Enterprise Strategy Group | Getting to the bigger truth.™

ESGホワイトペーパー

Managed Detection and Response：セキュリティ プログラムの迅速な成長への道筋

Dave Gruber（プリンシパル アナリスト）

2022 年 8 月

目次

要旨

デジタル トランスフォーメーションの加速化、クラウドの迅速な導入、より複雑な脅威ランドスケープ、セキュリティ スキルの不足が続く中、セキュリティ チームはその限界に追い込まれつつあります。現在のセキュリティ ソリューションでは対応できないため、多くがテクノロジーとプロセスを刷新するために SOC モダナイゼーション イニシアティブを優先せざるを得なくなっています。ゼロ トラストと検出および対応の拡張(XDR)に関する業界の大きなトレンドは、新しいビジョンを提供しています。しかし多くの組織は、これらの戦略の効果的なインプリメンテーションの実施と運用化に苦労しています。Managed Detection and Response (MDR)サービスは、この厳しい環境においてセキュリティ プログラムを強化するために必要な人材、プロセス、テクノロジーを多くの組織に提供します。

はじめに

ダメージを与えるサイバー攻撃のリスクが高まるにつれて、コア ビジネス目標からマインドシェアと予算が奪われるため、組織はサイバーセキュリティ プログラムを強化して対応する必要があります。一部の組織では、内部リソースを使用してセキュリティ プログラム全体を構築することが妥当ですが、ほとんどの組織には、プログラムの迅速な成長と拡張を可能にするサード パーティーのリソースが必要です。

あらゆるサイバーセキュリティ プログラムの中心となるセキュリティ運用(SecOps)は、デジタル攻撃対象のあらゆる側面の監視と保護を担当します。ネットワーク、エンドポイント、クラウド、ID、アプリケーション、データが対象に含まれ、SecOps に関連するセキュリティ テレメトリーとアラートの量が増えていることで、組織は限界に追い込まれ、多くの組織が MDR サービス プロバイダーに救いを求めています。

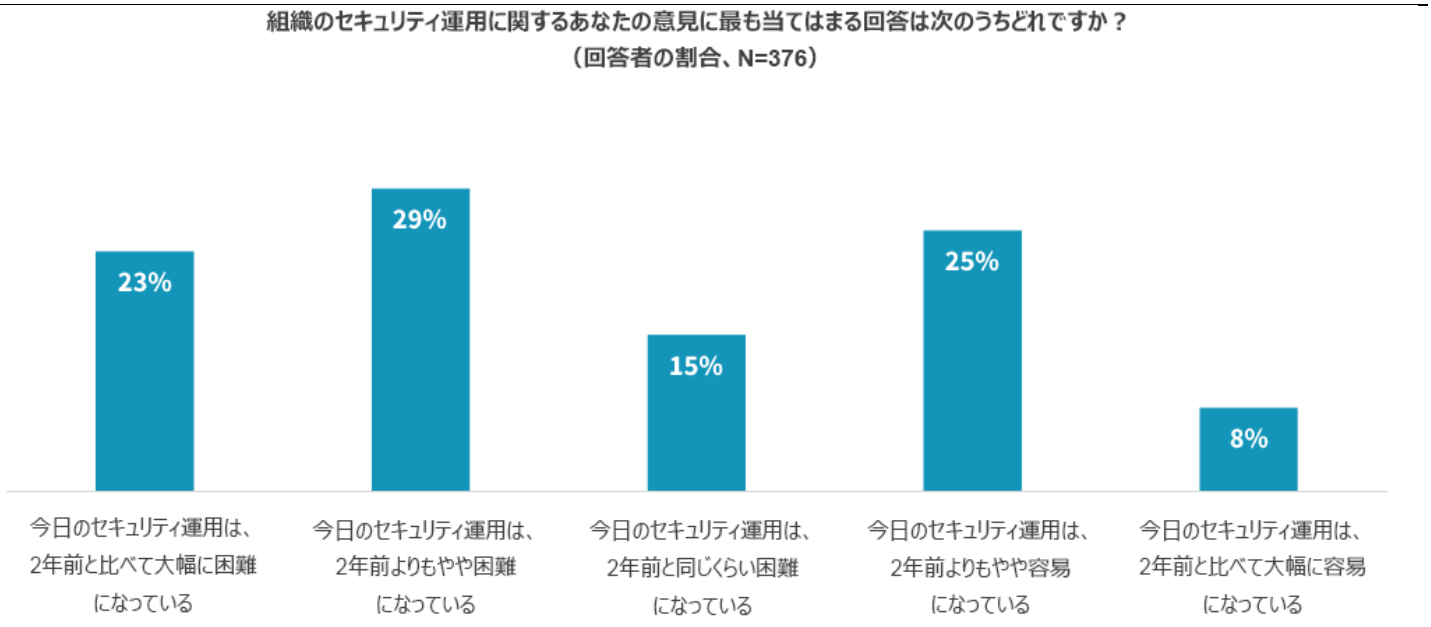
MDR サービス プロバイダーは、インシデント対応、24 時間体制のモニタリング、プログラム管理、リスク管理などのさまざまなセキュリティ サービスを提供することで、このような組織にとって重要なメカニズムとなっています。Enterprise Strategy Group (ESG)の調査によると、MDR サービスは、あらゆる規模とセキュリティ成熟度を持つ組織にとって、モダン サイバーセキュリティ戦略のメインストリーム コンポーネントとなっています。

