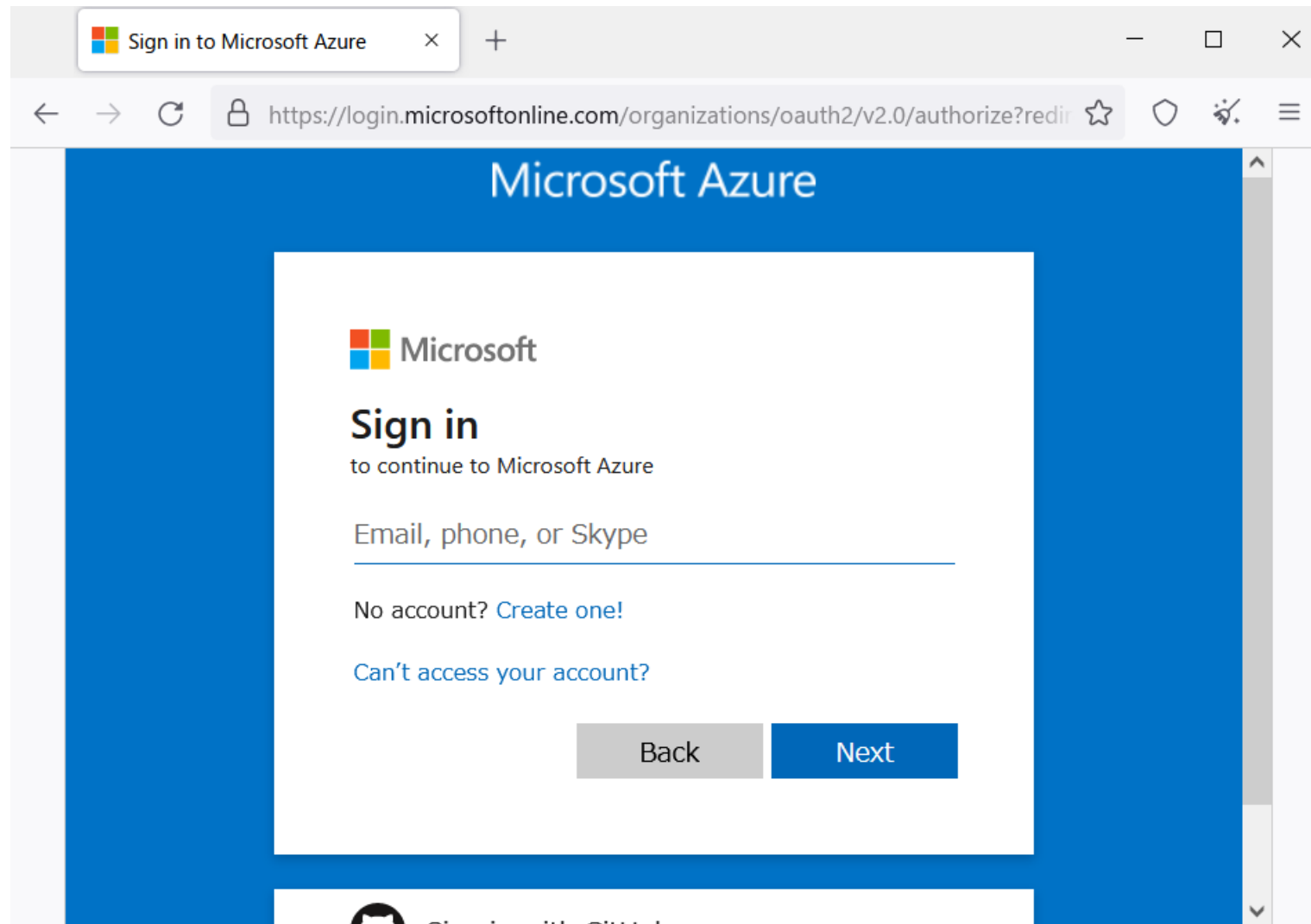
Protect yourself against tracking, surveillance, and censorship.

