バイヤーズガイド

BlackBerry Cybersecurity

マネージドXDR ソリューションの選び方

このバイヤーズガイドでは、以下について解説します。

- マネージドXDR（Extended Detection and Response）の概要
- お客様の組織にマネージドXDRサービスが必要となる理由
- ベンダーの評価方法と最適な選択肢の選び方
- マネージドXDR サービスが各関係者にもたらすメリット

マネージドXDR の概要

企業や組織は、3 つの大きなサイバーセキュリティ課題に直面しています。そのうち 2 つは解決が難しく、最後の 1 つは最近まで、多くの組織には実現不可能なものでした。1 つ目の課題は、無数の攻撃から組織を守る効果的なサイバーセキュリティツールを見つけ出すことです。

サイバー攻撃はさまざまな形をとるため、1 つの組織が大量のセキュリティ製品を管理していることも珍しくありません。事実、大規模な組織は平均 76 種類のセキュリティツール[1] を管理しています。管理するセキュリティ製品の数が多くなると、各製品が何らかの検知のたびに通知を送信し、アラート疲れを引き起こします。

2 つ目の課題は、高度に洗練されたサイバー攻撃が進化し続けている点です。脅威グループは、システムを悪用して侵害する新たな方法を絶えず見つけ出しています。

かつて大きく報じられた SolarWinds 社[2] や Kaseya 社 VSA ソフトウェアに対するサプライチェーン攻撃について考えてみましょう。攻撃者は信頼されたソフトウェアプロバイダを侵害し、何千もの顧客に配信される前の製品コードを改変していました。信頼されたソフトウェアをソースの時点で悪意のあるコードに改変することで、脅威アクターは従来のアンチウイルス（AV）によるセキュリティチェックを容易に回避していました。さらに悪いことに、脅威アクターは無防備な企業を利用して、そうした企業を信頼する顧客、つまり正規のソースからの脅威を検知しないであろう顧客にまで攻撃を拡散していたのです。大手企業がこのような攻撃の被害を受けた場合、中小企業や中堅企業はどのように攻撃から身を守ればよいのでしょうか？

組織が直面する課題の中で解決が最も難しいと考えられるのが、サイバーセキュリティのスキルとリソースの不足により、多くの組織が熟練した専門家にアクセスできていない点です。米国情報システムセキュリティ協会（ISSA）は 2021 年、企業や組織が世界的なサイバーセキュリティのスキル不足から大きな影響を受けていると報告しました[3]。

スキル不足の主な影響としては、現従業員の作業負荷の増加（62%）、セキュリティ関連の求人枠が数週間から数か月間埋まっていない（38%）、「燃え尽き」/離職率の高さ（38%）などが挙げられています。長年、業界の専門家らがこのスキル不足を追跡し文書化しているものの、改善の兆しはほとんど見られません。アラート疲れと高度なサイバー攻撃は深刻な課題ですが、十分な時間、労力、リソースがあれば対処できます。しかし採用候補者が求人枠に満たない場合、組織はサイバーセキュリティの専門家をどのように確保すればよいのでしょうか？

幸い、これらの課題はマネージド XDR サービスを活用すればすべて解決できます。このソリューションは、最先端のサイバーセキュリティテクノロジーと人間の専門知識を組み合わせ、あらゆる組織のセキュリティチームを自然に拡張します。このアプローチはあらゆる規模の組織に効果的で、また広く利用可能です。企業でセキュリティオペレーションセンター（SOC）の人員確保に必要な予算が不足している場合、マネージド XDR サービスは魅力的かつ手頃な選択肢となり得ます。しかし、エンドポイント保護プラットフォーム（EPP）やエンドポイント検知/対処（EDR）をすでに利用している組織にとっては、マネージド XDR の必要性が自明ではないかもしれません。マネージド XDR のユニークな利点をより深く理解するには、過去の脅威が今日のテクノロジーをどのように形成したかを振り返ることが有効です。

