opentext™

ガイド

ユーザー行動分析による高度な内部脅威検知

行動分析を使用して脅威をよりスマートかつ迅速に検知するためのガイド

目次

はじめに

内部ユーザーによる脅威は、現代の組織が直面している最も複雑な課題の 1 つです。外部からの攻撃が世間を騒がすことはよくありますが、内部ユーザーによる脅威は、より潜在的に進行して対処が難しいリスクをもたらします。これらの脅威は、組織内部で、悪意のある従業員、過失行為、または侵害されたアカウントから発生します。内部ユーザーによるインシデントは、長期 (ほぼ 3 か月) にわたって検知されないことが多く、対処に要する年間平均コストは 1,680 万ドルに上ります。これは対処すべき侵害の中で、最もコストがかさむ侵害の一種です [1]。

従来の検知ツールは、静的なルールや既知の攻撃パターンに大きく依存しており、予測可能な外部脅威を捕捉するように設計されています。しかし、内部ユーザーによる脅威は別物です。内部ユーザーによる脅威は、予測可能な経路をたどることはなく、そのアクティビティは多くの場合、想定されるユーザーの行動に溶け込んでいます。その結果、セキュリティチームは、大量の誤検知に対処しなければならず、無害な異常の調査で時間を無駄にする一方、本物の脅威は気付かれずに見過ごされます。

ここで、行動分析が状況を一変させます。行動分析は、事前定義されたルールのみに依存するのではなく、組織全体で「通常の」行動がどのようなものかについての動的な理解を確立させます。行動分析は、継続的に学習して適応していくことで、機密ファイルへの異常なアクセスや、重要なシステムへの不正な変更、疑わしいアクティビティパターンなど、内部ユーザーによる脅威を示唆している可能性のある逸脱を特定します。この高度なアプローチは、セキュリティチームが迅速かつ効果的に行動するために必要な明確な情報とコンテキストを提供します。

このガイドでは、内部ユーザーによる脅威の基本をわかりやすく説明し、行動分析を活用して比類ない可視性と制御を実現する方法を示します。既存のセキュリティ運用の強化を目指している場合も、内部脅威プログラムの構築の開始を検討している場合も、このガイドでは、組織を内部から保護するための知識と戦略を得ることができます。

1 Ponemon Institute、**2023 Cost of Insider Risks: Global Report**

1 内部ユーザーによる脅威を理解する

内部ユーザーによる脅威とは、従業員、契約業者、パートナー、またはシステム、データ、施設にアクセスできるあらゆるユーザーが組織内で発生させるセキュリティリスクです。内部ユーザーは、外部の攻撃者と違って、すでに一定の信頼とアクセス権を得ているため、内部ユーザーのアクションを検知して軽減するのはより難しくなります。これらの脅威は多くの場合、知らない間に進行し、手遅れになるそのときまで、日々の業務にシームレスに紛れ込んでいます。

内部ユーザーによる脅威は一般に、次の３種類に大別できます。

1. 悪意のある内部ユーザーによる脅威

これらの脅威には、組織に害を及ぼすために意図的にアクセス権を悪用する個人が含まれます。彼らの動機はさまざまで、金銭的な利益、復讐、さらには外部の脅威アクターとの共謀まで、多岐にわたります。

例：不満を抱いている従業員が、ダークウェブでの販売や、会社の評判を傷つけることを目的として、機密の顧客データを故意に流出させる。

2. 内部ユーザーの過失による脅威

過失による脅威は、悪意のある内部ユーザーよりも一般的であり、内部ユーザーが不注意またはリスクの高い行動によって、意図せずセキュリティを侵害した場合に発生します。これらのインシデントに悪意はありませんが、悪意のあるインシデントと同様に、害を及ぼす可能性があります。

