OpenText Core Threat Detection and Response

組織に影響が及ぶ前に、内部ユーザーによるリスク、新たな攻撃、APT (Advanced Persistent Threats) を検知

利点

- セキュリティの死角を除去
- 脅威ハンティングの効率と効果を改善
- 内部ユーザーによる脅威やその他の高度な攻撃を早期に検知
- 誤検出を減らしてアラート対応の労力を軽減

サイバーセキュリティに対して多額の投資が行われているにもかかわらず、内部ユーザーによる脅威は、コストが高くつく継続的なリスクをもたらし続けています。外部からの攻撃が注目と予算の大半を占めることが多い一方で、悪意のある内部ユーザーの行為や盗まれた識別情報の悪用はしばしば検知されず、結果として年間平均 1,620 万ドルの損失が発生しています[1]。内部ユーザーによる脅威に効果的に対処するには、有害な行為や識別情報の悪用を検知して低減することに特化したセキュリティソリューションが必要となります。

サイバーセキュリティの専門家を対象とした最近の調査では、回答者の 90% が、内部ユーザーによる攻撃の検知は外部からの攻撃と同等かまたはそれ以上に困難であると報告しており、内部ユーザーによる脅威の複雑さが浮き彫りになっています[1]。この課題をさらに深刻化させているのが、セキュリティの問題の予防やトラブルシューティングに必要なサイバーセキュリティスタッフの不足です。

1 CSO Online、「Cybersecurity workforce shortage reaches 4 million despite significant recruitment drive」、2023 年

80%
レッドチームによる
攻撃の検知成功率

10以上
特許取得数

内部ユーザーによる脅威に対処するには、内部ユーザーの行為と識別情報の悪用の両方を事前に検知して低減するように設計された、特殊なセキュリティテクノロジーが必要です。不注意な従業員、APT (Advanced Persistent Threats)、悪意のある内部ユーザー、特権昇格、新たな攻撃、ラテラルムーブメントなど、最大の脅威は組織内にすでに潜んでいる可能性が高く、今日の進化し続ける環境において、サイバーセキュリティの専門家は、次のような多くの課題に直面しています。

- セキュリティオペレーションセンター (SOC) のチームは、アラート対応の労力に圧倒され、誤検知に埋もれてしまい、正当な脅威を見つけることが困難になっています。
- 従来のセキュリティツールにはギャップがあり、内部ユーザーによる重大な脅威が気づかれないままになっています。
- すでに逼迫しているリソースは、真の脅威を無力化できず、ノイズの選別に過度に時間がかかっています。
- SOC チームは、通常は 20 もの異なるセキュリティツールを導入していますが、システムとの連携に欠けているため、効果的な通信が妨げられ、防御のギャップをさらしています。
- サイバーセキュリティスキルのギャップにより、セキュリティリーダーはスキルを備えた脅威ハンターを必要な数だけ雇うことができず、脅威検知能力を向上させることができません。

時間的余裕、インサイト、信頼が得られる脅威検知能力が必要とされています。OpenTextTM Core Threat Detection and Response ソリューションを利用すると、SOC チームは管理の負担を軽減しながら、重大な脅威をより迅速に特定し、コストのかかる損害の発生を未然に防ぎ、脅威が急速に進化する環境で優位に立つことができます。

特許取得済みの自己学習型 AI 搭載行動分析により、環境の変化に動的に適応する OpenText Core Threat Detection and Response は、既存のセキュリティソリューションと連携しながら、捉えどころのない内部ユーザーによる脅威と外部ユーザーによって盗まれた識別情報の悪用を発見します。

