DELL Technologies

ホワイトペーパー

# DELL MANAGED DETECTION AND RESPONSE

# 中小組織に適した包括的な管理型セキュリティ ソリューション

## 概要

企業を標的としたサイバー攻撃が増加傾向にあります。2021年におけるFBIのInternet Complaint Centerの報告によれば、攻撃件数は前年比で69%増、被害総額は42億米ドルにも上っています。[1]大企業に対する攻撃は大々的に取り上げられますが、その実、規模を問わずあらゆる企業が攻撃への脆弱性を抱えています。中でも攻撃のリスクが高いのは、大企業ほどの大規模なリソースを持たないスモールビジネスです。

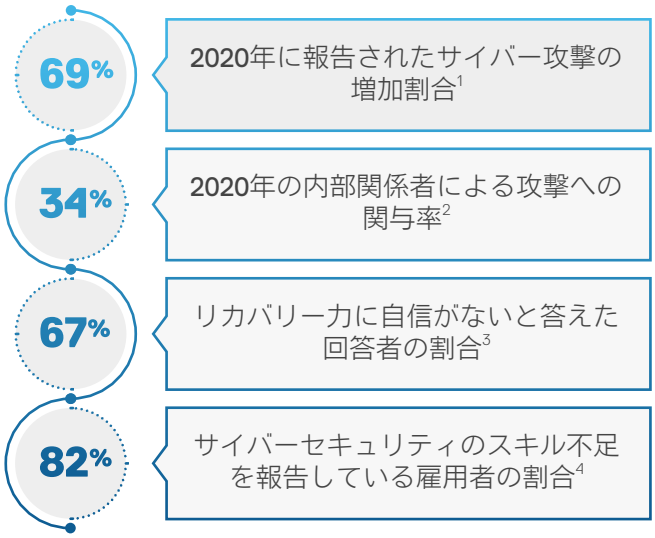
データ資産、業務、ビジネス継続性を保護するには、サイバーセキュリティが欠かせません。多くの大企業では、最新のテクノロジー、手法、インテリジェンスを備えた専任のセキュリティ チームを配備しています。しかし、中小企業ではセキュリティの専門家が1人か2人しかいないケースも見られます。そして、わずかこれだけの人数で、複雑化し続ける数々のセキュリティ アプライアンスやソフトウェア ツールの管理と運用をするように求められているのです。

### 難化し続けるIT課題

エンドポイント、サーバー、アプリケーション、ネットワーク、クラウドが猛攻撃を受ければ、膨大な量のアラートが生成され、瞬く間にセキュリティ チームやITチームでは対処しきれなくなっていまいます。そのうえ、攻撃者の手法は進化を続けており、昨日までは有効だった防御策も今日には巧妙に破られてしまいます。2020年代にIT環境を適切に保護するためには、専任のエキスパートが24時間365日通してモニタリングと対応を続けなくてはなりません。

とは言え、中小企業のITリーダーがサイバーセキュリティに十分なIT担当者と予算を当てようとすれば、アプリケーション開発やDevOpsといった重要な領域に負担が生じるでしょう。現代のサイバー攻撃から自社を保護するには人材、ツール、業務への投資が不可欠ですが、ほとんどの企業にそのような余裕はとうていないというのが実情です。

## サイバー攻撃の脅威はかつてないほど高まっている




### 解決の鍵は管理型の検出対応サービス

こうした背景を受け、外部サービス プロバイダーの管理型検出対応(MDR)ソリューションの検討を進める企業が増加しています。では、IT導入決定者の立場から、優れたMDRパートナーを見分けるにはどうすればよいのでしょうか？

有望なMDRソリューション プロバイダーを見分ける鍵は実装するテクノロジーです。テクノロジーが、既知のタイプの脅威を検出し、偽陽性を最小限に抑え、イベント間の関係を見出し、侵入者の活動順序を追跡し、封じ込めおよび防止の措置を自動化できるものでなくてはなりません。さらに、24時間365日通してアラートの分析と脅威の修復に対応するとともに、新しいタイプの脅威を探し出すために、スキルも経験も豊富なセキュリティ専門チームが必要です。

MDRサービスを提供するには、セキュリティ業務を構築し、プロセスの確立と改善を行わなければなりません。さらに、アナリストには知識と共有ツールを備え、脅威と手法の最新事情に通じるために定期的なトレーニングを受けることも求められます。