例：従業員が脆弱なパスワードを使用する。フィッシングリンクをクリックする。保護されていない個人用デバイスを介して機密ファイルを共有する。

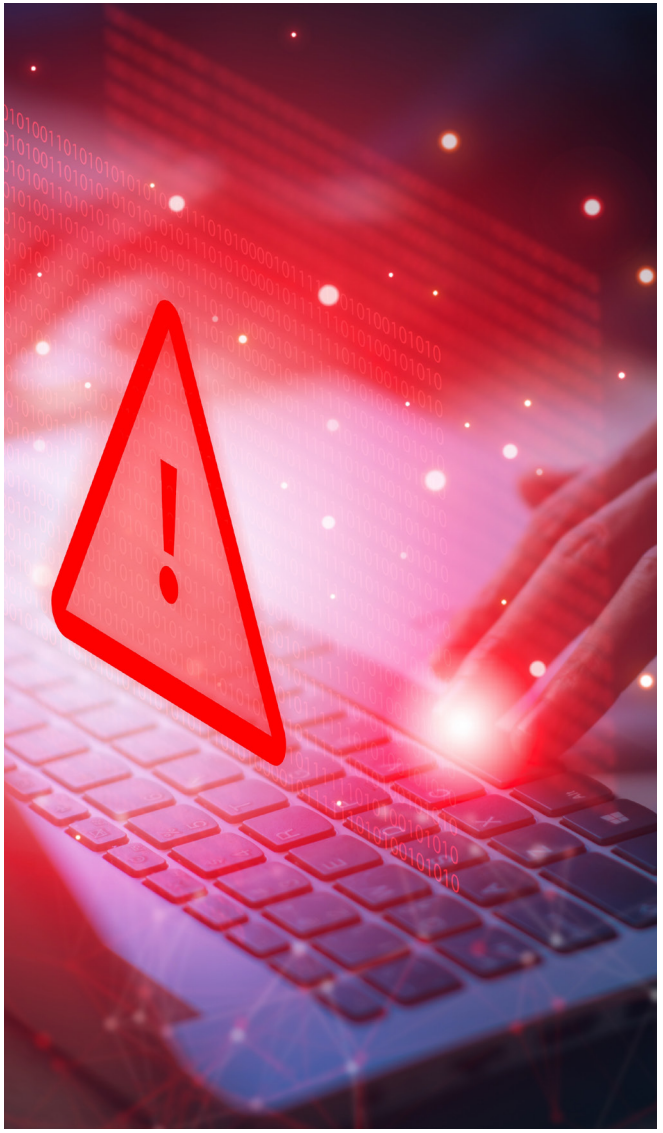
Gartner の最近の調査では、組織が過失によって直面するリスクが強調されています。回答者の 93% が、サイバーセキュリティリスクを高める行為と知っていながら実行していることを認めており、多くの場合、セキュリティよりも利便性を優先しています。さらに 69% の従業員が、企業のサイバーセキュリティガイダンスを意図的にバイパスしたことがあると認めています [2]。

3. 侵害された内部ユーザーによる脅威

侵害された内部ユーザーとは、アカウントやシステムが外部の攻撃者に乗っ取られた個人のことです。これらの脅威は、攻撃者に正当なアクセス権を与えるとともに、そのアクティビティが隠ぺいされるため、特に危険です。

例：フィッシング攻撃が成功して従業員の資格情報が侵害され、攻撃者が特権を昇格させてネットワークでラテラルムーブメントを行えるようになる。

これらの脅威は外部で発生するものの、いったん内部に侵入すると、脅威アクターのアクションは正当に見えるため、他の従業員のトラフィックと区別がつかない可能性があります。これらは社外で発生するにもかかわらず、内部ユーザーによる脅威の一種となっています。



2 Gartner、**Leadership Vision for 2024**

2 従来の手法では不十分な理由

従来のサイバーセキュリティ手法は、多くの外部脅威については効果的ですが、内部ユーザーによる脅威によって生じる固有の課題に対処しようとすると苦労します。静的ルール、シグネチャベースの検知、および手動調査には固有の限界があり、内部ユーザーのアクティビティの微妙に異なる行動を検知するのは困難です。特に、意図に悪意があることが明らかでない場合や、攻撃者がローアンドスロー (少しずつ、ゆっくりした) アプローチを取る場合は、なおさらです。

静的ルールの限界

静的ルールベースのシステムは、異常なログイン試行や制限付きファイルへのアクセスなどの脅威を識別するために、事前定義された基準に依存しています。これらのルールでは、わかりやすい異常は検知できますが、内部ユーザーによる脅威に関連するコンテキスト駆動の微妙な行動は見落とされることがよくあります。

例：従業員が遅くまで仕事をして機密ファイルにアクセスした場合、そのアクションは正当であっても、アラートがトリガーされる可能性があります。逆に、想定の範囲内で慎重な操作を行っている悪意ある内部ユーザーは、検知されない可能性があります。

