Phil Muncaster

2022 年 11 月

マネージドサービス型 EDR/XDR ソリューション MDR (MANAGED DETECTION AND RESPONSE) 選定ガイド

MDR とは何か？
MDR が今求められている理由とは？

Digital Security
Progress. Protected.

目次

概要

企業のサイバーリスク環境は急速に進化しています。新型コロナウイルスのパンデミックによって、さまざまな技術分野へ投資が進んだことで、攻撃対象領域も大幅に拡大しました。クラウドシステム、リモートの在宅勤務者、リモートアクセスのためのインフラストラクチャ、エンドポイントの分散化、複雑なサプライチェーンは、サイバー犯罪者にとって大規模で格好の標的になっています。また、サイバー犯罪者のための地下マーケットでも、独自の複雑なサプライチェーン、サービスとしてのマルウェア、TTP（戦術 / 技術 / 手順）の技術が進化しており、専門化が進んでいます。

このような背景から、脅威の予防に取り組むことは依然として重要ですが、攻撃を常に防ぐことは困難になっています。そのため、企業はセキュリティ防御を、予防、検出、対応を中心とする総合的なアプローチに進化させなければならなくなっています。このような包括的なアプローチによって、サイバー犯罪者によってシステムに侵入され深刻な損害を受けることが防ぐことが可能になります。予防の段階でネットワークへの侵入を防ぐことができなかった場合でも、検出と対応機能によって不審なイベントを特定でき、ネットワークの深部に侵入され脅威の影響が大きくなる前に解決できます。

しかし、企業はどのような検出と対応ツールを選べばよいのでしょうか？ XDR（Extended Detection and Response）は有用なツールですが、膨大なアラートが生成されるため業務が圧迫されることもあり、XDR の運用に必要な担当者を採用するために資金を調達しなければならないなど、別の課題が生じる場合もあります。

MDR (Managed Detection and Response) とは、ツール、テクノロジー、サイバーセキュリティの専門家が三位一体となって、強力な検出・対応能力を提供するマネージド型のセキュリティサービスです。MDR を適切に導入すれば、サイバーリスクをより効果的に管理できます。しかし、最も肝要なのはどのベンダーの MDR サービスを利用するかです。

高品質の脅威インテリジェンスとテクノロジーを提供し、高い検出率、低い誤検出率、軽量なフットプリントを実現している実績のあるプロバイダを選ばなければなりません。顧客サービスの充実度や、組織固有のニーズに合わせて MDR をどの程度まで最適化できるかも重要なポイントです。

XDR の仕組み

XDR は、EDR が進化したものであり、脅威の検出、調査、対応、ハンティングをリアルタイムで最適化します。XDR は、セキュリティエンドポイント製品による脅威検出と、ネットワーク分析と可視化（NAV）、メールセキュリティ、IAM（アイデンティティとアクセス管理）、クラウドセキュリティなどのセキュリティおよびビジネスツールのテレメトリ（監視データ）と統合します。ビッグデータインフラストラクチャを基盤に構築されたクラウドネイティブプラットフォームであり、セキュリティチームはこのプラットフォームを柔軟に活用できます。また、拡張性に優れ、セキュリティオペレーションを自動化することが可能です。

出典：Forrester、2021 年

現在の課題

サイバー攻撃者と防御側の熾烈な戦いが続いていますが、現在はサイバー攻撃者側がすべてのカードを持っているように思えることがあります。サイバー犯罪者を支援している地下マーケットの規模は年間数兆円規模に達しており、攻撃を容易に行うために必要なすべてのツール、ナレッジ、データを提供しています。これらのサイバー犯罪者は敵対国家に匿われていることも多く、法執行機関の捜査の手を恐れることなく攻撃を仕掛けているケースがあります。さらに、サイバー攻撃のための SaaS サービスが登場し、サイバー攻撃の民主化が始まっており、技術的な知識に乏しい組織であっても、大規模なキャンペーンを実行できるようになっています。

一方、最高情報セキュリティ責任者（CISO）とそのチームは、社内の多くの課題に応えなければならなくなっています。新型コロナウイルスのパンデミック時にはデジタルトランスフォーメーションへの投資が進み、サイバー攻撃対象領域が大幅に拡大しました。**リモートワーク環境**では、可視化と管理が行き届かなくなり危険な状況が生じています。エンドポイントにパッチが適用されない場合や、注意散漫なユーザーや、ミスを犯すユーザーもいます。多くのセキュリティチームは人員不足に陥っており、効率性に乏しい多くの個別最適のソリューションを扱っており膨大な業務量に圧迫されています。多くのソリューションがバラバラに導入されていることから、セキュリティ環境が複雑化しており、生産性も低下しています。

深刻なセキュリティ侵害が発生した場合に被る経済的および風評的な損害も、かつてないほど深刻になっています。しかし、このようなインシデントに関連するリスクを効果的に軽減する組織の能力は、むしろ低下しているのが現状です。データが侵害された場合に企業が負担するコスト（全世界平均）は、過去最高額に達しており、2021 年には 420 万米ドル以上になりました。また、世界的な保険会社によると、2021 年にサイバー攻撃を受けた米国と欧州の企業の 5 分の 1 が破産の危機に陥っていました。

このような背景から、**100% のサイバー攻撃を予防することはもはや現実的ではありません**。確固たる目的を持つ攻撃者は常に、標的の脆弱な領域を特定し、セキュリティを侵害する方法を見つけ出します。そのため、検出と対応の能力を強化してセキュリティ対策を補完することに注力する必要があります。しかし、この領域でも組織は攻撃者に後れをとっています。2021 年にセキュリティ侵害を特定して封じ込めるために要した全世界の組織の平均日数は 287 日でした。

XDR は、エンドポイント、ネットワーク、クラウド、メールなどの複数のセキュリティ階層で攻撃者による行動を分析、攻撃が疑われる活動を発見して、攻撃者による影響を組織が受ける前に阻止します。

