Guide des fonctionnalités clés de Tenable Identity Exposure

Dernière révision : 2 juillet 2025

Copyright © 2025 Tenable, Inc. Tous droits réservés. Tenable, Tenable Nessus, Tenable Lumin, Assure et le logo Tenable sont des marques déposées de Tenable, Inc. ou de ses filiales. Tous les autres produits ou services sont des marques commerciales de leurs propriétaires respectifs.

Table des matières

Bienvenue dans le Guide des fonctionnalités clés de Tenable Identity Exposure 3

Dashboards 5

Trail Flow 7

Centre de rapports 11

Indicateurs d'exposition 13

Indicateurs d'attaque 19

Prise en charge de Microsoft Entra ID 24

Chemin d'attaque 34

Gestion des utilisateurs 39

Intégration de Tenable Identity Exposure 40

Bienvenue dans le Guide des fonctionnalités clés de Tenable Identity Exposure

Bienvenue dans Tenable Identity Exposure (anciennement Tenable AD). Ce document est conçu pour améliorer votre expérience en offrant un aperçu complet des caractéristiques et des fonctionnalités du produit, que ce dernier soit déployé sur site ou via SaaS. Cette ressource a pour but de vous aider, que vous soyez un novice à la recherche de conseils ou un utilisateur expérimenté cherchant à approfondir ses connaissances.

Tout au long de ce document, vous trouverez différentes sections explorant un large éventail de sujets, notamment l'optimisation de l'utilisation du produit et la gestion des indicateurs d'attaque et des indicateurs d'exposition. Sachez toutefois que les informations précieuses fournies par ce guide sur l'utilisation de Tenable Identity Exposure ne doivent pas nécessairement être suivies à la lettre. Il propose plutôt des recommandations en vue d'une utilisation simple et efficace de la plateforme.

À propos de ce guide

Ce guide est basé sur le **Guide de l'utilisateur Tenable Identity Exposure Saas** que vous pouvez consulter pour obtenir des informations complètes.

Les exemples présentés dans ce guide pour mettre en évidence les fonctionnalités de Tenable Identity Exposure ne constituent pas une liste exhaustive et ne s'appliquent pas forcément aux spécificités de chaque environnement. Pour des mesures de sécurité optimales, nous vous recommandons de consulter notre documentation officielle ou nos services professionnels afin d'obtenir plus de détails et des conseils.

Principales parties prenantes

Les parties prenantes de Tenable Identity Exposure diffèrent en fonction de la taille, de la structure, des stratégies de sécurité et des cas d'utilisation prévus de votre organisation. En établissant des rôles et des responsabilités précis pour chaque partie prenante, vous favoriserez une adoption et une utilisation efficaces du produit.

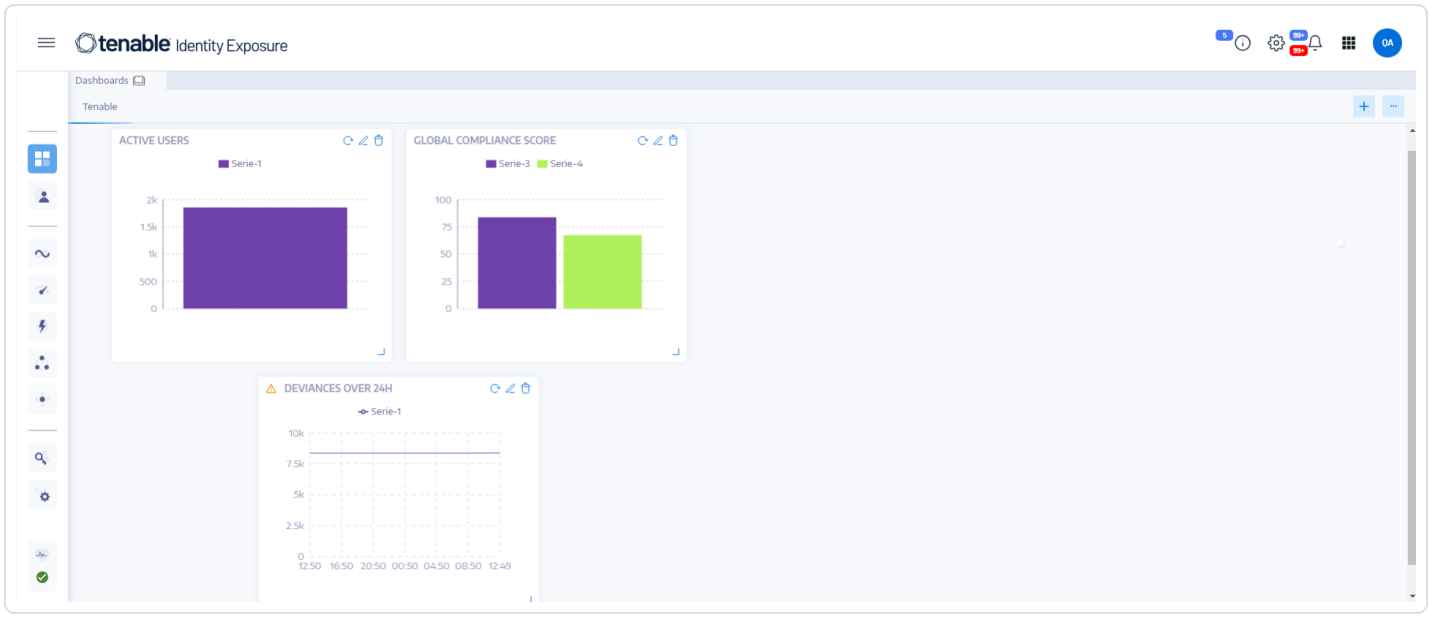
Lors de l'utilisation de Tenable Identity Exposure, il est essentiel d'identifier les diverses parties prenantes impliquées. Ces personnes et ces groupes jouent des rôles variés dans l'identification, l'atténuation et le signalement des risques de sécurité basés sur l'identité. En voici la liste :

