脅威検知・調査・対応のアーキテクチャ設計

AIを核とするNew-Scale Security Operations Platformは、脅威の検知・調査・対応（TDIR）を包括的に管理できるクラウドネイティブの統合ソリューションです。複数の製品を連携させることで、効果的なセキュリティオペレーションセンター（SOC）を運営する際に必要となる労力を大幅に削減できます。

本ホワイトペーパーでは、New-Scale Platformがいかにして脅威カバレッジを実現するかを解説します。同プラットフォームは、MITRE ATT&CK®フレームワークをはじめとする既存の知識や手法を活用し、脅威検知に必要なシグナルを的確に収集・処理します。この技術によりトリアージを高速化し、SOCリソースの効率的な活用を促進。さらに、相関ルールと機械学習ベースのユーザー／エンティティ行動分析（UEBA）という業界最先端の検知機能を駆使し、アラート発報とケース管理を自動化します。

本書では、ログ、Active Directory（AD）、クラウドリソース、その他のセキュリティ製品からデータを収集するためのCloud CollectorとSite Collectorの設定手順をはじめ、パーサーのチューニング、取り込みコンテンツのカスタマイズ、コンテキスト強化によって侵害指標（IoC）を検知する堅牢なイベントモデルを構築する方法をご紹介します。また、Outcomes Navigatorを用いて既存ログやデータストリームが特定のMITRE ATT&CK脅威検知に適しているかを評価する方法、検知ルールの選択、異常検知の感度調整、インシデント対応の自動化、説明責任やコンプライアンスに向けたダッシュボード・レポート作成の手順も取り上げます。

セキュリティ運用のスケーラビリティ課題に対応する

既存のセキュリティ情報・イベント管理（SIEM）基盤を扱うセキュリティアーキテクトは、スケーラビリティの課題に直面しています。脅威が増え続ける現在、10年前どころか5年前のSIEMツールでさえ、今日のセキュリティアーキテクチャが抱える根本的な問題である、対応可能なリソースをはるかに上回る膨大なアラート件数に追いつけなくなっています。

この課題を解決するには、以下のステップを統合した包括的なソリューションが必要です。

- 多種多様なソースから、大量のデータをリアルタイムで収集すること
- 収集データをイベントへ変換し、検索可能にすること
- 既知のパターン照合と異常検出により、脅威を識別すること
- 潜在的な脅威の一部をアナリストが調査すること

しかし、これらの要件を真に統合的に満たす製品はほとんどありません。New-Scale Platformは従来のSIEMが補えない部分をカバーし、エンドツーエンドのTDIRプロセスを支援するモジュール型ツール群を提供します。

Site CollectorとCloud Collectorは、ログやイベント、他社セキュリティ製品からデータを収集し、ユニバーサルパイプラインへ転送します。Exabeamは340社以上、650を超えるサービス向けのコレクターを用意しています。

- **Cloud Collector：**Microsoft Azureなど40以上のクラウドサービスに対応
- **Site Collector：**ローカル設置でAD、syslog、Splunk、LDAPなどを収集
- **Context Collector：**脅威インテリジェンスやジオロケーションなど外部コンテキストを付与

New-Scale Platformの**Log StreamとContext Management**は受信したデータを解析し、共通情報モデル（CIM）に整合させます。

Outcomes NavigatorはイベントをMITRE ATT&CK フレームワークなどにマッピングし、ログおよび相関／異常イベントルールの可視性を評価したうえで、カバレッジ向上に役立つ追加ログやフィールドを提案します。

Correlation Ruleは、あらかじめ用意されたルールやカスタムルールを用いて脅威を検知します。

UEBAは機械学習でユーザー・デバイス・ピアグループの行動ベースラインを確立し、そこからの逸脱をもとに脅威を検知します。

Exabeam Novaは自動化された調査サマリーの範囲を大幅に拡張し、セキュリティ運用を加速させる豊富で実用的なインサイトを提供します。高度なデータ相関分析とコンテキスト分析を活用し、数十あるいは数百件におよぶ検知結果を構造化された分かりやすい調査サマリーへと凝縮します。複雑な脅威パターンを分類・解釈できるよう設計されており、「内部不正」や「悪意ある内部者」などの主要ユースケースと各ケースを整合させます。

調査が開始されると同時に、Exabeam Novaは自動的に予備的なケース分析を生成し、アナリストが個々の検知結果を確認する前に重要なコンテキストを提供します。ユーザー、デバイス、役割などの関連エンティティを特定・抽出し、明確で構造化された形式で提示します。これにより精度が向上し、誤検知が減少し、修復のためのガイダンスも得られるため、セキュリティチームはより迅速に、より確信と精度をもって対応できるようになります。

Automation Managementはアラート通知やサードパーティのITサービス管理ツール(ITSM)、コラボレーションツール連携を含む対応プロセスを自動化します。

本書では、こうした統合型セキュリティアーキテクチャを段階的に解説し、New-Scale Platformが限られた貴重なセキュリティリソースを最適活用する方法をご案内します。

イベント量が急増する中でSOCの効率を最大化する

ここ本書でご紹介するプロセスは、オンプレミス環境・クラウド環境・ハイブリッド環境を問わず、既存のセキュリティ基盤にシームレスに組み込めるよう設計されています。組織規模やユーザー数にかかわらず適用でき、各種ログ管理／SIEM製品を併用したい場合も、まだ仕組みが整っていない場合も柔軟に対応できます。

プロセスの前提となるのは、MITRE ATT&CKフレームワークやExabeamユースケースカバレッジ分類を用いて、自組織の優先課題と目指す成果を明確にすることです。

このアプローチは、限られたアナリスト工数でしかも固定的、あるいは増加傾向にある大量のイベントを「識別 → IoC化 → 適切な修復」まで処理しなければならない組織に最適化されています。大量のイベントを前にSOCチームが手いっぱいになりがちな状況で性能を高める方法は、①チームを拡充するか②既存アナリストの生産性を引き上げるかの二択ですが、さまざまな理由から後者を選ぶのが得策です。

- **コスト効率：**SOCの効率を高める方が、人員を増やすより高い投資対効果（ROI）を得やすくなります。
  - Forrester TEIレポート（2022） — New-Scaleプラットフォームの中核「Exabeam Fusion SIEM」は、3年間で245 %のROIと6 か月未満の投資回収期間を達成しています。
  - NEC Australia —プラットフォーム効率・運用負荷削減・アナリスト生産性向上の相乗効果により、コストを35 %削減しました。
- **エンゲージメントと効率の向上：**アナリストは定型的な作業に費やす時間を減らせるため、業務効率が高まり、仕事への満足度も向上します。
- **チーム拡大に伴う課題：**人員を増やすには、競争の激しい人材市場でアナリストを採用して育成しなければならず、適任者を確保するのが難しい場合があります。
- **質的なメリット：**生産性向上は単に処理件数を増やすことだけではなく、誤検知の削減、対応時間の短縮、記録保持やコンプライアンスの改善など、より良い成果を達成することによっても評価されます。

たとえば、資格情報の侵害をとりわけ重視している組織を例にとってみましょう。資格情報侵害は数ある優先課題のひとつにすぎませんが、New-Scale Platformを使ってセキュリティ体制を分析・改善する方法を示す好例となります。実際には、どの優先課題を調査してカバレッジを強化する場合でも、手順は同じですし、順番に進めても並行して進めてもかまいません。

本書では手順を直線的に並べて説明していますが、実際のプロセスは反復的かつ継続的である点に留意してください。たとえば、障害や再構成、ベンダーのログ形式変更に備えてデータ品質を維持できるよう、データソースの可用性やパース状況を定期的に点検します。また、新たな脅威に対応するためにコレクターやパーサーを追加してカバレッジを向上させ、インシデントトリアージや定型対応の自動化を進めて、アナリストがより高度な調査に専念できる時間を確保していきます。

