商品情報 2025-03

TOSHIBA

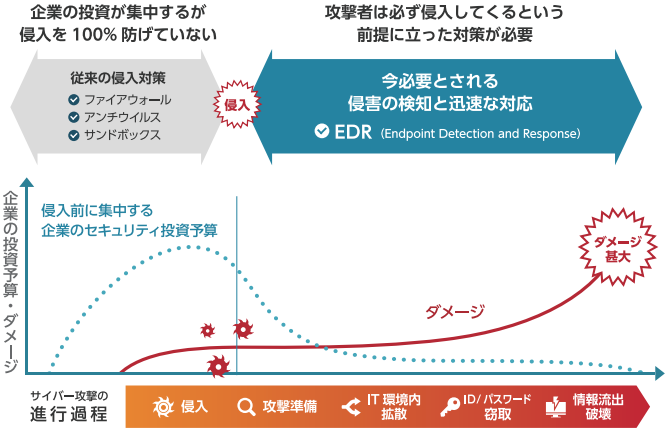
次世代エンドポイントセキュリティソリューション

Cybereason EDR

日本でもっとも選ばれている ランサムウェア対策

cybereason

- エージェントで防御・検知・対応・復旧までをカバー
- 攻撃の全体像をリアルタイムに可視化
- 攻撃された複数台の端末を遠隔から一度に対応
- 日本法人による強力なサポート体制
- ISMAP(政府情報システムのためのセキュリティ評価制度)に適合



~~ファイアウォールやアンチウイルスなどを入れているから、侵入は防げる！~~

ランサムウエア攻撃はアンチウイルスなどのウイルス対策ソフトでは検出が困難

~~中小企業だから狙われない！~~

サイバー攻撃は組織の規模を問わず発生

~~攻撃なんて頻繁にないから、セキュリティ担当は兼務で大丈夫！~~

情報資産を標的にした攻撃を封じ込めるためには、エンドポイントに特化したセキュリティ専門家が必要

東芝デジタルエンジニアリング株式会社

大企業が選んだ実績！！

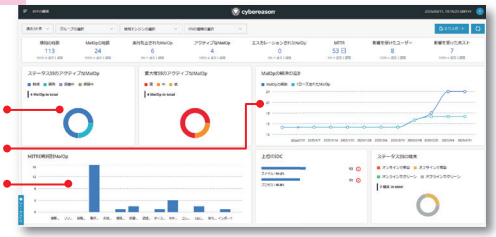
シェアNo1(※)の機能をそのままでリーズナブルに提供

(※)サイバーリーズン合同会社調べ

特長 1 「何が起きているか」を直観的に可視化

出社後まず管理画面を開き
アクティブなMalOp*がなければ
それで安心!!

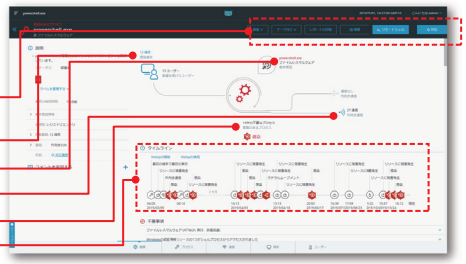
*MalOp：Malicious Operationsの略でサイバー攻撃の完全な一連の流れを表すもの



対応ステータス
時間別統計
攻撃の種類の統計

特長 2 いつどこで何がどう起こったのか自動解析

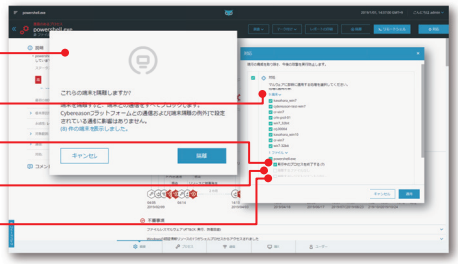
ワンクリックで対処へ（端末隔離、プロセス停止、レジストリ削除、ファイル隔離、リモートシェル）
影響する端末とユーザー
検知の根本原因
悪質な通信の状況
用いられた悪質なプロセス
複数の端末にまたがる攻撃もタイムライン表示



特長 3 遠隔でも複数の端末にワンクリックで対応

遠隔から影響ある端末を
確実に即座に隔離
業務上隔離できない端末には
個別の対応も可能

ネットワークから
エンドポイントを即座に隔離
指示を出す端末の選択
プロセスの停止
ファイルの隔離
レジストリの削除



特長 4 AIと相関解析で攻撃の全体像をあぶりだす

- 複数端末の相関解析
- 異常な振る舞いを絞り込み、検知
- AIによる異常検知と振る舞い分析
- 常時毎秒800万クエリをビッグデータ解析

東芝デジタルエンジニアリングならではのオリジナルサービス

実績と高い技術力でランサムウェア対策を強力にサポート！

導入サポートサービス

導入時のネットワーク設計、運用設計、エージェント配布方法、誤検知チューニング等、安心・安全に導入するためのサポートを提供します。

運用サポートサービス

導入当初の誤検知判断、定期的な対策効果の分析・レポート、万が一の感染時のPC復旧等、安心・安全に運用するためのサポートを提供します。

(LS00054)

東芝デジタルエンジニアリング株式会社

E-mail : TDEN-sales@ml.toshiba.co.jp
https://www.toshiba-tden.co.jp