New-Scale Security Operations Platform

AI駆動のNew-Scale Security Operations Platform：より迅速で簡単、かつ正確な脅威の検出、調査、対応（TDIR）

Exabeam Fusionとして提供されるNew-Scale Security Operations Platformは、SIEM、機械学習による脅威検出、調査、自動対応、そしてSOC全体の可視性を、1つのAI駆動型プラットフォームに統合します。行動分析、あらかじめ用意されたコンテンツ、既存ツールとのオープンなインテグレーションを組み合わせることで、効果的かつ効率的なセキュリティ運用を大規模に実現します。

- **セキュリティ運用の中核を統合：**ログ管理、UEBA、SOAR、TDIRの機能を統合し、すべてのSOC担当者を支援する一貫したワークフローを構築します。
- **オンボーディングと価値実現までの時間を短縮：**ノーコードインターフェース、共通情報モデル（CIM）、事前構築済みパーサーにより、データ取り込みを簡素化します。
- **検出と対応を改善：**脅威タイムラインを自動生成し、イベントを相関付け、高リスクの異常を優先してアナリストの迅速な対応を支援します。
- **既存投資を最大限に活用：**オープンアーキテクチャと650以上のあらかじめ用意されたインテグレーションにより、現在の技術スタックとの接続が容易になります。

自動化、行動分析、適応型リスクスコアリングを組み込むことで、New-Scale Security Operations Platformは運用負荷を軽減しつつ、脅威の検出と対応を向上させます。

あらかじめ用意されたプレイブックは対応ワークフローの標準化を支援し、可視化機能はMITRE ATT&CK®などのフレームワークに基づいて検出カバレッジをマッピングします。リアルタイム相関、自動生成されたタイムライン、AIによる検出を組み合わせることで、このプラットフォームはプロアクティブかつスケーラブルな防御戦略を支援し、より迅速で一貫性のあるTDIRと低い総所有コストを実現します。

利点

- **高リスクの脅威を正確に特定**
- **より迅速かつ正確な調査と対応**
- **脅威カバレッジの向上**
- **最も価値のあるログソースを把握**

現代のセキュリティ運用のために設計されたこのプラットフォームは、コンテキストに基づく脅威タイムラインの自動生成、調査の強化、対応アクションの標準化によってワークフローを効率化します。オープンアーキテクチャにより既存のツールと容易に統合でき、セキュリティチームが技術投資を最大限に活用しながら効率を向上させることが可能です。AIによる脅威検出と自動化された脅威管理により、New-Scaleプラットフォームは運用負荷を軽減し、セキュリティ成果を向上させます。これにより、プロアクティブかつスケーラブルな防御戦略を実現し、より迅速で一貫性のあるTDIRと低コストの運用を可能にします。

New-Scale Platformは、セキュリティワークフローにAIと自動化を適用し、最も効果的なTDIR（脅威の検出・調査・対応）を実現します。AIによる検出は、ユーザーやエンティティの通常の行動を学習することで高リスクの脅威を特定し、コンテキストに基づいたリスクスコアリングで異常の優先順位を付けます。自動化された調査は、データの相関付けと脅威タイムラインの生成により手作業を削減します。プレイブックは対応ワークフローを標準化し、可視化機能は主要なセキュリティフレームワークに対するカバレッジをマッピングします。これらの機能により、セキュリティチームはより迅速で正確、かつ一貫性のあるTDIRを実現できます。

