SOPHOS
Cybersecurity evolved.

Intercept X Advanced with EDR

脅威ハンティングと IT の運用のために構築 - EDR (Endpoint Detection and Response)

Sophos Intercept X Advanced with EDR は、強力な EDR (Endpoint Detection and Response) 機能を、比類のないエンドポイント保護に統合します。脅威を探し出し、アクティブな敵対行為を検出、または IT 運用を活用して IT セキュリティの予防状態を維持します。問題を検出した際には、リモートで的確な対応します。

主な特長

- EDR を最強のエンドポイント保護に統合
- セキュリティアナリストと IT 管理者向けに設計
- 被害が発生する前に、IT セキュリティの予防状態を積極的に維持し、脅威を検出
- 過去に何が起きたのか、今何が起きているのかについて質問
- すぐに使用可能で自由にカスタマイズできる SQL クエリ
- 現在および過去のディスク上のデータへの最長90日間の高速アクセス
- コマンドラインツールを使用して、正確にリモートで対応
- 機械学習を活用して、インシデントを検出、調査、優先順位付け
- 調査を迅速化し、攻撃者の滞留時間を短縮
- Windows、macOS、および Linux で使用

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、業界最高レベルのクラウドホスト型のエンドポイント保護と EDR を単一のソリューションに統合します。つまり、ほとんどの脅威が被害をもたらす前に阻止されるということです。Intercept X Advanced with EDR は、潜在的なセキュリティを検出、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、ノイズが低減するので、アナリストが誤検知や大量のアラートを追跡することに時間を費やす必要がなくなります。

人的リソースを追加せずに、専門知識を獲得

AI を活用して、脅威を自動的に検出、優先順位付け、調査： Intercept X Advanced with EDR は、機械学習を活用して、潜在的な脅威を自動的に検出し、優先順位を付けます。潜在的な悪意のあるファイルが検出された場合、ユーザーはディープラーニングによるマルウェア解析を活用して、ファイルの属性とコードを分析し、数百万ものファイルを比較をして、マルウェアの細部を自動的に解析します。

専門家のために設計されたすぐに使用可能なクエリ：セキュリティアナリストおよび IT 管理者は、ユースケース別に分類され、すぐに使用可能な SQL クエリを使用して、購入初日から Sophos EDR を使用できます。クエリは、カスタム検索用に簡単に編集したり、最初から作成したり、コミュニティから入手することができます。

本来アナリストによって提供されるスキルを再現することで、難しい質問に回答： 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。

脅威ハンティングと IT 運用のために構築

Sophos Intercept X Advanced は、IT 管理者およびセキュリティアナリスト向けに設計された初の EDR ソリューションです。これを使用することで、エンドポイントで過去に何が起こったのか、今何が起きているのかについて質問できます。脅威を探し出し、アクティブな敵対行為を検出、または IT 運用を活用して IT セキュリティの予防状態を維持します。問題を検出した際には、リモートで的確な対応します。これは、次の 2つの主要機能を活用することで実現されます。Live Discover と Live Response です。

Live Discover: 何でも質問 - Live Discover は、セキュリティアナリストと IT 管理者に、エンドポイントやサーバー全体で考えられるほとんどすべての質問に対する確認や、回答を提供します。IT 動作の問題を迅速に検出して IT セキュリティの予防状態を維持し、詳細な質問を行って疑わしいアクティビティを突き止めます。Live Discover では、すぐに使用できる強力な SQL クエリを使用しており、最大 90日間現在および過去のディスク上のデータを素早く検索できます。使用例は次のとおりです。

IT の動作

- なぜデバイスの動作が遅いのですか？再起動待ちですか？
- どのデバイスに既知の脆弱性、不明なサービス、または不正なブラウザ拡張機能がありますか？
- 削除すべきプログラムが実行されていませんか？
- リモート共有は有効になっていますか？デバイスに暗号化されていない SSH キーはありますか？ゲストアカウントは有効になっていますか？
- 特定のファイルのコピーがデバイス上にありますか？

脅威ハンティング

- 非標準ポートでネットワーク接続の確立を試みているのはどのプロセスですか?
- MITRE ATT&CK フレームワークにマッピングされている検出された IOC を一覧表示する
- ファイルまたはレジストリキーを最近変更したプロセスを表示する
- PowerShell の実行に関する詳細情報を検索する
- services.exe を装ったプロセスを特定する

Live Response: リモートで正確に対応 - 問題が検出されると Live Response は、ユーザーに組織全体のエンドポイントとサーバーへのコマンドラインのアクセスを提供します。デバイスにリモートアクセスして、さらに調査を実行したり、その他の問題を修正します。管理者は、デバイスの再起動、アクティブプロセスの終了、スクリプトの実行、構成ファイルの編集、ソフトウェアのインストール / アンインストール、フォレンジックツールの実行などを行うことができます。

Managed Detection and Response

Sophos MTR (Managed Threat Response) サービスとは、ソフォスの専門家チームが実施する脅威ハンティング、検出、対応を年中無休で提供するフルマネージド型サービスです。(ご注意、現時点では英語による対応となります。) 他社の Managed Detection and Response (MDR) サービスは、攻撃や疑わしいイベントを通知するだけですが、Sophos MTR を使用すると、脅威ハンターやレスポンスの専門家であるエキスパートチームがお客様に代わって最も洗練された脅威さえも中和し、組織を守ります。Sophos MTR を利用されるお客様は、Intercept X Advanced with EDR もご利用いただけます。

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	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

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

20-10-07 DS-JA (PC)