侵害された資格情報

機械学習に基づく脅威の検知と自動対応で、
アイデンティティの不正使用を早期に見抜く

脅威を理解する

多くの攻撃者は“こじ開ける”のではなく、普通に“ログイン”します。

侵害された資格情報は、依然として攻撃者にとって最も効果的なツールの一つです。フィッシング、侵害（情報漏えい）、ブルートフォース攻撃、トークン窃取などによる、資格情報を悪用した侵入は、境界防御をすり抜け、検知されることなく活動することを可能にします。いったん内部に侵入すると、攻撃者は権限を昇格させ、セキュリティ制御を無効化し、ラテラルムーブメント（水平展開）します。潜伏期間が長引くほど、データ窃取やランサムウェア、長期的な潜伏のリスクが高まります。

Verizon社のデータ侵害調査報告書（DBIR）によると、過去10年間において、侵害インシデントの31%で盗まれた資格情報が悪用されており、極めて危険な攻撃ツールであることが示されています。

従来型のSIEMツールでは、こうした脅威をタイムリーに検知することに苦慮しています。正規のユーザーの振る舞いを模倣するIDベースの攻撃は、静的ルールではほとんど見逃されがちです。Exabeamは、それとは異なるアプローチを提供します。異常を可視化し、リスクを相関付け、自動化された対応を起動します。

Exabeamでアイデンティティベースの攻撃に先手を打つ

Exabeamは、資格情報の侵害を早期に検知し、その影響範囲を把握して、事態が深刻化する前に攻撃者を阻止するのに役立ちます。Exabeam New-Scale Security Operations Platformは、機械学習による脅威検知・自動化・リスクスコアリングを組み合わせ、静的な指標に頼らず異常な活動を浮き彫りにします。

Exabeamで得られること：

- 盗難資格情報、トークン悪用、リモートアクセス、サービスアカウントの不正利用など、アイデンティティ不正使用の機械学習による検知
- ユーザーとシステムの挙動を結び付ける、コンテキスト対応の調査タイムライン
- 手動トリアージを必要とせずに、脅威の優先度付けと対応エスカレーションを行う自動リスクスコアリング

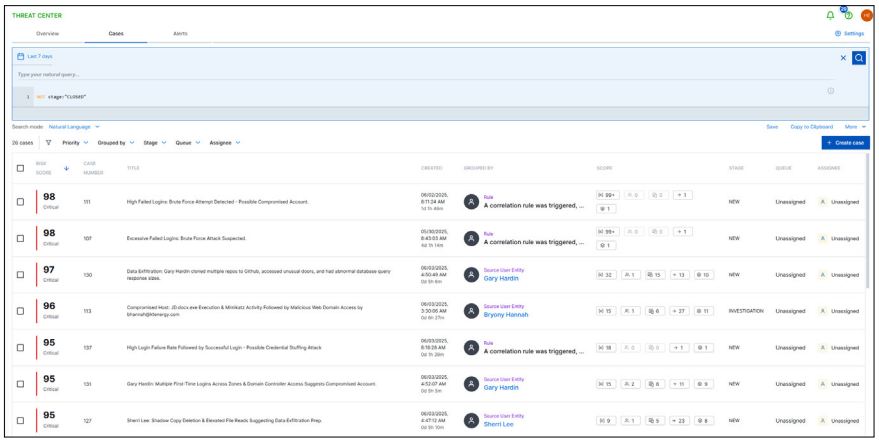

図1.
BitTorrentポートへの送信トラフィック失敗を示す脅威タイムライン。リスクのコンテキストと検知ルールに基づき不審としてフラグ付け。タイムラインは送信元IPごとにアクティビティをグルーピングし、プロトコル、ファイアウォール製品、宛先ホストといった関連フィールドを相関付けることで、アナリストによる不正使用やポリシー違反の調査を支援します。

課題1：侵害されたアカウントの検知

問題

資格情報の不正使用は、一見「通常の挙動」に見えがちです。静的ルールでは、異常なログイン時刻、トークンの再利用、場所の不整合といった微妙な兆候を捉えられません。

解決策

Exabeamは、ユーザー／デバイスごとに平常時の振る舞い（ベースライン）を学習し、そこからの逸脱を検知します。これにより「物理的に不可能な移動」「初めてのアクセス」「多要素認証（MFA）の異常な振る舞い」といった、資格情報の不正使用を示す兆候を明らかにします。

Outcomes Navigator は、アイデンティティログ・VPNセッション・認証イベントなどのデータソースの優先順位付けを支援し、検知カバレッジと可視性を向上させます。