セキュリティ運用の課題の増大

ESG の調査によると（図 1 を参照）、ほとんどの組織は、SecOps シナリオ全体が 2 年前よりも困難になっていると認めています。[1]

[1] 出典：ESG Complete Survey Results、『SOC Modernization and the Role of XDR』（2022 年 8 月）。このホワイト ペーパーに記載されているすべての ESG の参考資料とチャートは、特に記載のない限り、この調査結果から抜粋されたものです。

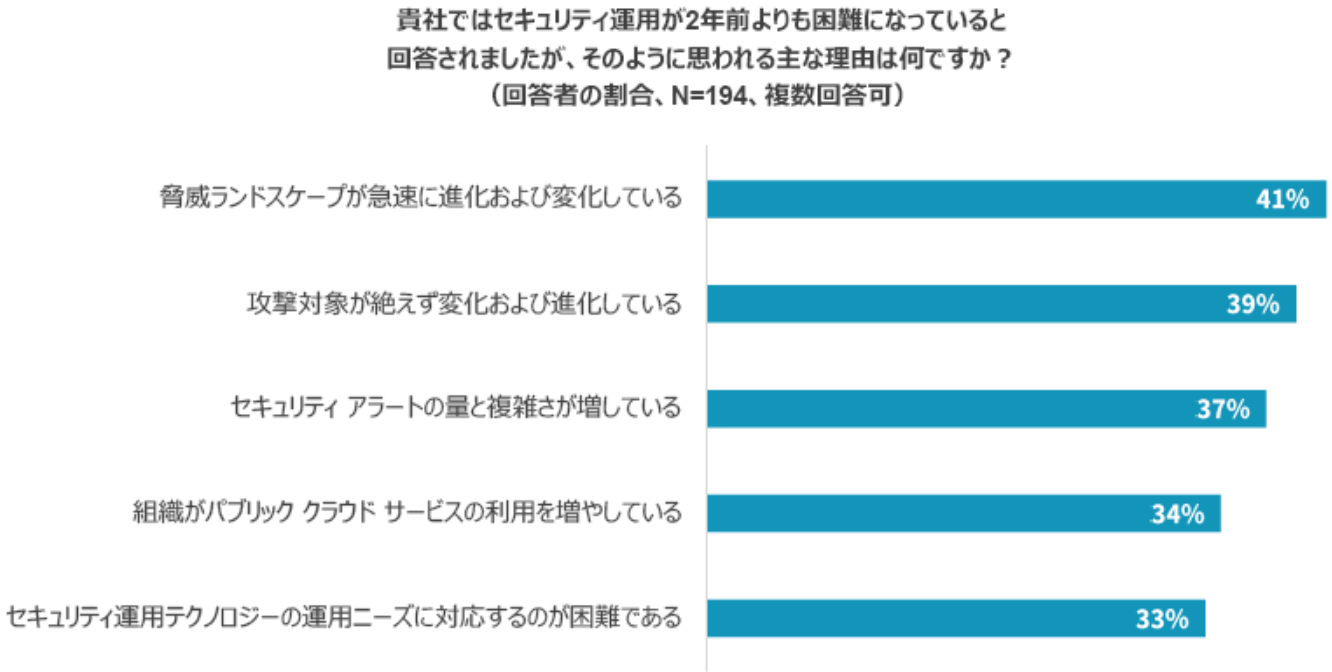
図 1：半数以上が SecOps はより難しいと考えている



出典：TechTarget, Inc.の一部門である ESG

図 2 に示すように、ESG の調査では、攻撃対象の拡大、脅威ランドスケープの拡大と多様性、広範なアプリケーションとユースケース向けのクラウド サービスの急増など、検出と対応によってこれまで以上に困難になっている他の課題も指摘されています。

図 2：SecOps がより難しくなっている上位 5 つの理由



出典：TechTarget, Inc.の一部門である ESG

検出および対応プログラムのモダナイズ

攻撃対象と脅威ランドスケープは規模と複雑さの両方で増加しており、それによってセキュリティ制御の使用率が高まり、数千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。アラートとインシデント トリアージのサポートおよび調査を行うには、セキュリティ チームはこのデータを集約、相関、分析する必要があり、多くの場合でこの作業には膨大な手動処理が必要となります。しかし、アラートとセキュリティ データの収集および分析以外にも、さらに多くの処理が必要です。

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およびリスク 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るために、全体的なプログラム運用を再考しています。例えば、ドメイン管理認証情報の盗難は、短期的にも長期的にも、組織の運用、財務、ブランドの評判に悪影響を及ぼす可能性があります。

セキュリティ リーダーが戦略を再考する際、より戦略的なセキュリティ活動に社内リソースを再投入するにつれて、日々の運用活動をサード パーティーにオフロードする組織が増えています。内部セキュリティ リソースはセキュリティ運用プロセスの再設計に重点を置いており、MDR サービス プロバイダーはインシデントの検出、トリアージ、対応を処理し、ダメージを防ぎ、潜在的なビジネス ディスラプションを制限するための迅速な措置を講じています。

プログラム開発全体に関するガイダンスを MDR プロバイダーに求める組織もあり、結果を最適化するために、専門家や実績のあるセキュリティ運用プロセスを取り入れています。

また、XDR の動きによって検出および対応プログラムのモダナイズに必要なビジョンとロードマップがさらに生まれることで、XDR グレードのソリューションの実装を支援するために MDR プロバイダーの活用を求める組織もあります。

