ネットワークの脅威を見逃さない

GREYCORTEX MENDEL

■ MENDEL の特長

優れた脅威検出機能とネットワークの可視化機能を備えたネットワークトラフィックアナライザ「MENDEL」

- **既知の脅威に加え、既存のセキュリティ対策製品が見逃してきた未知の脅威も高い精度で検出できます。**
- **弊社独自開発の異常通信遮断ソフト「i-Sniper」との連携により、感染した端末のネットワーク自動切り離しが可能です。また他のセキュリティ製品との連携による対処・感染被害の防止も可能です。**
- **接続機器や通信の一覧を作成し、資産・通信のアセスメントが可能です。**
- **通信量やサービス別、ボトルネック調査などのネットワーク分析機能により、ネットワーク障害や課題等の原因特定が可能。**

■ 管理しやすい直感的なインターフェイス

MENDELのインターフェイスは経験の浅いセキュリティ担当者にも使いやすく、セキュリティイベントを調査する際、ホストや通信先についての情報詳細のドリルダウンは非常に簡単です。

■ IDS + 機械学習で効果的な脅威検出

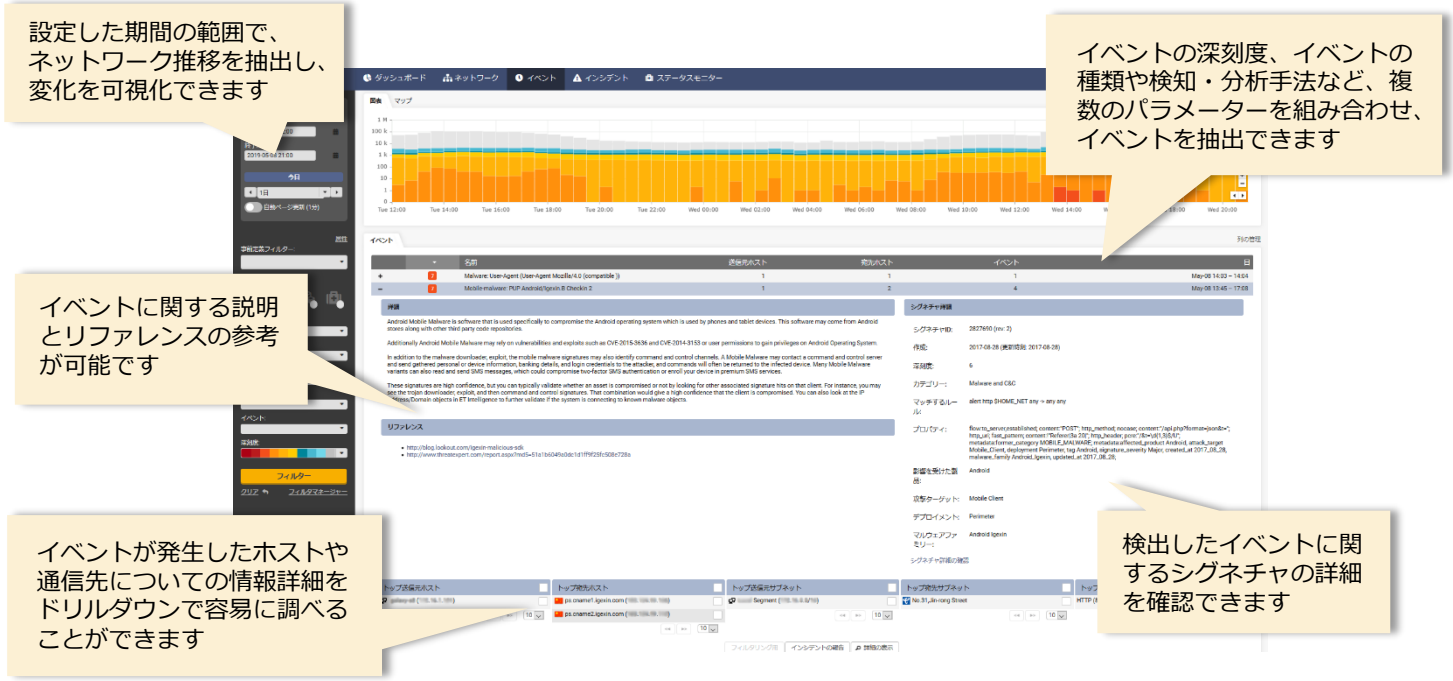
- 既出の脅威検出（既存のIDS製品やサンドボックス製品に置き換わる機能）を行うIDSに加えて、機械学習とNBA（Network Behavior Analysis）により、正常なネットワークの状態を自己学習します。
- マルウェアなどのふるまいを検知し、様々な攻撃を予兆できます。異常があれば危険度に応じてイベントを作成し、誤検知の登録により、不要なイベントを抑止します。
- サンドボックス等では対応できない内部不正に関しても検出が可能です。（日本に流通している他の製品では、IDS＋機械学習の機能を持ちませんが、MENDELではそれが可能です。）
- ネットワークトラフィック分析、マルウェア検知、ポリシー違反防止など、SOC運用に役立つ機能を複数備えています。