このように柔軟性が欠けているため、膨大な数の誤検知が発生し、セキュリティオペレーションセンター (SOC) チームにノイズがかかり、本物の脅威に集中する能力が低下します。

シグネチャベースの検知に関する課題

シグネチャベースのツールは、マルウェアシグネチャや既知の攻撃者に関連付けられた IP アドレスなど、悪意のあるアクティビティの既知のパターンを認識するように設計されています。シグネチャベースのツールは、外部からの攻撃に対しては効果的ですが、マルウェアや既知の攻撃ベクトルと関係しない内部ユーザーによる脅威に対しては、実質的に効果がありません。

例：機密データを自分の個人アカウントに電子メールで送信する従業員や、ネットワーク内でラテラルムーブメントを行う、侵害された内部ユーザーは、既存のシグネチャとは一致しないのが一般的です。

手動調査の負担

多くの組織は、自動化ツールでは処理されない箇所を補うため、手動調査に頼っています。このアプローチは多大な時間と労力を要し、アナリストは疑わしいアクティビティを明らかにするために大量のデータを調べる必要があります。

SOC の疲労：静的ルールとシグネチャベースの検知によって誤検知率が高くなるため、SOC チームに重い負担がかかり、アラート疲れを招きます。時間の経過とともに、このアラート疲れにより、効果的に対応する能力が低下し、本物の脅威を見落とすリスクが増大します。

悪意のない内部ユーザーによる脅威検知の難しさ

従来の手法は、過失または侵害された内部ユーザーの特定に関しては、特に効果がありません。

過失:脆弱なパスワードの使用、フィッシングリンクのクリック、セキュリティで保護されていないチャネルを介した機密ファイルの送信などのアクションは、本質的に悪意のあるものではないため、必ずしもアラートをトリガーするわけではありません。しかし、これらの行動は深刻なセキュリティインシデントにつながる可能性があります。

侵害されたアカウント：正当な従業員資格情報を使用する攻撃者は、従来の検知メカニズムの多くをバイパスできます。攻撃者は既存の特権や行動を利用するため、攻撃者のアクションは正常に見えます。

組織は、絶えず変化する環境に適応し、誤検知を減らし、悪意ある脅威、過失による脅威、侵害による脅威のいずれであるかにかかわらず、内部ユーザーによる脅威を SOC チームが効果的に検知して対応できるようにするソリューションを必要としています。AI 主導のインサイトを組み合わせた行動分析などの高度なツールは、これらのギャップを埋めることができ、組織がノイズを取り除き、本物のリスクに集中するのに効果的です。

セキュリティ侵害の 74% に人為的要素が含まれている (Verizon DBIR)[3] 現在では、時代遅れの手法に頼ることで組織は脆弱な状態になります。内部ユーザーによる脅威には、静的なルールや手動の介入にとどまらず、動的な行動ベースのインサイトに焦点を当てるアプローチが必要です。

3 Verizon、**DBIR Report 2023 - Summary of Findings | Verizon Business**、2023 年

3 行動分析：内部脅威検知の鍵

行動分析は、ユーザー、デバイス、システムの通常の行動を理解し、通常とは有意差のあるものを識別することに重点を置いたセキュリティ手法です。行動分析は、既知のシグネチャ、静的ルール、事前定義されたシナリオに依存する従来のアプローチとは異なり、動的パターンに基づいて機能します。また、継続的に学習し、組織のワークフロー、従業員の役割、テクノロジースタックに伴って進化します。

仕組み

行動分析には、環境内の各エンティティの通常のアクティビティがどのようなものかについての詳細なプロファイル、つまり「ベースライン」の作成が含まれます。ユーザーの場合、ベースラインにキャプチャされる可能性がある要素は次のとおりです。

- 通常のログイン時間帯と場所
- 一般的なファイルアクセスパターン (例：どのドキュメントを読み取り、作成、変更するか)
- 使用する優先デバイスとネットワークセグメント
- 管理アクションの実行頻度 (該当する場合)

行動分析は、長期にわたる大量のイベントデータを集約して分析することにより、エンティティごとに想定されるパターンの統計モデルを構築します。現行のアクティビティがこれらの確立されたパターンから逸脱している場合は常に、システムはそのアクティビティにフラグを付け、精査対象とします。たとえば、普段は午前 8 時から午後 6 時まで本社からログインしている従業員が突然、午前 3 時に離れた場所から接続して、これまで触れたことのない機密のデザインドキュメントにアクセスを試みた場合、それは有意な逸脱です。