- **Équipe de sécurité** : surveille et administre la solution Tenable, en tirant parti de l'analyse de données pour identifier rapidement les vulnérabilités et les risques, et y répondre.
- **Équipe des opérations informatiques** : soutient l'infrastructure et l'intégration de la solution Tenable, en assurant une connectivité transparente avec d'autres outils de sécurité et annuaires d'utilisateurs.
- **Équipes de développement d'applications** : chargées de sécuriser les applications et de traiter rapidement toutes les identités exposées, signalées par Tenable.
- **Équipe de gestion des identités et des accès** (IAM) : gère les comptes utilisateur, les autorisations et les contrôles d'accès, en travaillant en étroite collaboration avec ses homologues de la sécurité informatique pour résoudre les problèmes identifiés par Tenable Identity Exposure.
- **Responsables d'unités opérationnelles** : assument la responsabilité finale de la sécurité de leurs équipes et applications. Ils examinent les rapports, priorisent les stratégies d'atténuation des risques et attribuent des ressources pour améliorer les mesures de sécurité Active Directory.

Dashboards

Les dashboards vous permettent de visualiser des données et des tendances sur la sécurité de votre infrastructure Active Directory. Vous pouvez les personnaliser avec des widgets pour afficher des graphes et des compteurs selon vos besoins.

Le dashboard Tenable Identity Exposure fait office de centre de commande en temps réel pour la sécurité de l'infrastructure Active Directory (AD) de votre organisation. Il fournit un aperçu complet (une vue centralisée en temps réel) de votre paysage d'identité, mettant en évidence les vulnérabilités critiques et les vecteurs d'attaque potentiels pour permettre une atténuation proactive des risques.



Fonctionnalités clés du dashboard

- **Vue d'ensemble** : vérifiez en un clin d'œil l'état de la sécurité de votre infrastructure grâce à des métriques clés bien en vue telles que le score de conformité, les risques principaux et les tendances des activités utilisateur.
- **Informations détaillées en cascade** : approfondissez des domaines spécifiques à l'aide de widgets interactifs qui décomposent les facteurs de risque par sévérité, catégorie d'utilisateurs et d'autres critères pertinents.

- **Focus personnalisable** : créez des dashboards personnalisés en fonction de vos priorités, en utilisant des modèles prédéfinis ou en créant vos propres mises en page. Par exemple, pour créer un dashboard des erreurs de configuration les plus courantes par rapport à des IoE récurrents communs :
    - S'assurer de la cohérence de SDProp
    - Contrôleurs de domaine gérés par des utilisateurs mal intentionnés
    - Délégation Kerberos dangereuse
- **Surveillance en temps réel** : restez informé des menaces émergentes et des activités suspectes grâce à des mises à jour et des alertes en continu.
- **Informations exploitables** : profitez de recommandations pratiques en matière de remédiation, hiérarchisées en fonction de la sévérité et de l'impact potentiel.

Voir aussi

- Dashboards
- Tutoriel vidéo sur les dashboards

Trail Flow

Le Trail Flow de Tenable Identity Exposure affiche la surveillance et l'analyse en temps réel des événements qui affectent votre infrastructure AD. Il permet d'identifier les vulnérabilités critiques et les mesures correctives recommandées.

Dans la page **Trail Flow**, vous pouvez remonter dans le temps et charger des événements antérieurs ou rechercher des événements spécifiques. Vous pouvez également utiliser sa zone de recherche en haut de la page pour rechercher des menaces et détecter des modèles malveillants.

Le Trail Flow suit les événements suivants :

- **Modifications d'utilisateurs et de groupes** : inclut la création, la suppression et la modification de comptes et de groupes.
- **Modifications d'autorisations** : inclut les modifications apportées aux contrôles d'accès sur des objets tels que des fichiers, des dossiers et des imprimantes.
- **Ajustements de la configuration système** : implique les modifications des stratégies de groupe (GPO) et d'autres paramètres critiques.
- **Activités suspectes** : inclut les tentatives non autorisées, les élévations de privilèges et d'autres événements qui déclenchent des signaux d'alerte.