[Download for Windows](#) [Download for macOS](#) [Download for Linux](#) [Download for Android](#)

[Signature ?](#) [Signature ?](#) [Signature ?](#)

[Download in another language or platform](#) [Download the latest alpha build](#)

Torブラウザを起動し、<https://portal.azure.com/> に移動。適当なユーザーでサインイン。
※サインイン・サインアウトを何度か繰り返し、複数のインシデントを発生させる



Azure AD > セキュリティ > Identity Protectionの画面でも、
「危険度 - 中のユーザー」として、サインインが検出・記録される。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

test2021-1222@outlook...
既定のディレクトリ

ホーム > 既定のディレクトリ > セキュリティ >

Identity Protection | 概要

検索 (Ctrl+/)

詳細情報 | 更新 | フィードバックがある場合

概要

問題の診断と解決

保護

ユーザー リスク ポリシー

サインイン リスク ポリシー

MFA 登録ポリシー

レポート

危険なユーザー

危険なサインイン

リスク検出

通知

リスクのあるユーザーが検出された警告

週間ダイジェスト

期間 = 30 日

新しい危険なユーザーが検出されました ⓘ

ユーザーのリスク レベル = すべて

危険度 - 中のユーザー ⓘ

1

危険度 - 中のユーザーが検出されました。ユーザーを調査し、パスワードをリセットしてください。

ID セキュリティ スコア ⓘ

/ -

ID セキュリティの状態を監視し、改善します。

11/2712/0412/1112/18

カウント

-

ユーザー リスク ポリシーの構成 >

新しい危険なサインインが検出されました ⓘ

増やす (2)

100

80

60

40

Microsoft Sentinelの画面でも「インシデント」が発生したことが確認できる。
「最近のインシデント」をクリックして詳細へ移動。



インシデントの詳細が確認できる。

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

test2021-1222@outlook... 既定のディレクトリ

ホーム > Microsoft Sentinel > Microsoft Sentinel >

インシデント

インシデント ID 2

最新の情報に更新

Anonymous IP address
インシデント ID: 2

未割り当て
所有者

新規
状態

中
重大度

説明
Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)

製品名のアラート
• Azure Active Directory Identity Protection

証拠
該当なし 1 アラート 0 ブックマーク イベント

最終更新時間
21/12/22 22:11

作成時刻
21/12/22 22:11

エンティティ (2 個)
user1@test20...
185.100.87.72
すべての詳細を表示 >

方針 (1 個)
Initial Access

インシデントブック
インシデントの概要

分析ルール
Create incidents based on Azure Active Directory

タグ
+

タイムライン

警告

ブックマーク

エンティティ

コメント

検索

タイムラインコンテンツ: すべて

増やす (2)

12月 22
22:08

Anonymous IP address
中 | Azure Active Directory Identity Protection

説明
Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)

重大度
中

状態
新規

イベント
該当なし

製品名
Azure Active Directory Identity Protection

エンティティ (2 個)
user1
185.100.87.72

方針 (1 個)
Initial Access

システム アラート ID
5997dd60-5888-ef62-459...

規則名
--

最終更新時間
21/12/22 22:11

更新
0

開始時刻
21/12/22 22:08

終了時刻
21/12/22 22:08

アラートリンク
--

調査 操作

インシデントに、
タイトルとIDが付与される

タイムライン
(時系列情報)

タイムラインで
選択した項目の
詳細

説明文







発生場所

エンティティとして、サイン
インに使用されたユーザーID
と、送信元のIPアドレスが記
録される

「調査」をクリック

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)




test2021-1222@outlook...
既定のディレクトリ

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

インシデント

インシデント ID 2

最新の情報に更新

 **Anonymous IP address**
インシデント ID: 2

未割り当て
所有者

新規
状態

中
重大度

説明

Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)

製品名のアラート

- Azure Active Directory Identity Protection

証拠

該当なし
イベント

1
アラート

0
ブックマーク

最終更新時間

21/12/22 22:11

作成時刻

21/12/22 22:11

エンティティ (2 個)

user1@test20...

185.100.87.72

すべての詳細を表示 >

エンティティ (2 個)

user1

185.100.87.72

方針 (1 個)

Initial Access

インシデント ブック

インシデントの概要

分析ルール

Create incidents based on Azure Active Directory Identity Pr...

タグ

+

調査

操作

タイムライン

警告

ブックマーク

エンティティ


コメント

検索

タイムライン コンテンツ: すべて

増やす (2)

12月 22
22:08



Anonymous IP address
中 | Azure Active Directory Identity P

説明

Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)

重大度

中

状態

新規

イベント

該当なし

製品名

Azure Active Directory Identity Protection

エンティティ (2 個)

user1

185.100.87.72

システム アラート ID

5997dd60-5888-ef62-459...