AI駆動のNew-Scale Security Operations Platformでセキュリティ態勢を強化する

本書では、New-Scale Platformを活用して次のことを行う方法をご紹介します。

1. 目標とするセキュリティ成果に合わせてデータソースを選定する
2. クラウドとオンプレミスからデータ／ログを収集する
3. データを抽出し、共通情報モデル（CIM）を適用する
4. 抽出データをリスクモデルへマッピングする
5. ルールベース検知と異常検知を構築・チューニングする
6. インシデントレスポンスを自動化する
7. ダッシュボード出力を保存し、透明性とコンプライアンスを確保する

ステップ 1：

データソースの選定組織が扱うデータソースは、オンプレミスの多様なシステムからクラウド上のアプリケーションやインフラまで幅広く存在します。これらのデータをより多く取り込むことで、通常はセキュリティ管理の精度が向上します。以下はその一部の例です。

- Microsoft AD ログ：ドメインコントローラーでのユーザーとマシンの認証イベント
- Azure AD ログ：監査ログ、サインインログ、Identity Protectionなど
- AWS、Azure、GCPにて過剰な権限を持つユーザを作成あるいはユーザーにポリシーを追加
- SalesforceやWorkdayからのデータ持ち出し
- Oktaディレクトリマッピング・ファイアウォール製品のログ：ネットワーク境界、セグメントを越えるユーザーアクティビティ
- エンドポイント製品のログ：ファイル削除・作成などのファイル操作

ただし、プラットフォームは膨大なデータを取り込めるものの、利用可能なデータポイントをすべて保存する必要はありません。Outcomes Navigatorは、セキュリティユースケースや期待する成果に照らしてデータソースを賢く評価する手段を提供します。評価後、選定したソースはCollectorsでオンボードし、Context Managementでエンリッチし、Log Streamで活用を強化できます。

Outcomes Navigatorでは、Exabeamユースケースカバレッジモデルあるいは MITRE ATT&CKフレームワークの観点から環境を分析するかを選択できます。選んだフレームワークに基づき、重点的に対処すべき脅威を決定します。Outcomes NavigatorはExabeamプラットフォームに取り込まれるログフィードを代表的なセキュリティユースケースへマッピングし、カバレッジを高めるために追加すべきログやパーシング改善案を提案します。

たとえばランサムウェア対策から着手するとしましょう。ホーム画面（図 1）から Outcomes Navigator（図 2）を開き、Use Case Coverageタブ → External Threats → Ransomwareを選択すると、ランサムウェア用ユースケース詳細ページ（図 3）が表示されます。そこで必要ログや追加設定の推奨事項を確認できます。

