kaspersky

EDR

Endpoint Detection and Response

エンドポイント保護プラットフォームを迂回できる新しい未知の回避型脅威を特定し、日常のセキュリティタスクを自動化

VS

MDR

Managed Detection and Response

非常に複雑で巧妙な非マルウェア型の脅威に対しても継続的に保護を管理

VS

XDR

Extended Detection and Response

複数のインフラストラクチャレベルにまたがる複雑な脅威をプロアクティブに検知し、これらの脅威に自動的に対応および対抗

仕組み

- 防御メカニズムを迂回する脅威の高度な検知とハンティングを有効化
- 脅威の可視化と視覚化を強化
- 根本原因分析を簡素化
- 一元的で自動的な対応が可能

- セキュリティ製品からテレメトリを収集し、システムの動作に関するメタデータをプロアクティブに分析して活動中の攻撃や差し迫った攻撃の兆候がないかを調べ、マネージド型またはガイド付きの対応を実施

- 複数のツールとセキュリティアプリケーションを統合
- エンドポイント、ネットワーク、クラウド、Web サービス、メールサービスなどのデータを監視し、複雑な脅威を検知して排除
- 複数の製品にまたがるやり取りを自動化して情報セキュリティ管理を簡素化

最適なお客様

- 手作業のタスクを削減するためにエンドポイントの詳細な可視性と一元化された対応を必要とする社内 IT セキュリティチームを抱える企業

- 検知と対応に関連する主なタスクの負担を軽減することで社内 IT セキュリティチームのキャパシティを拡大しようとしている企業
- 自社で SOC を設置するために必要な予算やスペシャリストの確保が難しい組織

以下の条件を満たす単一プラットフォームをご希望で、セキュリティが成熟レベルにある企業：

- インフラストラクチャ全体で発生している事象を一貫した全体像として提示する
- 脅威ハンティングおよび脅威インテリジェンスが組み込まれている
- インシデントの優先度付けの機能に優れ、誤検知アラートが少ない

ビジネスバリュー

- アラートを待つのではなく積極的に脅威ハンティングを行うために必要な一元的な可視化と管理をセキュリティ担当者に提供
- 様々な分析、調査、対応プロセスを自動化することで既存の IT セキュリティチームの能力を最大活用
- IT セキュリティチームが複数のツールやコンソールを使い分ける必要がなくなり作業効率が高まることでコスト効率が向上

- 複雑な脅威に対する即時保護を可能にして、サイバーセキュリティ人材不足の課題を解決
- インシデント管理プロセスをアウトソーシングすることで、コストが高い限られた社内リソースを重要な調査結果の対応に投入
- 複雑なセキュリティソリューションの導入や多くのセキュリティ専門家の雇用が不要になることで全体的なセキュリティコストを削減

- 絶えず進化する脅威に対する包括的な保護機能を提供
- エコシステムアプローチによって、関連するサイバーセキュリティツールの効率の最大化、リソースの節約、リスクの軽減を実現
- IT セキュリティスペシャリストの仕事を簡素化し、マルチベクトル型攻撃の調査に必要な追加のコンテキストを提供
- 複雑な脅威や標的型攻撃の対処では重要な MTTD と MTTR を最小化
- セキュリティテクノロジースタック全体で一元化した自動対応が可能

セキュリティの成熟度が高い組織のお客様で XDR 機能のメリットにご関心をお持ちの方は、こちらをご覧ください

Kaspersky Expert Security

詳しくはこちら