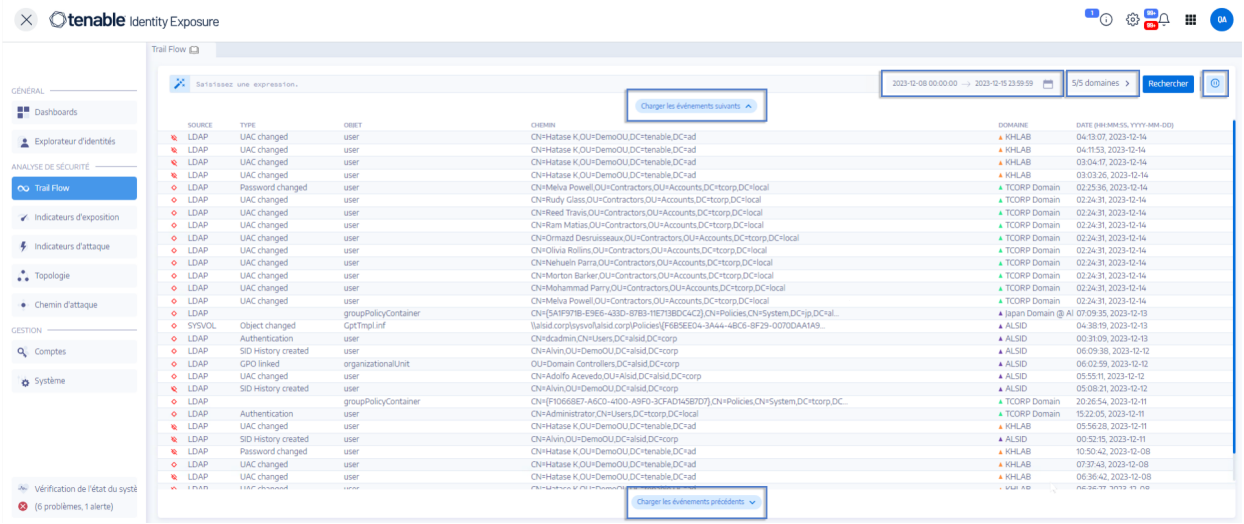
Tenable Identity Exposure propose les fonctionnalités suivantes pour exploiter les données du Trail Flow :

- **Recherche et filtrage** : navigation simple dans le flux d'événements à l'aide de mots-clés ou de critères spécifiques, permettant ainsi de concentrer l'attention sur des activités pertinentes tout en minimisant le bruit superflu.
- **Informations détaillées sur les événements** : chaque entrée d'événement fournit des détails exhaustifs qui incluent l'objet affecté, l'utilisateur responsable de la modification, le protocole utilisé et les indicateurs d'exposition (IoE) associés.
- **Relations visualisées** : les relations entre les événements sont représentées graphiquement pour éclairer la manière dont des activités, apparemment indépendantes les unes des autres, peuvent contribuer à une campagne d'attaque plus large.

Pour accéder au Trail Flow :

- Dans Tenable Identity Exposure, cliquez sur **Trail Flow** dans la barre de navigation sur la partie gauche.

  La page Trail Flow apparaît avec une liste d'événements. Pour plus d'informations, voir Trail Flow Table.



Pour sélectionner une période :

Pour sélectionner un domaine :

Pour afficher un événement :

Pour suspendre Trail Flow et le redémarrer :

Pour charger les événements suivants ou précédents :

Comment les données sont-elles affichées dans le Trail Flow ?

1. Lorsque vous effectuez une action au sein de votre interface Active Directory (AD), par exemple :
   - Création d'un nouveau compte utilisateur
   - Modification de l'appartenance d'un utilisateur à un groupe

- Réinitialisation d'un mot de passe
- Désactivation d'un compte
- Activation d'un compte
- Suppression d'un compte
- Déplacement d'un objet
- Modification d'autorisations

2. L'interface Active Directory (AD) génère automatiquement une entrée de journal d'événements qui consigne les détails de l'opération, et notamment :
    - Un horodatage
    - L'administrateur effectuant l'action
    - Le ou les objets affectés
    - Les modifications spécifiques apportées
3. Tenable Identity Exposure collecte et analyse ces journaux d'événements, met les événements en corrélation, identifie des tendances et détecte les anomalies, tout cela en continu.
4. La page Trail Flow affiche le flux et l'impact de l'opération :
    - Chronologie : affiche une séquence chronologique des événements, avec mise en évidence de l'opération la plus récente.
    - Détails de l'objet : fournit des informations spécifiques sur les objets affectés, notamment leurs attributs et leurs relations.
    - Historique des modifications : affiche l'historique des modifications apportées aux objets, y compris l'opération en cours.
    - Informations sur les risques : identifie les risques potentiels associés à l'opération, comme des autorisations excessives ou l'appartenance à des groupes sensibles.
    - Informations sur la conformité : indique toute violation de conformité liée à l'opération.

