New Scale Analytics

業界をリードする自己調整型のユーザーおよびエンティティ行動分析（UEBA）で、脅威の検知を加速します。

多くのセキュリティチームは、膨大なアラートの管理と高度化する攻撃への対処に追われ、対応が困難です。従来型ツールは資格情報ベースの巧妙な脅威を見落としがちで、組織を危険にさらすおそれがあります。New-Scale Analyticsは脅威の検知と調査を自動化し、状況を大きく一変させます。環境に適応し、正常な状態を学習・確立し、異常を明確に可視化します。結果として、チームは最も重要な対応に集中できます。

今日の課題に対応する脅威の検知

New-Scale Analyticsは単なるセキュリティツールではなく、拡張性を前提に設計されています。既に導入済みのセキュリティ情報・イベント管理（SIEM）の上で動作し、複雑な攻撃に対する検知と対応能力を強化します。ログを分析し、脅威インテリジェンスでデータを拡充し正常行動を学習することで、異常を迅速に特定してリスクスコアを付与し、対応の優先順位付けを支援します。さらにExabeam Novaにより、調査と対応の手探りをなくし、わかりやすい脅威サマリーを入手できます。

何が正常かを把握し、そうでないものを見抜く

環境における「正常」は常に変化します。Exabeamは機械学習（ML）を用いて、ユーザー／ピア／デバイスの行動に関するベースラインを確立し、パターンの変化に合わせて継続的に適応します。異常を検知した際はフラグを立て、文脈と重大度に基づくリスクスコアを付与します。これにより、チームはノイズの選別に費やす時間を抑え、実際の脅威により多くの時間を充てられます。

New-Scale Analytics

ExabeamのUEBA機能は、機械学習（ML）に基づく行動分析、高度な相関分析ルール、事前構築済みモデルを活用し、従来型ツールが見落としがちな高度な脅威を検知します。

対象には、資格情報ベースの攻撃、内部脅威、ラテラルムーブメント（水平展開）、外部脅威が含まれます。イベント相関を自動化し、アクティビティを脅威タイムラインとして整理することで、資格情報の使用方法や攻撃者の移動先にかかわらず、組織の技術基盤全体で攻撃者の行動を追跡できます。

自動化された多層リスクスコアリング

Exabeamは高度な機械学習（ML）を用いて多層のリスクスコアを生成し、重大度に基づくアラートの自動優先順位付けを実現して、アラート疲れの軽減につなげます。さらに、ユーザーの役割、場所、行動といったコンテキスト的・業務的要因を動的に計算へ取り込みます。イベントの希少性とコンテキストの把握を組み合わせることで、アナリストは最も重大な脅威に高い精度で集中できます。

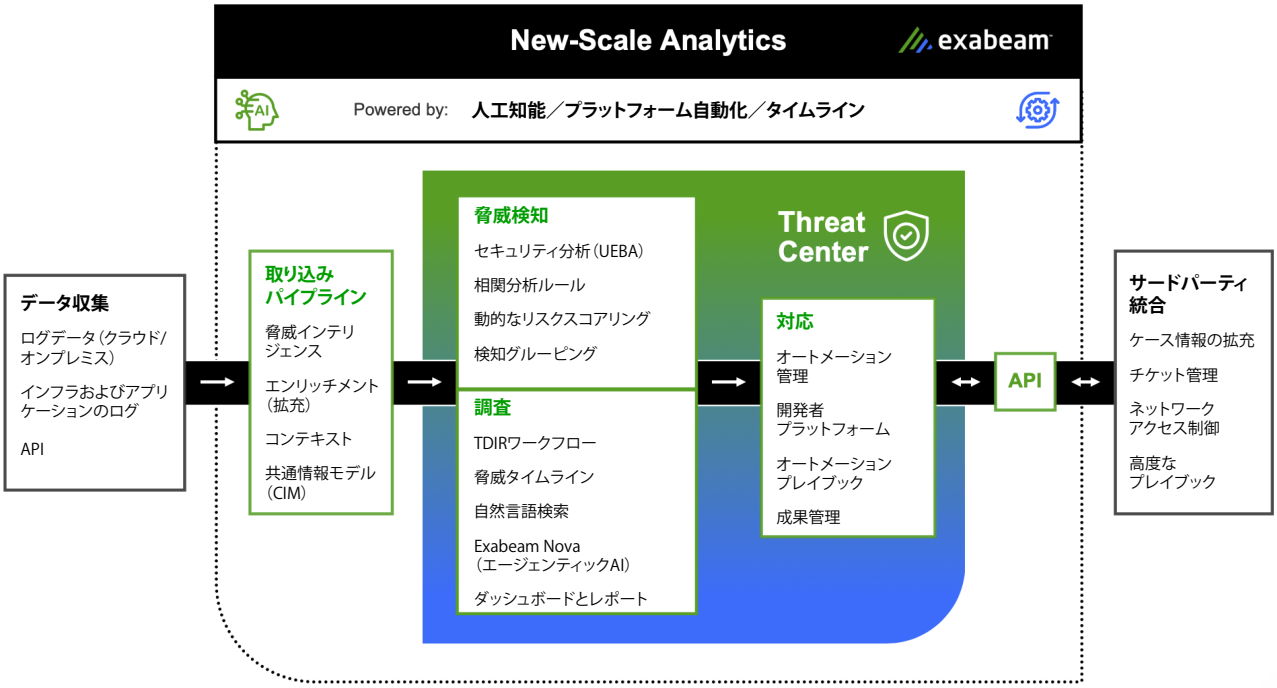

図 1. Exabeam Fusion（New-Scale Security Operations Platform）は New-Scale Analytics を支えます。

