EDRセキュリティ監視サービス　MSS for EDR

EDRの導入効果を活かし、侵入後の早期発見や被害の拡散・拡大防止

EDRの重要性と運用の課題

巧妙化するサイバー攻撃に備えるためにEDR（Endpoint Detection and Response）製品を導入する企業や組織が増えています。万一のインシデント発生時には、被害軽減のためにEDRを通じて迅速な検知／特定／対処が重要です。しかしながら、昨今のセキュリティ人材の不足や運用負荷の増大により、初動の遅れや、対処の高度な判断ができないなどの課題もあります。ソリトンシステムズのMSS for EDRはSBテクノロジー（ソフトバンクグループ）と提携し、専門のセキュリティアナリストがお客様が導入したEDR製品を24時間365日体制で遠隔監視するサービスです。 MSS for EDRはMicrosoftをはじめ主要なEDR製品に対応し、お客様のEDR運用負荷の低減と有事の際の迅速な初動対応を支援します。

24時間365日有人監視の マネージドセキュリティサービス

本サービスは、経験豊富なセキュリティ専門アナリストが、有人で24時間365日、お客様環境のさまざまなEDR製品を監視・対処・通報します。インシデント発生時には、EDR製品から出されるセキュリティログやアラートを分析して影響度を判断、ブロック等の対処を行うと同時に、発生原因や被害の影響範囲を特定し、迅速にお客様へ通知します。最新のセキュリティインテリジェンスとセキュリティアナリストの経験値により、サイバー攻撃の早期対応が可能となり、お客様の運用負荷を軽減するとともに、検出したインシデントを早期に対処することで、重大インシデントの被害拡大を防ぎます。

■ MSS for EDR　サービスモデル

監視対象EDR 製品

●Microsoft Defender for Endpoint　● Trend Micro Apex One SaaS
●Cybereason EDR　●CrowdStrike Falcon　●VMware Carbon Black Cloud

※2024年7月現在

■ SBテクノロジー　セキュリティ監視センター概要

生体認証を始め、複数の認証方式を用いたSBテクノロジーのセキュリティ監視センター(SOC)では、経験豊富なセキュリティ専門アナリストが24時間365日、お客様環境にあるEDR製品を常時監視します。ログや検知したアラートに対し対策案も含めて通知します。

監視拠点	■ 都内（場所非公開）及び国内・海外
稼働時間	■ 24時間 365日
監視ログ数	■ およそ1,200億ログ/月・およそ40億ログ/日 ※2022年4月時点
セキュリティ	■ 生体認証とICカードによる入室認証 ■ 24時間の監視カメラによる録画 ■ 記録可能デバイスの持ち込み禁止 ■ 運用監視通信の限定 ■ 非常用電源を72時間以上確保

MSS for EDR サービス概要・特長

■ お客様の課題をMSS for EDRが解決

テレワークが増え セキュリティを見直したい	社外で業務する社員の 端末管理が難しい	マルウェア対策として EDRを推奨されたけど…
ゼロトラスト環境に向けセキュリティ対策を見直したいけど運用・管理できるスキルがない	社外で仕事する社員が増え、一人一人の端末の管理が難しく運用に負荷がかかってしまう	不審な挙動を検知しても、隔離やシステム停止といった迅速な対応が行えるか不安

MSS for EDRで解決

ゼロトラストセキュリティ対策に有効なEDR	テレワーク環境下での端末管理を支援	当社のセキュリティ専門アナリストにお任せ
多数の導入実績のある当社のセキュリティエンジニアが設定から導入、運用まで支援	端末の可視化と的確な脅威対策で社員一人一人の端末のセキュリティを強化	感染後の対処に特化したEDRで、いち早く感染拡大や被害を防止

■ サービスの特長

特長1　EDR の導入からサポートまでお任せ
お客様環境における、EDR の管理システムやエージェントインストールの計画・設定・導入作業をサポートします
※個別見積となります

特長2　クイックレスポンス
EDRが検知し、アナリストが危険と判断した場合、EDRの機能を用いて一時対処します（一例：不審なプロセスの停止・感染したエンドポイントのネットワーク隔離）

特長3　オンデマンドリサーチ
お客様からのお問合せ（他セキュリティシステムで検出した気になる事象等）を起点にして、EDRでエンドポイントの状況確認を行い、ご報告します

特長4　プロアクティブコントロール
インシデント発生時、MSS契約監視対象で関連インシデントの分析、不正な活動の抑制作業を実施します
※別途、他監視対象のMSS契約が必要です

MSS for EDR ご提供サービス

スレットハンティング（オンデマンドサーチ）	マネージドセキュリティサービスを導入していないセキュリティ機器からのアラートや、社員が不審な添付ファイルを開いたといったEDR製品以外からの報告があった場合、SOCからEDR製品の機能を用いて調査
アラート分析	EDRのアラートを解析しセキュリティアナリストの基準で影響度を判定
一次対処	影響度の高いと判断した場合、セキュリティアナリストが EDRの機能を用いて端末のプロセス停止または隔離
通知	SOCで解析したアラートの影響度、一次対処した内容、対策等を緊急度に応じて、電話およびメールで通知
月次レポート	発生したインシデントのサマリーを月次で提供
お問合せ窓口	電話、メールにてお客様からお問合せいただけます
専用ポータル	お客様専用のポータルをご用意します 対応状況や契約情報等をご確認いただけます

お問合せはこちら：**株式会社ソリトンシステムズ**　サイバーセキュリティ事業部　cyber-sales@list.soliton.co.jp／ TEL 03-6369-8015