適切に設計された行動分析ソリューションは、逸脱や異常を警告するだけにとどまりません。このソリューションは、AI と高度な機械学習を使用して、個人とグループの異常のリスクを把握し、全体像に基づいて関連リスクスコアを適用します。これは、行動の侵害指標 (bIOC) に基づいた高品質な手掛かりを SOC チームに提供するための極めて重要なステップです。

ユーザーの行動のベースラインと逸脱

ベースラインの確立は、行動分析の基本です。これは、アクションをログに記録するだけでなく、アクションの頻度、コンテキスト、関連性を把握するということです。行動分析は、これをすべてのユーザー、システム、デバイスに対して大規模に行うことで、単独では無害に見えるが総合的には疑わしい異常を特定します。このコンテキスト駆動型アプローチは、無害なバリエーション (時折遅くまで働くユーザーなど) と本物のリスク指標 (連続して数日間にわたり、おかしな時間に専有データを突然ダウンロードするユーザーなど) を区別する際に、特に効果的です。

システムは、逸脱が検知されたときに一般的なアラートを送信するだけではありません。何が変わったのか、なぜ異常なのかに関するコンテキストを提供し、アナリストを問題の本質に迅速に導きます。これらのインサイトにより、誤検知に対して無駄に費やす時間が短縮され、セキュリティチームは潜在的なリスクへの理解を深めることができます。

誤検知とは

誤検知は、セキュリティシステムが正当なアクティビティを誤って脅威としてフラグ付けした場合です。これらのエラーのせいで、SOC チームに重い負担がかかり、本物の脅威に集中できなくなります。行動分析は、本当に異常な行動を正確に特定することで誤検知を減らします。

検知漏れとは

検知漏れは、セキュリティシステムが本物の脅威を検知できず、悪意のあるアクティビティが気付かれない状態に陥る場合に発生します。内部ユーザーによる脅威の場合、これは特に危険です。通常とは異なる微妙な行動は、従来の検知をすり抜ける可能性があります。行動分析は、潜在的なリスクを示唆する、微妙に異なるパターンを特定することで、検知漏れを最小限に抑えるのに役立ちます。

行動の侵害指標 (bIOC)

サイバーセキュリティでは長い間、既知のマルウェアシグネチャや疑わしい IP アドレスなど、従来の侵害指標 (IOC) に重点が置かれていました。IOC は、パターンに従う外部攻撃を検知するのに効果的ですが、内部ユーザーによる脅威に対処するのは困難です。なぜなら、内部ユーザーによる脅威は、企業のサーバーへのアクセスやファイルのダウンロードなど、表面的には正当に見えるアクティビティに関係することが多いからです。それらの脅威は、既知の悪意あるコードや容易に識別できる外部シグナルには依存しません。

行動の侵害指標 (bIOC) は、行動自体の性質に焦点を当てることで、このギャップに対処します。bIOC は、特定のマルウェアを探すものではなく、ユーザーやグループの確立された通常に反するアクションを探すものです。たとえば次のように利用できます。

- 通常はコードリポジトリにしかアクセスしないエンジニアが、機密の財務データベースを探索する。
- 人事スタッフが、大量の従業員データを未知のデバイスに突然エクスポートする。
- 管理アカウントが、短い期間内に、地理的に離れた複数の場所からログインする。