※IDS・・・Intrusion Detection System （不正侵入検知システム）の略

■ 資産・通信のアセスメント

- 接続機器や通信の一覧を作成しますので、自社ネットワークの状況を確実に可視化できます。（ネットワーク依存関係、過度のコミュニケーション、新しいデバイス情報、脆弱なアプリケーション　など）
- ネットワークのループやボトルネックを検知することで、ネットワーク障害の発生原因を特定することができます。
- VLANごとに通信量を可視化、分析することができます。
- ネットワーク構成によってはMACアドレスを取得することができます。
- ADやLDAPなどの認証システムと連携することができ、管理工数を減らすことができます。

■ 簡単に確認できるセキュリティイベントの詳細情報



ネットワーク挙動分析（予測分析、発見分析、フロー分析、反復分析、パフォーマンス分析）、ルールベース分析（IDS、Blacklist）、相関分析等、様々な分析手法で、イベントを検知します。

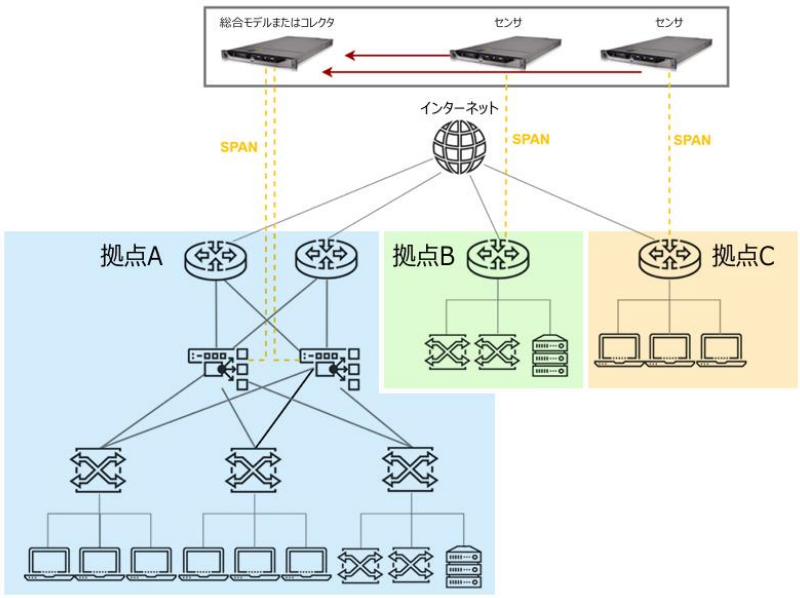
■ さまざまな環境に導入可能

MENDELは単に、先進的な機能を備えているだけではなく、導入も非常に簡単です。ミラーパケットのみを取得するため、お客様の既存ネットワーク構成に変更等は不要で、インストール・基本設定の時間はおよそ30~60分です。

センサ
- ◆ TAPまたはコアスイッチからミラーリング
- ◆ ASNMデータのアウトプットは
トラフィックの0.5~1%
- ◆ 10Gbpsまで対応

コレクタ
- ◆ 1コレクタに付きセンサ50個と
連携可能
- ◆ 40Gbps~の集約したインプットを対応
- ◆ イベントの集中管理コレクタあり

アプライアンス
- ◆ パッシブ
- ◆ オンプレミス
- ◆ HWまたは仮想
（VMware ESXi、Hyper-V、KVMなど）



海外拠点のネットワーク環境にも対応します。詳細はお問い合わせください。

- ◆ 他のセキュリティ製品と連携し、よりセキュアなネットワークを実現します。
- ◆ 主要なUTM製品と連携し、MENDELからポート制御（特定のポートを閉じること）することで、一元管理できます。

※内容は予告なく変更することがあります。（2019年8月作成）

情報セキュリティ株式会社

〒650-0012 神戸市中央区北長狭通4丁目9-26　西北神ビル3・8階
TEL：078-381-8980（10:00~17:00　土・日・祝除く）
FAX：078-381-8979
E-mail:　inquiry@isec.ne.jp　URL: https://isec.ne.jp