exabeam

Exabeam が提供する最先端のセキュリティ運用プラットフォーム

Detect the Undetectable™ ー検知が不可能な脅威を検知するー

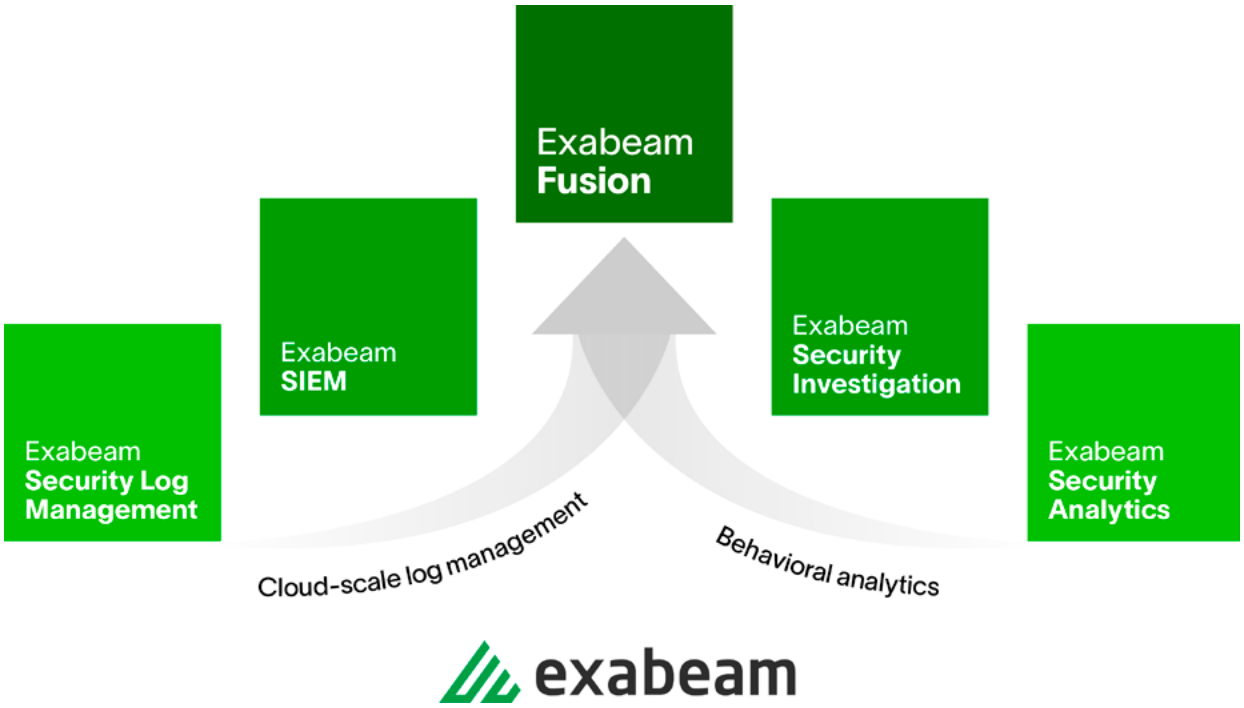
セキュリティ運用チームは現在、レガシーな SIEM の限界によってさまざまな課題に直面しています。データ量が加速度的に増加する中で市場のイノベーションは企業のニーズに追随することができず、また巧妙化するサイバー攻撃やクラウド移行ともあいまって、SIEM の有効性には大きなギャップが生じています。こうした中、セキュリティ運用チームは膨大なデータ量に圧倒され、どのデータを収集すればいいのかさえ判断できない状況に陥っています。しかし、従来のツールではインシデントの全体像を把握することは困難で、セキュリティ担当者やデータアナリストは日々大量に発生するアラートを前に、スピードに欠けた非効率かつ属人的な調査手法に頼らざるを得ないのが現状です。この間にもサイバー攻撃はさらに攻妙化し、検知が困難になると同時に、認証情報をターゲットとした攻撃はますます増加しています。

フィッシング、ランサムウェアやマルウェアといったさまざまな攻撃手法を駆使する脅威の多くは、有効な認証情報へのアクセスを主な目的としています。こうした状況を見ても、従来のルールベースのオンプレミス型の検知ソリューションから、異常な行動の把握と脅威の検知、また調査、対応（TDIR）のワークフローを自動化するクラウドネイティブな SIEM プラットフォームへの移行はもはや必然となっています。

セキュリティ運用チームが成功を手にするためには、Exabeam が提供する最先端の New-Scale SIEM™ による新たなアプローチが不可欠です。セキュリティ担当者が求めるすべての機能を網羅した New-Scale SIEM は、クラウドネイティブのデータレイク、データの迅速な取り込み、超高速なクエリパフォーマンス、また他のツールでは不可能な弱いシグナルの検知、行動分析など、アナリストの働き方を変革する強力な自動化機能を提供します。

Exabeam のセキュリティ運用プラットフォームは、企業が必要とする広範なセキュリティ機能を提供します。セキュリティログの管理においては、クラウドスケールのアーキテクチャを活用して、データの迅速な取り込み、パーサー、保存や検索を実現します。また行動分析の機能では、行動モデルヒストグラムによってユーザーとデバイス単位の正常な行動を自動的に学習して異常を検知し、リスクの優先順位に基づいて対応します。さらに、自動化された TDIR（脅威の検知、調査、対応）のワークフローによって脅威の全体像を把握し、人手に依存した複雑な作業を簡素化、自動化します。

従来のソリューションから New-Scale SIEM へ完全移行する、あるいは業界で最も卓越したユーザーとエンティティの行動分析（UEBA）と自動化機能を取り入れて既存の SIEM を補完するなど、方法はさまざまです。Exabeam の最先端のプラットフォームは、セキュリティ運用チームを確実に成功へと導きます。



Exabeam の製品

Exabeam Security Log Management

クラウド上の大規模なログ管理において、わかりやすいダッシュボードや相関ルールの機能を使って、迅速なログデータの取り込み、解析、保存、検索を実行

Exabeam SIEM

高速かつ最新の検索機能、高度な相関分析やレポート機能、ダッシュボード機能、さらにケース管理の機能までを備えたハイパースケールでクラウドネイティブな SIEM

Exabeam Fusion

最新のスケーラブルなセキュリティログ管理、強力な行動分析、自動化された脅威の検知、調査、および対応機能を備えた次世代 New-Scale SIEM™

Exabeam Security Investigation

ユーザーとエンティティの行動分析、高度な相関ルール、最新の脅威インテリジェンスの機能を備え、アラート、インシデント管理、自動トリアージ、そして対応ワークフローに裏付けられた脅威の検知、調査、および対応

