Soliton®

サイバー攻撃と
内部不正に対応するEDR

InfoTrace Mark II

インフォトレース マークII

InfoTrace Mark IIは、エンドポイントで広く深いログを取得することで、サイバー攻撃から内部不正まで、セキュリティリスク全体に対し、幅広い効果を発揮します。
詳細なログにより端末の状況を明らかにすることで、
企業・組織におけるインシデント対応を支援する国産EDRです。

InfoTrace Mark II の4つの機能

1 サイバー攻撃、内部不正の調査が可能

何が起きたのか明らかにする証跡ログ

ユーザーによる操作だけでなく、PCの動作を常時記録。サイバー攻撃や内部不正など想定外のインシデントの際にも、遡っての調査が可能です。テレワーク時の勤務実態や、端末状況の可視化もできます。

2 リモートから簡単に端末を隔離

被害を最小限にする端末隔離とアプリ実行禁止

アプリの実行や、端末の通信制御が行えます。端末の通信制御機能で、端末の隔離を実施することで、マルウェア感染等が疑われる端末を社内環境から安全に切り離すことが可能です。

3 進化するサイバー攻撃からPCを守る

後を絶たないマルウェア被害からPCを守ります

パターンファイルに依存しない防御を実現。未知のマルウェアに対して、振る舞い検知や脆弱性攻撃対策が可能です。ナレッジベースに基づいた運用支援機能も搭載しています。

4 デバイス制御で情報漏洩リスクを下げる

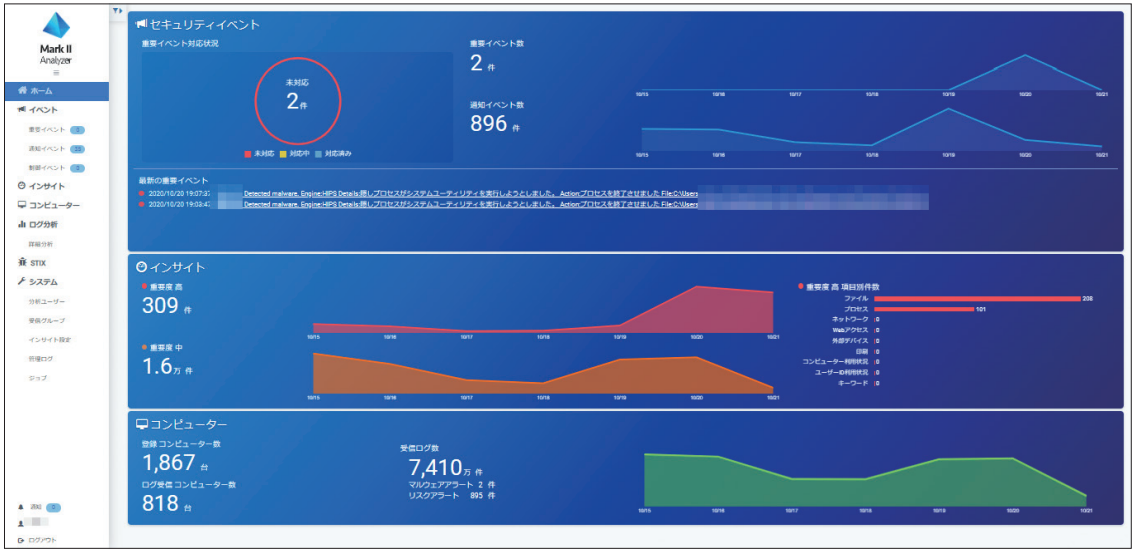
内部不正を防ぐ外部デバイス制御

クラウドサービスの利用が増える中でも、外部デバイスの利用はなくなりません。スマートフォンを含む、外部デバイスの利用を細かく制御し、管理者が意図しない利用を制限することが可能です。

InfoTrace Mark II で状況を把握する

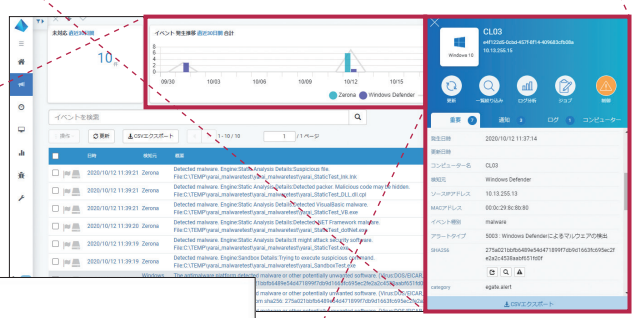
侵入を前提とした対策の第一歩は、エンドポイント（端末）の可視化です。
InfoTrace Mark IIは、エンドポイントの状況を把握できる環境を整え、いざという時の早期対応を支援します。

検知された攻撃や対応状況を表示
ドリルダウンで詳細を確認可能

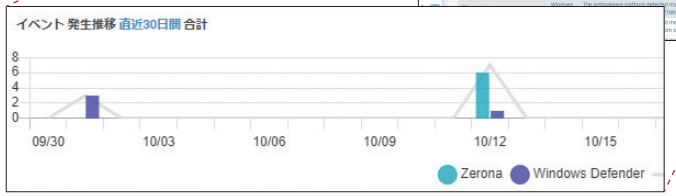


リスク指標となるインサイト（指定条件にヒットしたログ）の件数推移やログ受信状況を表示。
ドリルダウンで詳細まで確認できる

検知したファイルから侵入経路や脅威ハンティングできるほか、初動対応として端末の隔離なども実行可能



マルウェア防御機能のイベントに加え、
Windows Defender AntiVirusでの
検知情報も集約して表示



InfoTrace Mark II で出来ることまとめ

■ 強力な証跡機能

証跡ログ

- 攻撃検知有無に関わらず記録
- 全てのファイル（文書含む）のハッシュ値を記録

■ マルウェア防御

マルウェア防御

- 未知マルウェア防御
- 脆弱性攻撃防御

■ リアルタイム分析・SIEM連携

証跡ログ

- 指定条件でのリアルタイム分析での攻撃予兆把握
- 過去ログ分析
- SIEM連携機能（全ログ・特定ログのリアルタイム連携）

■ 初動対応

アプリ・通信制御

- ネットワーク隔離（プロセスごとに制御可能）
- プロセス実行禁止（ファイルパス、ハッシュ値などで指定）

■ 脅威ハンティング

証跡ログ

- リアルタイムのファイル保持端末の検索、強力なログ検索

■ デバイス制御

デバイス制御

- USBデバイスの許可・禁止

■ 脅威情報連携（STIX/TAXII対応）

証跡ログ

- 脅威情報を参照した自動ハンティング機能

■ 端末管理

端末管理（無償）

- インベントリ情報収集
- ファイル転送・コマンド実行

Soliton®

株式会社 ソリトンシステムズ　https://www.soliton.co.jp/
〒160-0022　東京都新宿区新宿 2-4-3　TEL 03-5360-3811
お問い合わせはこちら https://www.soliton.co.jp/contact/

ITMK2-P-2205A