# Veramine Inc.

サイバーセキュリティ

APTマルウエア

ディセプション

SOC EDR

DLP

IR

# Veramineの優れた特性

次はVeramineの独特な点です：

## データ収集

1)データ収集の品質：多様性・詳細・関連性・トラフィック量が少ない。全てのセキュリティ関連のアクティビティ、幾つかの重要なWindowsイベント、特にシステムセキュリティとSMBデータの収集は、おそらく次のようにVeramineによってのみ提供されます。

- プロセス：作成、画像の読み込み、コマンド引数；オープン、インジェクション、リモートプロセスアクセス、リモートスレッドの作成
- レジストリ：キーアクセス、値の操作、変更/作成時のWindowsレジストリキー
- システムセキュリティ：セキュリティトークンとフラグ、特権、ファイルセキュリティ、バイナリポリシー違反、サービス追跡
- ネットワーク：TCPやUDPなどのプロトコル、接続とポート、DNSキャッシュの監視、URLアクセス
- ユーザー：ログオンセッション、特権、コンソールの使用、リモート又はローカル
- SMB：セッションとファイルアクセス
- バイナリ：読み込んだ全てのバイナリ

2) リアルタイムで継続的な収集：一部の商品は、管理者が要求した時のみエンドポイントからサーバーにデータを移行します。

3) 柔軟な収集ポリシー：アドミンは収集対象のデータを選択できます。これは、パワー不足のマシンにも適しています。

4)適応の絞り込み：センサーが繰り返しイベントパターンを検出した場合、又はある大量のイベントは検出や分析に重要である可能性が低いと判断した場合、センサーはそれをサーバーに送信しません。これでセンサーによって送信され、サーバーによって処理されるTBのトラフィックを除外できます。それが、帯域幅を少量に制限しても大量のものを収集できる理由です。

5)元（生）のデータの提供：本格商品の外部、収集した生データを提供します。

## 検出ction

1）https://attack.mitre.org/wiki/Technique_Matrix（攻撃の辞書）により全ての攻撃戦術(キルチェーン：エクスプロイト、ペイロード、拡散、C&C、アクション…）とテクニックの検出を目指します。

2）多くの種類のデータを収集する程、データ分析アルゴリズムも多様になります。特に行動ベースの検出において、より良い検出ができます。例挙げると、

- SMBデータにより、横方向の動きとインサイダー脅威を検出できます。
- セキュリティトークンを収集することで正確な権限昇格（EOP）を検出できます。
- Lsassプロセスを開くと、認証情報とパスワードのダンプ（Mimikatz）を検出できます。
- コマンド引数により、悪意のPowershellファイルレスの侵入を検出できます。
- 異常なプロセス移行とインメモリプロセスインジェクション（メモリー内にプロセスを挿入）
- バイナリをロードするプロセスは、Dllサイドローディング/植え付けを検出することを可能にします。
- 実行可能ファイルは、インターネットからダウンロードされた後に実行されます。

3）ルールベースと機械学習を組み合わせています。機械学習検出アルゴリズムの例：

- プロセスプロファイリング：プロセス動作の正常基準からの逸脱
- ユーザー追跡：ユーザーのログオンおよびログオフ動作の基準からの逸脱
- データ漏洩：ネットワークボリュームの本来の基準からの逸脱
- SMBトラッキング：横方向の動きを示す通常のSMB動作からの逸脱

迅速な通知のために、検出アラートを電子メール経由で送信されます。検出は、Veramineポータルのインタラクティブなダッシュボードを介して、時間順で簡単にソートすることもできます。

## 調査stigation

メモリー内のYara検知（検索）：Veramineのみが備えているユニークなインシデントレスポンス機能です。センサーは、yara式に一致するプロセスを報告します（システム一致だけでなく、プロセス毎のこと）。

ファイルでのYara検知（検索）：センサーは、読み込まれた全てのバイナリをインテリジェントにアップロードします。Yaraで直ちに全ての新しいファイルをスキャンします。自動的にYaraの検知と合致するものをブロックします。

Veramineにより、攻撃を検知する検索ルールを作成し変更できます。ホスト又はプロセス

メモリダンプの攻撃を検知することはすぐにハンドルできます。

プロセス名、ハッシュ、コマンド、IPなどを含む柔軟な論理式を使用することで、収集された全てのデータを検索できます。検出の各アラートレベルは個別にフィルタリングして表示されます。

全ての実行可能なバイナリが収集されます。

## レスポンスアクション

他の殆どの製品にはバイナリブロッキングかホスト隔離（検疫）のみがあるのに対して、VEDRには、バイナリ、ユーザー、ホストからプロセスまで殆どの応答アクションがあります。Veramineはいくつかの基本的なイベントへの対応を導くこともできます。

- ホスト：ネットワーク隔離（検疫）、メモリダンプ、メモリ上のYara検索、監視の開始/停止、スリープ/シャットダウン/再起動
- プロセス：ネットワーク隔離（検疫）、メモリダンプ、メモリ上のYara検索、サスペンド、ターミネート（終了）
- ユーザー：無効化/有効化、ユーザーセッションの切断
- バイナリ/ファイル:ネットワーク検疫、ブロック、ウイルスのスキャン、ファイルの検疫

## 検出

殆どの既存のアプローチがパッシブディフェンスであるのに対して、Veramineによってアクティブディフェンスアプローチとして独自に提供されます。
不正なサービス、プロセス、ファイル、ミューテックス、イベント、リスナー、認証（資格）情報、共有、レジストリなど。
すべてのコンピューター（物理またはVM）をITシステム内でハニーポットにすることができます。
侵入のチート、検出、防止のためにキルチェーンに沿って配置されたトラップのプラットフォーム。

侵入者の活動を追跡し、トラップを使用して彼らの動作を制限します。

例えば、WannaCryはミューテックスをチェックして、システムがすでに感染しているかどうかを判断します。このような不正なミューテックスを設定できます。

## パフォーマンス

VEDRセンサーのみが、平均で1%未満のCPUと20 MBのRAMを使用することができます。

ホストあたりの平均ネットワークトラフィックは30 MB / 1日未満です。これは、センサーにより収集されるイベントを構成できる収集ポリシーを使用することで。さらに調整できます。

## デプロイメント

"phantom -install"を実行するだけで、簡単にインストールでき、VEDRをAD、SCCM、psexecなどの様々な方法で複数のクライアントにも展開できます。更新も楽に実施できます。Veramineエージェントは、Veramineのポータルを通して簡単に開始/停止できます。

競合の件なら、McAfee AV、Kaspersky EPP、Trend Micro AV、Symantec AVなどの正しく設計されたセキュリティまたはAV製品と競合しないようにするべきです。センサーを実装する時は、協力と互換性のモジュールの動作環境に関するすべてのルールと推奨事項に従います。

Veramineセンサーは、WindowsとLinuxの両方に導入することもできます。 Veramineは、Windows 7及び全ての新しいWindowsバージョン、Windows Server 2008 R2及びすべての新しいWindows Serverバージョンをサポートしています。

Veramineは、基本的にubuntu、centos、fedora、gentoo、slackwareなど5年前までにリリースされた、かつカーネルバージョン3.x以降の殆どの主流のLinuxディストリビューションをサポートしています。

Veramine EDRは、syslog / jsonを使用するSplunk、IBM Qradar、ArcSight、ELKなどの一般的なSIEMと簡単に統合できます。

Veramineはcsv形式のレポートもサポートしています。