Exabeam Security Analytics

高度な相関ルールと脅威インテリジェンスを利用して、ユーザーとエンティティの行動分析に基づく脅威の検知を自動化

Exabeam Security Log Management

セキュリティ上のさまざまなユースケースをサポートするために開発された業界の中でも卓越したクラウドネイティブなソリューションである Exabeam Security Log Management は、セキュリティデータの迅速な取り込み、パーサー、保存と検索を統合的に管理。過去数年分の膨大なデータを迅速に検索し、ダッシュボード上に表示します。プログラミングやクエリ構築の経験がなくても利用できる Exabeam Security Log Management によって、大きなコストをかけることなく高度なログ管理が実現します。

主な機能

Exabeam Collectors

Exabeam のセキュリティ運用プラットフォームには、脅威への対応で必要となるすべてのデータの広範な収集能力が備わっています。オンプレミス、クラウド、コンテキストのソースから Exabeam のプラットフォームへの大規模なデータ転送を、単一のインターフェースを使って安全に設定、管理、監視することができます。このプラットフォームは、200 以上のオンプレミス製品からデータを収集し、34 のクラウド型セキュリティ製品、11 の SaaS 型生産性アプリケーション、21 のクラウドインフラインフラにも対応しています。

Exabeam Log Stream

Log Stream は、100 万 EPS を超える処理能力で高速なログの取り込みを行います。中央コンソールを使って、Exabeam のすべての製品や機能で統一された取り込みパイプラインの中で、パーサーの可視化、作成、デプロイ、および監視することが可能です。取り込まれたデータは事前に組み込まれた 7,937 のログパーサーを使って解析され、オープンソースおよび市販の脅威インテリジェンスフィードから 3 つのコンテキストコレクターを使ってエンリッチ化されます。また Live Tail は、パーサーのパフォーマンスをセルフサービスでリアルタイム監視し、データパイプラインの可視性を向上します。

共通情報モデル（CIM）

Exabeam は、セキュリティ上のさまざまなユースケースに対応するために、生ログデータの正規化、分類、実用的なイベントへの変換を簡素化するスキーマを備えた共通情報モデル（CIM：Common Information Model）を構築しました。CIM では、セキュリティの専門家が使用する最も重要な 10 のフィールドと 76 のサブジェクトを定義して、それらをコア、検知、または情報提供として指定し、395 のアクティビティタイプと 2 つの結果（成功または失敗として指定）をサポートします。

検索

ペタバイト規模、あるいは過去数年分のデータに対して高速なクエリを実行し、即座に結果が表示される（ホットデータ / コールドデータを同じ速度で検索）シンプルな検索体験が得られます。

レポートとダッシュボード

あらかじめ組み込まれたコンプライアンスレポートを使用して、ダッシュボードデータの印刷、エクスポート、表示のほか、14 種類のグラフ（チャート）を使用したレポート作成や、ダッシュボードのカスタマイズを行うことができます。

相関ルールビルダー

相関ルールは、受信したイベントをエンティティ間の事前に定義された関係性と比較することで、異常を特定してエスカレーションします。Threat Intelligence Service（脅威インテリジェンスサービス）をソースとするアクティビティに対応したイベントの重要度を高く設定するなど、最も重要なビジネスエンティティやアセットに対して、最大で 1,000 のカスタマイズされた相関ルールを作成、テスト、適用、監視することができます。

Outcomes Navigator

Outcomes Navigator は、Exabeam Security Log Management に入力されたフィードを一般的なセキュリティのユースケースに照らし合わせてマッピングし、適用範囲を改善するための方法を提案します。Outcomes Navigator は、セキュリティギャップを埋めるためにイベントストリームや設定変更を解析し、成果にフォーカスした測定可能、かつ継続的な改善をサポートします。

Service Health and Consumption（サービスの健全性と使用状況）

接続とソースの監視を行いながら、アプリケーションなど各サービスの健全性に加えて、データの消費状況を可視化します。すべてのログパーサー、アプリケーション、データフロー、および接続の稼働時間と稼働状況、さらにストレージの長期的なキャパシティプランニングに役立つ、すべてのライセンスの使用状況が表示されるダッシュボードを備えています。

Threat Intelligence Service（脅威インテリジェンスサービス）

Exabeam Threat Intelligence Service は、Exabeam のすべての製品で追加費用なしで利用できます。市販あるいはオープンソースの複数の脅威インテリジェンスフィードを取り込み、それらを独自の機械学習アルゴリズムを用いて集約、精査、優先順位付けした上で、高精度かつ最新の IoC ストリームを生成します。さらに、外部の複数の脅威インテリジェンスサービスやフィードのイベントに対して、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイントなどを追加することで、コンテキストのエンリッチメントが実現します。また、脅威インテリジェンスのデータは 24 時間ごとに更新されます。

コンテキストエンリッチメント

コンテキストエンリッチメントは、脅威インテリジェンス、ジオロケーション、そしてユーザーホスト IP マッピングの 3 つの方法によるエンリッチメントに対応しています。最新の IoC を備えた Exabeam の脅威インテリジェンスサービスは、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイント識別などのエンリッチメントを加えて、既存の相関ルールや行動モデルの優先順位付けや更新を行います。ジオロケーションのエンリッチメントでは、ログに存在しないロケーションベースのコンテキストを提供します。また Exabeam のユーザーホスト IP マッピングのエンリッチメントによって、異常なアクティビティを検知する行動モデルを構築する際に重要となるログに、ユーザーの詳細が追加されます。

Exabeam SIEM

Exabeam SIEM は、Exabeam Security Log Management を TDIR（脅威の検知、調査、対応）の機能で拡張したクラウドネイティブな SIEM です。Exabeam SIEM では、ケース管理、調査と対応のための一元化された記録システム、組み込み済みの 100 以上の相関ルール、より高度な検知のための統合的な脅威インテリジェンスが提供されます。このソリューションがもたらすかつてないスピード、100 万 EPS を超える処理能力によって、アナリストはペタバイト規模、あるいは過去数年分のホットデータ / コールドデータに対して高速なクエリを実行し、即座に結果を得ることができます。また Alert and Case Management（アラート管理とケース管理）の機能は、ガイド付きのインシデントチェックリストと、セキュリティのために特別に設計されたチケットシステムにより、アナリストの生産性を向上します。ストレージの増強、保存期間の延長、処理能力の向上が必要な場合でも、Exabeam SIEM はニーズに応じて簡単に拡張することができます。

