Threat Center

自動生成タイムラインと組み込みのケース管理で、より迅速かつ的確な調査を実現

セキュリティチームには迅速な検知と対応が求められる一方で、調査の複雑さや人員の制約が足かせとなり、対応が遅れがちです。

Threat Centerは、自動生成される脅威タイムラインにより、ユーザー／デバイス／行動を横断して攻撃を可視化し、対応を加速します。Exabeam Nova Risk Scoring Agentを搭載したこれらのタイムラインは、関連イベントとリスクのコンテキストを浮き彫りにし、生ログの検索や複雑なクエリに頼らずにアナリストのインシデント調査を支援します。

脅威タイムラインとは

脅威タイムラインは、ユーザーやデバイスのアクティビティを視覚的なイベント時系列としてマッピングし、セキュリティインシデントを自動的に再構成します。生ログを総当たりで精査する代わりに、「何が・いつ・なぜ」起きたかをリアルタイムに明確に把握でき、その過程で異常やリスク指標が強調表示されます。

複雑なデータを構造化された実行可能なタイムラインに落とし込むことで、アナリストは調査を迅速化し、手作業を削減し、より高精度に脅威を検知できます。

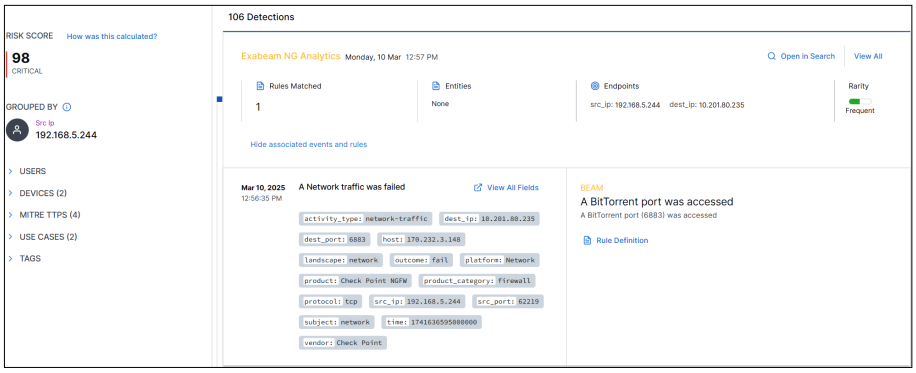

図1.
BitTorrentポートへのアクセスを繰り返し検知した自動脅威タイムライン（マルウェア活動または不正なファイル共有の可能性を示唆）

AI エージェントでインシデント対応を効率化

手作業の相関分析ルールからの脱却

従来の検知は、静的な相関分析ルールと手作業の調査に依存してきました。脅威タイムラインは従来とは異なるアプローチを取り、機械学習に基づく分析で異常を特定し、攻撃者の戦術に関する事前知識がなくても不審な挙動を強調します。

タイムラインはExabeamで構築した相関分析ルールでも、レガシーSIEMから取り込んだルールでも相補的に機能します。その結果、検知カバレッジを拡大しつつ、継続的なルール保守の負担を軽減できます。

複雑な脅威をリアルタイムに検知し対応

脅威タイムラインは、通常行動からの逸脱をリアルタイムに検知し、内部・外部の脅威の双方に自動でフラグ付けします。機械学習が発生時点で異常を強調するため、アナリストが散在するログをふるいにかけたり、攻撃シーケンスを手作業で復元したりする必要がなくなります。

ラテラルムーブメント（水平展開）を明確に追跡

ラテラルムーブメント（水平展開：攻撃者がシステム間を移動する挙動）は、従来型ツールでは検知が難しいことが少なくありません。脅威タイムラインはユーザーや資産を横断してアクティビティを関連付け、高リスク行動にフラグを立て、移動パターンを可視化します。これにより、アナリストは攻撃の追跡を迅速化し、精度の高い対応が可能になります。

脅威タイムラインのプロセス

ステップ 1：ログの収集

Exabeamは、300を超えるクラウドおよびオンプレミスのソースからセキュリティデータを取り込み、脅威タイムラインの作成を支援します。主なソースは次のとおりです：

- **Microsoft Active Directory（AD）：**Windows環境におけるユーザーとマシン間の認証イベントを記録します。
- **Azure AD：**監査ログ、サインインログ、Identity Protectionログを含み、認証アクティビティやセキュリティイベントの可視性を高めます。
- **クラウドインフラ：**AWS／Azure／GCP環境への広範なアクセスを許可するポリシー変更を記録します。
- **クラウドアプリケーション：**SalesforceやWorkdayなどのプラットフォームのアクティビティを記録し、データ持ち出しの兆候を検知します。
- **Okta：**ユーザー／グループ／デバイスを横断的に、アイデンティティおよびアクセスのイベントを追跡します。
- **ファイアウォール：**ネットワークの境界やセグメント化された環境におけるユーザーのアクティビティを記録し、アクセス試行や潜在的な脅威を特定します。
- **エンドポイント セキュリティ ツール：**作成／変更／削除といったファイル操作を追跡し、侵害や不正使用の兆候を検知します。

