Tenable Identity Exposure の主な機能ガイド

最終更新日: 2025 年 11 月 4 日

目次

Tenable Identity Exposure の主な機能ガイドへようこそ

Tenable Identity Exposure (旧称 Tenable AD) へようこそ。このドキュメントは、オンプレミスでデプロイされているか、SAAS を通じてデプロイされているかにかかわらず、製品の特徴と機能の包括的な概要を提供することで、ユーザーエクスペリエンスを向上させることを目的としています。このリソースは、ガイダンスを求めている新規ユーザーであるか、理解をさらに深めたい経験豊富なユーザーであるかにかかわらず、すべてのユーザーを支援することを目的としています。

このドキュメントには、製品使用の最適化、攻撃インジケーターと露出インジケーターの管理など、さまざまなトピックを扱うさまざまなセクションがあります。このドキュメントは貴重なインサイトを提供していますが、Tenable Identity Exposure の使用に関する厳格なルールブックとなるものではありません。代わりに、プラットフォームのシームレスで効果的な使用を実現するための推奨事項を提供しています。

このガイドについて

このガイドは、**Tenable Identity Exposure SaaS ユーザーガイド**に基づいています。包括的な詳細情報を得たい場合は、こちらのガイドを参照してください。

Tenable Identity Exposure の機能をハイライトするためにこのガイドに示されている例は、すべてを網羅したリストではなく、それぞれの固有の環境に直接対応するとは限りません。最適なセキュリティ対策を講じるために、Tenable 公式ドキュメントを参照するか専門サービスを利用して、さらに詳細やガイダンスを得ることをお勧めします。

主要なステークホルダー

Tenable Identity Exposure の個々のステークホルダーは、お客様の組織の規模、構造、セキュリティポリシー、対象となるユースケースによって異なります。各ステークホルダーに役割と責任を細かく設定することで、製品を効率的に導入して使用できるようになります。

Tenable Identity Exposure を操作する際、関係するさまざまなステークホルダーを把握しておくことは重要です。これらの個人およびグループは、アイデンティティ関連のセキュリティリスクを特定、軽減、報告する上で、さまざまな役割を担っています。全体的な内訳は次のとおりです。

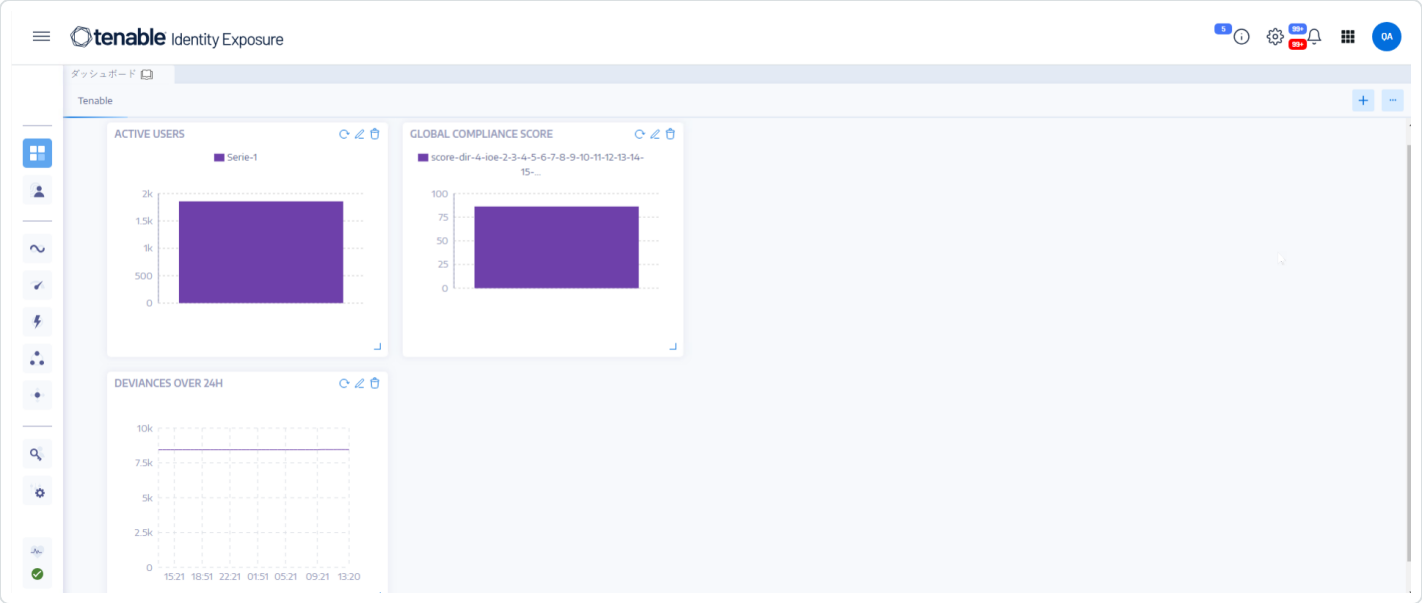
- **セキュリティチーム**: Tenable ソリューションを監督し管理します。データ分析を活用して脆弱性とリスクを速やかに特定して対応します。

- **IT 運用チーム**: 他のセキュリティツールやユーザーディレクトリとのシームレスな接続を確保しながら、Tenable ソリューションのインフラと統合のサポートを円滑化します。
- **アプリケーション開発チーム**: アプリケーションのセキュリティを確保し、Tenable によってフラグが立てられたリスクのあるアイデンティティに速やかに対処します。
- **アイデンティティアクセス管理** (IAM) チーム: ユーザーアカウント、アクセス許可、アクセス制御を管理します。IT セキュリティ担当者と緊密に連携して、Tenable Identity Exposure によって特定された問題に対処します。
- **ビジネスユニットリーダー**: チームやアプリケーションのセキュリティ態勢に関する最終的な責任を負います。レポートを確認し、リスク緩和戦略に優先順位を付け、リソースを割り当てて Active Directory のセキュリティ対策を強化します。

ダッシュボード

ダッシュボードでは、Active Directory のセキュリティに影響を与えるデータや傾向がビジュアル化されて表示されます。ウィジェットでカスタマイズし、要件に応じてグラフやカウンターを表示できます。

Tenable Identity Exposure ダッシュボードは、お客様の組織の Active Directory (AD) をセキュリティ保護するためのリアルタイムのコマンドセンターとして機能します。アイデンティ環境の包括的な概要 (リアルタイムの一元化されたビューなど) が表示されます。また、重大な脆弱性もハイライトされるので、潜在的な攻撃手法をピンポイントで特定し、プロアクティブにリスク緩和策を実行できます。



主なダッシュボード機能

- **一目で把握できる概要**: コンプライアンススコア、主なリスク、ユーザーアクティビティの傾向など、重要指標が目立つように表示されることで、セキュリティの状態を素早くチェックできます。
- **詳細情報へのドリルダウン**: 深刻度、ユーザーカテゴリ、その他の関連基準でソートしたリスク要因の内訳を示すインタラクティブなウィジェットにより、特定の領域をさらに掘り下げることができます。
- **カスタマイズ可能な視点**: 事前構築されたテンプレートを使用したり、独自のレイアウトを作成したりして、優先度に合わせてパーソナライズされたダッシュボードを作成できます。たとえば、再発する次の IoE でよく見つかる設定ミスを表示するためのダッシュボードを作成することができます。

    - SDProp の一貫性を確保する
    - ドメインコントローラーが不正なユーザーに管理されている
    - 危険な Kerberos 委任
- **リアルタイムモニタリング**: 継続的なアップデートとアラートにより、新たな脅威や不審なアクティビティに関する最新情報を入手できます。
- **実用的なインサイト**: 深刻度と潜在的な影響に基づいて優先順位が付けられた、修正に関する実用的な推奨事項が示されます。

関連項目

- ダッシュボード
- ダッシュボードに関する動画チュートリアル

イベントフロー

Tenable Identity Exposure のイベントフローは、AD インフラに影響を与えるイベントをリアルタイムで監視し分析した結果を表示します。イベントフローを使用して、重大な脆弱性と推奨される修正方法を特定できます。

[イベントフロー] ページを使用して、時間を遡って以前のイベントをロードしたり、特定のイベントを検索したりできます。ページの上部にある検索ボックスを使用して、脅威を検索したり悪意のあるパターンを検出したりすることもできます。

イベントフローは次のイベントを追跡します。

- **ユーザーやグループの変更**: アカウントやグループの作成、削除、変更が含まれます。
- **アクセス許可の変更**: ファイル、フォルダー、プリンターなどのオブジェクトに対するアクセス制御の変更が含まれます。
- **システム設定の調整**: グループポリシーオブジェクト (GPO) やその他の重要な設定への変更が含まれます。
- **疑わしいアクティビティ**: 不正な試行、権限昇格、および危険信号を示すその他のイベントが含まれます。

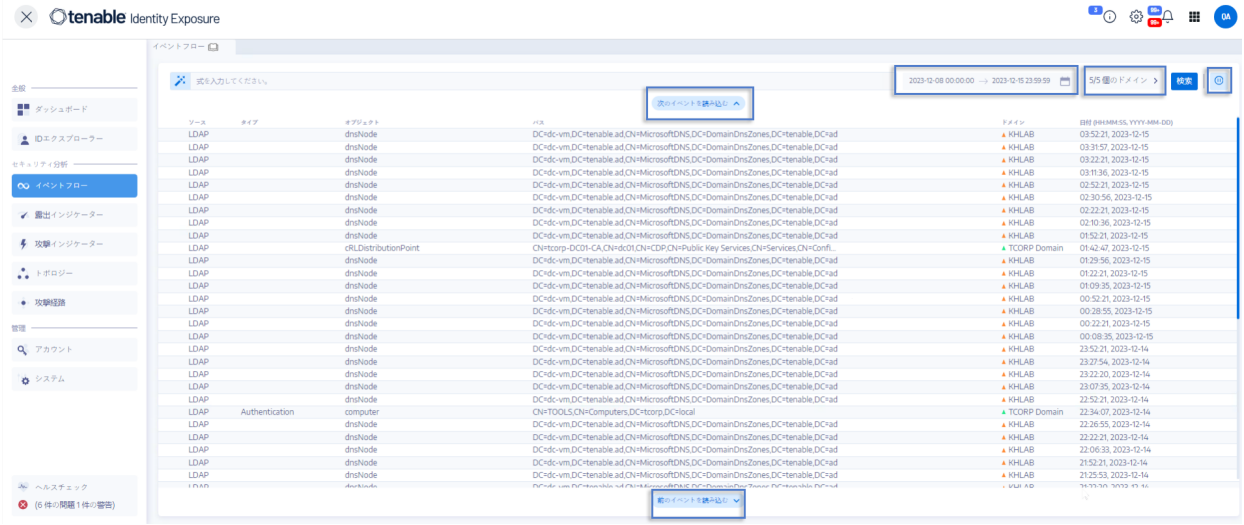
Tenable Identity Exposure は、次のような機能を提供して、イベントフローのデータを活用できるようにしています。