管理型の検出対応サービスを喧伝するサービス プロバイダーは数多くありますが、素晴らしいサービスを提供できるだけの能力と手腕を備えているプロバイダーはごくわずかです。

**Dell Managed Detection and Response**はエンドツーエンドかつ24x7対応のフル マネージド ソリューションであり、組織のIT環境全体にわたって脅威を監視、検出、調査、対応します。Dell MDRはエンドポイント数が50個から数千個までの企業に対応しており、IT担当者の負担を減らしながら社内のセキュリティ体制を短期間で大きく高められます。また、Dellが持つ人材、プロセス、ツールへの投資力を活かして、中小企業でも大企業並みのモニタリングと対応を実現できます。

### 管理型の検出対応(MDR)ソリューションを企業が採用する主な理由

- **雇用の難しいサイバーセキュリティ スペシャリストを利用できる**
- **モニタリング、検出、対応の範囲が網羅的**
- **IT担当者の負担を減らし、DevOpsに専念させられる**

## 脅威の現状

昨今の攻撃者は入念であり、数週間ないし数か月をかけて、貴重なアプリケーションやデータへのアクセスを取得する方法を検討しています。そして機会を見つけると、抜け穴の悪用や、ユーザーに不正な添付ファイルを開かせるフィッシングEメールの送信を行います。包括的なサイバーセキュリティ プログラムを実現するには、従業員のトレーニング、サイバーセキュリティ評価、脆弱性テストと侵入テスト、耐久性とリカバリーの計画策定と並んで、検出と対応が不可欠な要素なのです。

アクセスを取得した攻撃者は、まず、攻撃範囲を広げるための拠点を築こうとします。この時にも、攻撃者はゆっくりと時間をかけて、企業のインフラストラクチャ内に陣地を確保します。たとえば、多くのランサムウェア攻撃では、ビジネス システムへの攻撃に加えて、企業のバックアップ システムをオフラインにしてバックアップへのアクセスを遮断しようとします。こうすれば、企業はリカバリーを行えなくなり、ビジネスの継続のために身代金を払うしかなくなるからです。

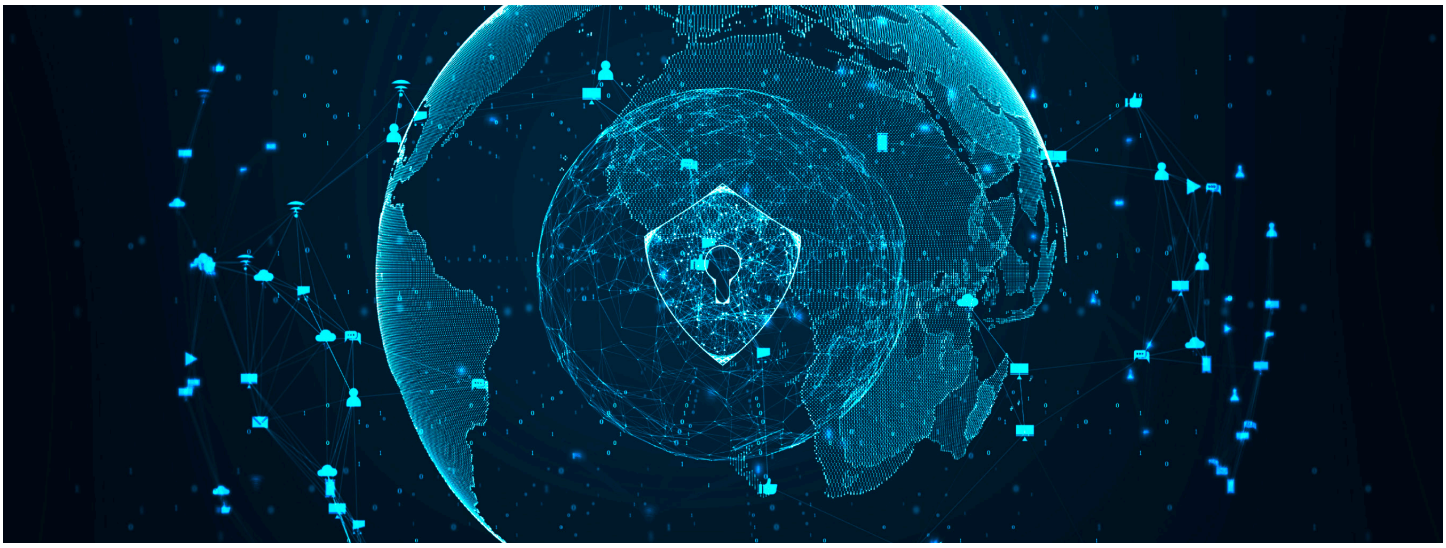
攻撃や他の手がかりを認識するには、常時更新され続ける高度な検出対応機能が欠かせません。企業が早期に警告を受け取ることができれば、攻撃の拡大前に被害を抑えるチャンスが生まれます。

