Tanium™ Reveal ユーザーガイド

バージョン 1.0. 0

2019年 6月 05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 をご覧ください。

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。

© 2019 Tanium Inc. All rights reserved.

目次

© 2019 Tanium Inc. All Rights Reserved

© 2019 Tanium Inc. All Rights Reserved

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 (医療保険の携行性と責任に関する法律)

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。

© 2019 Tanium Inc. All Rights Reserved

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。

この文書には、第三者が提供するコンテンツや製品(ハードウェアおよびソフトウェアを含む)、サービス(「第三者のアイテム」)に対するアクセス手段や、第三者のそうした情報そのものが含まれていることがあります。Tanium Inc.およびその関連会社は、(i)それらの第三者のアイテムに対して責任を負うものではなく、第三者のアイテムに関するすべての保証および責任を明示的に放棄し、(ii)お客様とTaniumとの間の有効な契約に明記されているのでない限り、かかる第三者のアイテムへのアクセスや、利用に起因する損失、費用または損害について責任を負いません。

また、この文書は、特定の第三者のアイテムの使用やTanium製品との組み合わせを求めるものでも、想定するものでもありません。そのような組み合わせによって生じた知的財産権の侵害について、Taniumおよびその関連会社は一切責任を負いません。第三者のアイテムとTanium製品の組み合わせが適切であるかどうか、また第三者の知的財産権を侵害しないかどうかの判定の責任はTaniumではなくお客様にあります。

はじめに

1. Tanium Revealをインストールします。詳細については、10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、13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、15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、17ページのルール一致の調査を参照してください。

© 2019 Tanium Inc. All Rights Reserved

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 2.7.7

Tanium Module Server

Revealがインストールされると、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。

© 2019 Tanium Inc. All Rights Reserved

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。

対象デバイス	プロセス
Module Server	`<Tanium Module Server>\services\ProductName\node.exe`

エンドポイントコンピュータ	`<Tanium Client>\Tools\EPI\TaniumExecWrapper.exe`
	`<Tanium Client>\Tools\EPI\TaniumEndpointIndex.exe`
	`<Tanium Client>\Tools\Reveal\win32\TaniumReveal.exe`

ユーザーロールの要件

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。

© 2019 Tanium Inc. All Rights Reserved

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

- リリースノート確認します。

> **注意：**Revealを使用するにはTanium Traceが必要です。Traceがインストールされていることを確認してください。詳細については、Traceのインストールを参照してください。

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 (インポートを続行する)]**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 Solutions (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。

© 2019 Tanium Inc. All Rights Reserved

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. **[Set Credentials (資格情報の設定)]**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. **[Reveal]**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。

Revealのバージョンをアップグレードする

[Solutions (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. [Main Menu (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。
   [Import Solution (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 (インポートを続行する)]**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。

© 2019 Tanium Inc. All Rights Reserved

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。

© 2019 Tanium Inc. All Rights Reserved

ルールの作成

概要

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

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。

- Tanium Indexによりインベントリに含まれます。
- サイズは32MB未満。このデフォルトのサイズ制限を引き上げるには、Revealのconfig.jsonとTanium Indexのconfig.iniの両方をアップデートします。config.iniのアップデートの詳細については、ファイルシステムのインデックス作成を参照してください。このデフォルトのサイズ制限を引き下げるには、config.jsonのみアップデートが必要です。
- ファイル形式は次のいずれかです。.doc、.ppt、.log、.rtf、.txt、.csv、.ppt、.xml、.xls、.html、.dev
- 圧縮可能にします。

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[Name (名称)]と[Description (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 (ルールを追加する)]**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 (条件を追加する)]**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。

© 2019 Tanium Inc. All Rights Reserved

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。**[Deploy Rules (ルールのデプロイ)]**をクリックすると、アップデートしたルールを直ちにデプロイします。

