Tanium™ Reveal ユーザーガイド

バージョン 1.1. 4

2020年 4月 01日

この文書の内容は予告なく変更されることがあります。また、本書に記載の内容は「現状のまま」提供されており、正確には万全を期しておりますが、Taniumの顧客販売契約に規定されている保証を除き、明示または暗黙を問わずいかなる保証もしません。別段の規定がない限り、Taniumはいかなる責任も負いません。TaniumおよびそのサプライヤはTanium Inc.がかかる損害の可能性を事前に通知されていたとしても、本書の使用または使用できないことから生じる、利益損失やデータ損失をはじめとする間接的損害や特別損害、結果的損害、および付随的損害に対して一切の責任を負いません。

本書で使用されているIPアドレスは、実際のアドレスであることを意図していません。本書に記載されている例、コマンド表示出力、ネットワークトポロジ図、およびその他の図は、例示の目的にのみ使用されています。例示コンテンツに実際のIPアドレスが使用されていたとしても、特別な意図はなく、偶然です。

最新のTanium製品のマニュアルについては、https://docs.tanium.com を参照してください。

Taniumは米国およびその他の国におけるTanium,Inc.の商標です。記載されているその他の社名、製品名、サービス名は各社の商標または登録商標です。

目次

Revealの概要

Revealを使用すると、IT環境全体のエンドポイントに保存されている機密の非構造化データを検知できます。Revealを使用して、パターンが一致するアーティファクトを継続監視します。パターンに一致する機密なコンテンツが見つかったとき、そのコンテンツが存在するファイルにラベルをつけ、さらに分析し、または措置をとり、法規制コンプライアンス、情報セキュリティ、データのプライバシー問題に対処することができます。

ルールセット

特定の基準へのコンプライアンスを評価するなど、特定の目的のために集合的に使用するルールセットグループの関連ルール、および特定のエンドポイントグループへのターゲットルール。

特定のエンドポイントグループに最も関連性のあるReveal機能を提供するために、ルールセットを作成、適用します。例えば、財務情報または健康の記録に特有の機密データを見つけるルールに適用するルールセットを作成できます。

Revealには以下のようなルールセットがあります。

PCI

PCIの基準により、クレジットカード情報を受け入れ、処理、保存、転送する企業は安全な環境を維持できます。

HIPPA

HIPPAの基準により、患者の健康に関する機密データを保護できます。

GDPR

GDPRの基準は個人データを保護し、欧州連合のコンプライアンスの順守を確保します。

CCPA

CCPAの基準により個人データが保護され、カリフォルニア州でのコンプライアンスを確保します。

ルール

ルールで、特定のタイプのファイルで一致するパターンと指定できます。また、Revealが一致を見つけたとき、ファイルまたはエンドポイントでアクションを実行できます。例えば、社会保障番号のパターンが一致するすべてのテキスト文書に「機密」ラベルを追加できます。

複数のルールを作成して、各エンドポイントにある同じファイルのコンテンツを評価できます。例えば、クレジットカード番号を検知するルール、社会保障番号を検知するルール、Eメールアドレスを検知するルールを作成し、特定のタイプのファイルで各ルールの評価ができます。各ルールの結果に、どのファイルにどのパターンの一致が含まれるか示されます。結果は各ルールごとに分類されていて、簡単にパターンの一致を見つけることができます。

パターン

Revealでは、パターンは他の情報のコンテキストに隠れている可能性のある、エンティティに一致する式です。

例えば、パターンはクレジットカード番号やEメールアドレスなどのエンティティに一致する場合があります。このようなパターンは、ワードプロセッサ文書、テキストファイル、PDF文書またはスプレッドシートのような非構造データのエンティティと一致させるためルールに割り当てられます。Revealは、クレジットカード番号、社会保障番号、Eメールアドレスなど、機密情報のいくつかタイプのパターンを提供します。リストを拡張するには、テクニカルアカウントマネージャにお問い合わせください。

はじめに

1. Tanium Revealをインストールします。詳細については、13ページのRevealのインストールを参照してください。
2. ルールを作成します。詳細については、16ページのルールの作成を参照してください。
3. ルールセットを作成します。詳細については、18ページのルールセットの作成を参照してください。
4. ルールの一致を管理します。詳細については、21ページのルール一致の調査を参照してください。
5. 検証を作成します。くわしくは、23ページのパターン一致の検証をご覧ください。
6. エンタープライズ全体で機密情報を検索します。くわしくは、25ページのエンタープライズ全体の検索をご覧ください。

