\Orchestrating a brighter world NEC

すり抜けて侵入したマルウェアによる攻撃を検知し、ダメージを制御するセキュリティ対策

セキュリティ運用サービス
For Cybereason EDR

※ Cybereason EDRはサイバーリーズン・ジャパン株式会社の製品です

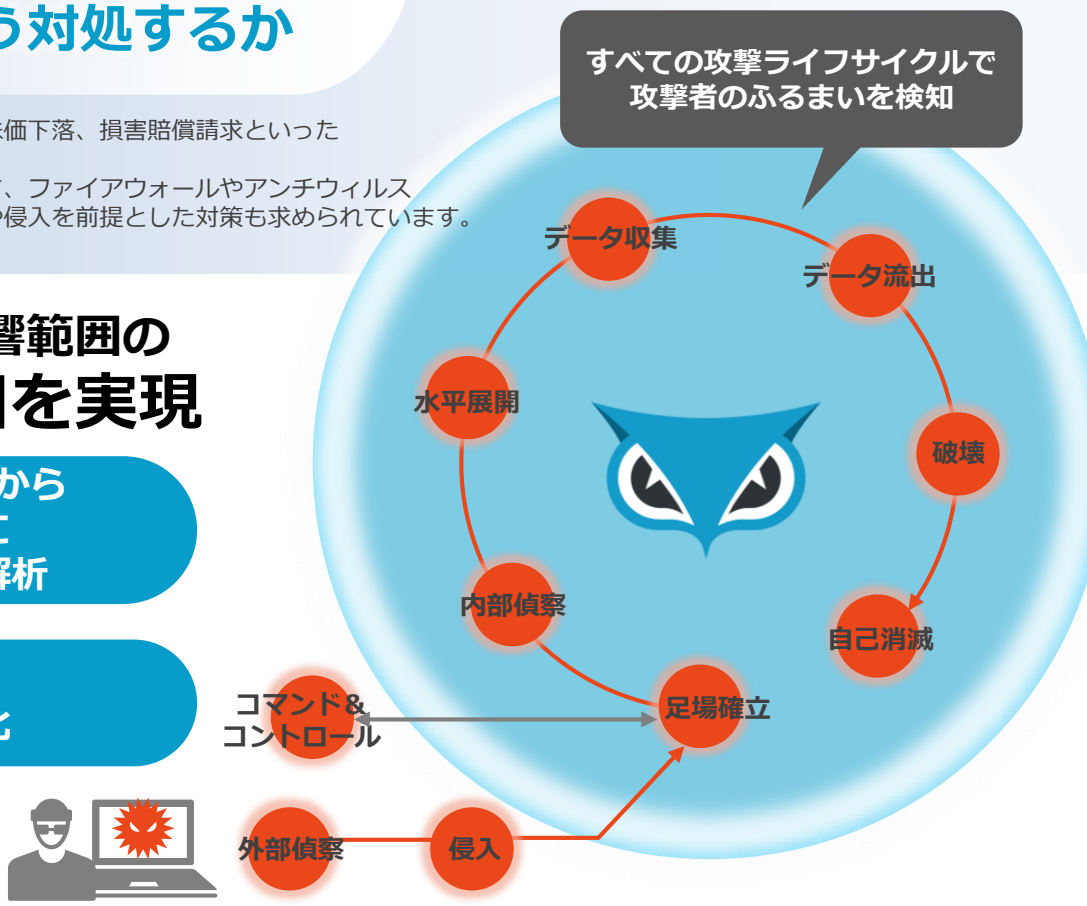
サイバーセキュリティによる企業経営課題にどう対処するか

マルウェア感染によるデータ流出は、株価下落、損害賠償請求といった企業経営の悪化に直結します。
高度化巧妙化するサイバー攻撃に対して、ファイアウォールやアンチウィルスなどの入口防御対策だけではなく、今や侵入を前提とした対策も求められています。

