ソリューションの概説

Sophos NDR

ネットワーク深部の重要な可視性

Sophos Network Detection and Response は、Sophos MDR と Sophos XDR の両方で使用でき、エンドポイントやファイアウォールでは検出できないネットワークの深部にある悪意のあるネットワークアクティビティを検出します。Sophos NDR は、未知のデバイスや管理対象外のデバイスから発生する異常なアクティビティ、不正なアセット、新しいゼロデイ C2 サーバー、予期しないデータの移動など、不審なパターンがないかトラフィックを継続的に分析します。

ユースケース

1 | 重要な可視性

期待される結果：他の製品では確認できないネットワークアクティビティの重要な可視性を得る

対策：Sophos NDR は、管理下のエンドポイントおよびファイアウォールと連携して、エンドポイントやファイアウォールが確認できない疑わしいパターンや悪意のあるパターンがないかどうかネットワークアクティビティを監視します。管理対象外のシステムや IoT デバイスからの異常なトラフィックフロー、不正なアセット、インサイダー脅威、これまで検知されなかったゼロデイ攻撃、ネットワークの奥深くにある異常なパターンを検出します。

2 | 早期検出

期待される結果：5つの独立した検出エンジンがリアルタイムで動作し、脅威を迅速に特定

対策：Sophos NDR には、ディープラーニング、ディープ パケット インスペクション、暗号化されたペイロード分析、ドメイン名分析、強力な分析などのテクノロジーを使用して、疑わしいトラフィックや悪意のあるトラフィックをリアルタイムで検出する 5つの独立した検出エンジンが含まれています。過剰なノイズを探し回らないように、ソフォス独自の分析で価値の高いアラートのみを提供します。

3 | 自動対応

期待される結果：アクティブな攻撃者や脅威をその場で自動的に阻止

対策：Sophos NDR、Sophos XDR、Sophos MDR、Sophos Firewall 間のソフォスの製品間の自動化により、アクティブな脅威をその場で阻止する迅速な対応が可能になります。Sophos NDR が感染の痕跡、アクティブな脅威、または攻撃者を特定すると、アナリストは直ちにアラートを受け、脅威フィードを Sophos Firewall に即座にプッシュして、自動対応をトリガーし、侵害されたホストを隔離できます。

4 | 単一のコンソールで管理

期待される結果：最小限の時間でネットワークセキュリティを管理

対策：Sophos Central では、NDR、XDR、エンドポイント、ファイアウォールなど、すべてのソフォス製品に対して単一のクラウド管理プラットフォームを使用できます。ソフォスのデータレイクを活用した豊富で強力なツールを利用して、製品間の脅威ハンティング、早期対応の管理、レポートと監査を行います。これにより、ネットワークセキュリティの管理に費やす時間が短縮されます。

保護されていないアセットや不正なアセットを特定

異常なデータ移動と内部脅威の明確化

未知の新しいゼロデイ攻撃の検出

詳細と無償評価
Sophos NDR

sophos.com/ndr

2023-11-06 DS-JA (MP)

SOPHOS