SentinelOne

ソリューションの概要

SentinelOne Singularity XDR

サイバーセキュリティの脅威の状況は、急速に進化し、拡大しています。エンドポイント、ネットワーク、クラウドなど、攻撃ベクトルが多様化する中、多くの企業は各領域の脆弱性を保護するための最善なソリューションで各攻撃ベクトルに対応しています。しかし、このようなポイントツールでは、テクノロジースタック全体の点と点を結ぶことはできません。その結果、コンテキストや相関関係を欠いた分断されたセキュリティデータを収集し、分析することになるため、各セキュリティチームが把握、検知する内容にギャップが生じます。また、手作業による調査プロセスには時間と手間がかかることが多く、セキュリティチームが脅威の封じ込めと修復に後れを取る原因となります。

Singularity XDR

SentinelOne Singularity XDRは、複数のセキュリティ層にまたがり検知と対応の機能を統合して拡張することで、セキュリティチームに一元的なエンドツーエンドの企業可視性、優れた分析、テクノロジースタック全体での自動対応機能を提供します。Singularity XDRを使用することで、お客様は統合されたプロアクティブなセキュリティ対策によってテクノロジースタック全体を保護でき、進行中の攻撃がビジネスに影響を与える前にセキュリティアナリストが容易に特定して阻止できるようになります。

主な機能

01 | スタック全体の可視性で盲点を解消

Singularity XDRを使用すれば、企業はあらゆるテクノロジー製品やプラットフォームから構造化データ、非構造化データ、半構造化データをシームレスかつリアルタイムに取り込み、データサイロを解消して重大な盲点を取り除くことができます。このソリューションにより、セキュリティチームはエンドポイント、クラウドワークロード、IoTデバイス、ネットワークなど、あらゆるプラットフォームからさまざまなセキュリティソリューションによって収集されたデータを単一のダッシュボードで確認できます。Singularity XDRにより、複数の異なるソリューションのイベント情報がコンテキスト化された1つの「インシデント」に集約され、そこからアナリストはインサイトを得ることができます。また、Singularity XDRは企業の包括的な可視性と自律的な予防、検知、対応を実現し、一元的な適用と分析のレイヤーポイントハブを提供し、組織がサイバーセキュリティの課題に統一的視点から対処できるように支援します。

02 | スタック全体での相関付けでステルス攻撃を検出

SentinelOneが特許を取得したStoryline™ テクノロジーは、エンタープライズ セキュリティ スタック全体で、リアルタイムの自動化されたマシン生成のコンテキストと相関関係を提供し、ばらばらなデータをリッチなストーリーに変換することで、セキュ

ソリューションのメリット

SOCの効率と生産性の向上

対応時にコンテキストを切り替えたり複数のダッシュボードを使用したりする必要がないため、遅延が最小限に抑えられます。1つのプラットフォームと 1 つのワークフローにより、アラートの数を減らし、盲点やデータのギャップをなくし、対応時にセキュリティ担当者がアクセスしなければならないインターフェースの数を減らすことができます。

