"Your Best Partner"
NISSHO ELECTRONICS

MSS for SIEM
- Microsoft Azure Sentinel -

標的型攻撃や内部不正を早期検知する統合監視を実現します

クラウドサービス活用の加速や、標的型攻撃の多様化・高度化に起因し、
広範なアタックサーフェスを統合監視するSIEM(セキュリティ情報イベント管理)に注目が集まってます。

セキュリティ課題	SIEMによる対応
標的型攻撃の多様化・高度化 典型的なパターンに当てはまらない未知の脅威の存在や、年々高度化していく手口に対応することが難しい。	**あらゆる情報を集めて異変を察知** 様々なデータソースから収集したログの相関分析や時系列分析により、普段とは異なる"異常"な行動を検出します。
従業員による不正行為への対策 従業員による内部不正や不注意による情報漏洩など、社内のコンプライアンス対策への負荷も高まっている。	**迅速な検知と対応** 「侵入の防止」ではなく、万一の侵入や内部不正に備えた迅速な検知と早期対応に注力し、被害を最小限に抑える。

SIEM導入／運用に必要な作業

SIEMツールの選定だけではなく、運用を前提にした設計と運用のPDCAを高速に回す必要があります。

要件定義	設計	構築	運用
・何を目的にSIEMを導入するのか？	・何をログソースにするのか？ ・どのようなルールで検知するのか？	・どのようにルールを作成するのか？ ・サイジングはどうするのか？	・アラートは本当に攻撃か？ ・検知された脅威への対応策はどうするのか？

SIEMを運用するための人材確保にお悩みではありませんか？

日商エレクトロニクスは、当社のセキュリティエンジニアが
お客様環境を**24時間365日体制**で監視を行うサービスを提供します。

日商エレクトロニクスのMSS for Azure Sentinelの特徴

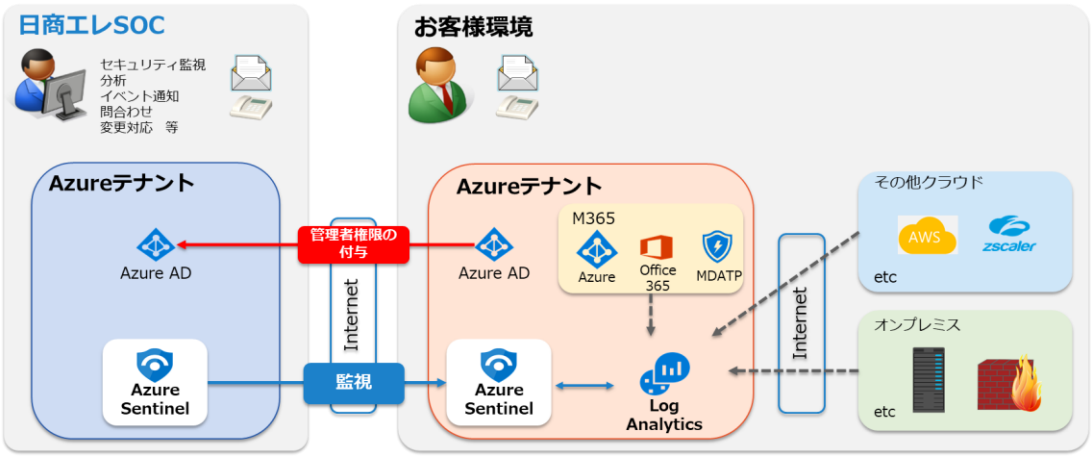
- **日商エレのSOCが24時間365日体制でアラートを監視**
- **お客様に合わせた3つのサービスプランを用意**
- **アナリスト独自の分析による誤過検知の削減・対策案の提示**

サービスフロー

お申込み → 現状調査 → 開通作業 → 契約書送付 → サービス開始

サービスイメージ

お客様のAzure Sentinel を監視し、検知されたアラートの分析および対応策の検討・通知などを24/365体制で行います。



サービスメニュー

・Basic / Standard / Premium の3つのプランをご用意しております。
・初期費用の中には、Sentinel環境の設計・構築作業費が含まれています。
　既にSentinel環境をお持ちのお客様は、別途御見積させていただきます。

メニュー	概要	Basic	Standard	Premium
簡易分析及び通知	Microsoft Azure Sentinelのセキュリティ検知ルールを対象とした分析及び推奨対応案を通知します。	○	○	○
詳細分析	インシデントの影響範囲や発生経路の特定に向けた分析を実施します。	○	○	○
カスタムルール作成／更新	運用中に、独自のルールをアナリストが必要に応じて追加します。セキュリティ状況の変化に合わせて、作成したルールの更新を行います。	×	○ ※1	○ ※2
誤／過検知チューニング	導入時および運用時に誤／過検知チューニングを実施します。	○	○	○
月次レポート	担当アナリストが一ヶ月分のイベントを分析し、レポートのコメントを追記し、提出します。	○	○	○
問合せ対応	通知・対応内容に関する問合わせ対応をいたします。	○	○	○
参考価格		**Basic**	**Standard**	**Premium**
初期費用	初期導入概算費用	￥2,800,000	￥3,600,000	￥3,600,000
月額費用	月額運用概算費用	￥1,800,000	￥2,400,000	￥2,800,000
オプション	ログソース追加		￥600,000	

※1 推奨ルール範囲内を対象とします。
※2 標準ルール範囲外も対象にします。

＊上記価格は参考価格であり、対象ログソースやカスタムルール数などにより価格が変動します。
＊見積もりにはお客様にヒアリングシートを記載して頂く必要があります
＊原則年間契約／一括支払いとなります。
＊記載されている会社名、製品名等は各社の商標もしくは登録商標です。
＊本チラシは、2021年10月現在の情報です。サービス内容は予告なく変更となる場合があります。

Azure Sentinelとは?

・Microsoft 社が提供するクラウドネイティ ブのSIEM機能とSOAR（Security Orchestration Automation and Response）機能を兼ね備えた統合セキュリティ監視サービスです。
・Microsoft365、Microsoft Azureと親和性が高く、Office365 の監査ログ、Azureのアクティビティログ、Microsoft Defenderソリューションから無料でログ取得を行うことが可能です。
・その他クラウド、オンプレミス製品からもログ を収集し、相関分析・横断的な検索に加え、統合アラート管 理が可能です。

MSS for Microsoft Azure Sentinel についての詳細は下記のサイトをご参照ください。
https://cloud.nissho-ele.co.jp/security/ms_azure_sentinel/

本パッケージに関するお問合せ先：
日商エレクトロニクス Azure担当　【E-mail】azure@nissho-ele.co.jp