SOPHOS
Cybersecurity delivered.

MDR サービスを利用する 5つの理由

ソフォス ホワイトペーパー2022年 9月

はじめに

サイバー脅威の数、複雑さ、影響力が増すにつれて、組織は、テクノロジーソリューションのみでは防ぐことができない高度な脅威を検出して無力化する MDR (Managed Detection and Response) サービスをますます利用するようになっています。実際、Gartner 社では、2025年までに、50% の企業が脅威の監視、検出、および対応に MDR を使用すると予測しています[1]。

しかし、市場での防衛ソリューションの急増により、MDR とは正確に何か、MDR が広範なサイバーセキュリティエコシステムにどのように適合するか、MDR サービスを使用する利点は何か、などを理解することが難しくなっています。このガイドでは、これらの質問に回答し、MDR サービスを選択する際に考慮すべき点について実用的なガイダンスを提供します。

Sophos MDR

Sophos MDR は、世界で最も信頼されている MDR サービスであり、ランサムウェアを含む最先端の脅威から 11,000[2] 社を超える組織を保護しています。Gartner Peer Insights™[3] で最高の評価を獲得し、2022 G2 Grid® で中規模市場[4] 向け MDR サービスのトップベンダーの認定を受けており、Sophos MDR はお客様のサイバー防御の保護に適しています。

MDR の定義

MDR の利点と、MDR サービスに対する需要の拡大の背景を理解するためには、MDR とは何か、そして、そうでないものは何かを理解することが重要です。

MDR (Managed detection and response) サービスとは、テクノロジーソリューションだけでは防ぐことができないサイバー攻撃の検出と対応を専門とする専門家が 24時間年中無休体制で提供する完全に管理されたサービスです。

MDR を、EDR (Endpoint Detection and Response) や XDR (Extended Detection and Response) と混同しないようにしましょう。MDR、EDR、XDR はすべて脅威ハンティングをサポートし、可能にしますが、EDR と XDR はアナリストが潜在的な侵害を探し、調査できるようにするツールです。MDR は、セキュリティベンダーのアナリストがお客様に代わって脅威を探し、調査して無力化します。

名前が示すように、EDR ツールはエンドポイント保護テクノロジーのデータポイントと連動し、XDR ツールはデータソースを幅広い IT スタック (ファイアウォール、メール、クラウド、およびモバイルセキュリティソリューションなど) に拡張して、より優れた可視性と洞察を提供します。ソフォスでは、MDR サービスを提供する際に、業界をリードする EDR と XDR のソリューションを活用しました。

MDR が行わないことは、セキュリティ技術の導入、ポリシーの更新、パッチの適用、アップデートのインストールなど、日常的なサイバーセキュリティの管理です。MSP (マネージド サービス プロバイダ) は、この分野のサポートを求めている組織に対して、IT セキュリティ管理サービスを提供します。

MDR サービスの対象者

IT リソースが限られている小規模企業から社内に SOC グループを持つ大業まで、あらゆる業種のあらゆるタイプの組織が MDR サービスを活用しています。問題は、MDR サービスをどのように利用しているかということです。MDR レスポンスモデルには、主に次の 3つがあります。

- MDR チームはお客様に代わって脅威対応を完全管理
- MDR チームは社内チームと協力して脅威への対応を管理
- MDR チームは社内チームに警告を送信し、改善のガイダンスを提供

ソフォスでは、この 3つのアプローチすべてをサポートし、必要に応じて個々のお客様の要件に対応します。

1 Gartner Market Guide for MDR 2021
2 2022年 8月現在。
3 2022年 8月 1日現在の過去 12ヶ月間のレビューです。Gartner Peer Insights のコンテンツは、プラットフォームに掲載されているベンダーとの独自の経験に基づいた個々のエンドユーザーの意見で構成されており、事実を示すものではありません。また、Gartner やその関連会社の見解を表すものでもありません。Gartner は、本コンテンツに記載されているベンダー、製品、サービスを保証するものではなく、本コンテンツに関して、商品性や特定目的への適合性を含む正確性または完全性について、明示的または黙示的に保証するものでもありません。
4 ソフォスは、2022 G2 Grid® で中規模市場向け MDR サービスでトップベンダーと評価されています。

