Trend Vision One – XDR 簡易運用ガイド

～初めてのXDR～

トレンドマイクロ株式会社

2023年5月9日

はじめに

- 本資料について
  - 本資料は、Trend Vision One– XDRを初めてお試しいただく方を対象にXDRの簡易的な運用イメージをご紹介する簡易運用ガイドとなります。
  - システム要件や制限事項、具体的な操作方法に関しては、オンラインヘルプ(https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-online-help.aspx)も併せてご確認ください。
  - 本資料は2023年5月時点で公開されている製品を元に作成されております。今後のバージョンアップや機能追加などによって内容は予告なく変更される場合がありますので、あらかじめご了承ください。
  - 本資料で紹介している運用例あくまで一例であり、特定のセキュリティレベルを担保するものではありません。
  - 本資料では監視対象の端末にセンサー（XDR: Endpoint and Server, C1WS）をインストールしている環境を対象にしています。

- 本資料で用いられる略称
  - Trend Vision One ・・・ Vision One
  - Trend Vision One XDR・・・ XDR
  - Trend Micro Apex One SaaS ・・・ Apex One SaaS
  - Cloud One – Workload Security・・・ C1WS
  - Observed Attack Techniques ・・・ OAT
  - ウイルス対策ツールキット・・・ATTK

改訂履歴

版数	改訂日	内容
第1版	2021/11/16	第1版として公開
第2版	2023/5/9	第2版として公開 追加機能についての情報アップデート

コンテンツ

1. セキュリティ運用の一般的な考え方
2. Trend Vision Oneセキュリティ運用の考え方
3. 攻撃シミュレーションを使った調査の流れ
4. Appendix

セキュリティ運用の一般的な考え方

定例的なセキュリティ運用

SOCにおいて、日々の運用では大きく以下のフェーズに分かれます

検出 **調査** **対処**

一般的にはこれらのフェーズは以下にように考えられます。

フェーズ	概要
検出	製品やサービスを設定/チューニングし、インシデントイベントを検出し、可視化する。SOCにおいては製品/サービスの特性を把握し、検出内容や検出傾向を理解しておく。
調査	検出イベントを調査する。原因究明や影響範囲の把握、深刻度などを確認し、調査結果によって、初動対応の対処を判断する。
対処	検出イベントに対する対処を行う。ここでは初動対応の対処について言及とする。

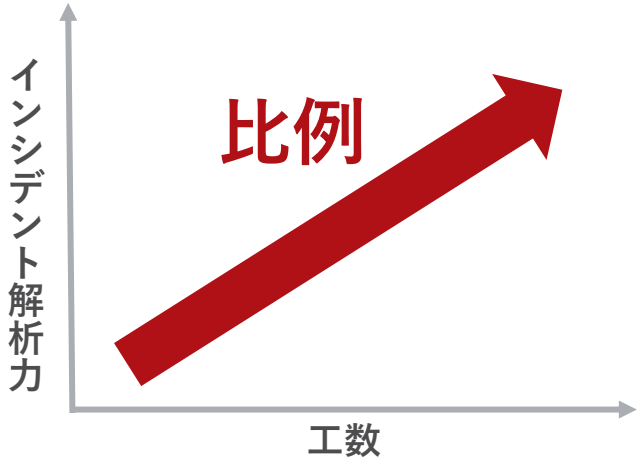
Vision Oneではこれらのフェーズのオペレーションを一つのコンソールで実現しています。

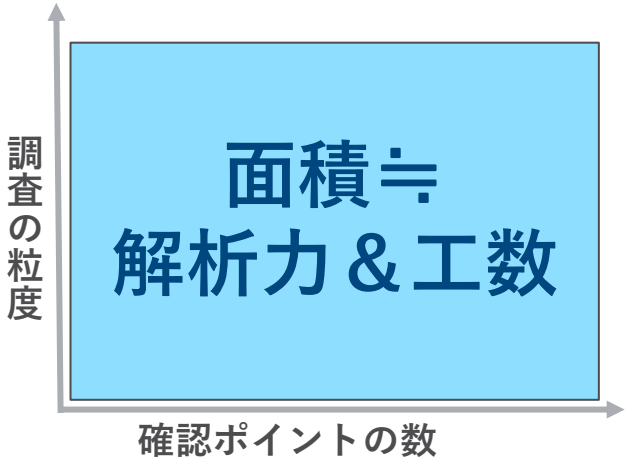
検出 検出技術の把握や設定/チューニング

- 運用するセキュリティ対策製品/サービスの**検出技術および検出イベントの内容を理解**しておく必要があります。
  - 例えば、パターンマッチングの技術による検出イベントは信用度は高いですが、ふるまい検知のような場合は過検知の可能性もあります。
- 複数の検出機能を有する製品/サービスを利用する場合は、利用する**機能のオン/オフ**、もしくは**設定のチューニング**を検討する必要があります。
- **製品/サービスの検出機能と検出ロジックの正しく理解**することを推奨します。調査時に検出イベントの内容理解に役立つためです。

