

ランサムウェアを筆頭としたサイバー攻撃の自動化/ビジネス化（RaaS）が進んだ結果、企業規模や業種に関係なく攻撃の対象となっており、企業のセキュリティ対策は喫緊の課題になっています。

## 「EPPによる感染前の検知」と「EDRによる被害の拡大防止」を適切に運用することが重要です。

シグネチャ / NGAV



EDR

適切な運用

### ■ 本サービスのおすすめポイント！

総合セキュリティサービスとして従来型のエンドポイント機能とEDR機能をワンストップで提供します。また、EDRはセキュリティ専任者のいない企業での運用を前提に「被害が広がる前に危険端末は隔離」し「インシデントログ全体を生成AIで要約」するなど少数の担当者でハンドリングできるサービスです。



法人で求められる機能を  
1つのサービスで網羅

EPPとEDR  
統合ポータルで効率よく管理

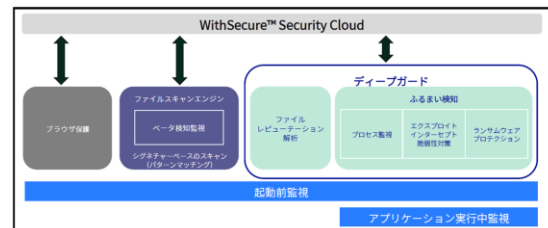
インシデント通知から  
端末の隔離までを自動化

専門家によるアラート解析  
MSSサービス

### ■ 多層防御によるウイルス対策

世界的なセキュリティソフトウェア評価機関であるAV-TESTが発表する「Best Protection Award」を最多受賞している **WithSecure Elements** のエンジンを採用。

AIを活用した高性能の振る舞い検知機能を標準で搭載し、多層防御による**“感染させない”対策**とEDRによる**“被害を拡大させない”対策**をご提供します。



### ■ インシデントログの可視化（EDR）

EDRがインシデントを検知した場合、管理者にアラートを通知し、ポータル上ではインシデントのログをツリー形式で可視化します。

ログからは、発生日時・検出箇所・検出理由などを確認することが可能です。




### ■ インシデント発生端末の自動隔離

EDRではインシデントのリスク度合いをポイント付けし、一定のリスク度（中/高/深刻）を超過した場合は、発生端末を自動でネットワークから隔離できます。



## ■ 生成AIによるアラート解析 (EDR)

インシデントの解析には専門知識が必要なケースもあり、全てのログの詳細を追うことは困難です。生成AIによりログの全体像を把握し検出理由を整理することで、アラート検証の負荷が大きく軽減されます。



BCD 141448805-21880 概要

この概要はAIが作成したものであり、真実に沿うものであることに留意されたい。すべての疑念に完全に対応するためには、さらなる調査と専門家による相助が必要な場合があります。

要約

2024年3月26日 午前8時14分37秒頃、AIRNETiK-kenichi ユーザーのホスト 'kkae01intraairnet.jp' で、7z.exe と explorer.exe プロセスによる異常なファイルアクセスが発生しました。その後、実行し、さらに同プロセスから (f1129 - 共有モジュール) が読み込まれました。その後、'invoice.exe' が実行され、(f1204 - ユーザー実行) が確認された。その後、'invoice.exe' プロセスが vproxy.jar.net.jp (08080ホスト) に HTTP接続を行い、(f1571 - 非標準ポート)、(f1071.0) 活動が検出されました。これらの活動は、カスタム/ワイルドカードの可能性を示唆しています。

主要事象

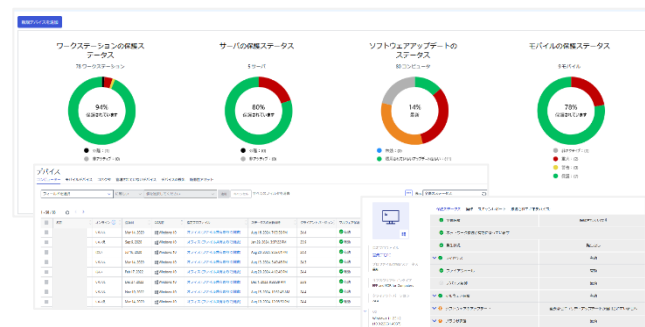
- 26.03.2024 17:1437 UTC+09:00: 7z.exe と explorer.exe による異常なファイルアクセスが発生
- 26.03.2024 17:1540 UTC+09:00: 'invoice.exe' が実行され、(f1204 - ユーザー実行) が確認された
- 26.03.2024 17:1540 UTC+09:00: 'invoice.exe' が (f1129 - 共有モジュール) を読み込まれた
- 26.03.2024 17:1545 UTC+09:00: 'invoice.exe' が vproxy.jar.net.jp (08080ホスト) に HTTP接続を行い、(f1571 - 非標準ポート)、(f1071.001 - ツープロトコル)、(f10011 - コマンド&C)