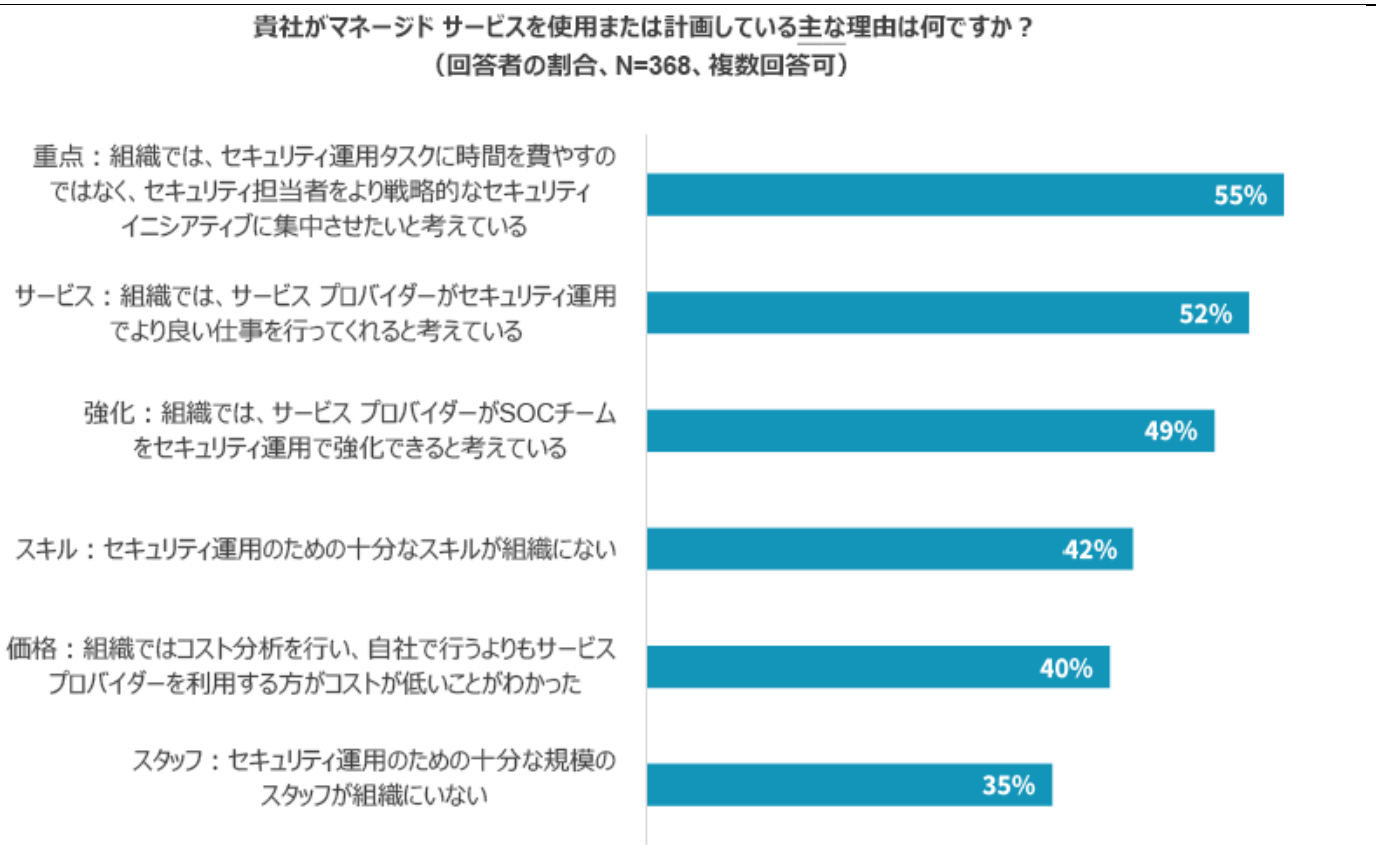
MDR のユース ケース

多くの MDR プロバイダーが幅広いセキュリティ サービスを提供しており、アラートの監視、トリアージ、調査を行う中核的な検出および対応サービスでは、多くの場合、早期のエンゲージメントが開始されます。運用モデルは MDR プロバイダーによって異なるため、セキュリティ リーダーは個々の組織の要件を、具体的な目標を達成できる MDR プロバイダーと慎重に調整する必要があります。例えば、一部のセキュリティ リーダーはセキュリティ運用を完全にアウトソーシングすることを選択し、MDR プロバイダーと連携して、攻撃対象の完全なカバレッジ、脅威の監視、修復を提供しています。このモデルでは、MDR プロバイダーは多くの場合、サービスを提供するために必要なテクノロジー スタック、プロセス、セキュリティ エキスパートを提供します。MDR サービスを社内のセキュリティ運用機能の拡張として利用し、主にテクノロジー スタックと運用プロセスを担当する社内チームに、営業時間外の保証やセキュリティ エキスパートを追加する組織もあります。これらの例は、MDR サービスが利用されている多くのユース ケースのうちの 2 つにすぎません。

したがって、MDR は「万能な」ソリューションではありません。代わりに、多くの場合、個々の組織のニーズに適用できるカスタマイズ可能な機能のセットとして表されます。

さまざまな組織が、社内のリソースとスキルに応じて、検出と対応のさまざまな面で MDR パートナーを選択するでしょう。ESG の調査によって明らかになった主な理由を図 3 に示します。

図 3：組織が MDR パートナーを選択する理由



出典：TechTarget, Inc.の一部門である ESG

MDR エンゲージメントの主な価値促進要因

セキュリティ プログラムの開発では効率性と有効性の両方に重点を置く必要があり、MDR サービスはそれぞれにプラスの影響を与える可能性があります。

- **運用の改善と効率性。**MDR 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の総コストを削減するのに役立ちます。また、「アラート対応の煩わしさ」の問題に対処したり、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。