規則名

--

最終更新時間

21/12/22 22:11

更新

0

開始時刻

21/12/22 22:08

終了時刻

21/12/22 22:08

アラート リンク

--

調査

調査

操作

「調査グラフ」画面：関連する「エンティティ」をクリックし、詳細情報を表示できる

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+/)

test2021-1222@outlook... 既定のディレクトリ

ホーム > Microsoft Sentinel > Microsoft Sentinel > インシデント > 調査 ...

元に戻す やり直し

Anonymous IP address インシデント 中 重大度 新規 状態 未割り当て 担当者

2021/12/22 22:11:21 最終インシデント更新時間

マウスホイールで拡大縮小

インシデント

エンティティ

エンティティ

185.100.87.72

Anonymous IP address

user1

AccountName user1

UpnSuffix test20211222outlook.onmicrosoft.com

AadTenantId f81dfeff-7055-43f3-a1eb-c106ed96309e

AadUserId fa211884-2609-4da0-b907-c36615b4972a

DisplayName user1

FriendlyName user1

すべての詳細を表示

タイムライン

情報

エンティティ

分析情報

ヘルプ

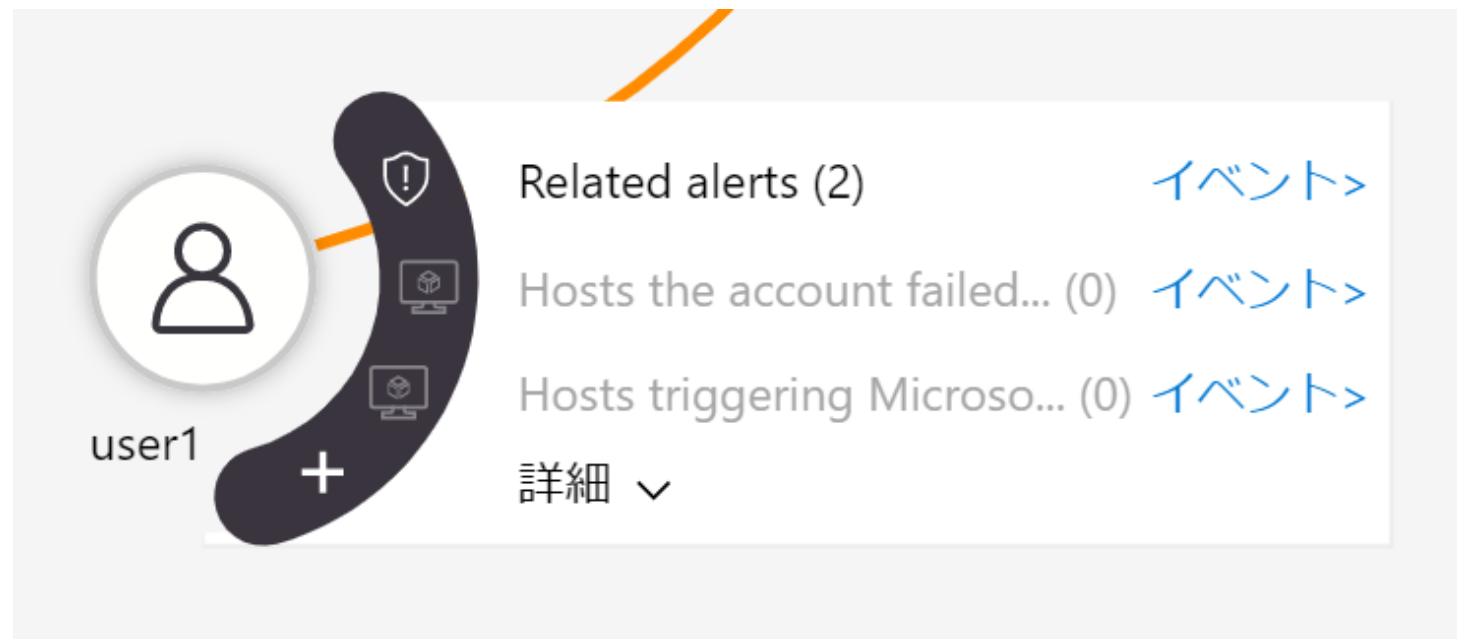
Related alerts (2) イベント>

Hosts the account failed... (0) イベント>

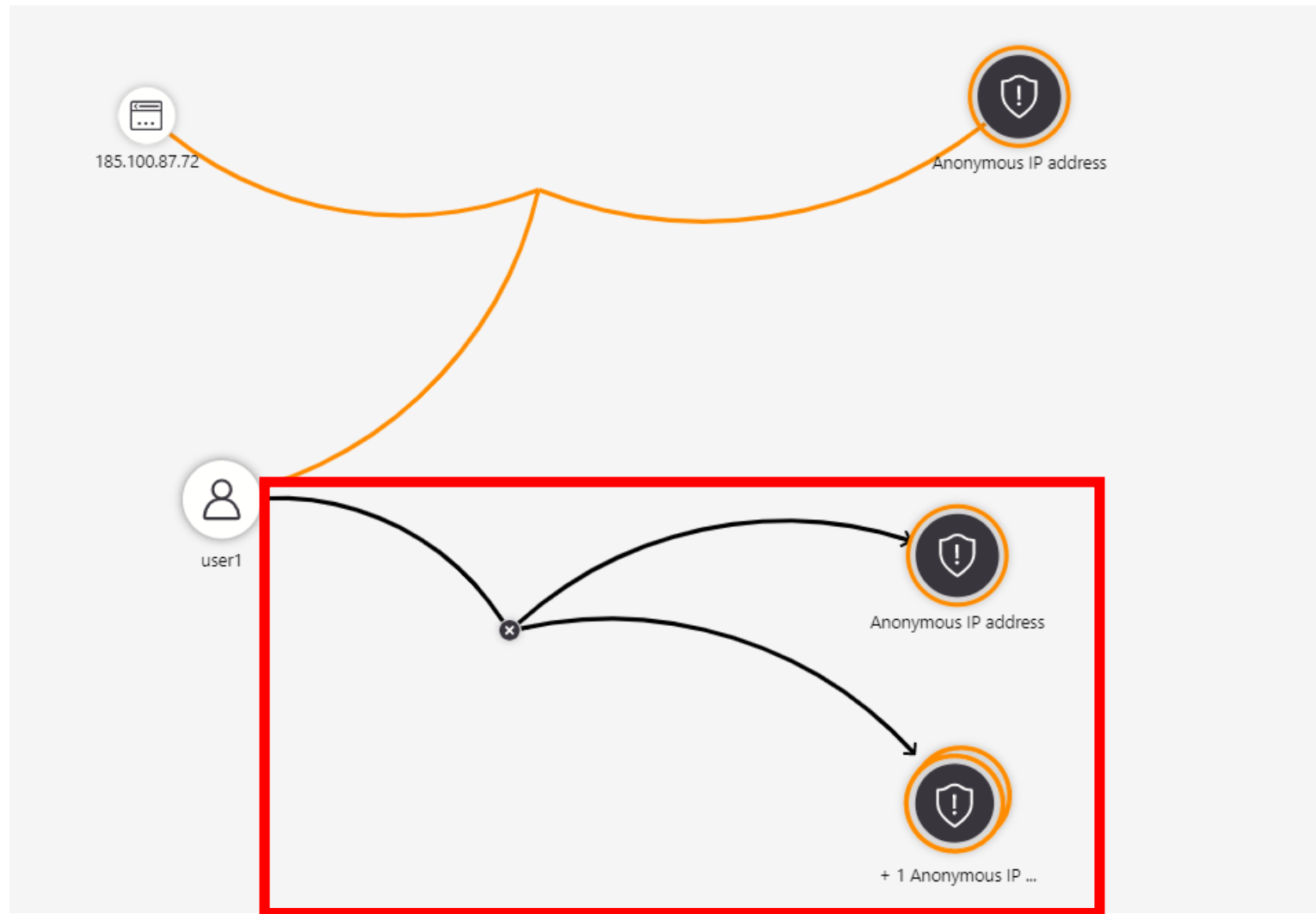
Hosts triggering Microso... (0) イベント>

詳細

エンティティをクリックし、「Related alerts」を選択



関連するアラート（インシデント）が「調査グラフ」に追加される。
このユーザーが、匿名IPアドレスを使って、何度もサインインしていることが判明する。



オートメーションルールの 作成

インシデント対応を自動化

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

既定のディレクトリ

ホーム > Microsoft Sentinel > Microsoft Sentinel >

インシデント ...

