

Exabeam Nova

より迅速でスマートなセキュリティ運用のための エージェントAIアシスタント

はじめに

今日のセキュリティ・オペレーション・センター (SOC) チームは、高度なサイバー脅威、長期化する調査、そして深刻な人員不足という最悪の状況に直面しています。Exabeam Novaは、これらの課題に取り組みます。Exabeam New Scale Security Operation Platform に組み込まれている Exabeam Novaは、プロアクティブなAIアシスタントとして機能します。

レスポンスタイムを短縮し、リアルタイムの洞察を提供します。余分なツールやコストは必要なく、少ないリソースでより多くのことを行うことができます。

なぜエージェントAIなのか？

従来のAIアシスタントはプロンプトを待っていました。エージェントAIは自律的に行動します。主導権を握り、データを分析し、人間の指示なしにSOCチームに助言を与えます。

エージェントAIがセキュリティ上の重要な問題に対処：

- 調査に時間がかかる：アナリストが手作業でデータの関連付けを行い、タイムラインを作成する時間が失われる。多くの組織では、1時間以内にインシデントに対応するのにさえ苦労している。
- 激化するAIによるサイバー脅威：AIを活用した攻撃は、従来の検知手法では対処できないほど急速に拡大している。
- データ収集のボトルネック：複数のツールから手作業でエビデンスを引き出すのは時間がかかり、ミスが発生しやすい。
- セキュリティ人材の不足：サイバーセキュリティの専門家は世界全体で 480 万人不足している (ISC2 2024 Workforce Study)。

Exabeam Nova: SOCチームの最新メンバー

Exabeam Novaは、従来のAIツールの域を超えています。自動化とインテリジェントな洞察で人間のアナリストを補強し、戦力として機能します。

独立したUIと追加コストを伴うスタンドアロン・アシスタントとは異なり、Exabeam Novaは New-Scaleプラットフォーム全体に組み込まれています。

余分な投資をすることなく、検知から対応までシームレスな体験を提供します。

脅威の検知と対応を迅速化：Exabeam Novaは証拠収集と分析を自動化し、平均検知時間 (MTTD) と平均対応時間 (MTTR) を短縮します。

Threat Summary	Analyst Assistant
<p>Case Summary:</p> <p>This case involves Jane Doe accessing multiple malicious domains over approximately 24 hours. Additionally, Jane Doe initiated first-time HTTP connections to Kazakhstan, Azerbaijan, and Tunisia, which is unusual for the organization. The combination of accessing malicious domains and unusual network connections raises concerns about potential malware infection and data exfiltration.</p>	
<p>Case Analysis:</p> <p>Threat Classification: Compromised Insider</p> <p>Reasoning: Jane Doe's actions, specifically accessing multiple known malicious domains, strongly suggest a potential compromise of this account or device. While there's no direct evidence of data exfiltration, the presence of malware (implied through malicious domain access) combined with unusual international connections significantly elevates the risk of data compromise.</p> <p>Identified Vectors and Behavioral Indicators:</p> <ul style="list-style-type: none"> • Unusual Network Connections: First-time HTTP connections to Kazakhstan (kz), Azerbaijan (az), and Tunisia (tn) originating from Jane Doe's user account. • Suspicious Resource Utilization: Not observed in the provided data. <p>Escalation Potential:</p> <p>Jane Doe's activity aligns with the "Compromised Insider" framework, particularly:</p> <ul style="list-style-type: none"> • Anomalous Network/Device Usage: Accessing known malicious domains and connecting to unusual geographic locations. • Abnormal Data Access and Transfer Patterns: Potential, but not confirmed with available data. The presence of malware and unusual connections creates a high likelihood of data access for exfiltration. <p>Without mitigation, this case could escalate to:</p> <ul style="list-style-type: none"> • Data Exfiltration: Malware could enable unauthorized data transfer to external servers in the identified countries. • Lateral Movement: The malware might attempt to spread to other systems within the organization. • Privilege Escalation: The malware could seek higher system privileges to access more sensitive data or systems. <p>Common Context Factors:</p> <ul style="list-style-type: none"> • The sudden access to multiple malicious domains deviates significantly from typical user behavior. • First-time connections to unusual geographic locations are highly uncommon and suspicious. <p>Threat Vector: Malware, potentially delivered via Phishing</p> <p>Threat Vectors and Contributing Behaviors:</p> <ul style="list-style-type: none"> • Malware: Accessing multiple known malicious domains suggests possible malware infection. This could have resulted from clicking malicious links or opening infected attachments, pointing towards a potential phishing attempt. • Phishing (Potential): While not explicitly observed in the data, the malware infection vector hints at a possible phishing campaign. <p>Most Interesting or Relevant Detections:</p> <ul style="list-style-type: none"> • Detection 1: "First HTTP communication to malicious web domain incloseinterest.com for Jane Doe" • Detection 2: "First HTTP communication to malicious web domain p.plowh.com for Jane Doe" • Detection 3: "First HTTP communication to malicious web domain p24000098.effectiverateqcm.com for Jane Doe" 	