テクノロジーレビュー：アンチウイルスからマネージドXDR まで

記録上で最初のコンピューターウイルスは、1971 年に書かれた実験的な自己複製型のコード片で、Creeper ワームと呼ばれています。このワームはインターネットの前身である APANET 内を移動しながら、感染したシステムで「*I'm the creeper, catch me if you can!（私はクリーパー。できるものなら捕まえてみろ！）*」というメッセージを表示するだけのものでした。1988 年にはより悪質な Morris ワームの事例が発生し、誕生して間もないインターネットに感染を広げ、接続されているシステムの約 10% をダウンさせました。また、同時期には初の AV 企業が登場し、サイバー攻撃の新たな脅威に対抗する製品とサービスを提供しました。

2021 年の ISSA の報告[4] では、サイバーセキュリティのスキル不足による以下のような影響が明らかになりました。

62%

の組織が、チームの作業負荷が増加していると報告

38%

の組織が、求人枠に空きがあることを報告

38%

の組織が、スタッフの燃え尽き率が高いことを報告

簡易年表

AV からマネージド XDR まで

1971 年 Creeper ワームが作成され、初のコンピューターウイルスとして広く知られる。

1987 年 初のウイルススキャンソフトウェアが発表される。

1988 年 Morris ワームがインターネットの約 10% をダウンさせる。

1980 年代後期 初の AV 企業が設立される。

2006 年 初の SIEM プラットフォームが構築される。

2011 年 第 2 世代の SIEM プラットフォームが登場する。

2013 年 EDR の概念が定義され、普及する。

2015 年 *EDR* の用語が形式化される。

2016 年以降 EDR、XDR、マネージド XDR がレガシーの AV ソリューションを置き換え始める。

初期の AV ソリューションの多くは、一意の識別子である*シグネチャ*を用いてウイルスの存在を検知し、阻止することに焦点を当てていました。ユーザーは手動でウイルススキャンを実行し、既知の脅威のシグネチャからなるローカルデータベースを照会することで、システム上でシグネチャの一致を検索していました。攻撃者はこれに素早く適応し、コードをわずかに変更してウイルスのファイルシグネチャを変更しました。対する防御側は、各脅威の特定の亜種を探すのではなくマルウェアファミリーを検知する手法を導入しました。こうした応酬が激化するにつれ、シグネチャライブラリは爆発的に大きくなり、手動のスキャンにかかる時間もますます増加しました。

また、組織はシステムを常に最新状態に保ち、AV ツールを一貫して効果的に利用するという課題にも直面していました。脅威に備えて環境を更新し監視する上で、個々のユーザーや小規模な IT チームに頼るのは煩雑であり、コストもかかるものでした。組織はテクノロジーを一元管理し、自組織の保護対策がすべてのデバイスを確実にカバーできる方法を必要としていました。そしてこの必要性が、SOC、セキュリティ情報およびイベント管理（SIEM）システム、EPP/EDR ソリューションの誕生につながります。

*エンドポイントでの脅威の検知と対処*という用語は、Gartner 社の担当者によって 2013 年に一般化され、2015 年に EDR へと更新されました[5]。EDR は、特にマルウェアに対抗するという考え方から、エンドポイントを狙ったより広範な攻撃に対処するという考え方へと、セキュリティ体制が変化したことを示していました。EDR ツールの狙いはディスクフォレンジックを行うことではなく、複数のソースから脅威テレメトリを収集し、対応策を提供することにあります。SOC、SIEM、EDR プラットフォームの登場により、組織がサイバーセキュリティのリソースを一元管理し、より大きな効果を得ることが可能になりました。