調査 セキュリティ運用における解析力と工数

- インシデント解析力と工数は比例します。
- 確認ポイント※の数と調査の粒度が多くなるほど、インシデント解析力および工数が増加します。



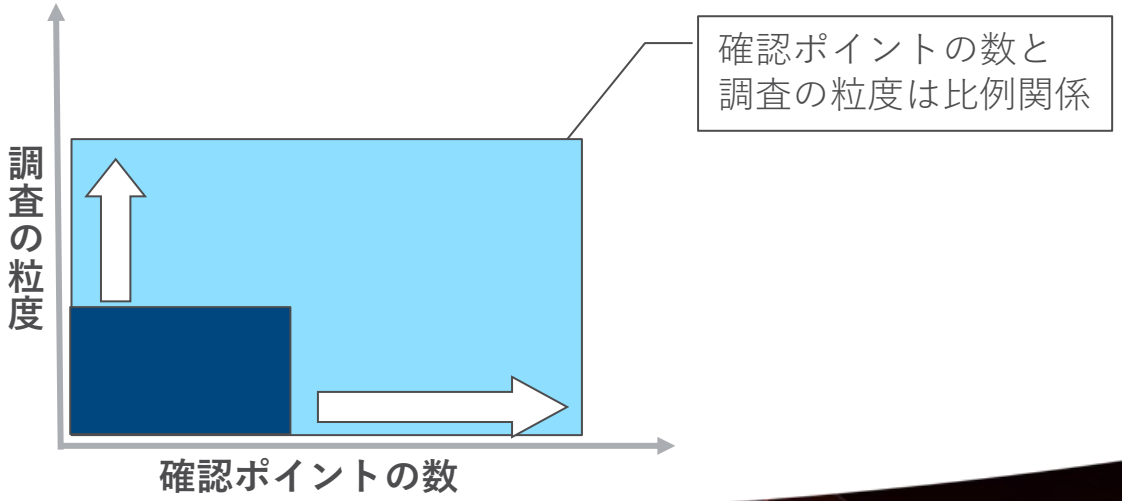


※確認ポイント：日々のセキュリティ運用においてオペレーターが確認をする項目
（例：Vision OneのWorkbench, OAT, カスタマイズされたクエリ項目のSearch結果など）

調査 運用のステップアップ

これからセキュリティ運用を始める場合は、段階的に運用をステップアップしていくことを検討しましょう。はじめは狭い範囲で確認ポイントを絞り、概要レベルの調査深度での運用を開始します。

次の段階でインシデント解析力を広げます。調査の粒度や確認ポイントの数は相関関係にあるため、確認ポイントを増やすと調査の粒度も連動して上がります。



対処 迅速な初動対応のための考え方

- 「すべての検出イベントで実施すべき汎用的な対処」はありません。検出イベントの内容や社内のポリシー、業務への影響によって対処は異なります。
- 標的型攻撃の場合、感染を抑えることや感染を広げないためには、迅速な初動対応が必要です。感染や感染の疑いがある端末を隔離し、感染原因や疑わしいファイルなどを調査します。