MDR は、XDR（eXtended Detection and Response）をアウトソーシングしたサービスと考えることができます。MDR は他のツールと組み合わされて利用される場合もあります。

多くの企業が、ツール、テクノロジー、サイバーセキュリティの専門家を統合したマネージドセキュリティサービスである MDR を利用するようになっています。Gartner は、2025 年までに世界の半数の組織が、脅威を封じ込めるために MDR を利用するようになると予測しています。XDR の場合、監視、検出、および対応を自社で行わなければなりませんが、MDR では、この重労働を信頼できるサイバーセキュリティプロバイダーに委託でき、社内のスタッフは他の価値の高い仕事に注力できるようになります。

91%

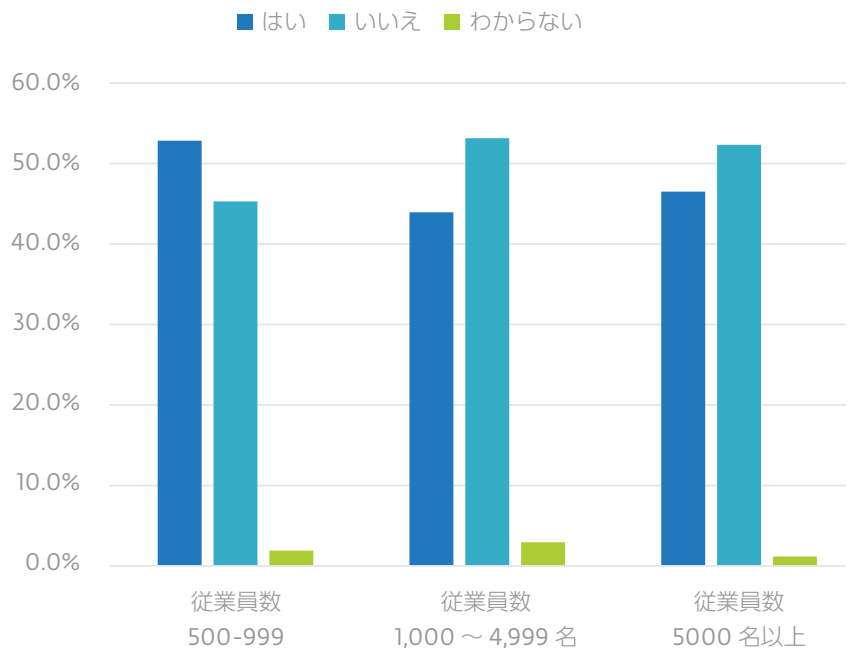
のエンタープライズ企業が、デプロイサービス、テクニカルサポート、サイバーセキュリティサポート、サイバーセキュリティ脅威のハンティングと監視をサービスとして既に利用しているか、利用することを検討しています。

出典：大規模企業の回答者 404 名を対象とした ESET Research による社内調査。

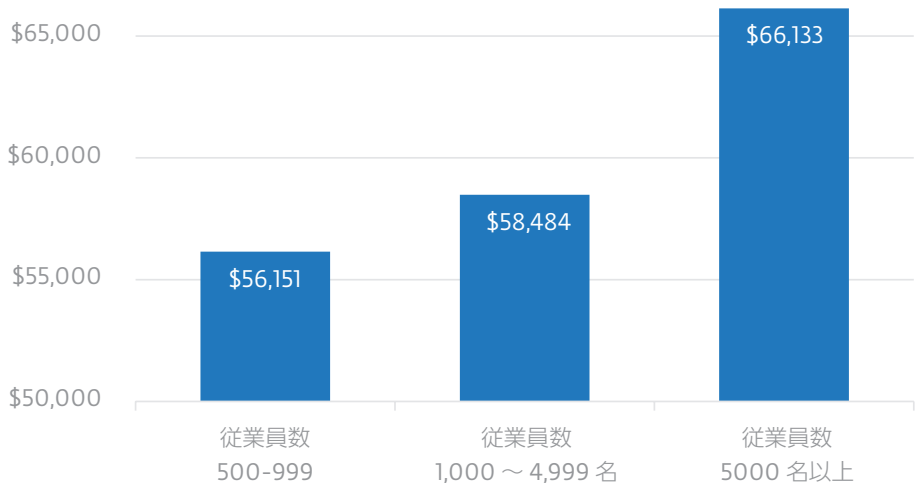
セキュリティ侵害は現実の脅威

IDC

過去 12 ヶ月から 24 ヶ月の間に、
セキュリティ侵害を経験しましたか？



セキュリティ侵害が 1 回発生した場合のコストは？



出典：IDC、Security Services Market Update、1Q22、Doc # US48907622, March 2022.

MDR が必要な理由

サイバーセキュリティへの平均支出額は、2021 年に従業員数が 250 ～ 999 名の企業では 2 倍に、従業員数 1,000 名以上の企業では 65% も増加していますが、現在でも大規模なセキュリティ侵害が発生しています。

米国では 2021 年に、公になったデータ侵害の件数記録的な数 になり、過去の最高値である 1,506 件を 23% 上回りました。英国では、59% の中堅企業と[1]、72% の大企業[2] が 2021 年にセキュリティ侵害やサイバー攻撃を検出したと回答しています。ランサムウェアの脅威は特に深刻であり、あるレポートでは 2021 年に検出された攻撃数は 6 億 2,300 万件に達し、前年比で 105% 増加したことを報告しています。

拡大する企業の攻撃対象領域

なぜ、企業や組織がサイバー攻撃者を排除するのに苦しんでいるのでしょうか？デジタルインフラへの投資やオフィスと自宅などのハイブリッドの働き方が広がったことで、攻撃対象領域が広がったことも一因です。McKinsey によると、新型コロナウイルスにより多くの企業が「技術的な転換期」に直面し、業務のあり方を大きく変えました。デジタルトランスフォーメーションを大きく加速させた組織も存在します。その結果、これらの企業は効率性を高め、革新的な顧客体験と従業員体験を提供できるようになった一方で、デジタル攻撃の対象領域が大幅に増加することになりました。ある調査によると、グローバル企業の 43% が、自社のデジタル攻撃対象領域が「コントロールできない状況に陥っている」ことを認めています。組織では以下のような攻撃対象領域が広がっています。