今日では、テクノロジーの急速な進歩と各種の新たな攻撃手法が従来のサイバーセキュリティモデルに影響を与え、その有効性を低下させています。多くの組織はクラウドサービスやクラウドストレージに移行し、攻撃者に新たな機会をもたらしています。脅威アクターは、クラウドプロバイダと顧客の間のセキュリティ責任が不明確、あるいは重複している脆弱性を探し続けています。また、モバイルデバイス、スマートフォン、在宅勤務、個人所有デバイスの持ち込み（BYOD）ポリシーも新たな脅威ベクトルを生み出しています。管理対象外のデバイスが境界外からビジネスリソースにアクセスする場合、組織のファイアウォール内でビジネス資産を保護するだけでは不十分です。モバイルコンピューティング、クラウドサービス、IoT（モノのインターネット）デバイスによってセキュリティが複雑化したことで、より強固なサイバーセキュリティソリューションであるマネージド XDR が必要となっています。

脅威アクターは、クラウドプロバイダと顧客の間のセキュリティ責任が不明確、あるいは重複している脆弱性を探し続けています。

組織にマネージドXDR サービスが必要となる理由

効果的なサイバーセキュリティツールを見つけ出すのは*難しい*課題ですが、これはただ*機能する*ソリューションを見出せばよいという話ではありません。すべての脅威に対処できるサイバーセキュリティツールは存在しないため、組織はそれぞれ特定の脅威に合わせた数十種類のソリューションを用意することになりがちです。中には運用に専門の担当者が必要となるツールもあるため、安全な環境を維持するためのコストは増すばかりです。

ツールの数が増え、その運用のために雇用する専門家の数が増えるにつれ、組織はツールの肥大化に悩まされ始めます。サイバーセキュリティツールの管理、監視、使用はますますコストがかさみ、増え続けるツールセットがもたらす見返りは減っていきます。また、こうした多数のツール群は、それぞれがおそらく 1 時間に複数回、セキュリティアナリストにアラートを送信します。これはセキュリティアナリストのアラート疲れにつながる恐れがあり、結果的に実際の脅威が見逃されるか、あるいは誤検知として無視される確率が上がります。

マネージド XDR は、複数のソースから脅威テレメトリを収集し、関連する脅威データに対するアラートをインテリジェントにフィルタリングすることで、この課題に対処します。

多くの組織では、脅威の検知、調査、対応に関する戦略が適切に定義されていないか、あるいは不完全なままです。特定の課題の解決方法を 5 人のアナリストに尋ねると、5 種類の答えが返ってくるかもしれません。実際、すべての答えが同じように導出されているわけではなく、またサイバー危機の最中に異なる理論を検証するのは無理があります。組織が成果を上げるためには、構造化された脅威の検知、調査、対応（TDIR）フレームワークが必要であり、マネージド XDR プラットフォームはこのプロセスに大きく貢献します。

慢性的なサイバーセキュリティの専門家不足はすべての組織に影響を与えていますが、その矢面に立たされているのが中小企業や中堅企業です。通常、大手企業は社内のセキュリティ専門家チームを確保するためのリソースを備えていますが、多くの中小企業や中堅企業はそうではありません。こうした現状に置かれた中小企業や中堅企業は、大規模な組織や国家から資金提供を受けていることが多い持続的標的型攻撃（APT）グループの攻撃にさらされています。マネージド XDR は、スキルやリソースのギャップに悩む組織に専門的なサイバーセキュリティサービスとツールを提供することで、条件を公平化します。マネージド XDR プラットフォームを活用すれば、同等のシステムを自社構築して人員配置するよりもコストが抑えられるため、大規模な組織もそのメリットを享受できます。

図 1（7 ページ）のコスト分析では、マネージド XDR サービスの各機能（SOC アナリスト、脅威インテリジェンスリソース、管理プラットフォームなど）を右側に示しています。図中の表示金額は、展開、製品統合、従業員の給与を含む各構成要素の固定費を概算で表しています。SOC アナリスト、脅威ハンター、プラットフォームエンジニアに続く 1 桁の数字は、最小限、中規模、および最適な構築時の従業員数を意味しています。たとえば、最小限の XDR 構築には SOC メンバー 5 名、脅威ハンター 1 名、プラットフォームエンジニア 1 名が含まれ、構築コストは 88 万 8 千ドルとなります。