Revealの要件

Revealをインストールおよび使用する前に要件を確認してください。

Taniumの依存関係

Reveal製品モジュールのライセンスに加えて、ご使用の環境が以下の要件を満たしていることを確認してください。

コンポーネント	要件
Platform	7.2.314.2831以降
Tanium Client	6.0.314.1540以降を推奨
Tanium Module	Tanium™ Trace 2.7.10.0001またはTanium™ Threat Response 1.1.0

Tanium Module Server

Revealがインストールされ、Tanium Module Serverのホストコンピュータ上のサービスとして実行されます。Module Serverへの影響は最小限であり、使用状況によって異なります。

エンドポイント

RevealはWindowsのMacOSのエンドポイントに対応します。最大2GBの空きディスク容量が必要です。

ホストとネットワークセキュリティの要件

Revealを実行するには、特定のポートとプロセスが必要です。

ポート

Revealの通信には、以下のポートが必要です。

コンポーネント	ポート	方向	目的
Module Server	17444	インバウンド	エンドポイントへのライブ接続用にModule Serverに接続します。

セキュリティの除外

未知のホストシステムプロセスを監視およびブロックするためにセキュリティソフトウェアが環境内で使用されている場合、セキュリティ管理者はTaniumプロセスを干渉なく実行できるように除外を作成する必要があります。

表1：Revealセキュリティの除外

対象デバイス	プロセス
Module Server	*<Tanium Module Server>*\services\Reveal\node.exe
エンドポイント	*<Tanium Client>*\Tools\EPI\TaniumExecWrapper.exe
	<Tanium Client>\Tools\EPI\TaniumEndpointIndex.exe
	<Tanium Client>\Tools\Reveal\TaniumReveal.exe
	<Tanium Client> \Tools\Trace\TaniumTraceWebsocketClient.exe

ユーザーロールの要件

ロールベースのアクセスコントロール(RBAC)のアクセス許可を使用して、Reveal機能へのアクセスを制限できます。

表2：Tanium Revealユーザーロール権限

アクセス許可	Reveal管理者	Reveal読み取り専用ユーザー	Revealサービスアカウント	Revealユーザー
Show Reveal (Revealを表示) Revealワークベンチへのアクセス				
Reveal Affected Files (Revealの影響を受けたファイル) 影響を受けたファイルの表示を有効化				
Reveal Quick Search (Revealクイック検索) クイック検索結果の表示を有効化				

アクセス許可	Reveal管理者	Reveal読み取り専用ユーザー	Revealサービスアカウント	Revealユーザー
Reveal Rules Deploy (Revealルールのデプロイ) エンドポイントへのルールのデプロイを有効化				
Reveal Rules Deploy Status (Revealルールデプロイステータス) Revealワークベンチへのアクセス	1			1
Reveal Rules Read (Revealルールの読み取り) ルールの表示とリストを有効化	1			1
Reveal Rules Write (Revealルールの書き込み) ルールの編集を有効化				
Reveal Rule Sets Read (Revealルールセットの読み取り) ルールセットの表示とリストを有効化	1			1
Reveal Rule Sets Write (Revealルールセットの書き込み) ルールセットの編集を有効化				
Reveal Service Use (Revealサービスユーザー) ユーザーがサービスアカウントユーザーとして作業を実施可能にする				

アクセス許可	Reveal管理者	Reveal読み取り専用ユーザー	Revealサービスアカウント	Revealユーザー
Reveal Service User Read (Revealサービスユーザーの読み取り) サービスアカウントユーザーの詳細を表示できます。	1			
Reveal Service User Write (Revealサービスユーザーの書き込み) サービスユーザーアカウントへの変更を有効化				
Reveal Snippets (Revealスニペット) 影響を受けるファイルのスニペットの表示を有効化します。				
Reveal Use API (Reveal APIの使用) APIを使用してReveal操作を実行する	1	1	1	1
Reveal Validations Deploy (Reveal検証のデプロイ) エンドポイントへの検証のデプロイを有効化				
Reveal Validations Deploy Status (Reveal検証のデプロイステータス) 検証デプロイのステータス表示を有効化	1			1

アクセス許可	Reveal管理者	Reveal読み取り専用ユーザー	Revealサービスアカウント	Revealユーザー
Reveal Validations Read (Reveal検証の読み取り) 検証の表示とリストを有効化	1			1
Reveal Validations Write (Reveal検証の書き込み) 検証の編集を有効化				