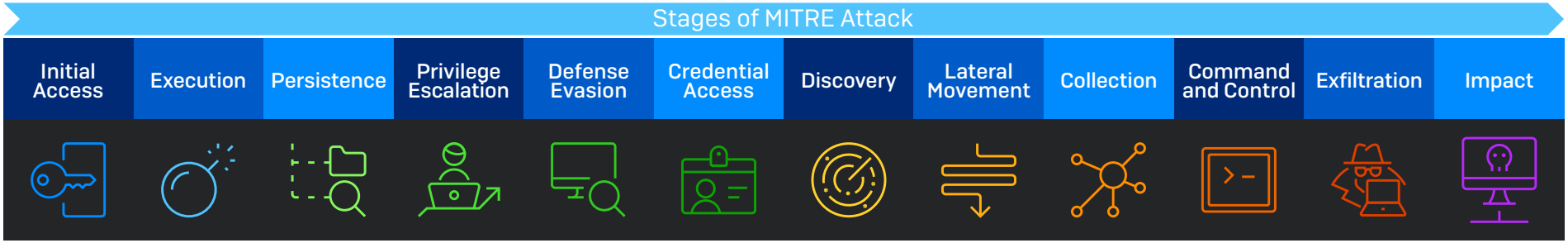
人間主導型の脅威検出と対応の必要性

現実には、技術的なソリューションだけではすべてのサイバー攻撃を防ぐことはできません。サイバーセキュリティソリューションによる検出を回避するために、悪意のある攻撃者は、正規の IT ツールを使用して、盗んだ認証情報やアクセス許可を悪用し、パッチが適用されていない脆弱性を利用して攻撃を実行することが多くなっています。悪意のある攻撃者は、権限を持つユーザーをエミュレートし、組織の防御の弱点を利用することで、自動検出テクノロジーのトリガーを回避することができます。

下の図は、2021年にソフォスの最前線の脅威ハンターによって確認された、MITRE ATT&CK チェーンの各ステージで攻撃者が使用する上位のアーティファクト (ツール) の詳細を示しています。ご覧のとおり、PowerShell、PsExec、RDP などの IT チームが日常的に使用するツールは、攻撃者によって頻繁に悪用されています。自動化されたテクノロジーでは、これらのツールを使用している正当な IT スタッフと、盗んだ認証情報を使用して不正利用を行っている攻撃者を区別するのに苦慮しています。

このような高度な「環境寄生型」攻撃を阻止するには、テクノロジーと人間の専門知識を組み合わせる必要があります。攻撃者がアクションを実行するたびに、信号が生成されます。人間の専門知識に強力な保護テクノロジーと AI を活用した機械学習モデルを組み合わせることで、セキュリティアナリストは、人間主導型の最も高度な攻撃を検出、調査、無力化して、データ侵害を防ぐことができます。

脅威のハンティング、調査、対応は、EDR や XDR ツールを使用して社内でのみ実行できますが、社内チームと一緒に、もしくは完全にアウトソースされたサービスとして MDR サービスを使用することは、さまざまな利点があります。



Artifacts

Remote Services	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	Network Browsing	Cobalt Strike	Rclone	Data Encrypted
Exploits	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Network Breach

Mitre attack チェーンの各ステージで使用される上位のアーティファクトです。Active Adversary Playbook 2022、ソフォス

今日の防衛において引き続き重要な役割を果たす保護テクノロジー

人間主導の MDR (Managed Detection and Response) はサイバーセキュリティの不可欠なレイヤーですが、高品質の保護テクノロジーは引き続き重要です。エンドポイント、ネットワーク、メール、およびクラウドのセキュリティテクノロジーは、今日の防御において引き続き重要な役割を果たしています。適切なソリューションにより、次のよう MDR サービスの有効性と影響力を高めることができます。