マネージドXDR サービスは、自社構築の場合に比べてわずかなコストで世界レベルのサイバーセキュリティを提供します。

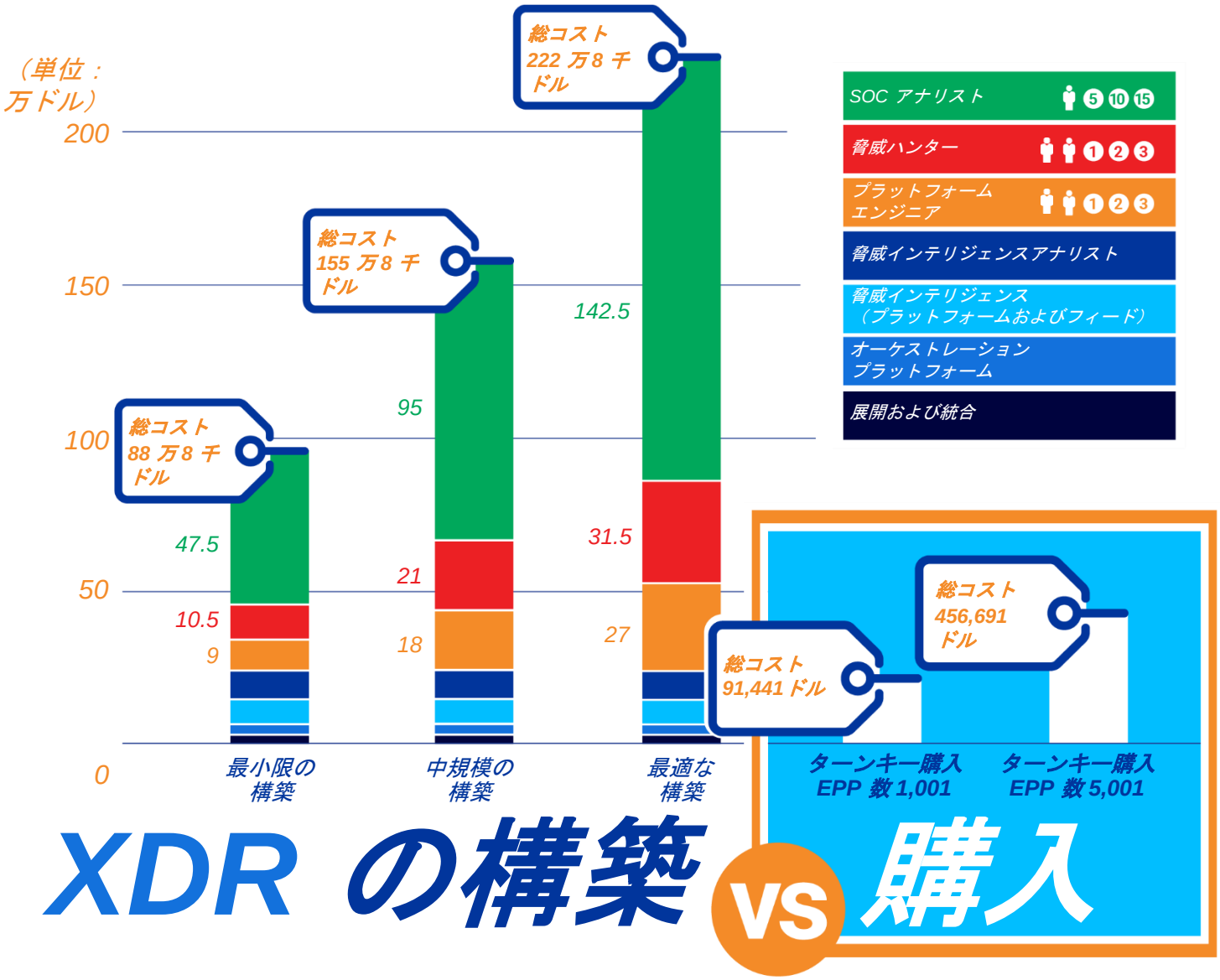


図 1：マネージド XDR の構築時と同等サービス購入時のコスト

なお、図中の表示金額はマネージド XDR プラットフォームの構築費用のみを表しており、EPP や EDR ソフトウェアは含まれません。また、最小限および中規模の構築では、人材関連の問題（病欠、休暇、その他の従業員の問題など）が発生し、不測の事態への対応で人員が不足した際に一部担当者が不在となる場合があるため、注意が必要です。

図 1 の重要なポイントとして、マネージド XDR サービスは、自社構築の場合に比べてわずかなコストで世界レベルのサイバーセキュリティを提供します。また、マネージド XDR はこれまで XDR 市場から排除されていた組織に対し、強力なプラットフォームと専門的なサイバーセキュリティアナリストへのアクセスを提供します。大規模な組織においても、運用コストを削減し、人員不足によるリスクを排除することで、マネージド XDR のメリットを享受できます。

マネージド XDR サービスの評価方法

マネージド XDR サービスはそれぞれ異なるため、組織のニーズに最適なサービスを選ぶことが重要です。各プロバイダを評価する際には、テクノロジー、機能、運用コスト、ベンダーの評判の違いに留意しましょう。以下のセクションでは、マネージド XDR の検討に役立つヒントをご紹介します。

注目すべき特徴

組織がマネージド XDR サービスから最大限のメリットを享受できるよう、以下の特徴に注目しましょう。

確かな実績を持つ企業

