GA technologies、UEBA搭載のExabeamで事業拡大に伴う内部漏えい対策を強化

テクノロジーを活用し、不動産をはじめ、様々な産業のビジネス変革に取り組む株式会社GA technologiesでは、従業員が快適に働けるIT環境の整備とともに、事業拡大に伴う内部不正・情報漏えい対策の強化が課題となっていた。そこで同社が採用したのが、UEBA（機械学習による振る舞い検知）を活用し、少人数でも効率的な運用が可能なExabeam。AIによる自動追跡・分析機能により、インシデント発生後の調査や対応が大幅に効率化され、その効果を実感している。

事業拡大によるセキュリティ強化と従業員のIT環境の確保の両立が急務

GA technologiesでは、AI不動産投資「RENOSY（リノシー）」をはじめとした不動産サービスの開発・運営に加え、M&Aや金融分野へも事業を拡大。さらに、グループ会社を通じて国内だけでなく北米やアジアにも事業を展開し、サイバーセキュリティに求められる要件も高度化している。

「テクノロジー×イノベーションで驚きと感動を生み続ける」をミッションに掲げる同社では、従業員が働きやすいIT環境の実現を重視している。一方で、60万人を超える顧客を抱える不動産事業に加え、M&Aや金融など高い機密性が求められる事業が増加したことで、重要情報を保護するための内部不正対策のさらなる強化が急務となっていた。

UEBAにより少数で効率的に運用できるExabeamの導入を決定

GA technologiesがExabeamを採用した理由は、「従業員の行動を能動的に追跡・分析できること」「少人数でも効率的に運用できること」「従業員の利便性を維持できること」の3点だった。

内部不正リスクは年々多様化・複雑化している。同社では、SaaSやエンドポイントのログを保存するだけでなく、「内部ユーザーがどのような行動を取ったのかを継続的に追跡・分析できる基盤が必要だと考えていました」と、IT戦略／Corporate IT部長の椿郷史氏は語る。

ポイント

- Exabeamの導入により、従業員のIT環境を保ちつつ、少人数で効率的に内部漏えいに対するセキュリティを強化。
- UEBAが行動の追跡・分析をし、通常の行動パターンとの差異を自動スコアリングすることで、インシデント調査が大幅に効率化。
- ツールの強みを活かしたセキュリティ対策により、コストの最適化を実現。

Exabeamは、UEBAにより、手動で検知ルールを作成しなくても、通常の行動パターンとの差異を自動でスコアリングできる。そのため、同社が目指していた「少人数のセキュリティチームでも属人化せず運用できる体制」の実現につながった。また、複数のログを一元的に集約し、自動分析できる仕組みも、事業拡大を進める上で大きなメリットとなった。

さらに、従来から導入していたDLP（データ損失防止）などの情報漏えい対策を過度に厳格化することなく、ルールをすり抜けるようなグレーな行動も検知できることから、従業員の利便性を損なうことなくセキュリティを強化できると判断し、Exabeamの採用に至った。

自社業務に合わせたカスタマイズと短期間でスムーズな運用に注力した導入

同社がSIEM製品の比較・検討を開始したのは2025年1月。7月にPoV（概念実証）を実施し、12月に契約を締結。その後約2か月の構築期間を経て、2026年3月に本番運用を開始した。

導入時に苦労した点について、IT戦略／Security チーフの山田拓人氏は、「PoVの段階で、ルールやパーサーのチューニングというSIEM特有の地道な作業に直面したこと」だと振り返る。Exabeamには標準のパーサーや検知ルールが数多く用意されているが、「内部不正」を高い精度で検知し、効率的にインシデント調査を行うためには、自社の業務に合わせたカスタマイズが不可欠だった。そのため、ログの取り込みや初期チューニングなどの構築作業は外部へ委託し、社内では検知後の対応プロセスの設計に注力した。

経営層に対しては、外部脅威の大量ログはEDRで対応し、Exabeamは内部不正に関わるユーザー行動の分析に特化させるという役割分担を明確に示すことで、コストを最適化できることを説明し、スムーズに理解を得ることができた。

また、他部門との連携では、IT戦略部門だけで完結できる範囲から段階的に導入を進めることを重視。他部門の業務に影響を与えないよう、Google WorkspaceやSlackなど全社共通基盤を対象にスコープを限定することで、調整負荷を抑えながら短期間で本番運用へ移行した。

インシデント調査の効率が向上

Exabeamの導入により、「インシデント調査の効率は大きく改善しました」と椿氏は話す。

これまでは、アラートが発生するたびに複数の管理画面へログインし、それぞれのログを手作業で突き合わせる必要があった。しかしExabeamのタイムライン機能では、「ログイン」「Google Driveからの大量ダウンロード」「別のクラウドストレージへのアップロード」といった点在していたログが、一人のユーザーの行動履歴として時系列で可視化される。その結果、調査開始までの時間が大幅に短縮され、担当者を問わず迅速に状況を把握できる体制が整った。現在はGoogle Workspace、Netskope、SlackなどSaaSのログを中心に監視しているが、今後は自社開発アプリケーションやCRMなどへ対象を拡大し、内部不正対策のカバレッジをさらに強化していく予定だ。

ツールごとの強みを活かし、セキュリティを強化

サイバーセキュリティの理想は、すべてのログを一つのSIEMへ統合すること。しかし、その実現にはコストや運用負荷という課題が伴う。だからこそ重要なのは、すべてを一つのツールに任せるのではなく、EDRとSIEMそれぞれの強みを理解し、「何を検知したいのか」に応じて適切に役割を分担することだ。最後に椿氏は、次のように語った。「セキュリティを強化しながら、従業員の利便性は損ないたくない。そして運用コストも最適化したい。そうした課題を抱える組織にとって、Exabeamは有力な選択肢の一つになると考えています。」

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/ →