DELL Technologies

ソリューション概要

CyberSense® for PowerProtect Cyber Recovery

AIベースの機械学習、分析、フォレンジック ツールでサイバー攻撃を検出、診断し、復旧

CyberSenseのメリット

CyberSense®はDell PowerProtect Cyber Recoveryヴォールト ソリューションと完全に統合されています。

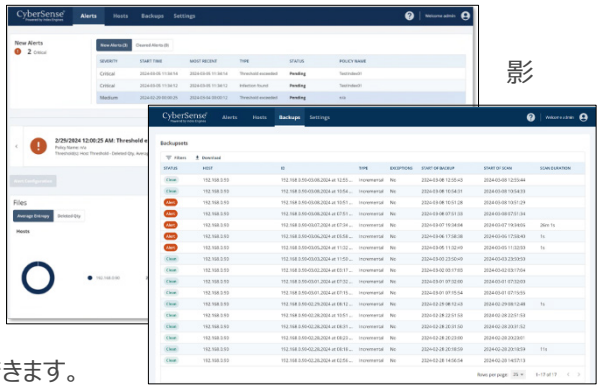
- この統合により、バックアップ データを定期的にスキャンしてデータの整合性を検証し、不審な振る舞いが検出されたときにアラートを発するというプロセスを自動化できます。
- CyberSenseは、Dell NetWorker、Avamar、PowerProtect Data Managerなどのバックアップ イメージ内部を直接スキャンする機能を備えており、データをリハイドレートすることなくコンテンツを分析できます。
- 他のソリューションにはないCyberSenseだけの機能として、データをスキャンするごとにフルコンテンツ分析を実施できるため、メタデータしか検査しない軽量のスキャン ツールでは見逃しやすい巧妙なランサムウェア攻撃も検出できます。
- CyberSenseは、攻撃の深度と範囲を把握するための攻撃後のフォレンジック レポートや、破損前の最後の正常なバックアップ セットを示すリストを作成します。そのため、攻撃が発生した場合でも、リカバリー プロセスを円滑に進められます。

CyberSenseは、他のデータ分析アプローチとは一線を画しており、バックアップ データの整合性が確保されていて攻撃発生後に迅速に復旧できるというワンランク上の安心感をもたらします。

従来のセキュリティ ツールではサイバー攻撃からデータを確実に保護できない場合、**CyberSense®**を利用することで、攻撃後のデータ破損を99.5%の正確度で検出し、インテリジェントで迅速なリストアを促進できます。CyberSenseは、世界中の何千もの組織にとって最後の防衛線かつリカバリーの最前線として機能します。コア インフラストラクチャや本番データベース、重要なドキュメントなどのデータ資産の整合性を確保し、データに悪意のある破損がないという安心感をもたらします。

CyberSenseは、データ バックアップを活用してデータの経時的な変化を観察し、次にAIベースの機械学習を利用してランサムウェア攻撃を示唆する破損の兆候を検出します。その後機械学習が、このような200以上のコンテンツベースの分析情報を調査し、99.5%の信頼度で破損を発見するため、ビジネスクリティカルなインフラストラクチャとコンテンツの保護に役立ちます。CyberSenseは、巧妙な攻撃の結果として発生する、コア インフラストラクチャ（Active Directory、DNSなど）やユーザー ファイル、重要な本番データベースにおける大量の削除や暗号化、その他の疑わしい変更を検出します。CyberSenseが破損の兆候を検出するとアラートが生成され、攻撃の規模と影響の詳細を示す追加情報とともにダッシュボードに表示されます。

不審な振る舞いが発生すると、CyberSenseは、サイバー攻撃の影響範囲を診断するための攻撃後のフォレンジック レポートを作成します。データの破損が検出されると、破損前の最後の正常なバックアップ データ セットのリストが提供されるので、迅速かつ的を絞ったリカバリーを行い、ビジネスの中断とデータ ロスを最小限に抑えることができます。