組織に導入されているサイバーセキュリティ ツールは、パスワード監査やネットワーク テスト、脆弱性検査、暗号化、モニタリング、脅威検出など多岐にわたり、IT担当者にはこれらすべてのツールからアラートが届きます。膨大な量のアラートへの対応は至難の業であり、ツール全体のイベント間の関係性を見出そうとすればなおさらです。さらに、ITセキュリティ担当者がこうしたあらゆるテクノロジーについて熟練し続けるためには、多大な時間を掛けなくてはなりません。

MDRの人的側面では、長年にわたるサイバーセキュリティの経験と、システム管理、サイバー フォレンジック、脅威調査、侵入テストなどのスキルを持った専門家集団が求められます。こうした専門家は探しづらく、雇用にお金がかかるうえに、知名度が高く資金の多い組織に絶えず採用されているものです。2021年のCIO（最高情報責任者）の最新状況に関する調査によれば、全IT職の中で最も雇用の難しい職種はサイバーセキュリティ職であるとされています。[5]ITリーダーにとって、セキュリティ アナリストの維持と退職したアナリストの穴埋めは、果てのない戦いなのです。

そのうえ、重要なツールと人材を獲得できたとしても、24x7体制のセキュリティ業務と施設を構築しなければなりません。

**図1. 攻撃者の戦略**



## Dell Managed Detection and Responseサービスなら、手頃な料金で最上層の機能が手に入る

多くの中小企業が適切な保護体制の構築に苦戦しているのも、不思議ではありません。今やサイバーセキュリティの領域は、絶えず変わり続ける複雑多彩な脅威のるつぼ。業務の激増によって求人要件が膨らみ、攻撃の複雑さから求める人材のレベルも高まっています。

Dell Managed Detection and Responseであれば、貴社のセキュリティ チームを拡充し、大手グローバル企業と遜色のないサイバーセキュリティの専門家、ツール、運用能力を揃えられます。ITチームの負担を減らしつつリスクを抑え、社内のセキュリティ体制を著しく高めることで、ビジネスの優先事項に注力できるようになります。

Dell Managed Detection and Responseには、テクノロジー、専門技術、運用のすべてが一体となって組み合わされています。このサービスでは、長年にわたり世界中の企業に保護の強化を支援してきたデル・テクノロジーズのセキュリティ アナリストならではの知識を活用できます。さらにDell MDRでは、高度なセキュリティ分析ソフトウェア プラットフォームであるSecureworks® Taegis™ XDRを採用しています。このプラットフォームは、20年以上にわたる巧妙な脅威の検出と対応の取り組みから得られた確かなノウハウ、現実世界における脅威インテリジェンスと研究、専門知識の結晶です。

### Secureworks Taegis XDR

Secureworks Taegis XDRは、セキュリティ分野にビッグデータ規模のソリューションをもたらすクラウドネイティブの特化型サイバーセキュリティ プラットフォームです。さまざまな攻撃元区分のテレメトリーとイベントに網羅的な脅威情報を組み合わせ、機械学習およびディープ ラーニング主導で継続的に評価を行います。

## Dell Managed Detection and Responseを選ぶ理由

### 要員

- 経験豊富なサイバーセキュリティ専門家
- Taegis XDR認定アナリスト
- CEH、GIAC、SANS、CISSP、CompTIAなどの認定も取得済み

### テクノロジー

- 業界をリードするセキュリティ分析基盤、Secureworks Taegis XDR
- 広範囲のエンドポイント、ネットワーク、クラウドから収集したテレメトリーを基にエンドツーエンドで継続的に脅威をモニタリング