Voir aussi

- Vue d'ensemble de Trail Flow
- Trail Flow Use Cases
- Tutoriel vidéo portant sur Trail Flow

Centre de rapports

Le **Centre de rapports** de Tenable Identity Exposure fournit une fonctionnalité très utile qui vous permet d'exporter des données importantes dans des rapports destinés aux principaux acteurs au sein d'une organisation. Le Centre de rapports permet de créer des rapports à partir d'une liste prédéfinie pour garantir un processus efficace et rationnel.

Il offre les fonctions suivantes :

- **Filtrage granulaire** : affinez les rapports à l'aide de filtres granulaires basés sur la plage de dates, le domaine, l'indicateur d'attaque (IoA), l'indicateur d'exposition (IoE) et d'autres paramètres, qui vous garantiront des informations extrêmement détaillées.
- **Livraison automatisée** : planifiez des rapports de façon à automatiser leur création et leur livraison aux intervalles souhaités, et simplifiez ainsi les processus de surveillance de la sécurité et de reporting.
- **Exportation flexible** : exportez des rapports dans différents formats, dont CSV, pour procéder à une analyse plus approfondie, les partager à l'aide d'une clé d'accès aux rapports ou les intégrer à vos workflows de création de rapports.

Les administrateurs peuvent créer différents types de rapports pour un éventail d'utilisateurs, portant sur des périodes flexibles pouvant aller jusqu'à un trimestre. La possibilité de partager des données d'identité critiques à partir de Tenable Identity Exposure permet à l'organisation d'atténuer les risques de manière proactive et d'identifier les attaques potentielles basées sur l'identité.

Pour télécharger un rapport, les utilisateurs reçoivent un e-mail contenant une URL d'accès à une page dans laquelle ils saisissent une clé d'accès au rapport, qu'ils ont reçue de leur administrateur. Les rapports peuvent être téléchargés pendant 30 jours. Passé ce délai, ils expirent et Tenable Identity Exposure les supprime. Les utilisateurs doivent télécharger leurs rapports avant que Tenable Identity Exposure n'en génère un nouveau pour la période spécifiée, qui va remplacer le précédent.

Pour accéder au Centre de rapports :

1. Dans Tenable Identity Exposure, sélectionnez **Systèmes** > **Configuration**.
2. Sous **Rapports**, cliquez sur **Centre de rapports**.

Un volet apparaît avec une liste des rapports configurés et leurs informations associées, telles que le nom du rapport, le type, le domaine, le profil, la période, la récurrence et les adresses e-mails des destinataires.

Voir aussi

- Centre de rapports
- Set Permissions for a Role

Indicateurs d'exposition

Tenable Identity Exposure mesure la maturité de la sécurité de vos infrastructures AD par le biais d'indicateurs d'exposition (IoE) et attribue des niveaux de sévérité au flux d'événements qu'il surveille et analyse. Tenable Identity Exposure déclenche des alertes lorsqu'il détecte des régressions de sécurité.

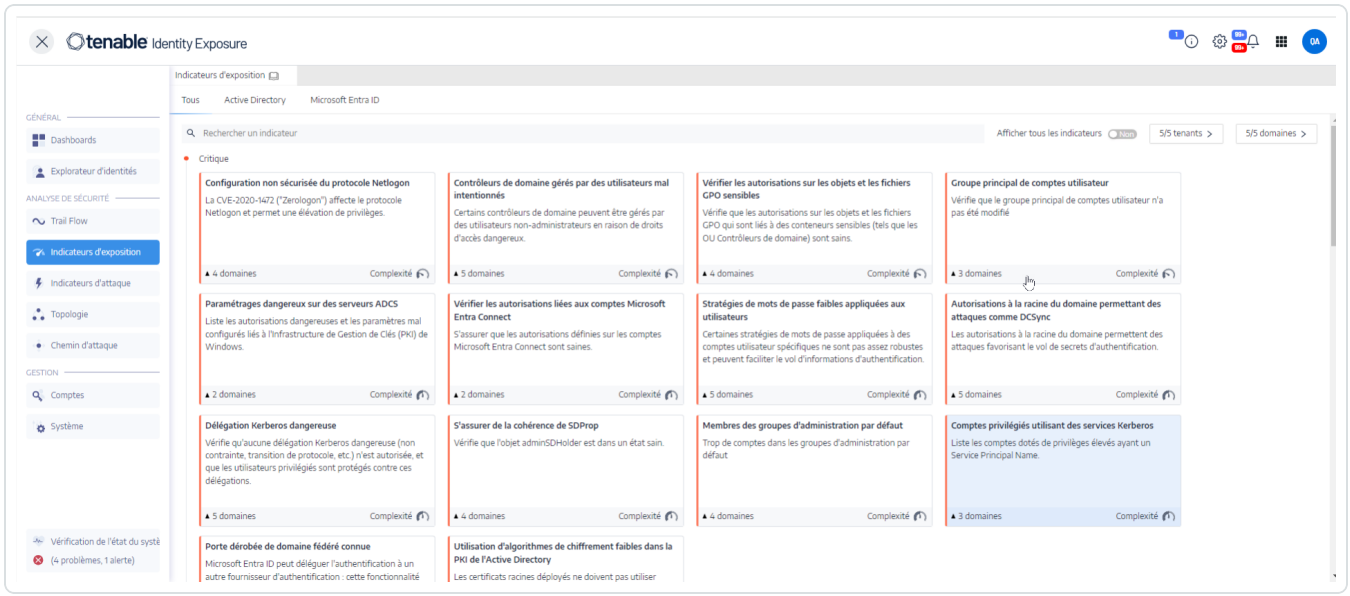
Ces IoE sont pré-configurés et toute déviation par rapport aux normes établies déclenche les alertes correspondantes.