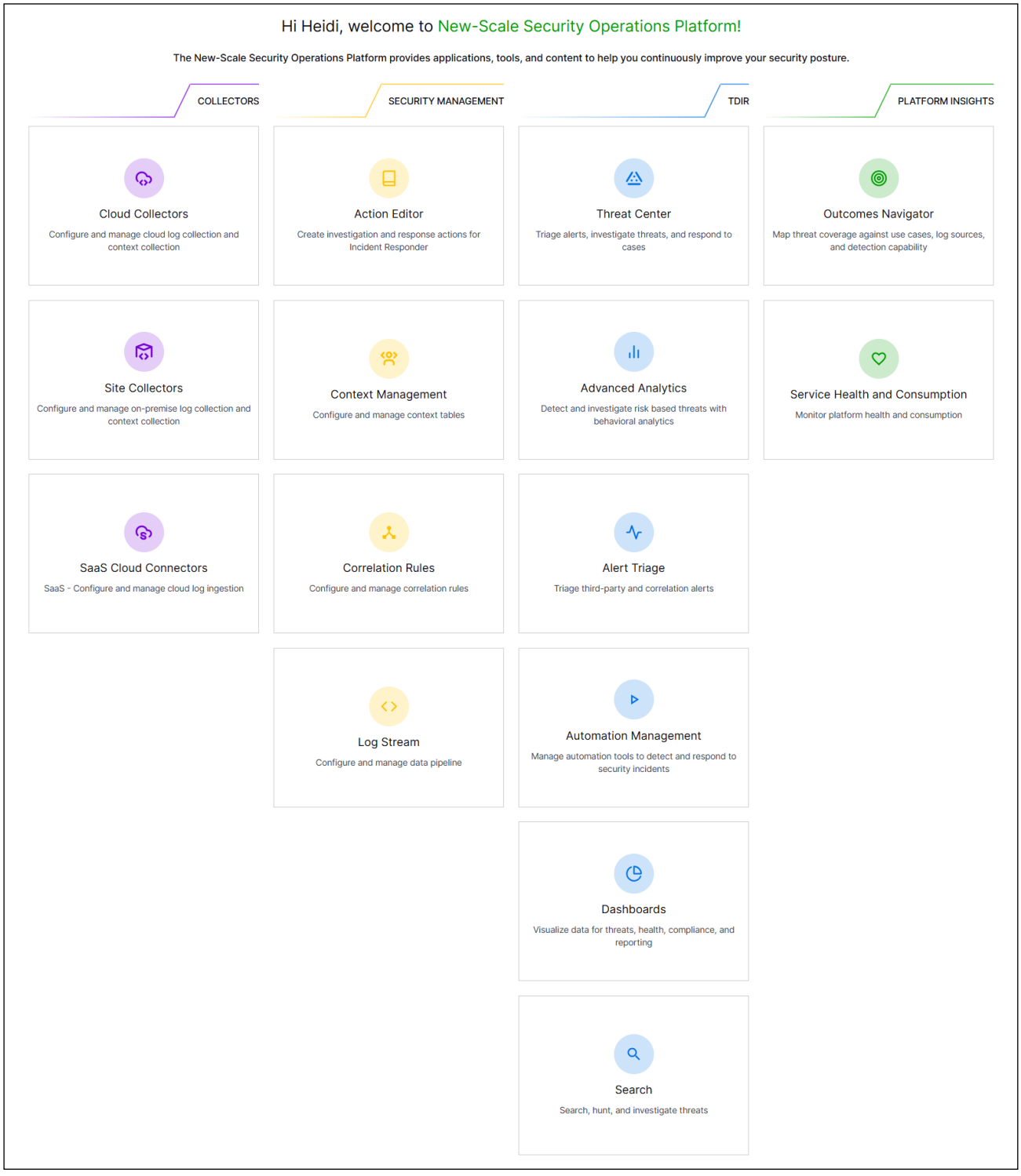

図1. Exabeamアーキテクチャモデル

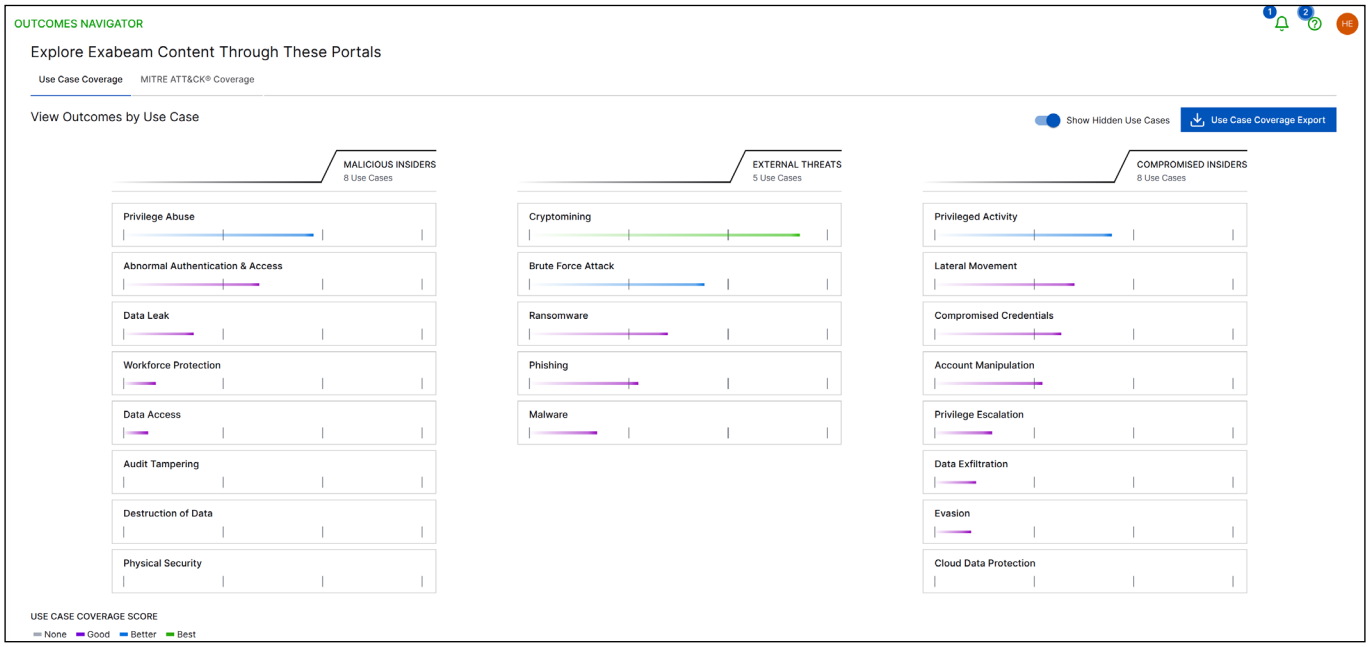

図2.Outcomes Navigator—ユースケースカバレッジタブ

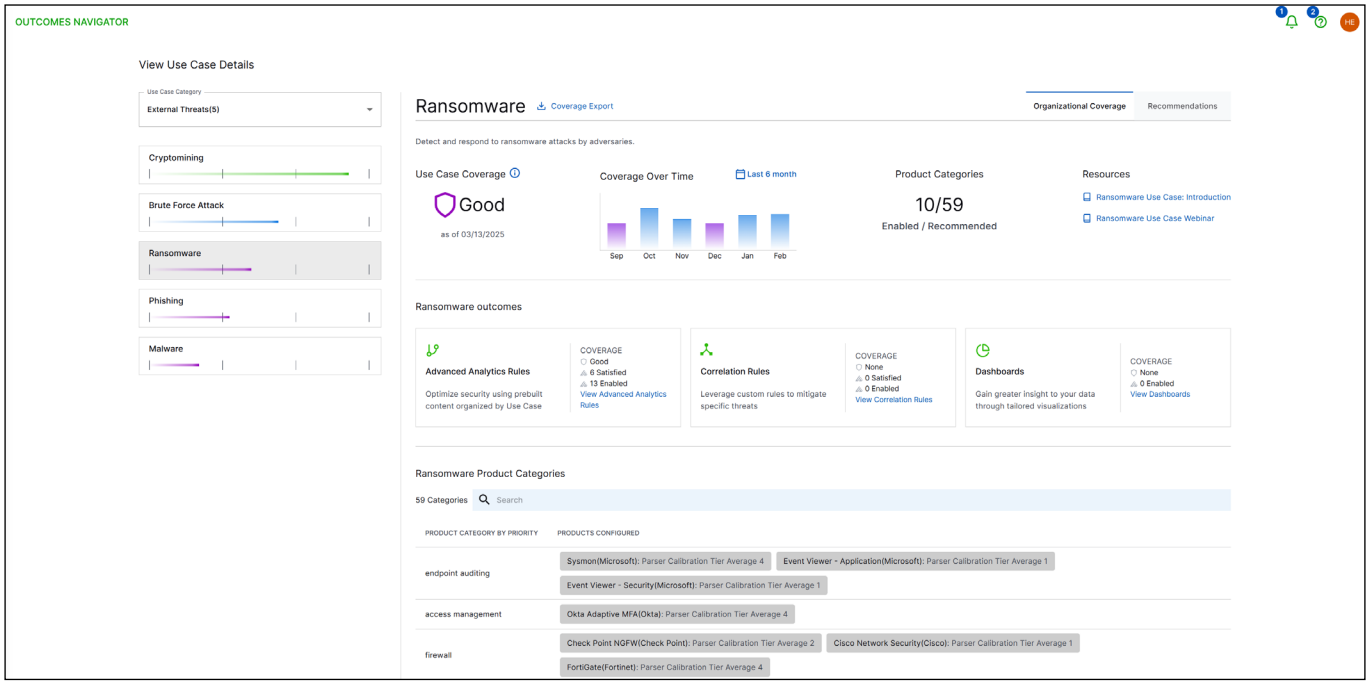

図3.Outcomes Navigator—ユースケース詳細画面

図3.のランサムウェアUse Case Detailsページの上部にはUse Case Coverageサマリーが表示され、次の項目を確認できます。

- 現在のカバレッジ評価（None／Good／Better／Bestの4段階）
- カバレッジのタイムライン
- 当該ユースケースを満たす製品カテゴリとイベント種別
- 本ユースケースのカバレッジを向上させるための推奨ワークフロー
- MITRE ATT&CK サマリー：本ユースケースに関連する最重要TTP（Tactics, Techniques, and Procedures）を一覧表示します。すべてのTTPを確認したい場合はView Allをクリックします。

ランサムウェアの場合、主なTTPはDefense Evasion、Impact、Initial Access、Persistence、Privilege Escalationです。ページ最下部にはProduct Categoriesの詳細パネルがあり、本ユースケース向けに設定済みの製品がカテゴリ別・優先度順に一覧表示されます。ユースケースを効果的にカバーするには、各製品カテゴリに少なくとも1つの製品を構成しておくことが推奨されます。

中央セクションには、このユースケースに対する検知カバレッジが表示されており、UEBA（異常検知）、相関分析ルールのカバレッジサマリー、そしてダッシュボードが確認できます。これらはのちに検知機能を構築する際に活用されます。

これらは後述の検知機能構築時に活用します。ユースケースのカバレッジを確認したら、Recommendations タブ（図 4）をクリックして改善提案を確認します。提案は次の2カテゴリに分類されます。

