SentinelOne
自律型サイバーセキュリティプラットフォーム

会社概要
2013年設立／米国
自律型サイバーセキュリティプラットフォームを提供
端末を起点に、検知・可視化・対応・復旧を支援

サイバー攻撃はAIで加速する時代 その攻撃の速さに対応できますか？

エンドポイントに対する攻撃を、検知から復旧まで自動対応。
検知だけで止めず、可視化・封じ込め・修復・復旧までつなげる。

サイバー攻撃がAIの活用により加速する今、手作業の対応では追いつけない

攻撃の高速化
AIで攻撃の準備・実行・横展開が加速

判断の分散
複数の製品やログの確認によって、初動が遅れる

復旧の長期化
調査・隔離・修復を手作業で行うと、被害と停止時間が拡大

守る側もAIを活用した自動対応が必要

SentinelOneが支援する4つの領域

検知・防御
脅威や不審な振る舞いを検知し、初動対応を支援

攻撃の可視化
個別イベントをつなげ、攻撃の全体像を把握

封じ込め
プロセスの停止・隔離により被害拡大を抑制

修復・復旧
攻撃後の復旧を支援

東京エレクトロン デバイス

PCだけでなく、
オンプレ環境も守れていますか？

クラウド接続に依存しない環境でも、検知から封じ込め・復旧まで自動対応

オンプレ環境が抱えるセキュリティ課題

1 閉域網でも侵入経路が残る

USBメモリ、保守PC、更新媒体など、物理的な接点からの侵入を完全には防げない

2 レガシーOS／パッチ制約

設備依存により、OS更新やパッチ適用を容易に進められない

3 OS内部の脅威が見えにくい

設備やネットワークは監視していても、不審なプロセスやマルウェアの振る舞いまでは把握できない

4 生産設備を止められない

24時間稼働などにより、調査・隔離・再起動に使える時間が限られる

制約が重なることで生じるリスク

侵入に気づくまで時間がかかり、初動が遅れやすい

- 端末内部で進行する不審な挙動を捉えにくい
- 侵入後の横展開・感染拡大を止めるまでに時間がかかる
- 対応が遅れるほど、生産停止や復旧長期化のリスクが高まる

閉域網環境でも実現する自律型EDR運用



オンプレミス対応で得られる3つの価値

閉域網内で一元管理

- オンプレミス管理サーバー構成
- インターネット非接続環境に対応

レガシー環境にも幅広く対応

- レガシーOSを含む幅広いOSをサポート
- 既存設備を活かしながらEDRを導入

検知から復旧まで自動化

- 不審な振る舞いをリアルタイムに検知
- 人的対応を待たず被害拡大を抑制

だから、オンプレ環境も自動対応へ

「侵入させない」だけではなく、「侵入されても早期に見つけて止める」セキュリティ

本紙に記載された会社名、ロゴ、ブランド名、製品名、サービス名は各社の商標または登録商標です。
その他全ての商標および登録商標はそれぞれの所有者に帰属します。

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

お問い合わせは、Webサイトのフォームよりお願いします。
https://cn.teldevice.co.jp/product/sentinelone/form.html

本社:〒150-6234　東京都渋谷区桜丘町１番１号
渋谷サクラステージ SHIBUYAタワー
Tel.03-6635-6000（代表）

名古屋:〒451-0045　451-0045　愛知県名古屋市西区名駅2-27-8
名古屋プライムセントラルタワー 8F

大阪:〒530-0001　大阪府大阪市北区梅田3-2-123　イノゲート大阪 17F