- **検索とフィルタリングが可能**: キーワードや特定の条件を使用してイベントストリームを簡単にナビゲーションできるため、無関係な情報を最小限に抑え、関連するアクティビティにフォーカスできます。
- **詳細なイベント情報**: 各イベントエントリには、影響を受けているオブジェクト、変更を担当したユーザー、使用されているプロトコル、関連する露出インジケーター (IoE) などの詳細情報が記載されています。
- **関係の視覚化**: イベント間の関係を図示する機能により、一見無関係に見えるアクティビティが、より広範な攻撃キャンペーンにどのようにつながる可能性があるかを明らかにします。

イベントフローにアクセスするには

- Tenable Identity Exposure で、左側のナビゲーションバーの **[イベントフロー]** をクリックします。

  [イベントフロー] ページが開き、イベントのリストが表示されます。詳細は、Trail Flow Tableを参照してください。



データはイベントフローにどのように表示されますか?

1. Active Directory (AD) インターフェース内で次のアクションを実行すると...
   - 新しいユーザーアカウントを作成する
   - ユーザーのグループメンバーシップを変更する
   - パスワードをリセットする
   - アカウントを無効化する
   - アカウントを有効化する
   - アカウントを削除する
   - オブジェクトを移動する
   - アクセス許可を変更する
2. Active Directory (AD) は、イベントログエントリを自動的に生成します。その際、次を含む、操作の詳細情報をキャプチャします。
   - タイムスタンプ

- アクションを実行する管理者
- 影響を受けたオブジェクト
- 具体的な変更内容

3. Tenable Identity Exposure はこれらのイベントログを引き続き収集して分析し、イベントを相関付け、パターンを特定し、異常を検出します。
4. [イベントフロー] ページで、操作のフローと影響が視覚化されて表示されます。
    - タイムライン: イベントを時系列で表示し、直近の操作をハイライトします。
    - オブジェクトの詳細: 属性や関係など、影響を受けたオブジェクトに関する具体的な情報を提供します。
    - 変更履歴: 現在の操作を含む、オブジェクトに加えられた変更の履歴を表示します。
    - リスクインサイト: 過剰なアクセス許可や機密性の高いグループのメンバーシップなど、操作に伴う潜在的なリスクを特定します。
    - コンプライアンス情報: 操作に関連するコンプライアンス違反を示します (ある場合)。

関連項目

- イベントフローの概要
- Trail Flow Use Cases
- イベントフローの動画チュートリアル

レポートセンター

Tenable Identity Exposure の**レポートセンター**には、重要なデータを組織内の主要ステークホルダー向けのレポートとしてエクスポートできる便利な機能があります。レポートセンターでは、事前定義されたリストからレポートを作成することができ、プロセスが効率的で簡潔になります。

次のような機能があります。

- **詳細なフィルタリング**: 日付範囲、ドメイン、攻撃インジケーター (IoA)、露出インジケーター (IoE) などに基づく詳細なフィルターを使用してレポートを絞り込めるので、的を絞ったインサイトが得られます。
- **自動配信**: レポートの自動生成をスケジュールし、希望の間隔で配信することで、セキュリティの監視とレポートのプロセスを効率化します。
- **柔軟なエクスポート**: レポートを CSV などのさまざまな形式でエクスポートして、詳細な分析を行ったり、レポートアクセスキーを使用して共有したり、既存のレポートワークフローと統合したりできます。

管理者は、最長 1 四半期の柔軟なレポート期間で、異なるユーザー向けにさまざまなタイプのレポートを作成できます。Tenable Identity Exposure から重要なアイデンティティデータを共有できるため、企業は積極的にリスクを軽減し、アイデンティティベースの攻撃の可能性を特定できるようになります。

ユーザーがレポートをダウンロードするには、管理者から受け取ったメールに記載された URL のリンク先ページにレポートのアクセスキーを入力します。レポートは 30 日間ダウンロードでき、その後期限切れとなり、Tenable Identity Exposure により削除されます。Tenable Identity Exposure が指定された期間分の新しいレポートを生成し、過去のレポートを上書きする前に、ユーザーはレポートをダウンロードする必要があります。

レポートセンターにアクセスするには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** を選択します。
2. **[レポート]** の **[レポートセンター]** をクリックします。

   ペインが開き、設定済みレポートのリストとそれに関連する情報 (レポート名、タイプ、ドメイン、プロファイル、期間、頻度、受信者のメールアドレスなど) が表示されます。

関連項目

- レポート センター
- Set Permissions for a Role

露出インジケーター

Tenable Identity Exposure は、AD インフラのセキュリティ成熟度を露出インジケーターを通じて測定し、監視および分析対象のイベントのフローに対して深刻度レベルを割り当てます。Tenable Identity Exposure は、セキュリティの悪化を検出するとアラートをトリガーします。

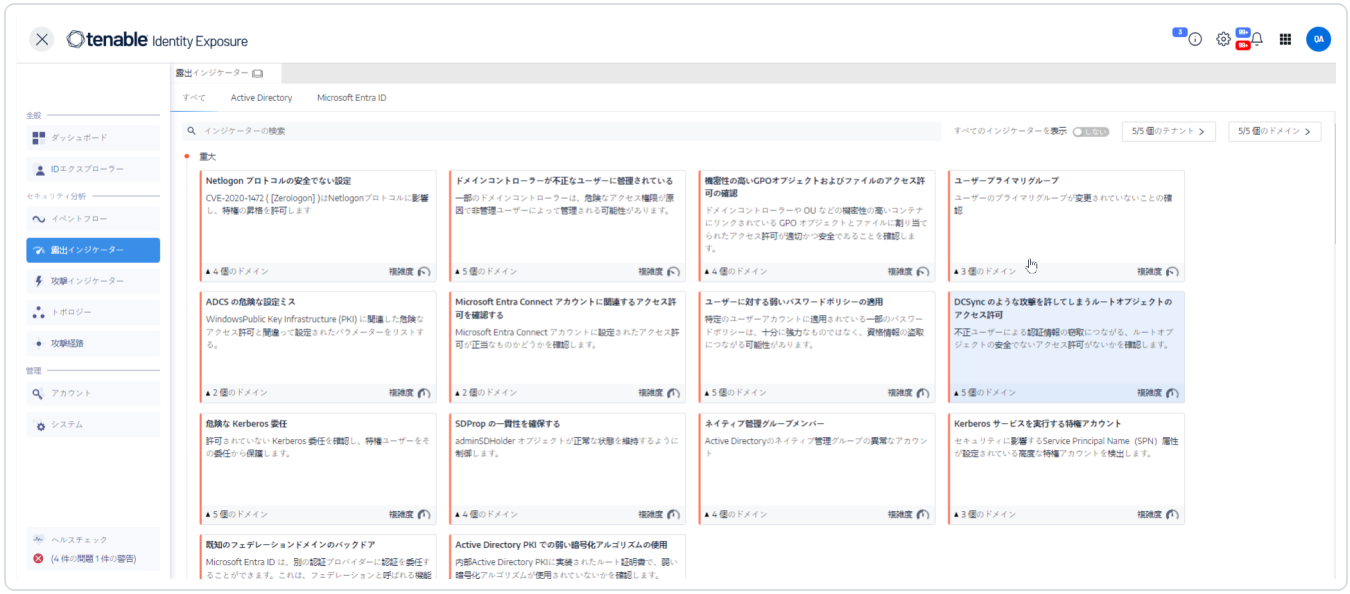
これらの IoE は事前設定されており、定められた基準から逸脱すると、対応するアラートがトリガーされます。

IoE を表示する方法

1. Tenable Identity Exposure で、ナビゲーションペインの **[露出インジケーター]** をクリックします。

   [露出インジケーター] ペインが開きます。デフォルトでは、Tenable Identity Exposure は逸脱を含む IoE だけを表示します。

2. (オプション) すべての IoE を表示するには、**[すべてのインジケーターを表示]** トグルをクリックして **[はい]** に切り替えます。



Tenable Identity Exposure の IoE には、ユーザーの調査能力を上げるために設けられたさまざまな機能が付いています。

- **検索とフィルタリングが可能**: フォレストとドメインに基づいてフィルターを適用することで、IoE を簡単に探索できます。
- **エクスポート機能**: 逸脱オブジェクトにより、IoE を CSV 形式でエクスポートできます。

- **IoE インシデントに対するアクション**: ホワイトリストからサイバーエクスポージャーを削除するか、再有効化します。

IoE のデータには、次のものが含まれます。

- **情報セクション**: このセクションでは、既知の攻撃ツール、影響を受けたドメイン、関連ドキュメントなど、各露出インジケーター (IoE) に関するエグゼクティブサマリーが表示されます。
- **脆弱性の詳細**: このセクションでは、Active Directory の設定ミスに関する詳細な情報が表示されます。
- **逸脱したオブジェクト**: このセクションは、アタックサーフェスをさらに広げる可能性のある Active Directory の設定ミスをハイライトします。
- **推奨事項**: このセクションでは、アタックサーフェスを最小限に抑えるための効果的な設定戦略について説明します。