### プロセス

- 問題の解決にかかる時間が短い
- 24時間365日対応
- エージェント導入支援が付属
- 四半期ごとに40時間のリモート修復ガイダンス
- 年間40時間に及ぶインシデント対応研修

### 信頼されるパートナー

- デバイスとインフラストラクチャのサポートで世界中から厚い信頼
- ビジネス耐久性のイノベーションで20年以上の実績
- 人材、プロセス、ツールに継続的に投資している

図2. Threat Intelligence


巧妙な攻撃を特定し対応する唯一の手段は、まず攻撃者の脅威の程度とその動機を知ることです。SecureworksのXDR担当チームが年間に実施しているインシデント対応活動はおよそ1,000件。そのため同チームは、他社にはない立場から、クライアントのビジネスに効率よく侵入するための攻撃者の戦略、手法、プロセスが定期的に変化する様を観察できています。

Taegis XDRでは、エンドポイント、ネットワーク、クラウド システム、オンプレミスのビジネス システムから収集したセキュリティ面で重要なデータを分析し、脅威を検出します。既存のセキュリティ インフラストラクチャを補完する完全にオープンなプラットフォームなので、保護を包括的に展開するとともに、従来の投資も保護できます。

Taegis XDRには対応、修復、インサイトの自動化機能が備わっており、セキュリティ業務の効率化を高めるとともに、脅威発生時に措置を講じるうえで必要な可視性を対応チームに提供できます。世界中の顧客および共有インテリジェンス サービスから数十万に上るデータ ポイントを収集し、開発されたThreat Intelligenceを利用できることが、Dell MDRのメリットです。

## お客様専任の一流セキュリティ専門チーム

高度なトレーニングを受けたセキュリティ アナリストで構成されるグローバル チームが、お客様のシステムで生じるトラブルを常時見張ります。Dellの熟練のサイバーセキュリティ専門家は、脅威の調査、脅威ハンティング、エンドポイント セキュリティ、インシデント対応、リカバリーなど、脅威検出と緩和におけるあらゆる段階の経験を積んでいます。また、DellのアナリストはXDR認定を受けており、CEH、GIAC、SANS、CISSP、CompTIAなどの国家資格や業界認定資格も取得済みです。さらに、Dell MDRのセキュリティ オペレーション センターは「フォローザサン」型の分散体制であり、365日年中無休で運営されています。

Dell MDRチームの活動の始まりは、お客様の社内業務とITインフラストラクチャを把握することです。XDR経由で提供される数千のIT環境から収集した脅威情報と機械学習を組み合わせて、お客様の環境を監視します。警告が表示されると即座に行動を開始。アラート データを調査して、トレーニングと経験を積んだセキュリティ アナリストにしか見つけられないつながりやパターンを探り出します。そして、調査結果を踏まえ、お客様の対応チーム メンバーに最善の対応方針をお伝えします。