インシデント ID 2

最新の情報に更新

Anonymous IP address

インシデント ID: 2

未割り当て所有者

新規状態

中重大度

説明

Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)

製品名のアラート

Azure Active Directory Identity Protection

証拠

該当なし 1 イベント

1 アラート

0 ブックマーク

最終更新時間

21/12/22 22:11

作成時刻

21/12/22 22:08

エンティティ (2 個)

user1@test20...

185.100.87.72

すべての詳細を表示 >

方針 (1 個)

Initial Access

インシデントブック

インシデントの概要

分析ルール

Create incidents based on Azure Active Directory Identity Protection...

タグ

+

オートメーション ルールの作成 (プレビュー)

Team の作成 (プレビュー)

調査

操作

タイムライン

警告

ブックマーク

エンティティ

コメント

検索

タイムライン コンテンツ: すべて

増やす (2)

12月 22 22:08

Anonymous IP address

中 | Azure Active Directory Identity Protection

説明

Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)

重大度

中

状態

新規

製品名

Azure Active Directory Identity Protection

方針 (1 個)

Initial Access

システムアラート ID

5997dd60-5888-ef62-459...

規則名

--

最終更新時間

21/12/22 22:11

更新

0

開始時刻

21/12/22 22:08

終了時刻

21/12/22 22:08

アラートリンク

--

操作>

オートメーションルールの作成

インシデントに対する対応を自動化する「オートメーションルール」を設定できる

新しいオートメーション ルールの作成

オートメーション ルール名

Anonymous IP address

トリガー

インシデントが作成されたとき

条件

次の場合:

分析ルール名

次を含む

Create incidents ba...

および

アカウント名

次と等しい

user1

および

IP アドレス

次と等しい

185.100.87.72

+ 条件の追加

アクション ①

状態の変更

終了

無害な陽性 - 不害ですが、予期されています

コメント

インシデントを閉じると、関連付けられているチームがアーカイブされます。

適用

取り消し

この場合、ユーザーIDや
IPアドレスなどを使った
条件設定ができる

アクションの
種類を選択

アクション ①

状態の変更

プレイブックの実行

状態の変更

重大度の変更

所有者の割り当て

タグの追加

プレイブック
(Logic App) を実行

状態を「終了」にする
(インシデントを
閉じる)

オートメーションの作成

Logic Appsデザイナーを使用して、インシデント対応を自動化

「オートメーション」をクリック

ホーム > Microsoft Sentinel > Microsoft Sentinel



Microsoft Sentinel | オートメーション ...

選択したワークスペース: 'loga90182374'

検索 (Ctrl+/)



+ 作成



最新の情報に更新



編集



有効にする



上へ移動



下へ移動



削除



ガイドとフィードバック

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

コンテンツ管理



コンテンツ ハブ (プレビュー)



リポジトリ (プレビュー)



コミュニティ

構成



データ コネクタ



分析



ウォッチリスト



オートメーション



設定



0
オートメーション ルール



0
有効なルール



0
有効なプレイブック

オートメーション ルール (プレビュー)

アクティブなプレイブック

プレイブック テンプレート (プレビュー)



自動化ルールが見つかりませんでした

概要

自動化ルールを使用すると、インシデント処理のすべての自動化を一元的に管理できます。自動化ルールを使用すると、Microsoft Sentinel で自動化の利用が合理化され、インシデント オркестレーション プロセスの複雑なワークフローを簡素化することができます。

仕組み

自動化ルールは、インシデントの作成によってトリガーされます。インシデントとエンティティの詳細および分析ルールに基づいて、アクションを実行するタイミングを制御する条件を設定できます。アクションの順序とルールの有効期限を設定することもできます。

内容



インシデント構成の自動化

プレイブックを実行することなく、インシデントのステータスや重大度を直接設定したり、所有者を割り当てたり、インシデントの作成時にタグを追加したりします。



Microsoft プロバイダーのプレイブックをトリガーする

アラートから作成されたインシデントにルールを適用することにより、Microsoft セキュリティ アラートの処理を自動化します。



インシデントのプレイブックを実行する

自動化ルールからプレイブックを実行して、他のサービスと統合したり、複雑な



インシデント抑制の適用

ルールを使用して、偽陽性または無害な陽性と判明したインシデントを自動的に解決できます。たとえば、侵入テス

「インシデント トリガーを使用したプレイブック」を作成

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+/I)

ホーム > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | オートメーション ...