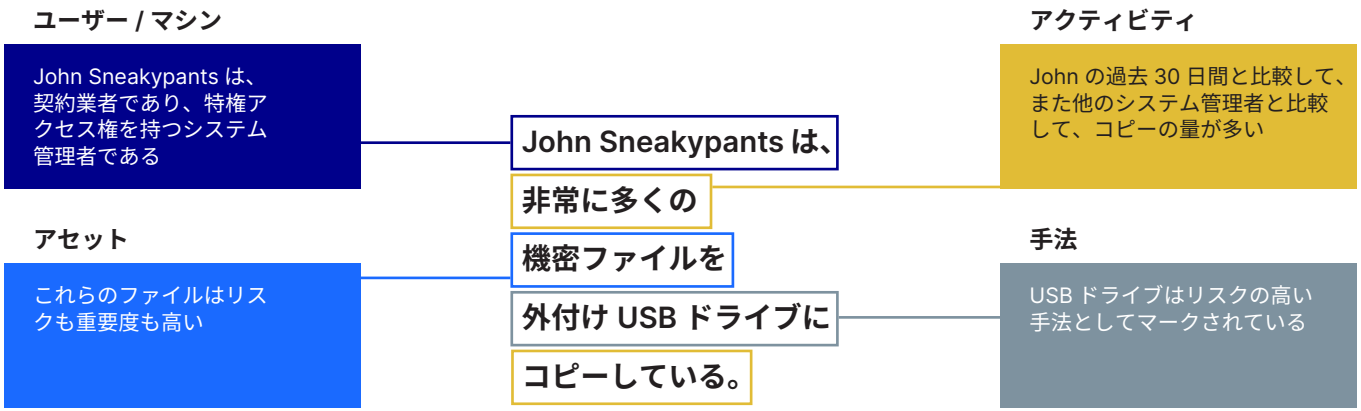
特別に作成されたベースラインとアクティビティを照合することで、これらの異常が特定されるため、bIOC は組織固有のコンテキストに適応します。それらは、「悪質な」行動の静的リストではありません。bIOC は逆に動的です。より多くのデータを処理し、環境内で「通常」がどのようなものかについての認識を改良するにつれて、精度が向上し、インサイトが充実します。

堅牢な行動分析ソリューションは、環境から直接学習し、コンテキストをゼロから構築します。行動分析は、普遍的なデータセットで事前設定できるルールベースのツールとは異なり、他の誰かのベースラインに接続するだけで直ちに結果が得られるものではありません。ユーザーアクティビティを観察し、インサイトを収集して、組織固有の微妙な異常を正確に検知できるように微調整されたシステムへと成熟するには、時間 (多くの場合は数週間) が必要です。

行動分析が検知精度を向上させる理由

行動分析は、既知の脅威の固定セットではなく、ユーザーの行動を中心に据えることで、セキュリティアラートの精度と関連性を飛躍的に向上させます。行動分析は、コンテキスト (時間、場所、通常の職務など) を把握することで誤検知を減らし、仕事パターンの正当な変化に対する不必要なフラグ付けを防ぎます。同時に、クリーンなシグネチャや事前定義されたルールに適合しない脅威を捕捉することで、検知漏れを最小限に抑えます。

行動のリスクに対する原則的アプローチ



行動分析ソリューションから発せられるアラートの例。ルールベースの脅威検知ソリューションでは、事前定義された多数のケースが必要となるのに対し、行動分析ソリューションは、異常に関するコンテキストを把握し、ルールに縛られないアラートを動的に作成する。

行動分析は、表面的な指標を超えて見通すための強力な視点をセキュリティチームに提供します。行動分析は、通常のアクティビティとそうでないアクティビティを把握し、巧妙で高度な脅威が本格的なインシデントへと発展する前に検知できるようにします。内部ユーザーが知らないうちに、または意図的に、重大な被害を引き起こす可能性がある時代において、行動分析は、進化するリスクに先手を打つために必要な適応性、コンテキスト、深いインサイトを提供します。

4 行動分析の主要なユースケース

1. データ流出の検知

データ流出、つまり、機密データが安全な環境から持ち去られることは、セキュリティリーダーや経営陣にとって最大の懸念事項です。行動分析は、ユーザーのアクティビティにおいてデータ窃盗の兆候かもしれない微妙な変化を特定するのに役立ちます。たとえば、通常は少数のファイルにしかアクセスしない従業員が突然、大量の専有ドキュメントのダウンロードを開始した場合、行動分析では異常としてフラグ付けされます。静的ルールは既知の「悪質な」ファイルシグネチャに対してのみトリガーされる可能性がありますが、このアプローチは静的ルールとは異なり、アクティビティのコンテキストとボリュームに焦点を当て、重大な損害が発生する前にセキュリティチームが迅速に介入できるようにします。

2. 資格情報の悪用や不正利用の識別

資格情報の悪用は、内部ユーザーが意図的に特権を不正利用した場合や、外部の攻撃者が正当なアカウントを侵害した場合に発生する可能性があります。表面的には、ユーザーが「通常の」ログインを実行しているため、従来のツールでは、これを検知するのに苦労する場合があります。行動分析は、現在のアクションを確立されたベースラインと比較することで、この問題を解決します。侵害されたアカウントは、予期しない場所から通常とは異なる時間帯にリソースにアクセスしたり、そのユーザーの役割には一般的に関連しない情報を検索したりすることがあります。行動分析は、これらの逸脱に焦点を当てることで、侵害された資格情報をセキュリティチームが早期に特定し、攻撃者の機会を減らすのに役立ちます。