深刻度レベル

深刻度レベルにより、検出された脆弱性の深刻度を評価し、修正アクションに優先順位を付けることが可能になります。

[露出インジケーター] ペインに IoE が次のように表示されます。

- カラーコードを使用した深刻度レベル。
- 垂直方向 – 深刻度の高い順 (赤が最も優先順位が高く、青が最も低い)。
- 水平方向 – 複雑度の高い順。Tenable Identity Exposure は複雑度の指標を動的に計算して、逸脱した IoE の修正の難易度を示します。

深刻度	説明
重大 – 赤	特定の非特権ユーザーによる Active Directory の攻撃や侵害を防止する方法を示します。
高 – オレンジ	認証情報の盗取やセキュリティ機能のバイパスにつながる侵入後のテクニック、または危険な状態へと連鎖的につながる可能性のある手口を示します。
中 – 黄	Active Directory インフラに対する限定的なリスクを示します。
低 – 青	優れたセキュリティ対策を示します。特定のビジネス環境では、必ずしも AD のセ

	キュリティに影響を与えるとは限らない影響度の低い逸脱が許容される場合もあります。これらの逸脱は、管理者が非アクティブなアカウントをアクティブ化するなどのミスをした場合にのみ、AD に影響を与えます。

修正の優先順位付け

システムによって特定された深刻度の高い IoE に対する修正作業を優先的に行います。さらに、IoE 内のリスクメーターを使用して、重大なカテゴリ内でさらに優先順位を付けることができます。

所属組織の権限範囲内または運用上の許可範囲内の IoE であるなら、許可リストに追加できます。

ユースケース

次のユースケースでは、[パスワードが決して期限切れにならないアカウント] という IoE に注目します。

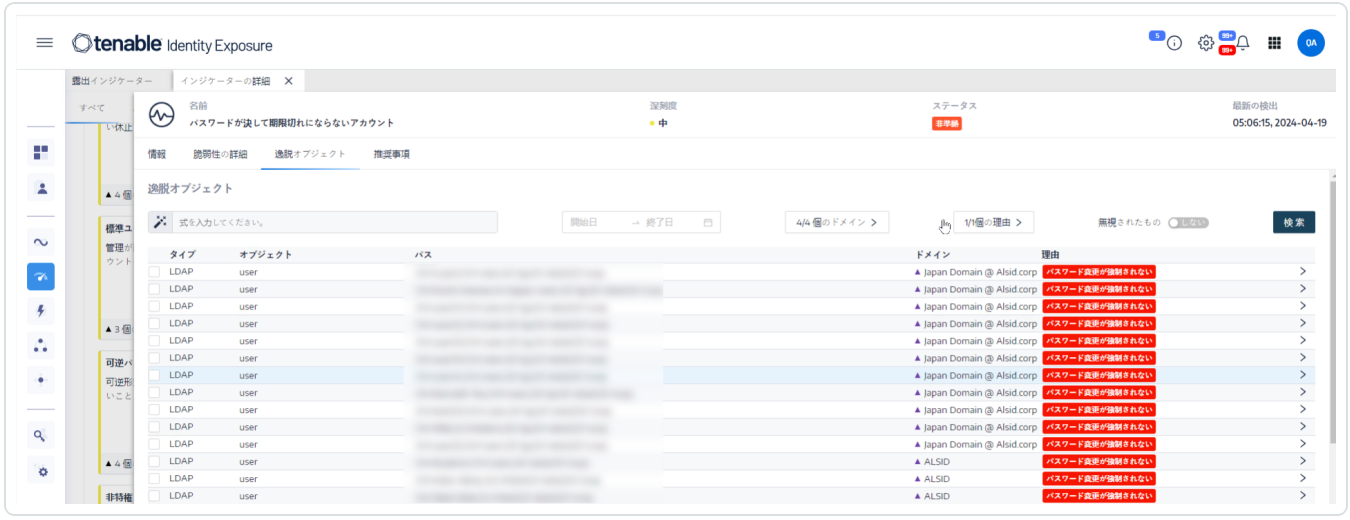
1. Tenable Identity Exposure が IoE にフラグを立てると、その IoE は [露出インジケーター] ペインに表示されます。

2. この IoE に関するさらなるインサイトを表示するには、その IoE をクリックして追加の詳細にアクセスします。情報ページ内には、簡潔な概要、その IoE に関連付けられている潜在的な攻撃ツールの詳細、影響を受けたドメイン、および問題を理解し効果的に対処するのに役立つ関連ドキュメントの詳細を含むエグゼクティブサマリーが表示されます。

3. 

4. IoE の詳細を表示するには、[脆弱性の詳細] タブをクリックします。

5. [パスワードが決して期限切れにならないアカウント] 設定が有効になっているアカウントを確認するには、[逸脱したオブジェクト] をクリックします。このアクションにより、システム内でこの設定を持つアカウントのリストを参照できます。



6. 逸脱したオブジェクトをクリックすると、IoE がフラグを立てたアカウントが表示されます。

7. Active Directory 管理者に連絡して、影響を受けているアカウントで [パスワードが決して期限切れにならないアカウント] オプションが有効になっている理由を確認してください。

8. その回答に基づいて、アカウントをホワイトリストに登録するか、Active Directory 管理者が問題に対処するための推奨事項を作成できるように支援します。

9. 推奨事項については、IoE の推奨事項セクションを参照できます。

10. アカウントに例外がある、または想定内の動作であると確認された場合は、このIoEを無視することができます。その場合、**[逸脱オブジェクト]**に移動して、該当する逸脱を選択し、選択されたオブジェクトを**無視**するか、要件に応じて選択されたオブジェクトの無視を停止します。

関連項目

- Indicators of Exposure
- 露出インジケーターの動画チュートリアル
- Customize an Indicator

攻撃インジケーター

Tenable Identity Exposure の攻撃インジケーター (IoA) は、組織が最も高度な攻撃手法によって Active Directory (AD) インフラが侵害されそうになった際に、迅速に検知して対応できるよう支援します。対象には以下が含まれます。

- **上位 3 件のインシデント**: IoA の統合された表示では、AD に影響を与えた上位 3 件のインシデントがリアルタイムのタイムラインで示され、攻撃の分布もすべて 1 つのインターフェース内で表示されます。
- **IoA の詳細**: Tenable Identity Exposure 内の IoA パネルには、AD 内で発生した攻撃に関する情報が表示されます。
- **IoA に関連するインシデント**: IoA インシデントのリストは、AD を標的とする特定の攻撃に関する包括的な詳細情報を表示します。この情報により、IoA の深刻度レベルに応じて適切に対応できます。

攻撃インジケーターには、調査能力を高めるために設計されたさまざまな機能が備わっています。

- **検索とフィルタリングが可能**: タイムラインを利用して IoA を簡単に探索できます。また、フォレスト、ドメイン、重大度レベルに基づいてフィルターを適用することで効率的に絞り込まれた結果を取得できます。
- **エクスポート機能**: IoA データを PDF、CSV、PPTX 形式でエクスポートすることができます。
- **グラフタイプの変更:** グラフタイプを変更できるオプションがあります。これにより、攻撃深刻度の分布または上位 3 つの攻撃を、それぞれの発生回数とともに表示できます。
- **IoA インシデントに対するアクション**: インシデントを選択して、クローズしたり再オープンしたりできます。

深刻度レベル

Tenable Identity Exposure は、攻撃を検出し、以下の深刻度レベルを割り当てます。

レベル	説明
重大 – 赤	前提条件としてドメインの支配が必要な、実証済みの悪用後の攻撃を検出しました。

高 – オレンジ	攻撃者がドメインの支配を可能にする重大な攻撃を検出しました。
中 – 黄	IoA は、危険な権限昇格や、機密性の高いリソースへのアクセスの許可につながる可能性のある攻撃と関連しています。
低 – 青	偵察活動や影響度の低いインシデントに関連する疑わしい動作について警告しています。

修正の優先順位付け

お客様固有のセキュリティリスクや懸念事項に応じて、重大かつ影響の大きい IoA を特定します。

誤検出のリスクや実際の攻撃の見落としリスクを軽減するには、お客様の環境に合わせて IoA を調整することが重要です。これには、以下を行うことが含まれます。

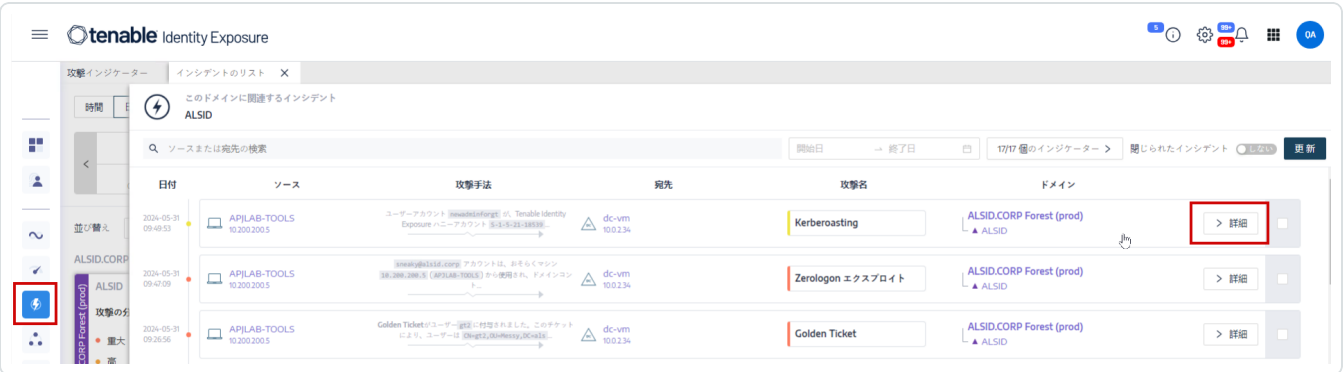
- しきい値を調整する: IoA の感度を調整して誤検出を減らし、アラートが意味のある実用的なものになるようにします。
- アカウントとアクティビティをホワイトリストに登録する: 正当なアクティビティが IoA をトリガーしないように除外することで、アラートの精度と調査の効率を高めます。
- IoA を相関付ける: さまざまな IoA 間の関係を分析して、より広範な攻撃パターンを特定します。