端末隔離

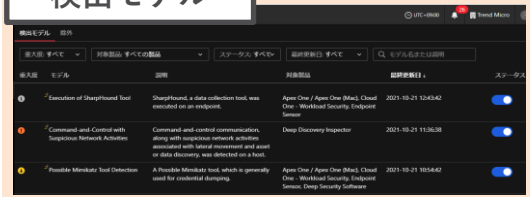
解析

Trend Vision One
セキュリティ運用の考え方

Vision One XDR 各機能の位置づけについて

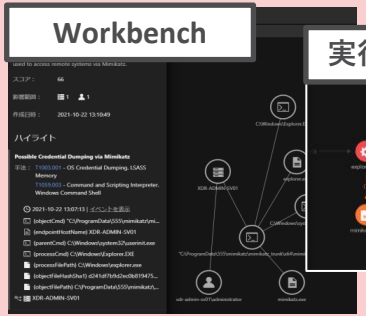
検出 → 調査 → 対処

検出モデル



収集したアクティビティデータを相関分析して、検出モデル(Detection Model)に沿って脅威を検出します。

Workbench

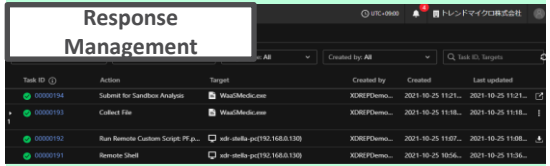


検出モデルによって脅威イベントの関連性を可視化します。

実行プロファイル

プロセスツリーを表示します。

Response Management



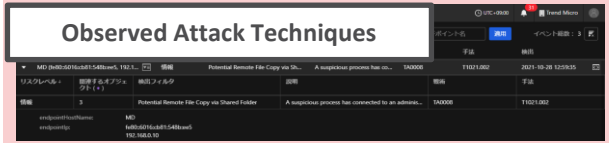
実行したレスポンス機能のステータスを表示します。

簡易運用時の範囲

Search

アクティビティデータの検索結果を表示します。

Observed Attack Techniques

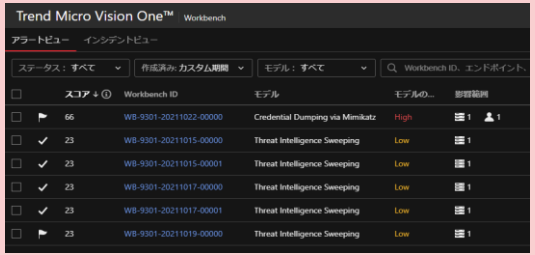


粒度の細かい攻撃手法の検知情報を表示します。

Vision One XDR 運用時に確認をする項目（毎日）

調査 → **対処**

①Workbenchを確認



脅威スコアの高いアラートを調査

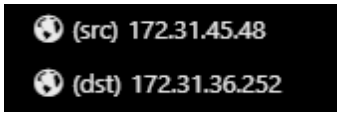
②アラートの内容を確認する

ハイライトの中から以下の情報を確認し、
通常の運用で発生したイベントかどうか確認します。

確認ポイント1　**実行コマンド**

※右クリック>実行プロファイル：プロセスチェーン確認可能

確認ポイント2　**アクセス元/先のIPアドレス**

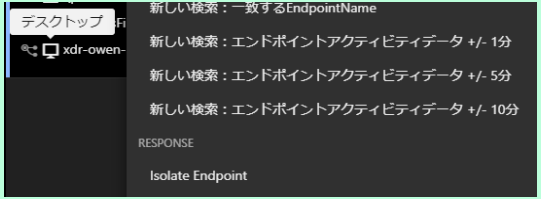


確認ポイント3　**不審なファイル**

確認の結果、リスクなしと判断　→　**対応終了**

③論理隔離

Vision Oneコンソールから端末隔離を実施します
ハイライトの端末名を右クリック>Isolate Endpoint



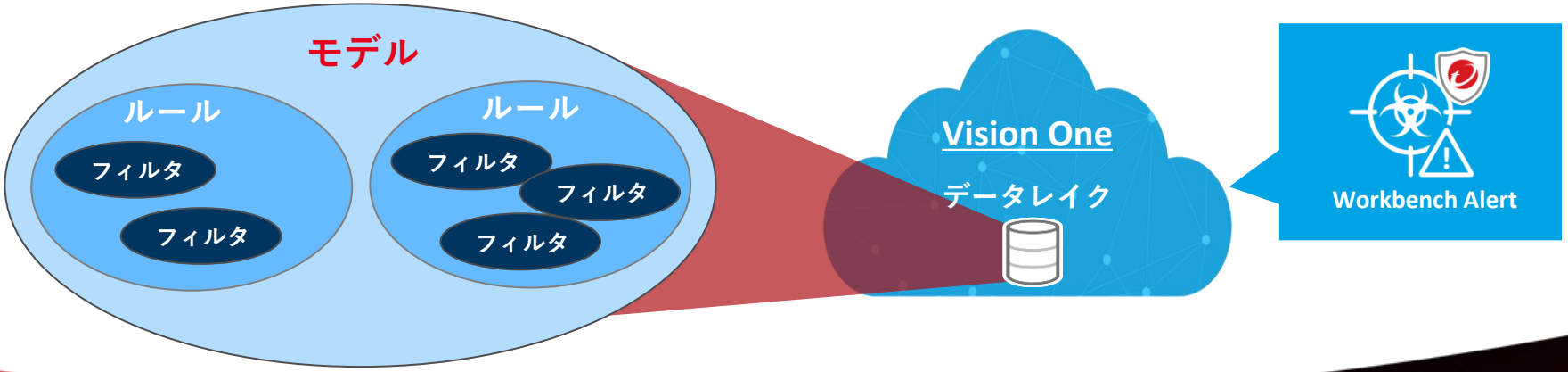
④不審ファイルを回収/解析

Vision Oneコンソールからファイルを回収し、
トレンドマイクロへ解析依頼を行います。
パターンファイルに反映されたら、
パターンのアップデートを実施します。