図1. Exabeam Nova ケース分析

SOCチームの強化: Exabeam Novaは、ルーチンワークを軽減し、アナリストが優先度の高い作業に集中できるようにします。検出、分析、分類、優先順位付け、およびレポート作成をサポートします。

プロアクティブ・アドバイザー: Exabeam Novaは、ユースケースのカバレッジを強化し、データフィードを最適化し、実行可能な改善策を含む脅威サマリーを生成するための推奨事項をリアルタイムで提供します。

AIによる攻撃を防御: Exabeam Novaは、行動分析と機械学習により、異常や脅威が拡大する前に特定します。

アナリストの疲弊を軽減: Exabeam Novaは、データの解析やケースの要約など、繰り返しの多い作業を処理することで、アナリストをより価値の高い作業に集中させ、士気と定着率を向上させます。

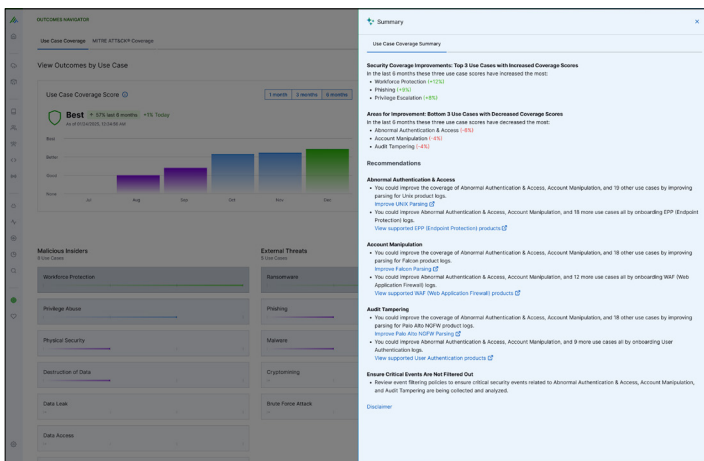


図 2. Exabeam Novaは、Outcomes Navigatorと統合されユースケースカバレッジの向上に貢献。

機密データを保護し、コンプライアンスを維持: Exabeam Novaは、転送中のデータを暗号化し、調査コンテンツをクラウドにキャッシュしません。これにより、規制やコンプライアンスを維持し、厳格なデータプライバシー基準を遵守することができます。

Exabeam Novaは、New-Scale プラットフォームの一部です。追加コストはありません。ワークフローがバラバラになることもありません。AIを活用した合理的なセキュリティ・オペレーションを実現します。

結論

Exabeam Novaは、SOCチームが脅威を先取りして検知し、対応時間を短縮し、よりスマートに作業できるよう支援します。自動化、AI主導の洞察、シームレスなプラットフォーム統合を組み合わせることで、アナリストの負担を軽減し、脅威の網羅性を高め、成果を向上させます。

Exabeam Novaがあれば、SOCはより効率的に、よりプロアクティブになり、次の攻撃を未然に防ぐことができます。

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。



詳細はこちら

www.exabeam.com →

ExabeamおよびLogRhythmの名称およびロゴ、関連する製品名、サービス名、機能名、関連するスローガンは、米国およびその他のExabeam (またはその関連会社) のサービスマーク、商標、登録商標です。その他のブランド名、製品名、商標は、それぞれの所有者に帰属します。

© 2025 Exabeam, LLC. 無断複写・転載を禁じます。