### 【生成AI Luminen での解析】

生成AIを用いて該当アラート全体を解析し、どの端末で何が原因で発生したアラートなのかを分析し表示してくれます。

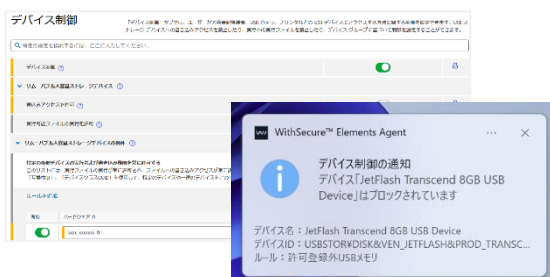
単一のログを確認する従来の機能に比べ、発生時系列やログ同士の関連性が分かりやすく、インシデント調査が効率的に行えます。

## ■ 管理ポータルでの一元管理



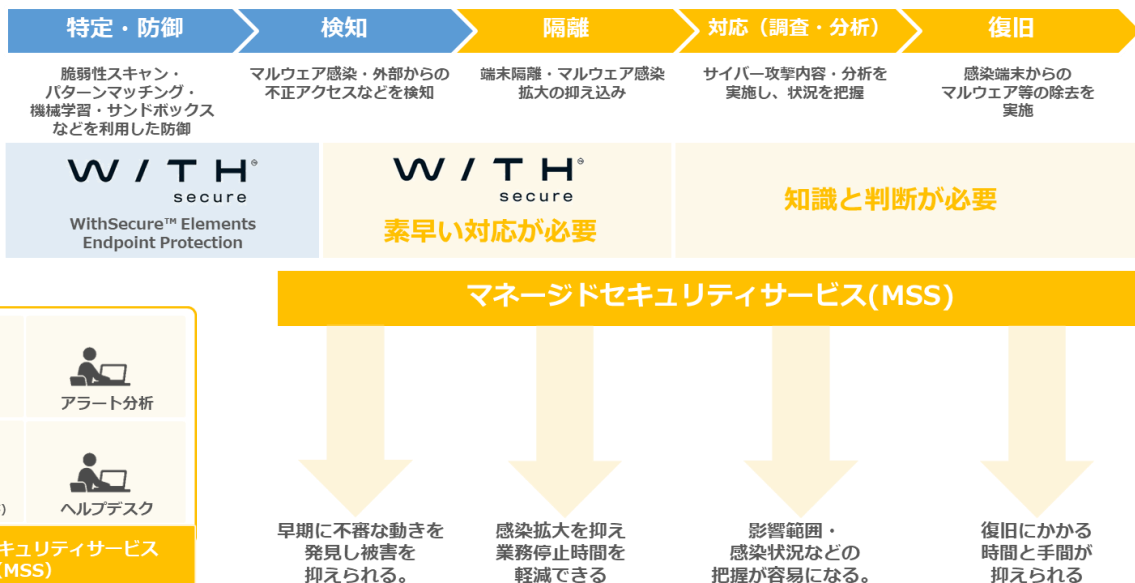
## ■ USBデバイスの利用制限

USBデバイスを制限し情報漏洩対策も可能です。



## ■ MSS (セキュアイノベーション社 運用支援サービス)

自社での運用に不安のあるお客様は、運用支援サービス (MSS) をご契約いただくことで、専門チームでのアラート監視及びインシデント対応の支援を受けることができます。



お客様へはインシデント発生時の対応報告と毎月発行の運用レポートをご提出します。

サービスの詳細、ご提供条件等に関する場合は、弊社営業担当までお気軽にお問い合わせください。無料トライアルのご用意もございます。