[1] 提供された許可を示します。

コンテンツセットとアクセス許可の詳細および説明については、Tanium Core Platformユーザーガイド：ユーザーとユーザーグループを参照してください。

ルールの一致を調査するためエンドポイントに直接接続するユーザーは全員、**[Trace Live Connections Write (Traceライブ接続書き込み)]**へのアクセス許可が必要です。

> **注意：[Bypass Action Approval (アクションの承認をバイパス)]**という高度なロール**[Trace Analysis (Trace分析)]**コンテンツセットに与えて、アクションの承認を経ずTraceユーザーがエンドポイントにライブ接続できるが、残りのアクションすべてでは承認が必要なままにします。

Revealのインストール

Revealは**[Tanium Solutions (Taniumソリューション)]**ページからインストールできます。

使用を開始する前に

- リリースノートをお読みください。
- 8ページのRevealの要件を確認してください。

> **注意：** Revealを使用するには、Tanium™ Trace 2.7.10.0001またはTanium™ Threat Response 1.1.0が必要です。くわしくは、TraceのインストールまたはThreat Responseのインストールをご覧ください。

Revealをインポートする

[Tanium Solutions (Taniumソリューション)]ページからRevealをインポートします。

1. メインメニューから、**[Tanium Solutions (Taniumソリューション)]**をクリックします。
2. **[Tanium Reveal]**の下で、**[Import (インポート)]**をクリックします。

   > **注意：** Tanium Revealはライセンスされたソリューションです。**[Tanium Solutions (Taniumソリューション)]**ページにTanium Revealが掲載されていない場合は、テクニカルアカウントマネージャにご連絡ください。

3. **[Content Import Preview (コンテンツインポートのプレビュー)]**ウィンドウでパッケージを展開して、インストールされるTaniumコンテンツを確認することができます。**[Proceed with Import (インポートを続行)]**をクリックします。
4. インストール処理が完了したら、ブラウザをリフレッシュします。
5. メインメニューから、**[Reveal]**をクリックします。Revealのホームページが表示されます。

インストールを検証する

Revealがインストールされていることを確認するには、Taniumソリューションページに移動し、インストール済みのバージョンを確認します。Revealのホームページでインストールされているバージョンを確認するには、情報 をクリックします。

Revealを設定する

サービスアカウントを構成する

サービスアカウントは、Revealの定期的なメンテナンス活動に使用されます。

1. Revealのホームページから、**[Configure Service Account (サービスアカウントの設定)]**をクリックします。
2. ユーザー名とパスワードを入力します。
3. **[Save (保存)]**をクリックします。

> **注意：**サービスアカウントを構成するとエンドポイントにRevealツールがインストールされ、Revealのサービスが開始します。最初のツールのデプロイ後、エンドポイントでステータスが表示されるまでに最大4時間かかることがあります。

Revealのアクショングループを構成する

アクショングループは、Revealパッケージをデプロイするエンドポイントのセットを定義します。デフォルトでは、Revealアクショングループ用の**[Computer Group Targets (コンピュータグループのターゲット)]**設定は、**[No Computers (コンピュータなし)]**になっています。アクショングループを、**[All Computers (すべてのコンピュータ)]**または定義した任意のコンピュータグループに設定できます。

1. メインメニューから、**[Actions (アクション)] > [Scheduled Actions (予定済みアクション)]**の順にクリックします。
2. **[Tanium Reveal]**のアクショングループをクリックした後、**[Edit (編集)]**をクリックします。
3. Revealに使用するエンドポイントグループのコンピュータグループを選択します。**[Save (保存)]**をクリックします。
4. 資格情報を入力して**[OK]**をクリックします。

Revealのバージョンをアップグレードする

ソリューションページから最新バージョンにRevealをアップグレードします。

1. メインメニューから、**[Tanium Solutions (Taniumソリューション)]**をクリックします。
2. Revealを特定し**[Upgrade to X.X.X.XX (X.X.X.XXへのアップグレード)]**をクリックします。
3. **[OK]**をクリックします。
   ソリューションのインポートウィンドウが開き、すべての変更とインポートオプションのリストが表示されます。

4. **[Proceed with Import (インポートを続行)]**をクリックしてパスワードを入力してください。インストールおよび構成プロセスが開始されます。
5. アップグレードを確認するには、**[Tanium Solutions (Taniumソリューション)]**ページに戻り、**[Installed: X.X.X.XX (インストール済み: RevealのバージョンX.X.X.XX)]**のRevealバージョンを確認します。