© 2019 Tanium Inc. All Rights Reserved

ルールセットの作成

概要

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。

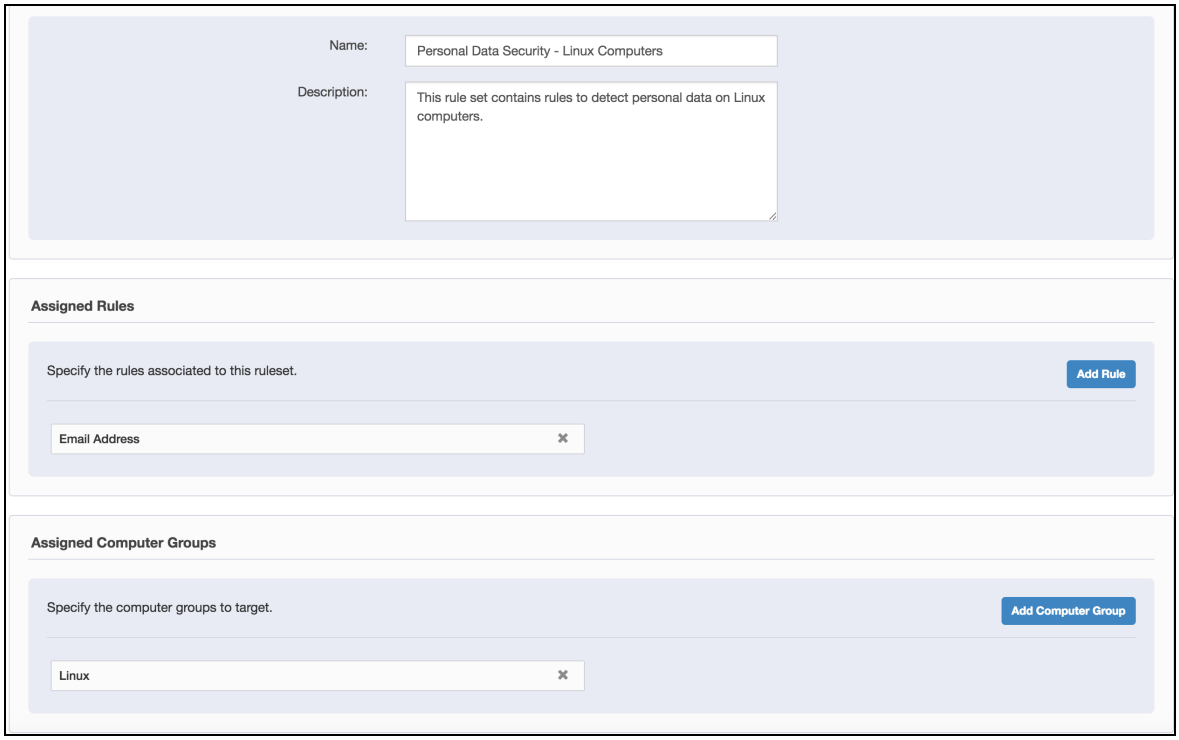
デフォルトで、各ルールセットには割り当てられたルールが1つあります。デフォルトのルールは編集できませんが、削除や、そのルールを複製して特定のニーズに合わせたカスタマイズができます。

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 sert (新しいルールセット)]**をクリックします。

© 2019 Tanium Inc. All Rights Reserved

2. ルールセットの[Name (名称)]と[Description (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 (ルールを追加する)]**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 (ルールを追加する)]**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。

© 2019 Tanium Inc. All Rights Reserved

ルールー致の調査

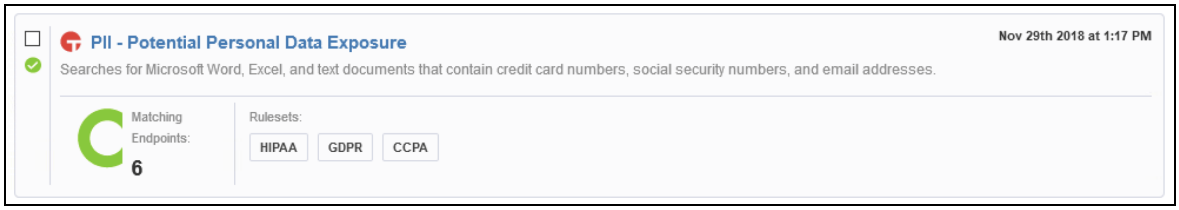
概要

Revealがルールとのー致を見つけると、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ー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。ー致の詳細についてさらに調査できます。各ルールには、ー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ー定期間のー致数を調査でき、またコンピュータグループまたはキーワードでー致をフィルタすることができます。

