Sophos SD ユースケース

Intercept X Advanced with XDR および
Intercept X Advanced for Server with XDR で利用可能

ビジネスに重要な IT 運用と脅威ハンティングの質問に答え、必要に応じて対処します。IT 管理者とサイバーセキュリティアナリストの両者が、強力な機能を活用できます。

IT セキュリティの運用と脅威ハンティングのタスクを実行

- 事前に作成され、自由にカスタマイズ可能なテンプレートのユースケースから選択
- 必要な情報を取得したら、迅速に対応
- エンドポイント、サーバー、ファイアウォール、メール、クラウドホスト、モバイル、O365 が対象

IT 運用のユースケース

IT 運用のユースケースは、IT 運用の予防状態を最高な状態にしておくのに優れています。ユースケースの例をいくつか紹介します。

デバイスのヘルスチェック

パフォーマンスの問題が発生しているデバイスを特定し、リモートでアクセスして、必要なアクションを実行します。

- 少ないディスク容量、利用率の高いメモリや CPU、または再起動を保留にしているデバイスの検索
- デバイスにリモートアクセスしてディスク領域を解放し、使用率の高い原因を調査し、必要に応じて再起動を実行

脆弱性

マルウェアや攻撃者によって悪用される可能性のある問題や脆弱性があるデバイスを検出します。

- ソフトウェアの脆弱性、実行されている不明なサービス、不正なブラウザ拡張機能があるデバイスを突き止め、共有または盗難されたアカウントの認証情報を検出
- デバイスにリモートアクセスして、パッチのインストール、不明なサービスの調査して終了、ブラウザ拡張機能をアンインストール、クラウドアカウントの認証情報をアップデート

不要なソフトウェア

コンプライアンスや生産性の問題を引き起こす可能性のあるソフトウェアを追跡します。

- Spotify、Steam、BitTorrent などの不要なプログラムを検索
- デバイスにリモートアクセスして、ソフトウェアをアンインストール

構成を管理

セキュリティリスクを引き起こす可能性のある設定に問題があるデバイスとクラウドワークロードを検索します。

- RDP および SSH が有効になっているサーバー、ネットワークポートが開いたままのクラウドセキュリティグループ、パブリッククラウドホスト、コンテナなどを監視およびインベントリ
- サーバーにリモートアクセスし、RDP/SSH を無効にしたり、オープンポートで待機しているサーバーを確認

コンプライアンス

オンプレミスとクラウド上のコンプライアンスの問題を特定し、対処します。

- 機密ファイルを検索し、AWS、Azure、GCP 環境の構成を評価
- デバイスにリモートアクセスして機密ファイルを削除し、CIS ベンチマークに対して安全なクラウド構築を確保

プロジェクトのロールアウト

IT プロジェクトがすべてのデバイスにロールアウトされているかどうかを確認します。

- ロールアウト全体の進捗状況を測定するために、ソフトウェアがデバイスに導入されているかどうかを確認
- デバイスにリモートアクセスして、導入が正常に行われるようにし、必要に応じて再起動して必要な変更を実施

SOPHOS

オフィスネットワークの問題（Sophos Firewall が必要）

オフィスサイト全体のネットワークの問題を確認して、修正します。

- オフィスのネットワークに問題がある場合、パフォーマンスが低下している原因を把握
- 問題の原因となっているアプリケーションを特定

デバイス管理（Sophos Firewall が必要）

組織の IT 環境内のデバイスを特定し、理解します。

- ノート PC、モバイル、IoT デバイスなどの管理対象外のデバイスや保護対象外のデバイスを確認
- 特殊な医療機器など、従来のデバイスや管理不可能なデバイスをさらに監視

予想外のことを予想する

30 日間のクラウドストレージでは、予期しないイベントに巻き込まれることはありません。

- 紛失し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
- デバイスが削除や破棄された場合でも、デバイスに起こったことを確認

脅威ハンティングのユースケース

掴みどころがない回避的な脅威を追跡し、すばやく駆除します。ユースケースの例をほんのいくつか紹介します。

ネットワーク攻撃

異常なネットワークアクセスを試みているプロセスを特定します。

- 非標準ポートで接続の確立を試みているプロセス、またはクラウドワークロードからの異常な送受信トラフィックを検出
- クラウドセキュリティグループを分析して、公共のインターネットに公開されているリソースを特定
- デバイス / ワークロードにリモートアクセスし、プロセスを終了してラテラルムーブメントの動作を確認

変更されたファイル

予期しない方法で変更された項目を検索します。

- 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特定
- デバイスにリモートアクセスし、変更を確認して処置を実行

難読化されたスクリプト

ファイルレスのメモリベースの攻撃は、一般的な攻撃ベクトルとなっています。

- 予期しない PowerShell 実行の詳細を調査
- デバイスにリモートアクセスし、追加のフォレンジックツールを実行して、疑わしいプロセスを終了

なりすましのプロセス

悪意のあるプロセスの中には、検出を避けるためになりすましを行うプロセスがあります。

- なりすましたプロセスを検出
- デバイスにリモートアクセスして、疑わしいプロセスを終了し、フォレンジックツールを実行

MITRE ATT&CK フレームワーク

MITRE ATT&CK フレームワークは、攻撃手法を識別するために一般的に使用されるテンプレートです。

- 独自のクエリ、またはソフォスのクエリを使用して、攻撃者が使用する攻撃戦術と手法を特定
- 識別手法に基づいて、潜在的なフォローアップ攻撃やダブルチェックする領域を調査する技術を向上

インシデントの範囲

インシデントの影響度と、影響を受けたデバイスとユーザーを把握します。

- フィッシングメールからリンクをクリックしたデバイスを特定
- フィッシングサイトからファイルをダウンロードしたデバイスを確認し、リモートアクセスしてクリーンアップを実行

SOPHOS

調査期間の延長

デバイスとリアルタイムの状態で 90日間のデータに加えて、30日間のクラウドデータを使用できます。

- デバイスをオンラインに戻すことなく、30日間のデータを調査
- 攻撃で無力化されたデバイスに何が起こったのかを確認

リッチネットワークデータの使用 (Sophos Firewall が必要)

ネットワークデータを脅威ハンティングと調査に取り込みます。

- クロスリファレンスが、より広範な攻撃を把握するために、他の IoC で悪意のあるトラフィックをブロック
- ファイアウォールから ATP や IPS 検出を使用して、疑わしいホストとデバイスを調査

リッチネットワークデータの使用 (Sophos Email が必要)

メール情報を組み合わせ、インフラ環境に関する詳細な情報を入手

- メールヘッダー情報を他の IoC と比較して、インシデントをよりよく把握
- 疑わしいファイルを特定し、デバイスや O365 メールボックスからすばやく削除

クラウドワークロード保護機能の強化

(Cloud Optix Advanced が必要)

同じコンソールからパブリッククラウドインシデントを検出して対応します。

- AWS CloudTrail へのシームレスな統合により、AWS クラウド環境 API、CLI、および管理コンソールのアクティビティを調査
- 攻撃者の戦術に関連するさまざまなクエリを使用：初期アクセス、永続性、権限の昇格、およびデータ窃取

Sophos XDR ヘッドの詳細については、Sophos.com/XDR を参照してください。

22-01-04 UC-JA (NP)