主な機能

Exabeam Collectors

Exabeam のセキュリティ運用プラットフォームには、脅威への対応で必要となるすべてのデータの広範な収集能力が備わっています。オンプレミス、クラウド、コンテキストのソースから Exabeam のプラットフォームへの大規模なデータ転送を、単一のインターフェースを使って安全に設定、管理、監視することができます。このプラットフォームは、200 以上のオンプレミス製品からデータを収集し、34 のクラウド型セキュリティ製品、11 の SaaS 型生産性アプリケーション、21 のクラウドインフラインフラにも対応しています。

Exabeam Log Stream

Log Stream は、100 万 EPS を超える処理能力で高速なログの取り込みを行います。中央コンソールを使って、Exabeam のすべての製品や機能で統一された取り込みパイプラインの中で、パーサーの可視化、作成、デプロイ、および監視することが可能です。取り込まれたデータは事前に組み込まれた 7,937 のログパーサーを使って解析され、オープンソースおよび市販の脅威インテリジェンスフィードから 3 つのコンテキストコレクターを使ってエンリッチ化されます。また Live Tail は、パーサーのパフォーマンスをセルフサービスでリアルタイム監視し、データパイプラインの可視性を向上します。

共通情報モデル（CIM）

Exabeam は、セキュリティ上のさまざまなユースケースに対応するために、生ログデータの正規化、分類、実用的なイベントへの変換を簡素化するスキーマを備えた共通情報モデル（CIM：Common Information Model）を構築しました。CIM では、セキュリティの専門家が使用する最も重要な 10 のフィールドと 76 のサブジェクトを定義して、それらをコア、検知、または情報提供として指定し、395 のアクティビティタイプと 2 つの結果（成功または失敗として指定）をサポートします。

検索

ペタバイト規模、あるいは過去数年分のデータに対して高速なクエリを実行し、即座に結果が表示される（ホットデータ / コールドデータを同じ速度で検索）シンプルな検索体験が得られます。

レポートとダッシュボード

あらかじめ組み込まれたコンプライアンスレポートを使用して、ダッシュボードデータの印刷、エクスポート、表示のほか、14 種類のグラフ（チャート）を使用したレポート作成や、ダッシュボードのカスタマイズを行うことができます。

相関ルールビルダー

相関ルールは、受信したイベントをエンティティ間の事前に定義された関係性と比較することで、異常を特定してエスカレーションします。Threat Intelligence Service（脅威インテリジェンスサービス）をソースとするアクティビティに対応したイベントの重要度を高く設定するなど、最も重要なビジネスエンティティやアセットに対して、最大で 1,000 のカスタマイズされた相関ルールを作成、テスト、適用、監視することができます。

組み込み済みの相関ルール

マルウェアや侵害された認証情報など、最も一般的なユースケースに対応した 100 以上の相関ルールとモデルが事前に組み込まれています。

Outcomes Navigator

Outcomes Navigator は、Exabeam Security Log Management に入力されたフィードを一般的なセキュリティのユースケースに照らし合わせてマッピングし、適用範囲を改善するための方法を提案します。Outcomes Navigator は、セキュリティギャップを埋めるためにイベントストリームや設定変更を解析し、成果にフォーカスした測定可能、かつ継続的な改善をサポートします。

Service Health and Consumption（サービスの健全性と使用状況）

接続とソースの監視を行いながら、アプリケーションなど各サービスの健全性に加えて、データの消費状況を可視化します。すべてのログパーサー、アプリケーション、データフロー、および接続の稼働時間と稼働状況、さらにストレージの長期的なキャパシティプランニングに役立つ、すべてのライセンスの使用状況が表示されるダッシュボードを備えています。

Threat Intelligence Service（脅威インテリジェンスサービス）

Exabeam Threat Intelligence Service は、Exabeam のすべての製品で追加費用なしで利用できます。市販あるいはオープンソースの複数の脅威インテリジェンスフィードを取り込み、それらを独自の機械学習アルゴリズムを用いて集約、精査、優先順位付けした上で、高精度かつ最新の IoC ストリームを生成します。さらに、外部の複数の脅威インテリジェンスサービスやフィードのイベントに対して、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイントなどを追加することで、コンテキストのエンリッチメントが実現します。また、脅威インテリジェンスのデータは 24 時間ごとに更新されます。

Alert and Case Management（アラート管理とケース管理）

Exabeam SIEM とセキュリティデータレイクの大きな違いは、アラートを重要度別に分類し、ケースやインシデントにまとめ、アナリストが解決に導くことができる点にあります。Alert and Case Management の機能によって、Exabeam またはサードパーティ製品から発生したイベントやアラートを一元的に管理して、個別または大量のレビュー、あるいは条件を設定してアラートのトリアージ（優先順位付け）のワークフローを自動化し、イベントやアラートをエスカレーションすることができます。また、アナリストチームはインシデントにタグやイベントを追加し、グループやタイムゾーンを横断したコラボレーションを行うことで、リスクを緩和または解決するための成果を最優先にしたカスタマイズ可能な手順をチームで共有することができます。

コンテキストエンリッチメント

コンテキストエンリッチメントは、脅威インテリジェンス、ジオロケーション、そしてユーザーホスト IP マッピングの 3 つの方法によるエンリッチメントに対応しています。最新の IoC を備えた Exabeam の脅威インテリジェンスサービスは、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイント識別などのエンリッチメントを加えて、既存の相関ルールや行動モデルの優先順位付けや更新を行います。ジオロケーションのエンリッチメントでは、ログに存在しないロケーションベースのコンテキストを提供します。また Exabeam のユーザーホスト IP マッピングのエンリッチメントによって、異常なアクティビティを検知する行動モデルを構築する際に重要となるログに、ユーザーの詳細が追加されます。

MITRE ATT&CK フレームワークの活用

Exabeam のセキュリティ運用プラットフォームでは、MITRE ATT&CK フレームワークを効果的に活用することで、セキュリティ環境の可視性の向上を支援しています。このサポートは、MITRE ATT&CK フレームワークで推奨される 101 の手法や、それに準ずる 180 の手法を含む全 14 カテゴリーをカバーしています。