Cyber Recoveryのワークフロー

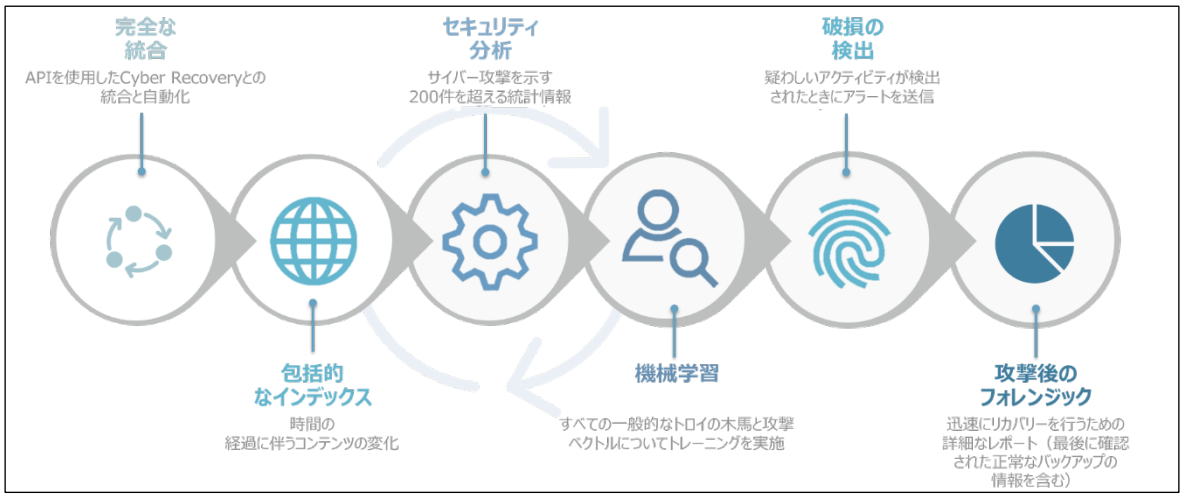
CyberSenseはDell PowerProtect Cyber Recoveryとシームレスに統合されており、ファイルとデータベースをアクティブにモニタリングして、データの整合性を分析することでランサムウェアによる破損を検出します。データがCyber Recoveryヴォールトに複製され、保存ロックが適用されると、CyberSenseはバックアップ データの包括的なスキャンを自動的に開始し、ファイル、データベース、コア インフラストラクチャのポイントインタイムの観測記録を作成します。CyberSenseはこの観測記録を利用して、ファイルの経時的な変化を綿密に追跡し、巧妙なサイバー脅威によるデータ破損も効果的に発見します。

CyberSense のスキャンでは、バックアップ イメージ内のデータを直接操作するため、元のバックアップ ソフトウェアやデータのリハイドレートが不要です。CyberSense は、高度な分析を通じて、ファイルまたはデータベース ページの暗号化や破損の特定、マルウェアが使用する既知の拡張子の認識、ファイルの大量削除や作成の検出などを行います。

CyberSense は、最新のトロイの木馬とランサムウェアでトレーニングされた AI ベースの機械学習アルゴリズムを利用して、サイバー攻撃を示唆するデータ破損について確定的な判断を下します。攻撃を受けた場合、重要なアラートが Cyber Recovery ダッシュボードに即座に表示されます。さらに CyberSense が作成する攻撃後のフォレンジック レポートを利用して、ランサムウェア攻撃に関する診断とリカバリーを円滑かつ迅速に行い、データ ロスを最小限に抑えることができます。

フル コンテンツ分析

CyberSenseは、すべての保護対象データに対してフルコンテンツベースの分析を行う市場で唯一の製品です。CyberSenseが他のソリューションと大きく異なるのはこの点です。一般的なソリューションは、データのハイレベル ビューを取得し、メタデータに基づいて破損の明らかな兆候を探す分析を利用します。メタデータレベルの破損（例：ファイル拡張子が「.encrypted」に変更される、ファイル サイズが大幅に変化している）を検出するのは難しくありません。しかし、このような種類の攻撃は、現代的なサイバー犯罪者による巧妙な攻撃では用いられません。



CyberSenseは、メタデータのみを利用するソリューションとは異なり、フル コンテンツ分析を使用してデータ破損を検出します。ファイル構造のコンテンツ部分のみを破損する攻撃や、ドキュメントまたはデータベース ページの内部を部分的に暗号化する攻撃が発生していないか、ファイルやデータベースを監査します。このような攻撃は、ファイル内部をスキャンして経時的な変化を比較する分析を利用しなければ検出できません。フルコンテンツベースの分析を行わないと、検出漏れの件数が膨大になり、データの整合性とセキュリティに対する過信が生まれてしまいます。また、変更されたファイルやファイル タイプ、追加または削除されたファイルやエントロピーのホスト全体にわたる件数や割合に基づいて、カスタムのしきい値アラートを作成できます。

サポートされているデータ タイプ

CyberSenseは、幅広いデータ タイプからの分析を生成できます。例えば、DNSやLDAP、Active Directoryなどのコア インフラストラクチャ、ドキュメントや契約書、知的財産などの非構造化ファイル、OracleやDB2、SQL、PostgreSQL、Epic Cachéなどのデータベースに対応しています。

概要

CyberSenseはDell PowerProtect Cyber Recoveryと完全に統合されており、データを監査し、侵害や破損の兆候を検出します。CyberSenseを導入すると、発生しているサイバー攻撃の影響範囲をプロアクティブに把握し、迅速な診断と復旧のための計画を円滑に実施できるため、ビジネスの中断とそれに伴う多額の損失を軽減できます。

Dell PowerProtect Cyber Recovery の詳細はこちら	デル・テクノロジーズのエキスパートに問い合わせる	CyberSense の詳細はこちら	#PowerProtect で会話に参加