モダンな MDR ソリューション プロバイダーに求められること

一般的に、MDR ソリューションは新しいものではありません。実際、これらのソリューションはしばらくの間、成功を収めることにおいて優れた実績を確立してきました。しかし、多くの「第 1.0 世代」の MDR ソリューションは、データの削減、脅威の低減、検出のシ

ンプル化など、さまざまな時代に対応するように設計および実装されました。次世代の MDR ソリューションとこれらを導入および管理するサード パーティーは、検出と対応がこれまで以上に重要で困難になる、より広範で深く複雑な一連の課題を考慮する必要があります。

MDR ソリューションを評価する場合、組織は次のような機能を求める必要があります。

- イベントとログの 24 時間 365 日のモニタリング、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の生成。
- 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。
- 豊富なテレメトリー。
- 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。
- 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を備えた、クラウドベース MDR への長期的な取り組み。
- 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。

MDR に対するデル・テクノロジーズのアプローチ

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、デル・テクノロジーズのグループ企業である 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全体にわたって完全に調査された脅威を検出、分析、処理して、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 のパワーは、Dell の大規模なセキュリティ アナリストおよびエンジニア グループの専門知識とスキルを通じて最大限に活用されます。このグループの知識には、既知の脅威と未知の脅威の両方から組織を保護するために数十年にわたって培った専門知識が含まれています。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。その大部分は、継続的に更新される脅威インテリジェンス データベースによって実現されます。また、Dell Managed Detection and Response は、攻撃者の行動を監視、分析、特定して、平均検出時間と対応時間を短縮します。

サブスクリプションベースのマネージド サービスとして構成および導入される Dell Managed Detection and Response は、より多くの脅威、攻撃、アラートに対処できるようにするために、組織がセキュリティ 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、組織の内部機能を効率的かつ効果的に補完し拡張します。その結果、社内の SecOps 担当者は、他のセキュリティ関連タスクにより多くの時間とエネルギーを集中させることができます。

成功事例：MDR は実際にどのように機能するか

ESG は、Dell MDR のお客様の IT リーダーやセキュリティ リーダーと話し合い、特定のユース ケース、運用モデル、成果に関するインサイトを得ました。

例 1：中規模の地方自治体

地方自治体の IT およびサイバーセキュリティ リソースが民間企業に匹敵することは稀ですが、同じような問題に直面しないわけではありません。この例では、米国南東部にある中規模の郡が、増え続けるセキュリティの脅威に立ち向かい、克服するだけでなく、厳しい制約の中で支出を維持することにも苦労していることを取り上げます。

新任の IT ディレクターが採用されたとき、彼は直ちに、小規模なチームが直面している増大する脅威ランドスケープを認識し、検出および対応機能で潜在的な脆弱性を発見しました。「私たちのセキュリティ体制は不十分ですが、人件費を増やさずに能力を拡張できるようにする必要がありました。これは、経営陣の意思決定者にとって非常にセンシティブな課題です」と彼は述べています。「ですが、脆弱性に対処する必要性を指摘しながら、財政的な節約に対する彼らの懸念に対して訴えることができたと思います。」

彼はまず、郡の現任のエンドポイント セキュリティ ベンダーを評価し、その後で、検出と対応の改善に対処するために、ソフトウェア アップグレードの 90 日間の「無料トライアル」を宣伝しました。しかし、ニーズに合った機能がソフトウェアにないことや、ベンダーのコミュニケーションが期待に沿っていないことがわかり、より包括的な MDR ソリューションを採用することに決めました。

「幸いなことに、仮想 CSO（最高セキュリティ責任者）の提供に Dell を手配していたため、郡のリーダーは、この場合の検出と対応に対してマネージド サービス アプローチを取ることのメリットを認識していました。」彼は、Dell のチームが、郡で配備していた小規模な組織内セキュリティ チームと IT プロフェッショナルの代わりではなく、彼らを補完する役割を果たしていたと付け加えました。「彼らは私たちのチームの延長にいる存在であり、スタッフと非常にシームレスに協力してくれました。」