Exabeam Fusion

TDIR（脅威の検知、調査、対応）を支援する包括的な機能を備えた Exabeam Fusion は、業界で最も強力かつ高度なクラウドネイティブ SIEM です。Exabeam Fusion には、Exabeam Security Log Management、Exabeam SIEM、Exabeam Security Analytics、Exabeam Security Investigation のすべての機能が統合されています。ここでは、クラウドネイティブのデータレイク、データの迅速な取り込み、超高速なクエリパフォーマンス、また他のツールでは不可能な弱いシグナルの検知、行動分析など、アナリストの働き方を変革する強力な自動化機能が提供されます。事前に組み込まれた 549 以上のサードパーティのセキュリティツール、1,800 を超える実証済みの相関ルールと 750 以上の行動モデルヒストグラムの統合により、ユーザーとデバイス単位の正常な行動を自動的に学習し、リスクの度合いに基づいて異常を検出、優先順位に基づいて対応します。また、Exabeam は脅威インテリジェンス、ジオロケーション、そしてユーザーホスト IP マッピングの 3 つの方法によるイベントのエンリッチメントに対応しています。Exabeam Fusion を使用することで、アナリストは単一のコントロールプレーンからエンドツーエンドの TDIR ワークフローを実行することができ、アラートのトリアージや優先順位付け、インシデントの調査、対応などの時間を短縮し、一貫性のある再現可能な成果を生み出すことができます。

主な機能

Exabeam Collectors

Exabeam のセキュリティ運用プラットフォームには、脅威への対応で必要となるすべてのデータの広範な収集能力が備わっています。オンプレミス、クラウド、コンテキストのソースから Exabeam のプラットフォームへの大規模なデータ転送を、単一のインターフェースを使って安全に設定、管理、監視することができます。このプラットフォームは、200 以上のオンプレミス製品からデータを収集し、34 のクラウド型セキュリティ製品、11 の SaaS 型生産性アプリケーション、21 のクラウドインフラインフラにも対応しています。

Exabeam Log Stream

Log Stream は、100 万 EPS を超える処理能力で高速なログの取り込みを行います。中央コンソールを使って、Exabeam のすべての製品や機能で統一された取り込みパイプラインの中で、パーサーの可視化、作成、デプロイ、および監視することが可能です。取り込まれたデータは事前に組み込まれた 7,937 のログパーサーを使って解析され、オープンソースおよび市販の脅威インテリジェンスフィードから 3 つのコンテキストコレクターを使ってエンリッチ化されます。また Live Tail は、パーサーのパフォーマンスをセルフサービスでリアルタイム監視し、データパイプラインの可視性を向上します。

共通情報モデル（CIM）

Exabeam は、セキュリティ上のさまざまなユースケースに対応するために、生ログデータの正規化、分類、実用的なイベントへの変換を簡素化するスキーマを備えた共通情報モデル（CIM：Common Information Model）を構築しました。CIM では、セキュリティの専門家が使用する最も重要な 10 のフィールドと 76 のサブジェクトを定義して、それらをコア、検知、または情報提供として指定し、395 のアクティビティタイプと 2 つの結果（成功または失敗として指定）をサポートします。

検索

ペタバイト規模、あるいは過去数年分のデータに対して高速なクエリを実行し、即座に結果が表示される（ホットデータ / コールドデータを同じ速度で検索）シンプルな検索体験が得られます。

レポートとダッシュボード

あらかじめ組み込まれたコンプライアンスレポートを使用して、ダッシュボードデータの印刷、エクスポート、表示のほか、14 種類のグラフ（チャート）を使用したレポート作成や、ダッシュボードのカスタマイズを行うことができます。

相関ルールビルダー

相関ルールは、受信したイベントをエンティティ間の事前に定義された関係性と比較することで、異常を特定してエスカレーションします。Threat Intelligence Service（脅威インテリジェンスサービス）をソースとするアクティビティに対応したイベントの重要度を高く設定するなど、最も重要なビジネスエンティティやアセットに対して、最大で 1,000 のカスタマイズされた相関ルールを作成、テスト、適用、監視することができます。

組み込み済みの相関ルール

マルウェアや侵害された認証情報など、最も一般的なユースケースに対応した 100 以上の相関ルールとモデルが事前に組み込まれています。

Outcomes Navigator

Outcomes Navigator は、Exabeam Security Log Management に入力されたフィードを一般的なセキュリティのユースケースに照らし合わせてマッピングし、適用範囲を改善するための方法を提案します。Outcomes Navigator は、セキュリティギャップを埋めるためにイベントストリームや設定変更を解析し、成果にフォーカスした測定可能、かつ継続的な改善をサポートします。

Service Health and Consumption（サービスの健全性と使用状況）

接続とソースの監視を行いながら、アプリケーションなど各サービスの健全性に加えて、データの消費状況を可視化します。すべてのログパーサー、アプリケーション、データフロー、および接続の稼働時間と稼働状況、さらにストレージの長期的なキャパシティプランニングに役立つ、すべてのライセンスの使用状況が表示されるダッシュボードを備えています。

Threat Intelligence Service（脅威インテリジェンスサービス）

Exabeam Threat Intelligence Service は、Exabeam のすべての製品で追加費用なしで利用できます。市販あるいはオープンソースの複数の脅威インテリジェンスフィードを取り込み、それらを独自の機械学習アルゴリズムを用いて集約、精査、優先順位付けした上で、高精度かつ最新の IoC ストリームを生成します。さらに、外部の複数の脅威インテリジェンスサービスやフィードのイベントに対して、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイントなどを追加することで、コンテキストのエンリッチメントが実現します。また、脅威インテリジェンスのデータは 24 時間ごとに更新されます。

Advanced Analytics（高度な分析）

Advanced Analytics では、クラウドインフラのセキュリティなど 1,800 を超えるファクトベースの相関ルールと、ユーザーやデバイスの正常な振る舞いを自動的にベースライン化する 750 以上の行動モデルヒストグラムを備えたUEBA が利用することができ、リスクに基づく異常の検知、優先順位付け、および対応が可能になります。Advanced Analytics は、これらのイベントを Smart Timelines™ で自動的に可視化して、イベントフローやアクティビティをすべて表示し、次の適切なアクションを通知します。