1. 新しい製品の設定
2. ログパーシングの見直しと改善

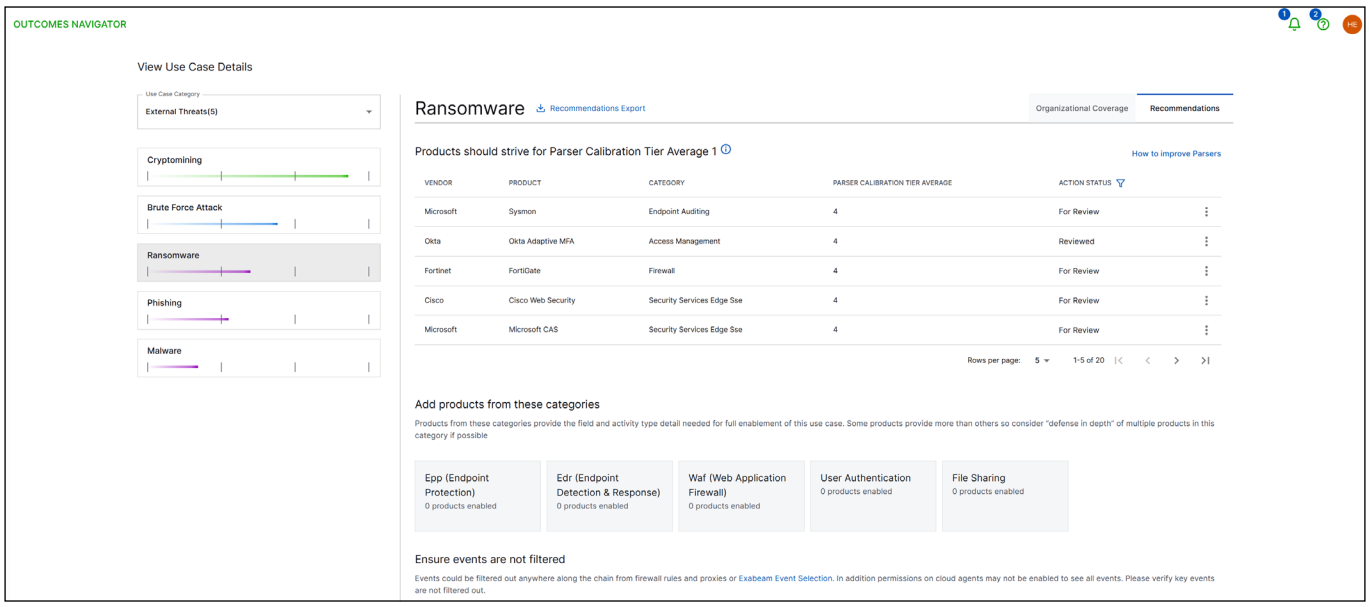

図4.Outcomes Navigator推奨事項

カバレッジを高めるには、次のステップ2で説明する手順に従い、新しい製品を追加して取り込み・パースの対象とすることができます。

また、既存製品や新規追加製品については、ステップ3で説明する方法によりパーシングを改善し、データのカバレッジと品質を向上させることが可能です。

ログパーシングの状況は Parser Calibration Tier（図 5）で評価されます。Tier 4（未パース）から Tier 1（イベントフィールドの 70 %超が構築済み）まで4 段階あり、すべての製品を必ず Tier 1にする必要はありませんが、一般的にキャリブレーションが良いほどカバレッジは効果的になります。セキュリティアーキテクトは、必要なログ・ソース・ストレージとコスト／予算のバランスを取りつつ、継続的に最適化を図ることが望ましいです。

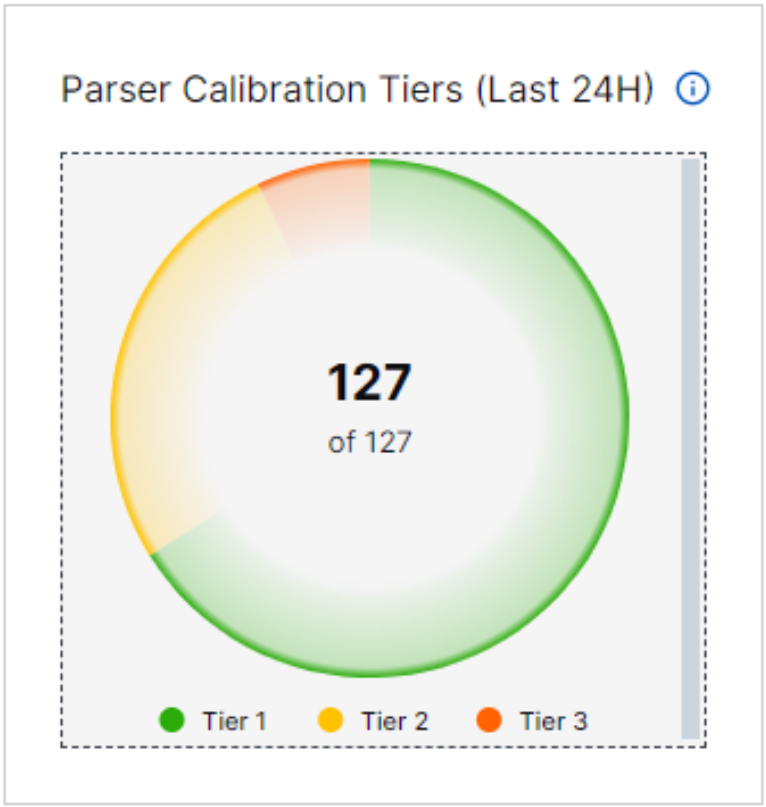

図5.Parser Calibration階層（Tiers）

Step 2：データソースの収集

必要なデータソースを特定したら、Collectorを使ってそのソースをオンボードします。ログをNew-Scale Platformの統合インジェストパイプライン（図 6）へ流し込む入口としては、Site Collector、Cloud Collector、Webhook、Cribl Feed、Context Management などが利用できます。

ログ収集を正しく設定することは、Exabeamの処理・分析ツールに対して完全かつタイムリーで実用的なインテリジェンスを提供するための第一歩となります。図6に示すように、Collectorからのデータストリームは結合され、Log Streamに送られてエンリッチメント、抽出、保存が行われます。

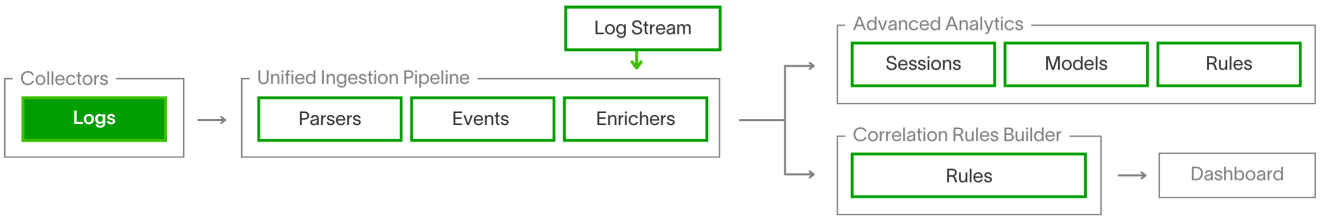

図6.データ取り込みパイプライン

Cloud Collectorを使えば、複数クラウドベンダーのデータを一括で収集できます。本サービスはクラウドネイティブであり、ダウンタイムなしに取り込み量を自動スケールします。

Cloud Collectorのセットアップ手順は接続先のクラウドリソースによって異なりますが、一般的には次の流れになります。

1. 管理者権限を取得
2. アクセスキー／シークレットを作成
3. Cloud Collectorsで対象リソースを選択
4. 画面のインストール手順を実行

たとえば、あらかじめ用意されたCrowdStrike® Falcon Cloud Collectorを選択すると、CrowdStrike Falconのログを取り込む設定が簡単に行えます（図 7）。

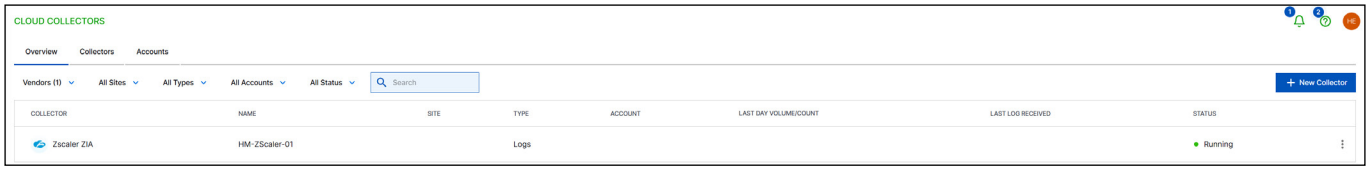

図7.Cloud Collectorの例

Site Collectorは、外部サーバー・システム・データセンターに加え、オンプレミスの Syslog、Windows、Windows Active Directory、Splunk、Oracle、Microsoft SQL、MySQL などのソースからログ／イベントデータを収集します（図 8）。収集したログは、圧縮・暗号化されたデータストリーム経由で New-Scale Platform に送信されます。

