exabeam

ケーススタディ

EXABEAMの次世代SIEM活用によって

グローバルビジネスにおけるセキュリティの運用管理を最大化するNTTデータ社

NTTデータ社は、世界をリードする技術とサービスを提供するプロバイダーの1社です。同社は1988年に設立され、50以上の国と地域にて129,000名の従業員からなるグローバルチームを擁しています。NTTデータ社は、グローバルビジネスの成功へ向け、従来のシステムインテグレーターとしての役割からグローバルビジネスパートナーへの転換を進めています。従業員は日本事業部のみで34,500人を有し、行政や金融向けのサービス展開を主軸に、建設、不動産、製造、物流、小売、放送、メディア、広告、通信、運輸、およびエネルギー分野において、多くの顧客企業へサービスを提供しています。同社の株式はNTTデータ（TSE:9613）として上場取引されており、2019年3月31日時点の年間連結純売上額は、2兆1,000億円（189億USドル）でした。

「大企業である弊社にとって、Exabeamのフラットなユーザーライセンス課金体系のData Lakeと魅力的な価格モデルは際立った価値となりました。」

NTTデータ社 技術革新統括本部 システム技術本部 セキュリティ技術部長 本城啓史氏

NTTデータ社は急速な変革と成長戦略に伴い、数多くの企業買収を行いました。従来の技術プラットフォームの継承とシステム統合を行う上で、内部よりサイバーセキュリティとコンプライアンスの懸念が指摘されていました。

NTTデータ社 技術革新統括本部 システム技術本部 セキュリティ技術部長 本城啓史氏は次のように述べています。「当社のお客様、特に日本のお客様より、弊社のサービス、ソリューションに対して非常に高い期待をお寄せいただいており、何らかのセキュリティ問題があった場合、グローバルレベルの重大な影響、損害を引き起こす可能性があります。」

NTTデータ社セキュリティ部門のビジネス課題は、事業買収後に残った複数の旧SIEM（SECURITY INFORMATION AND EVENT MANAGEMENT/セキュリティ情報イベント管理）プラットフォームの管理でした。従来の機能では、過去5年で桁違いに急増している全ての運用とセキュリティデータを分析することはできませんでした。また、従来のSIEMはログ容量を基にした従量課金モデルのため、同社の大規模なグローバルオペレーションでは膨大なコストがかかりました。

「私達は、より優れた方法でリスクを検出、追跡し、全体像を把握できるソリューションが必要でした。また、ヨーロッパのGDPR（GENERAL DATA PROTECTION REGULATION/ EU一般データ保護規制）などの国際法規制へ準拠する必要があり、適切なITインフラストラクチャに投資を実施する機会でした。」と、本城氏は話します。

ベンダー選定

本城氏をはじめとした技術革新統括本部のセキュリティスペシャリスト達は、従来のSIEMによる相関ルールへの依存は、将来深刻な制約を引き起こすことを認識していました。

そのため、同社にとって、ルールベース検出を逃れる最新の脅威について詳細な可視性を得ることが不可欠でした。加え、従来の方法による検知、分析に費やされる作業を効率化するための機能も求めていました。

NTTデータ社は、複数の競合製品の中からEXABEAMを選択しました。評価基準は、価格モデル、機械学習とビックデータを活用するためのユーザーおよびエンティティの行動分析（UEBA）機能、サポート対象地域、および多言語対応などを含みました。

本城啓史氏は次のように述べています。「大企業である弊社にとって、EXABEAMのフラットなユーザーライセンス課金体系のDATA LAKEと魅力的な価格モデルは際立った価値となりました。」

2018年8月から11月の期間、東京オフィスにて概念実証と移行が行われました。このプロジェクトは大幅なSIEMのアップグレードとなりましたが、技術革新統括本部システム技術本部の旧SIEMに対する熟練の経験とEXABEAMのエンジニアの連携により、迅速に初期導入が実施されました。プロジェクトチームは、優先順位を速やかに決定し、選択したユースケースの行動分析をサポートするためのデータ取り込みの構築に集中しました。