Exabeam Novaによる自然言語ベースの脅威検索

Exabeam Novaは、戦術・技術・手順（TTPs）に基づく行動検知と、侵害指標（IoC）に関する脅威インテリジェンスを統合します。アナリストは自然言語で検索を実行でき、異常特定のプロセスを簡素化し、脅威ハンティングの能力向上に役立ちます。

動的な脅威タイムライン

脅威タイムラインは、関連する証拠を自動収集・編成して一貫したイベント系列を構築し、攻撃の詳細なストーリーを形成します。各異常イベントにはリスクスコアが付与され、セキュリティチームは迅速に調査して脅威の範囲を把握できます。これらの動的タイムラインにより、アナリストはスピードと精度を両立した対応が可能です。

広範なルール・マッピングとカバレッジ評価

Outcomes Navigatorにより、アナリストはカスタム相関分析ルールを異常なTTPsに関連する行動異常へマッピングできます。さらに、一般的なユースケースに対する検知カバレッジを評価し、検知効率の向上に有効な追加ログソースを推奨します。

既存ツールとのシームレスな統合

Exabeamは、既存のセキュリティ情報・イベント管理（SIEM）、拡張型検知・対応（XDR）ツール、そして多様なログソース（クラウドデータレイク、クラウドアクセスセキュリティブローカー（CASB）、ウェブゲートウェイなど）と統合します。こうした包括的な統合により、可視性を集約し、正常行動のベースラインを確立し、多段階の攻撃経路を特定・追跡するための強力な相関機能を提供します。

ネイティブなNetMon連携による検知強化

ネットワーク・テレメトリの異常を検知エンジンに取り込むことで、Exabeamはネットワーク行動に基づく脅威の検知能力を拡張します。NetMonとの統合により、検知フレームワークにもう一つの分析軸が加わり、複雑かつ微妙なネットワーク起因の攻撃を見極める力が高まります。

動的なケース・トリアージ

Exabeamは、遅れて到着するイベントデータを進行中の調査に自動で取り込み、脅威の評価を正確かつ最新の状態に保ちます。この機能により、アナリストは調査の勢いを失うことなく、進化する脅威状況に適応できます。

New-Scale Security Operations Platform を基盤に構築

New-Scale Security Operations Platformは、組織の拡張に合わせてスケールするクラウドネイティブ基盤を提供します。ログデータの収集と分析、行動分析による攻撃の検知、インシデント対応の自動化を実現します。高度なダッシュボードでセキュリティ環境の健全性を監視し、稼働率の確保、データフローの最適化、測定可能なセキュリティ態勢の向上を支援します。さらに、プラットフォームが設定変更の推奨を継続的に提示し、ギャップを解消して防御を強化します。

New-Scale Analyticsの利点

卓越した脅威の可視性

関連イベントを特定し、数百のクエリを手動で組み立てる必要性を低減します。自動生成される脅威タイムラインがイベントを結び付け、リスクスコアとともに時系列で提示します。

自由な選択肢

既存導入済みのSIEMをそのまま活用できます。New-Scale AnalyticsはあらゆるSIEMと統合し、迅速な脅威検知と効率的な検索を提供します。

シンプルなデータソース統合

共通情報モデル（CIM）により、新たなセキュリティログ入力の取り込みと監視を容易にし、ログの収集・パースを迅速化します。

価値実現までの時間を短縮

事前構築済みコンテンツにより、数百～数千の相関分析ルールの構築・保守に費やす時間を削減します。

高リスクで異常なユーザー／エンティティ行動を自動特定

自己調整型の検知エンジンが、ユーザーおよびエンティティの正常活動を追跡し、脅威の兆候となり得る逸脱を検知します。

あらゆるスキルレベルに対応した脅威ハンティング

侵害指標（IoC）、MITRE ATT&CKにマッピングされた相関イベント、ユースケース、異常アクティビティを、生成AI対応の検索アプリケーション上で一元的にハンティングできます。

カバレッジの不足を特定して成果につなげる

主要なユースケースにセキュリティデータソースをマッピングし、データソース／推奨アクション、相関や可視化の改善に関する推奨事項を受け取れます。

手作業で設定する相関分析ルールへの依存を低減

New-Scale Analyticsが、あらゆる行動の組み合わせに対するルールのバリエーションを自動生成するため、手動設定に頼る必要はありません。

Exabeamについて

Exabeamは、世界の先進企業のセキュリティ運用を支えるインテリジェンスとオートメーションの分野をリードしています。グローバルなサイバーセキュリティのイノベーターとして、脅威の検知・調査・対応（TDIR）をより迅速かつ正確に行うための、実績あるセキュリティ特化型で柔軟なソリューションを提供します。

Learn more at www.exabeam.com →