選択したワークスペース: 'loga90182374'

検索 (Ctrl+/) << + 作成 > 最新の情報に更新

全般

- 概要
- ログ
- ニュースとガイド

作成管理

- オートメーション ルール (プレビュー)
- インシデント トリガーを使用したプレイブック
- アラート トリガーを使用したプレイブック
- 空のプレイブック

プレイブック名を入力

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

プレイブックの作成 ...

① 基本 ② 接続 ③ 確認と作成

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 * wkspcrg ▼
[新規作成](#)

リージョン *
米国東部 ▼

プレイブック名 *
playbook1 ✓

☐ Log Analytics で診断ログを有効にする ①

Log Analytics ワークスペース
loga90182374 ▼

☐ 統合サービス環境との関連付け ①

統合サービス環境
▼

次: 接続 >

「次：確認と作成」をクリック

ホーム > Microsoft Sentinel > Microsoft Sentinel >

プレイブックの作成 ...


✓ 基本

2 接続

③ 確認と作成

このプレイブックで使用するコネクタごとに、別のプレイブックからの既存の接続を使用することを選択できます。それ以外の場合は、プレイブックのデプロイ後に Logic Apps デザイナーに戻ったときに、新しい接続を作成して認証する必要があります。

▼

 Azure Sentinel

マネージド ID を使用して接続する

前へ

次: 確認と作成 >

「デザイナーを作成して続行」をクリック

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

プレイブックの作成 ...

✓ 基本


✓ 接続

3 確認と作成


基本

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	wkspcrg
リージョン	米国東部
プレイブック名	playbook1
診断ログ ワークスペース	無効
統合サービス環境	無効

接続

 **Azure Sentinel**

マネージド ID を使用して接続する

 注: デプロイ後にマネージド ID にアクセス許可を付与します。

前へ

デザイナーを作成して続行

「Microsoft Sentinelのインシデントの発生時に、Microsoft Teamsにメッセージを投稿する」といった自動対応を設定することができる。

ホーム > Microsoft Sentinel > Microsoft Sentinel > playbook1

playbook1 | ロジック アプリ デザイナー

ロジック アプリ

検索 (Ctrl+/)

保存 破棄 トリガーの実行 デザイナー コード ビュー パラメーター テンプレート コネクタ

概要

アクティビティ ログ

アクセス制御 (IAM)

タグ

問題の診断と解決

開発ツール

ロジック アプリ デザイナー

ロジック アプリ コード ビュー

バージョン

API 接続

クイック スタート ガイド

設定

ワークフロー設定

承認

アクセス キー

ID

プロパティ

ロック

監視

警告

メトリック

When Azure Sentinel incident creation rule was triggered (プレビュー)

操作を選択してください

teams

おすすめ すべて ビルトイン 標準 エンタープライズ カスタム

Acti

Asite (US Gov.)

Azure DevOps

ClickUp Team Manager...

Derdack SIGNAL4

GroupMgr

HipChat

トリガー

アクション

もっと見る

Microsoft teams

チャットの作成
Microsoft Teams

チャットまたはチャンネルでメッセージを投稿する
Microsoft Teams

チャットやチャンネルにアダプティブ カードを投稿する
Microsoft Teams

チャット一覧を作成
Microsoft Teams

チャンネルの一覧表示

Microsoft Sentinel まとめ

■ 概要

クラウドネイティブな SIEM(分析) / SOAR(対応)ソリューション。

SIEM: セキュリティ情報イベント管理

SOAR: セキュリティ オークストレーション自動応答

■ Log Analyticsワークスペース

Log Analyticsワークスペースを作成し、Microsoft Sentinelを「追加」する。

■ データコネクタ

Azure、Microsoft 365、その他のクラウド等の「データソース」に接続して情報を集めることができる。
様々なデータソースに接続するため、120の「データコネクタ」が提供されている。

■ インシデント

検出されたアラートは「インシデント」として登録される。

例: 匿名IPアドレスからのサインイン (Identity Protectionで検出)

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る。

■ 調査グラフ

インシデントに含まれるエンティティ（関連データ。IPアドレスやユーザーIDなど）を線でつないで表示。
エンティティをクリックして関連するアラートを調査グラフに追加することができる。

■ 自動対応

「セキュリティプレイブック」（Logic Apps）を使用して、インシデントに自動対応できる