Pour afficher les IoE :

1. Dans Tenable Identity Exposure, cliquez sur **Indicateurs d'exposition** dans le volet de navigation.

   Le volet **Indicateurs d'exposition** apparaît. Par défaut, Tenable Identity Exposure affiche uniquement les IoE qui contiennent des déviances.

2. (Facultatif) Pour afficher tous les IoE, cliquez sur le curseur **Afficher tous les indicateurs** pour activer l'option **Oui**.



Les IoE Tenable Identity Exposure sont dotés d'une série de fonctionnalités conçues pour renforcer vos capacités d'investigation :

- **Recherche et filtrage** : explorez facilement les IoE en appliquant des filtres basés sur la forêt et le domaine.
- **Fonction d'exportation** : l'objet déviant vous permettra d'exporter les IoE au format CSV.
- **Action sur les incidents IoE** : supprimez une exposition de la liste blanche pour la réactiver.

Les données des IoE incluent :

- **Section Informations** : cette section fournit un résumé de chaque indicateur d'exposition (IoE), en précisant les outils d'attaque connus, les domaines affectés et la documentation pertinente.
- **Détails de la vulnérabilité** : cette section fournit des informations plus détaillées concernant la mauvaise configuration d'Active Directory.
- **Objets déviants** : cette section met en évidence les mauvaises configurations d'Active Directory qui peuvent contribuer à élargir la surface d'attaque.
- **Recommandation** : cette section détaille des stratégies de configuration efficaces pour minimiser votre surface d'attaque.

Niveau de sévérité

Les niveaux de sévérité permettent d'évaluer la sévérité des vulnérabilités détectées et de prioriser les actions de remédiation.

Le volet **Indicateurs d'exposition** affiche les IoE comme suit :

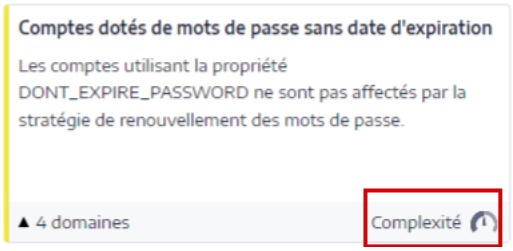
- Par niveau de sévérité en utilisant des codes couleur.
- Verticalement – du plus sévère au moins sévère (rouge pour la priorité absolue et bleu pour la priorité la plus basse).
- Horizontalement – du plus complexe au moins complexe. Tenable Identity Exposure calcule dynamiquement l'indicateur de complexité afin d'indiquer le niveau de difficulté de la correction de l'IoE déviant.

Sévérité	Description
Critique – Rouge	Indique comment empêcher les attaques et la compromission de l'infrastructure Active Directory par certains utilisateurs sans privilèges.

Élevé – Orange	Traite des techniques de post-exploitation conduisant au vol d'identifiants ou à un contournement de sécurité, ou des techniques d'exploitation qui doivent être enchaînées à d'autres pour être dangereuses.
Moyen - Jaune	Indique un risque limité pour l'infrastructure Active Directory.
Faible - Bleu	Affiche les bonnes pratiques de sécurité. Certains contextes opérationnels peuvent autoriser des déviances à faible impact qui n'affectent pas nécessairement la sécurité AD. Ces déviances n'ont d'impact sur l'infrastructure AD que si un administrateur commet une erreur, en activant un compte inactif par exemple.

Priorisation de la remédiation

Vous allez prioriser les efforts de remédiation sur les IoE à sévérité élevée identifiés par le système. En outre, vous serez en mesure de prioriser davantage au sein de la catégorie critique, en vous aidant du compteur de risques intégré à l'IoE.