価値実現までの時間を短縮

複数の異なる製品をすぐに統合できます。そのため、既存のサイバーセキュリティ投資の価値を迅速に最大化できます。

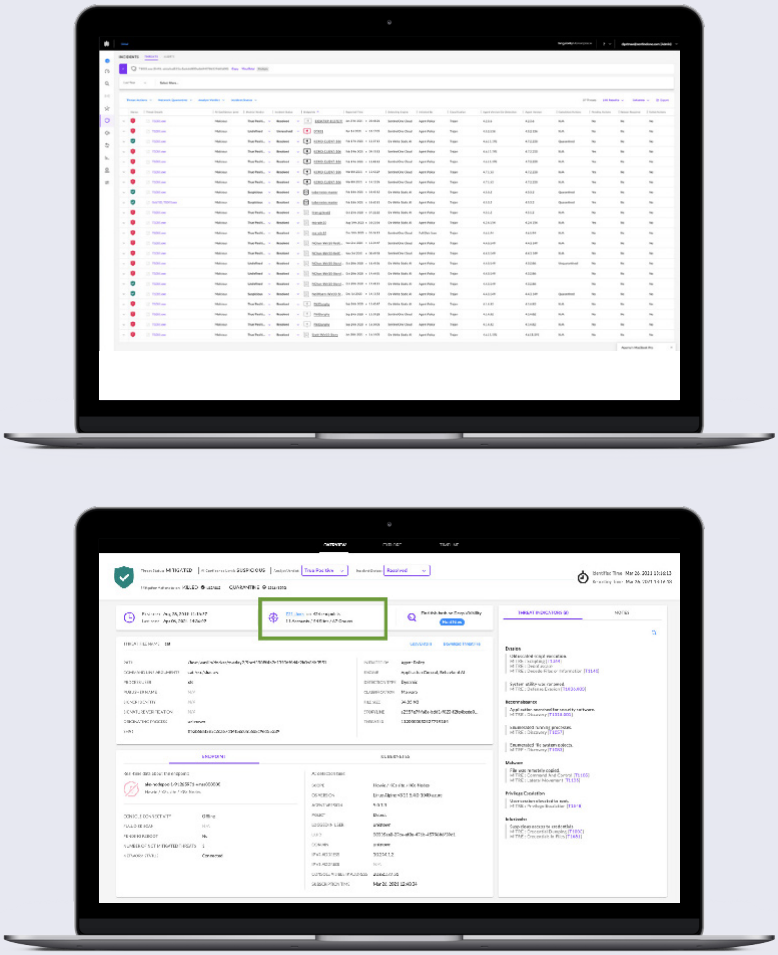
オペレーションとワークフローの合理化

サイロ化されたデータストリームを一元的に可視化して分析できます。

総保有コスト（TCO）の削減

完全に統合されたサイバーセキュリティプラットフォームにより、複数のポイントソリューションの設定や統合に伴うコストを削減できます。

リティアナリストは自社の環境内で発生したすべての出来事を把握できるようになります。Storylineは、関連するすべてのイベントとアクティビティを自動的につなぎ、一意の識別子を持つストーリーラインを作成します。これにより、セキュリティチームは発生した出来事の詳細なコンテキストを数秒以内に確認でき、数時間、数日、あるいは数週間かけてログの相関付けやイベントの関連付けを手動で行う必要はありません。SentinelOneの行動エンジンは、ファイルやレジストリの変更、サービスの開始と停止、プロセス間の通信、ネットワークアクティビティなど、環境全体のすべてのシステムアクティビティを追跡します。また、ステルス行動を監視し、ファイルレス攻撃、ラテラルムーブメント、ルートキットのアクティブな実行を効果的に識別するために、悪意のある行動の指標となるテクニックや戦術を検知します。Singularity XDRは関連するアクティビティを統合されたアラートに自動的に相関付けることで、攻撃キャンペーンに対するインサイトをもたらします。これにより、企業はさまざまなベクトルにわたってイベントを相関付け、アラートを単一のインシデントとして容易にトリアージできるようになります。



