Enterprise Strategy Group | Getting to the bigger truth.™

MDRによるセキュリティ運用のギャップの解消

サイバー攻撃の被害のリスクが高まることで、主要なビジネス目標のマインドシェアや予算は減少するため、組織はサイバーセキュリティ プログラムを強化することで対応する必要があります。すべてのサイバーセキュリティ プログラムの中心となるのはセキュリティ運用(SecOps)であり、デジタル攻撃対象のあらゆる側面を監視し保護する役割を果たします。

投資しているにもかかわらず、セキュリティ運用はより困難になっている

回答者の半数以上が、2年前と比べて、今日のSecOpsはより困難になっていると回答しています。

» SecOpsがより困難になっている上位5つの理由。

1. **41%**
脅威ランドスケープが急速に進化および変化している

2. **39%**
攻撃対象が絶えず変化および進化している

3. **37%**
セキュリティ アラートの量と複雑さが増している

4. **34%**
組織がパブリック クラウド サービスの利用を増やしている

5. **33%**
セキュリティ運用テクノロジーの運用ニーズに対応するのが困難である

プログラム戦略の再考

攻撃対象と脅威のランドスケープは、規模と複雑さが増しており、セキュリティ管理の使用率も高まっていることから、数千件ものアラートや大量のセキュリティ データが生成されています。セキュリティ チームは、ITチームと基幹業務チームの資産とリスク データをさらに組み込み、組織の目標に最も重大なリスクをもたらす脅威に焦点を当てられるように、プログラム全体の運用を再考しています。

組織の
98%
は、すでにMDRプロバイダーと連携しているか、今後12か月間でエンゲージメントを予定しています。

これらの組織の
88%
は、今後12か月間でMDRの使用を増やすことを予定しています。

» MDRエンゲージメントの主な価値促進要因。

運用の改善と効率性。
MDRにより、組織は、インフラストラクチャ、人員、管理など、いくつかの方法でセキュリティ運用における総所有コストを削減することができます。「アラート対応疲れ」の問題にも対処し、誤検出が大幅に減少する可能性を高めることもできます。

サイバーセキュリティの有効性の向上とリスクの低減。
MDRは、組織がすでに進行中の脅威を阻止し、潜在的な脅威と高度で持続的な攻撃の検出を向上させ、プロアクティブな脅威ハンティングを有効にし、より強力な制御を組織化することで、将来の攻撃を特定して防止することができます。

» 貴社がマネージド サービスを使用または計画している主な理由。

55%
重点:
組織では、セキュリティ運用タスクに時間を費やすのではなく、セキュリティ担当者をより戦略的なセキュリティ イニシアティブに集中させたいと考えている

52%
サービス:
組織では、サービス プロバイダーがセキュリティ運用でより良い仕事を行ってくれると考えている

49%
強化:
組織では、サービス プロバイダーがSOCチームをセキュリティ運用で強化できると考えている

42%
スキル:
セキュリティ運用のための十分なスキルが組織にない

> 「多くの『第1.0世代』のMDRソリューションは、データの削減、脅威の低下、検出のシンプル化という、異なる時代に合わせて設計および実装されました。」
>
> ESG主席アナリスト、**Dave Gruber**氏

MDRの新しい要件

多くの「第1.0世代」のMDRソリューションは、データの削減、脅威の低下、検出のシンプル化という、異なる時代に合わせて設計および実装されました。次世代のMDRソリューションでは、より多様な攻撃対象を保護し、より複雑な脅威を検出して、よりリスク中心のアプローチを活用して優先順位付けと軽減を行う機能を備えている必要があります。

- イベントとログの24時間365日体制のモニタリング。
- ボリューム、場所、タイプ別の疑わしい活動とアラートに関する迅速で可視性の高い情報。
- 継続的で拡張性に優れたネットワーク モニタリングと脅威分析。
- コンテキスト対応オプションに関するAI主導の推奨。
- 法令遵守に関するレポート作成。
- 社内チームと直接やり取りする「人間」のセキュリティ アドバイザー。
- 脅威の検出、トリアージ、調査、フォレンジックに基づく詳細なリアルタイムの分析。
- 脆弱性の評価、優先順位付け、軽減のガイダンス。

一部、ほとんど、またはすべてのアウトソーシングされたMDR機能を提供できる多数の潜在的なサービス プロバイダーを検討する際、組織は以下を提供できるパートナーを探す必要があります。

- コンテキスト対応可能な脅威インテリジェンス。
- 組織の地理的対象範囲、垂直的市場、規制プロファイルにおける実績。
- 実証された脅威ハンティング機能。
- クラウドベースのMDRへの長期的な取り組み。
- マルチクラウドおよびハイブリッド クラウド環境での広範な機能、ゼロ トラスト、クラウド セキュリティの責任共有モデル。
- 革新的なテクノロジー、実証済みのプロセス、従業員により実証済みの専門技術に基づいて、時間の経過とともにサービスを拡張できる実証済みの能力。

総括

サイバー攻撃の被害のリスクが高まることで、主要なビジネス目標のマインドシェアや予算は減少するため、組織はサイバーセキュリティ プログラムを強化する必要があります。ユース ケースはさまざまですが、ほとんどの場合、MDRサービス プロバイダーを活用してプログラムの成長と拡張を図っています。

デル・テクノロジーズのマネージド検出および対応アプローチは、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ることで、あらゆる規模の組織とリソース プロファイルがセキュリティ プログラムを加速し、強化できるように支援します。

さらに詳しく

DELL Technologies

出典：ESG Complete Survey Results, 「SOC Modernization and the Role of XDR」（2022年8月）。