対応終了

検出 検出モデルとWorkbenchの理解

- 検出モデルは不要なアラートを削減するために、『モデル』-『ルール』-『フィルタ』の３層構造となっています。
- 各フィルタやルールはトレンドマイクロが収集したビッグデータからアナリストによる脅威解析や機械学習技術による脅威情報が実装されています。
- Vision Oneのデータレイクのデータを検出モデルで相関分析を行い、Workbench Alertが検出されます。



調査 Workbench Alertの確認

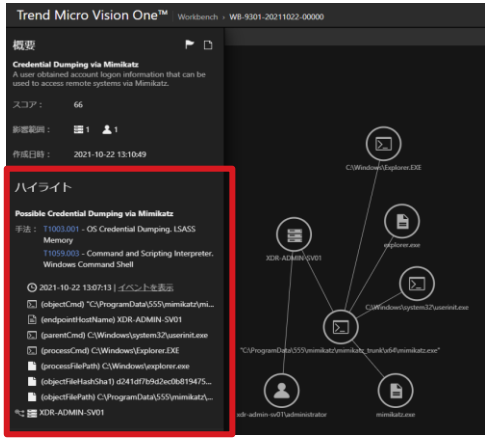
以下のステップで確認をします。

① Workbenchを確認

基本的にはすべてのWorkbenchアラートを確認します。
複数のアラートが表示されている場合は、脅威スコアが高いアラートを優先して調査を進めます。

② アラートの内容を確認する

Workbench Alertの「ハイライト」情報を調査していきます。



確認ポイント1　実行コマンドの確認
確認ポイント2　アクセス元/先のIPアドレスの確認
確認ポイント3　不審なファイルの確認

これらの情報が検出結果の判断材料となります。
調査の結果、攻撃によるものではない場合、
ここまでの調査で**対応完了**となります。

調査 アラート内容を見極めるポイント

SecOps

Workbenchの検出内容が「業務運用によるものかどうか?」をできるだけ簡単に行う方法は？

1. ユーザ・時間帯・セグメントを確認する
2. 管理者・利用者に実施有無を確認
3. Workbench等の不審接続先などを確認

運用である=意図的に実行した ですが、意図的に実行した→攻撃に繋がるということもありえます

運用であることが分かれば、一安心と言いたいところです。ですが、次のページのその例を示しますが、不審ファイルを開いたことで攻撃に繋がるケースもありますので、可能であれば上記の3番を行うことが理想です。ただし、もし攻撃が更に進んだ場合、他のWorkbenchが検出されることがありますので、その時点で気づける可能性もあります。

従って、上記1番，2番などの方法で運用確認を行い、可能であれば、Workbench等の情報を参照し、攻撃であるか？の確度を高めることが判断プロセスにおいての基礎となります。

対処 Vision Oneによるアラート対応

対処が必要と判断したWorkbench Alertについては必要に応じて、
以下の対処を実施します。※レスポンス機能を使う場合は、端末がオンラインである必要があります。

③ 論理隔離

Workbench Alertから端末名を右クリック＞”Isolate Endpoint”

④ 不審ファイルを回収/解析

不審ファイルを特定した場合：
Vision Oneコンソール＞”Collect File”
不審ファイルの特定が出来ない場合：
不審なホストにてATTK※を実行し、不審ファイルの収集

⑤ その他

レスポンス機能を使用することで、以下の対処も可能です。

ブロックリスト登録　(Sha1/IP/URL/Domain) | プロセス停止 | ファイル収集 | エンドポイント論理隔離 | リモートシェル | リモートカスタムスクリプト | メール隔離削除

※ATTK（ウイルス対策ツールキット）の詳細はp19参照

対処 参考：検体解析依頼の方法

トレンドマイクロでは不審なファイルの検体解析サービスを提供しております。トレンドマイクロ製品をご利用のお客様はサポートセンターWebページより検体のアップロードと解析依頼が行えます。