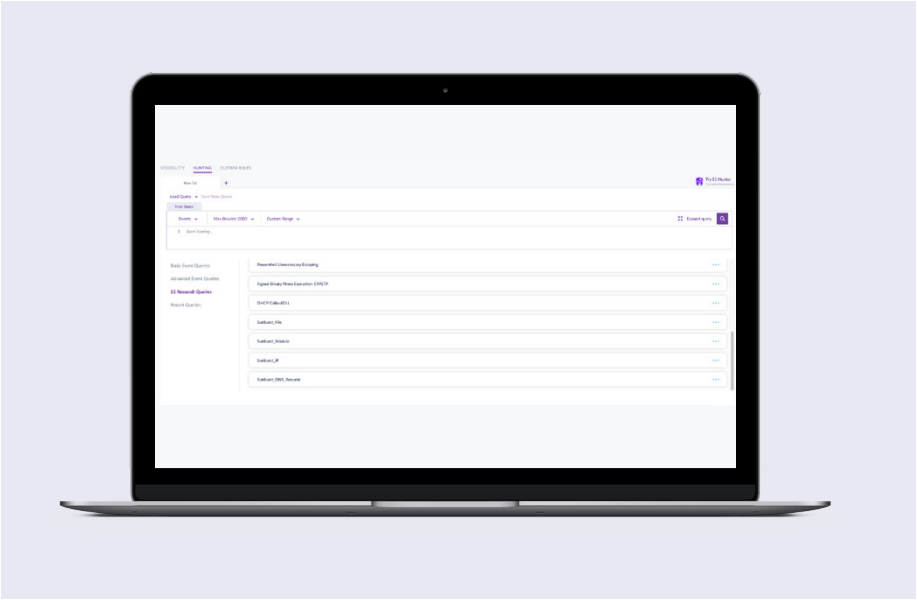
主な統合

- エンドポイント
- IoT
- クラウド
- 脅威インテリジェンス
- ID
- メール
- ネットワーク
- SASE

03 | 統合された脅威インテリジェンスによる脅威データの自動エンリッチ化

Singularity XDRは、主要なサードパーティのフィードからの検知とエンリッチ化のための脅威インテリジェンスと、エンドポイントのインシデントをリアルタイムの脅威インテリジェンスで自動的にエンリッチ化するSentinelOne独自のソースを統合します。これにより、セキュリティチームはIP、ハッシュ、脆弱性、ドメインなど、侵害の痕跡（IoC）に関するコンテキストに即した追加のリスクスコアを取得できます。た

とえば、Recorded Future社との統合により、80万を超えるソースによって脅威データが自動的にエンリッチ化されるため、お客様は脅威の調査とトリアージを迅速に実行できます。また、SentinelOneの調査によってキュレートされた脅威ハンティング用のクエリライブラリも利用できます。調査では、新しいIoCや戦術、テクニック、手順（TTP）を明らかにするために、新しい方法論を常に評価しています。



04 | 異なるドメイン間で対応を自動化

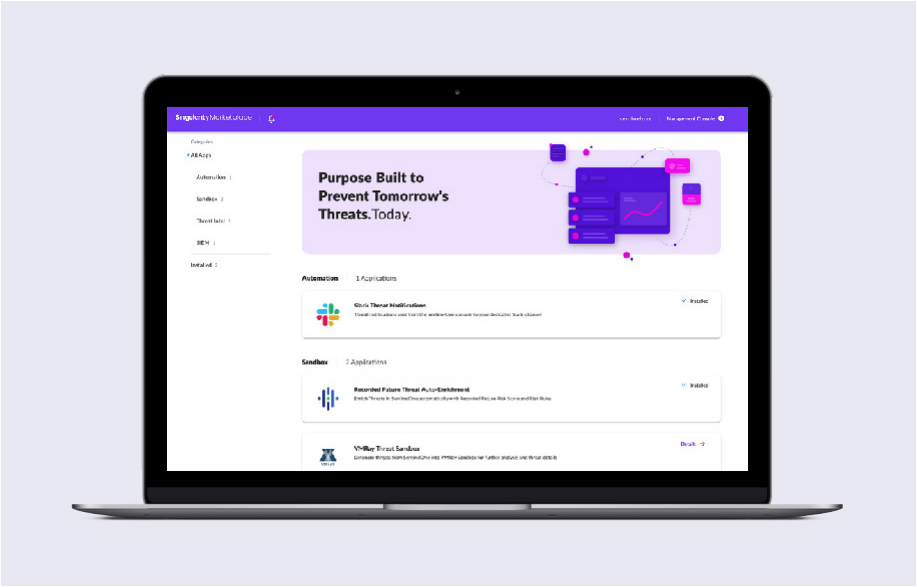
Singularity XDRを使用すると、アナリストは必要なすべてのアクションをワンクリックで実行し、脅威を自動的に解決できます。社内の1つ、複数、あるいはすべてのデバイスでスクリプトを記述する必要はありません。アナリストはネットワークの隔離、不正なワークステーションへのエージェントの自動デプロイ、クラウド環境全体でのポリシー適用の自動化などの修復アクションをワンクリックで実行できます。

また、Singularity XDRでは、Storylineが提供するインサイトを活用して、Storyline Active Response（STAR）で環境に適したカスタム自動検知ルールを作成することもできます。STARを使用すると、企業はビジネスコンテキストを組み込み、ニーズに合わせてEDRソリューションをカスタマイズできます。Storyline Active Response（STAR）のカスタム検知ルールを使用して、クエリを脅威ハンティングの自動ルールに変換することができます。ルールに一致する脅威が検知されると、アラートと対応が開始されます。STARを利用すれば、環境に応じてカスタムのアラートと対応を柔軟に作成できます。たとえば、プロセスを自動的に強制終了して、環境全体の脅威を自動的かつ迅速に検知して封じ込めることができます。

