Press Release

アルプス システム インテグレーション株式会社 広報事務局
03-6427-1627

2021年10月7日

従業員の行動分析を低価格で実現
Sumo Logicで「異常行動分析オプション」を提供開始
～セキュリティ専門人材不足の企業でも内部不正対策がスムーズに～

アルプス システム インテグレーション株式会社(本社:東京都大田区、代表取締役社長:永倉 仁哉、以下ALSI〔アルシー〕)は、同社が販売するクラウドSIEMソリューション「Sumo Logic(スモー ロジック)」のオプションとして、従業員の異常行動分析のためのログ活用コンサルティングを提供開始いたします。

テレワークの拡大・継続により、企業におけるセキュリティ対策は外部からのサイバー攻撃への対策に加えて、従業員によって情報が盗み出される内部不正への対策もより重要な課題となっています。

内部不正への対策には従業員の異常行動の検知・分析が不可欠です。本オプションは、従来は管理が難しく高額だった異常行動分析を、Sumo Logicで取得するログの活用によって、低価格かつシンプルな形で実施することができます。また本オプションで作成する異常行動分析ダッシュボードにより、セキュリティ専門人材の少ない情報システム部門でも、手軽に従業員のリスクある行動の分析を可能とします。

【サービス概要】

サービス名	Sumo Logic「異常行動分析オプション」
提供開始日	2021年10月7日
強み	• 既存のユーザー行動分析(UEBA※)に比べて低価格でシンプルに実施することができる • 導入時の難しい定義、設定、チューニングを ALSI のコンサルティングにより支援 • オリジナルダッシュボードにより従業員の異常行動をいち早く発見し対策ができる
ターゲット	• 従業員の行動分析を検討している企業 • 内部不正による情報漏洩対策を検討している企業 • セキュリティ人材の育成、確保にお困りの企業
提供価格	50万円(税別)～　※ヒアリングからダッシュボード作成、利用開始まで
詳細情報URL	https://www.alsi.co.jp/industry/blog/article/2202/index.html

※User and Entity Behavior Analytics:ユーザーおよびエンティティのふるまい検知

【従業員の異常行動分析をする上での課題】

従業員の異常行動を的確に検出することは難しく、多様な課題が存在しています。例えばよくある失敗として、各部門における通常の従業員の行動を把握できていないために、単純にファイルのダウンロード数が多いだけで異常行動と判断してしまう、などが挙げられます。

業務の都合上、たまたま資料のダウンロード回数が多くなることや、業務内容によって普段から他の従業員よりも資料ダウンロード回数が多い、というようなことは往々にして発生します。

なにをもって異常行動と判断するのか、その定義は従業員の業務内容やその時の状況によって異なります。異常行動の分析のためには、まずは平常時に各従業員がどのような動きをしているのかを把握・分析して、「正常」「異常」の定義を明確にすることが必要です。そのために有用なのがUEBAですが、UEBAはセキュリティの高度な専門知識をもつ人材が必要なうえ、高額な費用がかかる傾向があります。

本件に関する報道関係者からのお問い合わせ先

アルプス システム インテグレーション株式会社　広報事務局(株式会社カーツメディアワークス)
担当:和田、佐藤　TEL:03-6427-1627　FAX:03-6730-9713　E-mail:contact@kartz.co.jp

アルプス システム インテグレーション株式会社　管理部　広報担当　黒澤 宏子
TEL:03-5499-8043　FAX:03-3726-7050　E-mail:hiroko.kurosawa@alsi.co.jp
〒145-0067 東京都大田区雪谷大塚町1-7　URL: https://www.alsi.co.jp/

