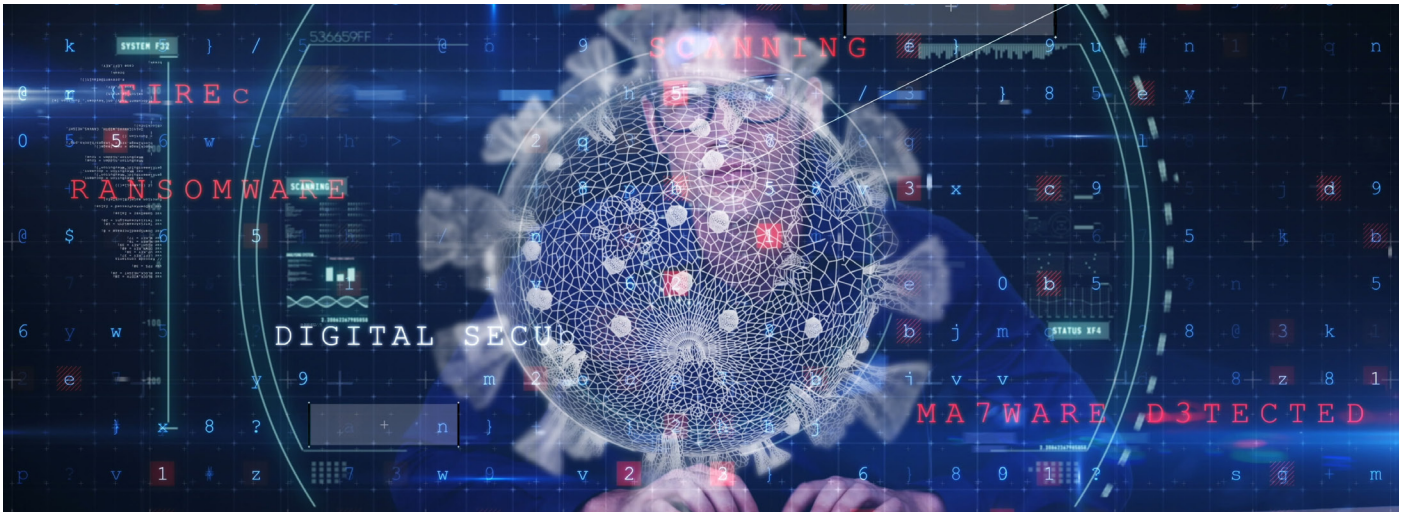
OpenText Endpoint Forensics & Response

サイバー防御では DFIR の精度がすべてを左右するため、エビデンスの収集、脅威の分離、修復を迅速に実施



メリット

- 100 万以上のエンドポイントまで拡張可能なため、より広範な可視性を実現
- アーティファクト主導のワークフローで、ノイズを低減し、対応を迅速化
- エンドポイントの分離により、脅威を封じ込め、中断を最小限に抑制
- 活動中の脅威をリモートで隔離する修正処理

侵害を受けた組織は、多くの場合、発生内容、発生の経緯、アクセスされたデータの詳細、依然として脅威が存在するのかどうか、法的責任の有無など、重大な疑問への答えを得るのに苦慮します。従来のセキュリティツールは、詳細なフォレンジックの可視性に欠けていて手作業でワークフローを進める必要があるため対応に遅れが生じるか、さもなければ調査中に防御性を維持できません。その結果、滞留時間が長期化し、十分な根本原因分析を実施できず、規制準拠上のリスクが生じ、リカバリが遅れます。

OpenText™ Endpoint Forensics and Response を利用すると、セキュリティチームは単一のスケーラブルなプラットフォーム内でより迅速に真相を発見して即座に防止対策を講じることができるため、サイバーセキュリティのデジタルフォレンジックとインシデント対応を最適化できます。