[Rule (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ー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

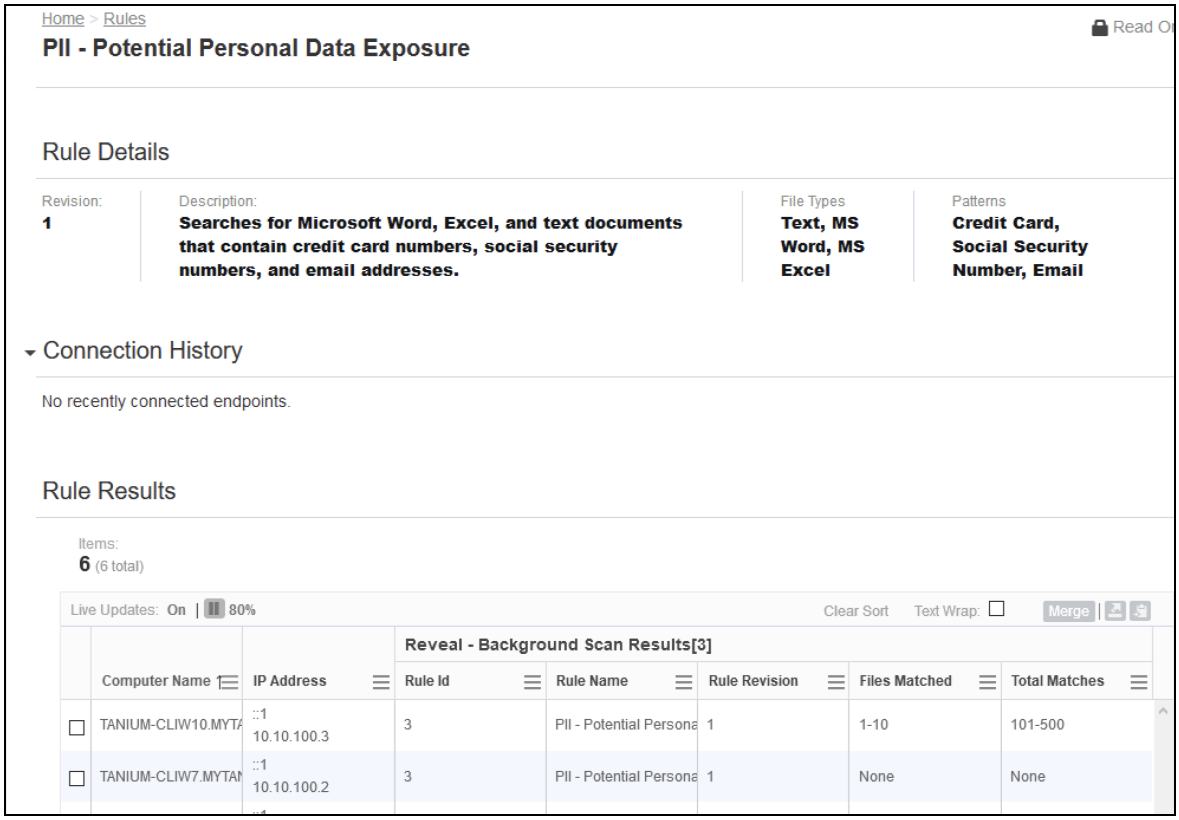
1. Revealメニューから、**[Rules (ルール)]**をクリックします。
2. 調査するー致を含むルールをクリックします。



3. Revealにー致のあるエンドポイントが表示されます。
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ー致を含むファイルを表示します。
5. エンドポイントをクリックしてルールのー致を含むファイルを表示します。ー致のあるファイ

© 2019 Tanium Inc. All Rights Reserved

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。



© 2019 Tanium Inc. All Rights Reserved