ヒント: オプションと推奨値の詳細については、Tenable Identity Exposure 攻撃インジケーターリファレンスガイド (https://jp.tenable.com/downloads/identity-exposure から入手可能) を参照してください。これらのオプションと値をセキュリティプロファイル内の各 IoA に適用します。

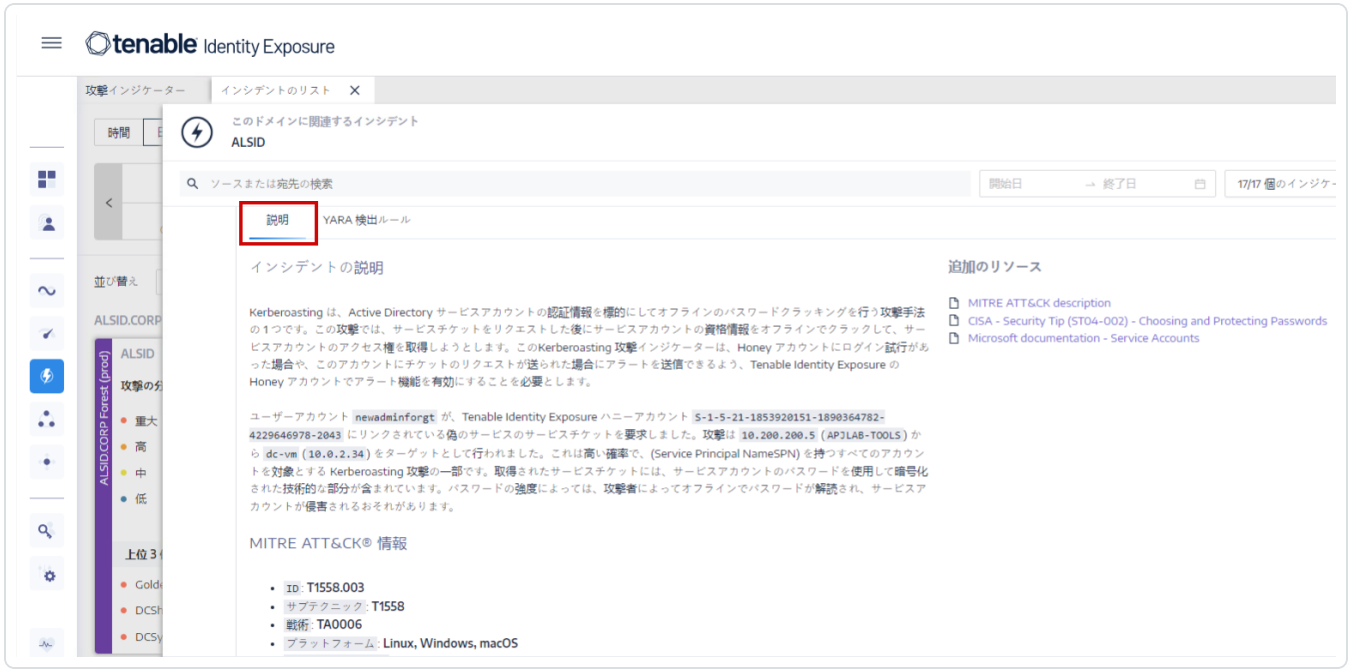
ユースケース

1. IoA がアクティブになったら、ナビゲーションペインの [攻撃インジケーター] を選択するか、ホームページの右上にあるベルアイコンをクリックします。

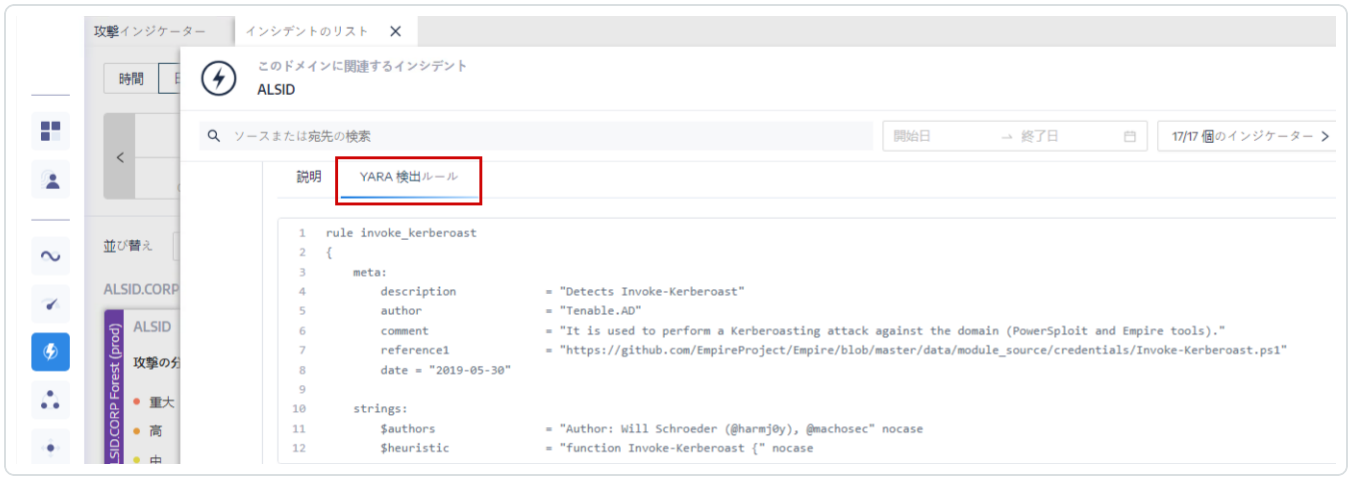
2. 各インジケーターにはインシデントに関する詳細情報が表示され、確認後に適切なアクションを取ることができます。
    - 攻撃が発生した日時
    - 攻撃の説明
    - 攻撃起点
    - 攻撃のターゲット
    - MITRE ATT&CK® 情報
    - YARA 検出ルール
    - ほかのリソース
3. この例では、ローカル管理者の列挙に焦点を当てていますが、説明にアクセスするには、[詳細] を選択します。



4. [説明] タブには、Active Directory (AD) に対する特定の攻撃に関する情報が表示されます。



5. [YARA 検出ルール] タブには、Tenable Identity Exposure がネットワークレベルの Active Directory 攻撃を検出するために使用する YARA ルールに関する情報が表示されます。これにより、Tenable Identity Exposure の全体的な検出機能が強化されます。



6. Active Directory 管理者または関連するステークホルダーと協力して、インシデントを調査して解決し、インシデントのクローズや再オープンを判断するとともに、再発防止策を実施します。

7. 認知または承認された攻撃である場合、それに応じて IoA をカスタマイズして、それ以降のインスタンスでこの IoA がフラグを立てないようにすることもできます。

関連項目

- Indicators of Attack
- Customize an Indicator
- 攻撃インジケーターの動画チュートリアル

Microsoft Entra ID をアイデンティティプロバイダーとして設定する

Tenable Identity Exposure は Active Directory のほかに Microsoft Entra ID (旧 Azure AD または AAD) もサポートし、組織内で使用できるアイデンティの範囲を広げています。この機能では、Microsoft Entra IDに固有のリスクにフォーカスした、新しい露出インジケーター (IoE) が使用されます。

Microsoft Entra ID を Tenable Identity Exposure と統合するには、次のオンボーディングプロセスに厳密に従ってください。

1. 前提条件を満たす
2. アクセス許可をチェックする
3. ネットワークフローをチェックする
4. Microsoft Entra ID の設定
5. Microsoft Entra ID のサポートのアクティブ化
6. テナントスキャンの有効化

前提条件

「cloud.tenable.com」にログインし、Microsoft Entra ID のサポート機能を使用するには、Tenable クラウドアカウントが必要です。この Tenable クラウドアカウントは、ようこそメールに使用されたメールアドレスと同じものです。「cloud.tenable.com」のメールアドレスがわからない場合は、サポートまでご連絡ください。有効なライセンス (オンプレミスまたは SaaS) をお持ちのお客様は、「cloud.tenable.com」で Tenable クラウドにアクセスできます。このアカウントを使用して、Microsoft Entra ID にかける Tenable スキャンを設定したり、スキャン結果を収集したりできます。

注意: Tenable クラウドにアクセスするのに有効な **Tenable Vulnerability Management** ライセンスは必要ありません。現在有効なスタンドアロン Tenable Identity Exposure ライセンス (オンプレミスまたは SaaS) があれば十分です。

注意: Tenable Identity Exposure は、中国および米国政府の専用エリアが含まれている**各国のクラウドでは Microsoft Entra ID をサポートしていません**。Microsoft Entra ID が提供している各国のクラウドは、特定の規制およびコンプライアンスのニーズに合わせて設計されており、物理的に独立した Azure インスタンスです。Tenable Identity Exposure がサポートしているのは、グローバル Microsoft Entra ID 環境だけであり、中国のナショナルクラウドと米国政府のナショナルクラウドは含まれていません。Microsoft Entra ID の各国のクラウドの詳細については、Microsoft ID プラットフォームの Microsoft Entra の認証と各国のクラウド を参照してください。

アクセス許可

Microsoft Entra ID をサポートするには、ユーザー、グループ、アプリケーション、サービスプリンシパル、ロール、アクセス許可、ポリシー、ログなどのデータを Microsoft Entra ID から収集する必要があります。このデータは、Microsoft の推奨に従い、Microsoft Graph API とサービスプリンシパル認証情報を使用して収集されます。

- Microsoft Graph で**テナント全体の管理者の同意を付与するアクセス許可を持つユーザー**として Microsoft Entra ID にサインインする必要があります。つまり、Microsoft が定めた条件によると、グローバル管理者または特権ロール管理者のロール (または適切なアクセス許可を持つカスタムロール) がなければなりません。
- Microsoft Entra ID の設定とデータ視覚化にアクセスするには、**Tenable Identity Exposureユーザーロール**に適切なアクセス許可がなければなりません。詳細は、Set Permissions for a Roleを参照してください。