Site Collectorを導入する際は、まずオンプレミスに1台以上のSite Collectorインスタンスを作成します。インスタンスを作成したら、その Site Collectorを使ってオンサイトの各リソースからの収集設定を行います。たとえば、Collectors LibraryでSyslog Site Collectorを選択し、対象のSite Collectorインスタンスを指定すれば、Syslogログの収集がすぐに開始できます。

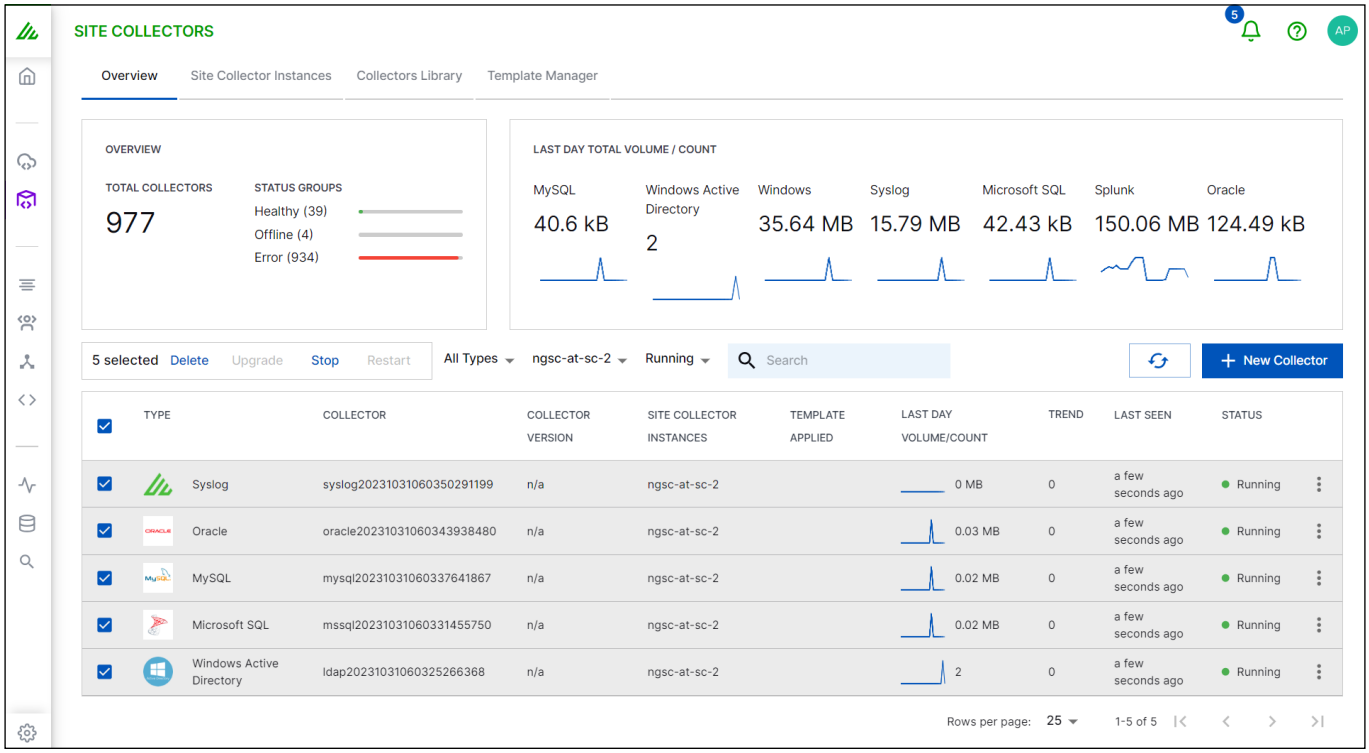

図8.稼働中のSite Collector一覧

ステップ 3：

ストリームから有用なデータを抽出する生ログを収集したら、侵害指標（IoC）の検索やベースライン／異常検知に利用できるようパース処理を行います。ExabeamはCIM 2.0に基づくセキュリティ中心の共通情報モデル（CIM）を策定し、オープンソース仕様としてテクノロジーパートナーへ提供しています。CIM はすべてのイベントを次の多層フォーマットに正規化し、サイバーセキュリティのユースケースを支えます。

Universal > Subject > Activity Type >

たとえば図9は、メール送信イベントが各レイヤーにどのように分類されるかを示しています。

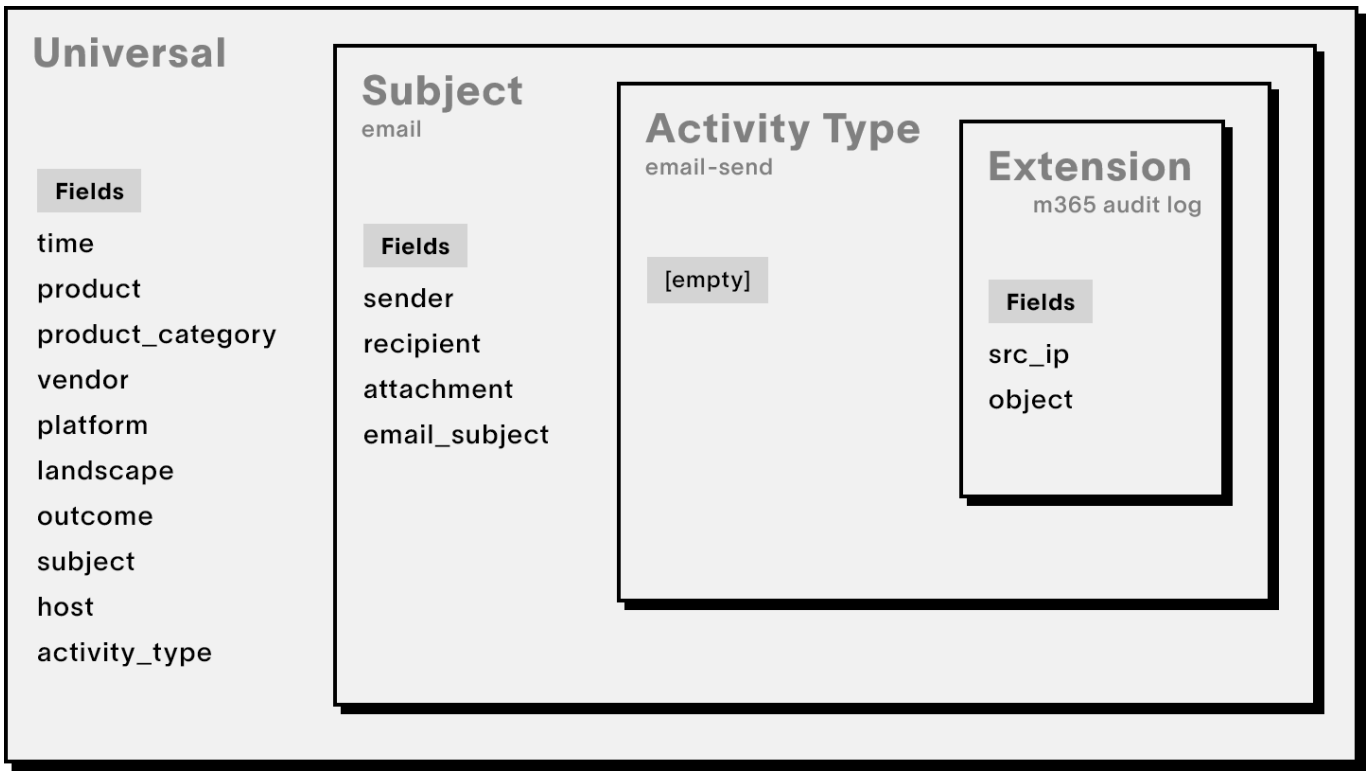

図9.CIMモデルの階層

New-Scale Platformはこのイベントモデルを基盤として、脅威の検索・識別・表示・報告を行います。インジェスト時にパーサーが作動し、多様なログ形式から標準化されたCIM フィールドを生成します。Exabeamでは、主要なセキュリティ製品や情報システムログを網羅する数千種類のプリセットパーサーを提供しています。