①検体の特定

Workbench Alertや実行プロファイルから不審なファイルを特定します。

②検体の圧縮

検体についてはパスワード付きZipで圧縮をかけてください。パスワードは『virus』と設定をお願いします。※

③検体のアップロード

弊社サポートセンターWebページより検出時の状況など必要な情報を入力の上、検体をアップロードしてください。

※検体をVision Oneコンソールから取得する際は、自動的に圧縮パスワードがかけられた状態でダウンロードされます。（パスワードはランダムに生成されます）
検体解析依頼時は検体を二重圧縮していただき、その際のパスワードを『virus』と設定をお願いします。
解析依頼の備考欄にVision Oneコンソールで自動生成されたパスワードの記載をお願いします。

※詳細については以下FAQを参照願います。
■疑わしいファイル(ウイルス検体)の調査依頼方法
https://success.trendmicro.com/jp/solution/1305428

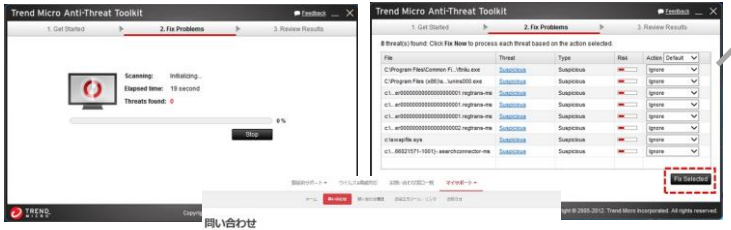
対処　参考：ATTKの使用方法

ウイルス対策ツールキット(ATTK)は、コンピュータの不具合の原因を調べるために必要な各種システム情報（IPアドレス、コンピュータ名等を含む）を記録したログファイルの出力、また不正プログラムであると疑われるファイルのチェックと収集を行います。

①ATTKのダウンロード

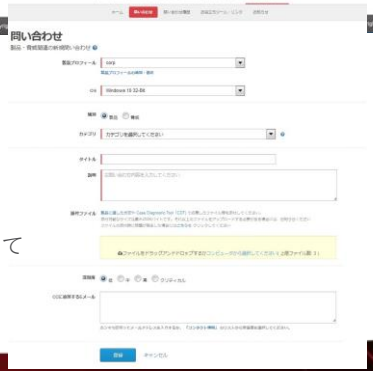
弊社サイトよりATTKをダウンロード
http://downloadcenter.trendmicro.com/index.php?regs=jp&clk=latest&clkval=4436&lang_loc=13&_ga=2.203713560.904196116.1590366638-1395949253.1545360807#fragment-4436

②ATTKの実行(調査ログ収集)



対象の端末でATTKを実行して調査ログを収集

③調査ログのアップロード



ビジネスサポートポータルから調査ログをアップロード

※詳細については以下FAQを参照願います。
■調査ログ収集用ウイルス対策ツールキット（ATTK）の使用方法について
https://success.trendmicro.com/jp/solution/1097836

攻撃シミュレーションを使った調査の流れ

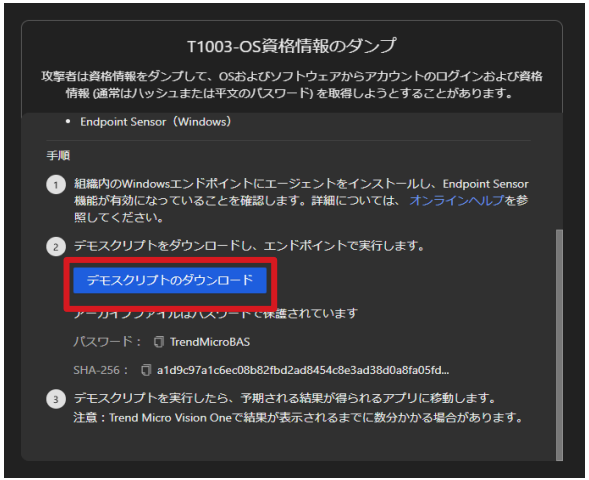
攻撃シミュレーション調査の流れ

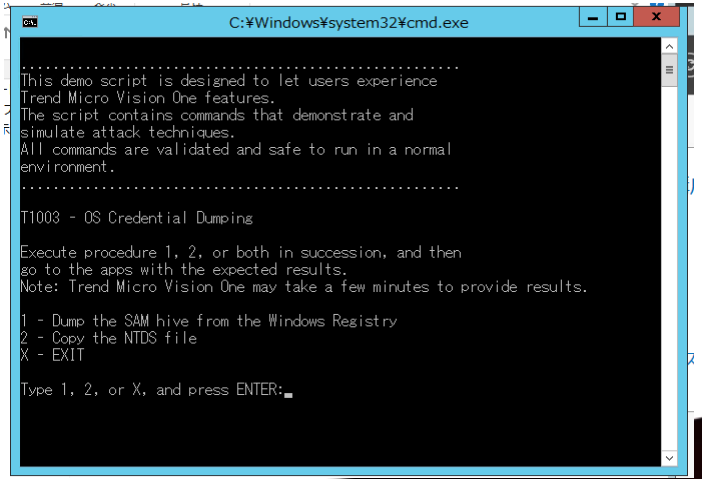
Vision Oneを使ったセキュリティ運用を評価するために、Vision Oneコンソールからダウンロード可能な攻撃シミュレーション用デモスクリプトを実行し、検出の確認、調査、対処の流れを確認していきます。