専門の脅威ハンターは、長年の経験を基に組織の脅威を適切に特定し、効果的に阻止します。マネージド XDR は、経験豊富なサイバーセキュリティアナリストへのアクセスを組織に提供します。競争の激しい雇用環境でそうした人材を確保する必要はありません。

24 時間 365 日体制での脅威の監視と緩和

マネージド XDR は、組織が IT セキュリティのリソースを他のタスクに再配置できるよう、継続的な脅威の検知と対応の機能を提供する必要があります。

サードパーティの統合

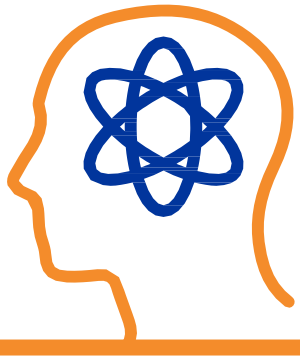
多数のソースから脅威テレメトリを収集して解釈できることは、マネージド XDR の強力な機能です。この統合により、組織のインシデント対応時間、アラート疲れ、誤検知が削減されます。

セキュリティアナリストへのアクセス

XDR の管理をサイバーセキュリティの専門家に一任できるだけでなく、そうした専門家に助言を求め、環境内の具体事例について質問できるとなおよいでしょう。

高度なテクノロジー

一部のマネージド XDR プロバイダは、AI 駆動型の脅威予防や自動化されたインシデント対応など、高度なテクノロジーを含むサービスを提供しています。こうしたテクノロジーを適切に導入できれば、戦力が倍増し、人員追加のコストをかけずに組織の保護を強化できます。

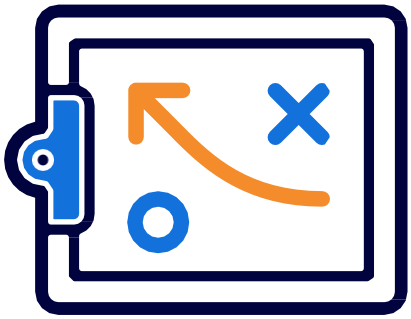


複数のチャネルを介した関連データの配信

効果的なマネージド XDR システムは、複数のソースから脅威テレメトリを収集するだけでなく、メール、SMS、アラート、その他のチャネルを介して関連データを組織に配信します。