ヒント: Revealのバージョンが更新されていない場合は、ブラウザのウィンドウを更新してください。

次にやるべきこと

Revealの使用について詳しくは、7ページのはじめにを参照してください。

ルールの作成

ルールとは、指定する条件と、条件が満たされたときに実行するアクションの組合せです。ルールは、1時間ごとにTanium™ Indexにハッシュされたファイルのすべてで評価されます。ルールのすべての条件が満たされたときに、アクションがトリガーされます。例えば、機密情報の社会保障番号パターンとの一致を含むファイルにラベル付けすることができます。複数のルールを同じファイルを対象に適用できるため、同じファイルセットで多種の機密情報を検出できます。

ルール評価の基準

ファイルを評価するルールでは、ファイルは次の基準に一致しなければいけません。

- ファイルは、ハッシュタイプMIMEを使用してTanium Indexがハッシュする必要があります。
- ファイルは、Tanium Revealが読み取ることができる形式でなければなりません。これには、テキストファイル(テキスト、XML、CSVなど)およびバイナリファイル(PDF、Microsoft Officeなど)を含みます。
- バイナリファイルは32MB未満でなければなりません。このデフォルトのサイズ制限を増やすには、Revealのconfig.jsonにある`max_file_size_kb`設定を更新します。テキストファイルにはサイズ制限はありません。
- Revealのconfig.jsonにある`filter_stems`または`filter_regexes`設定ではファイルをフィルタリングしてはいけません。

ルールを作成する

1. Revealメニューから、**[Rules (ルール)]**をクリックします。**[New Rule (新しいルール)]**をクリックします。
2. ルールの名称と説明を入力します。
3. ルールを含める1つまたは複数のルールセットを選択します。**[Add Rule Set (ルールを追加)]**をクリックし、ルールと関連付けるルールセットを選択します。**[Save (保存)]**をクリックします。
4. 条件を追加します。条件にはファイルタイプやパターンが含まれます。**[Add Condition (条件を追加)]**をクリックし、**[File Type (ファイルタイプ)]**または**[Pattern (パターン)]**を選択します。
    1. ファイルタイプの条件で、ルールの対象となるファイルタイプを選択します。少なくとも1つのファイルタイプを選択しないと、ルールは評価を行いません。
    2. パターンで、一致するパターンを選択します。

5. 条件が一致したときにルールが実行するアクションを選択して、**[Apply (適用)]**をクリックします。一致を含むファイルへラベルを適用するよう選択できます。
6. **[Save (保存)]**をクリックします。

デプロイのルール

Revealはルールパッケージを通じてエンドポイントにルールをデプロイします。ルールパッケージには、ルールセットにルールをマップする情報と、ルールを監視する特定のコンピュータグループのエンドポイントの決定方法も含まれます。エンドポイントには複数のルールセッチを適用できます。また、適用できるルールセットにあるすべてのルールが評価されます。

既存のルールをアップデートしたり、新しいルールを作成すると、ルールは次の予定済みデプロイで自動的に含められます。更新済みルールをただちにデプロイするには、**[Deploy Rules (ルールのデプロイ)]**をクリックし、資格情報を入力して**[OK]**をクリックします。

ルールセットの作成

ルールはグループルールをまとめて設定し、特定のエンドポイントグループに割り当てます。ルールを、機密情報の特定のカテゴリに対処する、または特定のファイルタイプを監視するルールセットにグループ化できます。

たとえば、エンドポイントの1つのグループに特定のるルール適用して監視したいが、他のグループはそのままにしておきたいことがあるでしょう。あるいは、使用可能なルールのサブセットをあるグループのエンドポイントに適用したいこともあるでしょう。