1. Workbenchを確認
2. アラートの内容を確認
    1. 実行コマンド
    2. アクセス元／先のIPアドレス
    3. 不審なファイル
3. 論理隔離
4. 不審ファイルを回収／解析

Step0 デモスクリプトをダウンロードし、端末上で実行する

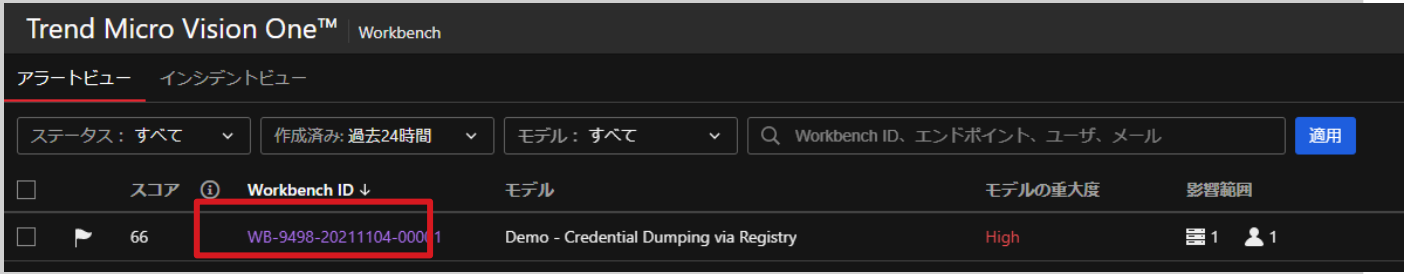
Step	対応内容	確認内容
0	攻撃をシミュレーションするデモスクリプトを実施する	☐ Vision Oneコンソール下部のアイコンから、[シミュレーション] – [Workbench] – [シミュレーションを試す]をクリック ☐ T1003-OS資格情報のダンプ [デモスクリプトのダウンロード]をクリック ☐ 記載されたパスワードを使って” T1003_Demo_Script.zip”を解凍し、センサーが有効になっている端末でシナリオ1,2を実行する ※センサーにおいて挙動監視機能が有効になっているとデモスクリプトの実行が完了しないため、予め無効にしておく必要があります。

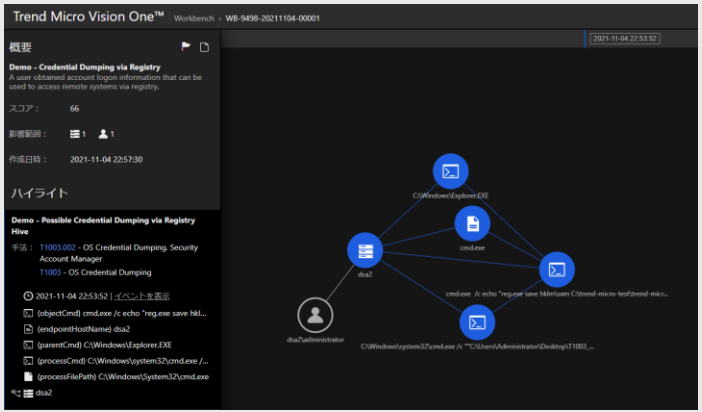




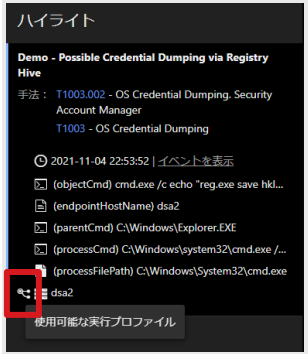
Step1　Workbenchを確認

Step	対応内容	確認内容
1	Workbenchを確認	☐ “Demo - Credential Dumping via Registry”アラートが発令されていることを確認
2	アラートの内容を確認	☐ Workbench IDをクリックし、内容を確認