Alert and Case Management（アラート管理とケース管理）

Alert and Case Management の機能によって、アナリストチームはインシデントにタグやイベントを追加し、グループやタイムゾーンを横断したコラボレーションを行うことで、リスクを緩和または解決するための成果を最優先にしたカスタマイズ可能な手順をチームで共有することができます。

ターンキープレイブック

侵害された認証情報、マルウェア、悪意のある内部関係者を調査するための反復型ワークフローを、解決に向けたガイド付きチェックリストを使用して自動化します。

インシデントレスポンダー

100 のサードパーティ製品に対応した API を使用して、半自動または全自動の 576 のアクションと操作で反復型ワークフローを調整、自動化するためのオプション機能です。

アラートのトリアージ

サードパーティまたは Exabeam のシステム内で生成されたセキュリティアラートを分類、集約、エンリッチ化することで、アナリストは単一の画面からアラートを効率的に解除またはエスカレートすることができます。

動的なアラートの優先順位付け

機械学習を用いてサードパーティのセキュリティアラートの優先順位付けを自動化します。アナリストがトリアージプロセスを開始する出発点となり、組織に最も高いリスクをもたらすアラートに時間とリソースを集中することができます。

コンテキストエンリッチメント

コンテキストエンリッチメントは、脅威インテリジェンス、ジオロケーション、そしてユーザーホスト IP マッピングの 3 つの方法によるエンリッチメントに対応しています。最新の IoC を備えた Exabeam の脅威インテリジェンスサービスは、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイント識別などのエンリッチメントを加えて、既存の相関ルールや行動モデルの優先順位付けや更新を行います。ジオロケーションのエンリッチメントでは、ログに存在しないロケーションベースのコンテキストを提供します。また Exabeam のユーザーホスト IP マッピングのエンリッチメントによって、異常なアクティビティを検知する行動モデルを構築する際に重要となるログに、ユーザーの詳細が追加されます。

MITRE ATT&CK フレームワークの活用

Exabeam のセキュリティ運用プラットフォームでは、MITRE ATT&CK フレームワークを効果的に活用することで、セキュリティ環境の可視性の向上を支援しています。このサポートは、MITRE ATT&CK フレームワークで推奨される 101 の手法や、それに準ずる 180 の手法を含む全 14 カテゴリーをカバーしています。

Exabeam Security Analytics

現在の市場で提供されている多くの SIEM 製品には、ユーザーおよびエンティティの行動分析（UEBA）のための機能が備わっていません。利用できたとしても、機能の統合が不十分であったり、旧世代の機能であったり、あるいは機械学習を装った単なる統計分析のいずれかであることがほとんどです。既存のサードパーティのレガシー SIEM やデータレイク上で動作する唯一の UEBA 製品である Exabeam Security Analytics は、組織を守るためのセキュリティ機能を継続的にアップグレードしながら、高度な認証情報ベースの攻撃にも対応することができます。Exabeam Security Analytics は、広範なログデータを取り込み、データエンリッチメントと脅威インテリジェンスを用いた CIM（共通情報モデル）によって正規化および解析を行い、イベントを構築します。この CIM はクラウドインフラのセキュリティなど 1,800 を超えるファクトベースの相関ルール、またユーザーとデバイスの正常な行動を自動的にベースライン化する 750 以上の行動モデルヒストグラムを備えており、リスクに基づく異常の検知、優先順位付け、および対応が可能になります。Smart Timelines™ は、インシデントの全履歴を保有しており、イベントフローとアクティビティをすべて表示して、各イベントに関連するリスクをスコア化します。これにより、アナリストは何百ものクエリを記述する必要がなくなり、これまでの業務手法は刷新されます。

主な機能

Exabeam Collectors

Exabeam のセキュリティ運用プラットフォームには、脅威への対応で必要となるすべてのデータの広範な収集能力が備わっています。オンプレミス、クラウド、コンテキストのソースから Exabeam のプラットフォームへの大規模なデータ転送を、単一のインターフェースを使って安全に設定、管理、監視することができます。このプラットフォームは、200 以上のオンプレミス製品からデータを収集し、34 のクラウド型セキュリティ製品、11 の SaaS 型生産性アプリケーション、21 のクラウドインフラインフラにも対応しています。

Exabeam Log Stream

Log Stream は、100 万 EPS を超える処理能力で高速なログの取り込みを行います。中央コンソールを使って、Exabeam のすべての製品や機能で統一された取り込みパイプラインの中で、パーサーの可視化、作成、デプロイ、および監視することが可能です。取り込まれたデータは事前に組み込まれた 7,937 のログパーサーを使って解析され、オープンソースおよび市販の脅威インテリジェンスフィードから 3 つのコンテキストコレクターを使ってエンリッチ化されます。また Live Tail は、パーサーのパフォーマンスをセルフサービスでリアルタイム監視し、データパイプラインの可視性を向上します。

共通情報モデル（CIM）

Exabeam は、セキュリティ上のさまざまなユースケースに対応するために、生ログデータの正規化、分類、実用的なイベントへの変換を簡素化するスキーマを備えた共通情報モデル（CIM：Common Information Model）を構築しました。CIM では、セキュリティの専門家が使用する最も重要な 10 のフィールドと 76 のサブジェクトを定義して、それらをコア、検知、または情報提供として指定し、395 のアクティビティタイプと 2 つの結果（成功または失敗として指定）をサポートします。

Anomaly Search（異常の検索）

より高速なクエリと瞬時の検索が、かつてないシンプルな検索体験を提供します。アナリストは単一のインターフェースを使用して、データリポジトリ全体の中から Exabeam で検知されたイベントを検索することができます。Anomaly Search のドロップダウンメニューを用いてイベントリストに対するクエリを容易に作成し、インシデントの判定が可能になります。また、行動ベースの TTP 検知と既知の IoC を組み合わせることで、セッション、ルール、ユーザー、アセット、MITRE TTP、異常の識別、ユースケースなど、さまざまな対象の脅威ハンティングと相関ルールのテストを強化できます。

レポートとダッシュボード

あらかじめ組み込まれたコンプライアンスレポートを使用して、ダッシュボードデータの印刷、エクスポート、表示のほか、14 種類のグラフ（チャート）を使用したレポート作成や、ダッシュボードのカスタマイズを行うことができます。

