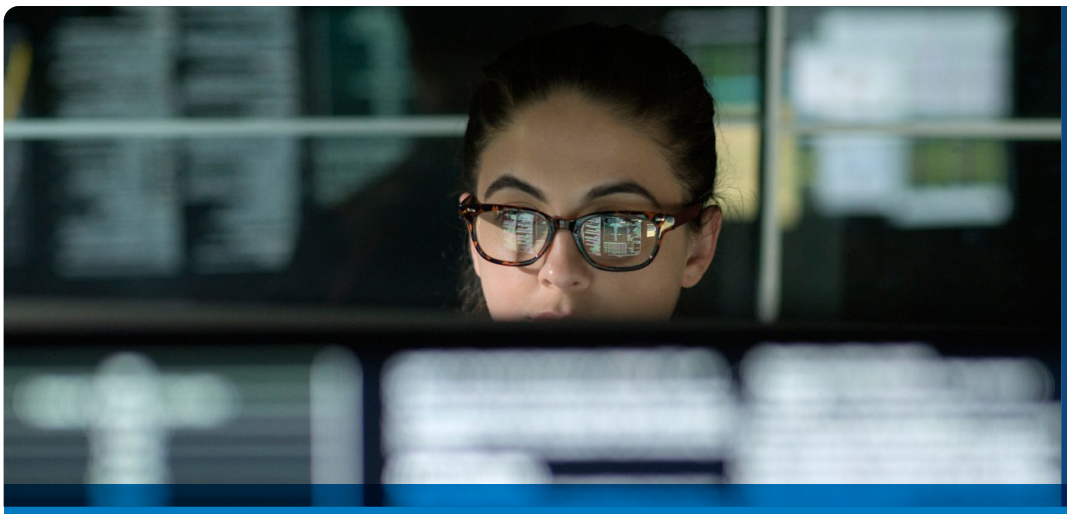
IT環境全体に対する脅威の予防と対応



脆弱性を特定し、早急な対応が必要な問題に優先的に取り組む

Managed Detection and Response Proの概要

脆弱性管理とManaged Detection and Responseを1つのソリューションに統合し、IT環境の安全確保を支援

2022年のデータ侵害に対する平均コストは435万ドルでした。[1] 実際に、2021年には約22,000件もの新たな脆弱性が明らかになっており、この数字は増加を続けています。[2] 組織は、増え続けるセキュリティの脅威と、侵害が引き起こす影響から環境を保護する方法を見つけなければなりません。

IT環境を保護するためには、脆弱性を特定して、脅威を調査し、効果的に対応することが必要です。組織は、資格を持ったセキュリティの専門家を探して確保するという課題にも直面しています。またIT組織では、重要な要求への対応や毎日のビジネス運営に労力が費やされています。

この問題を解決するために、Managed Detection and Response Proが設計されました。MDR Proは、脆弱性を特定して優先順を設定し、24時間365日の脅威検出と対応を可能にするフルマネージド型のソリューションです。当社のエキスパートが御社のセキュリティ チームと協力して、IT環境の保護、着実なセキュリティ体制の改善、脅威への防御体制を継続的に支援します。

攻撃対象全体に対する脆弱性の特定と優先順位の設定

Dellのエキスパートは、先進のテクノロジーを使用して定期的にIT環境を精査し、エンドポイント、ネットワーク インフラストラクチャ、クラウドの資産の全体における脆弱性を監視できるようにします。また、機械学習を利用して、現在悪用されている脆弱性や、近い将来狙われる可能性が高い脆弱性をピンポイントで特定します。これにより、最も高リスクな脆弱性や、重要な資産に対するパッチ適用の優先順位を設定しやすくなります。

主なメリット：

- 反復的な脆弱性スキャンと管理で、防御を最新状態に維持
- エンドポイント、ネットワーク インフラストラクチャ、クラウド全体にわたる脆弱性の詳細情報を提供
- 悪用される前に対処すべき重大な脆弱性の優先順位を設定
- エコシステム全体に対する統合された検出と対応
- 継続的に更新される脅威データベースを使用して新しい攻撃タイプを検出
- イベントを関連付け、攻撃者によるエンドツーエンドのアクティビティを追跡
- Dellのセキュリティ チームの知識と専門技術を活用

損害の発生前に攻撃者を検出して対応

Managed Detection and Responseは、IT環境全体にわたる脅威の監視、検出、調査、対応を行う、エンドツーエンドのフルマネージド型24時間365日対応のサービスです。50以上のエンドポイントを持つ組織の場合、セキュリティ体制を迅速かつ大幅に改善し、IT部門の負担を軽減できます。

このサービスでは、以下の2つの重要な能力と機能が活用されます。

- 世界中の組織がビジネスをより適切に保護できるようにサポートしてきた長年の経験から得た、デル・テクノロジーズのセキュリティ アナリストの専門知識
- 20年以上にわたって培ってきたSecOpsのノウハウ、実用的な脅威インテリジェンスとリサーチ、高度な脅威を検出し対応してきた経験を基に作成された、先進のXDRセキュリティ分析ソフトウェア

主要機能

脅威の検出と調査

- Dellパートナーと御社は環境を把握し、追加料金なしで、ソフトウェア エージェントを適切なエンドポイントに導入できるように支援
- 過去1年間で1,400件以上のインシデントに対応した経験から得た攻撃者データを活用
- 複雑な状況であっても、脅威を封じ込める手順を詳しく説明
- 四半期ごとに最長40時間のリモート修復に関する指導を実施
- 年間で最長40時間に及ぶリモートでのインシデント対応で、調査活動を迅速に開始可能

脆弱性の特定と優先順位の設定

- 毎月の脆弱性スキャンに加え、Dellのチームとお客様の話し合いで決定される追加スキャンを実施
- 資産インベントリーを現在知られている脆弱性に関するデータベースと照合して、脆弱性と必要なアップデートを特定
- 優先的に対処すべき高リスクの脆弱性についてのフィードバックを行い、パッチ適用のガイダンスを提示
- MLベースの先進的なプラットフォームを使用してスキャンを実行
- 四半期ごとにレビューを行い、お客様の環境と業界における脆弱性の傾向についてお客様に説明

Dellと協力して環境を安全に保護

データ侵害の頻度とコストは上昇を続けています。Managed Detection and Response Proは、IT環境のセキュリティを確保して、悪意ある攻撃者から最も重要な資産を保護できるように支援すると同時に、組織のセキュリティ体制を改善します。

セールス担当者にどうぞお問い合わせください。

[1]IBM。（2022年）。2022年のデータ侵害コストに関するレポート。2022年9月20日、https://www.ibm.com/downloads/cas/3R8N1DZJより取得

[2]Tenable (2021) Tenableの脅威状況のまとめ（2021年）。2022年8月、https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospectiveより取得