クラウドコンピューティング

IaaS、PaaS、SaaS は、IT のアジリティを向上し、コスト面でも大きなメリットをもたらしますが、特に IaaS や PaaS を利用する場合、組織がその環境のセキュリティを確保することは容易ではありません。多くの企業が複数のハイブリッドクラウドを管理していることもあり、複雑さに拍車をかけています。設定ミスも多く発生しており、2021 年におけるのクラウドセキュリティのインシデントの最も多い原因となっています。サイバー犯罪者は定期的にシステムの構成ミスをスキャンして、侵入口を探しています。

---

1) 中堅企業とは、従業員数 50 人以上 249 人以下の企業を指します。中堅企業 149 社を対象に調査を行いました。
2) 大企業とは、従業員数 250 人以上の企業を指します。大企業 134 社を対象に調査を行いました。

リモートワーク

多くの従業員が自宅で使用しているシステムは、十分に保護されていないことが懸念されています。従業員は、会社から支給されたノートパソコンにパッチを適用しなかったり、個人で所有しているデバイスを最新の状態で維持せずに、セキュリティを疎かにしたりしている場合もあります。2021 に公開されたレポートでは、IT リーダーの 45% が、プリンターのセキュリティが侵害され、さらなる攻撃に悪用されたことがあると報告しています。従業員の自宅の作業環境は、サイバー犯罪者にとって企業ネットワークを侵害するための魅力的な攻撃経路として悪用されるケースが増加しています。そして、ハイブリッドワークが普及する中で、モバイルワーカーが公共の Wi-Fi ホットスポットや共有コンピュータを経由して企業のネットワークに接続するようになり、さらに脅威が高まっています。

在宅勤務

リモートワークで使用されるデバイスが攻撃対象になることも多くありますが、デバイスの所有者も同様に標的となっています。マイクロソフトによると 80% のセキュリティプロフェッショナルが、リモートワークへの移行が始まってから、セキュリティの脅威が増加した回答しています。また、これらの回答者の 62% は、さまざまな脅威の中でフィッシング攻撃が最も増えたと述べています。在宅で勤務する従業員は、オフィスで勤務する従業員よりも注意力が散漫になり、リスクの高い行動をしてしまうことも多いことから、ソーシャルエンジニアリングの格好の標的になっています。フィッシングは、ランサムウェア、データ漏洩、またその他のセキュリティ侵害の起点になる恐れがあります。3分の1以上(35%)の企業が、従業員がセキュリティ対策を回避したり、無効化したりしていると回答しています。

「2015 年以降、
報告されたセキュリティ侵害の件数は 25% 増加し、
漏洩したレコードの数は 500% 増加し、
2017 年以降に発生したランサムウェア攻撃の数は
231% 増加しています。」

Best Practice: Security Matters, Now What? Forrester Research Inc, May 2, 2022

リモートアクセスインフラストラクチャ

リモートワークを行う従業員数が激増したことで、社外から社内のリソースにアクセスするための仮想プライベートネットワークやリモートデスクトッププロトコル（RDP）などのツールの利用も急増しました。これらのツールを利用するときの課題は、パッチが適用されない、あるいは正しく設定されないことが多いことです。多要素認証によって保護が強化されているケースは少なく、多くの RDP アカウントは、簡単に予測される認証情報や漏洩した認証情報で保護されています。このため、攻撃者は正規のユーザーになりすまし、簡単に企業ネットワークにアクセスできるようになっています。RDP はランサムウェア攻撃で悪用される経路のトップ 3 に入っており、試行された攻撃回数は、過去最高の 45 億件に達しています。[3]

2022 年 1 月 10 日に RDP への攻撃試行が過去最高を記録

2021 年 T3 から 2022 年 T1 における RDP 接続試行と RDP 接続を報告したユニーククライアント数の傾向。7 日移動平均で算出。出典：ESET テレメトリ

3) 7 日移動平均で算出。

サプライチェーン

サプライチェーンとは、パートナーやサプライヤーの物理的なエコシステムやデジタルエコシステムのいずれかを意味します。物理的な環境では、ネットワークにアクセスできる従業員や契約社員が騙されてパスワードを教えたり、泥棒にマシンを盗まれたりするリスクが後を絶ちません。ソフトウェアサプライチェーンでは、サイバー犯罪者が、ソフトウェアの開発、デプロイ、アップデートに使用されるメカニズムやツールがマルウェアによって汚染されることがあり、さらに大きな脅威となるケースがあります。IT 管理ソフトウェアプロバイダである Kaseya のセキュリティがランサムウェアグループ「REvil」によって侵害され、Kaseya のアクセス権限が悪用され、悪意のあるソフトウェアアップデートが MSP クライアントに配信される大規模なインシデントも発生しています。この攻撃では、1000 社を超える Kaseya の顧客が影響を受けました。もう一つの懸念はオープンソースのコードです。オープンソースのコードは、価値実現までの時間を短縮するために DevOps チームによって広く使用されていますが、複雑なソフトウェアの依存関係があり管理が困難であり、新たなリスクをもたらす恐れがあります。5 分の 2 以上 (41%) の組織が、使用しているオープンソースソフトウェアのセキュリティに信頼を置いておらず、オープンソースの使用に関するセキュリティポリシーを確立している組織はわずか 49% であることが報告されています。

49%

49% の組織しか、オープンソースソフトウェアに対応する
セキュリティポリシーを設定していない。

出典：State of Open Source Security Report, Snyk, 2022

専門化し技術革新を続けるサイバー犯罪者

一方、このようなセキュリティギャップを悪用して攻撃するサイバー犯罪者の数は、近年急増しています。窃取したデータを販売したり、アクセスやツールを購入したり、新たな人材を雇うための地下マーケットも存在します。サイバーセキュリティの専門家は不足していますが、サイバー犯罪で生計を立てようとする人材は豊富にいるようです。