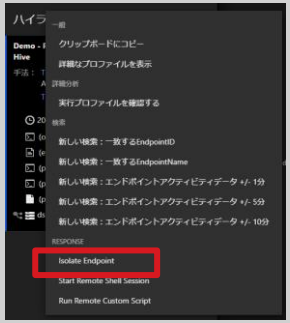


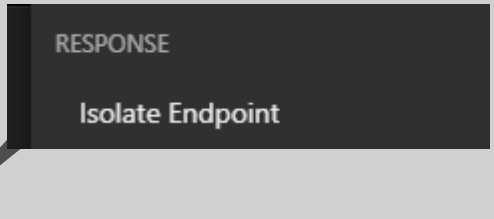
Step2　アラート内容を確認

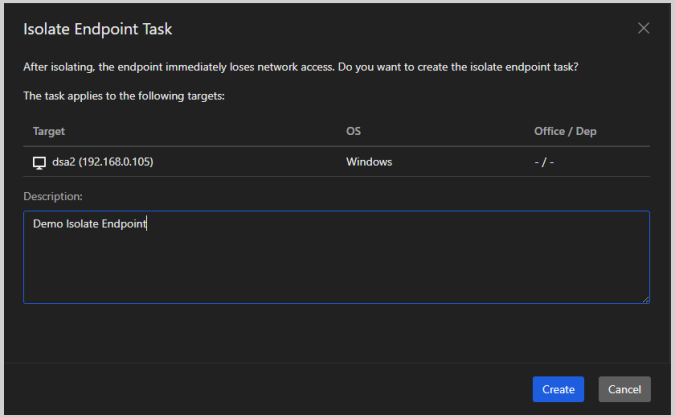
Step	対応内容	確認内容
2-1	アラートの内容を確認 （実行コマンド）	☐ 左側のハイライト-(objectCmd)を確認  cmd.exe　/c echo "reg.exe save hklm¥sam C:¥trend-micro-test¥trend-micro-test.hive"
2-2	アラートの内容を確認 （不審ファイル）	☐ 実行プロファイルを表示 ☐ プロセスツリーから” T1003_Demo_Script.bat”を不審ファイルとして確認  

Step3　論理隔離

Step	対応内容	確認内容
3	論理隔離	☐ Workbenchに戻り、ハイライト - [ホスト名]を右クリック – [Isolate Endpoint]をクリック

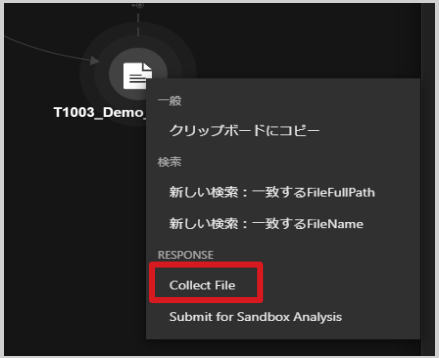


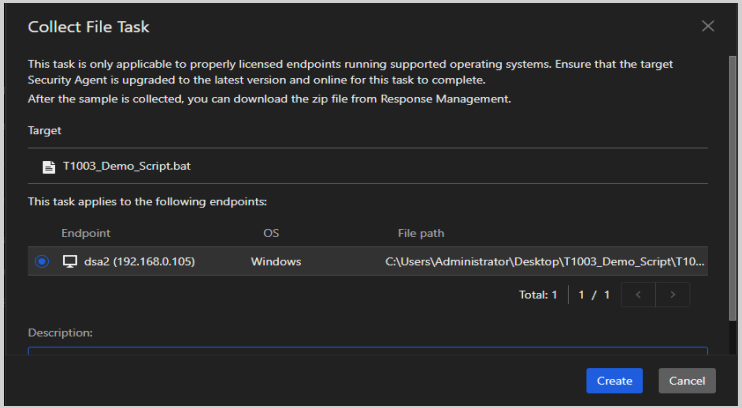




Step4　不審ファイルを回収/解析

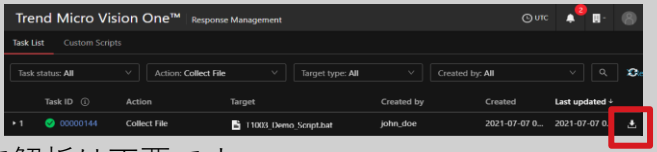
Step	対応内容	確認内容
4	**不審ファイルを回収**	◘ 実行プロファイルを再度表示し、不審ファイルを右クリック – [Collect File]





