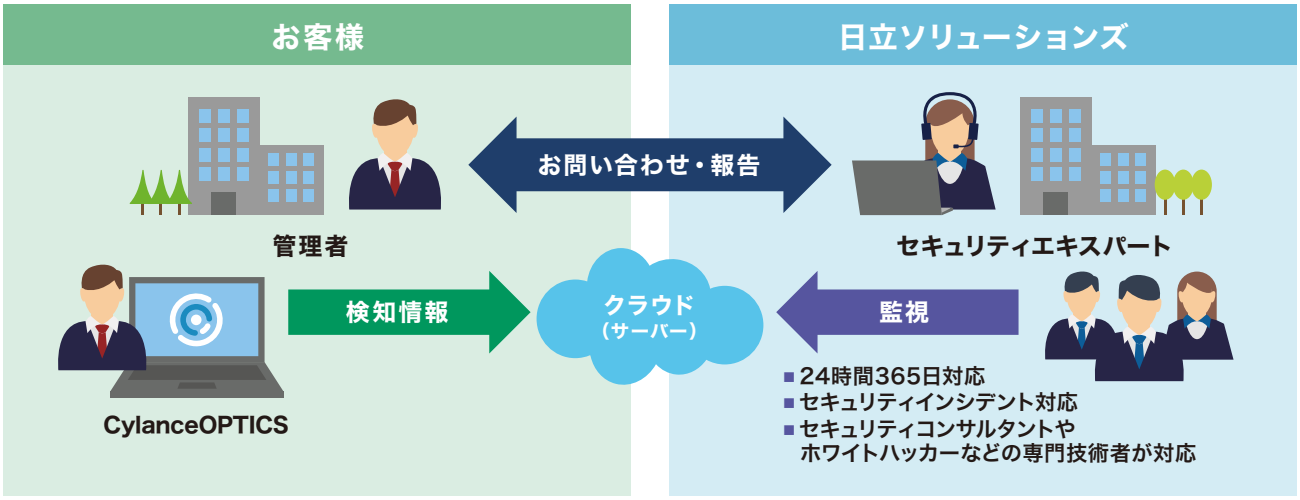
HITACHI
Inspire the Next

外部脅威対策の運用サービス

MDRサービス for BlackBerry®

セキュリティコンサルタントやホワイトハッカーといった専門技術者が
外部脅威対策の運用をサポートします。
CylanceOPTICS®*1の分析結果など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端末のフォレンジック調査や、
オンサイトでの対応方針策定などを支援します。
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 BlackBerryは、CylanceOPTICSの運用から対策までのサイクルをワンストップで提供



運用から対策までをワンストップで提供

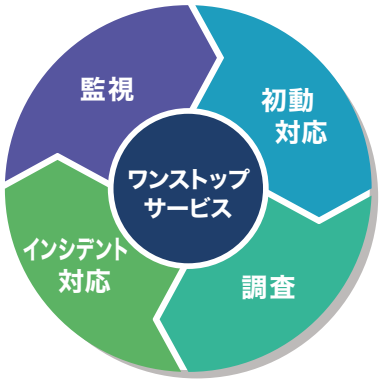
インシデントの監視から対応までワンストップで提供。
セキュリティエキスパートが支援します。

24時間365日体制でサポート

インシデント発生時は、遠隔操作で感染端末をネットワーク隔離するなど、
迅速な初動対応を行い、被害を低減します。

マルウェアの侵入経路や影響範囲のレポートを提供

マルウェアの侵入経路や影響範囲などを、セキュリティエキスパートが
調査・分析し、レポートでご報告します。



情報セキュリティ担当者の負担を軽減します

＊1 CylanceOPTICS：次世代マルウェア対策製品 CylancePROTECT® のオプション機能。脅威の可視化、分析、調査、迅速な対応を実現
＊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

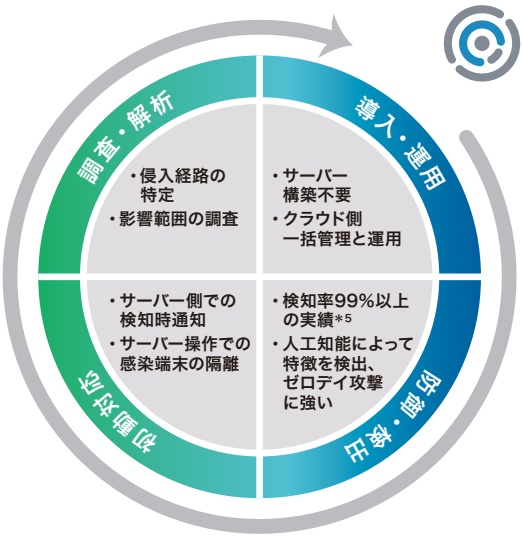
製品導入 → ❶監視 → ❷初動対応 → ❸調査 → ❹インシデント対応

運用フェーズ	サービス内容
❶ 監視	脅威イベントを監視して報告
❷ 初動対応	脅威イベント検知時に必要な初動対応を代行 ・端末のネットワーク隔離 ・セキュリティエキスパートによる状況確認や、対策方針の策定
❸ 調査	マルウェアの侵入経路や、潜伏範囲を調査して報告 セキュリティエキスパートによる詳細な被害調査を実施 毎月の運用レポートを作成・報告
❹ インシデント対応	端末のフォレンジック調査や対応方針の策定支援

CylanceOPTICS について

CylanceOPTICS は、次世代マルウェア対策製品 CylancePROTECT*3にEDR機能*4を付加するオプションです。マルウェアがどのような経路で侵入してきたか、どこに潜伏しているかなどをマルウェアが残したさまざまな痕跡から調査・解析できます。例えば、CylancePROTECT で防御したマルウェアの侵入経路を調査することで、入口対策の強化など、さらなるセキュリティの向上を図ることができます。

*3 CylancePROTECT：非常に高い検知率を誇るAIエンジンによって、マルウェアによる感染被害を防ぐ次世代マルウェア対策製品
*4 EDR：Endpoint Detection and Responseの略。マルウェア感染後の調査にフォーカスした製品



*5 2018年4月NSS Labs調べ

■マルウェアが残した痕跡の例

項目	内容
ファイル	作成、変更、削除、名称変更、属性変更
プロセス	ロード、インジェクション、関連付け、 他の項目（ファイル・レジストリ）との関連付け
ネットワーク	接続先IPアドレス、発信元・先のポート番号
レジストリ	キーやエントリの作成・変更・削除、永続化改ざん
ユーザー	ユーザーと実行したアクション、悪意のある アクテビティとの関連付け
リムーバブル	コピー先・元のファイル、デバイスプロパティ、 リムーバブル経由の侵入識別

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/cylance/product/mdr/

S18K-14-05 | 2023.07