

Dell SafeGuard and Response

Secureworks® Taegis™ XDR

セキュリティとリスク削減の成果向上に役立つ自動化で、サイバーセキュリティの脅威を管理して対応

主な特長

- エンドポイント、ネットワーク、クラウド環境など、**攻撃対象領域を包括的にカバー**
- 複数の攻撃経路から収集し、包括的な脅威インテリジェンスによって強化された**テレメトリーとイベントを機械学習/ディープラーニングを活用して分析**
- 必要なときに必要な場所で動作する、必要なすべてのコンテキストとデータで強化された**忠実度の高いアラート**
- **コンソールに用意されている自動プレイブックによるワンクリック対応アクション**
- サードパーティーのセキュリティツールとの幅広い統合を提供する**オープンなXDRソリューション**。事前に構築された統合を利用できるほか、カスタム統合を簡単に作成可能

Secureworks Taegis™ XDRクラウドネイティブSaaSプラットフォームは、脅威ランドスケープに関する詳細なセキュリティ知識を取り入れて、セキュリティ運用の有効性と効率性の向上を支援します。

- 組織のIT環境全体からリアルタイムのテレメトリーを集約して、Windows、macOS、Linuxのエンドポイント、ネットワーク、クラウド環境を総合的に可視化し、制御できます。
- AIを活用した分析、数千もの組み込み自動対策、一連の機械学習脅威検出機能、関連する低レベルのイベントを結び付ける高性能なTactic™ Graphsを使用して、高度な脅威とMITRE ATT&CK TTPを検出します。Taegisでは、機械学習とAIを利用して下位レベルのイベント内のパターンを認識し、共通点がある場合にそれらのパターンを結び付けます。
- 重要なアラートに集中し、調査を迅速化します。Taegis XDRでは、インシデント対応データと脅威ハンティングツールを利用できます。また、使いやすい1つのクラウドコンソールで、自動化されたプレイブックを手軽に使用できるようになっています。

Taegisに組み込まれているすべての機能は、Secureworks Counter Threat Unit™とSecureworksチームが完了した数千件の実際のインシデント対応エンゲージメントからの包括的な脅威インテリジェンス情報によって、絶えず強化されています。

セキュリティの有効性を最大化

Taegis XDRは、ネットワーク、クラウド、エンドポイント、その他のセキュリティ ツールからの信号を脅威インテリジェンスとともに集約します。そのため、環境を一元的に可視化して、攻撃対象領域を管理できます。

TaegisのAI搭載検出機能では、最先端の機械学習アルゴリズムと分析手法を利用して、環境内に悪意のある活動がないかを継続的にモニタリングし、攻撃者の行動を早期に認識します。Taegis XDRの自動ブレイブックとワンクリック対応アクションは、迅速な対応を可能にします。また、巧妙な攻撃を検出、把握して、それらの攻撃が被害を及ぼす前に防止するのに役立ちます。

Secureworks Counter Threat Unitによって継続的に生成される包括的な脅威インテリジェンスを利用すると、新たな脅威と脅威アクターの意図および行動を詳細に分析できます。この情報は、攻撃を阻止するためにTaegis XDRの対策に組み込まれています。さらに、お客様のチームはこの情報を利用して、脅威の攻撃者、内容、発生時刻、理由、手法を理解できます。

セキュリティの運用効率を向上

重要な事項の調査： Taegisは、さまざまなセキュリティ ツールから得た脅威インテリジェンス、ログ、イベントを関連付けて、アラートの検証と優先順位付けを行います。これにより、アナリストが偽陽性に対処する時間が少なくなり、実際の脅威に対処するための時間が増加します。

攻撃に関する疑問を速やかに解決： Taegisは、エンドポイント、ネットワーク、クラウド環境全体で関係するイベントを自動的に関連付けて、攻撃の根本原因を特定できるようにします。

単一のプラットフォームで調査を実行： Taegisは環境全体からデータを収集するほか、MITRE ATT&CK TTPなど、包括的な脅威ハンティング ツールキットを組み込んでいます。そのためアナリストは、セキュリティ インフラストラクチャの全体像を把握して、ツール間でデータを手動でつなぎ合わせることなく、プラットフォーム内で調査を実行できます。

よりスマートかつ迅速に連携： アナリストが関連情報を迅速に組み立てて、それを他人と共有して調査で共同作業（コメントの作成、関連データの追加または削除、ステータスの変更など）ができるようにする柔軟な検索およびレポート作成機能があり、共同作業の改善と意思決定の迅速化を通じて調査をスピードアップできます。

お客様のソフトウェア向けDell ProSupport

お客様のDell製エンドポイント セキュリティ ソフトウェア ソリューションには、Dellのサポートが付属しています。Dell ProSupport for Softwareでは、高度な資格を持つ認定技術者から24時間365日体制で包括的なソフトウェア サポートを受けられるため、ソフトウェアを安心してご利用いただけます。

セキュリティ体制の強化に役立つSafeGuard and Response製品については、担当のDellエンドポイント セキュリティ スペシャリスト(endpointsecurity@dell.com)までお問い合わせください

システム要件：Taegis XDRコンソール - クラウド ネイティブ アプリケーションのため、最新のブラウザが必要です（Chrome、Edge、またはFirefox）。Taegis XDR Agentのサポート対象システム：Microsoft Windows - Windows 10、11、Windows Server 2016および2019、macOS：macOS Catalina 10.15、Big Sur 11、Monterey 12 (+M1)、その他：CentOS 7、Amazon Linux 2、Ubuntu 18.04

詳細については、DellEMC.com/endpointsecurityをご覧ください

© 2022 Dell Technologiesまたはその関連会社。