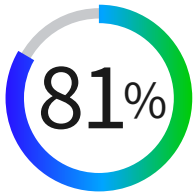
Trellix

エグゼクティブブリーフ

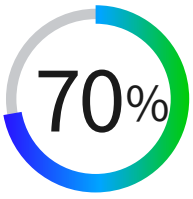
セキュリティを常に進化させるTrellix

常に変化する状況に適応できるXDRのエコシステムで、ビジネスを活性化

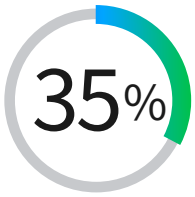
数字で見るセキュリティの状況



CISO意識調査では、回答者の81%が、「攻撃者に遅れを取ってはならない」と常に頭を悩ませています。[1]



ITセキュリティ関係者の70%が、過去5年間にセキュリティ警告の量が2倍以上になったと回答しています。[2]



セキュリティアナリストの35%は、キューがいっぱいになるとアラートを無視しています。[3]

データ侵害を特定し、封じ込めるまでの平均日数は287日です。[4]

グローバルインシデントの対応に要する時間は平均20.9時間です。[5]

現代の世界は、日々複雑化するダイナミックな脅威にあふれています。

これは組織にとって大きな難題となります。静的で縦割り型のセキュリティ手法では、常に変化する現代の脅威環境に対処できないことも少なくありません。

ダイナミックな攻撃にすかさず対処し、不安を解消するため、より一元的に可視化し、すばやくセキュリティ問題を解決することが求められています。

XDRは、Extended Detection and Responseの略語です。

- **Extended**（拡張）とは、エンドポイント、ネットワーク、クラウド、Eメール、その他のサードパーティのセキュリティ製品を含む複数のセキュリティ経路にソリューションが拡張することを指しています。
- **Detection**（検出）は、脅威が発生した瞬間に複数の経路で脅威を検出できることを意味します。
- **Response**（対応）とは、リアルタイムで効果的に攻撃に対応する態勢を整えることができることを意味しています。

次世代セキュリティであるスマートで適応可能なXDRのエコシステムがあれば、ビジネスを守ることができます。

1. State of Cybersecurity Resilience 2021, Accenture, 2021 | 2. 2020 State of SecOps and Automation, Dimensional Research, 2020 | 3. The Voice of the Analysts, IDC, 2021 | 4. Cost of a Data Breach, IBM, 2021. | 5. Voice of SecOps, Deep Instinct, 2021

既存のセキュリティソリューションでは次なる脅威への対応が不十分な理由

脅威が高度化する現在、多くの組織が攻撃を受けやすくなっている理由はすぐお分かりになるでしょう。しかし、組織が危険にさらされ続けている最大の理由は、既存のセキュリティソリューションが組織のニーズを満たしていないことにあります。

1.最近受けた脅威の解決に集中し過ぎ、次なる脅威への備えが疎かに

多くの組織は現在の脅威に対しては予防的に対応し、最新の情報を得ていますが、本当に心配する必要があるのは将来の脅威です。残念ながら、非常に多くの組織で、入ってくる攻撃を監視するのに必要な専門知識とスタッフが不足しています。さらに重要なことに、将来の攻撃を制御するための先を見据えた機能が不足しています。機械学習と人工知能を用いることで、優先すべき攻撃を特定し、意思決定を改善、問題を解決するために必要な洞察を得ることができます。

2.自動化でなく、エラーの生じやすい手作業のプロセスへの過度の依存

適切なソリューションを整えていても、多くのITチームは、セキュリティのインフラストラクチャを管理するために手動プロセスに依存することを強いられています。これにより、組織には数多くの問題、つまり非効率性が生じます。セキュリティの警告を受け取ったITチームのメンバーは、それが正当なものかを知る必要があります。正当性が不明な場合、実はまったく問題のない事象の調査に貴重な時間と資源を費やすことになりかねません。

3.セキュリティチームがすべての侵入経路とポイント製品を幅広くカバーすることが困難

多くの組織は、セキュリティソリューションを自社開発すればコストを削減できると考えています。しかし、このようなソリューションは、既製のソリューションより高くつくことが多いのが実状です。セキュリティチームはすべての脅威の侵入経路を幅広くカバーすることができず、ダイナミックに対応することもできないため、自社開発のソリューションは悩みの種となることが多く、定評と信頼のあるソリューションよりもセキュリティレベルが低いうえに手間のかかるものとなっています。

セキュリティ対策のあり方を刷新するストーリーを書き換えるTrellix

TrellixはXDR革命の最前線に立ち、検出、対応、および修復を1つのエコシステムにまとめた常に進化を続ける最新のセキュリティソリューションを革新的な方法で提供します。Trellixの革新的なXDRエコシステムには、次の特徴があります。

- 常に学習して適応するソリューションで、瞬時にデータを分析して攻撃を予測し、防止することが可能
- セキュリティ対策のオーケストレーションを自動化するため、オープンでネイティブなパートナーシップを実現することが可能
- セキュリティオペレーションの複雑さを軽減し、効率性を高めるため、エコシステムと専門家の知見でサポート

XDRへの新しい統合アプローチを体験

Trellix XDRは、エンドポイント、Eメール、ネットワーク、クラウド、その他のセキュリティ製品から成る弊社の幅広いポートフォリオとシームレスに統合します。また、サードパーティのセキュリティ製品とも容易に接続することができます。この接続性により、インテリジェントな脅威検出、分析、自動対応の機能を配備することができます。

より統合されたエクスペリエンスにより、以下を行うことができます。

すべての経路上での高度な攻撃を検出

Trellix XDRの採用により、自信を持ってセキュリティインシデントの検出ができるようになります。組織全体の多数の資産から発せられるテレメトリ情報からの洞察を明らかにし、その情報を活用して大規模な攻撃を阻止します。

攻撃の検出から脅威に対する防御へとシフト

Trellix XDRは、Eメール経由、ネットワーク経由、エンドポイントに直接行われる攻撃を阻止します。適応性の高いエコシステムを構築することにより、迫りくる脅威を予測・防止し、根本原因を特定し、リアルタイムで対応することができます。

次世代のセキュリティを運用に組み込む

Trellix XDRは、ガイド付きの調査ワークフローを提供します。また豊富なインテリジェンスを提供し、プロセスを自動化やセキュリティ上の懸念の優先順位付けを可能にします。

Trellixでビジネスを常に進化させる

未来へ邁進するためには、現在を守ることが必要です。つまり、問題が起きてから対応するだけでなく、先を見越して対応できることが求められています。自由に機会をつかめるようにすること、脅威より優位に立てるようにすることが必要なのです。

Trellix XDRは、革新的なテクノロジーと人の専門的な知見を組み合わせて、以下を実現します。

- 常に変化するグローバルな脅威状況にすばやく適応することにより、よりレジリエントなデジタル環境を生み出す
- 複数のツールで起きた別々の事象を関連付け、対応に活かすことができる洞察へと変換することにより、今日発生した脅威を明日の防御に活かす
- 自動化された攻撃検出と対応を通じて組織のリスクを軽減することにより、ビジネスの成長を支える

XDRでビジネスを進化させてみませんか？ trellix.comにアクセスいただき、ぜひ一度ご覧ください。または、弊社のXDR専門家にご相談ください。トレリックスが御社の成長をどのようにサポートできるのか、ご説明させていただきます。