ステップ 2：ログを実行可能なデータにパース

セキュリティログは情報量が多く、ベンダー間で形式も不統一です。Exabeamは 9,500以上の事前構築済みパーサーでログを自動的に構造化フィールドへパースし、この複雑さを解消します。既存のパーサーがない場合でも、Log Streamによりカスタムパーサーを迅速に作成でき、処理ボトルネックを取り除けます。

さらにExabeamは、すべてのソースからのデータを共通情報モデル（CIM）で正規化します。こうした標準化によりベンダー間の一貫性が保たれ、検索・分析・検知への活用が容易になります。

ステップ 3：ログフィールドの組み合わせによるイベント生成

Exabeamは関連するログフィールドを自動的にグルーピングして、意味のあるセキュリティイベントを生成します。これにより、アナリストが数千件の生ログを手作業で精査する必要がなくなります。ログを構造化イベントとして整理することで、手作業の解釈に頼らずにアクティビティの追跡や脅威タイムラインの構築を容易にします。

ステップ 4：AIによるコンテキスト付与

生ログだけでは、セキュリティイベントの理解に必要なコンテキストが不足しがちです。Exabeamは機械学習（ML）・行動分析・サードパーティのインテリジェンスなどのAIを用いて、ログデータをリアルタイムに拡充（エンリッチ）し正規化します。HadoopやSnowflakeのようなデータレイクにログを蓄積して事後処理に頼るのではなく、取り込み時点で断片的なログを構造化された実行可能なインサイトへと変換します。

このAI 駆動のデータ拡充（エンリッチメント）により、時間を節約し、複雑さを低減でき、アナリストは難解なログ形式の読解ではなく実在する脅威への対処に集中できます。

データ拡充（エンリッチメント）の内容：

- **ユーザー種別の分類：**実ユーザーアカウントと自動化されたシステムアカウントを区別します。
- **資産種別の識別：**ホスト名・IPレンジ・行動パターンに基づき、ホスト／IPアドレスがワークステーション、サーバー、クラウドリソースのいずれに属するかを判定します。
- **ピアグループ・マッピング：**類似行動のユーザーを自動的にグループ化し、異常検知の精度向上と誤検知の低減につなげます。
- **資産オーナーシップの検出：**特定のシステムやデータに通常アクセスするユーザーを特定し、その関係から逸脱したアクセス試行にフラグを立てます。
- **IPとホスト名の関連付け：**IPアドレスをホスト名に紐付け、ラテラルムーブメントやステルス的な攻撃パターンを可視化します。

Exabeamはマルコフモデリング（Markov modeling）も適用し、確立済みの行動パターンと照合することで、想定外の権限昇格や不自然なアカウント作成などの異常なイベント系列を検出します。これらのモデルは動的な環境に適応し、静的な検知手法では見落とされがちなリスクを明らかにします。

調査をさらに効率化するため、Exabeamは以下を行います。

- **イベントコードを平易な表現に翻訳し**、アナリストの認知負荷を軽減します。
- リモートログイン、DLPアラート、メールアクティビティなどの**イベントをエンリッチメント**し、検知カバレッジを拡大します。
- 業界固有のユースケース、社内ポリシー、検知の優先度に基づく**エンリッチメントのカスタマイズを可能に**します。

これらの機能により、アナリストはユーザー／デバイスの行動をコンテキスト付きでリアルタイムに可視化でき、検知を加速し、精度を向上させ、断片的なログを手作業でつなぎ合わせる必要をなくします。

ステップ 5：セッションの作成とリスク評価

Exabeamは、関連イベントをセッション（一定期間におけるユーザーまたはデバイスの活動を表す時間ウィンドウ）にまとめます。個別のログを単体で分析するのではなく、行動の一連の流れを俯瞰できるため、異常の検知や意図の把握が容易になります。

たとえば、勤務日全体を1つのセッションとして、ログイン、ファイルアクセス、システムとのやり取りをすべて取り込みます。この構造により、通常の活動と、異常なアクセスや権限の使用といった侵害の兆候を見分けやすくなります。疑わしい挙動が蓄積すると、Exabeamはそのセッションに動的なリスクスコアを算出します。事前に定義したしきい値を超えたユーザー／エンティティは注目対象（Notable）としてフラグが立ち、優先度の高い脅威に即時の調査の焦点を当てられます。

ステップ6：AI駆動の行動モデリング

Exabeamは機械学習で学習した行動モデルを用いて、正常活動からの逸脱を検知し、静的ルールでは見落としがちな脅威を顕在化させます。これらのモデルは、ユーザーの役割、アクセスパターン、位置情報などの状況的要因を分析し、イベントが想定どおりかリスクが高いかを判断します。

たとえば、あるユーザーが通常は米国・カナダ・ドイツからログインしているのに、突然中国から認証した場合、Exabeamはユーザーの履歴プロファイルに基づき不審な挙動としてフラグを立てます。