相関ルールビルダー

相関ルールは、受信したイベントをエンティティ間の事前に定義された関係性と比較することで、異常を特定してエスカレーションします。Threat Intelligence Service（脅威インテリジェンスサービス）をソースとするアクティビティに対応したイベントの重要度を高く設定するなど、最も重要なビジネスエンティティやアセットに対して、最大で 1,000 のカスタマイズされた相関ルールを作成、テスト、適用、監視することができます。

組み込み済みの相関ルール

マルウェアや侵害された認証情報など、最も一般的なユースケースに対応した 100 以上の相関ルールとモデルが事前に組み込まれています。

Outcomes Navigator

Outcomes Navigator は、Exabeam Security Log Management に入力されたフィードを一般的なセキュリティのユースケースに照らし合わせてマッピングし、適用範囲を改善するための方法を提案します。Outcomes Navigator は、セキュリティギャップを埋めるためにイベントストリームや設定変更を解析し、成果にフォーカスした測定可能、かつ継続的な改善をサポートします。

Service Health and Consumption（サービスの健全性と使用状況）

接続とソースの監視を行いながら、アプリケーションなど各サービスの健全性に加えて、データの消費状況を可視化します。すべてのログパーサー、アプリケーション、データフロー、および接続の稼働時間と稼働状況、さらにストレージの長期的なキャパシティプランニングに役立つ、すべてのライセンスの使用状況が表示されるダッシュボードを備えています。

Threat Intelligence Service（脅威インテリジェンスサービス）

Exabeam Threat Intelligence Service は、Exabeam のすべての製品で追加費用なしで利用できます。市販あるいはオープンソースの複数の脅威インテリジェンスフィードを取り込み、それらを独自の機械学習アルゴリズムを用いて集約、精査、優先順位付けした上で、高精度かつ最新の IoC ストリームを生成します。さらに、外部の複数の脅威インテリジェンスサービスやフィードのイベントに対して、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイントなどを追加することで、コンテキストのエンリッチメントが実現します。また、脅威インテリジェンスのデータは 24 時間ごとに更新されます。

Advanced Analytics（高度な分析）

Advanced Analytics では、クラウドインフラのセキュリティなど 1,800 を超えるファクトベースの相関ルールと、ユーザーやデバイスの正常な振る舞いを自動的にベースライン化する 750 以上の行動モデルヒストグラムを備えたUEBA が利用することができ、リスクに基づく異常の検知、優先順位付け、および対応が可能になります。Advanced Analytics は、これらのイベントを Smart Timelines™ で自動的に可視化して、イベントフローやアクティビティをすべて表示し、次の適切なアクションを通知します。

アラートのトリアージ

サードパーティまたは Exabeam のシステム内で生成されたセキュリティアラートを分類、集約、エンリッチ化することで、アナリストは単一の画面からアラートを効率的に解除またはエスカレートすることができます。

Alert and Case Management（アラート管理とケース管理）

Alert and Case Management の機能によって、アナリストチームはインシデントにタグやイベントを追加し、グループやタイムゾーンを横断したコラボレーションを行うことで、リスクを緩和または解決するための成果を最優先にしたカスタマイズ可能な手順をチームで共有することができます。

コンテキストエンリッチメント

コンテキストエンリッチメントは、脅威インテリジェンス、ジオロケーション、そしてユーザーホスト IP マッピングの 3 つの方法によるエンリッチメントに対応しています。最新の IoC を備えた Exabeam の脅威インテリジェンスサービスは、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイント識別などのエンリッチメントを加えて、既存の相関ルールや行動モデルの優先順位付けや更新を行います。ジオロケーションのエンリッチメントでは、ログに存在しないロケーションベースのコンテキストを提供します。また Exabeam のユーザーホスト IP マッピングのエンリッチメントによって、異常なアクティビティを検知する行動モデルを構築する際に重要となるログに、ユーザーの詳細が追加されます。

MITRE ATT&CK フレームワークの活用

Exabeam のセキュリティ運用プラットフォームでは、MITRE ATT&CK フレームワークを効果的に活用することで、セキュリティ環境の可視性の向上を支援しています。このサポートは、MITRE ATT&CK フレームワークで推奨される 101 の手法や、それに準ずる 180 の手法を含む全 14 カテゴリーをカバーしています。

Exabeam Security Investigation

サードパーティのレガシー SIEM やデータレイク上で動作する Exabeam Security Investigation には、脅威の検知、調査、対応（TDIR）のための高度な機能が網羅されています。Exabeam Security Investigation は、Exabeam Security Analytics のユーザーおよびエンティティの行動分析（UEBA）の機能を、特定の脅威や手法にフォーカスした所定のワークフローやコンテンツ（MITRE ATT&CK フレームワークなど）と組み合わせることで、ランサムウェア、フィッシング、マルウェア、および不正な悪意のある内部関係者を対象にした成果重視の TDIR を可能にします。クラウドインフラのセキュリティなど 1,800 を超えるファクトベースの相関ルール、またユーザーとデバイスの正常な行動を自動的にベースライン化する 750 以上の行動モデルヒストグラムによって、リスクに基づく異常の検知、優先順位付け、対応を行うことができます。アナリストは単一のコントロールプレーンからエンドツーエンドの TDIR ワークフローを実行することができ、アラートのトリアージや優先順位付け、インシデントの調査、対応など、これまで手作業に依存してきた多くのタスクは自動化されます。これにより、アナリストの生産性向上に加えて、何百ものセキュリティオーケストレーション、自動化、応答（SOAR）の統合によってセキュリティ運用における調査や対応の時間が短縮化し、一貫性のある再現可能な成果を生み出すことができるようになります。

主な機能

Exabeam Collectors

Exabeam のセキュリティ運用プラットフォームには、脅威への対応で必要となるすべてのデータの広範な収集能力が備わっています。オンプレミス、クラウド、コンテキストのソースから Exabeam のプラットフォームへの大規模なデータ転送を、単一のインターフェースを使って安全に設定、管理、監視することができます。このプラットフォームは、200 以上のオンプレミス製品からデータを収集し、34 のクラウド型セキュリティ製品、11 の SaaS 型生産性アプリケーション、21 のクラウドインフラインフラにも対応しています。

