CASE STUDY —導入事例—

サワイグループホールディングス株式会社様

次世代SIEMプラットフォーム Exabeam

「UEBA（User Entity Behavior Analytics）として自動的に怪しい行動を検知してくれる」、「コスト面の優位性」、「クラウドサービスである」ことなどが採用のポイントになりました。

サワイグループホールディングス株式会社様のご紹介

サワイグループホールディングス（以下、サワイグループ）は、沢井製薬株式会社の持株会社体制への移行に伴い、2021年4月1日に設立された純粋持株会社です。企業理念「なによりも健やかな暮らしのために」のもと、グループ全体の事業戦略の策定や経営管理を通じて、社会とともに持続的に発展するヘルスケア企業グループを目指しています。

国内外での事業内容を教えていただけますか

サワイグループは、ジェネリック医薬品を中心とした医療用医薬品の製造販売を日本国内および米国で展開しています。

日本国内では、グループの中核企業である沢井製薬を中心に、ジェネリック医薬品を中心とした医療用医薬品の製造販売を展開しています。患者さんの負担軽減と医療費削減に貢献するなど、ジェネリック医薬品のリーディングカンパニーとしての地位を確立しています。

米国においては、グループ会社のUpsher-Smith Laboratories が、ジェネリック医薬品を中心とした医療用医薬品の製造販売を展開しています。

また、グループの中核事業であるジェネリック医薬品の安定供給とともに、IT・デジタル分野をはじめとした多様なプレーヤーとの協働を通じて、従来の治療薬の枠を超えた高度な価値を有する製品・サービスの提供にも積極的に取り組んでいます。

検討のきっかけや背景を教えていただけますか

サワイグループでは情報セキュリティ対策として、各種の攻撃に対応するセキュリティシステムを目的別に導入してきております。そのため、それぞれのセキュリティシステム単位で、監視運用・検出されたインシデント対応を行っております。

攻撃手法は常に進化・多様化しており、複数のセキュリティシステムのログを横断した調査が必要なケースも増加しており、調査・対応完了までに長時間を要することもあります。また、各システムごとの操作方法を習得する必要があることも運用負荷の増加を招いております。

このような状況を改善するために、一元的にセキュリティログを監視でき、かつ柔軟な解析（既存のデータベースと連携など）が行える製品を導入し、セキュリティ管理業務の精緻化、迅速化、効率化を図ることを検討しました。

社内にどのような課題や問題がありましたか

情報セキュリティ対策に関わる運用負荷の増大とともに、社外のビジネスパートナとの情報共有を安全・安心に行えるようにしつつ、それに伴う情報漏洩リスクを極小化させることが課題としてありました。特に、メールやインターネット上の共有ディスクを、業務上必要な場合にだけ利用できるようにする対策やUSBメモリなどリムーバブル媒体へのデータ書き出しを制限することが喫緊の課題でした。また、日常とは異なる操作や挙動がPC上やサーバに対して発生した場合に、それらを不正アクセスと捉え、早期に検知するような仕組み（振る舞い検知型システム）の導入が求められていました。

サワイグループ
ホールディングス株式会社
グループIT部
グループIT・インフラG
江口 隆文 氏

サワイグループ
ホールディングス株式会社
グループIT部
グループIT・インフラG
マネージャー
木戸 繁之 氏

サワイグループ
ホールディングス株式会社
グループIT部　部長
竹田 幸司 氏

サワイグループホールディングス株式会社

■所在地
大阪市淀川区宮原5丁目2-30

■設立
2021年4月1日

■資本金
100億円

■従業員数（2021年3月末現在）
3,003名<連結>

■代表者
代表取締役社長
末吉 一彦

どのような解決策を検討しましたか

情報セキュリティ対策の専門組織であるSOC（Security Operation Center）を導入して監視することも検討しましたが、かなりのコストが発生しますので、自社内で運用できる方法として、各種ログから不審な動きやその兆候を早期に検知して被害を最小限に抑えることができるSIEM（Security Information and Event Management）製品やサービスの導入を検討しました。

他社サービスを検討しましたか

多くの実績を持つ各社のSIEM製品およびサービスとExabeamを比較検討しました。また、SOCにおいて活用したパターンも検討しました。

Exabeam製品採用のポイントや決定打はどのようなところでしたか

「UEBA（User Entity Behavior Analytics）として自動的に怪しい行動を検知してくれる」、「コスト的にも最も安価に目的を達せられる」、「クラウドサービスである」ことなどが採用のポイントになりました。

UEBAは、ユーザーやEntity（機器等）の正常な振る舞いを機械学習し、怪しい行動を異常な振る舞いとして自動的に検知する技術です。これにより、内部不正や内部に潜んでいる脅威の予兆を検知してくれます。

また、ExabeamはクラウドにSIEMとUEBAプラットフォームを構築するSaaSサービスとして提供されますので、ハードウェアやインフラに関する管理・運用やハードウェアのセットアップなどが不要となり、コストを抑えたかたちで利用することができます。

さらに、実際には限られた人数で運用していくことになりますので、Exabeamの性能面やコスト面とともに、サポートサービスの内容なども採用のポイントになりました。

効果・効用をお聞かせください

メールなどを経由した情報漏洩対策として、パブリックドメインへの送信を検知するなど、送信者の上司が内容を確認できる仕組みを構築しました。不正アクセスについても、不正アクセスが疑われる不審な動きや兆候が生じた場合に、迅速にその状況を現場へ確認するなどの対応を行えるようになりました。

今後の展開についてお聞かせください

Exabeamを活用し、まずはログの収集・一元管理・不正攻撃やセキュリティ脅威の早期検知・解析・迅速な対応を行えるようにしました。今後は、セキュリティ脅威の予兆検知・解析された結果からインシデント対応を自動化できるような形に運用を拡充して行きたいと思っております。そして、Exabeamをサワイグループのセキュリティ対策の要として、拡充・連携を進めていきます。

Exabeam導入前の主な課題や問題点

情報漏洩リスクの極小化
- メールやインターネット上の共有ディスクを業務上必要な場合にだけ利用できるようにすること
- USBメモリなどのリムーバブル媒体へのデータ書き出しを制限すること

不正アクセス対策
- 日常とは異なる操作や挙動がPC上やサーバに対して発生した場合に早期に検知すること

Exabeam導入による効果・効用

- メールなどを経由した情報漏洩対策として、パブリックドメインへの送信を検知するなど、送信者の上司が内容を確認する仕組みを構築した
- 不正アクセスが疑われる不審な動きや兆候が生じた場合に、その状況を現場へ確認するなどの対策を行えるようになった

次世代SIEMプラットフォーム Exabeam

Exabeam Platformは、セキュリティ運用の構成要素であるCollect（ログの収集）→ Detect（攻撃の検知・解析）→ Respond（インシデント対応）の運用要素をより効率的・効果的にするためのセキュリティプラットフォームです。クラウドベースでログ（各種情報）収集／保存から、UEBAによる分析、SOARと呼ばれるツールによって、Playbook（タイムラインストーリー）を作成し、インシデントに対して処理を予め自動化させることが可能になります。これによって、人的に行った場合のオペレーションミスなどを防ぐことが可能になります。

お問合せ

KEL KANEMATSU ELECTRONICS LTD.
兼松エレクトロニクス株式会社
〒104-8338　東京都中央区京橋2-13-10

GSX GLOBAL SECURITY EXPERTS
グローバルセキュリティエキスパート株式会社
〒105-0022　東京都港区海岸1-15-1　スズエベイディアム4F