ソリューション概要

Sophos ITDR

アイデンティティ脅威の検知と対応

Sophos Identity Threat Detection and Response (ITDR) は、従来のアイデンティティセキュリティ制御を回避する脅威を検知して対応するためのソリューションです。Sophos ITDR は、Sophos XDR と Sophos MDR と完全に統合され、セキュリティポスチャを改善します。また、環境内のアイデンティティリスクや設定ミスを継続的に監視し、漏洩した認証情報に関するダークウェブのインテリジェンスも提供します。

ユースケース

1 | アイデンティティの脅威への対策

期待される成果：ビジネスに影響が及ぶ前にアイデンティティベースの攻撃を無力化

対策：90% の組織が過去 1 年間にアイデンティティの侵害を経験しています。[1] Sophos ITDR は、影響が生じる前に高度な脅威を特定し、攻撃の初期段階で MITRE ATT&CK の認証情報アクセス手法 [2] の 100% を防ぎ、迅速かつ正確に対応することを可能にします。経験豊富な Sophos MDR のアナリストが、リスクの高いアクティビティを調査し、ユーザーの無効化、パスワードリセットの強制、アカウントロック、セッションの強制終了などの対応をお客様に代わって瞬時に実行します。

2 | アイデンティティのアタックサーフェスを縮小

期待される成果：設定ミスや、アイデンティティに関するセキュリティギャップを特定して修正します。

対策：Microsoft Entra ID 環境の 95% に重大な設定ミスが存在しています。[3] これらの問題を放置すると、サイバー犯罪者はこれらの弱点を悪用して権限を昇格して、アイデンティティを標的とした攻撃を実行する可能性があります。Sophos ITDR は、Entra ID 環境を継続的にスキャンし、設定ミスやセキュリティギャップを迅速に特定して、修正に役立つ推奨事項を提供します。

3 | 漏洩または窃取された認証情報の発見

期待される成果：漏洩した認証情報が攻撃に悪用されるリスクを最小限に抑えます。

対策：アイデンティティは、ランサムウェアによる侵入経路の中でも依然として主要な手段の 1 つです。ソフォスの調査では、ダークウェブ最大級のマーケットプレイスで販売されている窃取された認証情報の数は、過去 1 年間で倍増しています。[4] Sophos ITDR は、ダークウェブやデータベースで漏洩した認証情報を継続的に監視し、認証情報が漏洩した際にアラートを発行し、攻撃で悪用されるリスクを低減します。

4 | リスクの高いユーザーの動作の特定

期待される成果：リスクの高いユーザーの動作を把握して対処することで、企業を守ります。

対策：通常とは異なるログインパターンや攻撃が疑われるユーザーアクティビティを監視することで、サイバーセキュリティリスクを大幅に軽減し、重要な資産を保護します。Sophos ITDR は、悪意のある攻撃である可能性のあるリスクの高い行動や、ユーザーの認証情報が漏洩している可能性を示す行動を特定し、ソフォスのセキュリティアラートで特定された組織のユーザーの詳細を提供します。

Gartner Peer Insights Customers' Choice 2025

EDR (Extended Detection and Response) 部門で、2025 年 Gartner® Peer Insights ™ Customers' Choice を獲得。

MDR および XDR 部門の G2 Overall Grid® Reports でリーダーに選出 (顧客による評価とレビュー)。

MITRE | ATT&CK® Evaluations

エンタープライズ製品部門およびマネージドサービス部門の MITRE ATT&CK® 評価で優れた成績を獲得。

詳細情報：
Sophos.com/ITDR

[1] 2024 年の Identity Defined Security Alliance (IDSA) による調査。| [2] MITRE ATT&CK フレームワークにマッピングされたソフォスの検知機能に基づく
[3] ソフォスが実施した数千件のインシデント対応で収集されたデータ。| [4] Sophos X-Ops Counter Threat Unit (CTU) のデータ、2024 年 6 月から 2025 年 6 月。

Gartner Peer Insights ™ 'Voice of the Customer' : Extended Detection and Response, Peer Contributors (2025 年 5 月 23 日)Gartner Peer Insights のコンテンツは、個々のエンドユーザー自身の経験による主観的な意見が集約されたものであり、Gartner またはその関連会社の見解を表すものではありません。Gartner は、商品性または特定目的への適合性の保証を含む、その正確性または完全性について、本コンテンツの内容に関する一切の責任を、明示または黙示を問わず負うものではありません。GARTNER は、米国内外における Gartner, Inc. および / またはその関連会社の登録商標およびサービスマークであり、PEER INSIGHTS は Gartner, Inc. および / またはその関連会社の登録商標で、Gartner, Inc. の許可を得て使用されています。All rights reserved.

2025-09-16 SB-JP (MP)