データストリームを取り込んだあと、必要に応じてパーサーをカスタマイズできます。カスタマイズはイベントモデルの品質向上のほか、次のような目的でも役立ちます。

- 不要データを除外して ストレージおよび処理コストを削減する
- ベンダー側でログフォーマットが変わった際に調整する
- 自組織で使用する正規表現を管理・文書化する

CIMではフィールド（いずれのレベルでも）をCore／Detection／Informationalの3 種別で分類します。

Coreフィールド：タイムスタンプ、製品名、ベンダー名、結果など、イベント構築に必須

Detectionフィールド：製品カテゴリやプラットフォームなど、検索と脅威検知を高度化

Informational フィールド：ホストや送信先MACアドレスなど、追加情報を提供
これらの層別化により、ログの質と可視性を高めながら効率良く脅威を検出できます。

Log Stream でパーサーを設定する例

Log StreamにはLive Tail機能があり、データの取り込みとパーシングをリアルタイムで監視できます。データソースを開発する際は、Log Streamで変更結果を即座に確認しながら調整できます。

またContext Managementを利用してイベントにコンテキスト（付加情報）を加えることができます。コンテキストを追加すると、Search・Correlation Rules・Detection・Dashboardsの各機能におけるカバレッジが向上します。

Step 4：抽出データをリスクモデルへマッピングする

ここまでで、データ抽出とイベント生成が目的のセキュリティ成果とどのように連動するかを確認しました。Log StreamとContext Managementが自動でイベントを構築し、Outcomes Navigatorがイベント種別を結果にマッピングします。

リスク検知の細部については、New-Scale Platformに組み込まれた脅威インテリジェンスが自動的に処理しているため、まだ意識する必要はありません。

次にOutcomes NavigatorのOrganizational Coverageタブに戻り、2 番目のセクション “Ransomware outcomes”（図10）に注目してください。ここではUEBA Rules Coverage とCorrelation Rules Coverageのスコアが表示され、両者を合わせてUse Case Coverage が算出されます。

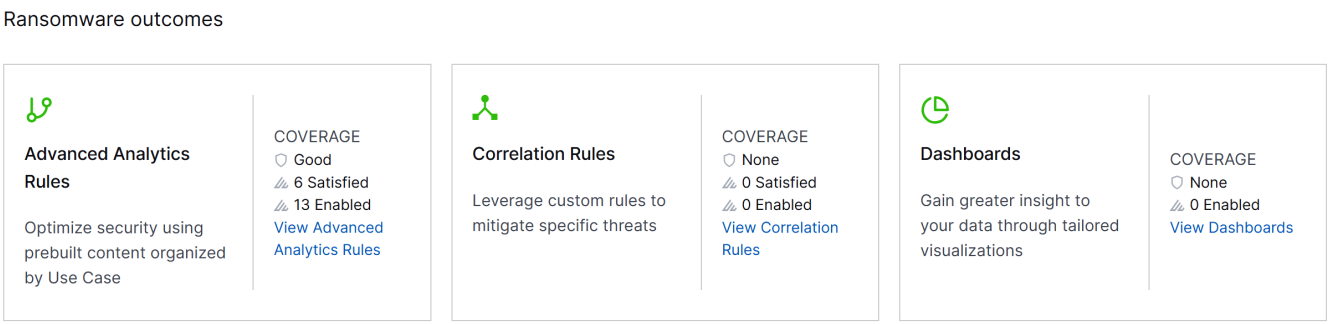

図10.Outcomesサマリー

いよいよ脅威検知の構築に進みます。New-Scale PlatformはCIMを基盤とするUEBAで異常行動を検知するとともに、従来型の相関分析ルールでIoC ベースのアクティビティを検知します。どちらのメカニズムも、ルール定義を組織のセキュリティアーキテクチャに合わせてカスタマイズ可能です。

View Advanced Analytics Rulesをクリックすると、カバレッジスコアを構成する個別ルールの一覧が表示されます。同様にCorrelation Rulesも確認できます。図11では、ランサムウェア攻撃に対して構成されている Correlation Ruleが1 件しかないことがわかります。これでは手薄に見えるため、次のステップとして自社環境に合わせてルールを追加することをおすすめします。