Exabeamは静的ルールでは見逃されがちな早期の侵害指標（IoC）を顕在化させます。あらかじめ用意された検知モデルにより手動のルール調整が不要になり、設定負荷を削減して価値実現までの時間（Time to Value）を短縮します。

例：あるユーザーが、勤務時間外に未知のドメインから不審な実行ファイル（suspicious.exe）をダウンロード。Exabeamは、このイベントを相関分析して、ユーザーのリスクスコアを引き上げ、事態が深刻化する前に脅威として警告します。

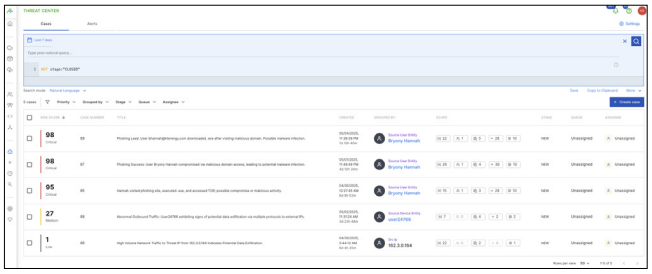

図2.

高リスクユーザーが不審なドメインから実行ファイルをダウンロードしたタイムライン。Exabeamが活動を相関分析し、事態が深刻化する前にリスクスコアを引き上げます。

ExabeamのData Insightsは、主要な挙動を要約し、関与ユーザーを特定。アナリストが不審な活動をひと目で評価できるよう支援します。

効果

既知シグネチャがなくても、Pass-the-Hash、トークン窃取、権限の不正利用などの高リスク行為を早期に可視化できます。

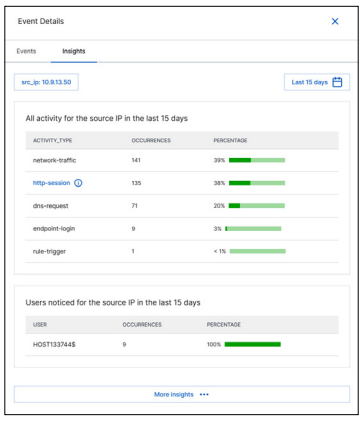

図3.

不審IPに対するユーザーアクティビティを要約したData Insights。過去15日間のHTTP／DNSの頻繁な挙動を強調表示しています。

課題2：IDドリブンな攻撃の調査

問題

従来型ツールでは調査が遅く、複雑で誤りが生じやすいのが現実です。アナリストは多数の手動クエリを実行せざるを得ず、アラート疲労を招きます。その結果、67%のアラートが無視されています。

解決策

Exabeamは、ユーザー／ホスト／IPを横断して挙動を相関分析し、タイムライン生成を自動化します。Threat Centerは関連する MITRE ATT&CKの戦術、ユースケース、エンドポイントを含む攻撃の全体像を提示します。

内蔵AIアシスタントであるExabeam Novaは、ケースの種別を分類し、関連エンティティを抽出し、次のアクションを提案します。これによりアナリストは、豊富なコンテキストを備えた検知内容と生ログを活用し、複雑なクエリを記述することなく調査を迅速化できます。

脅威タイムラインの自動生成機能は、価値の低い作業を最大30%削減し、迅速かつ根拠ある意思決定に集中できるよう支援します。

r-tec社は、Exabeam導入後、顧客からの調査依頼コールを80%削減しました。

効果

アナリストは、不審な活動の全体像を優先順位付けされた形で数分で把握でき、手作業を削減しながら調査の精度を向上できます。

実際の攻撃の90%で、侵害された資格情報が悪用されています。r-tec社のサイバーディフェンスセンター（CDC）がExabeam を導入した決め手は、単なるアラートに頼るのではなく、複数ソースからの振る舞い分析によってこれらの脅威を検出できるからです。

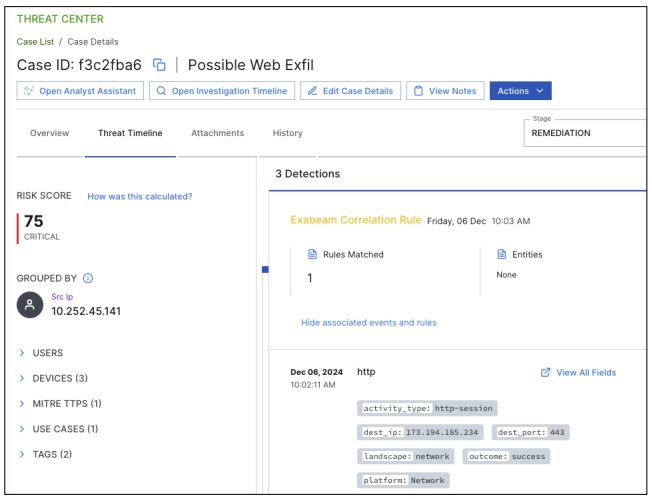

図4.