3. 異常なアクセスパターンの監視

信頼できる善意の従業員であっても、異常なアクセスパターンが過失や悪意によるリスクを示唆している場合があります。通常は営業時間内に人事のドキュメントを取得しているが、深夜に、または遠隔地からアクセスしているユーザーについて考えてみましょう。単一のインスタンスに悪意はない可能性がありますが、行動分析によりパターンが検知され、コンテキストが提供されます。このコンテキスト認識により、アナリストは、アクティビティをより詳しく調査する必要があるかを迅速に判断でき、明らかな「警告」の欠如から脅威が見過ごされる事態を防ぐことが可能となります。

4. 特権昇格など、リスクの高い行動への対応

特権昇格、つまりシステム内で不正なアクセスレベルを獲得することは、多くの高度な攻撃における重要なステップです。従来の制御では、特権が変更されたことのみが通知され、なぜ疑わしいのか、また、本当に疑わしいアクティビティなのかどうかについては通知されないことがあります。行動分析では、ユーザーの典型的なアクセスパターンと責任が把握されます。以前はアクセスが限定的だったアカウントが突然、セキュリティ設定の変更や機密性の高い財務データの表示を試みた場合、システムでは、異常な行動として認識されます。

行動分析では、アナリストが手動でイベントを相関付ける必要はなく、重大なインシデントが発生する可能性があるという明確でコンテキストに富むシグナルが提示されます。

すべてを統合

行動分析は、静的なルールや既知のシグネチャだけでなく、ユーザーやエンティティの行動に焦点を当てることで、より高精度で微妙な違いを識別する形態の検知を提供します。データ窃盗の防止、攻撃者による正当なアカウント悪用の阻止、異常なアクセス試行の捕捉など、この適応性に優れたコンテキスト駆動型アプローチは、セキュリティチームが攻撃者の一歩先を行くのに役立ちます。その結果、高度な脅威を早期に捕捉するだけでなく、タイムリーな対応の妨げとなることが多いノイズを軽減する、よりレジリエントなセキュリティ体制が実現します。

5 高度な行動分析を実装する方法

セキュリティオペレーションセンター (SOC) に高度な行動分析を実装することで、内部ユーザーによる脅威をはじめとする高度なリスクへの検知と対応を行うチームの能力を大幅に向上させることができます。成功は、現在のセキュリティエコシステムとワークフローに沿った、適切に構造化されたアプローチから始まります。

統合のステップ

- **現在の環境の評価：**SIEM、EDR プラットフォーム、IAM ソリューションなど、既存のセキュリティツールとデータソースをレビューすることから始めます。カバレッジのギャップを特定し、行動分析により可視性と検知を最大限に向上させることができる領域を特定します。これは、まず識別情報管理に焦点を当てるか、機密データが保存されているアプリケーションサーバーに焦点を絞るか、ということになる場合があります。
- **行動分析ソリューションの選定：**内部ユーザーによる脅威、資格情報の悪用、異常なアクセスパターンの検知に優れたプラットフォームを選定します。Microsoft Defender for Endpoint や Microsoft Entra ID など、利用しているツールとのシームレスな統合がサポートされていることを確認します。厳密なルールのアップデートを必要とすることなく、独自の環境から学習する適応性の高い機能を探します。
- **データフィードとベースラインの確立：**選定したソリューションを、関連データソースに接続します。ソリューションは、時間の経過とともに、各ユーザーとシステムの「通常の」行動、たとえば、通常アクセスするファイル、ログインする時間帯と場所、ネットワーク内での移動方法などを定義するベースラインを確立します。これらの行動に関するインサイトを収集するために、十分な時間を確保することが重要です。ベースラインの品質は、システムが取り込むデータの量と多様性によって決まります。
- **既存のワークフローとの統合：**行動分析の真の力は、それが現在の運用に直接組み込まれたときに発揮されます。アラートとインサイトを SIEM、チケットシステム、インシデント対応ツールに統合して、アナリストが複数のプラットフォームを切り替える必要がないようにします。これにより、疑わしいすべての異常が既存のワークフロー内でコンテキスト化され、インシデントの追跡、責任の割り当て、解決の迅速化が容易に実現されます。
- **微調整とキャリブレーション：**ベースライン期間が終了したら、システムのアラートと推奨事項を確認します。優れたシステムは人間の介入なしに自動的に調整されるべきですが、自動的に調整されない場合は、必要に応じてしきい値を調整し、組織が「リスクの高い」行動と見なすものを改良するようにします。行動分析は継続的に学習して適応していくため、継続的なキャリブレーションが自動的に行われ、時間の経過とともに精度と関連性が向上します。
- **チームのトレーニング：**行動分析が従来のルールベースの検知とどのように異なるかをアナリストが理解できるように、専用のトレーニングセッションを提供します。異常を解釈し、無害な異常と本物の脅威を区別し、プラットフォームのコンテキストに富むインサイトを活用する方法を具体的に示します。SOC は、自信と能力を築くことで、検知から情報に基づいたアクションへと迅速に移行できます。