ネットワークフロー

Entra ID サポートをアクティブ化するために、次のアドレスで、ポート 443 でのセキュリティエンジンノードサーバーからの送信を許可します。

- sensor.cloud.tenable.com
- cloud.tenable.com

ライセンス数

Tenable は、**Tenable クラウドの同期機能が有効になっている場合にのみ**、重複しているアイデンティティをライセンス数としてカウントしません。この機能がない場合、Microsoft Entra ID と Active Directory のアカウントを照合できず、各アカウントを個別にカウントします。

- **Tenable クラウドの同期なしの場合**: AD アカウントと Entra ID アカウントの両方を持つ 1 人のユーザーは、2 人の別々のユーザーとしてライセンス数にカウントされます。
- **Tenable クラウドで同期が有効な場合**: システムは複数のアカウントを 1 つのアイデンティティに統合するため、複数のアカウントを持つ 1 人のユーザーは 1 回だけカウントされます。

Microsoft Entra ID の設定

次の手順 (Microsoft のクイックスタート: Microsoft ID プラットフォームにアプリケーションを登録するのドキュメントから引用) を使用して、Microsoft Entra IDで必要なすべての設定を行います。

1. **アプリケーションを作成する**

   a. Azure 管理者ポータルで、**[アプリの登録]** ページを開きます。

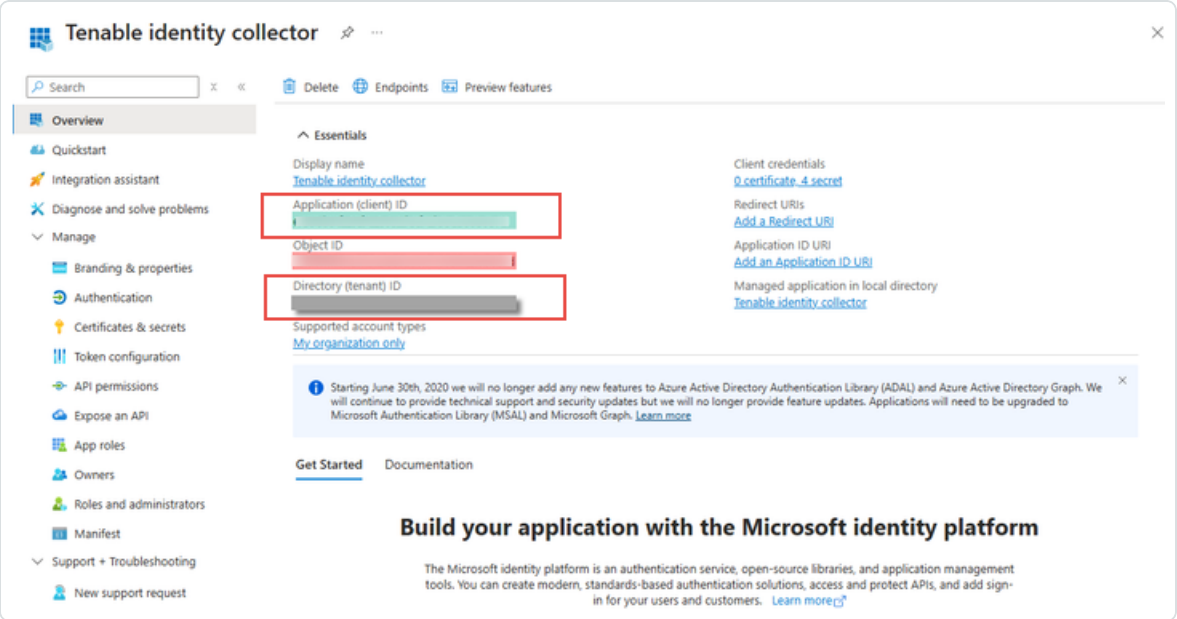
   b. **[+ 新規登録]** をクリックします。

   c. アプリケーションに名前を付けます (例: Tenable Identity Collector)。その他のオプションについては、デフォルト値のままにしておくことができます。

   d. **[登録]** をクリックします。

   e. この新たに作成されたアプリの [概要] ページにある、「アプリケーション (クライアント) ID」と「ディレクトリ (テナント) ID」を書き留めます。これらは、後の手順 新しい Microsoft Entra ID テナントを追加する方法 で必要になります。

   > **警告**: 設定を機能させるには、**[オブジェクト ID] ではなく [アプリケーション ID]** を選択してください。



2. **認証情報をアプリケーションに追加する**

   a. Azure 管理者ポータルで、**[アプリの登録]** ページを開きます。

   b. 作成したアプリケーションをクリックします。

c. 左側のメニューにある **[証明書とシークレット]** をクリックします。

d. **[+ New client secre]** (+ 新しいクライアントシークレット) をクリックします。

e. **[説明]** ボックスに、このシークレットに実際に使用する名前と、ポリシーに準拠した**有効期限**の値を入力します。有効期限が近づいたら忘れずにこのシークレットを更新します。

