ESG ショーケース

MDR がモダン サイバーセキュリティ戦略に不可欠となっている理由

日付：2022 年 8 月 **著者：**Dave Gruber、ESG プリンシパル アナリスト

要約：サイバーセキュリティ プログラムにおける検出および対応機能の重要性について議論する人はいません。大きな問題は、脅威の数が増え、ほとんどの組織が適応できるペースよりも早く複雑さが増している場合には、タイムリーかつ正確で、信頼性が高く、一貫性のある検出および対応を実現することがどれほど最善であるかということです。サード パーティーのマネージド サービスとしての Managed Detection and Response (MDR)は、組織がこのペースに対応できるようにするアプローチです。

はじめに：MDR の台頭

サイバーセキュリティの脅威が急速に増加し、攻撃対象が拡大しており、脅威を検出して対応する従来のプロセスとツールではもはや不十分です。あらゆる組織がこれらの厳しい現実に直面しています。脅威そのものとそれを実行する攻撃者の両方がより巧妙になり、攻撃者はさらに熟練し、俊敏性と持続性を備えており、企業資産の保護を担当するセキュリティおよび IT プロフェッショナルにデジタルのターゲットを移しています。

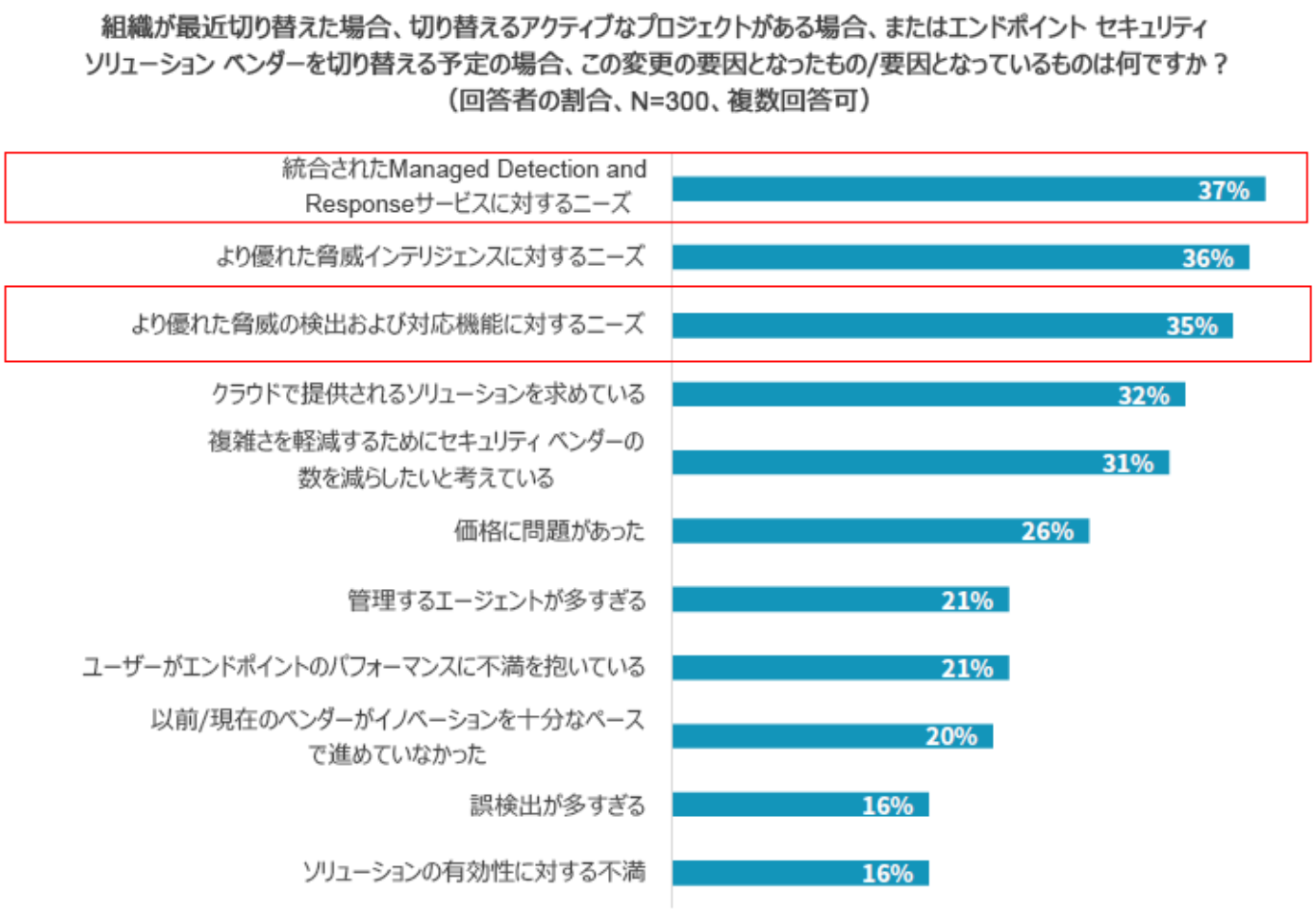
大量のセキュリティ制御により、検出と対応の取り組みに対するコストと複雑さが増加します。これによってセキュリティ チームは、誤検出から有効な脅威を探り出すために、大量のアラートを手動でトリアージする必要があります。より大規模なセキュリティ オペレーション センター(SOC)を構築し、より多くのツールとセキュリティ エンジニアを配置することには多額のコストがかかります。これは、組織がサイバーセキュリティ スキルのギャップが大きく増大している中で、十分なセキュリティ プロフェッショナルを特定して採用できることを想定しています。