05 | 主要なSOARツールとのスムーズな統合

SOCに他のセキュリティツールやテクノロジーを導入しているお客様向けに、SentinelOneはSIEMやSOARなどのサードパーティシステムとの統合機能のポートフォリオを拡充しており、Singularity Marketplaceで提供しています。Singularity アプリケーションは拡張性に優れたサーバーレスのFaaSクラウドプラットフォーム上でホストされており、数回のクリックでAPI対応のITおよびセキュリティコントロールと連携できます。Singularity MarketplaceはSentinelOneプラットフォームの一部であり、一度統合を設定すれば、すぐに効果を実感できます。複雑なコードを記述する手間が省け、自動化がシンプルになり、ベンダー間の拡張が可能になります。さまざまなドメインのセキュリティツール間で統合され、調整された対応を促進することで、セキュリティチームは、急速に進化する脅威を修正して阻止するための最善策を簡単に実施できます。

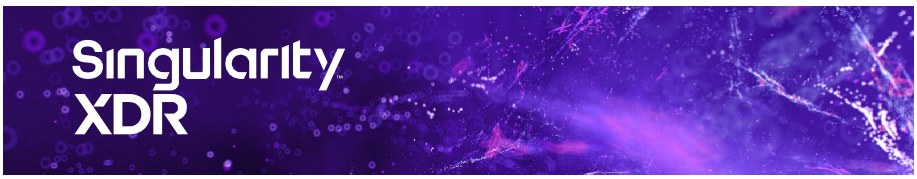
> “
>
> データの取り込みは、ほとんどのベンダーにとって大きな課題です。セキュリティデータの量、速度、多様性に対応するために、XDR テクノロジーは、ハイブリッド IT 全体でセキュリティデータを大規模に収集して処理できる最新のデータパイプラインによって支えられている必要があります。
>
> また、XDR テクノロジーは自動化されたマシン生成のコンテキストと相関関係を提供し、エンタープライズ セキュリティ スタック全体にわたる自動化されたインサイトをセキュリティチームに提供できる必要があります。
>
> **Dave Gruber**
>
> エンタープライズ戦略グループ
> シニアアナリスト



06 | セキュリティチームの拡張とSOCの効率化

Singularity XDRは、次の機能により、単一の統合されたプラットフォームによる拡張された脅威検知、調査、対応、ハンティングを実現します。

- 優先順位付けされたアラートの単一ソース（複数のソースからデータを取り込み、標準化）。
- セキュリティ層全体の攻撃の進行状況をすばやく把握できる単一の統合ビュー。
- 脅威をプロアクティブにハンティングし、すばやく対応できる単一のプラットフォーム。



ソリューションの特徴

さまざまなソースからデータをシームレスに取り込む

あらゆるテクノロジー製品やプラットフォームから構造化データ、非構造化データ、半構造化データをリアルタイムに取り込みます。

エンタープライズスタック全体の攻撃キャンペーンを発見する

エンタープライズ セキュリティスタック全体にわたるリアルタイムかつ自動化されたマシン生成のコンテキストと相関関係を取得して、さまざまなデータをリッチなストーリーに変換します。

実用的な自動対応で攻撃をすばやく封じ込める

ワンクリックで自動的に脅威を解決できます。社内の1つ、複数、あるいはすべてのデバイスでスクリプトを記述する必要はありません。

調査と脅威ハンティングを加速する

中央データリポジトリに共通のクエリ機能を提供して、高度な攻撃者をプロアクティブに発見します。

信頼性と評価の高い革新的なソリューション

Gartner

2021年のエンドポイント保護プラットフォーム分野のマジッククアドラントのリーダーに選出

クリティカルケイパビリティレポートのユースケースすべてにおいて最高ランクを獲得

MITRE ENGENUITY

過去最高のATT&CK評価

- 検知漏れがゼロであり、100%の可視性を提供
- 2年連続で最も完全なアナリティック検知を実現
- 遅延がなく、構成の変更が不要

Gartner peerinsights 4.9

Gartner Peer Insights™ の98%が高評価

「お客様の声」の多くがSentinelOneを推奨

FedRAMP

ISO 27001 CERTIFIED by schellman

100 VIRUS virusbtn.com

TEVORA PCI DSS Attestation HIPAA Attestation

SentinelOneについて

より多くの機能を、よりシンプルに。SentinelOneは、エンタープライズレベルの機能を損なうことなくセキュリティスタックを簡素化するために、自律的な分散型エンドポイントインテリジェンスを活用してサイバーセキュリティの未来を開拓しています。SentinelOneの技術は、脅威への対応を自動化してスムーズに行えるようにすることで、セキュリティ担当者の生産性が向上するよう設計されています。ぜひ、SentinelOneのソリューションをお試しください。

sentinelone.com

sales@sentinelone.com

+ 1 855 868 3733