- 攻撃者が自動化、AI、マルウェア・アズ・ア・サービスを活用して脅威を増殖させる中、自動化された保護テクノロジーにより、防御者は増え続ける攻撃の先手を打つことができます。Sophos Endpoint Protection は、脅威が組織に影響を与える前に、99.98% の脅威を自動的にブロックします。
- 脅威ハンターの実用上の最大の課題の1つはノイズです。非常に多くの信号を受け取るため、木を見て森を見ずの状況になる場合があります。優れた防御テクノロジーにより、人間のアナリストが調査する必要のある警告の数を削減できます。脅威ハンターがより少ない数で、より正確な検出に集中できるようにすることで、高品質の防御テクノロジーが人間主導の脅威への対応を加速させます。
- 人間のアナリストは、保護テクノロジーからの検出とシグナルを使用して、疑わしいアクティビティを特定し、調査します。検出の頻出が向上し、コンテキストに関する洞察が高くなればなるほど、調査や対応が迅速かつ適切になります。

それを念頭に置いて、MDR サービスを利用することで得られる利点の上位 5つを見てみましょう。

1. サイバー攻撃に対する防御の強化

社内専用のセキュリティ運用プログラムよりも MDR プロバイダーを使用する主な利点の1つとしては、ランサムウェアやその他の高度なサイバー脅威に対する保護が強化されていることです。

MDR を使用すると、プロバイダーのアナリストの幅広い経験と深い知識を活用することができます。MDR ベンダーは、個々の組織よりもはるかに大量かつ多様な攻撃を経験するため、社内で再現するのはほとんど不可能なレベルの専門知識を提供します。

また、MDR チームは毎日インシデントを調査して対応するため、脅威ハンティングツールの使用において熟知しています。これにより、重要なシグナルの特定から、潜在的なインシデントの調査、悪意のあるアクティビティの無力化まで、プロセスのすべての段階でより迅速かつ正確に対応することができます。

また、大規模なチームの一員としては働くことで、アナリストの知識や洞察を共有し、対応をさらに加速化させることができます。Sophos MDR チームは、遭遇する脅威や特殊な攻撃者ごとにランブックを照合します。調査の過程で攻撃者を特定した場合、攻撃時に広範な調査を行う必要がなくなり、チームはランブックを参照して、すぐに行動に移ることができます。

ランブックは継続的に更新され、アナリストは次のようなすべてのエンゲージメントについて需要な情報を記録します。

- 特定の攻撃や脅威アクターに共通または特有した TTP (戦術、手法、手順)。
- 関連する IoC (感染の痕跡)。
- 公開された脆弱性に関するエクスプロイトの既知の概念実証 (PoC)。
- 特定の攻撃や脅威アクターに対処する際に役立つ脅威ハンティングクエリ。

MDR サービスのもう 1つの利点は、ある顧客からの情報を同じターゲットプロファイルに一致する他の顧客に適用することで、そのコミュニティで類似した攻撃を未然に防止できます。Sophos MDR チームがお客様の組織全体を事前調査するシナリオの例としては、以下のようなものがあります。

- 特定の業種に属するお客様が、特定の方法で標的にされている。
- Sophos X-Ops が、特定の業界や組織のプロファイルを標的とした重大な攻撃に関する情報を提供する。
- セキュリティ環境で重大なイベントが発生し、お客様が影響を受けていないか確認を希望する。

万が一、アナリストが不審なシグナルを検出した場合、迅速に調査と修正を行い、対象となるグループにコミュニティの免疫を作り出します。

Sophos MDR チームは、幅広い豊富な経験と、お客様の環境全体に学習した内容を適用する能力によって、組織の防御力を自社で達成できるレベル以上に高めることができます。

「Sophos MDR の具体的な成果としては、調査が必要な高リスクの脅威の検出にかかる時間を 90% 短縮、攻撃元と脅威の種類の特定にかかる時間を 95% 短縮し、検出の制度を向上させることができました」
インド、Chitale Dairy 社

「ペンテスターは、脆弱性が見つからなかったことに感動していました。その時に、ソフォスのサービスは絶対に信頼できると確信しました。」
オーストラリア、サザンクイーンズランド大学