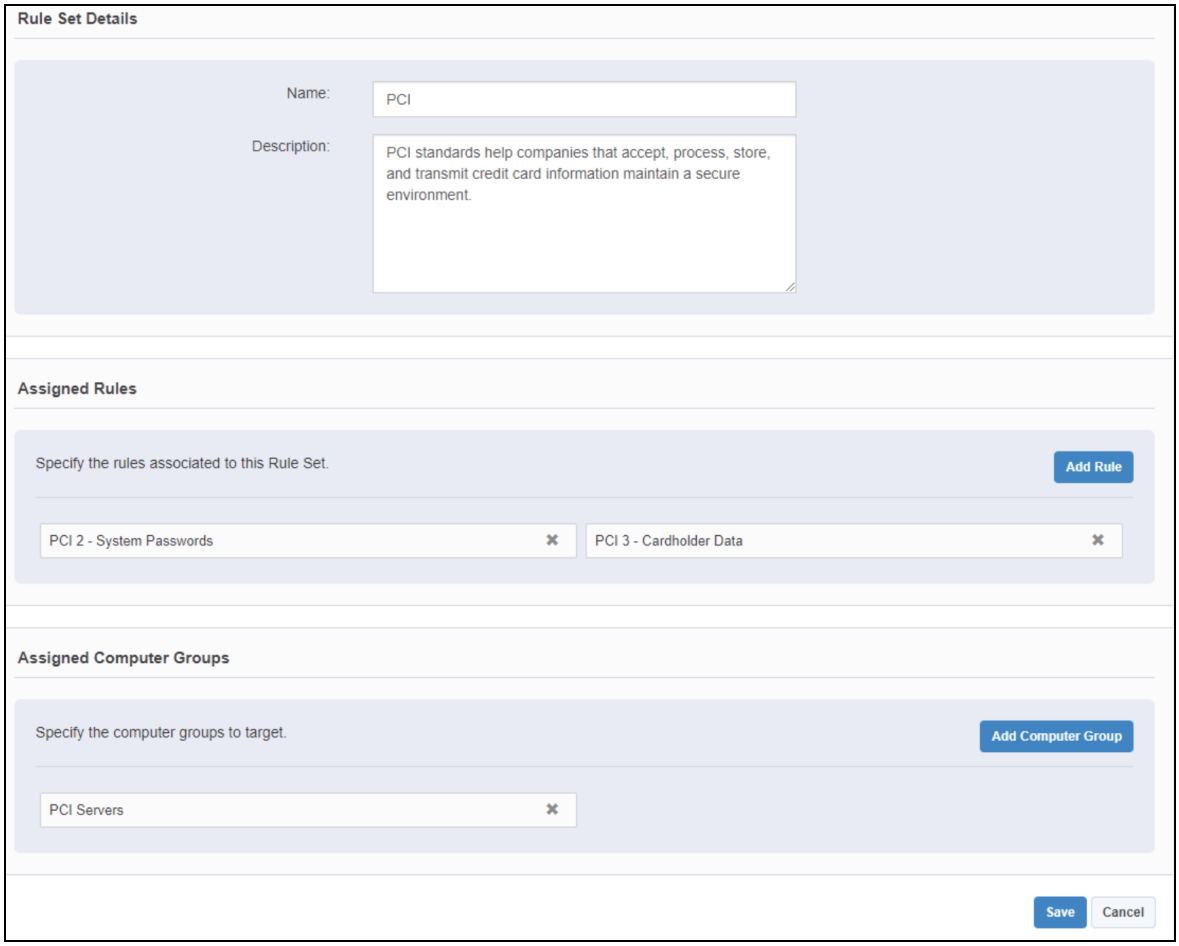
各ルールセットに割り当てられたルールの数、ターゲットのコンピュータグループ、また関連するルールへの変更の保留があるかどうかを表示できます。

デフォルトで、各ルールセットには割り当てられたルールが1つあります。デフォルトのルールは編集できませんが、削除や、そのルールを複製して特定のニーズに合わせたカスタマイズができます。

ルールセットを作成する

1. Revealメニューから、**[Rule sets (ルールセット)]**をクリックします。**[New Rule Set (新しいルールセット)]**をクリックします。

2. ルールセットの名称と説明を入力します。



3. ルールセットに関連付けるルールを1つまたは複数選択します。**[Add Rule (ルールを追加)]**をクリックし、ルールセットに関連付けるルールを選択します。**[Save (保存)]**をクリックします。
4. ルールセットのターゲットとなるコンピュータグループを追加します。ルールセットに関連付けられたルールは、指定したコンピュータグループのエンドポイントに適用されます。
5. **[Save (保存)]**をクリックします。

既存のルールセットにルールを追加する

1. Revealメニューから、**[Rule sets (ルールセット)]**をクリックします。
2. ルールを1つまたは複数追加するルールセットのタイトルをクリックします。
3. **[Add Rule (ルールを追加)]**をクリックし、ルールセットに関連付けるルールを選択します。**[Save (保存)]**をクリックします。

ルールセットを削除する

1. Revealメニューから、**[Rule sets (ルールセット)]**をクリックします。
2. 削除するルールセットを選択します。
3. **[Action (実行)] > [Delete (削除)]**をクリックします。ルールを削除することを確認します。