大量の履歴データを必要とする従来システムと異なり、Exabeamのモデルは数週間分の活動から学習を開始します。挙動の変化に応じて動的に調整し、進化する環境でも継続的な検知を可能にします。Exabeamには735超の事前構築済みモデルが含まれており、データサイエンスの専門知識なしで検知を微調整できます。こうした柔軟性により、誤検知の低減、アラートの信頼性向上、組織固有の環境への適応が実現します。

ステップ 7：異常検知

Exabeamは複数の異常検知モデルを適用し、時間・場所・行動パターンをまたいでユーザー／システムの活動を分析します。静的ルールに依存するのではなく、適応型モデルで予期しない挙動をリアルタイムに検知します。

各異常はセッションの総合リスクスコアに寄与します。スコアが設定しきい値を超えると、システムはユーザー／エンティティを自動的に調査対象としてフラグを立て、アナリストの負荷を増やすことなく高リスク活動を優先的に提示します。

不要なノイズを抑えるため、アナリストは特定の異常タイプ、個別インシデント、あるいはセッション全体をミュートできます。カスタマイズ可能なアラートにより、重要な脅威に集中でき、雑音の最小化と対応効率の向上につながります。

Exabeam Nova Risk Scoring Agentを基盤とする異常検知は、変化する挙動に基づいて継続的に適応し、学習の進展に伴ってより正確で関連性の高いアラートを提供します。

ステップ8：異常活動に基づくリスクスコアリング

Exabeam Nova Risk Scoring Agentは、行動上の異常と状況的要因に基づいて動的なリスクスコアを付与します。セッション内で不審な活動が蓄積するとスコアが上昇し、即時対応が必要なユーザー／エンティティを特定しやすくなります。

日常的な活動と真の脅威を区別するために、Exabeamはベイズ統計モデルを用い、各イベントの希少性と重大度を加味します。たとえば、通常のログインはリスクが最小である一方、パスワードリセットや特権アカウントの作成はより高いスコアとなります。

リスクしきい値は、イベントの種類や行動のコンテキストによって異なります。たとえば、ユーザーが初めてサーバーにログインした後に大量の特権操作を行った場合、Exabeamはセッションのリスクスコアを引き上げ、調査対象としてフラグを立てます。

リアルタイムに継続的なスコア調整を行うことで、Exabeamはアナリストが最重要インシデントに集中できるよう支援し、誤検知の低減と検知精度の向上を実現します。

ステップ 9：TDIRにおける脅威タイムラインの活用

脅威タイムラインは、トリアージ・調査・対応のための統一かつ直感的なインターフェースを提供し、脅威の検知・調査・対応（TDIR）全体のワークフローを効率化します。ばらばらのアラートを個別に確認するのではなく、関連アクティビティを時系列で示し、コンテキストの詳細な情報・リスクスコア・視覚的指標によって意思決定を支援します。

ユーザーまたはデバイスがリスクしきい値を超えると、Exabeamは注目対象として自動的にフラグを立て、アナリスト用ダッシュボードにタイムラインを表示して即時対応を促します。アナリストは関連エンティティを掘り下げ、攻撃経路を追跡し、他のユーザーや部門へ調査を拡張して、深刻化する前に関連脅威を明らかにできます。

脅威タイムラインは、SOAR（セキュリティオーケストレーション／自動化／対応）プレイブックと連携し、封じ込めや是正の自動化をサポートします。アナリストは同一インターフェース内で、IPのブロックやアカウントの無効化などの直接アクションを、ツールを切り替えることなく実行できます。

追加機能：

- **迅速なアラートトリアージ：**タイムラインが関連イベントを結び付け、重大度と影響を数秒で把握できるようにします。
- **脅威ハンティングの簡素化：**MITRE ATT&CKにマッピングされた戦術・技術・手順（TTPs）を、複雑なクエリを書かずに検索できます。
- **効率的なインシデント対応：**Exabeamがインシデント種別、影響を受けたユーザー、行動のコンテキストなどの主要情報で自動分類し、段階的チェックリストで調査をガイドします。

脅威タイムラインにより、アナリストは生ログをふるいにかけることなくイベントの詳細を迅速に確認できます。ユーザー／デバイス／資産をまたぐ関連アクティビティを自動的に浮き彫りにすることで、調査時間を短縮し、高度な専門知識への依存を抑えます。こうした広いコンテキストにより、追加クエリを実行しなくてもインシデントの全体像を把握しやすくなります。

集中型のワークベンチが関連データを一元化し、あらゆるスキルレベルのアナリストが自信を持って迅速に調査・対応できるようにします。ユーザー行動のリアルタイムな関連情報ビューを提供することで、Threat Centerは調査の完了とインシデント解決をより効果的に後押しします。

結論

Exabeam NovaのAI エージェント群は、インシデント再構成を効率化し、検知・調査・対応を加速します。イベント相関の自動化と関連するコンテキストの強調により、タイムラインは手作業を排し、アナリストが高優先度の脅威に集中できるようにします。

直感的なインターフェースとAI 駆動のインサイトにより、セキュリティチームはより賢く、より迅速に対応し、進化するサイバー脅威に先手を打てます。

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 →