「Sophos MDR のおかげで、脅威への対応時間が大幅に短縮されました。」
インド、Tata BlueScope Steel 社

「リアルタイムで脅威の通知を受信します。」
イタリア、Bardiani Valvole 社

2. IT の作業能力の向上

脅威ハンティングは時間がかかり、予測不可能です。複数の作業と優先順位を処理している IT 専門家にとって、課題に取り組むことは困難なことです。IT チームの 79% は、ログを確認して疑わしいシグナルやアクティビティの特定をすることが完全にできていないことを認めています[5]。

攻撃が組織に与える潜在的な影響を考えると、何か疑わしいものが検出されたら、すぐに脅威を調査して対処できるようにすべてを中断する必要があります。作業の緊急性により、チームはより戦略的で、より興味深い課題に集中することができなくなります。

MDR サービスを使用することで、IT の作業能力が向上し、ビジネスに重点を置いた戦略を実施することができます。Sophos MDR を使用している組織では、ソフォスのサービスを使用することで IT の効率が大幅に向上し、組織の目標を適切にサポートできるようになったことを一貫して報告しています。

「ソフォスを導入して以来、運用時間を大幅に短縮することができたため、学生の満足度を高める取り組みに注力できるようになりました。」
英国、ロンドン・サウスバンク大学

「Sophos MDR は脅威を迅速に修正または削除し、注意を喚起することができるたえ、価値の高い作業に集中することができます。」
オーストラリア、Tomago Aluminium 社

「Sophos MDR があるからこそ、脆弱性管理、パッチ適用、セキュリティ意識向上など、組織の他の分野を強化し、しっかりさせることができます。」
米国、The Fresh Market 社

「ソフォスは最新のアクティビティや脅威を常に把握しているので、お客様やアーティストに安全かつ世界最高レベルのサービスを提供することに専念できます。」
米国、CD Baby 社

5 2022年 1月と 2月に、IT プロフェッショナル 5,600人を対象に独立調査を実施。ソフォスの委託により、Vanson Bourne が実施しました。

3. 24時間体制による安心感

悪意のある攻撃者は世界中の至る所に存在するため、攻撃はいつでも発生する可能性があります。攻撃者は、IT チームがオンラインである可能性が最も低い時間帯である夜間、週末、休日に最も活動的になります。したがって、脅威検出と対応は 24時間体制で行わなければならず、営業時間内だけでの対応では組織が危険にさらされた状態になります。

MDR サービスは、24時間体制のサポートにより、心の平穏と安心感を提供します。IT チームにとって、このことは言葉通り、夜の睡眠が改善されることを意味します。そして、MDR プロバイダーが責任を持つことで安心でき、個人の時間を取り戻すことができます。

管理職やお客様にとって、24時間年中無休の専門家による対応と常に高いレベルのサイバーレディネスが提供されることは、データと組織そのものが十分に保護されているという強い安心感をもたらします。

「Sophos MDR チームが、24時間年中無休で保護してくれているため、安心して眠ることができます。」
カナダ、Vancouver Canucks

「ソフォスチームはゴールキーパーのような役割を果たし、そのスキルで私たちの後ろに立って、サポートしてくれているという安心感を与えてくれます。」
英国、Inspire Education Group