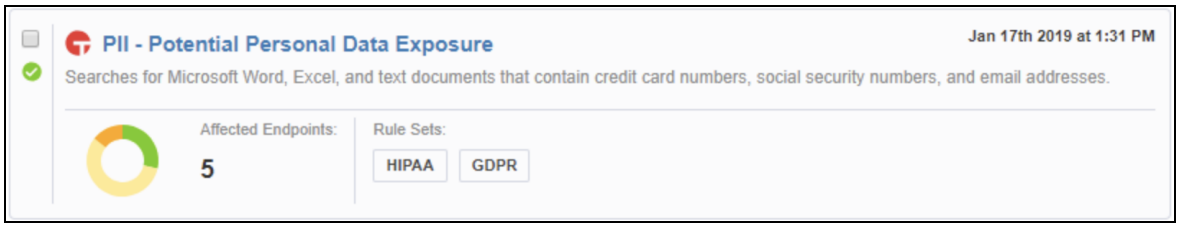
ルールー致の調査

Revealがルールとの一致を見つけると、ルールとルールセットページは、エンドポイントに発生した一致の数に基づきルールの影響を受けたすべてのエンドポイントの内訳を表示し、更新されます。一致の詳細についてさらに調査できます。各ルールには、一致が検出されたエンドポイント数の情報が表示されます。エンドポイントとのTraceライブ接続を作成でき、またさらに分析を実行するためドリルダウンできます。エンドポイント全体で一定期間の一致数を調査でき、またコンピュータグループまたはキーワードで一致をフィルタすることができます。

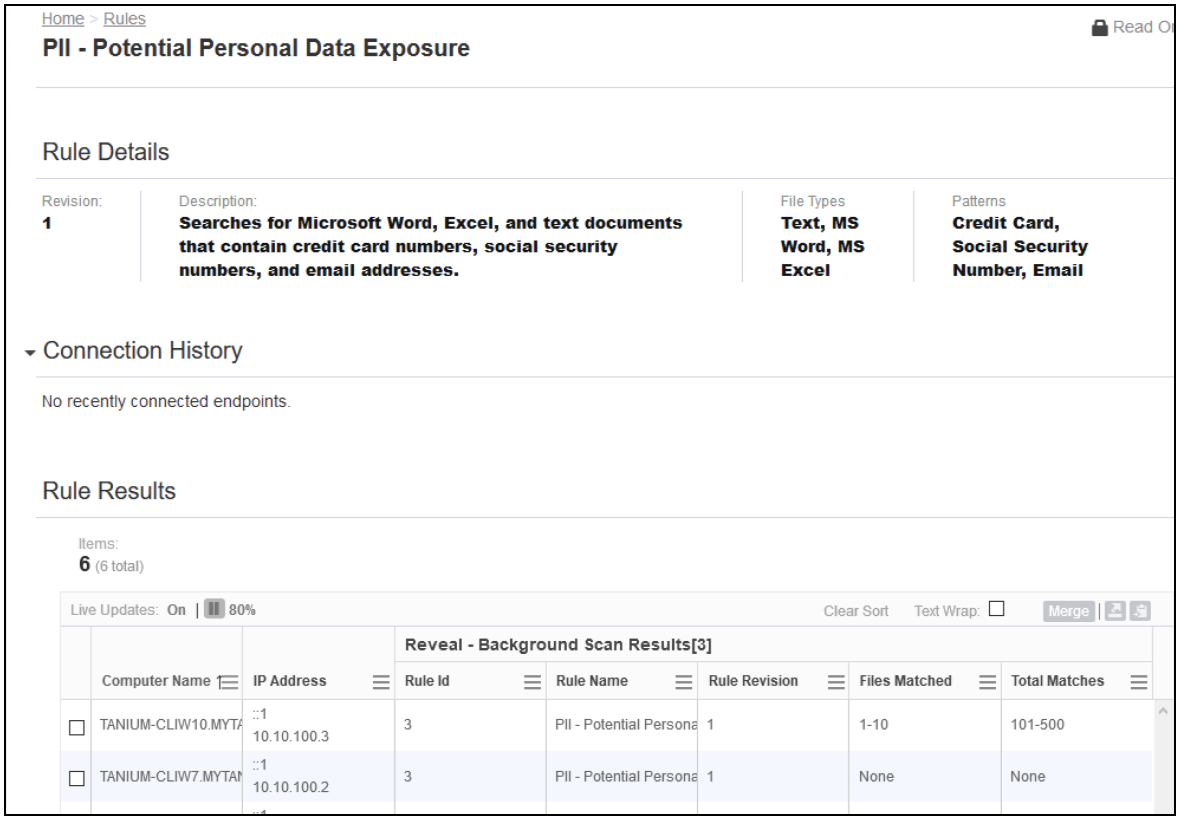
ルールページから、ルールー致が起きたときに影響を受けたエンドポイントと一致が検出されたファイルを調査できます。