このサイバー犯罪のための地下マーケットでは、あらゆる領域で技術革新が進んでおり、ネットワークを防御する側にとっては好ましくない状況が続いています。以下のような新しい攻撃手法やサービスが見られるようになりました。

1 サービスとしてのランサムウェア（RaaS）

SaaS モデルが普及し、クラウドからソフトウェアを簡単に展開できるようになったように、RaaS によってランサムウェア攻撃を簡単に開始して管理できるようになり、ランサムウェア攻撃がビジネスとして運営されています。RaaS を利用するアフィリエイトグループは、攻撃で得た収益の最大 80% を手にすることができます。RaaS の利用料を支払う見返りとして、ランサムウェアのペイロードと攻撃インフラ、および窃取したデータを提供・販売するサイトが含まれるスターターキットが利用可能になります。

2 マネタイズの手法

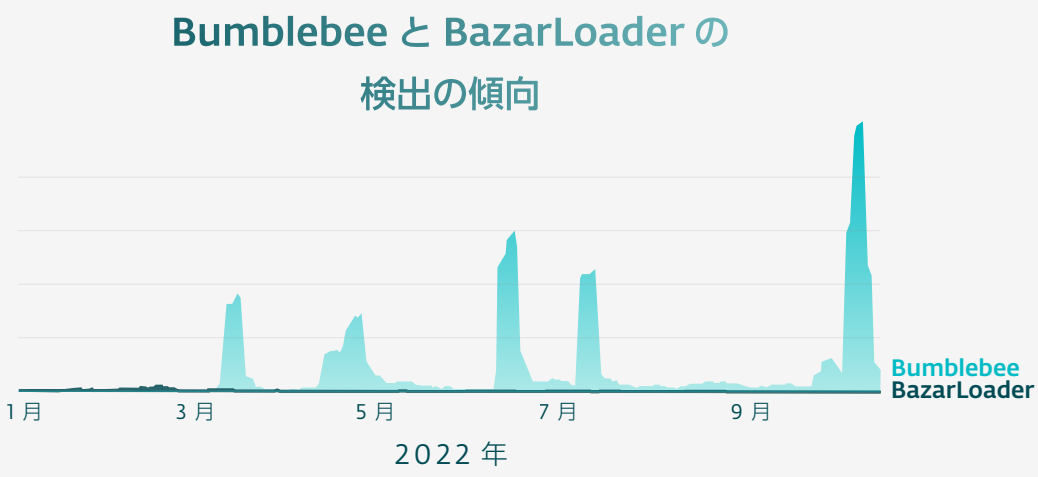
現在、多くのランサムウェアの攻撃は、データを外部に送信して漏洩させ、金銭の支払いを強要します。しかし、アフィリエイトグループは、さらにさまざまな手口で被害者にプレッシャーをかけるようになっています。例えば、分散型サービス拒否（DDoS）を仕掛けたり、顧客、パートナー、ジャーナリストにサイバー攻撃が発生していることを意図的に伝えたりする場合もあります。あるランサムウェアグループは、被害を受けたグループ企業のサイトを改ざんし、身代金を要求する文章を表示しました。別のグループは、攻撃した各組織向けにリークサイトを作成し、顧客や従業員が自分のデータが流出しているかを確認できるようにしていました。

3 脆弱性が公開された直後にエクスプロイトが開発される

米国の国家脆弱性情報データベース（NVD）で追跡されている脆弱性の数は、2021 年に過去最高を記録しました。セキュリティ管理者は、公開されている膨大な数のパッチを常に把握することがますます困難になっています。さらに、ゼロデイ脆弱性を機敏に悪用するサイバー攻撃組織も増えており、脅威はますます拡大しています。Microsoft Exchange Server の ProxyLogon の脆弱性を修正するパッチが提供されてから数日のうちに、10 もの APT グループがこの脆弱性を悪用した攻撃を行い、115 カ国以上の 5,000 台以上の Exchange Server が影響を受けました。

4 サイバー攻撃のためのサプライチェーン

サイバー犯罪の地下マーケットは拡充を続けており、専門化も進んでいます。特殊なスキルを有する専門家グループが参入しており、商業面と運用面に関する要件に対応するようになっています。例えば、認証情報の窃取を専門としており、他の組織にアクセス情報を大量に販売しているイニシャルアクセスブローカーが出現しています。2021 年にサイバー犯罪者向けのフォーラムで広告を行ったイニシャルアクセスブローカーの数が前年から 57% 増加していることがある調査チームから報告されています。そして、追加のペイロードをダウンロードして実行するように設計されたローダーである Bumblebee も販売されています。Bumblebee は、2020 年に 2 回のテイクダウンを乗り越え驚異の復活力を示した「TrickBot」の後継として悪用されているローダーです。しばらくは、TrickBot の代わりとして BazarLoader が 2022 年の初めまで広く利用されていましたが、その後すぐに Bumblebee に取って代わられました。Bumblebee ローダーは、TrickBot や BazarLoader と同じサイバー犯罪者によって運営されている可能性が高く、2022 年 8 月中旬に最新のキャンペーンを開始し、現在も活動を続けています。



5 正規のツールとファイルレスマルウェア

サイバー犯罪者は標的のネットワークに侵入すると通常、正規のツールやファイルレスマルウェアを使用して、従来のセキュリティツールによる検出を回避します。これは、一般的に使用されているプログラムを利用して、ラテラルムーブメント、データの流出、プロセスの検出、クレデンシャルダンプ、任意のコマンドシェルの実行などの悪意ある操作を実行するという発想です。利用されているプログラムには、PowerShell、PsExec、Cobalt Strike などがあります。