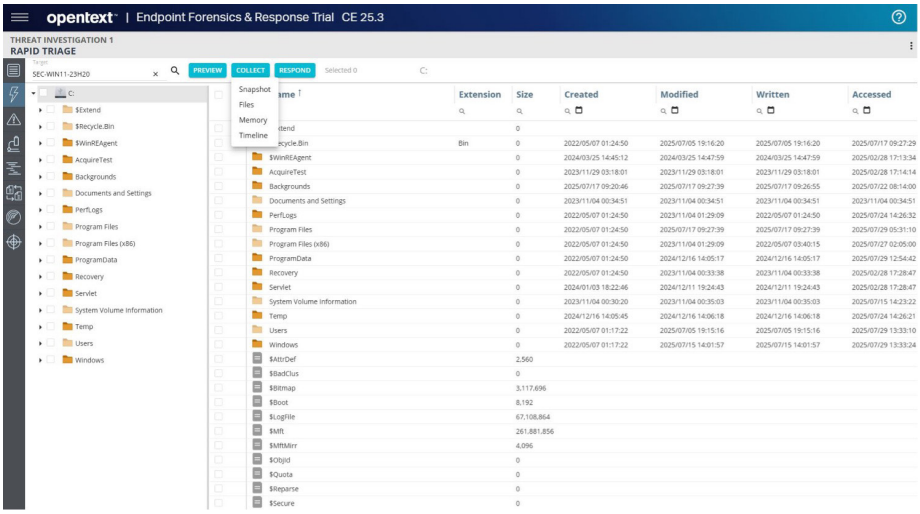
エンドポイントの分離、ファイル / プロセスの修正、レジストリのクリーンアップ、IoC スキャンなど、ほぼリアルタイムでのインシデント対応機能と、充実したデジタルフォレンジック機能を統合することで、OpenText Endpoint Forensics and Response は、滞留時間を短縮し、ラテラルムーブメントを防ぎ、脅威の解決を迅速化する、シームレスに統合されたソリューションを提供します。

セキュリティ担当者は、いくつものツールの間を行き来する必要がなくなり、貴重なコンテキストを失わずにすみます。OpenText Endpoint Forensics and Response では、同じインターフェイス内で調査および対応を実行できるため、生産性が向上し、中断を最小限に抑え、企業全体のサイバーレジリエンスを強化できます。

スケーラビリティ：パフォーマンスの低下に悩まされたり、ケースバイケースで使用するように設計されている DFIR ソリューションとは異なり、OpenText Endpoint Forensics & Response は、100 万以上のエンドポイント間での収集を同時に処理できるように作成されています。そのため、分散型ハイブリッド環境のグローバル企業に最適です。大規模なインシデントが発生した場合でも、ボトルネックのない迅速で信頼性の高い調査を実現できます。

OpenText Cyber Resilience Program (CRP) は、お客様が効果的にリスクを低減し、信頼を維持し、混乱を最小限に抑えるうえで役立ちます。当社は、予防、検知、対応からリカバリ、調査、コンプライアンスに至る、サイバーレジリエンスの構築をサポートします。

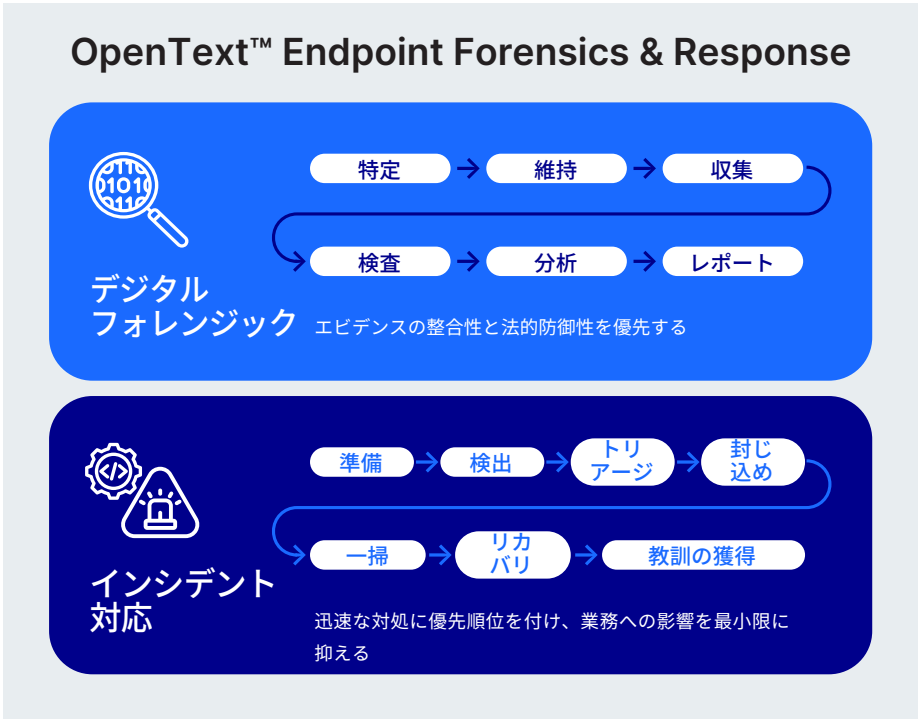
サイバーセキュリティサービス ›



自動化と効率化：OpenText Endpoint Forensics & Response は、単独で運用することも、手動による引き継ぎの必要もなく、既存の SIEM、SOAR、EDR ツールと統合でき、インシデント対応プレイブックの有効性を高めます。エンドポイント層全体に自動化を拡張することで、チームはオーケストレーションされたワークフロー内で直接、エビデンス収集のトリガー、システムの分離、脅威の修正を行うことが可能になります。その結果、手作業が削減され、対応にかかる時間が短縮され、より統一性の高い、コンテキスト豊富な調査プロセスが確保されます。