エンドポイント別に調査する

1. Revealメニューから、**[Rules (ルール)]**をクリックします。
2. 調査する一致を含むルールをクリックします。



3. 一致のあるエンドポイントがRevealに表示されます。



4. エンドポイントを選択して**[Create Connection (接続の作成)]**をクリックします。エンドポイントへのライブ接続が開きます。エンドポイントの接続が**[Active (アクティブ)]**と表示されている場合、エンドポイント名をクリックして一致を含むファイルを表示します。
5. 一致のあるファイルには、ファイル名、ルールID、ヒット数、変更日、サイズ、およびパスが表示されます。
6. 影響を受けたファイルをクリックして、コンテキストでパターンが一致するスニペットを表示します。

ルールが一致するファイルにアクションを取る

ルールー致を含むファイルにルールがラベルを適用する場合、TaniumのQuestionを使用して、影響を受けたファイルに対するアクションを実行できます。

1. メインメニューからInteractをクリックします。
2. 次のQuestionを実行します：**[Get Reveal - Label Results from all machines]**。結果グリッドには、ファイルに適用されたラベルとラベル付けされたファイルの数が表示されます。
3. アクションが必要なラベルの行を選択し、それから**[Deploy Action (アクションのデプロイ)]**をクリックします。アクションをデプロイするワークフローのページが表示されます。

詳細については、Tanium Interactユーザーガイド：Questionを参照してください。

パターン一致の検証

ルールのパフォーマンスの正確性を改善し、ルールが対象とするデータに関する偽陽性結果の数を減らすための検証を作成します。パターン一致が正確であり、対象データで一貫することを確認し、ルールを検証します。ルールを検証することで、関連するパターンマッチで確認または拒否された結果に関するデータの分析に集中できます。

検証には、検証中に表示されるものとテキストが完全に一致するというルールの観点に従い、パターンマッチを適用します。新しい検証は保留中の状態で表示され、作成したユーザーのみ閲覧することができます。保留中の検証は自動的にスニペット結果に適用されますが、公開されるまではルールのヒット数には影響しません。

検証の作成

1. Revealメニューから、**[Rules (ルール)]**をクリックします。
2. **[Rule Results (ルールの結果)]**で、パターンと一致する1つ以上のファイルがあるエンドポイントを選択します。**[Create Connection (接続の作成)]**をクリックします。
3. 1つ以上のパターンの一致を含むファイルを選択します。
4. パターンの一致が検出されたことを示すスニペットを表示します。**[Add Validation (検証を追加)]**をクリックして、パターンの一致を確認または拒否します。
5. スニペット内の関連テキストをハイライト表示します。検証は、最初の一致に対して追跡されます。
6. **[Confirm (確認)]**または**[Reject (拒否)]**を選択します。拒否されたスニペットは将来の結果から除外されます。**[Apply (適用)]**をクリックします。
7. 検証の名前と説明を入力します。Revealは検証したテキストのプレビューを表示し、現在のファイルで検証に影響するパターン一致の数、検証に影響するルール、マッチングパターンを確認または拒否すべきかどうかをレポートします。
8. **[Save (保存)]**をクリックします。

検証のデプロイ

検証をデプロイして、すべての保留中の検証を公開済み検証に移動します。検証をデプロイして、新しい**[Reveal-Validations (Reveal-検証)]**パッケージを作成し、**Reveal - Deploy Validations (Reveal - 検証のデプロイ)**]保存済みアクションを再作成します。他のユーザーの保留中の検証は保留中のままです。

公開済みの検証は、対応するルールのすべての一致に適用されます。拒否された一致は無視されます。

1. Revealメニューから、**[Rule Validations (ルールの検証)]**をクリックします。
2. **[My Pending (マイ保留中)]**をクリックして、保留中のルール検証を表示します。
3. **[Deploy Validations (検証のデプロイ)]**をクリックします。

公開済み検証の監査

検証の監査は、検証の適用により影響を受けたパターン一致のスニペットを表示します。

1. Revealメニューから、**[Rule Validations (ルールの検証)]**をクリックします。
2. 公開済みの検証をクリックして、検証を適用したパターン一致を含むエンドポイントを表示します。
3. エンドポイントをクリックして、検証により影響を受けるファイルを表示します。
4. ファイルをクリックして、検証に一致するスニペットを表示します。