f. シークレットは Azure に 1 度しか表示されないため、シークレットの値を安全な場所に保存してください。紛失した場合は再作成する必要があります。

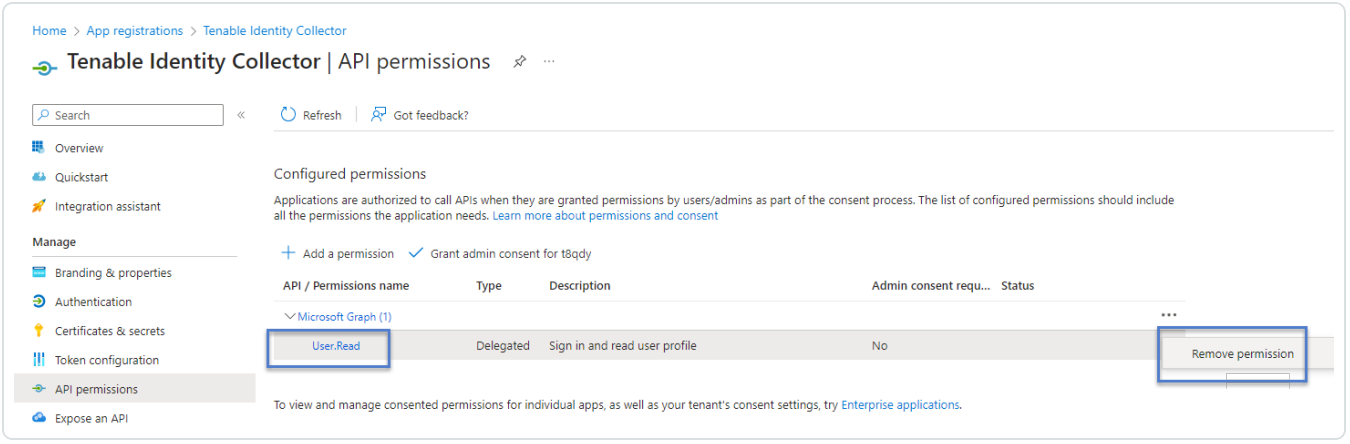
3. **アプリケーションにアクセス許可を割り当てる**

a. Azure 管理者ポータルで、**[アプリの登録]** ページを開きます。

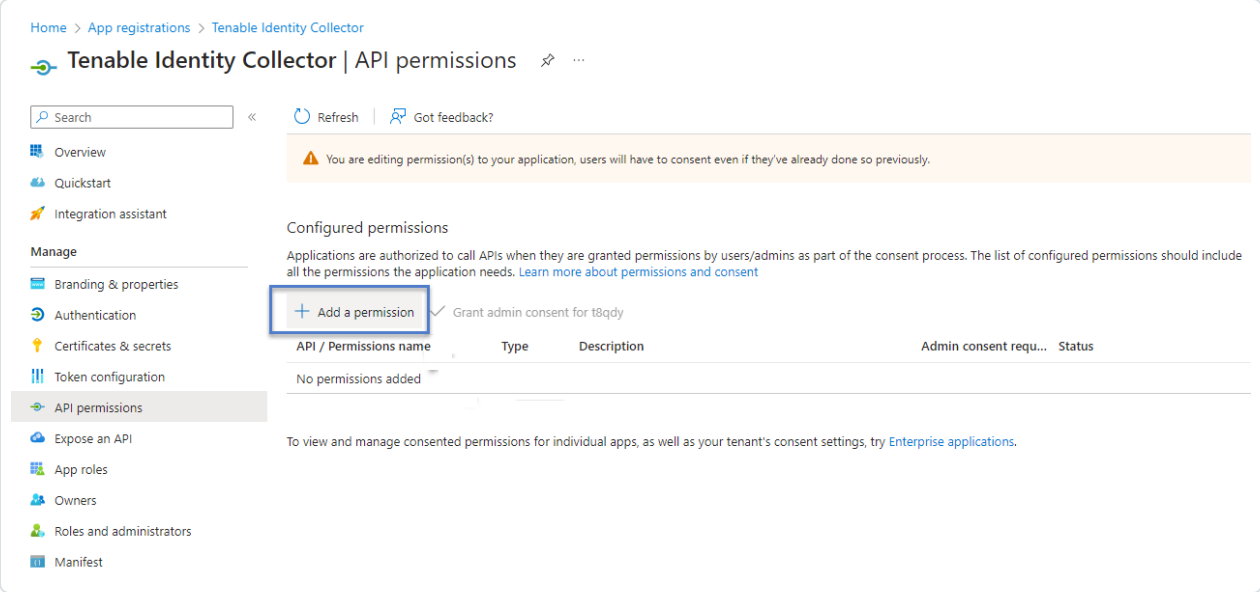
b. 作成したアプリケーションをクリックします。

c. 左側のメニューにある **[API のアクセス許可]** をクリックします。

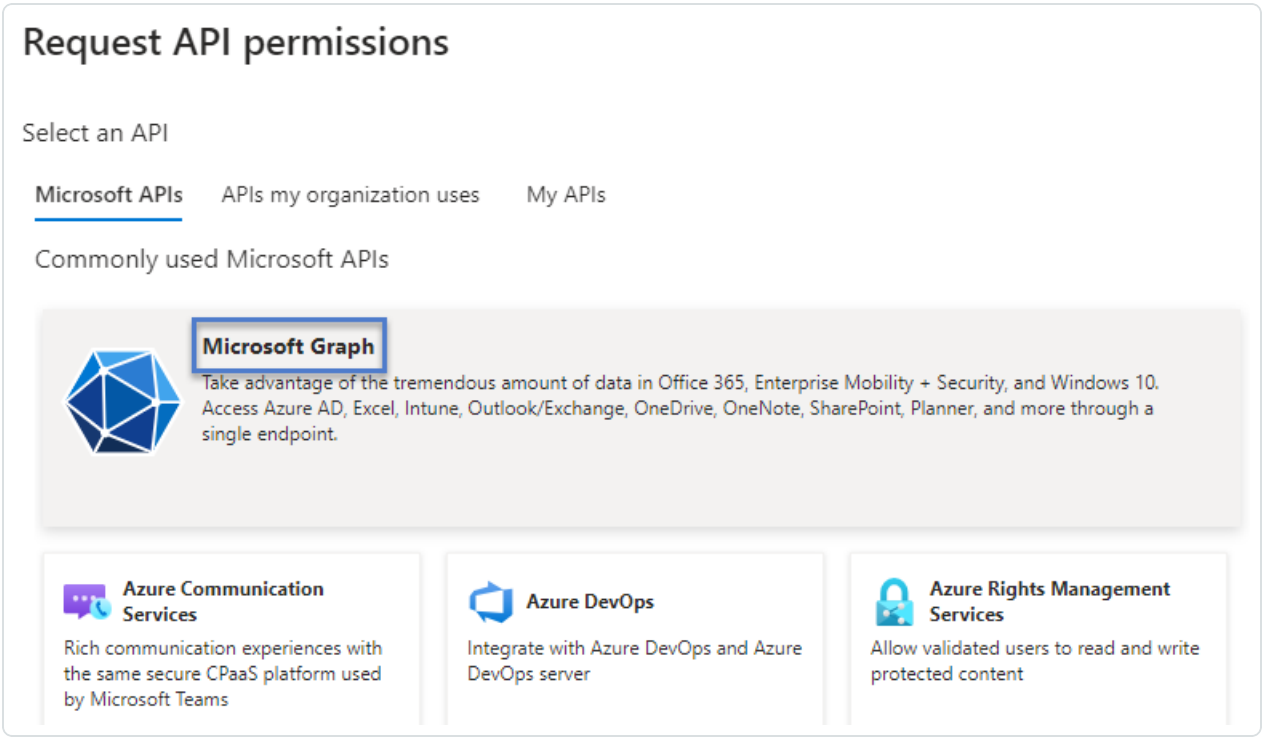
d. 既存の `User.Read` アクセス許可を削除します。



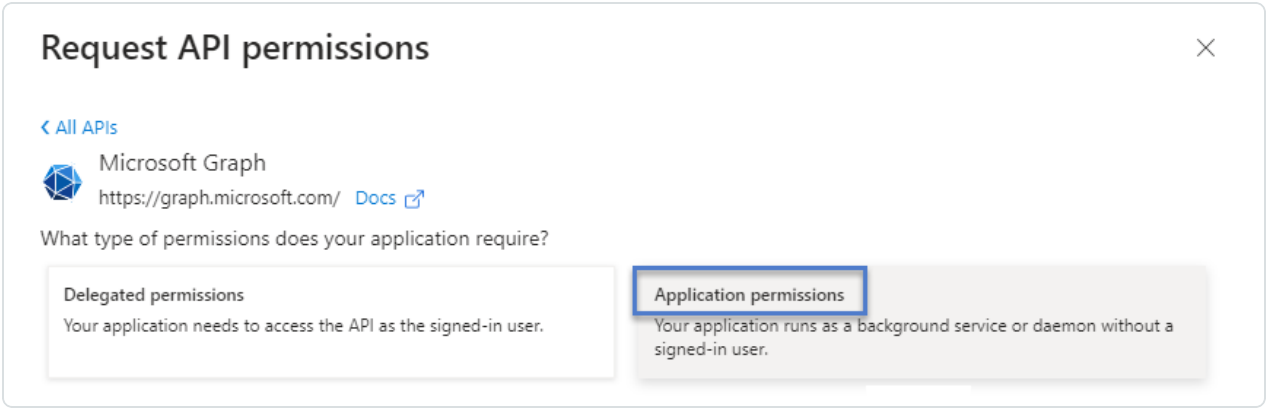
e. **[+ アクセス許可の追加]** をクリックします。



f. **[Microsoft Graph]** を選択します。



g. **[アプリケーションのアクセス許可]** を選択します ([委任されたアクセス許可] ではありません)。

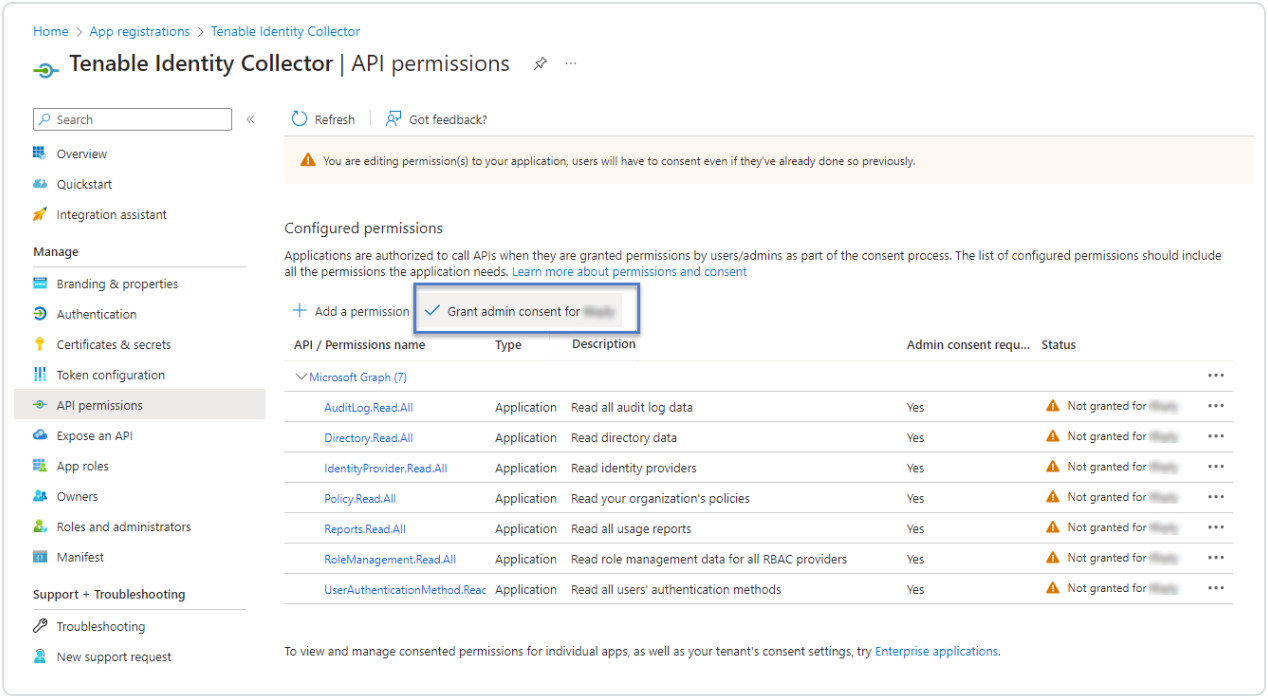


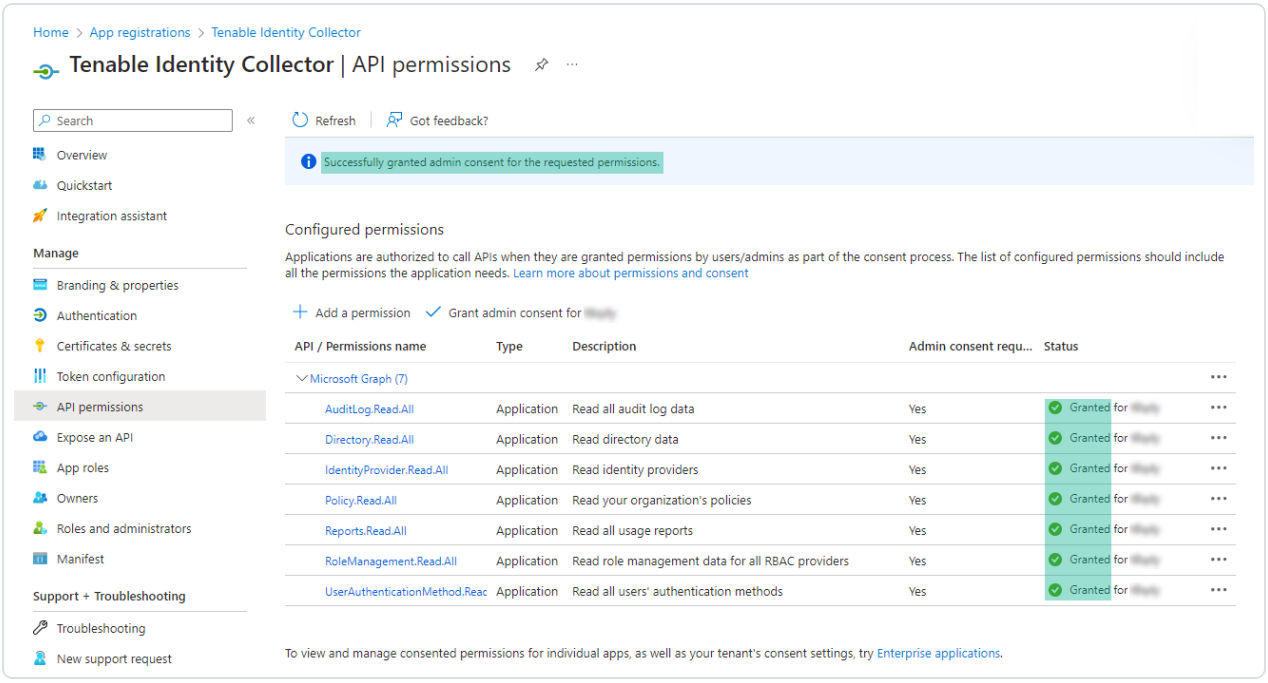
h. リストか検索バーを使用して、次のすべてのアクセス許可を見つけて選択します。