この手配の真のメリットは、この郡を含め幅広い組織で使用されている一般的なプラットフォームである Microsoft Exchange の Web メールが世界的なハッキング キャンペーンのターゲットとなった際にすぐに明らかになりました。「Microsoft は攻撃を発見した直後にパッチを開発して送信しましたが、攻撃に対するゼロ デイはおそらく 1 か月前でした」と郡の IT ディレクターは述べています。「営業時間外に Dell の仮想 CSO から連絡を受け、Dell MDR チームが対応に参加しました。サーバーをチェックするためのスクリプトが送信され、サーバーの 1 つが侵害されたことがすぐに分かったのです。」

「Dell（および Secureworks パートナー）は、何を実施しているかを本当に理解していました。1 日に 2、3 回、毎日、侵害の試みに対処する期間の間中連絡がありました。」彼は、インシデント対応チームが郡の担当者と調査結果を確認し、コード スニペットやその他の侵害の兆候と侵害の証拠を示していたと付け加えました。

最終的に、侵害の試みの潜在的な影響に対処するだけでなく、より広範な視点と期間にわたって郡のサイバーセキュリティ プロファイルを強化した、技術的および技術以外の推奨事項が数多く提供されました。

「私たちの経験から言えることは、強化された検出と対応を求める場合、EDR ソフトウェアをアップグレードするための安価な方法を求めるのではなく、以前にこのような経験をしている信頼性と実績のある信頼できる MDR スペシャリストを見つけるべきだということです」と彼は述べています。「侵害の試みがあった後だけでなく、定期的に彼らと協力する中で、私たちの安全を守るために取り組んでくれる良いチームがいることに安心したことを覚えています。」

例 2：中規模学区

学区はこれまで、IT 全般、特にサイバーセキュリティへの投資が不足しています。しかし、学区に対するランサムウェアやその他のサイバー攻撃が増加する中、地域の公的機関の職員は、より高い信頼性と手頃な価格で脆弱性から保護することができないか模索していました。

例えば、米国のとある中規模学区がランサムウェアによる攻撃を受け、テクノロジー主導の運用全体がシャットダウンされたことが明らかになりました。8,500 人の学生とスタッフが 21 の施設に分散しているため、学生とスタッフの 11,000 台以上のデバイスに接続された、100 台の物理サーバーと別の 63 台の仮想サーバーを含む、合理的な規模の IT プロファイルを導入していました。明らかに、この学区には攻撃者にとって多くの潜在的なエントリー ポイントがあり、迅速に対処できるパートナーを必要としていました。

ランサムウェア攻撃が実際に発生し、すぐに対処が必要であることがわかった後、学区の IT チームは Dell Managed Detection and Response に連絡しました。「攻撃の 2 日目までに、Dell から 10 人の人材が派遣されました」と同学区の IT ディレクターは振り返ります。「私たちは Dell のチームと非常に信頼できる関係を築き、すぐに担当してもらいました。」

幸いなことに、その結果は学区にとってプラスの結果でした。「システム内の 600 万個を超えるファイルのうち、失われたファイルは 6 つだけでした」と IT ディレクターは述べています。「攻撃者による金銭的な被害はまったくありません。私たちはランサムウェアを乗り切り、安全に業務を続けることができた実例と言えます。」

「Dell との連携は良い経験でした。私たちのオンサイト セキュリティ アナリストは、Dell の担当者と話をした後は常に満足しており、Dell と協力して Managed Detection and Response で対処する前と比べて、現在の体制は 95%向上しています。」

総括

ダメージを与えるサイバー攻撃のリスクが高まるにつれて、コア ビジネス目標からマインドシェアと予算が奪われるため、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、ほとんどの組織が、MDR サービス プロバイダーを活用してプログラムを成長および拡張しています。

MDR サービス プロバイダーは、セキュリティ エキスパート、実証済みのプロセス、拡張性に優れた導入しやすいセキュリティ テクノロジーなど、成功するセキュリティ プログラムを構築するうえで認識される多くの課題を克服する道筋を提供します。

デル・テクノロジーズは、組織が脅威をほぼリアルタイムで検出して対応できるように、緊密に統合されたテクノロジー、経験豊富なセキュリティ エキスパート、ベスト プラクティスを組み合わせました。このホワイト ペーパーの事例に示されているように、デル・テクノロジーズは、さまざまな業界やリソース プロファイルにわたる幅広い組織が、企業全体への新たな脅威の影響を阻止できるよう支援しています。

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