Sophos XDR

Intercept X Advanced with XDR、Intercept X Advanced for Server with XDR

Intercept X は、ネイティブのエンドポイント、サーバー、ファイアウォール、メール、クラウド、O365 セキュリティを同期する業界唯一の XDR ソリューションです。専用の SOC チームと IT 管理者ともに、脅威検出、調査、対応のための豊富なデータセットと詳細な分析を使用して、組織の環境の全体像を把握できます。

IT 運用や脅威ハンティングに関する質問に回答

ビジネスに不可欠な質問への回答を迅速に得られます。IT 管理者とサイバーセキュリティの専門家の両者は、日常で IT 運用と脅威ハンティングタスクを実行している際に、真の付加価値を見出せるでしょう。

最適な保護から始める

Intercept X は、侵害が開始される前にそれを阻止します。つまり、保護が強化され、自動的に阻止されるべきインシデントの調査時間を短縮できます。また、詳細な脅威インテリジェンスにアクセスして、情報に基づいた迅速なアクションを実行するために必要な情報を提供します。

対処する場所をすぐに特定

疑わしい検出や脆弱な構成の優先順位付きリストを参照して重要な問題に焦点を当ててください。このリストには、詳細な調査をするための情報が含まれています。事前に作成されたテンプレートのライブラリから選択して、さまざまな IT 運用および脅威ハンティングに関する質問を行ったり、またはご自身で作成できます。

最小限に抑えた調査時間と対応時間

AI ガイドの調査により、インシデントの範囲と原因をすばやく把握し、対応までの時間を最小限に抑えることができます。リアルタイムの状態、および最大 90日間の履歴データ、またはデータレイク内の 30日間の履歴データのデバイスにアクセスします。

製品間における可視性

Intercept X、Intercept X for Server、Sophos Firewall、Sophos Email、Sophos Mobile、Cloud Optix および Microsoft Office 365 データをネイティブに統合することで、組織の可視性を最大限に高めます。

マルチプラットフォーム、マルチ OS のサポート

Windows、macOS、Linux、Amazon Web Services、Microsoft Azure、Google Cloud Platform、および Oracle Cloud Infrastructure の展開全体で、クラウド、オンプレミス、または仮想のいずれの環境でも検査します。

主な特長

- ビジネスの重要な IT 運用や脅威ハンティングに関する質問に回答
- 検出と AI ガイドによる調査の優先リストを活用
- 対象のデバイスに対して、リモートで修正措置を実行
- 組織の IT 環境の全体像を把握し、必要に応じて詳細に調査
- ネイティブエンドポイント、サーバー、ファイアウォール、メール、クラウド、モバイルと O365 の統合
- 事前に作成され、カスタマイズ可能なテンプレートのユースケースのライブラリにアクセス

SOPHOS

使用例

IT 運用

- デバイスの動作が遅い理由は?
- 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るか?
- 削除すべきプログラムが実行されていないか?
- 管理されていないゲストおよび IoT デバイスを特定
- オフィスのネットワーク接続が遅いのはなぜか? 原因となっているアプリケーションはどれか?
- 紛失したデバイスや破壊されたデバイスでの異常なアクティビティを 30日間遡り確認
- パッチが適用されていない、もしくはソフトウェアが古いモバイルデバイスを検索

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か?
- 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
- 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
- デバイスをオンラインに戻すことなく調査を 30日間へ延長
- ファイアウォールから ATP や IPS 検出を使用して、疑わしいホストを調査
- メールヘッダー情報、SHA、その他の IoC を比較して、悪意のあるドメインへのトラフィックを特定
- 認証に複数回失敗したユーザを特定

含まれる機能

	XDR (Extended Detection and Response)
製品間のデータソース	✓
製品間の検出、調査、対応	✓
優先検出リストと AI ガイドによる調査	✓
Sophos Data Lake	✓
Data Lake の保持期間	30 日間
リアルタイムの状態の情報	✓
ディスク上のデータ保持期間	最大 90日間
脅威ハンティングと IT 運用テンプレートライブラリー	✓
Intercept X の保護機能	✓

ライセンスの詳細については、Intercept X および Intercept X for Server のライセンスガイドを参照してください。

無償評価版

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

ソフォス株式会社営業部
mail: partnersales@sophos.co.jp

22-01-06 DS-JA (MP)