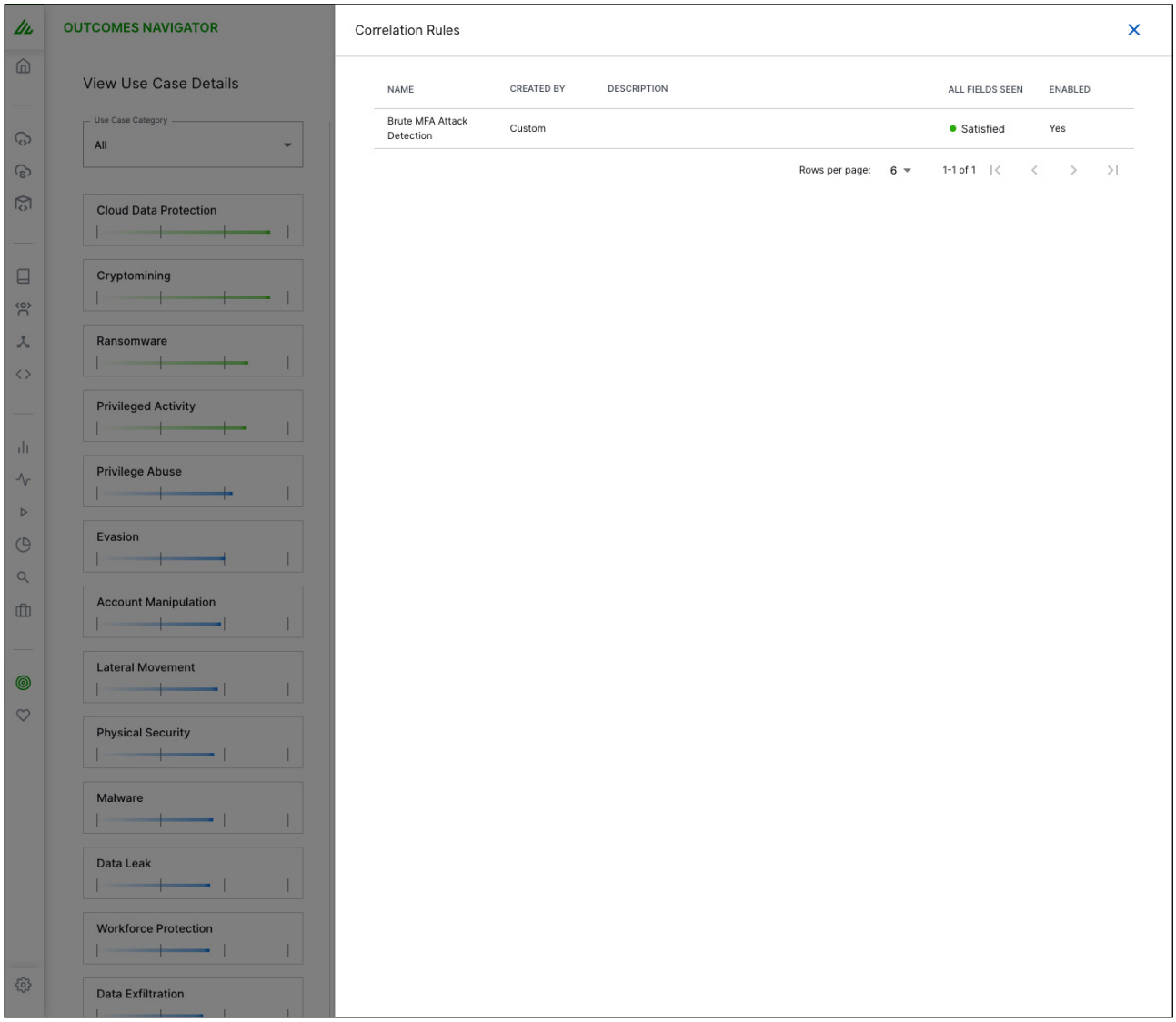

図11.ランサムウェア相関分析ルール一覧

Step 5：リスクモデルに対応する検知ロジックの構築

新しいCorrelation Ruleを作成する一例として、ルールの元となるログを検索する方法があります。図12はSearchページの例です。SQLを知らなくても、フィールドを選択してインターフェース上で検索を構築できます。さらにExabeamでは自然言語検索の機能があり、平易な質問文を高度なクエリ言語へ自動変換できるため、新任のアナリストでも複雑なクエリの作成方法を学びやすくなっています。

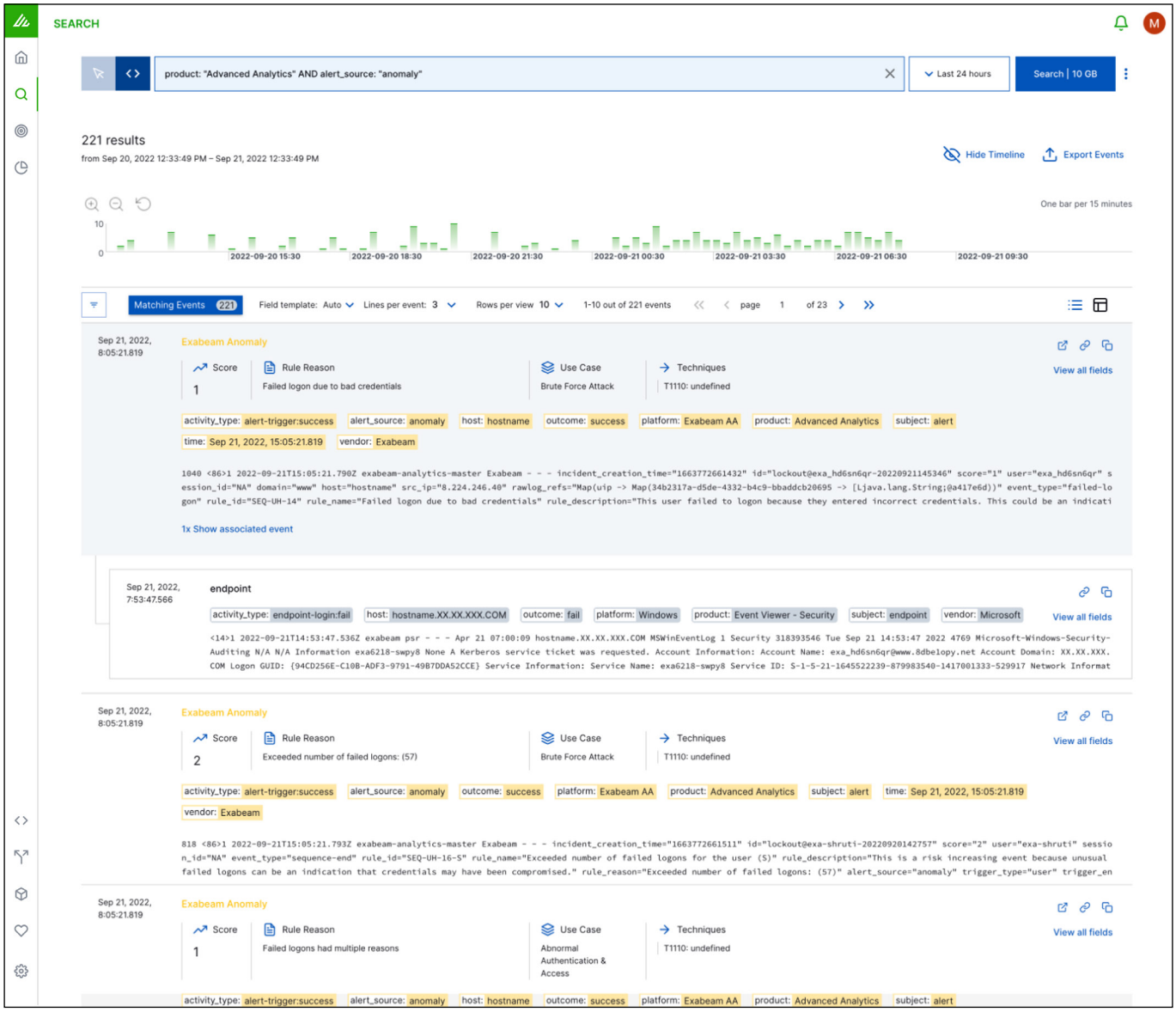

図12.Searchページ

ルールの条件を組み立て終えたらCreate New Ruleをクリックします。Create New Rule ページ（図 13）では、アラート発報・メール通知・新規ケース作成などの対応手段を選択できます。あわせてルール名を設定し、MITRE ATT&CKフレームワークにマッピングして分類すれば、カバレッジ指標をさらに強化できます。