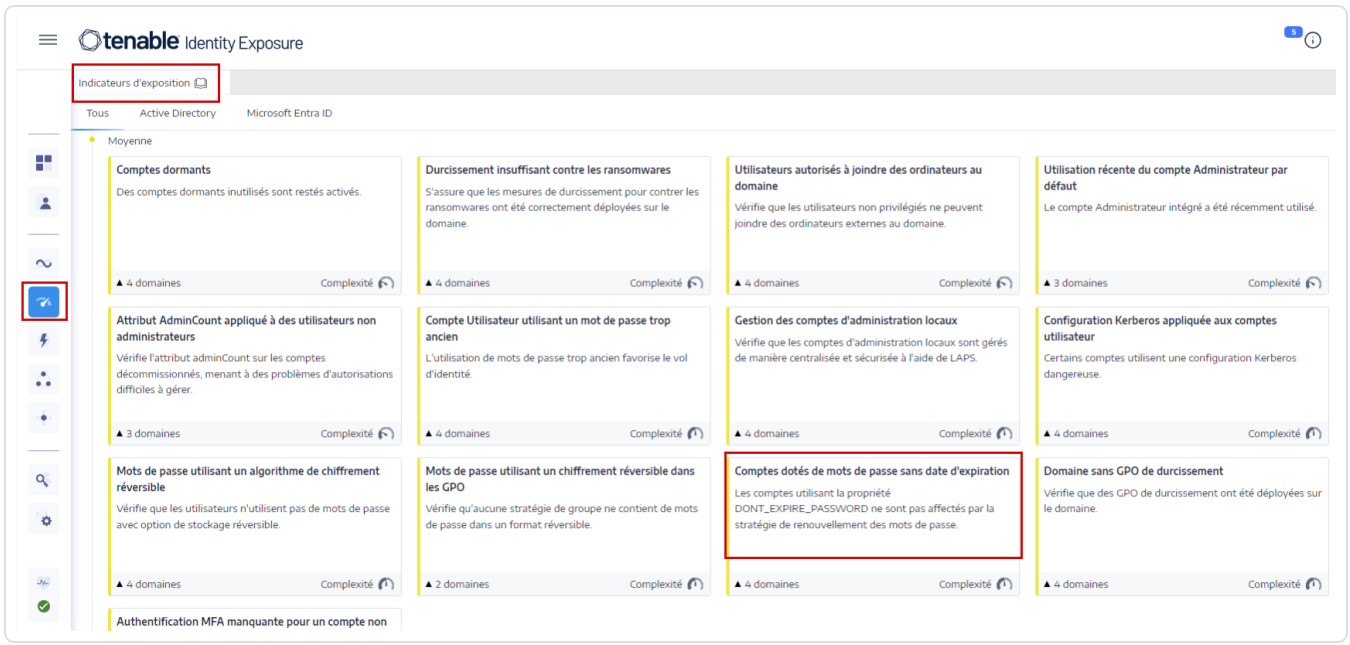


Si vous pensez que l'IoE relève de la compétence ou du mandat opérationnel de votre organisation, vous pouvez l'ajouter à la liste blanche.

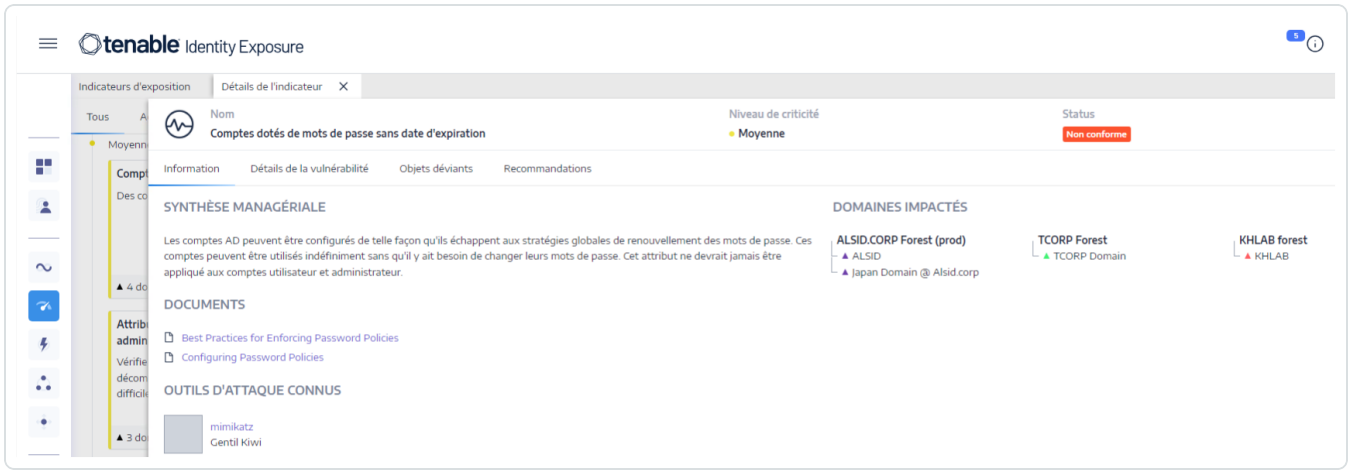
Cas d'utilisation

Le cas d'utilisation suivant se concentre sur l'IoE appelé « Comptes dotés de mots de passe sans date d'expiration ».