「[OpenText Core Threat Detection and Response] によって、当社では行動の変化が可能になりました。事業部が IT やサイバー環境に変更を加えるにあたり、私は CISO として、事業部から私に事前連絡させたことはありません」

- CISO、世界的なインターネット小売業者

6 OpenText が提供する支援

内部ユーザーによる脅威、新種の攻撃、高度で継続的な脅威に対する高度な脅威検知を探している場合は、OpenText™ Core Threat Detection and Response が最適です。OpenText Core Threat Detection and Response は、最新の行動駆動型の内部脅威管理および高度な検知アプローチを提供します。

静的なルールや既知のシグネチャに依存するのではなく、ユーザーとエンティティの行動に焦点を当てることで、セキュリティチームは、悪意ある行動、過失による行動、侵害による行動が、害を及ぼすインシデントへと発展する前に、それらの微妙なパターンを自社の環境全体で発見できるようになります。

Threat Detection & Response は、セキュリティオペレーション (SecOps) にとどまらず、DLP、IAM、EDR、NDR などを網羅します。

お客様のセキュリティレジリエンス：OpenText を活用

OpenText Threat Detection and Response を含む Open XDR アーキテクチャ

データ損失の防止 (DLP)

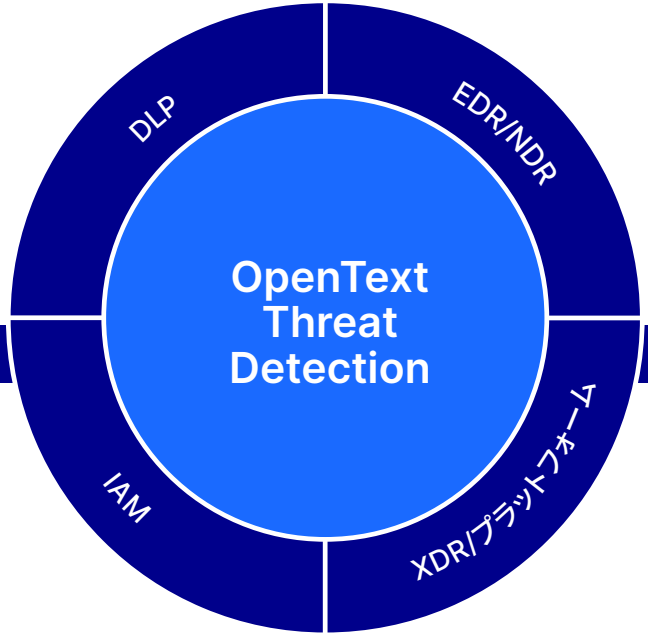
一般的な DLP に含まれるもの：
- アセット検出
- データ分類
- データ暗号化
- ユーザー管理
- ポリシー管理
- パーミッション管理
- コンプライアンスレポート
- 自動ユーザー教育
- 自動応答 / 戦略ガイド

OpenText を活用：
- データパーミッション管理とルールベースのロジックでデータの脅威を発見する
- AI ベースの検知を活用し、データ流出を防ぎ、ML モデルを動的に進化させる
- 高度な脅威をすべてカバーする
- IAM でデータアクセスログを取り込む

Endpoint/Network Detection & Response (EDR/NDR)

一般的な EDR/NDR に含まれるもの：
- エンドポイント / ネットワークレベルのテレメトリ
- 豊富なデータソース
- ルールベースの応答
- オンマシンでの迅速な対応
- 堅牢な応答機能

