TIS
TIS INTEC Group

Microsoft Sentinel向け 活用サービス

ハイブリッドクラウド／マルチクラウド環境でのセキュリティログ監視＆運用を実現するMicrosoft Sentinel(旧：Azure Sentinel)の導入サービス。短期間でのSIEM導入を実現します。

既存SOCのよくある課題

ログ収集	脅威の検出	インシデント調査	対処
ログが際限なく溜まる	どれが脅威かわからない	原因が特定できない	件数が多く対処が大変

Microsoft Sentinelなら

必要分だけ利用できるログ領域	AIを使った脅威検出	GUIによる簡単調査	Playbookによる自動対処

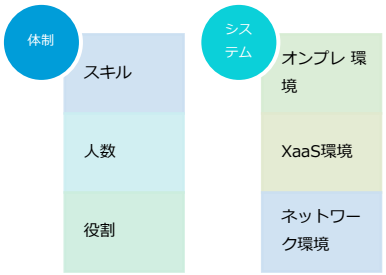
セキュリティの専門家じゃなくても使えるCloudSIEM

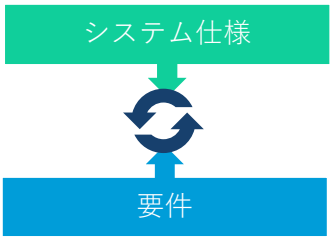
Microsoft Sentinelによる次世代SOCの実現

Microsoft Sentinelの活用に必要なさまざまな支援サービスを TISのCloud & Securityの知見を元にご提供します

アセスメントサービス

システム面と体制面から現状の分析を行い、導入プラン策定のご支援をいたします。





導入計画案
- 分析対象一覧
- 分析機能一覧
- 構成概要図
- 運用体制概要図
- スケジュール案

導入タスク一覧
- 課題一覧
- 運用課題一覧

ヒアリング 2weeks → ディスカッション 4weeks → Output 2weeks

導入サービス

Microsoft Sentinelの構築および操作説明を行います。

2つのメニューから選べる

スタートアップサービス

- Azureログソース３つまで対応
- ログソース取込設定
- 管理者ロール設定
- 操作説明（簡易）

エンタープライズサービス

- Azureログソース無制限
- ログソース取込設定
- 管理者ロール設定
- 外部ログソース取り込み
- 個別ルール作成、Workbook作成
- Playbook作成
- 個別手順書作成
- その他スクリプト開発

サポートサービス

お客様が運用される上で必要となるサービスを幅広くラインナップしております。

QAサービス

操作方法、アラート内容に対するQA。Chatbotによる即時対応（ComingSoon）

オリジナルルール提供

TIS独自の脅威情報、脆弱性を元にAzureMLを利用したオリジナル分析を提供

スポットサービス

スポットでの操作説明、レポート作成、Workbook,Playbookの作成支援

IR・フォレンジック対応

インシデント発生時のオンサイト、リモート支援

TIS TIS INTEC Group

TIS株式会社 IT基盤技術事業本部 IT基盤技術事業部
〒135-0061 東京都江東区豊洲２-２-１ 豊洲ベイサイドクロスタワー
Tel.050-1702-4063 E-mail. ps-info@ml.tis.co.jp