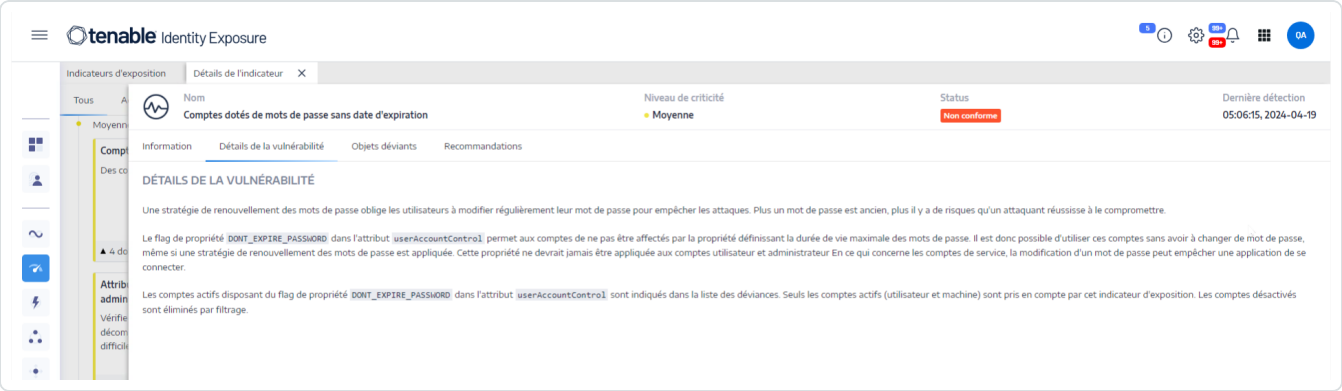
1. Lorsque Tenable Identity Exposure signale un IoE, ce dernier apparaît dans le volet Indicateurs d'exposition :



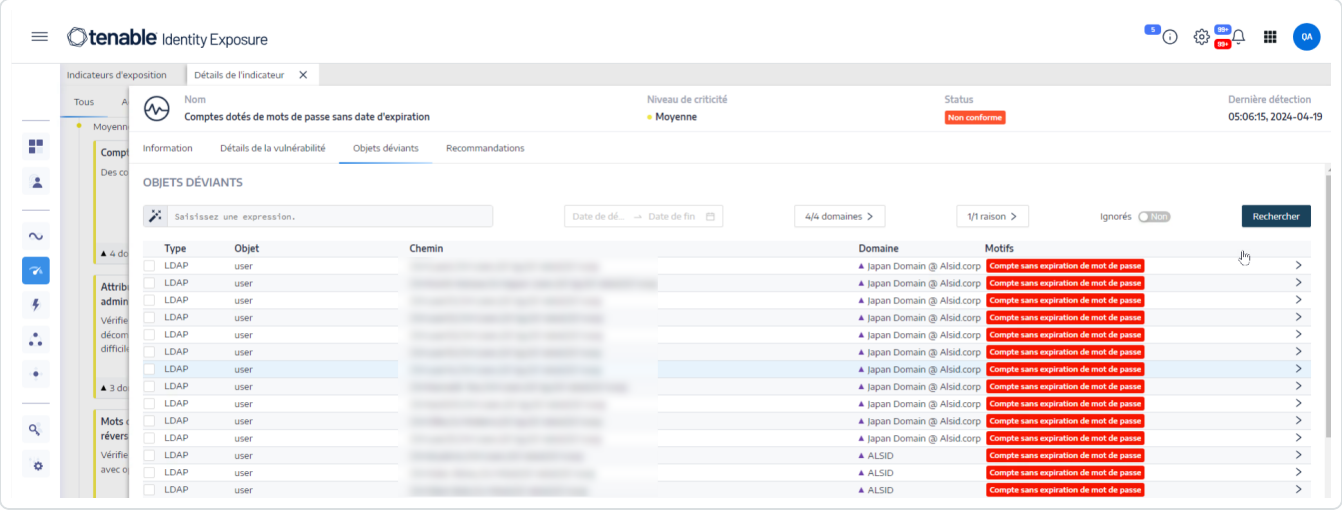
2. Pour obtenir plus d'informations sur l'IoE, cliquez dessus pour accéder à des détails supplémentaires. Sur la page d'informations, vous découvrirez un résumé fournissant une présentation rapide, des détails sur les outils d'attaque potentiels associés à l'IoE, les domaines affectés et de la documentation pour vous aider à comprendre et à résoudre efficacement le problème.

3. 