- **内部ユーザーによる脅威に適応型防御を活用：**当社の AI ソリューションは、お客様の特定の環境にシームレスに適合し、変化に合わせて進化します。これにより確実に、リスクの高い内部ユーザーによるアクティビティを事前に検知し、新たな内部ユーザーによる脅威に対して比類のない保護を提供できます。
- **既存のセキュリティへの投資の ROI を向上：**現在のセキュリティインフラストラクチャと統合して、内部ユーザーによる脅威の検知をさらに強化するとともに、セキュリティへの投資の ROI を向上させます。
- **チームの影響力を倍増：**人材の不足と脅威の増大は、最高の SOC でさえも逼迫させます。当社のソリューションには、新たな脅威を自動的に特定する自己学習 AI に基づく行動型脅威検知機能が備わっているため、既存のチームの作業の有効性が増幅します。さらに、自動化された脅威ハンティングにより異常行動のパターンと高品質の信号が検知されるため、攻撃ライフサイクルのはるかに早い段階で脅威を発見できます。
- **コストの回避：**OpenText Core Threat Detection and Response では、攻撃ライフサイクルの早い段階で高度な脅威が検知されるため、インシデントの修正コストが削減 (または排除) されます。

リソース

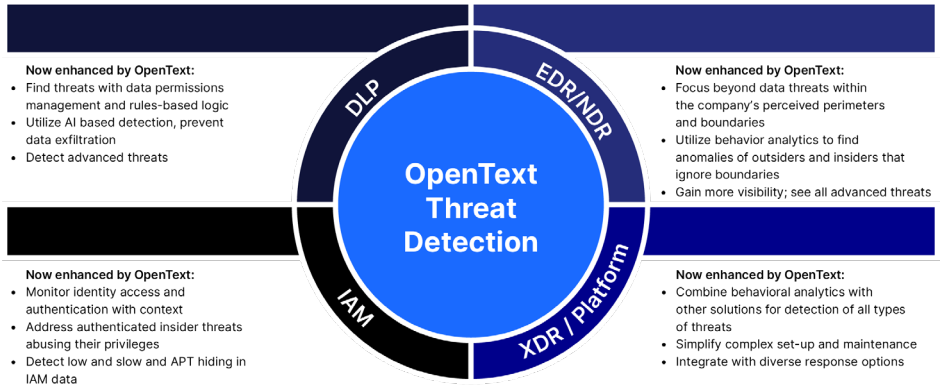
OpenText Core Threat Detection and Response の実際の動作を確認
セルフガイドツアーを試す ›

製品ページを見る
詳細はこちら ›

ローンチの詳細を確認
ブログを読む ›

セキュリティレジリエンス：OpenText で強化

OpenText Threat Detection and Response

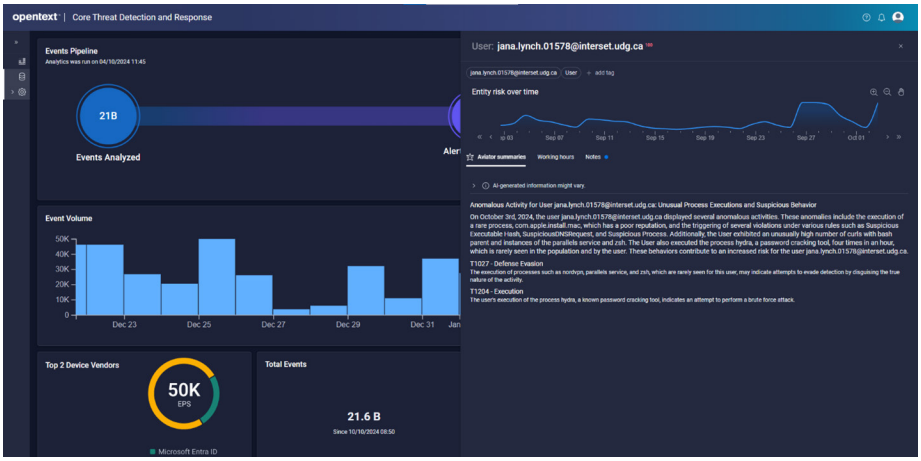


サイバー脅威が進化し続けるなか、OpenText Core Threat Detection and Response を利用すると、組織は最も洗練された攻撃でさえも検知して対応する準備を確実に整えることができます。