Exabeam Log Stream

Log Stream は、100 万 EPS を超える処理能力で高速なログの取り込みを行います。中央コンソールを使って、Exabeam のすべての製品や機能で統一された取り込みパイプラインの中で、パーサーの可視化、作成、デプロイ、および監視することが可能です。取り込まれたデータは事前に組み込まれた 7,937 のログパーサーを使って解析され、オープンソースおよび市販の脅威インテリジェンスフィードから 3 つのコンテキストコレクターを使ってエンリッチ化されます。また Live Tail は、パーサーのパフォーマンスをセルフサービスでリアルタイム監視し、データパイプラインの可視性を向上します。

共通情報モデル（CIM）

Exabeam は、セキュリティ上のさまざまなユースケースに対応するために、生ログデータの正規化、分類、実用的なイベントへの変換を簡素化するスキーマを備えた共通情報モデル（CIM：Common Information Model）を構築しました。CIM では、セキュリティの専門家が使用する最も重要な 10 のフィールドと 76 のサブジェクトを定義して、それらをコア、検知、または情報提供として指定し、395 のアクティビティタイプと 2 つの結果（成功または失敗として指定）をサポートします。

Anomaly Search（異常の検索）

より高速なクエリと瞬時の検索が、かつてないシンプルな検索体験を提供します。アナリストは単一のインターフェースを使用して、データリポジトリ全体の中から Exabeam で検知されたイベントを検索することができます。Anomaly Search のドロップダウンメニューを用いてイベントリストに対するクエリを容易に作成し、インシデントの判定が可能になります。また、行動ベースの TTP 検知と既知の IoC を組み合わせることで、セッション、ルール、ユーザー、アセット、MITRE TTP、異常の識別、ユースケースなど、さまざまな対象の脅威ハンティングと相関ルールのテストを強化できます。

レポートとダッシュボード

あらかじめ組み込まれたコンプライアンスレポートを使用して、ダッシュボードデータの印刷、エクスポート、表示のほか、14 種類のグラフ（チャート）を使用したレポート作成や、ダッシュボードのカスタマイズを行うことができます。

相関ルールビルダー

相関ルールは、受信したイベントをエンティティ間の事前に定義された関係性と比較することで、異常を特定してエスカレーションします。Threat Intelligence Service（脅威インテリジェンスサービス）をソースとするアクティビティに対応したイベントの重要度を高く設定するなど、最も重要なビジネスエンティティやアセットに対して、最大で 1,000 のカスタマイズされた相関ルールを作成、テスト、適用、監視することができます。

組み込み済みの相関ルール

マルウェアや侵害された認証情報など、最も一般的なユースケースに対応した 100 以上の相関ルールとモデルが事前に組み込まれています。

Outcomes Navigator

Outcomes Navigator は、Exabeam Security Log Management に入力されたフィードを一般的なセキュリティのユースケースに照らし合わせてマッピングし、適用範囲を改善するための方法を提案します。Outcomes Navigator は、セキュリティギャップを埋めるためにイベントストリームや設定変更を解析し、成果にフォーカスした測定可能、かつ継続的な改善をサポートします。

Service Health and Consumption（サービスの健全性と使用状況）

接続とソースの監視を行いながら、アプリケーションなど各サービスの健全性に加えて、データの消費状況を可視化します。すべてのログパーサー、アプリケーション、データフロー、および接続の稼働時間と稼働状況、さらにストレージの長期的なキャパシティプランニングに役立つ、すべてのライセンスの使用状況が表示されるダッシュボードを備えています。

Threat Intelligence Service（脅威インテリジェンスサービス）

Exabeam Threat Intelligence Service は、Exabeam のすべての製品で追加費用なしで利用できます。市販あるいはオープンソースの複数の脅威インテリジェンスフィードを取り込み、それらを独自の機械学習アルゴリズムを用いて集約、精査、優先順位付けした上で、高精度かつ最新の IoC ストリームを生成します。さらに、外部の複数の脅威インテリジェンスサービスやフィードのイベントに対して、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイントなどを追加することで、コンテキストのエンリッチメントが実現します。また、脅威インテリジェンスのデータは 24 時間ごとに更新されます。

Advanced Analytics（高度な分析）

Advanced Analytics では、クラウドインフラのセキュリティなど 1,800 を超えるファクトベースの相関ルールと、ユーザーやデバイスの正常な振る舞いを自動的にベースライン化する 750 以上の行動モデルヒストグラムを備えたUEBA が利用することができ、リスクに基づく異常の検知、優先順位付け、および対応が可能になります。Advanced Analytics は、これらのイベントを Smart Timelines™ で自動的に可視化して、イベントフローやアクティビティをすべて表示し、次の適切なアクションを通知します。

アラートのトリアージ

サードパーティまたは Exabeam のシステム内で生成されたセキュリティアラートを分類、集約、エンリッチ化することで、アナリストは単一の画面からアラートを効率的に解除またはエスカレートすることができます。

Alert and Case Management（アラート管理とケース管理）

Alert and Case Management の機能によって、アナリストチームはインシデントにタグやイベントを追加し、グループやタイムゾーンを横断したコラボレーションを行うことで、リスクを緩和または解決するための成果を最優先にしたカスタマイズ可能な手順をチームで共有することができます。

ターンキープレイブック

侵害された認証情報、マルウェア、悪意のある内部関係者を調査するための反復型ワークフローを、解決に向けたガイド付きチェックリストを使用して自動化します。

インシデントレスポンダー

100 のサードパーティ製品に対応した API を使用して、半自動または全自動の 576 のアクションと操作で反復型ワークフローを調整、自動化するためのオプション機能です。

動的なアラートの優先順位付け

機械学習を用いてサードパーティのセキュリティアラートの優先順位付けを自動化します。アナリストがトリアージプロセスを開始する出発点となり、組織に最も高いリスクをもたらすアラートに時間とリソースを集中することができます。

コンテキストエンリッチメント

コンテキストエンリッチメントは、脅威インテリジェンス、ジオロケーション、そしてユーザーホスト IP マッピングの 3 つの方法によるエンリッチメントに対応しています。最新の IoC を備えた Exabeam の脅威インテリジェンスサービスは、ファイル、ドメイン、IP、URL レピュテーション、TOR エンドポイント識別などのエンリッチメントを加えて、既存の相関ルールや行動モデルの優先順位付けや更新を行います。ジオロケーションのエンリッチメントでは、ログに存在しないロケーションベースのコンテキストを提供します。また Exabeam のユーザーホスト IP マッピングのエンリッチメントによって、異常なアクティビティを検知する行動モデルを構築する際に重要となるログに、ユーザーの詳細が追加されます。