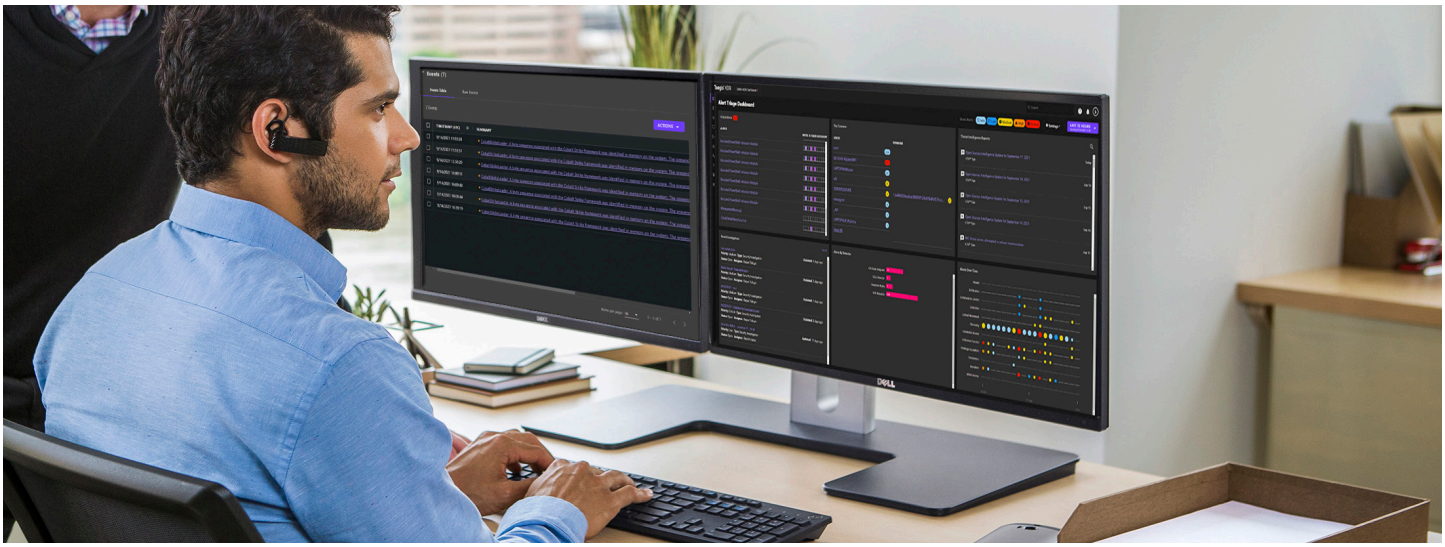
Dell MDRは、Dellが数十年にわたり実施している、世界レベルのITサービス組織を作り上げる取り組みの一環です。すなわち、Dell MDRのサイバーセキュリティ専門家は、脅威の修復方法について優れたサポートができるだけでなく、あらゆる組織に通用する脅威管理のスキルとノウハウも備えています。

## 脅威ハンティング — 自動システムでは検出できない脅威を特定

自動検出システムの存在は攻撃者にも把握されており、こうしたシステムをくぐり抜けるための新しいタイプの攻撃や既存タイプの攻撃のバリエーションが生み出されています。Taegis XDRのようなシステムについても、この種の回避策は容易ではないものの不可能ではありません。

このような「ステルス型」の脅威を特定するためにセキュリティ アナリストが採用している手法が、侵害の徴候を調べる脅威ハンティングです。徴候の一例としては、アカウントへのログインが複数回連続して失敗してから成功している、通常の営業時間外など普段とは異なるログインが行われている、短期間にファイルの変更が繰り返し行われている、といったものがあります。

脅威ハンティングを効果的に実施するには、テクノロジーと人の連携が欠かせません。Taegis XDRプラットフォームでは、侵入者の活動について膨大な詳細情報が得られます。Dell MDRのアナリストはこうした詳細情報をくまなく調査し、巧妙に隠された活動さえも明らかにします。



## DELL MDRにご相談ください

政府や国際企業によるサイバーセキュリティの脅威の封じ込めがニュース メディアを賑わせています。中小企業のみなさんは、もうこのような脅威に自社だけで立ち向かう必要はありません。Dell MDRなら、お客様を専任で保護する熟練のセキュリティ エキスパートと、業界をリードするセキュリティ プラットフォームのSecureworks Taegis XDRをご利用いただけます。また、Dellならではの人材、プロセス、ツールへの投資力を活用し、お客様の組織のニーズに合った管理型セキュリティ サービスを組み立てられます。世界レベルでありながら、どなたでもご利用いただけるサイバーセキュリティ サービス。それがDell Managed Detection and Responseです。

Dell MDRの詳細は
こちらをご覧ください

Dell MDRエキスパートに
ご相談ください

1. FBIへの攻撃が69%増加：https://blog.isc2.org/isc2_blog/2021/03/fbi-cybercrime-shot-up-in-2020-amidst-pandemic.html
2. 34%で内部関係者が関与：https://www.verizon.com/business/resources/reports/dbir/
3. 回答者の67%が破壊的なサイバー攻撃を受けた後のリカバリー力に自信がない：www.delltechnologies.com/gdpi
4. 雇用主の82%がサイバーセキュリティのスキル不足を報告している：https://www.csis.org/analysis/cybersecurity-workforce-gap
5. 採用難のIT職トップ13：https://www.cio.com/article/221772/10-most-difficult-it-jobs-for-employers-to-fill.html



DELL Technologies