サイバーセキュリティ プログラムが再設計されるにつれて、組織はより頻繁に Managed Detection and Response プロバイダーに支援を求めています。

サイバーセキュリティ プログラムが再設計されるにつれて、組織は、プロセスを改善し、リソースとスキルのギャップを埋め、セキュリティ運用ツールをモダナイズするために、Managed Detection and Response プロバイダーに対してより頻繁に支援を求めています。ESG の調査によると、統合された MDR サービスの必要性が、組織がエンドポイント セキュリティ ソリューション ベンダーを変更する要因となっていることが明らかになっているため、多くが MDR をエンドポイント セキュリティと関連付けています（図 1 を参照）。[1]

[1] 出典：ESG Complete Survey Results、『Endpoint Security Trends』（2021 年 12 月）。このショーケースのすべての ESG 調査の参考資料とチャートは、この調査結果セットから抜粋されています。

図 1：エンドポイント セキュリティ ベンダーを変更する要因



出典：TechTarget, Inc.の一部門である ESG

しかし、セキュリティ チームが検出および対応プログラムを拡張し、より包括的な検出および対応の拡張(XDR)ソリューションにアップグレードするにつれて、MDR 製品は、より包括的な攻撃対象への対応と高度な脅威検出を提供できるテクノロジーと運用モデルの両方をアップデートするパスを組織に提供しています。24 時間体制のモニタリング、リアルタイムのグローバル脅威インテリジェンス、オートメーション、高度な機械学習分析を組み合わせた新しいアプローチが求められています。これらはすべて、迅速な検出と脅威ハンティングをサポートするために、大量のセキュリティ テレメトリーを使用することで可能になります。XDR は進化と成熟を続けていますが、MDR サービスにより、あらゆる規模とセキュリティ成熟度レベルの組織は検出および対応を運用化することで、高度な脅威を軽減できます。これは、組織がデータセンターからエッジやクラウドに至るサイバーセキュリティ境界の範囲と規模を再定義する際に特に重要です。MDR は、分散型エンタープライズ全体で脅威の検出および対応のユース ケースを拡張するために必要な人材、プロセス、テクノロジーを統合します。

MDR 導入の主な要因

MDR サービスの使用は増加傾向にあり、セキュリティ チームはカバレッジを拡大して、スタッフ配置のギャップを埋め、プログラム全体の目標を強化しています。ユース ケースは多岐にわたりますが、基盤となる要因は次のとおりです。

- **脅威のランドスケープ：**サイバー攻撃の数とそれらの攻撃の高度化により、検出および対応をより迅速かつ確実に行うという大きな負担が組織にかかっています。
- **攻撃者の意図：**攻撃者は、攻撃の計画および実行方法において、よりスマートかつ持続的で、さらに戦略的になっています。強力な「犯罪エコシステム」が登場し、攻撃者が手口を共有して、共同で攻撃を仕掛けることさえあります。
- **経済：**SOC の構築と拡張に対する CAPEX のコミットメントは非常に大きく、通常で 7 桁の支出であり、場合によってはさらに増加します。
- **サイバーセキュリティ テクノロジーの更新：**セキュリティ運用活動のすべてまたは大部分を社内で行う組織では、サイバーセキュリティの統制スタックをより頻繁に更新する必要があります。これには、第 1 世代のエンドポイントの検出および対応から、より包括的な XDR/MDR フレームワークへの移行が含まれます。
- **スキル不足：**よく議論されているサイバーセキュリティ スキルのギャップは、長年の問題です。社内のサイバーセキュリティ ポジションに適切なスタッフを配置できないと、多くの場合、検出および対応の目標に課題が生じることになり、資産が危険にさらされます。

サイバー攻撃は無差別に行われます。スタッフや予算が限られている、また、過去にあらゆるタイプの攻撃を受けた経験がある中小規模の組織はリスクにさらされます。非常に大規模な組織でも、進化する脅威のランドスケープを検出しこれに対応するための戦略に対して、補足的なスタッフ配置、拡張性の高い統制、経営陣レベルのコンサルティングが必要です。

MDR サービスと MDR サービス プロバイダーに何を求めるべきか

MDR サービスを評価する組織には、次のような重要で難しい要件がいくつかあります。

- **コンテキストに応じた脅威インテリジェンス：**脅威を特定したり、誤検出を無視したりするための複数のインジケーターの相関を含む、リアルタイムの脅威インテリジェンスと検出を可能にします。
- **プロアクティブなユース ケース：**既知の脅威のアクティブなハンティングをサポートします。
- **豊富なテレメトリー：**新たな脅威を特定するために特に重要である、詳細なフォレンジック調査と高度な分析を実施します。
- **修復：**コンテキスト固有で AI 主導型の修復ガイダンスを提供します。
- **リスク軽減：**脆弱性の評価と管理。