MITRE ATT&CK フレームワークの活用

Exabeam のセキュリティ運用プラットフォームでは、MITRE ATT&CK フレームワークを効果的に活用することで、セキュリティ環境の可視性の向上を支援しています。このサポートは、MITRE ATT&CK フレームワークで推奨される 101 の手法や、それに準ずる 180 の手法を含む全 14 カテゴリーをカバーしています。

	Exabeam Security Log Management	Exabeam SIEM	Exabeam Fusion	Exabeam Security Investigation	Exabeam Security Analytics
Exabeam Collectors	●	●	●	●	●
脅威インテリジェンスサービス	●	●	●	●	●
Exabeam Log Stream	●	●	●	●	●
検索	検索	検索	検索	異常の検索	異常の検索
組み込み済みのレポート	コンプライアンス	コンプライアンス ケースマネジメント	コンプライアンス ケースマネジメント 異常と検知	ケースマネジメント 異常と検知	ケースマネジメント 異常と検知
組み込み済みのダッシュボード	●	●	●	●	●
ダッシュボードのカスタマイズ	●	●	●		
相関ルールビルダー	●	●	●	●	●
サービスの健全性と使用状況	●	●	●	●	●
100 以上の組み込み済みの相関ルール		●	●	●	●
アラート管理とケース管理		●	●	●	●
高度な分析			●	●	●
Outcomes Navigator	●	●	●	●	●
動的なアラートの優先順位付け			●	●	
ターンキープレイブック			●	●	
アドオンのオプション					
インシデントレスポンダー (プレイブックのカスタマイズ / アクションエディタ)			テナントごとに販売	テナントごとに販売	
検索と長期保存のサブスクリプションアドオン	●	●	●		

Exabeam Customer Success Services（カスタマーサクセスサービス）

Exabeam Customer Success Services は、単なるソリューションの導入や運用管理を目的とするものではありません。お客様が目指すビジネス目標とセキュリティ施策の成果の達成を支援する役割を果たします。また最適な Exabeam 環境を維持するために、技術的な専門知識を備えた経験豊富なチームが 24 時間体制でサポートします。

Exabeam Support Services（サポートサービス）

Exabeam は、運用上のアセスメント、レポーティング、継続的なチューニングサービスを含む 3 つのレベルのサポートを提供しています。

スタンダードサポート

Exabeam のすべてのお客様にご利用いただけます。スタンダードサポートには、サポートポータルの利用や Exabeam コミュニティへの参加が含まれます。多くのセキュリティ担当者が参加するこのコミュニティでは、最新のウェビナーや動画などが公開されており、Exabeam のデプロイや独自のユースケースの課題解決にお役立ていただけます。

プレミアムサポート

スタンダードサポートのすべての特典に加えて、年次アカウントレビュー、365 日 24 時間利用可能な電話対応によるエスカレーションが含まれ、よりミッションクリティカルなサポートを必要とするお客様に最適です。

プレミアムプラスサポート

スタンダードサポートとプレミアムサポートのすべての特典に加えて、お客様をサポートする Customer Success Manager が配置されます。Customer Success Manager はお客様のビジネス目標を理解し、常にお客様に寄り添いながら目標を達成するためのプランの作成をお手伝いします。プレミアプラスのサポート契約を締結されたお客様は、エグゼクティブビジネスレビューを含む最高水準のサポート SLA や、高度なエンジニアリングサービスをご利用いただけます。

Exabeam Customer Success Management

Exabeam のカスタマーサクセスマネージャーはお客様の戦略的なパートナーとして、Exabeam を活用したビジネス目標の達成を幅広く支援します。

- Exabeam を活用した**お客様のセキュリティ運用全体を支援**
- お客様のニーズに応じて**必要となるリソースの調整と手配**
- **Technical Adoption Manager（TAM）との協働**を通じた、Exabeam の価値を最大化するベストプラクティスの提供

Exabeam のカスタマーサクセスサービスは、経験豊富なサポートチームが 24 時間体制で対応し、Exabeam 環境の最適な運用に必要な技術的な専門知識をお客様に提供します。

Exabeam Professional Services（プロフェッショナルサービス）

Exabeam Professional Services では、お客様の成果の最大化に向けて、Exabeam の導入、統合、プラットフォーム管理を支援するデリバリーパッケージやオーダーメイドサービスを提供しています。これらの専門サービスは、デプロイの迅速化、価値創出までの時間の短縮、ポリシー管理などをお客様自身で行えるように設計されています。

- Deployment Services（デプロイメントサービス）は、お客様のセキュリティチーム内のリソースに基づいてパッケージ化された定額のオーダーメイドサービスです。これにより価値創出までの時間を短縮し、ROI を高めることができます。
- Staff Augmentation Services（スタッフ増強サービス）は、経験豊富なスタッフ（専任の常駐エンジニア、または非常駐のエンジニア）が必要に応じてお客様のリソースを補完します。

Exabeam Education（教育サービス）

Exabeam Education では、アナリストやエンジニアのスキルアップのためのリモートおよびハンズオンのトレーニングコースを提供しています（インストラクターによるトレーニングや自習用のオンラインメニューなど）。お客様のチームは、Exabeam 製品の機能を活用して、このプラットフォームから最大限の価値を引き出す方法を学ぶことができます。Exabeam の教育サービスチームは、あらゆる学習ニーズに対応したトレーニングメニューの開発に取り組んでいます。

受講いただけるコースには、次のようなものがあります。

- 高度な分析の管理
- 共通情報モデル（CIM）について
- Log Stream の基礎
- 検索について
- Exabeam のセキュリティ運用プラットフォームにおける行動分析と調査
- Exabeam のセキュリティ運用プラットフォームにおけるセキュリティ検索とダッシュボード

Exabeam について

Exabeam は、これまでのセキュリティ運用を変革する画期的な製品である New-Scale SIEM™ を提供するサイバーセキュリティ領域のグローバルリーダーです。セキュリティをめぐる状況が変化する中で、常に平時の状態を把握することで「Detect the Undetectable™（検知が不可能な脅威の検知）」を可能にする Exabeam によって、セキュリティチームはインシデント全体の包括的な視点に基づいて、より迅速かつ完全な脅威への対応が可能になります。

Exabeam について、さらに詳しく知る。

デモのリクエスト →