- AuditLog.Read.All
- Directory.Read.All
- IdentityProvider.Read.All
- Policy.Read.All
- Reports.Read.All
- RoleManagement.Read.All
- UserAuthenticationMethod.Read.All

i. **[アクセス許可の追加]** をクリックします。

j. **[<テナント名> に管理者の同意を付与する]** をクリックし、**[はい]** をクリックして確定します。





4. Microsoft Entra ID で必要なすべての設定をしたら、以下を実行します。

   a. Tenable Vulnerability Management で「Microsoft Azure」タイプの新しい認証情報を作成します。

b. 「キー」認証方法を選択し、前の手順で取得した値 (テナント ID、アプリケーション ID、クライアントシークレット) を入力します。

Microsoft Entra ID のサポートのアクティブ化

- **Microsoft Entra ID** を使用するには、Tenable Identity Exposure 設定でその機能をアクティブ化する必要があります。
- 手順については、Identity 360, Exposure Center, and Microsoft Entra ID Support Activation を参照してください。

テナントスキャンの有効化

新しい Microsoft Entra ID テナントを追加する方法

テナントを追加すると、Tenable Identity ExposureとMicrosoft Entra ID テナントがリンクして、そのテナントに対してスキャンを実行できるようになります。

1. [設定] ページで、**[アイデンティティプロバイダー]** タブをクリックします。

   [テナント管理] ページが開きます。

2. **[テナントの追加]** をクリックします。

   [テナントの追加] ページが開きます。

3. **[テナントの名前]** ボックスに名前を入力します。
4. **[認証情報]** ボックスのドロップダウンリストをクリックして、認証情報を選択します。
5. 使用する認証情報がリストに表示されない場合は、次のいずれかを行うことができます。
    - Tenable Vulnerability Management (Tenable Vulnerability Management > **[設定]** > **[認証情報]**) で作成します。詳細については、Tenable Vulnerability Managementの Azure タイプの認証情報を作成する手順を参照してください。
    - Tenable Vulnerability Management で、認証情報に「使用可能」または「編集可能」アクセス許可があることを確認してください。これらのアクセス許可がない限り、Tenable Identity Exposure のドロップダウンリストに認証情報が表示されません。
6. **[更新]** をクリックして、認証情報のドロップダウンリストを更新します。
7. 作成した認証情報を選択します。
8. **[追加]** をクリックします。

Tenable Identity Exposure がテナントを追加したことを確認するメッセージが表示され、テナント管理ページのリストに表示されるようになります。

テナントのスキャンを有効にするには

注意: テナントスキャンはリアルタイムでは行われず、テナントの規模にもよりますが、ID エクスプローラーに Microsoft Entra ID のデータが表示されるまで少なくとも 45 分必要です。

- リストでテナントを選択し、トグルをクリックして **[スキャン有効]** に切り替えます。

Tenable Identity Exposure はテナントに対するスキャンをリクエストし、その結果が露出インジケーターページに表示されます。

注意: 2 つのスキャン間の必須の最小遅延時間は **30 分**で、1 日あたり少なくとも 1 回発生します。テナントの規模に応じて、ほとんどのお客様のデータは 1 日に複数回更新されます。

攻撃経路

Tenable Identity Exposure には、グラフィック表示を通してビジネス資産の潜在的な脆弱性を視覚化する方法が複数用意されています。

- **攻撃経路**: 攻撃者がエントリポイントから資産を侵害する可能性のある経路を示します。
- **影響範囲**: 任意の資産から Active Directory に入る可能性のあるラテラルムーブメントを示します。
- **露出資産**: 資産をコントロールする可能性のあるすべての経路を示します。

攻撃経路を理解することで、攻撃者による脆弱性の悪用を阻止するために必要な軽減手順を特定できます。これには、システムへのパッチ適用、設定の堅牢化、より強力なアクセス制御の実装、ユーザーの意識向上が含まれます。

Tenable Identity Exposure の攻撃経路を使用する利点

- **プロアクティブなセキュリティ**: 潜在的な攻撃手法を予測し、悪用される前に対応するのに役立ちます。
- **優先順位付け**: 最も重大な脆弱性と攻撃経路にセキュリティの取り組みを集中させることができます。
- **視覚化**: AD 内の複雑なセキュリティ関係を明確かつ分かりやすく表示します。
- **伝達**: 潜在的な攻撃シナリオの証拠を視覚的に示すことで、セキュリティリスクのステークホルダーへの伝達を円滑化します。

攻撃経路を表示するには

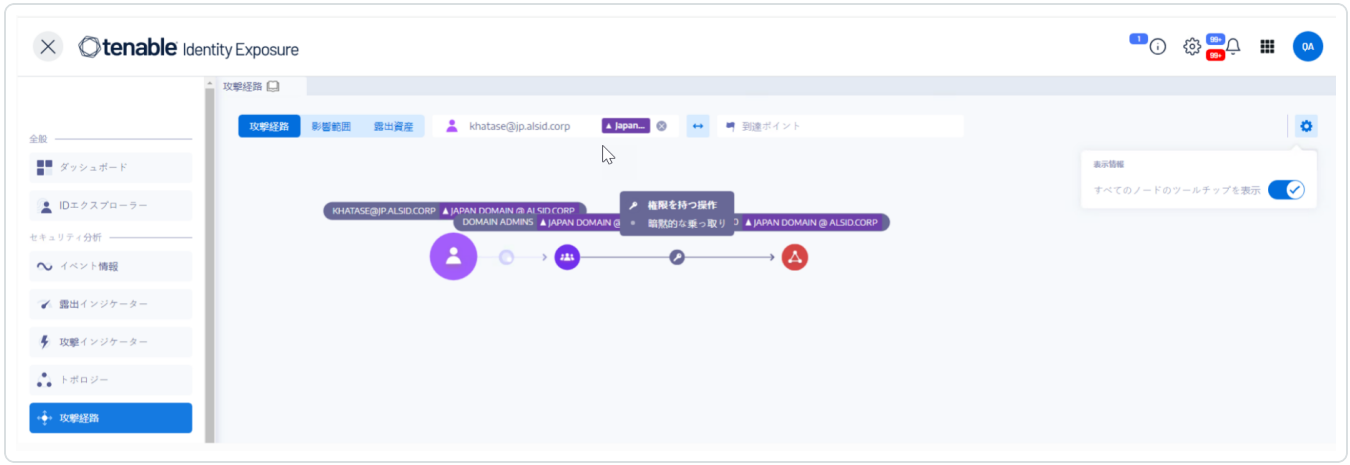
AD 内の任意の資産 (ユーザーアカウント、コンピューター、グループなど) を開始点として指定します。攻撃者が最終的に侵害しようとしている資産 (ドメインコントローラー、機密データサーバーなど) を表す、到達点を定義します。

1. Tenable Identity Exposure で、サイドバーメニューの **[攻撃経路]** をクリックします。

   [攻撃経路] ペインが表示されます。

2. バナーの **[攻撃経路]** をクリックします。
3. **[開始ポイント]** ボックスに、エントリポイントとなる資産を入力します。
4. **[到着ポイント]** ボックスに、経路の最終ポイントとなる資産を入力します。
5. 🔍 アイコンをクリックします。

   Tenable Identity Exposure が 2 つの資産間の攻撃経路を表示します。



6. オプションで、⚙ アイコンをクリックして以下を実行できます。

- **[ズーム]** スライダーをクリックして、グラフの縮尺を調整します。
- **[すべてのノードツールチップを表示]** トグルをクリックして、資産に関する情報を表示します。

影響範囲を表示するには

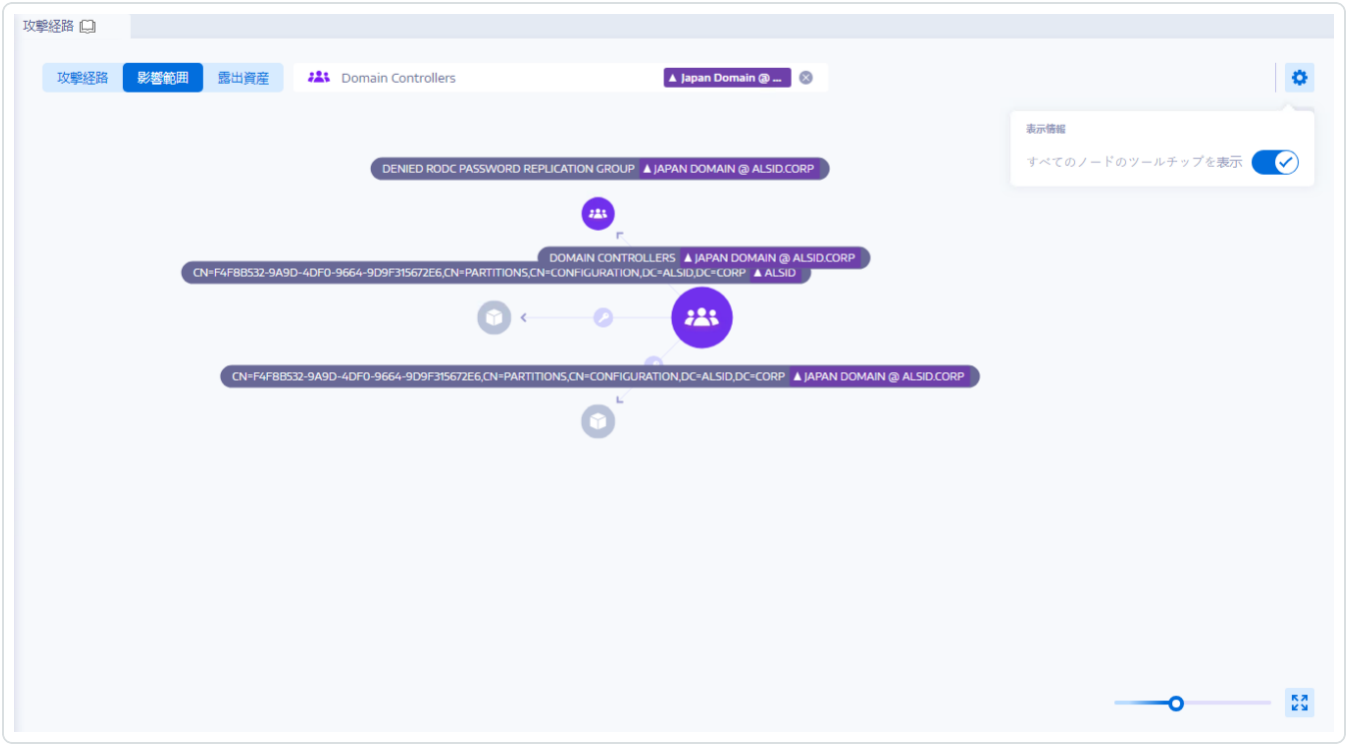
Tenable Identity Exposure は、潜在的な攻撃経路をグラフィカルに表示し、資産間のつながりをハイライトします。各つながりは潜在的な脆弱性または設定ミスを表し、攻撃者が悪用して AD 内を水平展開する可能性があります。経路の詳細をよりよく理解するために、拡大したり縮小したりできます。