エンタープライズゼロトラスト：OpenText Endpoint Forensics & Response は、ゼロトラストセキュリティモデルを採用している組織向けに設計されています。分散したエンドポイント (ネットワーク上とネットワーク外の両方) 全体でエビデンスの収集と対応を一元管理でき、企業のエコシステムにシームレスに統合できます。堅牢なデジタルフォレンジックおよびインシデント対応ツールである OpenText Endpoint Forensics & Response により、脅威を検知、分離、調査するうえで必要なフォレンジックの可視性とほぼリアルタイムの対応が、セキュリティチームに確実にもたらされます。

コラボレーションとマルチユーザーアクセス：コラボレーションがレポーティングフェーズの分析後のアクティビティとなっている、個々のアナリストワークフロー向けに設計されたツールとは異なり、OpenText Endpoint Forensics & Response を使用すると、マルチユーザーの同時アクセス可能な、ほぼリアルタイムのコラボレーションおよび一元的なケース管理を実現できます。



リソース

OpenText Endpoint Forensics and Response
製品ページ ›

DFIR：サイバーセキュリティの影の英雄
ブログを読む ›

SOC アナリストの日々 ›

DFIR の精度、スピード、およびフォレンジックレベルの整合性

OpenText Endpoint Forensics & Response を使用すると、インシデントの根本原因の特定、脅威の封じ込め、法的に有効なエビデンスの保全など、チームは業務の中断を最小限に抑えながら、滞留時間を短縮し、修正を迅速化し、コンプライアンスを強化することができます。OpenText Endpoint Forensics & Response は、拡張性、統合性、セキュリティに特化したエンタープライズファーストアーキテクチャと評価されており、今日の脅威を克服し、将来に対応できるサイバーレジリエンスを確保するうえで必要な DFIR の精度、スピード、フォレンジックレベルの整合性を組織にもたらします。

特徴	メリット
アーティファクト主導のワークフロー	関連データのみに焦点を当て、ノイズを削減し、効率性とアナリストの生産性を高め、対応時間を短縮することで、調査を迅速化します。
詳細なフォレンジック調査機能	根本原因を明確にし、隠れた脅威を明らかにし、法的に有効なエビデンスを提供し、情報に基づいた対応と規制への対策を可能にします。これにより、セキュリティチームはより迅速かつスマートに、より高い確信をもって、混乱状態を制御された状態へと回復させることができます。
エンドポイントの分離	フォレンジックアクセスを維持しながら脅威を即座に封じ込め、ラテラルムーブメントを阻止し、業務の中断を最小限に抑え、インシデント対応の信頼性を高め、ゼロトラストの原則をサポートします。
ファイルの修正	SOC チームが即座に対応し、悪意のあるファイルをリモートで削除、隔離、無効化することで、滞留時間、損害、および業務の中断を軽減します。
プロセスの修正	活動中の脅威を即座に停止させます。攻撃の影響を最小限に抑えるために不可欠です。
YARA サポートを伴う IoC スキャン	脅威をより迅速かつプロアクティブに検知し、調査を自動化し、リスクエクスポージャーを低減することで、検知の精度と範囲を強化します。
レジストリ検索とライブ修復	DFIR チームが脅威を特定して無効化し、事業運営を維持し、ダウンタイムなしでセキュリティ体制を強化します。
調査から対応へ直接進行	セキュリティチームはスピード、明快さ、制御を得られるようになり、リスクの高い状況でより迅速かつスマートに意思決定を行えるようになります。
最新の Web UI	措置を講じるまでにかかる時間の短縮、アナリストの生産性の向上、リモートチームや分散したチームへのサポートの提供を実現しながら、IT のオーバーヘッドを削減し、部門間のコラボレーションを改善し、ツールの採用を強化します。
統合された脅威インテリジェンス	DFIR の運用を、よりスマートで、より迅速かつ戦略的な機能へと変革します。これにより組織は、進化する脅威にも対応できるように、早期に検知し、正確に対応し、継続的に進化できるようになります。

opentext™