セキュリティ製品から発せられる大量ログの相関分析を自動化し属人化した運用体制から脱却

鴻池運輸株式会社はセキュリティ運用負担を軽減すべくExabeamを導入し、サイバーレジリエンス強化に取り組んでいます。

鴻池運輸について

鴻池運輸は、国内・国際物流をはじめ、鉄鋼・食品などの製造業界向けや医療・空港などのサービス業界向けの請負サービスなど、多角的に事業を手掛ける1880年創業の総合物流サービス企業です。同社ではサイバーレジリエンスを高めるべく、複数のセキュリティ対策ソリューションを導入していましたが、そこから発せられる大量のログを分析し、対応するまでに多くの工数を費やしていました。そこで、次世代SIEMプラットフォーム「Exabeam」を導入。アラート監視や相関分析の自動化を推進し、セキュリティ運用負担の軽減と内部不正対策の強化を実現しました。

導入以前の課題：セキュリティ対策ソリューションから発せられるログの分析工数が飛躍的に増加

1880年の創業から百数十年の歴史を持つ総合物流サービス企業の鴻池運輸株式会社（以下、鴻池運輸）。同社では、国内外のグループ全体を包括したセキュリティ対策に注力し、攻撃を未然に防ぐことは当然のこと、有事の際にも被害を最小限に抑えて早期の復旧を図ることができるサイバーレジリエンスの能力を高めることを目指しています。

同社 ICT推進本部 副本部長でありデジタルトランスフォーメーション推進部 部長を兼務する佐藤 雅哉氏は、「ICT推進本部が発足した2018年に私は鴻池運輸に入社していますが、率直なところセキュリティ対策はかなり遅れていると感じました。そこで、セキュリティ対策全般の見直しが必要と考え、外部からの攻撃に対する防御を強化するため、EDRやクラウドプロキシ、IDaaSなどの導入を進めてきました。さらに近年では、内部不正対策にも注力しています。」と話します。

こうしてセキュリティ対策の骨組みが整ってきたことから、同社では次のステップとしてセキュリティソリューションを最適に運用できるようSOCの体制を整えるとともに、有事の際の対応に備えたCSIRT構築も進めてきました。

ただ、そうした中に新たな課題が浮上してきました。それは、各セキュリティ対策ソリューションから発せられる大量のログを分析する工数が、相乗的に増加していたことです。

同社 デジタルトランスフォーメーション推進部 担当課長の戸松 聡氏は、「何らかのアラートを検知した際に、複数のソリューションからばらばらに上がってくるログを時系列で突き合わせ、相関関係を読み解かなければ、確かな根拠に基づいて原因にたどり着くことができません。ほぼ手作業となるためいつも大変な苦労をしてきました。」と話します。

続けて佐藤氏も「ログの相関分析を行える高度な知見とスキルをもったセキュリティ人材は、部内でも限られており、負荷が集中してしまったのです。」と語ります。

選定ポイント：セキュリティ運用負担を軽減するアラート監視や相関分析の自動化に着目

さっそく鴻池運輸ではSIEMソリューションの選定を開始し、2023年9月に次世代SIEM（Security Information and Event Management）ソフトウェアのExabeamを導入しました。

「実はExabeamについては以前から強い関心をもっており、情報収集を進めていました。SIEMの分野では他にも著名なソリューションが数多くありますが、比較検討したものは、どれも設定や運用は複雑なため、どのツールも使いこなすには相応の知識が必要で、負担軽減や属人化の解消にはつながらないと判断しました。これに対してExabeamは大量のログから瞬時にユーザーおよび機器単位のタイムラインを作成し、ログの相関分析を自動化するため、誰でも即座にアラート発生時の原因特定にあたることができます。」（佐藤氏）

さらに、AIを活用したUEBA（User and Entity Behavior Analytics）の機能による内部不正対策も、選定の大きなポイントになったと佐藤氏は続けます。

「Exabeam に搭載されているUEBAにより、ユーザーの通常の振る舞いと異常な振る舞いをスコアリングして動的に識別し、タイムラインに組み込んで独自のルールで監視できます。これによりセキュリティ運用負担を軽減するとともに、内部不正対策の強化も可能になります。」（佐藤氏）

導入後：セキュリティ運用負担を軽減して重要業務にリソースを集中

鴻池運輸では、2024年1月1日よりExabeamの正式運用を開始。現時点では、オンプレミス環境のActive Directory、Azure AD、ZscalerのZIA（クラウドプロキシーサービス）/ZPA(リモート接続サービス)、CrowdStrike、Oktaといったセキュリティ対策ソリューションのほか、Microsoft 365などのSaaS型アプリケーションからもログを取り込んで監視や分析を行っています。

「Exabeamの導入を機に、多岐にわたるセキュリティ対策ソリューションやアプリケーションから大量のログを収集するようになったため、アラート監視や相関分析といった作業の絶対量が増えているため工数を単純に比較することはできません。ただし、そうした作業は現在までに、すべてSOCチームに移管されています。これに伴い私個人の作業工数はゼロになりました。」（戸松氏）

続けて佐藤氏は「Exabeamの本質的な導入効果は、単なる工数削減ではありません。

> **「Exabeamの本質的な導入効果は、単なる工数削減ではありません。私たちが最大の成果と考えているのは、ログ分析の属人化を解消し、負担の重い作業から解放できたことにあります」**
>
> **— ICT推進本部 副本部長兼デジタルトランスフォーメーション推進部 部長**
>
> **佐藤 雅哉 氏**

セキュリティ対策には決して終わりはなく、ますます巧妙化・悪質化していく攻撃者の最新動向を常にキャッチアップしながら、先手を打った見直しを図っていかなければなりません。そういった今後のセキュリティ戦略立案などの重要な業務に注力するリソースを割くことが可能となりました。」と語ります。

今後の展望：セキュリティ人材の底上げを図り、サイバーレジリエンスのさらなる強化を目指す

Exabeamの運用が軌道に乗り始めた鴻池運輸では、さらなるセキュリティ強化に向け社内のセキュリティ人材の育成に注力する方針です。

「Exabeamで一元管理された大量ログの監視業務を移管できたことで、SOCチームの中にもログデータの相関分析や、セキュリティインシデント発生時の原因特定など、高度な知識やスキルをもつ人材が育ちつつあります。今後に向けても実践的なノウハウをもったセキュリティ人材を社内でさらに増やし、層を厚くしていきたいと考えています。」（戸松氏）

さらにその先の展開として、鴻池運輸がグループ全体の経営視点から目指しているのは、サイバーレジリエンスの強化です。佐藤氏は「SOCの強化と共にCSIRTの構築も進めており、KONOIKEグループのどの拠点で攻撃が起こっても迅速に対処し、復旧できる強靭なシステムの運用体制を、できるだけ早期に確立したいと考えています。」と強調し、セキュリティ脅威の最新動向を捉えたサイバーレジリエンスのあるべき形を追求していく構えをみせました。

記事内の部署名、役職は取材当時のものです。

Exabeamについて

Exabeamは、AIを活用したセキュリティ運用を提供する世界的なサイバーセキュリティのリーダーです。高度なデータインジェスチョン、強力な分析、ワークフロー自動化により、脅威検知・調査・対応(TDIR)のための業界最先端のセルフホスティング型クラウドネイティブセキュリティ運用プラットフォームを提供します。

exabeam

詳細はこちら
www.exabeam.com/ja/ →