マネージドセキュリティサービス for EDR

マネージドセキュリティサービス for EDR は、お客様環境のエンドポイントを 24 時間 365 日リアルタイムで監視し、不審な動作の通知、セキュリティアナリストの知見を活かしてログの分析を行い重大なセキュリティインシデントからお客様の情報資産を守ります。

EDR運用時のこんな課題を解決・サポートします！

- リモートワークで生じるセキュリティリスクに対応したい
- すでにMDEを導入しているが、どう活用してよいか分からない
- 次々と出てくる新たな脅威に対して、リアルタイムかつ迅速に対応したい
- セキュリティ運用監視の代行を依頼したい

EDRとは？

EDR (Endpoint Detection and Response) とは、エンドポイントを、**リアルタイムでモニタリング**することでサイバー攻撃による被害を防ぐサービスです。

サービス概要

名称	マネージドセキュリティ サービス for EDR
対象の製品	Microsoft Defender for Endpoint
サービス提供時間	24 時間 /365 日

マネージドセキュリティサービス for EDRで実現できること

アラート/インシデント通知

検知後に MDE の自動調査が走り、「悪意ある挙動」と判定された場合、そのプロセスを停止し検出されたファイルが検疫されます。
また、SOC でも解析を行い、重要アラートと判定した場合、お客様へ通知いたします。

アラート/インシデント分析

アラートの通知後、分析が必要となった場合には、セキュリティアナリストが分析を行い、分析結果についての内容をメールでご報告いたします。

チューニング作業

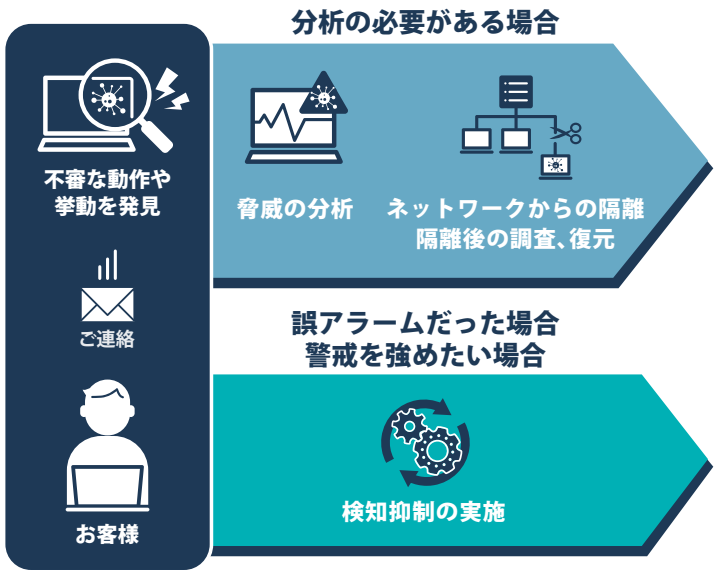
挙動（行動ログ）をベースにした検知抑制を実施
ご依頼をベースに、検知されたアラートを基に検知抑制を行います。

アラート発報の許可 / 不許可の適用作業
ご依頼をベースに、アラート検知の設定作業を実施します。

エンドポイントの論理的な隔離

ネットワークからの論理的な隔離
ご依頼や事前の取り決めに基づいて、リモートから管理デバイスをネットワークから隔離することが可能です。

隔離実施後の調査
隔離後も、継続しての調査、ネットワークへの復帰も実施できます。



お問い合わせ

株式会社クレスコ
〒108-6026
東京都港区港南 2-15-1 品川インターシティ A 棟 26 階
TEL03-5769-8080　URL https://www.cresco.co.jp/
https://wakuwaku.cresco.co.jp/contact

CRESCO