脅威タイムラインの自動生成：個人メールへの大量データ送出を、関連する複数の異常検知を相関分析し、脅威として警告しています。

課題 3：アカウント乗っ取りへの対応

問題

連携の取れた対応ワークフローがないと、資格情報を悪用する攻撃により事態が急速に深刻化する可能性があります。

解決策

Automation Managementが、セキュリティスタック全体にわたる対応アクションをオーケストレーションします。高リスクユーザーはウォッチリストに登録され、アラートはメールやWebhook で自動送信できます。SOAR連携により、セッションの強制終了やアカウント無効化といった是正措置を実行可能です。

対応はMITRE ATT&CKのテクニックに準拠しており、柔軟性に欠けるスクリプトに依存せず精緻な運用を実現します。

効果

振る舞い駆動による自動化されたワークフローにより、脅威の潜伏時間（dwell time）が短縮され、アナリストはより迅速に行動できます。

The Missing Link社は、Exabeamの導入により、検知および対応にかかる時間を50%以上削減しました。

組み込みの検知コンテンツ

Exabeamは、MITRE ATT&CKに準拠した検知コンテンツを継続的に更新して提供します：

検知例

- 盗まれた資格情報の使用、またはなりすましトークンの利用
- 多要素認証（MFA）の回避または改ざん
- 未知の場所やデバイスからの不審なアクセス
- 異常なセッションハイジャックやCookieの窃取
- Torなどの匿名化サービスの使用

主要データソース

- 認証／IDログ（SSO／IAM／MFAプラットフォーム）
- OSログ（Windows／Linux／Mac）
- クラウドアプリケーションのテレメトリー
- VPNおよびゼロトラストのアクセスログ
- EDRツール
- ファイアウォール／プロキシのログ
- ファイルアクセスおよびDAM（Database Activity Monitoring）ログ
- アプリケーション／SaaSのアクティビティログ

Outcomes Navigatorは、これらのソースをMITRE ATT&CKのテクニックおよび検知ユースケースにマッピングし、オンボーディングとカバレッジを向上させます。

主要な検知ルール

Exabeamは、以下を含む事前構築済みのルールとモデルにより、資格情報の不正使用を検知します：

- ファイル・データベース・VPN・アプリのアクセスパターンにおける逸脱
- リスクの高い／不自然な地理位置からの認証試行
- 悪意あるウェブサイトへのアクセス
- ネットワークスニファの使用
- 資格情報ダンピングに関連する不審なプロセス活動
- 連携ツールからのアラート
- 特権ユーザーによるラテラルムーブメント（水平展開）
- ハイブリッド環境全体にわたる窃取の兆候

MITRE ATT&CKテクニックのカバレッジ

対象となる主なテクニック例：

- 資格情報へのアクセス（Credential Access）：T1003、T1552、T1555
- 初期アクセス（Initial Access）：T1110、T1133
- 防御回避（Defense Evasion）：T1027
- 探索／収集（Discovery／Collection）：T1083、T1213
- C2（コマンド＆コントロール）／データ持ち出し（Exfiltration）：T1102、T1071、T1567
- ネットワーク傍受（Network Interception）：T1040、T1557
- 資格情報の使用（Credential Usage）：T1078

これらのマッピングにより、資格情報の不正使用、リモートアクセスの濫用、IDの永続化（Persistence）の検知に役立ちます。

対応アクション

Exabeamは、IT・人事・セキュリティ各種ツールと連携したカスタマイズ可能なワークフローをサポートします。チームは次の対応が可能です：

- ユーザー／管理者／人事部門への通知
- 高リスクなエンティティの検索を実行
- 是正対応のためのITチケットを起票
- 監査対応に備えたインシデント対応チェックリストの参照

資格情報を狙う脅威に先手を打つ

多くのツールが「侵害そのもの」に注目するのに対し、Exabeamは「振る舞い」に着目します。

機械学習に基づく脅威検知、コンテキスト情報が豊富なタイムライン、自動化された対応により、Exabeamは資格情報ベースの攻撃を事態が深刻化する前に封じ込めます。

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。

exabeam

Learn more at www.exabeam.com →