MITRE ATT&CK のマッピングとカスタムのプレイブック

MITRE ATT&CK® のマッピングをテクノロジープラットフォームに統合し、カスタムの対応プレイブックを作成することで、極めて迅速な脅威予防レイヤーが実現できます。



継続的認証

信頼できるエンティティだけに組織のリソースへのアクセスを許可することは、ゼロトラストフレームワークに移行するための重要な要素です。

最適なマネージドXDR ベンダーの選び方

組織にとって最適なマネージド XDR ベンダーを選定することは、候補企業がそれぞれ最善のソリューションを提供すると主張している場合には困難を伴います。幸い、各企業とそのソリューションについていくつかの重要な側面を考慮すれば、検討候補は絞り込めます。たとえば、どのベンダーも自社製品の効果が極めて高いと主張していますが、その成果はどのように測定するのでしょうか？ 彼らの例は現実世界でのパフォーマンスを反映しているのか、単に実験から得られた結果なのか、どちらでしょうか？ 彼らは検知を成果と見なしているのか、それとも彼らのソリューションは脅威の予防も可能なのでしょうか？ 多くのサイバー脅威は攻撃の成功前に*何らか*の形で検知されますが、検知が予防につながらないのであれば、その意義は一体何なのでしょうか？

考慮すべきもう 1 つの要素は、脅威ハンティング、脅威予防、プラットフォーム管理に関する候補企業の専門知識レベルです。長年の経験を持つマネージド XDR ベンダーは、サイバー脅威、サイバーセキュリティテクノロジー、業界の変化など、さまざまな進化を乗り越えてきています。確かな実績は、当該ベンダーが強靭で変化に適応できることの証左として、セキュリティリーダーに安心感をもたらします。また、マネージド XDR ベンダーはネットワーク、モバイル、エンドポイントのセキュリティに関して高度な専門知識を持つことを示す必要もあります。

組織においては、休日を含め 24 時間 365 日体制でサービスを提供するマネージド XDR ベンダーのみを検討すべきです。攻撃者は休むことなく活動し、多くの場合、標的の防御が弱まると考えられる時間帯に合わせて攻撃を計画します。場合によっては、ベンダーのテクノロジーやアナリストに関する過去の業績評価に基づいて、検討候補を絞り込むのもよいでしょう。