6 フィッシングとソーシャルエンジニアリングの進化

昔ながらのやり方が最も効果的となる場合もあります。フィッシングは、ランサムウェア攻撃の経路のトップ 3 に入っており、2022 年 Q1 には過去最高の検出数を記録しています。サイバー犯罪者は、メールフィルターやセキュリティトレーニングプログラムを出し抜くために、常に手を変え品を変えています。最も一般的なフィッシングは、メールスレッドを乗っ取る手法です。これは、攻撃者はある受信箱を乗っ取り、そのユーザーになりすましてこれまでの対話に乗ってフィッシングリンクをばら撒くものです。返信されるメッセージは、新しいメッセージよりも本物らしく見えるため、メールにあるリンクがクリックされる確率が高くなります。また、スマートフォンに巧妙なショートメッセージ（SMS）を送信してクリックさせるスミッシング（SMS フィッシング）という手法も悪用されています。あるベンダーは、2021 年に米国におけるスミッシングの試行回数が 2 倍になり、500 件以上のスレッドハイジャックキャンペーンが同年に実行され、16 種類のマルウェアが配信されたことを記録しています。

予防から XDR まで

XDR は、EDR が進化したものであり、脅威の検出、調査、対応、ハンティングをリアルタイムで最適化します。ランサムウェアではさまざまな方向に進化を続けています。イギリス政府のセキュリティ専門家によると、ランサムウェアは組織にとって最大のサイバーリスクになっています。あるランサムウェアグループ（Conti）は、わずか 2 年間で、少なくとも 859 の組織のセキュリティを侵害することに成功しており、僅か 1 ヶ月で 40 社への攻撃を成功させ、その過程で数十億円の暗号通貨を手にしたことからも、その脅威の大きさを容易に理解できるでしょう。ある試算によると、2021 年の 9 か月間におけるランサムウェアの検出数は前年から 148% 増加して 4 億 7000 万件に達し、過去最悪になっています。

しかし、現在のグローバル企業にとって、ランサムウェアが唯一の脅威ではありません。データ窃取、クリプトマイニングマルウェア、バンキングトロイ、スパイウェアなど、さまざまな脅威が組織を狙っています。

このようなトレンドの影響により、IT セキュリティのリーダーは、避けられない真実を直視せざるを得なくなっています。**それは、脅威を予防することは依然として重要であるが、攻撃を完全に防ぐことはできないという事実です。**サイバー犯罪者が検出されることなく企業環境に侵入する方法はあまりにも多く存在します。そのため、企業は予防、検出、対応をバランスよく取り入れる必要があります。ここで注目されるのが、複数のセキュリティテクノロジーレイヤーを融合させ、予防、検出、対応の能力を組み合わせた ESET の EPDR のアプローチです。予防段階では、悪意のあるコードやサイバー犯罪者が組織のシステムに侵入したり、被害を与えたりするのをブロックします。しかし、侵入された場合でも、強力な検出と対応機能によってシステムを侵害する高度な脅威による影響を軽減します。

これは、ドアや窓を施錠し、チェーンまでかけておきますが、万が一侵入者があった場合には、人感センサーを設置して不審な行動を察知するような仕組みです。XDR はここで重要な役割を果たします。セキュリティオペレーション（SecOps）チームは、IT 環境を一元的に可視化し、精度の高いアラートを利用して、脅威を示す異常を特定できるようになります。XDR[5] は、EDR が進化したものであり、脅威検出、調査、対応およびハンティングを最適化します。

---

5) Forrester による XDR の定義、2021 年

XDR は、セキュリティエンドポイント製品による脅威検出と、ネットワーク分析と可視化（NAV）、メールセキュリティ、IAM（アイデンティティとアクセス管理）、クラウドセキュリティなどのセキュリティおよびビジネスツールのテレメトリ（監視データ）と統合します。これは、ビッグデータインフラストラクチャを基盤に構築されたクラウドネイティブプラットフォームであり、セキュリティチームはこのプラットフォームを柔軟に活用できます。また、拡張性に優れ、セキュリティオペレーションを自動化することが可能です。

XDR を利用することで、サイバー攻撃に関連する以下のような重要な情報を取得できます。

- **脅威はどのように始まったか？**
- **どこで始まったか？**
- **いつ始まったか？**
- **どのエンドポイントが感染したか？**
- **脅威は封じ込められているか？**
- **今後、どうすればこの脅威を防げるか？**

最も重要なことは、組織が深刻な影響を受ける前に、迅速に改善策を講じてインシデントを解決できることです。

MDR が企業にもたらす価値

XDR を利用する場合であっても、SecOps チームは運営に関する大きな課題に直面することになります。社内におけるサイバーセキュリティに関する専門的な知識やリソースの不足が顕著である中小企業が、特にこれらの多くの課題を抱えています。組織の全体的な課題としては、以下のようなものが挙げられています。

人材不足

サイバーセキュリティ業界では、現在 270 万人の労働者が不足しており、セキュリティオペレーションセンター（SOC）のアナリストは採用が最も困難な人材になっています。2023 年には、アラート疲れ、ストレス、燃え尽き症候群のため、多くのセキュリティアナリストが退職することが予測されており、この問題はさらに悪化することが懸念されています。IT のジェネラリストは、XDR ソリューションを運用するのに 1 日数時間を割くことができないことも多くあります。この問題は、中小企業で最も深刻になります。多くの中小企業は、SOC を運用するために必要となる専門知識が社内にないため、MDR を最大限に活用できない場合があります。

コスト

セキュリティリーダーが検討しなければならないのは、SOC を担当する人材の雇用と確保にかかるコストだけではありません。アナリストが必要とする実用的な情報を提供するために、適切なツールを組み合わせなければなりません。これらのツールを導入するためには、初期費用と継続的なライセンス料など、大きな負担がかかることがあります。

SecOps を自社内で運営することを選択する場合には、大きな経済的負担が生じます。ある調査は、管理が複雑化しているために、SOC の ROI（投資利益率）は、半数以上の組織で低下していることを報告しています。この報告書では、セキュリティエンジニアリングのコストが年間 300 万ドルに上っており、このような社内運用の取り組みが効果的であると評価している組織は 51% に過ぎないことも明らかにしています。