※Collect Fileには20分ほど時間がかかる可能性があります

◘ Response Management から検体ファイルをダウンロード可能



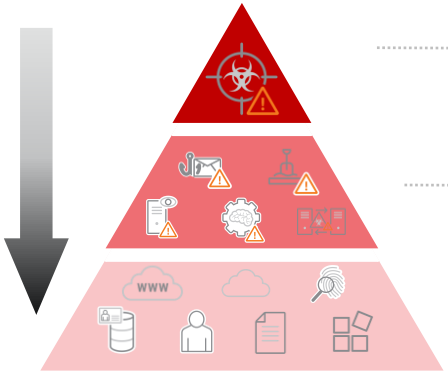
今回はデモファイルなので解析は不要です。
実際のインシデント対応の場合は、以下の手順を実施します。

◘ 不審ファイルをトレンドマイクロへ解析依頼を行う
◘ パターンファイルに反映されたら、パターンのアップデートとフルスキャンを実行し、対応完了

Appendix

参考：Vision Oneにおけるレベル別監視運用案

スキル・工数・精度：低



スキル・工数・精度：高

案1

Workbenchを主体としたベーシックな運用、アラートが少なく、確度が高いアラートに絞りたい場合

案2

案1とObserved Attack Techniqueの検出を組み合わせ、Workbenchの範囲外の攻撃手法も注視

案3

案1と2+Threat Huntingの領域、Vision Oneで明確な検出のないものも外部情報を組み合わせサーチ

Vision Oneの運用案

Model=Workbenchと同義、RuleやFilterを組み合わせた精度の高いアラート

Rule=Filterで取得された情報を組み合わせ、攻撃手法を定義したもの

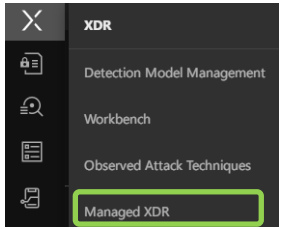
Filter=データの源泉となる最も粒度の細かいデータ、正常挙動も多く含む

Filterまたは、外部情報との連携等

Vision Oneでの検知レイヤー

Vision Oneは、元来SOC向けの高度なオペレーションを前提として設計されていますが、主要な機能のみ扱うことで、組織の人材や経験が不足している場合でも運用が可能です。例えば、上記の案1にあるWorkbenchに絞った運用を行うことで、最低限のリソースで既存製品のすり抜けに対する効果的な対応が可能になります。もちろん、案2、3レベルの監視が行えることが理想ですが、組織の態勢やスキルレベルの向上を計画しながら、徐々に移行できることが理想です。

参考：組織力に応じた運用案を選択する



テスト運用でどのような検出があるかを知り、自社のスキルレベルとリソースから運用モデルを判断する

外部委託

自社では難しいので、SOCベンダに監視を依頼する

運用案1

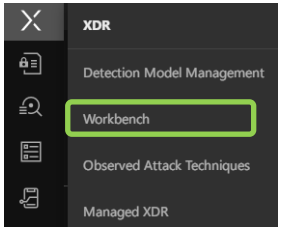
運用案2

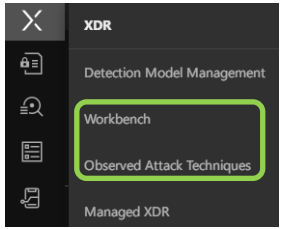
運用案3

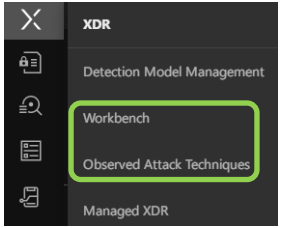
WorkbenchのHighリスク以上のみを調査

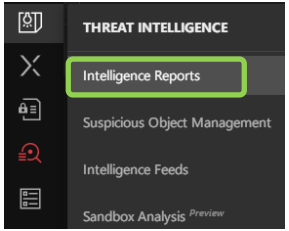
WorkbenchとOATのMediumリスク以上を調査

WorkbenchとOATのMed以上、かつThreat Huntingも行う









Workbench主体

WorkbenchはSOCのアラート疲弊に対処するためにデザインされた確度の高いリスクをアラートするために設計されています。

Workbench+OAT

Workbenchに加え、攻撃で悪用される手口を単体で定義しているのがOATです。この二つを注視することで、見逃しのリスクは低くなります。

Workbench+OAT+Threat Hunting

WorkbenchとOATに加え、外部Intelligenceの参照やMITREのTechによるThreat Huntingを行い、リスクを限りなく低減します。

難易度高

参考： Trend Vision One シミュレーター

- Trend Vision One シミュレーターでは、仮想環境上に予め設定およびログデータが準備されており、実際のご利用いただく場合に近しい環境で機能の操作や製品の体験をいただくことが可能です。
- 下記の「Trend Vision One シミュレーター」のURLリンクにアクセスして下さい。
- https://resources.trendmicro.com/vision-one-test-drive-jp.html