Press Release

アルプス システム インテグレーション株式会社 広報事務局
03-6427-1627

2021年10月7日

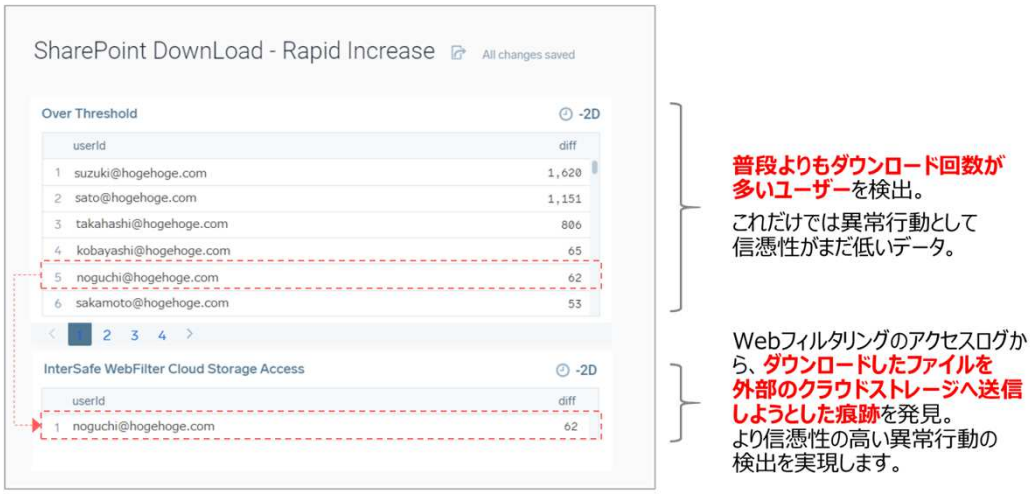
Sumo Logic「異常行動分析オプション」

　このたび提供を開始する「異常行動分析オプション」は、Sumo Logicで収集できる各種システム、アプリケーション、サービスなどのログを分析・可視化して従業員の異常行動を分析するサービスです。導入時の複雑な設定や、各企業に合った異常行動の定義、チューニングなどをコンサルティング支援し、従来のUEBAと比較して低価格かつシンプルな形で行動分析を開始することができます。
　また本オプションでは企業ごとのポリシーや業務内容にあわせたオリジナルダッシュボードを作成します。各種ログの分析により平時の従業員の行動を把握し通常時の値を定義することにより、閾値を超えた異常行動の検出を実現します。

主な支援内容
- 適切な分析が可能なログの選別
- 各企業に合った異常行動の定義
- 分析クエリ(分析用オリジナルダッシュボード)の開発

■異常行動オプションのユースケース:クラウドの共有サーバー × Webフィルタリング

　クラウドの共有サーバー(SharePoint Online)内の機密情報を扱うサイトから、普段よりも多くのファイルをダウンロードしたユーザーを検出します。
さらに、Webフィルタリング(InterSafe WebFilter)のアクセスログを照合して、外部クラウドストレージへのアクセス形跡を調査します。
　このように複数のログを参照することで、機密データをダウンロードして外部に持ち出そうとしている可能性が高いと判断することができます。



< Sumo Logic ダッシュボード(管理画面)イメージ >

■「Sumo Logic」について

「Sumo Logic」はSumo Logicジャパン株式会社が提供する、あらゆるログを取り込み一元化しリアルタイムな相関分析を行うクラウドSIEM(Security Information and Event Management)ソリューションです。企業の重要な情報資産であるログを、情報システム部門の負担を軽減しながら活用し、サイバー攻撃や内部不正への対策、ワークスタイルの変革などへの適用を実現します。

■アルプス システム インテグレーション株式会社について

　アルプス システム インテグレーション株式会社(ALSI〔アルシー〕)は、電子部品と車載情報機器の総合メーカー アルプスアルパイン株式会社のグループ会社として、1990年に設立しました。製造業の現場で培った「ものづくり」の思想を原点に、「デジタルソリューション」「セキュリティソリューション」「ファームウェアソリューション」「IoTソリューション」を展開しています。今後もALSIは、IT環境の変化に素早く柔軟に対応し、お客様の企業競争力強化と業務改革に貢献してまいります。

本件に関する報道関係者からのお問い合わせ先

アルプス システム インテグレーション株式会社　広報事務局(株式会社カーツメディアワークス)
担当:和田、佐藤　TEL:03-6427-1627　FAX:03-6730-9713　E-mail:contact@kartz.co.jp

アルプス システム インテグレーション株式会社　管理部　広報担当　黒澤 宏子
TEL:03-5499-8043　FAX:03-3726-7050　E-mail:hiroko.kurosawa@alsi.co.jp
〒145-0067 東京都大田区雪谷大塚町1-7　URL: https://www.alsi.co.jp/