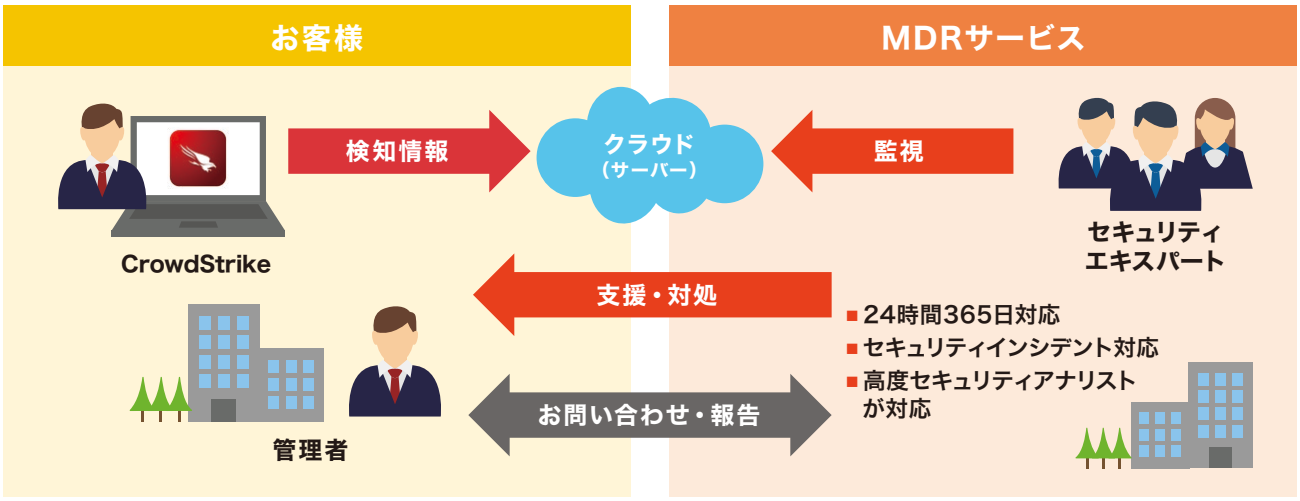
HITACHI
Inspire the Next

外部脅威対策の運用サービス

MDRサービス for CrowdStrike

セキュリティスペシャリストが外部脅威対策の運用をサポートします。
CrowdStrike*1の分析結果をもとにインシデントの監視を行い、
インシデント発生時にはエンドポイントの隔離といった初動対応や、
横展開でマルウェア感染した端末も含めた脅威除去対応などを実施します。
これにより、管理者の業務負荷を軽減すると同時に、
高度で安心なセキュリティ対策を実現できます。

MDRサービス*2 for CrowdStrikeは、CrowdStrikeの運用から対策までのサイクルをワンストップで提供



監視から対策までワンストップで提供

インシデントの監視から対応までワンストップで提供。
セキュリティエキスパートが支援します。

24時間365日体制でサポート

インシデント発生時は、アラート解析により危険度を判定し、
対応が必要な脅威の場合は封じ込めなどの対処まで実施します。

アラートの原因となった脅威を除去し、復旧を支援

アラートの原因となったマルウェア本体だけでなく、そこから派生した
ファイルやレジストリキーの除去などの対応を徹底して行います。

情報セキュリティ担当者の負担を軽減します

＊1　CrowdStrike：CrowdStrike社のエンドポイントセキュリティ製品
＊2　MDRサービス：Managed Detection and Responseの略。外部脅威対策の運用として、インシデント対応などを支援するサービス

サービスメニュー

製品導入 → ❶監視 → ❷初動対応 → ❸復旧支援 → ❹調査

運用フェーズ	サービス内容
❶ 監視	24時間365日イベントを監視し、アラートを解析することにより危険度を判定し、具体的な侵害状況や早期対応に必要な情報を通知
❷ 初動対応	アラート発生時にエンドポイントのネットワーク隔離を実施
❸ 復旧支援	マルウェアの駆除など、エンドポイントに残存する脅威の除去作業を支援 再発防止策の案内および作業の代行*3 *3 プロセス停止、レジストリ修正、ファイル削除、ブラックリスト・ホワイトリストへのハッシュ値登録
❹ 調査	検知・対応したアラートの情報や、組織内に侵入・潜伏している未検知の脅威に加え、脆弱性などの情報を調査し月次レポートにて報告

CrowdStrike について

CrowdStrikeは、既知・未知のマルウェアやファイルレス攻撃といった脅威に対して、AI（機械学習）や振る舞い検知を用いた自動検知・防御はもちろん、万が一侵入された場合の調査分析・迅速な対処までトータルで対応可能なエンドポイントセキュリティ製品です。
CrowdStrike社のセキュリティの専門家が24時間365日体制で脅威を監視する強力なサポート体制もあり、安心してご利用いただけます。また、端末の脆弱性情報の可視化や未管理端末の洗い出しができる資産管理など、機能も豊富です。さらに、クラウドサービス利用状況の可視化・制御を行う製品や、メールセキュリティ製品など、さまざまな製品と連携可能なため、幅広い活用を実現します。

万が一侵入された場合の
調査分析・迅速な対処までトータルで実現

- アラート情報や端末内でのプロセスの可視化により、複数端末への脅威の拡散状況を把握
- リモート操作による感染端末のネットワーク隔離や危険なプロセスの停止
- インシデントの対応優先順位付けや企業全体の脅威レベルのスコア表示

- AI（機械学習）による検知、振る舞い検知により、既知・未知問わずマルウェアやファイルレス攻撃を高精度に検知
- プロセスインジェクションや、認証情報を搾取するような振る舞いなど、幅広い攻撃を自動で防御
- 専門家による24時間365日の監視

ご提案から導入まで、日立ソリューションズがワンストップで支援します。
また、お客様環境下での無償トライアルのご利用も可能です。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/security/sp/solution/task/mdr_crowdstrike.html

S22S-03-00 | 2023.01