- **セキュリティの盲点を排除：**攻撃者は常にルールを破るわけではありませんが、常に異常な行動をとります。AI の精度で組織固有のユーザーやエンティティの行動を可視化して、あらゆる異常を見逃さず、高度な攻撃も見逃さないようにすることができます。
- **脅威ハンターの効率と有効性を改善：**すべてのアラートが同等に作成されるわけではありません。従来のサイバーツールのノイズを排除し、高品質でコンテキスト豊富な手がかりで脅威ハンターをサポートします。現実的で差し迫った脅威に集中して、数か月ではなく数日でインシデントを修正できます。OpenText の脅威ハンティングサービスチームは、行動分析機能を使用することで、レッドチームによる攻撃の検知において 80% 以上の成功率を達成しています。
- **内部ユーザーによる脅威やその他の高度な攻撃を早期に検知：**最大の脅威はすでに内部に潜んでいるかもしれません。組織に大混乱をもたらす前に、内部ユーザーによる脅威を特定して無力化しましょう。データ窃盗や特権昇格から巧妙で長期にわたる攻撃まで、行動分析はルールやしきい値だけでは見逃される異常を検知できます。
- **誤検出を減らしてアラート対応の労力を軽減：**セキュリティは万能ではなく、他の人に合わせて構築すべきではありません。当社の AI を活用したセキュリティソリューションは、ルールベースのツールでは手動更新が必要になる組織全体の変化にも自動的に適応します。本人を把握するセキュリティにおける誤検知を大幅に削減し、セキュリティチームがノイズではなく正当な脅威に集中できるようにします。
- **Microsoft のセキュリティツールとシームレスに統合：**すでに収集している Microsoft Defender for Endpoint と Entra ID のデータを活用し、直感的な OpenText Core Threat Detection and Response ユーザー環境と Microsoft Security Copilot を通じて、脅威アクティビティに関するより深いインサイトを提供します。既存のセキュリティ投資を置き換えるのではなく、強化します。自己学習型 AI に基づく行動型脅威検知を使用して、新たな脅威を特定し、リスクの高いエンティティの行動を要約し、追加のコンテキストを提供することで、SOC における複雑さを低減できます。

セキュリティの再構築

OpenText Core Threat Detection and Response は、脅威検知の新たな進化を体現する製品です。業界をリードする行動分析を活用して、内部ユーザーによる脅威をより高速かつ正確に特定できます。組織が脅威を検知して対応する方法を変革することで、OpenText Core Threat Detection and Response はセキュリティの盲点を排除し、真の教師なし機械学習によって SOC のパフォーマンスを向上させます。Microsoft Defender for Endpoint、Entra ID、Copilot とのシームレスな統合により、OpenText Core Threat Detection and Response は比類のない脅威検知機能を提供します。



アナリスト、脅威ハンター、およびセキュリティ管理者は、環境の全体像を把握できるとともに、高リスクのリードのリストを確認して迅速にフォローアップできるようになります。

特長	説明
適応型の行動駆動型分析	組織の進化するワークフローから学習し、検知のベースラインを自動的に調整します。役割、テクノロジー、ビジネスプロセスの変化に合わせて、「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	既存のエコシステムとシームレスに連携することにより、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	疑わしい行動が特定された場合に、明確な言語でコンテキストに富んだインサイトを提供します。SOC のアナリストは、難解なアラートの解読や無害な異常の調査に時間を無駄にすることがなくなるため、応答時間が改善され、あらゆるレベルの専門知識からの内部ユーザーによる侵害のリスクが低減します。
AI ベースのノイズ低減とリスクベースのアラート優先順位付け	価値の低いセキュリティイベントを自動的に抑制し、リスクの高いインシデントをアナリストに昇格させます。作業負荷とアラート対応の労力が大幅に削減されると同時に、真の脅威に集中できるようになります。
スケーラブルで将来にも対応	組織の成長に合わせて行動モデルを拡張および適応させることができるため、各種のリスクや内部ユーザーによる脅威の戦術に先手を打てるよう、チームの体制を整えることができます。OpenText の専門サービスと継続的なイノベーションにより、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が提供されます。
脅威の優先順位付けのためのリスクスコアリング	行動ベースのリスクスコアリングにより、悪意のある内部ユーザーなど高リスクの脅威に優先順位付けを行うことができます。これによりアラートに対応する労力が軽減し、チームは最も重大なインシデントに数か月ではなく数日で対応できるようになります。