OpenText を活用：
- 会社で認識されている境界線や防御線の内側におけるデータの脅威のみにとどまらずに焦点を当てる
- 行動分析を活用して、境界線を無視する部外者や内部ユーザーの異常を見つける
- 可視性を向上し、高度な脅威をすべて表示する
- エンドポイント / ネットワークデータを取り込む



アイデンティティ管理とアクセス管理 (IAM)

一般的な IAM に含まれるもの：
- アクセスログデータ
- アイデンティティログデータ
- 認証
- コンプライアンスレポート
- ゼロトラスト
- 役割管理
- グループ管理

OpenText を活用：
- 脅威ハンティングによりアイデンティティアクセスと認証を管理する
- エントリポイント / 脆弱性が存在する可能性のある場所まで遡って内部脅威検知に取り組む
- ローアンドスローおよび APT 検知機能を追加
- 取り込み機能を備えた IAM は、検知を強化するための貴重なデータソースである

XDR/ プラットフォーム

現行の XDR に含まれるもの：
- 一元的に可視化するダッシュボードのための EDR/NDR ソリューションの進化
- ほとんどのデータソースとの統合
- 堅牢な応答機能
- さまざまな脅威タイプの検知

OpenText を活用：
- 行動分析と DLP タイプの制御と応答を組み合わせて、あらゆるタイプの高度な脅威を検知：IAM を含む多くのデータソースを使用してデータを引き出す
- 複雑なセットアップとメンテナンスのメリットが得られる：時間のかかる構成
- 多様な対応オプションを利用可能

コンテンツ管理 | サービス管理 | IT 運用管理 | サプライチェーン管理

適応型の行動駆動型分析

ルールの頻繁な手動更新を必要とする従来のソリューションとは異なり、OpenText Core Threat Detection and Response は、検知ベースラインを自動的に調整し、組織の進化するワークフローから学習します。役割、テクノロジー、ビジネスプロセスの変化に合わせて、このソリューションは、「通常」の定義を継続的に改良し、検知の精度を高め、誤検知を減らします。

既存の投資とのシームレスな統合

OpenText Core Threat Detection and Response は、Microsoft Defender、Entra ID、その他の重要なセキュリティツールに依存しているかどうかにかかわらず、確立されたエコシステムとシームレスに連動します。この相互運用性により、現行の運用を中断したり、テクノロジースタックの見直しを余儀なくされたりすることなく、可視性が強化され、盲点が減少します。

コンテキストに富む、アクション可能なアラート

ソリューションは、疑わしい行動を特定すると、コンテキストに富むインサイトを、明確で理解可能な言葉で提供します。SOC アナリストは、暗号化されたアラートの解読や無害な異常の調査で時間を無駄にせずにすみます。それどころか、検知から意思決定に迅速に移行できるため、応答時間が短縮され、あらゆるレベルの専門知識から内部ユーザー主導の侵害のリスクが軽減されます。

SOC ワークロードとアラート疲れの軽減：

OpenText Core Threat Detection and Response は、ノイズをフィルタリングし、リスクの高いインシデントを優先することで、アナリストは本物の脅威に集中することができます。その結果、効率性が向上し、アナリストの士気と効果が高まり、よりプロアクティブでレジリエントなセキュリティ体制につながります。

スケーラブルで将来にも対応

組織の成長と進化に合わせて、OpenText Core Threat Detection and Response も拡張されます。行動モデルは継続的に適応していき、チームは新たなリスクや進化する内部脅威戦術に先手を打てるようになります。OpenText の専門サービスと継続的なイノベーションのサポートにより、今日の課題と明日の未知の脅威に対処するように設計されたソリューションを利用できます。

OpenText Core Threat Detection and Response が内部脅威戦略を向上させる仕組みをご確認ください。

リソース

詳細情報：OpenText の製品ページにアクセスして、高度な行動分析の詳細をご覧ください。

デモのリクエスト：お客様の組織固有の環境に合わせてカスタマイズされたリアルタイム脅威検知の能力をご体験ください。

OpenText のエキスパートとつながる：お客様の目標と課題に関するご相談は、OpenText のセキュリティスペシャリストによるコンサルティングをご予約ください。

よりプロアクティブでレジリエントなセキュリティ体制に向けて、次のステップに進みましょう。内部脅威防御はここから始まります。

opentext™