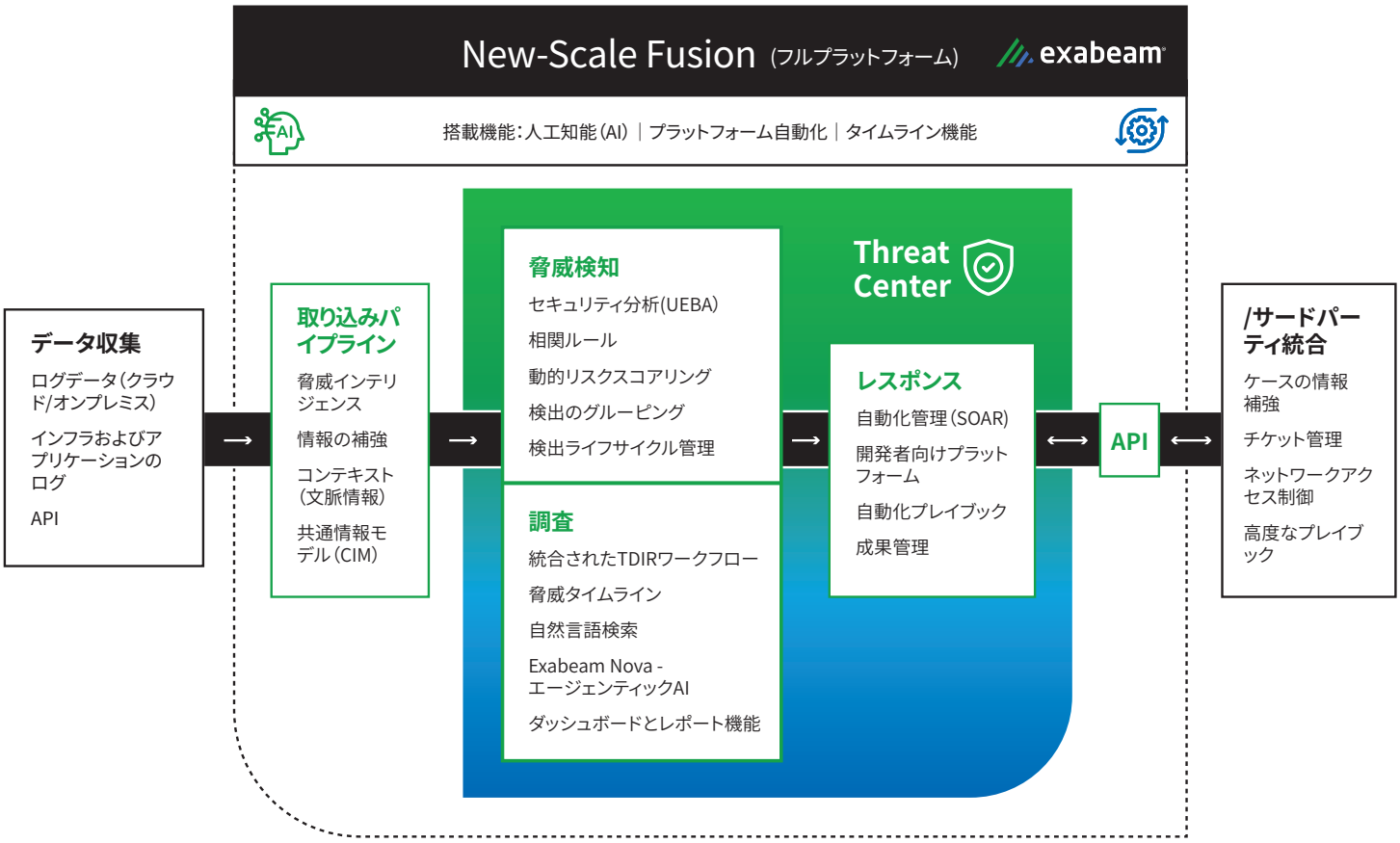

Figure 1. Exabeam Fusion, the New-Scale Security Operations Platform

AIを活用した統合型脅威管理

New-Scaleプラットフォームは、大規模なセキュリティ運用を加速させます。オープンアーキテクチャにより、ログのオンボーディングを最大70%高速化し、高度なスキルを必要とせず、既存のセキュリティ投資を最大限に活用できます。スケーラブルな保持機能、高速なデータ取り込み、AI支援によるクエリ性能により、アナリストは必要なデータへ迅速かつ柔軟にアクセスできます。

このプラットフォームには、650以上のあらかじめ用意されたインテグレーションと2,500以上の相関ルールが含まれており、脅威を自動的に検出・優先順位付け・対応します。これにより手動での調整が不要になり、検出カバレッジが向上します。

中心にあるのは、TDIR（脅威の検出・調査・対応）のための統合ワークベンチ「Threat Center」です。インテリジェントな相関分析によりアラートのノイズを60%削減し、個別のイベントだけでなく攻撃チェーン全体の緩和をアナリストが行えるよう支援します。証拠の自動収集とタイムラインの作成により調査が効率化され、あらかじめ用意されたプレイブックと対応アクションにより、修復作業を最大50%高速化します。

Exabeam Novaは、プラットフォームに組み込まれたAIエージェントのチームであり、ワークフローのあらゆる段階を強化します。Exabeam Novaは従来のAIアシスタントを超え、検出結果を積極的に相関付け、調査にコンテキストを加えて充実させ、次のステップを提案することで、チームがより迅速かつ自信を持って対応できるよう支援します。