50種類のユースケースの迅速な展開

2019年前期、日本本社でのEXABEAMの展開は、徐々に北米、ヨーロッパ、およびアジア太平洋地域に拡大し、従来のSIEMからの移行が進んでいます。導入チームは移行を後押しするため、50を超えるユースケースの利用を推進しました。ユースケースとは、EXABEAM SIEMが適用される独自のセキュリティシナリオで、検出、追跡、対処に使用されます。50種類のユースケースの使用は大規模なSIEM展開プロジェクトにおいて積極的なスタートとなりましたが、EXABEAMから400を超えるユースケースのサポートモデルの提供により、展開を後押ししました。

NTTデータ社が選択した上位のユースケースの中には、VERIZON社 (米国大手電気通信事業者)の『2018年度データ漏洩/侵害調査報告書』にてデータ漏洩の主要原因として報告されている「ユーザー資格情報のセキュリティ侵害」があり、UEBA機能により、ユーザーアカウントの資格情報、デバイス、またはIPアドレスを横断的に組み合わせて、不正アクセスを検出します。その他選ばれたユースケースは、「特権ユーザーのセキュリティ侵害」があります。これはハッカーが特権ユーザーの資格情報を取得した場合、従来のSIEMでは攻撃が「通常」の活動として判断、対処されるためです。EXABEAMのUEBAテクノロジーを利用すると、特権ユーザーの資格情報を使用した不正な行動を識別できます。NTTデータ社が導入した「内部関係者のアクセス権の悪用」ユースケースはさらに一歩進み、特権を持つ内部関係者による通常の基準ライン以外の危険な活動の実施を判断し、検出します。

NTTデータ社が積極的に複数のユースケースを展開する目的は2つあり、1点目は同社の検知と対応能力を強化すること、2点目は企業や行政機関の顧客に役立つ経験を得ることです。

NTTデータ社によるお客様企業へのEXABEAMの展開

本城氏は次のように述べています。「弊社にとってEXABEAMは重要なパートナーです。私たちは同社のソリューションを活用して、当社のグローバルビジネスを守っています。現在、当社の大切なお客様向けに、同ソリューションの提供を進めています。」本城氏によると、NTTデータ社の上位のお客様企業は、会社を保護するために膨大な予算を費やしています。お客様が使用されている従来のSIEMは、脅威の検出と追跡の点で同じ制約があり、行動分析ベースのアプローチが求められています。またどのお客様も同様に、ビッグデータに対応しない従来の従量課金モデルにおいて、予算に対して慎重です。「私たちの希望は、お客様企業にグロバルビジネスのセキュリティ強化において、EXABEAM SIEM活用が正しいアプローチであることを理解していただくことです。」と、本城氏は述べています。

EXABEAMの主な特徴

NTTデータ社が考えるEXABEAM展開による具体的なメリットは以下のとおりです。

- ユーザーライセンス課金の為、ログ量を気にせず大量のログを一元管理できる。
- 高いグローバル企業向けセキュリティとコンプライアンス、UEBA技術によって、ルールベースのアプローチでは検知できない未知の脅威の予兆を検知できる。
- 企業リスクを詳細な可視化を可能とし、セキュリティ問題対処へ向けた事前の対処ができる。

EXABEAMについて

EXABEAMはSMARTER SIEM™の会社です。当社は、企業がサイバー攻撃をより効率的に分析（検知・調査）、対処できるよう一元管理できる次世代SIEMプラットフォームを提供し、セキュリティ運用/内部脅威対策チームがより効果的には働けるように支援いたします。

企業はセキュリティのために関わる、ログ量増加による従量課金コストの増加負担や、未知の攻撃や脅威の見逃し、手動での調査と修復の実施を行う必要がなくなりました。EXABEAM セキュリティマネジメントプラットフォーム（SMP）はログの収集、分析（検知・調査）、対処を一元管理できるSIEMプラットフォームです。EXABEAM SMPはスケールしやすいビックデータインフラクチャー上でデータサイエンス、行動分析、機械学習を活用し高度分析を行うことで外部・内部ネットワークの両方からの脅威を検知、追跡し、運用の効率化・標準化を支援します。HTTPS://WWW.EXABEAM.COMにて更なる詳細をご覧ください。

今すぐHTTP://EXABEAM.COMにアクセスし、EXABEAMの便利な機能をご確認ください。