セキュリティギャップ

ツールを組み合わせても、適切な効果が得られない場合があります。その場合、アラートの処理業務の負荷が増大し、アラート疲れにつながる恐れがあります。SOC のスタッフが誤検知に振り回されると、本当の脅威を示すシグナルを見逃したまま、成果を得ることなく、何時間も無駄に費やしてしまうことになりかねません。また、SOC で複数のツールを利用する場合、検出すべき脅威にギャップが発生することがあります。

管理

製品を購入し、設置し、正しく設定することは、最初のステップに過ぎません。いくつものSOCツールやアナリストを複数の場所で管理することも大きな課題になります。すでにリソースが限界に達している場合には、重要なタスクが見落とされることがあります。さまざまな脅威に向き合い、戦略的な計画を立てる時間を確保できなくなることも多くあります。

大規模企業のITセキュリティ担当者は、購入したソフトウェアを十分に理解し、サイバー脅威に対抗できる高度なSOCを社内で構築するなど、急速に拡大している課題に取り組む必要があることを認識しています。実際、ESETが実施した調査4では、以下の結果が明らかになっています。

68% セキュリティベンダーによるセキュリティ製品の導入サービスの提供を受けることを望んでいる組織の割合

75% サポート、コンサルテーション、インシデント対応をベンダーが提供することを望んでいる組織の割合

87% 24時間365日体制でサイバーセキュリティをサポートするサービスを望んでいる組織の割合

90% 脅威の監視、ハンティング、対応、修正サービスを提供するベンダーを必要としている組織の割合

4) 大規模企業の回答者404名を対象としたESET Researchによる社内調査。

MDR の主な利点

サイバーリスクを軽減しなければならないが、十分な社内リソースを確保して効果的にチームを運用できない組織にとって、MDR は非常に大きな利点をもたらします。プロバイダーによって提供している MDR の内容は異なりますが、少なくとも以下のいくつかの要素が含まれていなければなりません。

脅威の検出

サイバー犯罪者は、境界型の防御を潜り抜ける方法を無数に持っています。しかし、行動分析を活用すれば、攻撃を早期に特定し、攻撃による影響が拡散することを防ぐことができます。また、プロアクティブな脅威ハンティングによって、セキュリティ製品による自動検出を回避するような巧妙な攻撃を特定できるようになります。

優先順位付け

MDR システムでは、インテリジェントな分析によってコンテキストが生成され、データが実用的な知見に変換されるため、精度の高いアラートを配信できます。多くの SOC チームが膨大なアラートに圧迫されていることを考えると、これは MDR のワークフローでも特に重要な段階です。

「MDR サービスは、XDR の目的の多くを既に達成しています。MDR は、脅威インテリジェンス、脅威ハンティング、24 時間 365 日の監視、高度な分析、データの外部への流出や破壊が疑われるインシデントやセキュリティ侵害の抑制と除去などを行うためのツールやテクノロジーを提供し、優れた成果をもたらします。MDR はガイダンスや推奨される対策を提供するだけではなく、それ以上のサービスを提供すべきだと IDC は考えています。」

出典：IDC Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now?, Doc # US47705821, February 8, 2022, Ch. Kissel, M. Suby, F. Dickson

分析

行動分析を自動化し、アナリストの評価を取り入れながら、アラートが本当の脅威を示しているのか、また、問題解決のためにどのような手順が必要であるかを調査します。

対応

分析により、脅威を封じ込めて排除し、侵害されたシステムを修復するために、どのような対応が必要かを明確に把握できるようになります。パスワードのリセット、特定のエンドポイントへのパッチ適用、また、コンピュータにイメージを再インストールしなければならない場合もあります。

検出と対応をアウトソーシングすると、以下のような明確な利点がもたらされます。

- MDR プロバイダーは、バックエンドテクノロジーの管理をすべて担うため、組織のスタッフは膨大なアラートに埋没することなく、価値の高い戦略的な業務に集中できます。
- また、MDR プロバイダーは、各顧客のリスクプロファイルやインフラに合わせて、バックエンドテクノロジーを最適化し、管理できます。
- 検出と対応をサードパーティーに依頼すれば、SOC を運用する優秀な人材を雇用・維持するために必要な高額な給与が不要になります。
- MDR を利用する組織は、プロバイダーの規模の経済性、優秀な人材の確保、他の顧客の組織や脅威環境に関する知見などの恩恵を受けることができます。

MDR ソリューションに求められるもの

多くの MDR ソリューションが利用できるようなっている中で、何を基準に選定を始めたら良いのかわからない場合もあるでしょう。少なくとも以下の機能やサービスを提供するプロバイダーを検討してください。