攻撃者は休むことなく活動し、多くの場合、標的の防御が弱まると考えられる時間帯に合わせて攻撃を計画します。

マネージドXDR のチェックリスト

組織にとって、マネージド XDR の導入はメリットがあるのでしょうか？ 次のチェックリストがその判断に役立ちます。

課題	業界統計	マネージドXDR ソリューションの導入根拠
アラート疲れ	• 83% のセキュリティ専門家がアラート疲れを経験[6] • 27% の SOC で毎日 100 万件のアラートが発生[7]	• 外部のセキュリティ専門家がアラートを処理 • XDR プラットフォームがアラートを収集・精査し、それらを分類して優先順位付けするため、アナリストが信頼性の高い脅威情報の調査に専念できる
スキルとリソースのギャップ	• 全世界で推定 400 万人のサイバーセキュリティ従事者が不足[8] • 75% の中小企業が IT セキュリティ担当者の不足を報告[9] • 43% のサイバー攻撃が小規模企業を標的としている中で、セキュリティ対策を実施している企業はわずか 14%[10] • 38% の調査回答者が、スキル不足による影響の上位に「スタッフの燃え尽き率の高さ」を回答[11]	• マネージド XDR は、サイバー攻撃対策としてサイバーセキュリティの専門家と高度な XDR プラットフォームの両方を提供 • マネージドサービスは総所有コスト（TCO）を削減し、XDR を必要としながらも社内ソリューションの構築コストが許容できない組織を支援 • マネージド XDR は、ダウンタイム、休日、病欠、燃え尽きの心配のない 24 時間 365 日体制のセキュリティカバレッジを提供
高度な脅威との競争	• 攻撃者は検知されるまでにネットワーク内に平均 200 日間滞在しており、捕捉が困難[12] • 最終的に起訴されるサイバー犯罪は 0.3% で、たとえ逮捕されても攻撃者はしばしば処罰を回避[13] • 悪意のあるプログラムが毎日 45 万件以上新たに登録[14]	• マネージド XDR は、予測 AI やその他のテクノロジーで従来およびゼロデイマルウェアを検知・予防可能 • XDR はエンドポイント上、環境全体、さらにはネットワーク境界を越えて、インテリジェントな脅威ハンティングを実現 • XDR は脅威テレメトリを収集してコンテキストに当てはめ、従来のソリューションが見落としがちな危険を察知
一元化の欠如	• 82% の組織が、複数製品を統合したセキュリティアーキテクチャを構築[15] • 77% の企業が、提携するセキュリティベンダーの数を整理統合[16] • 大規模組織が提携するセキュリティベンダーの数は平均 10 社[17]	• マネージド XDR は、各種ツールやプラットフォーム全体で脅威インテリジェンスを統合して一元化し、参照と利用を容易化 • 熟練のアナリストがマネージド XDR プラットフォームを運用するため、社内スタッフが複数のセキュリティツールを習得して監視する必要性が低下 • 環境全体の複数ツールから収集したデータを分析し、悪意のある挙動の証拠を得るための共通クエリを脅威ハンターが作成

マネージドXDR が各関係者にもたらすメリット

マネージド XDR プロバイダの選定は重要なタスクであり、場合によっては、サービスの導入が各関係者の状況をどのように改善するかを説明する必要があるかもしれません。以下の例は、説明先に応じた議論の出発点を示しています。

SOC アナリスト

マネージド XDR は環境全体のソースから脅威テレメトリを収集し、ノイズの中から関連データをフィルタリングします。また、単独では不明瞭でも他のデータと組み合わせると明らかになる各種の痕跡を関連付けることで、脅威インテリジェンスにコンテキストを付加します。マネージド XDR は誤検知を削減し、脅威データを集約し、情報を優先順位付けすることで、さらなる調査のための関心事項を迅速に検知できるよう、SOC アナリストを支援します。

IT チーム

マネージド XDR サービスでは、XDR プラットフォームに関して特別に訓練された外部の技術専門家が、脅威の検知、予防、対応を実施します。こうしたサービスを活用すれば、社内の IT 担当者が専門分野に注力し、組織のために各自の能力を最大限に発揮できるようになります。

CEO/CFO

5 万件のデータレコードが侵害された場合の平均コストが 630 万米ドル[18] に上るこの時代、マネージド XDR は財務的にも優れた選択肢です。被害が生じる前に攻撃を阻止する予防ファーストのサイバーセキュリティソリューションを採用すれば、組織は防御が成功するたびに数百万ドルを節約できます。

CIO

マネージド XDR サービスは、高度なテクノロジーと人間の専門知識を提供し、環境を 24 時間 365 日体制で保護します。

継続的かつ包括的なセキュリティカバレッジが定額で提供されるため、CIO は残りのリソースをミッションクリティカルなタスクに集中できます。この投資により、「*既知および未知の脅威の検知に必要なものがすべて準備できているか ?*」と自問する必要がなくなり、安心感が得られます。その準備はすでにできているのです。

COO

サイバー攻撃は事業運営に壊滅的な影響を与えます。それゆえにマネージド XDR は、運営を維持する必要のある組織に大きな価値をもたらします。マネージド XDR サービスはインフラの安全を維持しながら、月次および四半期ごとのレポートを提供し、サイバー保護の強化が事業運営にどのような好影響を与えているかを明らかにします。