MDR サービス プロバイダーの選択において、組織は次のような具体的で実証済みの機能を提供できるパートナーを探す必要があります。

- **24 時間 365 日対応のカバレッジ：**24 時間 365 日ベースで継続的なモニタリングを提供します。
- **What-If シナリオ**の計画とコンサルティング。
- サービス プロバイダーによる**人間の専門技術**と経験。
- C レベル幹部と役員への**ガイダンス**。
- **ガバナンス**、コンプライアンス、ビジネス継続性を確保する能力。

組織は潜在的な MDR パートナーにサービス レベル目標について尋ねる必要があります。これらの機能には、アラート発生から調査開始までの平均対応時間、調査開始から組織にインシデント分析が提供されるまでの平均対応時間、調査開始から解決までの平均時間が含まれます。

MDR に対するデル・テクノロジーズのアプローチ

MDR サービス プロバイダーを特定し、評価し、提携するには、組織は脅威の検出および対応に関する現在のニーズだけでなく、それらのニーズが将来どのように進化し拡張する可能性があるかについても重点的に取り組む必要があります。サイバーセキュリティの脅威の将来を予測できる組織はありませんが、各組織は革新的なテクノロジー、実証済みのプロセス、実証済みの専門技術に基づいて時間とともにサービスを拡張できる実績のある MDR パートナーを探す必要があります。

Managed Detection and Response に対するデル・テクノロジーズのアプローチは、柔軟性、インテリジェント、拡張性に優れたテクノロジーと経験豊富なサイバーセキュリティ プロフェッショナルを組み合わせたものです。サブスクリプションベースのサービスは、組織がコストの予測可能性を高め、必要に応じてより高いレベルのサービスにシームレスに移行できるように設計されています。

Dell Managed Detection and Response のテクノロジー プラットフォームは、Dell のビジネス ユニットである Secureworks によって開発され、完全に管理されたクラウド ネイティブ サービスの Taegis XDR です。Taegis XDR は、分散した多様な攻撃対象にわたって徹底的に調査された脅威の検出、分析、対応を行い、大規模なグローバル企業から比較的小規模な企業までの組織を保護するのに役立ちます。

Taegis XDR は、数十年にわたる専門知識を持つ Dell の大規模なセキュリティ アナリストとエンジニア グループのスキルによってさらに強化されており、既知の脅威と未知の脅威の両方から組織を保護するのに役立ちます。この組み合わせにより、IT アーキテクチャ全体にわたって検出と対応を効率的に統合できる方法が提供されます。このほとんどは、継続的に更新される脅威インテリジェンス データベースを通じて実現されます。また、Dell Managed Detection and Response は、攻撃者の行動を監視、分析、特定して、検出と対応の平均時間を短縮します。

また、Dell Managed Detection and Response は、攻撃者の行動を監視、分析、特定して、検出と対応の平均時間を短縮します。

Dell Managed Detection and Response はマネージド サービスであるため、すでに過剰な負担がかかっている社内の IT およびセキュリティ運用チームのためにセキュリティ プロフェッショナルを探して採用する必要性を大幅に軽減します。Dell Managed Detection and Response は、コスト パフォーマンスに優れた戦略的な方法で組織独自の機能を補完および拡張するように設計されています。

総括

攻撃対象の急速な拡大、繰り返されるランサムウェア攻撃、一般的に複雑さを増している脅威ランドスケープにより、組織が脅威の検出および対応プログラムをモダナイズする際の XDR および MDR への投資と採用の勢いは増しています。個々のセキュリティ戦略は状況によって異なりますが、攻撃対象をより広範に把握する必要性や、それを保護する個々のセキュリティ統制から大量のセキュリティ データの集約、関連付け、分析を行う機能は、制御を得るための重要なステップです。

セキュリティ チームが MDR プロバイダーを活用してスキル、プロセス、セキュリティ テクノロジーを強化するうえで、Managed Detection and Response サービスは効果的で、すぐに利用できます。ESG の調査によると、XDR に投資している組織は、これらのソリューションの実装と運用を支援するコンパニオン MDR サービスを求めています。これは、セキュリティ ソリューションとサービスの両方の提供において実績のあるソリューション プロバイダーと連携することを意味します。時間の経過とともに適用されると、IT チームとセキュリティ チームがセキュリティ プログラムを開発および拡張する際に役立ちます。

ESG では、これらの目標の達成に役立つ人材、プロセス、テクノロジーを備えたデル・テクノロジーズなどの企業の MDR ソリューションを検討することをお勧めします。

Enterprise Strategy Groupは、市場インテリジェンス、実用的なインサイト、ゴートゥマーケット コンテンツ サービスをグローバルなITコミュニティーに提供する、統合されたテクノロジー分析、調査、戦略を行っている企業です。

www.esg-global.com contact@esg-global.com 508.482.0188