「今では、セキュリティ設定の信頼性、堅牢性、包括的な性質に対する信頼が向上しました。」
インド、Aligned Automation

「Sophos MDR により、業務の耐障害性が大幅に向上しました。」
オーストラリア、McKenzie Aged Care Group

4. 人員を増やすことなく、専門知識を獲得

脅威ハンティングの操作は非常に複雑です。この分野の各担当者は、特殊でニッチなスキルが必要であり、脅威ハンターに求められる典型的な特性は次のとおりです。

- **創造的で好奇心旺盛** – 脅威を探すことは、針穴に糸を通すような作業と似ています。脅威ハンターは、脅威を発見するためにさまざまな方法を駆使して、何日もかけて脅威を探すことがよくあります。
- **サイバーセキュリティの経験** – 脅威ハンティングはサイバーセキュリティの中でも最も高度な業務の 1つです。そのため、これまでの現場での経験や基礎知識は必須となります。
- **脅威の状況に関する知識** – 未知の脅威を探し出し、無力化するためには、最新の脅威の傾向を理解することが不可欠です。
- **攻撃側の思考** – ハッカーのように考える思考力が、今日の人間主導のアプローチに対抗するには重要となります。
- **テクニカルライティング能力** – 脅威ハンターは、調査プロセスの一環として、発見事項を記録する必要があります。そのため、このような複雑な情報を伝える能力は、ハンティングを最後まで追跡する上で非常に重要です。
- **OS とネットワークに関する知識** – 両方の高度な実務知識が不可欠です。
- **コーディング / スクリプトの経験** – これは、脅威ハンターがプログラムの構築、タスクの自動化、ログの解析、データ分析タスクの実行と調査を支援および進行する際に必要です。

このリストは、IT 部門でのスキル不足が原因で、多くの組織にとって脅威ハンティングの専門知識を採用することが困難な (不可能ではないにしても) 作業になっている、稀なコンピテンシーの組み合わせを表しています。

MDR サービスは、お客様に専門知識を提供します。ソフォスには、世界中のお客様に継続的な MDR サービスを提供する数百名の専門のアナリストがいます。Sophos MDR を使用すると、人員を増やすことなく、セキュリティ運用機能を拡張できます。

「これで、社内で独自の機能を構築することなく、既存のセキュリティプラクティスを拡張できるようになりました。」
オーストラリア、Hammondcare

「Sophos MDR のおかげで、セキュリティ運用チームを増員することなく、増大する量と高度化するサイバー脅威に対応することができました。」
インド、Tourism Finance Corporation of India Limited

「ソフォスのおかげで、この業務を担当するための新しい人員、最大 5名の採用コストを節約できました。」
英国、AG Barr

5. サイバーセキュリティ ROI の向上

24時間年中無休体制の脅威ハンティングチームを維持するのはコストかかります。24時間体制で対応するには、少なくとも 5〜6人のサイバーセキュリティスタッフが別々のシフトで働く必要があります。スケールメリットを活用することで、MDR サービスは組織を保護し、サイバーセキュリティの予算をさらに拡大するための費用対効果の高い方法を提供します。

さらに、MDR サービスは、保護を強化することで、コストのかかるデータ侵害の発生のリスクを大幅に軽減し、重大なインシデントに対処するための経済的な問題を回避します。中規模の組織におけるランサムウェア攻撃の修復平均コストが、2021年[6]には 140万ドルに達したことを考えると、予防に投資することは賢明な財務判断であると言えます。

エンドポイントやその他のサイバーセキュリティ製品も提供している MDR ベンダーを利用する場合、単一のプロバイダーとの統合とベンダー管理作業の合理化により、かなりの TCO のメリットを享受できます。

最後に、現在使用しているセキュリティテクノロジーと統合するベンダーを選択することで、既存の投資から利益を高めることができます。ソフォスでは、ベンダーに依存しない MDR へのアプローチを採用しており、既存の製品を活用して脅威の検出、調査、対応を行い、ROI を向上させることができます。Sophos MDR では、ソフォスの世界トップクラスのツール、ソフォス以外のツール、またはこれらの 2つの組み合わせを使用できます。

「ソフォスは、6人のフルタイムスタッフと同等の対応と作業量を 1人以下のコストで提供してくれます。」
オーストラリア、Detmold Group

「すべてのセキュリティ製品を 1ヵ所にまとめることで、コストを削減し、効率を高めることもできました。」
英国、Independent Parliamentary Standards Authority

「Sophos MDR は、確実に採算が取れます。1年に 1件の重大なインシデントを阻止できれば、少なくとも 10倍以上の元が取れたことになります。」
オーストラリア、Hammondcare

「1週間に 15時間節約でき、生産性が 2.6倍向上しました。」
インド、Tourism Finance Corporation of India Limited

