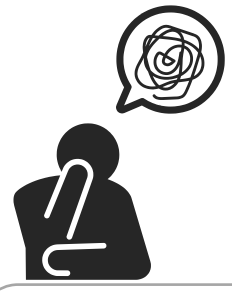
日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

防御・検知から復旧まで
自動対応可能なマルウェア対策

SentinelOne®

ITが進化する中、ランサムウェアを含めたマルウェアの被害は拡大し続けています。
そこでサイバーセキュリティの要件として、既知・未知のマルウェアを防御し、侵入後も即時対応が求められています。SentinelOneはエンドポイントに自律型AIを搭載しており、自動検知・防御はもちろん、復旧まで自動で行うことが可能です。



このような課題を解決します！

課題	解決
高度化するマルウェア攻撃に対して、適切なセキュリティ対策が分からない	一つの製品で、複数の検知エンジンを用いた防御・検知が可能なため、実行前（既知・未知）・実行中のマルウェアへの対策が可能
マルウェア実行後のインシデント対応に、特別なスキルが必要で、対応にも時間がかかる	AIによって自動的にダメージを軽減し、マルウェア実行後も自動復旧が可能なため、インシデント対応が即時完了
ログが集約されていないため、インシデント発生後の調査が困難	端末のログ取得を常時行い、ストーリーラインで過去の挙動について関連付けを行うため、スムーズな調査が可能

SentinelOneの３つの特長

①複数の検知エンジンにより、実行前や実行中のマルウェア対策が可能

パターンマッチング

既知のマルウェアに対する
シグネチャ方式の
パターンマッチング

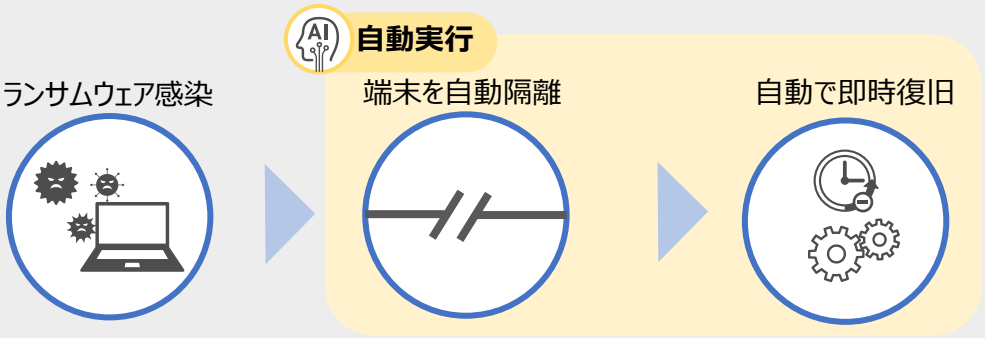
NGAV・EPP

未知のマルウェアに対する
ファイルの構造解析

Active EDR

ユーザーレベル・カーネルレベルの
ふるまいをエンドポイントのAIが
検知して防御するEDR

②AIによって自動的にダメージを軽減、復旧



- 特別な知識やスキルが不要
- インシデント対応が即時完了

人的対応が不要で、
自動で即時復旧！

③マルウェア実行後の調査のためのデータ、ツールを装備

プロセスツリーでの把握

Storyline

- 関連した挙動のプロセスを束ねて管理

端末の常時ログ取得

Deep Visibility

- URLやファイルアクセスなど、多彩な項目を取得
- 独自の検知ルールをカスタム可能

リモートからの端末調査

Remote Shell

- Windows ：PowerShell
- Mac OS ：Bash

MITRE ATT&フレームワークに即した表記

- 具体的なセキュリティ対策まで落とし込める
  フレームワークとして注目を集め、普及が
  進んでいるフレームワークに即した表記

導入に関するお問い合わせは、
株式会社日立ソリューションズ・クリエイトまでご連絡ください。

Webによる受付

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールによる受付

hsc-contact@mlc.hitachi-solutions.com

＊ ご相談・ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用も含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。

東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp/

HSC202410