優れた調査能力：
業界最高クラスの調査能力によってもたらされる最高水準の脅威インテリジェンスを提供している。

高品質なカスタマーサービス：
世界各国に拠点があり、多くの言語をサポートしながらサービスを提供している。

カスタマイズ：
お客様の規模、IT 環境の複雑さ、必要な保護レベルに合わせてパーソナライズされるオーダーメイドのソリューションを実現している。

業界をリードする検出および対応能力：
独立機関によるテストで、検出率の高さ、誤検出の少なさ、フットプリントの軽量さが評価されている製品を提供している。

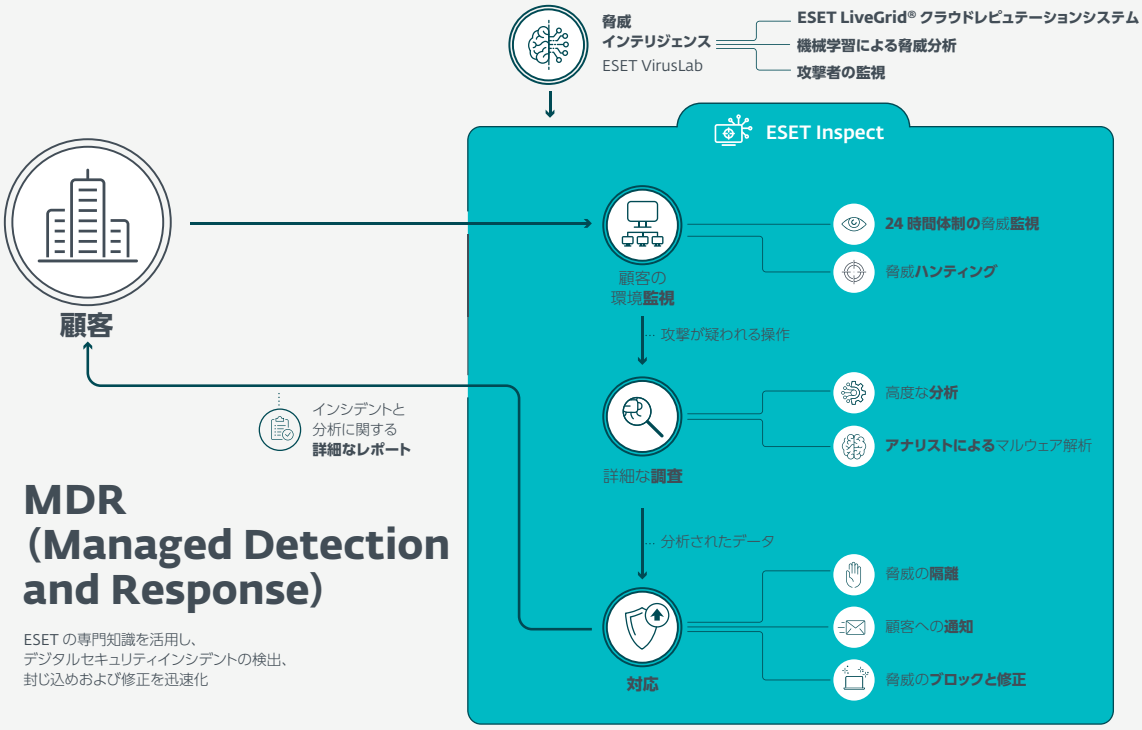
サイバー脅威ハンティング：
高度なツールと専門知識を駆使して、ネットワークに潜む巧妙な脅威をプロアクティブにハンティングする専門アナリストが存在する。

24 時間 365 日体制のオペレーション：
サイバー犯罪者は世界中に存在し、攻撃が発生する時間帯がさまざまであるため、MDR サービスは 24 時間で厳重に警戒する体制を提供する必要があります。

ESET の MDR の特長

ESET の MDR は、XDR などの**業界をリードするテクノロジー**ソリューションと、**30 年以上の専門知識**に基づく世界最高クラスのセキュリティ調査と脅威インテリジェンスを組み合わせたものです。ESET の MDR は、マルウェア、ソーシャルエンジニアリング、難読化技術、APT グループなどに関する**高度な調査・研究**に基づいて構築されたツール群を備えたエンタープライズクラスの SOC から提供されます。

しかし、あらゆる組織に適用できる万能型の MDR は存在しません。各顧客について、その環境、インフラ、組織構成、サイバーセキュリティ文化全般についての最初に評価します。これにより、**個々の顧客のセキュリティプロファイル**を作成でき、組織が既に構築している IT セキュリティ機能の延長線上に ESET の MDR を展開できます。ESET は**あらゆる業界の顧客を保護**してきた豊富な経験を持ち、さまざまな業界や業種に特化した専門知識を有しています。あらゆる企業や組織が、ESET のテクノロジーと豊富な経験をセキュリティ対策に活用できます。



ESET MDR サービス「ESET PROTECT MDR」は、さまざまな地域に対応する包括的な製品とサービスを提供します。

- **サイバーセキュリティの専門家チーム**が、さまざまな規模の組織における導入、最適化、継続的な監視、定期的な脅威ハンティング、マルウェア分析、インシデント対応に対応します。また、各国のチームが、MDR などのマネージドサービスの中核をなすグローバルな脅威インテリジェンスチームと密接に連携します。

- ESET は、**30 年以上にわたってマルウェアの調査と研究を続けており**、高度な脅威や侵入手法について顧客の環境を監視するための専門知識を蓄積してきました。また、世界的にも知名度が高く、評価されている情報サービス「WeLiveSecurity」を支える専門家が、サービスを提供します。

- 基本的および詳細なファイル解析、リバースエンジニアリング、デジタルフォレンジック、インシデント対応支援などを含む**インシデントの調査と対応**。

- パートナー、各国オフィス、ESET 本社および世界各地にあるマルウェア調査研究チームから構成される大規模なネットワークによって、**世界のさまざまな地域の組織をサポートします**。

- **エンドポイントセキュリティをサポート**し、マルウェアの検出ミス、除去の問題、不審な動作の調査、ランサムウェア攻撃による影響の軽減に取り組みます。

- **ESET Inspect サポート**が、カスタムルールや例外の作成など、XDR ツールに関するあらゆる質問に対応します。

- **24 時間 365 日継続的に脅威を監視し**、環境が最新の状態になっており保護されていることを確認しながら、脅威の早期発見を可能にします。毎月レポートを提供し、ESET の監視結果と実施したサービスについて報告します。また、ESET のセキュリティアナリストが推奨するセキュリティ対策もこのレポートには掲載されています。

- 3 カ月に一度の**プロアクティブな脅威ハンティング**をデフォルトで実施し、最新の脅威から顧客の環境を確実に保護します。これらの調査では、多くの ESET の顧客からもたらされるセキュリティ侵害の痕跡（IoC）や潜在的な脅威に関する ESET の広範な知識が活用されます。

ESET が作成したレポート に掲載されるこれらの対策を実践することで、検出される脅威やインシデント数が時間とともに減少することが確認されています。これらのレポートには、ESET 製品や設定に関連する情報だけでなく、ブルートフォース攻撃の検出やフィッシングなど組織の環境で特定されている活動の種類、さらに、これらのフィッシングリンクをクリックする傾向にある特定のユーザーなどの実用的なアドバイスも含まれます。