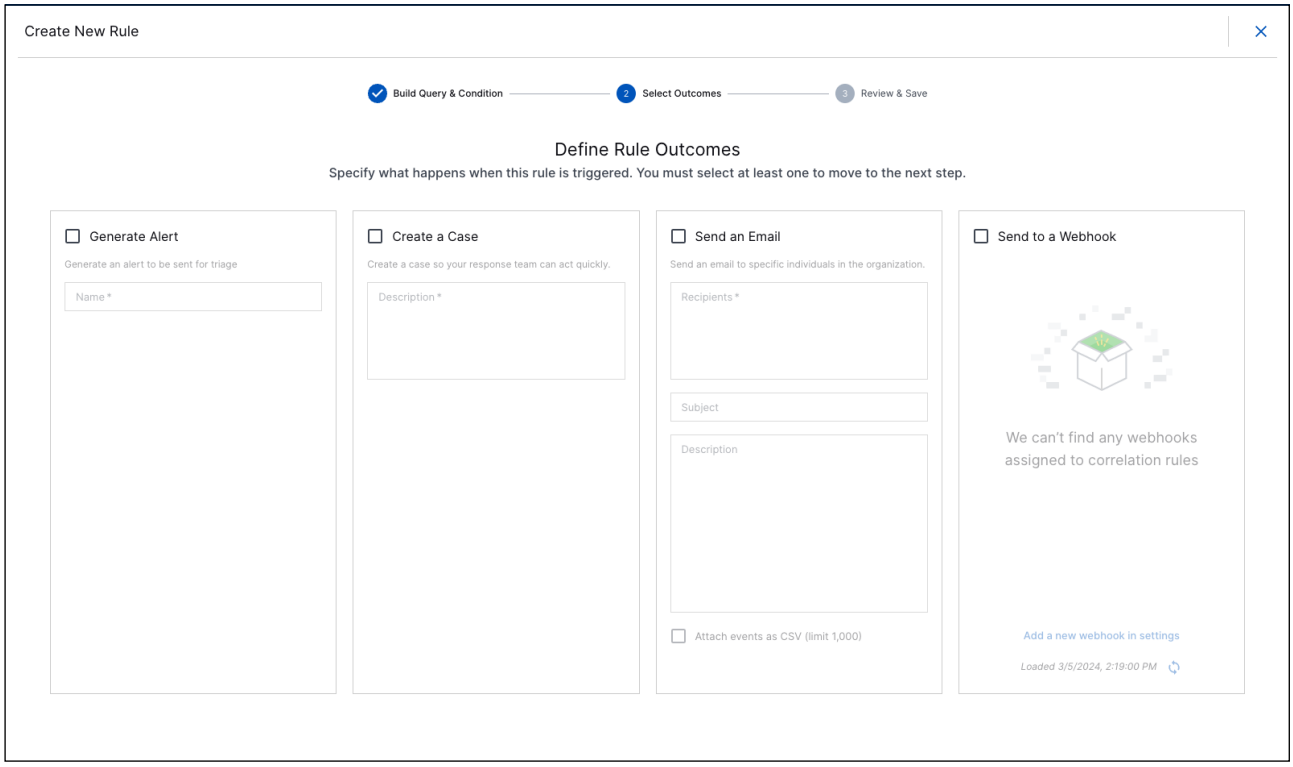

図13.ルール作成画面での設定

UEBAルールも同様の手順で作成できますが、アセットやユーザーの履歴イベントを学習した 行動モデルとの比較が加わる点が特徴です。たとえば「ログオン失敗が異常かどうか」を検知するルールであれば、特定アセットが1日に経験する平均ログオン失敗数をモデル化し、それを大きく上回るイベントが発生したときにトリガーを発動させる、といった形です。

Step 6：検知と調査の自動化

Threat CenterはNew-Scale Platformを基盤とする統合ワークベンチであり、高度なAI 支援と自動化によってTDIR（脅威検知・調査・対応）機能を強化し、脅威を一貫したビューで提示します。Threat Center内のAutomation Management機能を活用すると、アナリストは貴重な時間を取り戻し、より的確な判断を下せます。

迅速なTDIRを実現するには、アナリストが適切な情報に即座にアクセスできることが不可欠です。元SOC実務者がアナリスト向けに設計したThreat Centerでは、コンテキストに応じたリスクスコアリングによりアラートとケースの優先順位を自動的に決定します。リスクスコア、発生からの経過時間、観測されたMITRE ATT&CK TTP、トリガーされたルール、そのほかの証拠など、関連情報を一覧表示します。またThreat Centerは、相関分析ルールと異常検知が自動的にケースへ集約され、あらかじめ用意された脅威タイムラインとともに確認できます。

Automation Managementは、アラートのトリアージ、ケースのエスカレーション、コンテキスト情報の収集、脅威の修復など、SOCワークフローに欠かせない自動化ルールをアナリストやエンジニアが作成できるようにします。反復的な作業を排除し、対応作業を効率化することで、脅威の検知・調査・対応に費やす時間を短縮できます。たとえばITSMシステムでチケットを発行する場合でも、Microsoft TeamsやSlackで通知を送るだけの場合でも、適切なレスポンスとコンテンツを自動化しておくことで、迅速で再現性の高い調査フローを実現できます。

Step 7：結果の保存

イベントとコンプライアンスダッシュボードを利用すると、New-Scale Platform全体のデータを可視化できます。あらかじめ用意された多様なダッシュボードは、満たすべきコンプライアンス要件ごとに分類でき、代表的なユースケース向けにも用意されているため、すぐに活用を開始できます。

これらのダッシュボードは複製してカスタマイズすることも、一から独自に作成することも可能です。

代表的なコンプライアンスダッシュボード例

- アクセス許可／取り消しアクティビティ ダッシュボード
- アカウント ログアウト サマリー ダッシュボード
- アカウント 管理 アクティビティ ダッシュボード
- アプリケーションセキュリティイベント概要ダッシュボード
- ホスト上の認証済みユーザーアカウント ダッシュボード
- AWS CloudTrail 概要ダッシュボード
- データ損失防止（DLP）アクティビティダッシュボード — ホストベース
- データ損失防止（DLP）アクティビティダッシュボード — ユーザーベース
- データ損失防止（DLP）アクティビティ概要ダッシュボード
- 既定アカウントアクセス ダッシュボード
- 既定資格情報の使用・変更アクティビティ ダッシュボード
- 拒否された Web アクセスアクティビティ ダッシュボード
- 無効化されたユーザーアカウント概要 ダッシュボード
- 攻撃元・攻撃先別検出攻撃ダッシュボード
- エンドポイント検知・対応（EDR）ダッシュボード
- 失敗した監査ログ概要ダッシュボード
- ユーザー別ホストログイン失敗回数ダッシュボード
- VPN ログイン失敗 & リモートセッションタイムアウト ダッシュボード
- ファイアウォールアクティビティ ダッシュボード
- ファイアウォール／ルーターインタフェース ダッシュボード
- IoC（侵害指標）統計ダッシュボード
- 安全でない認証試行ダッシュボード
- Microsoft Windows概要ダッシュボード
- ネットワークトラフィック量別アプリケーション ダッシュボード
- ポート使用状況トレンド ダッシュボード
- 特権アクセス ダッシュボード
- 特権アクセス ダッシュボード — ユーザーベース
- ネットワークトラフィック別プロトコル ダッシュボード
- リモートセッション概要 ダッシュボード
- セキュリティアラート概要ダッシュボード — 影響を受けたホスト
- セキュリティアラート概要ダッシュボード — 発生源ホスト
- セキュリティアラート概要ダッシュボード — ユーザー
- データベースログイン成功アクティビティダッシュボード
- 上位攻撃者ダッシュボード
- ユーザーアカウント作成概要ダッシュボード
- ユーザーアカウントロックアウトアクティビティ ダッシュボード
- ベンダー認証アクティビティダッシュボード
- ホスト別Windows監査失敗概要ダッシュボード
- ユーザー別Windows 監査失敗概要ダッシュボード
- Windowsユーザー権限昇格ダッシュボード
- Zscaler HTTPダッシュボード

結論

サイバーセキュリティ脅威の規模と複雑性は増す一方です。New-Scale Security Operations Platformは、データ取り込み・分析・対応の各段階で発生する単調で時間がかかり、ミスの起こりやすいアナリスト作業を取り除く統合ソリューションを提供します。運用のあらゆるフェーズで効率を最大化する複数のモジュールを組み込み、「がむしゃらではなく、賢く戦う」対策を実現します。

- Collectors：多種多様なソースから大量データをスケールさせて取り込みます
- Log Stream：共通情報モデル（CIM）でデータをパースし、イベント同士を結び付けつつエンリッチメントを行います。
- Outcomes Navigator：これらのイベントを脅威にマッピングし、カバレッジを評価します。
- カスタマイズ可能な相関分析ルールとAI ベースのUEBA：既知の攻撃ベクトルと異常行動の両方から脅威を検知します。
- Automation Management：日常的な検知・アラートを自動化し、サードパーティ製品とも連携します。

本ホワイトペーパーでは、AI ドリブンのNew-Scale Platform（製品名 Exabeam Fusion）を活用し、組織の要件に合わせてセキュリティアーキテクチャを評価し、大規模にログやデータを取り込んでCIMを基盤とする豊富なイベントモデルを構築する方法をご紹介しました。

さらに、ログのエンリッチメント、相関分析ルールとUEBAモデルによるカバレッジ評価・強化、インシデント対応を自動化する手順についても解説しました。New-Scale Platformはアナリストの業務を効率化するだけでなく、組織が直面する脅威の爆発的な増加に対して、セキュリティ運用チームがスケールできる環境を提供することで、セキュリティオペレーションという課題そのものを解決可能なものへと変えてくれます。

About Exabeam

Exabeamは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、世界有数の企業のセキュリティ運用を支えています。グローバルなサイバーセキュリティ革新企業として、Exabeamは実績豊富で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、脅威の検出・調査・対応（TDIR）をより高速かつ正確に実現します。

Learn more at www.exabeam.com →