サイバー攻撃の影響範囲の早期特定と復旧を実現

全エンドポイントからリアルタイムに情報収集・相関解析

攻撃全体を時系列で可視化



導入効果・運用ポイント

1 1エージェントで防御-検知-対応-復旧までを全カバー

既知、未知、ファイルレス、ランサムウェアのブロックから、侵入後の悪意ある振る舞いに対する検知、対応、復旧までをカバー

2 攻撃の全体像をリアルアイムに可視化

侵入ポイント、根本原因、影響を受けた端末、影響を受けたユーザーを把握、攻撃の流れを自動分析、時系列で表示

3 攻撃を受けた複数の端末を、遠隔から一括対応可能

影響を受けた端末に対して、遠隔から一度に端末の隔離、プロセス停止、ファイルの隔離、レジストリの削除をおこなうことが可能

4 業務端末に影響しない

ユーザーモードで動作するためOSのアップデートなどの影響を受けにくく、低CPU使用率、低メモリ使用量、低ネットワーク負荷

5 日本語画面 日本語レポート

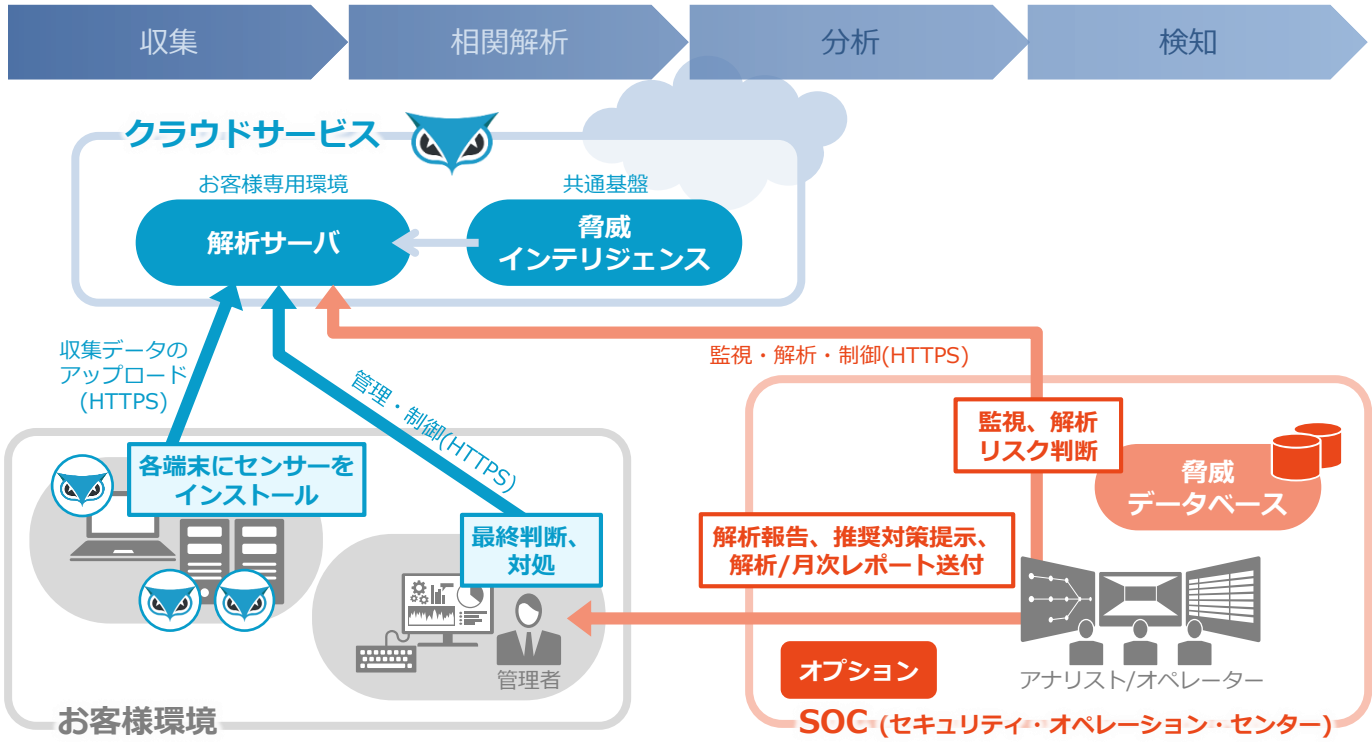
管理ユーザーごとに日本語・英語を選択することができ、状況・事象を正確に把握することで迅速なインシデント対応が可能

6 NECネッツエスアイの強力なサポート体制

当社SOC(セキュリティ・オペレーション・センター)のセキュリティ専門家による監視・解析・報告サービスが活用可能

NECネッツエスアイ

全体構成イメージ



セキュリティ・オペレーション・センター

攻撃を見逃さない！
迅速に対処案を提示
緊急隔離で影響範囲最小化

専門アナリストによるエンドポイント監視・解析サービスを提供

Cybereason EDRが検出したセキュリティインシデントは、独自の脅威インテリジェンスを活用して分析します。
インシデントは、当社SOCにて24時間365日監視し、セキュリティアナリストによる解析により脅威の深刻度を判定します。
危険性の高いインシデントについては、インシデント詳細と推奨対応方法を報告し、セキュリティチームの理解を助け、
脅威に対する素早い対策実行を支援します。

サービス項目		内 容
基本	稼動監視	Cybereason管理コンソールの稼動状況の監視（HTTPSステータス監視）
	問い合わせ	お客様からのお問合せ対応（サービス内容・セキュリティ脅威）
	セキュリティインシデント解析・通報	セキュリティインシデント解析 緊急度の高いインシデントについて通報・対処案の提示
	緊急隔離対応	緊急遮断対応（所定の手順に沿ったSOCによるプロセス停止処置、端末隔離処置）
選択	月次レポート	月次レポート提出（通報インシデント詳細、その他インシデントの統計 等）
	設定変更	設定変更作業（ホワイトリスト / ブラックリスト登録）

基本サービス 月額46万円(税抜)～

お問い合わせは、下記のNECネッツエスアイへ

デジタルソリューション事業本部
オフィスソリューション事業部　マネージドセキュリティサービス部
電話　03-6699-7524
E-mail: cybereason-sales@ml.nesic.com
https://www.nesic.co.jp

※記載されている会社名、サービス名、商品名は、各社の商標または登録商標です。
※記載内容は、2020年3月現在のものです。予告なく変更する場合がございます。

NECネッツエスアイ株式会社　〒112-8560　東京都文京区後楽2-6-1　飯田橋ファーストタワー　電話 03-6699-7000