ESET PROTECT MDR は、予防、検出、対応を網羅する製品とサービスを組み合わせた包括的なソリューションです。このソリューションには以下の製品が含まれ、一元的に管理されます。

- 管理コンソール（ESET PROTECT）
- エンドポイント保護プラットフォーム（ESET Endpoint Security）
- ファイルサーバーセキュリティ（ESET Server Security）
- 高度な脅威の防御（ESET LiveGuard Advanced）
- フルディスク暗号化（ESET Full Disk Encryption）
- EDR（ESET Inspect）
- MDR サービス（ESET Detection and Response Ultimate）
- プレミアムサポートサービス（ESET Premium Support Advanced）

MDR の展開を成功させる要素

ROYAL SWINKELS BREWERY 社の事例

Royal Swinkels 社はオランダ第 2 位の醸造所であり、世界 8 ヶ所以上の醸造所で 300 種類以上のビールを製造し、130 ヶ国以上で販売しています。同社は ESET の MDR を導入したときの体験を紹介しています。近年のビール製造では、IT や OT（インダストリアルオートメーション）を活用したプロセスの自動化が進んでいます。セキュリティ侵害や運用に悪影響を及ぼすイベントが発生すると、サプライチェーンの混乱を招き、納品や収益に大きな影響を与える恐れあります。ESET の MDR は、そのようなリスクから組織を保護します。ESET のチームは、高い能力を有する IT セキュリティスタッフから構成され、24 時間 365 日体制のサービスとして、検出と対応を管理し、すべてのアラートをフィルタリングし、環境を監視しています。

「同社のような規模のあらゆる企業が近年、IT に大きく依存しています。自社独自のセキュリティオペレーションセンターを稼働させるほど、当社の規模は大きくありませんが、何か問題が発生するまで待つことができるほど小規模な会社でもありません。問題に対して受け身になるのではく、未然に防ぐことを当社は目指していました。そのために MDR を選択し、ESET にその管理を委託したのです。」

Robert Heines 氏、
Royal Swinkels Family Brewers 社

ESET の製品やサービスによって予防、検出、対応をどのように強化できるかについては、ESET PROTECT MDR と EDR（extended detection and response）に関する参考資料を参照してください。

まとめ

セキュリティを担当する意思決定者は、新型コロナウイルスのパンデミックの収束という世界的なトレンドの中で、困難な時期を迎えています。世界的なこの危機が発生してから数年間で、企業のデジタル攻撃対象領域が大きく拡大しました。同時に、サイバー犯罪者はますます大胆になり、明確な動機を持ち、攻撃のための十分なリソースを確保するようになりました。チームが疲弊し、多くのポイント製品を導入したことでひずみが生じ、リソースが欠乏する中で、セキュリティオペレーションの管理者は巧妙化する攻撃を防ぐことが難しくなっています。このような状況下で、24 時間 365 日体制の本格的な SOC に投資することは、大企業以外には現実的ではありません。

セキュリティ侵害が発生することは避けられない事実になっています。しかし、攻撃者を迅速に発見し、インシデントをすばやく解決できれば、経済的および風評的な深刻な損害を受けることはありません。MDR は、このような環境で求められる全ての要素を提供するために作られたソリューションです。顧客は、セキュリティ管理の重労働を専門的なプロバイダーに委託し、セキュリティリスクを最小限に抑えることが可能になります。また、自社のスタッフをより価値の高い業務に従事させることが可能となり、収益性を向上できます。

「サービスプロバイダーは、顧客の既存の能力、サイバーセキュリティパートナーが提供するツールやサービス、および自社独自の知的財産を組み合わせて、MDR サービスを展開することができます。このパートナーシップにより、高度な EDR/XDR ソリューション、アナリストの専門知識、脅威インテリジェンス、脅威ハンティング、充実した管理機能があるコンソール、ダッシュボードおよびレポート、そして MDR サービスプロバイダーが開発したさまざまな知的財産を組み合わせ、強力なサービスを形成できます。」

出典：IDC, The Evolution of Managed Security Services, Doc # US48459521, December 2021, P. D. Harris, CISSP, CCSK

独自性、完全性、技術革新、専門性は、ESET がサイバーセキュリティソリューションを構築するための基盤となっており、その優れた成果は数多くの受賞歴に表れています。

ESET 製品を使用することで、以下のような利点を得ることができます。

- 顧客の規模、IT 環境の複雑さ、必要な保護レベルに合わせたオーダーメイドのソリューション
- ESET のサイバーセキュリティの専門家がサイレントパートナーとして稼働し、包括的なカバレッジを実現
- 信頼されるパートナーによって機密情報が取り扱われる安心感
- 多くの国の言語をサポート
- 30 年にわたるサイバーセキュリティの専門知識に基づく優れた調査・研究能力
- ランサムウェア対策、マルウェア解析、デジタルフォレンジック、インシデント対応などのサービスを追加費用なしで提供
- パフォーマンスを最適化しながら、強力な検出機能を提供する業界最高レベルのエンドポイントセキュリティ
- マルウェアの調査研究チームが、数十年にわたって蓄積した専門知識を提供し、顧客のスキル不足を軽減

ESET PROTECT MDR の詳細情報

ESET について

ESET は 30 年間にわたり世界中の個人および法人に向けて、業界をリードする革新的な IT セキュリティソフトとサービスを開発し、サイバーセキュリティ脅威に対する包括的な多層防御ソリューションを提供してきました。

ESET は長年にわたり、マルウェアの予防、検出、対応を行う機械学習とクラウドテクノロジーのパイオニアとして活動しています。ESET は、科学的な研究開発を世界的に推進している非公開会社です。

数値で見る ESET

10 億人＋
インターネット
ユーザーを保護

40 万＋
顧客数

200 ＋
国と地域に
展開

13
世界各国の
研究開発拠点

世界的なテクノロジーリーダー企業である ESET の製品を
自社を保護するためにぜひご利用ください