報道資料

SB Technology

2020年10月27日

SIEM構築支援サービス for Azure Sentinel、11月2日より提供開始

～クラウドネイティブなセキュリティ対策を自社運用で実現、最適な構築メニューを提供～

SBテクノロジー株式会社（本社：東京都新宿区、代表取締役社長 CEO：阿多 親市、以下SBT）は、日本マイクロソフト株式会社（以下 マイクロソフト）が提供するクラウドネイティブなSIEM[*1]ソリューション「Azure Sentinel」の導入支援を行う『SIEM構築支援サービス for Azure Sentinel』の提供を11月2日より開始することをお知らせします。

導入支援のサービスメニュー一覧

Azure Sentinelは、大きく下記の3つの特徴をもつクラウドネイティブのセキュリティ運用ソリューションです。

- SIEM機能：あらゆるイベントログを一元管理し相関分析を行うことで脅威を検知
- SOAR[*2]機能：各種脅威情報の統合からインシデント対処まで運用の自動化を実現
- UEBA[*3]機能：人(User)やモノ(Entity)の行動(Behavior)を解析(Analytics)することによって、その人(モノ)が通常とらないような異常な行動を発見

Azure Sentinelを活用することで、セキュリティインシデントのアラート検知・分析・対応を高速化し、かつ運用を自動化することができます。

一方で、Azure Sentinelの利用を開始するには、ログ収集・分析におけるルール設定や、運用自動化のためのSOAR構築など、セキュリティに対する知見やノウハウが求められます。そのため、セキュリティ専任の担当者がいない企業にとっては自社だけでの導入は難しい場合があります。

『SIEM構築支援サービス for Azure Sentinel』は、ログ収集やアラートルールなど初期構築に必要な作業をメニュー化し、各種設定をスムーズに行います。また、企業自身での運用が可能となるようトレーニングも実施します。運用支援においてもAzure Sentinelを使い続ける上で必要となる支援サービスを提供予定です。(2021年1月提供開始)。

■背景

ミック経済研究所の「情報セキュリティマネージド型・クラウド型サービス市場の現状と展望 2020 年度版」によると、SIEM 運用サービスの売り上げ規模は、2019 年度が前年対比 130.8%の 25.5 億円、2020 年度は同 123.5%の 31.5 憶円と予想されています。2016 年頃から CSIRT やプライベート SOC を設置する企業が大幅に増えており、その際に複雑化するセキュリティ機器やソフトウェアなどのログを収集・分析する SIEM を導入することが多くなっています。そのような中、SIEM を自社で運用できないというケースが少なくないため、運用サービスの利用が拡大しています。

Azure Sentinel は SIEM 機能を持つだけでなく、自社運用に適した SOAR 機能による自動化、UEBA 機能を用いることで勤怠常用分析などコンプライアンス観点でのログ分析も行うことができ、従来のセキュリティ対策より広い範囲での分析が可能となります。

*1 SIEM：Security Information and Event Management（セキュリティ情報イベント管理）
*2 SOAR：Security Orchestration, Automation and Response（セキュリティオーケストレーション自動応答）
*3 UEBA：User and Entity Behavior Analytics（ユーザー、エンティティの振る舞い解析）

■エンドースメント

本サービスの提供開始について、日本マイクロソフト株式会社よりコメントをいただいています。

この度の SB テクノロジー株式会社様の『**SIEM 構築支援サービス for Azure Sentinel**』の提供開始を心より歓迎いたします。多くの企業がニューノーマルに対応した新しい働き方にシフトしていく中で、セキュリティの新しい課題に直面しています。Azure Sentinel は、クラウドの有用性を持ちながら、企業全体のセキュリティをインテリジェントに分析し、AI によりセキュリティ運用におけるユーザーの負担を軽減します。

SB テクノロジー株式会社様のクラウドの技術力により、お客様の課題に合わせた最適な構築を提供されることで、ニューノーマルに対応した新しいセキュリティ対策を実現できるものと確信しております。

今後も日本マイクロソフトは、SB テクノロジー株式会社様との連携を通じて、お客様のセキュリティ対策を支援してまいります。

日本マイクロソフト株式会社 パートナー事業本部 副事業本部長 業務執行役員 近藤 禎夫

■SBT の強みであるクラウドの知見を掛け合わせたセキュリティサービス

SBT は「Cyber Resilience（サイバーレジリエンス）を顧客と共に実現する」をセキュリティ事業のミッションに掲げ、様々なセキュリティサービスを提供しています。お客様のシステムを止めず、インシデントの被害を最小限に防ぎ、本業（サービスやシステム）の復旧を早めるために、セキュリティ機器・サービスの導入だけでなく、脅威の分析・封じ込めまで行う MSS（マネージドセキュリティサービス）、セキュリティコンサルティング、CSIRT 構築支援サービスなどを提供しています。

■『SIEM 構築支援サービス for Azure Sentinel』の詳細はこちらをご覧ください。

https://www.softbanktech.co.jp/service/list/microsoft-azure/azure-sentinel/

報道関係者様向け お問い合わせ窓口	SB テクノロジー株式会社 経営企画本部 経営企画部 コーポレートコミュニケーショングループ（吉田、與儀）
	Email：sbt-pr@tech.softbank.co.jp