Exabeam New-Scale Security Operations Platform 概要

Features	Core	Add-on Options
Collectors	●	
Context Management	●	
UEBA Security Analytics	●	
Threat Center	●	
Exabeam Nova	●	
Outcomes Navigator	●	
Threat Intelligence Service	●	
Log Stream	●	
Search	Past 30 days	
Pre-built Dashboards	Correlations Notable events and alerts Case management	
Custom Dashboards	●	
Detection Management	●	
Audit Logging	●	
Service Health and Consumption	●	
Notifications Service	●	
New-Scale API	●	
Correlation Rules expansion packs (100)		○
UEBA expansion packs (100)		○
Long-term Search add-on (sold by TB)		○
Long-term Storage add-on (sold by TB) - unlimited duration		○
Threat Center case retention		+90 days

機能説明

Behavioral Analytics

機械学習（ML）を用いてユーザーやデバイスの通常の行動を学習し、リスクに基づいて異常を検出・優先順位付け・対応します。500以上の行動モデルを含み、クラウド脅威検出をサポート。検出結果は自動的に脅威タイムラインに反映され、Threat Centerと統合されて調査が効率化されます。

Exabeam Nova

SOC向けに設計されたAIエージェントのチームで、スコアリング、調査、アシスタント、検索、アドバイザー、可視化などのエージェントを含みます。検出を統合し、関連エンティティを抽出、脅威を分類し、対応アクションを提案・自動化します。

Threat Center

脅威管理、調査、自動化を単一のインターフェースに統合。インテリジェントな優先順位付け、自動証拠収集、タイムライン作成により、脅威の一貫した構造的な可視化を実現します。

Automation Management

SOAR機能と事前構築済みプレイブック、ノーコードエディタを組み合わせ、繰り返し作業の自動化、対応ワークフローの標準化、迅速なインシデント対応を可能にします。

Collectors

オンプレミス、クラウド、コンテキストソースからのデータ収集を単一のインターフェースで安全に構成・管理・監視します。

Common Information Model (CIM)

共通情報モデル（CIM）：生ログデータをTDIRに最適化された構造化フィールドに正規化・分類します。

Context Management

コンテキスト管理：脅威インテリジェンス、地理情報、ユーザー・ホスト・IPマッピングでログを強化し、相関ロジックやダッシュボード、調査を改善します。

Dashboards

コンプライアンスや調査向けのあらかじめ用意された、カスタマイズ可能なダッシュボードを提供。14種類のチャート、エクスポート機能、自動検索をサポート。

Log Stream

ログストリーム：統合コンソールで毎秒200万件以上のイベントを取り込み、リアルタイム監視を提供。

Outcomes Navigator

ログデータをユースケースやATT&CKにマッピングし、検出カバレッジのギャップを特定。

Search

Exabeam Novaの検索エージェントと自然言語処理（NLP）によるAI強化検索。高速なリアルタイム・履歴検索をサポート。

Service Health and Consumption

パーサーの稼働状況、データフロー、プラットフォーム性能を監視し、ライセンス使用状況を追跡。

Threat Intelligence Service

商用およびオープンソースの脅威インテリジェンスをMLで統合・評価し、高精度なIoCを提供。

Notifications Service

メール、Microsoft Teams、Slackなどのチャネルでアラートや脅威通知を配信。

New-Scale APIs

RESTful APIを通じてセキュリティワークフローを拡張し、検索結果や相関ルールなどを外部ツールに連携可能。

オプション機能

Correlation Rules expansion

100ルール単位で販売。

Long-Term Search

検索、相関ルール、ダッシュボードを含む12か月の保持（TB単位で販売）。

Long-Term Storage

10年以上のログ保持を可能にし、検索可能な状態を維持（TB単位で販売）。

Threat Center Case Extensions

90日単位で保持期間を延長。

Additional API connections

インテグレーション容量を必要に応じて拡張可能。

Exabeamについて

Exabeamは、世界で最もスマートな企業のセキュリティ・オペレーションを強化するインテリジェンスと自動化のリーダーです。世界的なサイバーセキュリティのイノベーターとして、Exabeam は、より迅速で正確な脅威の検知、調査、対応（TDIR）のための、業界で実証された、セキュリティに特化した柔軟なソリューションを提供しています。

exabeam

詳細はwww.exabeam.comをご覧ください →