CISO

マネージド XDR は、組織が現在採用しているテクノロジー（EDR、EPP など）を統合し、熟練のセキュリティアナリストが管理する包括的なセキュリティプラットフォームを実現します。これにより、組織は既存のセキュリティ支出の価値を維持しながら、各種機能をアップグレードしてセキュリティ体制を強化できます。また、サードパーティのセキュリティアナリストが継続的なサポートを提供するため、担当者の入れ替わりに伴う対応漏れのリスクも排除できます。

攻撃者が新たな脅威ベクトルを発見し、新種のテクノロジーを採用し、攻撃手口を刷新するにつれ、脅威環境は絶えず進化します。脅威グループの多くは標的となる組織よりも技術力が高く、また資金も豊富です。そうした相手に固定的なセキュリティツールセットと限られた人員で立ち向かうのは、惨事を招く行為です。マネージド XDR は、機会をうかがう攻撃者に負けず劣らず柔軟で動的、かつ適応性のあるサイバーセキュリティ体制を維持する方法を組織に提供します。

CylanceGUARD について

BlackBerry は、予測 AI、自動化された対応、継続的監視、その他多くの高度なテクノロジーを、マネージド XDR プラットフォームの CylanceGUARD® に統合します。これらのツールにより、組織は予防ファーストのセキュリティ体制を採用し、プロアクティブに脅威に対処して、被害が生じる前に攻撃を阻止できます。CylanceGUARD プラットフォームには受賞歴のあるサイバーセキュリティチーム[19] が配置され、24 時間 365 日体制で世界レベルのサポートを提供します。

BlackBerry は、高度かつ協調的なサイバー攻撃から組織を守るお客様を支援いたします。詳細については、こちらからお問い合わせください。

出典：

1. https://www.infosecurity-magazine.com/news/organizations-76-security-tools/
2. https://blogs.blackberry.com/ja/jp/2020/12/a-blackberry-perspective-the-solarwinds-fireeye-attack
3, 4. ISSA、「Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment」、2021 年 7 月 28 日
5. Chuvakin, Anton、「Named: Endpoint Threat Detection & Response」、Web ブログ記事、Gartner Blog Network、Gartner、2013 年 7 月 26 日
6. Scroxton, Alex、「Majority of security pros fed up with alert fatigue」、Web ブログ記事、ComputerWeekly.com、2020 年 4 月 9 日
7. https://threatpost.com/its-time-for-your-soc-to-level-up/151343/
8. https://www.hdi.global/infocenter/insights/2020/cyber-skills-gap/
9. https://purplesec.us/resources/cyber-security-statistics/
10. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html
11. https://www.issa.org/cybersecurity-skills-crisis-continues-for-fifth-year-perpetuated-by-lack-of-business-investment/
12. https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_269210.pdf
13. https://www.theregister.com/2020/01/30/cops_crime_failure/
14. https://www.av-test.org/en/statistics/malware/
15. https://www.csoonline.com/article/3193701/toward-enterprise-security-technology-integration.html
16. https://www.csoonline.com/article/3566312/3-xdr-market-challenges.html
17. https://www.csis.org/analysis/cybersecurity-and-problem-interoperability
18. https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/
19. https://blogs.blackberry.com/ja/jp/2021/03/blackberry-triumphs-at-soc-x-championship

BlackBerry Cybersecurity

BlackBerry（NYSE：BB；TSX：BB）は、インテリジェントなセキュリティソフトウェアとサービスを世界中の企業と政府機関に提供しています。BlackBerry のソリューションは、1 億 9,500 万台の車両を含む 5 億以上のエンドポイントを保護しています。BlackBerry はカナダのオンタリオ州ウォータールーに本拠を置き、AI と機械学習を活用してサイバーセキュリティ、安全、データプライバシーソリューションの分野に革新的なソリューションを提供しています。また、エンドポイントセキュリティ、エンドポイント管理、暗号化、組み込みシステムの分野におけるトップクラスの企業です。BlackBerry のビジョンは明確です。つながる未来に信頼性あるセキュリティを確保することです。

詳細については、BlackBerry.com にアクセスし、@BlackBerryJPsec をフォローしてください。