6 ランサムウェアの現状 2022年版、ソフォス31ヶ国 5,600 人の IT 専門家を対象とした独立調査

MDR サービスを選択する際に考慮すべき点

MDR サービスは、プロバイダーごとに異なります。サービスを評価する際に考慮すべき点は多数ありますが、次の 4つの分野を必ず確認してください。

1. **提供されるサポートレベルとやり取りレベル**

   MDR ベンダーに脅威への対応を完全に管理してもらいたいですか？チームと共同で脅威対応を管理したいですか？または、チームに警告を送信してアクションを実行したいと考えていますか？お客様が希望するサポートレベルとやり取りレベルを確認し、ベンダーがどのような状況にあるかを確認してください。

   ソフォスでは、お客様の IT チームの延長としての役割を果たし、お客様が必要とする能力を提供します。完全に管理された 24時間年中無休体制のサポートから、社内チームの指揮まで、お客様のご希望に合わせて対応します。

2. **脅威における幅広い豊富な経験**

   サイバー脅威への対応をより広く、より深く経験することが、より優れた防御につながります。ベンダーの MDR アナリストがアクセスできる経験の規模、およびお客様の組織全体でどのようにして全体的な学習内容を適用するか理解します。

   また、ベンダーの MDR チームの背後にあるセキュリティに関する専門知識の深さや、アナリストが警告の優先順位を付けて調査を行う際に役立つコンテキストの情報の質についても確認します。

   Sophos MDR は、医療、教育、製造、小売、テクノロジー、金融、政府、サービスなど、さまざまな業界で活躍する世界中の 11,000 社以上の組織のセキュリティを保護しています。この幅広い豊富な経験により、お客様に比類のない保護を提供することができます。

   Sophos MDR の背後には、Sophos X-Ops チームがいます。Sophos X-Ops は、30年以上にわたるマルウェアの専門知識と業界をリードする AI 機能を備えており、深い洞察と解析を提供することで、MDR エージェントが攻撃を迅速に特定して無力化できるように支援します。

3. **日々のお客様の体験**

   効果的な MDR ベンダーは、お客様のチームの延長線上にあります。契約を締結する際に、連携したいベンダーであることを確認してください。既存のお客様に話を聞いて体験を理解したり、独立調査会社のレビューサイトでお客様からのフィードバックを確認してください。

   Sophos MDR は、2022年 8月 1日現在、Gartner Peer Insights で最もレビュー数が多く、平均評価 4.8/5* の高評価を得ている MDR プロバイダーです。お客様の声 (英語) はこちらをお読みください。

4. **テレメトリの広さと深さ**

   攻撃者は、単一のテクノロジーパスをたどることはありません。MDR ベンダーの脅威ハンティングも同様です。アナリストの可視性が環境全体で高まるほど、アナリストは悪意のあるアクティビティをより適切に検出して対応できます。ベンダーに、セキュリティの統合について、また IT 環境全体からどの程度幅広く信号を統合できるかを確認してください。

   Sophos MDR は、エンドポイント、ネットワーク、クラウド、メール、および Microsoft 365 テクノロジーとのネイティブおよびサードパーティ製品との統合を含む、完全な IT スタック全体に広範な統合を提供します。ソフォスのベンダーに依存しないアプローチにより、アナリストはお客様の環境全体を幅広く可視化でき、脅威の検出、調査、および対応が向上します。

まとめ

サイバー脅威が進化し続ける中、MDR はあらゆる規模の組織にとって急速に必須の保護となりつつあります。信頼と実績のある MDR ベンダーと連携することで、脅威ハンティングを完全にアウトソースする場合でも、社内サービスを補完して強化する場合でも、次のようなメリットが得られます。

1. サイバー攻撃に対する防御を強化する
2. IT の作業能力を向上させる
3. 24時間体制による安心感を得られる
4. 人員を増やすことなく、専門知識を獲得する
5. サイバーセキュリティ ROI が向上する

Sophos MDR の詳細については、ソフォスのパートナーにお問い合わせいただくか、www.sophos.com/mdr をご覧ください。

www.sophos.com/mdr

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2022-09-16 JA-WP (DD)

SOPHOS