SOPHOS
Cybersecurity made simple.

Intercept X Advanced with EDR

高度な Endpoint Detection and Response

Sophos Intercept X Advanced with EDR は、高度なエンドポイントの EDR (Endpoint Detection and Response) 機能を、業界で高く評価されているマルウェア検出とエクスプロイト対策、および他の卓越したエンドポイント保護機能に統合します。

主な特長

- EDR を最強のエンドポイント保護に統合
- ディープラーニングによるマルウェア解析
- SophosLabs がまとめた脅威解析情報をオンデマンドで利用
- 疑わしいイベントを機械学習で検出し、対処の優先度を表示 *
- 手順に従ってインシデントに対応できるので、EDR は使いやすいだけでなく強力
- ワンクリックでインシデントに対応

最強のエンドポイント保護を基盤にした EDR

発生前にセキュリティ侵害を阻止するには防止対策が重要です。Intercept X は、卓越した保護とエンドポイントの検出と対応機能を統合し、単一のソリューションとして提供しています。したがって、脅威の大半は被害を与える前にブロックされます。Intercept X Advanced with EDR は、潜在的なセキュリティ脅威を検出、調査、対応し、より確実なサイバーセキュリティ対策を提供します。

EDR は高い評価を獲得しているエンドポイント保護ソリューションに統合されているため、その負荷は Intercept X によって大幅に削減されます。より多くの脅威が阻止されるので、セキュリティチームは、限られた少数の脅威に集中的に対処することができます。これによって主要リソースの使用を最適化し、誤検知や膨大な量の警告などの対処に追われることなく、本来の IT 業務に専念することができます。

人的リソースを追加せずに、専門知識をアップ

Intercept X Advanced with EDR は、従来、熟練したアナリストによって実行される作業を再現するので、組織に人的リソースを追加することなく、専門知識を増やすことができます。熟練したアナリストが適切な方法で解析し、データを解釈する他の EDR ソリューションとは異なり、Intercept X Advanced with EDR は機械学習によって支えられており、SophosLabs がまとめた脅威解析情報で強化されています。

セキュリティの専門知識 * : Intercept X Advanced with EDR は、潜在的な脅威を自動検出し、対処の優先度を表示するので、IT 管理者は提供されるセキュリティの専門知識を活用することができます。疑わしいイベントは、機械学習を使用して検出され、重要で対処の優先度が高いイベントとして表示されます。したがって、IT 管理者は至急に対処が必要なイベントを直ちに見極めて、影響を受けている可能性のあるマシンを把握することができます。

マルウェアの専門知識 : たいていの組織は、マルウェア解析の専門家が行う、疑わしいファイルのリバースエンジニアリングによる解析に依存しています。しかし、この方法は、時間がかかり難しいだけでなく、たいていの組織にはない高レベルのサイバーセキュリティの専門知識を前提としています。一方、Intercept X Advanced with EDR は、ディープラーニングによるマルウェア解析を活用するより優れた方法を使用しています。これは、マルウェアを細部にわたって自動的に解析し、ファイル属性とコードを分解し、数百万ものファイルと比較を行います。IT 管理者は、どの属性やコードセグメントが、既知の「正規」ファイルまたは「不正」ファイルに似ているかを簡単に把握して、ファイルのブロック/許可を判定できます。

脅威解析情報の専門知識：Intercept X Advanced with EDR で、対処の優先度が高い疑わしいファイルが表示されると、IT 管理者は SophosLabs がまとめた脅威解析情報にオンデマンドでアクセスして詳細情報を取得できます。SophosLabs は、毎日、およそ 40万件の未知のマルウェアを受信・処理しています。この情報および他の脅威解析情報は収集、集約、要約され、簡単な解析結果が生成されます。したがって、専門の脅威解析アナリストがいない、または高価で理解が困難な脅威フィードへのアクセスのない IT チームでも、世界最高レベルのサイバーセキュリティの研究チーム、およびデータサイエンスチームの専門知識を活用することが可能になります。

手順に従ってインシデントに対応

Intercept X Advanced with EDR を活用すると、管理者はセキュリティインシデントに関する複雑な問題点に答えることができるようになります。攻撃の範囲、攻撃の経路、影響範囲、および対応方法などを一目で把握できます。手順に従って調査を実施できるので、専門知識のレベルを問わず、すべてのセキュリティチームは、組織のセキュリティ状態をすばやく把握することができます。ビルトインの専門知識を基に、推奨される次のステップや、わかりやすい視覚的な攻撃経路などが表示されます。

インシデントの調査が完了したら、IT 管理者はボタンを1つクリックするだけです。迅速な対応のオプションには、即座に修復を行うためのエンドポイントの隔離、ファイルのクリーンアップとブロック、およびフォレンジック分析のスナップショットの作成などがあります。

高度な EDR のユースケース

高度な EDR にある可視性と専門知識を活用して、セキュリティチームは、インシデント対応作業の一環として回答が必要な複雑な問題点に答えることができます。

次のような手順を実行して、インシデントに関する複雑な問題点に答えることができます。

- セキュリティインシデントの攻撃の範囲および影響範囲を把握
- これまで検出されていなかった攻撃を検出
- ネットワークで感染の痕跡を検索
- 詳細な調査が必要なイベントの優先度を表示
- 脅威または不要と思われるファイルであるかを解析
- 組織のセキュリティ状態に関する詳細なレポートを常時生成

EDR をはじめとする多層防御のアプローチ

Intercept X Advanced with EDR は、多種多様な脅威を阻止するために、1つの主要機能に依存することなく、包括的な多層防御のアプローチを採用してエンドポイントを保護しています。主要かつ基本的な技術と最新の技術を組み合わせて、「プラスの力」を発揮しています。Intercept X Advanced with EDR は、業界で高く評価されているマルウェア検出とエクスプロイト対策、および高度な EDR 機能を統合しています。

最新の技術には、ディープラーニングによるマルウェア検出、エクスプロイト対策、およびランサムウェア対策の機能などがあります。基本的な技術には、マルウェア対策、動作解析、Malicious Traffic Detection (MTD)、データ流出防止などがあります。

Intercept X Advanced with EDR は、エンドポイントの検出と対応機能を、Intercept X にある最新の技術および Sophos Endpoint Protection にある基本的な技術と組み合わせています。そして、これは単一のソリューションとして統合エージェントで提供されます。

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
従来型の技術	✓	✓		✓
ディープラーニング	✓	✓	✓	
エクスプロイト対策	✓	✓	✓	
CryptoGuard ランサムウェア対策	✓	✓	✓	
EDR (Endpoint Detection and Response)	✓			

無償評価版

無償評価版の登録 (30日間)
www.sophos.com/ja-jp/intercept-x

* 2019年初旬にリリース予定

ソフォス株式会社
営業部
Email: sales@sophos.co.jp

18-10-02 DS-JA (3098-DD)

SOPHOS