エンタープライズ全体の検索

Revealを使用して、企業全体で機密情報の特定の項目を検索します。検索文字列と一致する機密情報をリアルタイムで検索でき、ルールー致からのアラートを待つことはありません。クイック検索は、Revealアクショングループ内のすべてのエンドポイントを対象とします。検索でターゲットにしたい、検索文字列とパラメータを使用します。Revealは、提供する検索条件に一致する結果の一覧を表示します。

Revealは検索文字列を小文字に変換し、句読点を削除し、冠詞などの一般的なストップワードを削除します。Revealは次に、環境全体でトークンの正確な順序を検索します。たとえば、検索クエリが`process is started`であれば、これは`["process","started"]`としてトークン化されます。これらのトークンは`the malicious process has started`には一致しますが、`started the process`には一致しません。トークンはクエリと同じ順序ではないためです。

クイック検索の実行

1. Revealメニューから、**[Quick Search (クイック検索)]**をクリックします。
2. 検索フィールドに、検索文字列を入力します。たとえば、123-45-6789と入力し、完全な一致を見つけます。
3. 希望に応じて、**[Search Parameters (検索パラメータ)]**キャレットを展開します。
4. **[Add Condition (条件の追加)]**をクリックします。**[File Type (ファイルタイプ)]**を選択します。
5. 検索のターゲットにする1つ以上のファイルタイプを選択します。
6. **[Search (検索)]**をクリックします。

クイック検索結果の調査

クイック検索結果は、Revealが検索基準に一致したものを発見したことを示しています。各一致について、一致が発生したコンピュータ名を表示できます。一致を含む1つ以上のコンピュータ名を選択し、**[Live Connection (ライブ接続)]**をクリックすると、コンピュータへのライブ接続を作成し、一致が発生したファイルを調査します。

> **注意：**クイック検索クエリと検索可能なデータの両方が、一方向性ハッシュで暗号化されます。ハッシュは、クエリがエンドポイントに配信される前に発生し、暗号化されていないクエリおよび結果は保持されません。クエリは、検索ワークフロー中のみにブラウザで保持されます。結果のスニペットが要求された場合、エンドポイント上でファイルはオンデマンドに読み取られ、結果は直接Revealに戻されます。Revealは暗号化されてない

ファイルコンテンツをディスクには書き込まず、暗号化されてないクエリや結果はTaniumコンテンツとして送信することはありません。

Revealのトラブルシューティング

トラブルシューティングのために情報を収集してTaniumに送信するには、ログなどの関連情報を収集します。

ログを収集する

情報は、ブラウザでダウンロードできるZIPファイルとして保存されます。

1. Revealのホームページからヘルプ をクリックし、**[Troubleshooting (トラブルシューティング)]**タブをクリックします。
2. **[Create Package (パッケージの作成)]**をクリックします。ステータスがパッケージを完了したと表示していれば、**[Download Package (パッケージをダウンロード)]**をクリックします。
3. `reveal-troubleshooting.zip`ファイルをローカルダウンロードディレクトリへダウンロード。
4. Taniumサポートケースフォームにzipファイルを添付するか、担当のテクニカルアカウントマネージャに送信してください。

Tanium Revealは、次のディレクトリにある`Reveal.log`ファイルにログ情報を保存しています: `\Program Files\Tanium\Tanium Module Server\services\Reveal` ディレクトリ。

Revealのアンインストール

トラブルシューティングのため、Tanium Module ServerからRevealを削除することが必要になる場合があります。

1. Taniumコンソールから、**[Solutions (ソリューション)]**をクリックします。
   ソリューションページが開きます。
2. Revealを検索し、**[Uninstall (アンインストール)]**をクリックします。
   アンインストールウィンドウが開き、削除されるコンテンツ一覧が表示されます。
3. **[Proceed with Uninstall (アンインストールを続行)]**をクリックします。
4. アンインストールプロセスを開始するには、パスワードを入力してください。
   インストールパッケージが削除されると、進捗バーが表示されます。
5. **[Close (閉じる)]**をクリックします。
6. 確認するには、**[Solutions (ソリューション)]**ページにもどり、**[Import (インポート)]**ボタンが使用可能であることを確認します。

ヒント： Revealモジュールがコンソールで更 新 されていない場 合 は、ブラウザをリフレッシュしてください。