1. Tenable Identity Exposure で、サイドバーメニューの **[攻撃経路]** をクリックします。

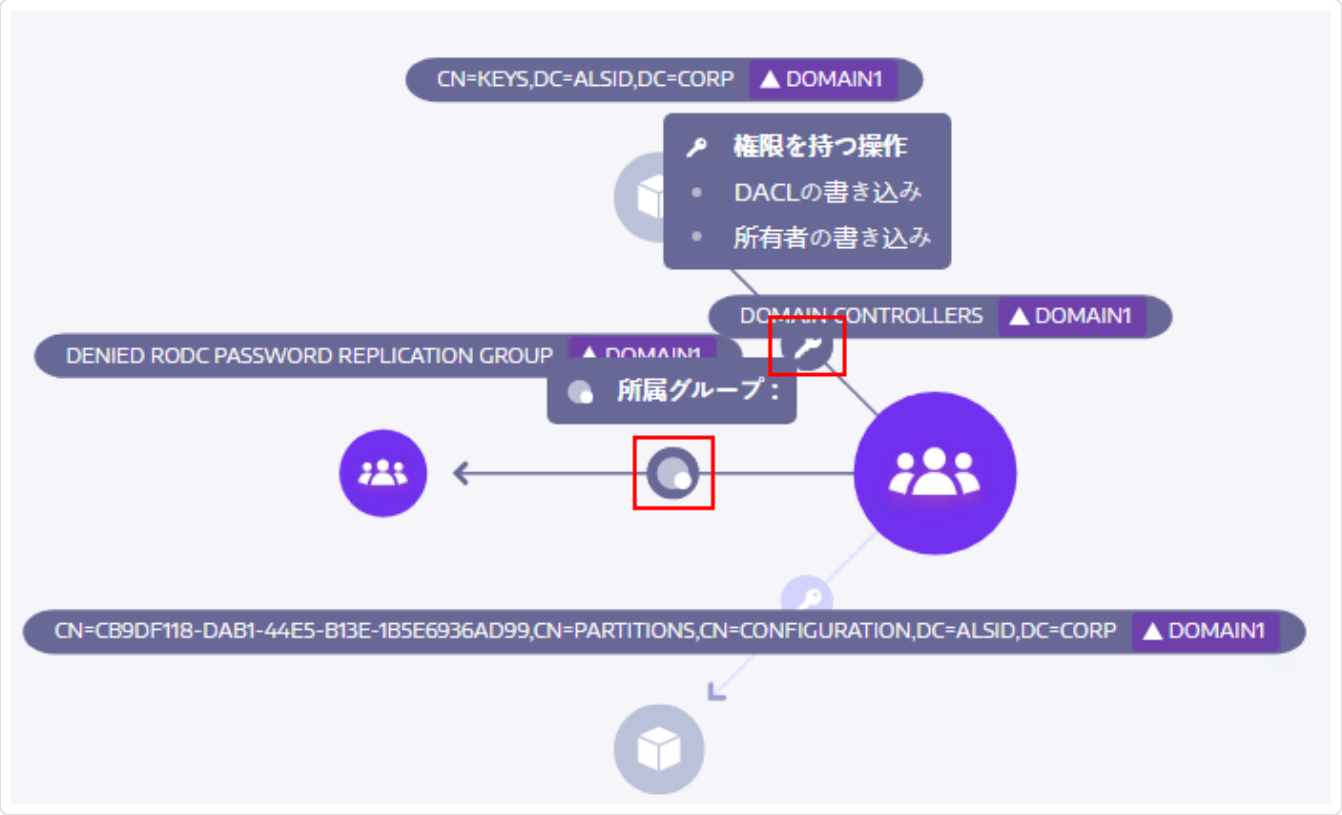
   [攻撃経路] ペインが表示されます。

2. バナーの **[影響範囲]** をクリックします。
3. **[オブジェクトを検索]** ボックスに、資産の名前を入力します。
4.  アイコンをクリックします。

   Tenable Identity Exposure はその資産から放射状に広がる横方向の接続を表示します。



5. 資産と資産をつなぐ矢印アイコンをクリックして、資産相互の関係を表示します。



露出資産を表示するには

攻撃経路の各ステップは、脆弱性の深刻度を示すリスクスコアに関連付けられています。これにより、どの経路が最も重大な脅威になるのか、早急な対応が必要なのか、優先順位を付けることができます。個々の接続ポイントをクリックすると、関連する特定の脆弱性や設定ミスに関するより詳しい情報を確認することもできます。

1. Tenable Identity Exposure で、サイドバーメニューの **[攻撃経路]** をクリックします。

   [攻撃経路] ペインが表示されます。

2. バナーの **[露出資産]** をクリックします。

3. **[オブジェクトを検索]** ボックスに、資産の名前を入力します。

4. アイコンをクリックします。

   Tenable Identity Exposure が資産につながる経路と資産同士の関係を表示します。

5. 資産と資産をつなぐ矢印アイコンをクリックして、資産相互の関係を表示します。

攻撃経路の表示を固定するには、次のようにします。

関連項目

- Attack Relations
- Identifying Tier 0 Assets
- Accounts with Attack Paths
- Attack Path Node Types

ユーザー管理

重要な要素

- **ロール**: デフォルトのロールには、管理者、セキュリティアナリスト、ユーザー、ゲストがあり、それぞれアクセス許可が異なります。カスタムロールを使用すると、特定のニーズに合わせてきめ細かく制御できます。
- **アクセス許可**: アクセス許可は、ユーザーが Tenable Identity Exposure 内でアクセスし実行できるものを定義します。これには、レポートやダッシュボードの表示から、ユーザーの管理、インジケーターの設定、アカウントの無効化などの操作が含まれます。
- **範囲限定**: Tenable Identity Exposure では、アクセス許可の範囲を、Active Directory 内の特定のドメイン、グループ、さらには個別のオブジェクトに限定することができます。これにより、ユーザーは自分のロールと責任に応じて、関連性のあるデータのみにアクセスすることができます。

利点

- **Active Directory セキュリティの強化**: きめ細かなアクセス制御により、機密アイデンティティデータへの不正アクセスのリスクを最小限に抑えます。
- **効率化とワークフローの改善**: ユーザーは必要なツールとデータにアクセスできるため、調査とインシデント対応が効率化されます。
- **コンプライアンスの遵守**: ロールベースのアクセス制御により、Active Directory 内のアイデンティティアクセス管理のコンプライアンス要件を満たすことができます。

関連項目

- User Roles

Tenable Identity Exposure の統合

Tenable Identity Exposure をご使用の SIEM、SOC、SOAR ソリューションと統合することで、リアルタイムモニタリング、自動応答、アラート管理の強化が可能になります。

Syslog 統合によるリアルタイムモニタリング

シームレスな Syslog 統合により、重大な露出インジケーター (IoE) に関するアラートを即時で受け取れます。

主な利点

- **一元化されたログ記録**: Tenable Identity Exposure のイベントを他のセキュリティソリューションと一緒に集約して、包括的な分析を行います。
- **リアルタイムの通知**: 潜在的なアイデンティエクスポージャーや攻撃に関する通知を即時で受け取ります。
- **セキュリティ管理の強化**: さまざまなソースからのイベントを関連付けて、複雑な脅威をより迅速に特定します。
- **SIEM 可視性の強化**: Tenable Identity Exposure のデータを SIEM にシームレスに統合し、状況認識と相関分析を強化します。
- **効率化されたワークフロー**: Syslog データに基づいてアラートのトリアージと応答を自動化し、セキュリティ運用を最適化します。

リアルタイムモニタリングを実現する IoE の例

- **ADCS の危険な設定ミス**「認定中古車」攻撃の可能性を示している AD 証明書サーバーの変更を検出および特定します。
- **GPO 実行の健全性**: グループポリシー内のスクリプト実行を通してバックドアを仕掛けようとする試みを検出および特定します。
- **ユーザーにコンピューターをドメインに参加させることが許可されている**:「RBCD」バックドア攻撃の前兆として特徴的な、許可されていないドメインコンピューターの追加を検知します。

SOAR プラットフォームによる応答の自動化

既存の SOAR (Security Orchestration, Automation, and Response) プラットフォームを活用して、TIE データに基づいて自動化された修正アクションを実行します。主な利点は次のとおりです。

- **迅速な軽減**: 重大な IoE への対応を自動化することで、ダウンタイムと影響を最小限に抑えます。
- **効率の改善**: セキュリティチームが反復タスクから解放され、戦略的なセキュリティ施策に集中できるようになります。
- **セキュリティ対策の強化**: 検出された設定ミスにプロアクティブに対処し、全体的なセキュリティ状況を強化します。

重要: 自動化スクリプトのトラブルシューティングやサポートは、Tenable サポートの範囲外です。サポートが必要な場合は、Tenable の専門サービスチームにお問い合わせください。