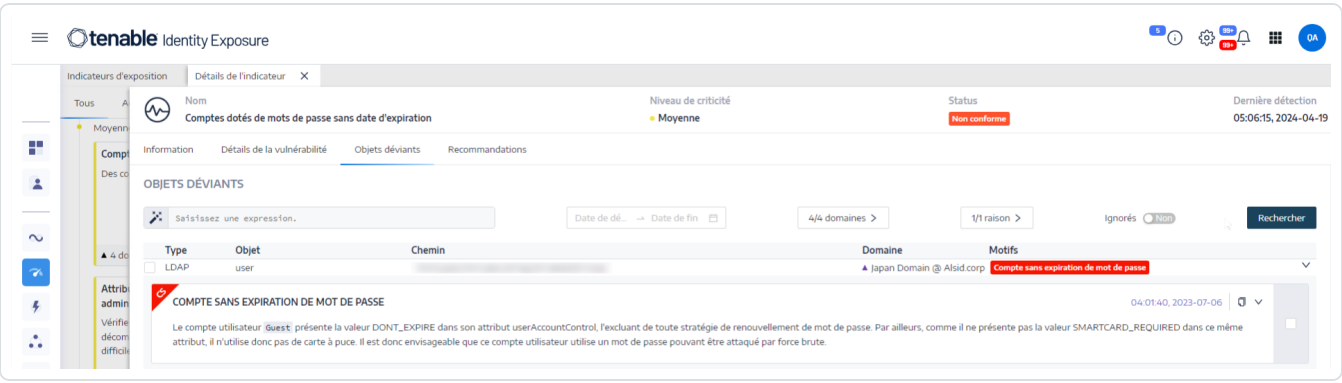
4. Pour plus de détails sur l'IoE, cliquez sur l'onglet « Détails de la vulnérabilité ».



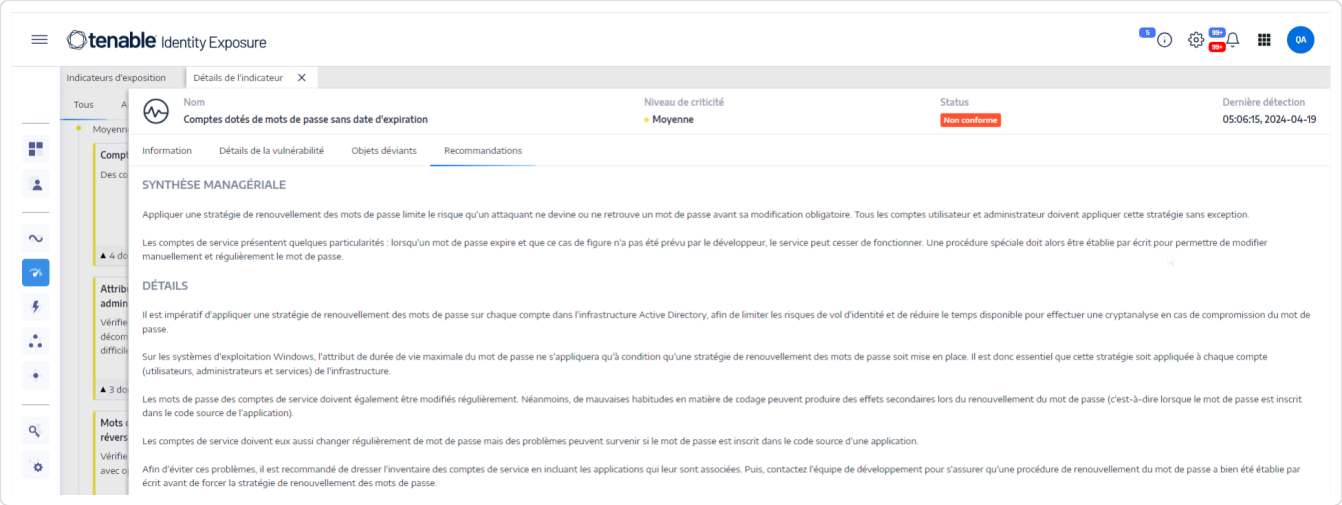
5. Pour vérifier sur quels comptes le paramètre « Comptes dotés de mots de passe sans date d'expiration » est activé, cliquez sur « Objets déviants ». Vous aurez alors accès à la liste des comptes qui possèdent cette configuration au sein de votre système.



6. Cliquez sur l'objet déviant pour afficher les comptes signalés par l'IoE.



7. Consultez votre administrateur Active Directory pour comprendre pourquoi l'option « Comptes dotés de mots de passe sans date d'expiration » est activée pour le compte concerné.
8. En fonction de la réponse, vous pouvez soit choisir d'ajouter le compte à la liste blanche, soit aider votre administrateur Active Directory à formuler des recommandations pour résoudre le problème.
9. Dans le deuxième cas, vous pouvez vous référer à la section « Recommandation » de l'IoE.



10. Si le compte est associé à une exception ou fonctionne comme prévu, vous pouvez ignorer l'IoE en accédant à **Objet déviant** > Sélectionnez la déviance respective > **Ignorer** l'objet sélectionné (ou) Ne plus ignorer l'objet sélectionné, selon les besoins.

Voir aussi

- Indicators of Exposure
- Tutoriel vidéo portant sur les indicateurs d'exposition
- Customize an Indicator

Indicateurs d'attaque

Les indicateurs d'attaque (IoA) de Tenable Identity Exposure permettent à votre organisation de détecter les tentatives de compromission de vos infrastructures Active Directory par les techniques d'exploitation les plus avancées et de prendre immédiatement les mesures qui s'imposent, notamment :

- **3 principaux incidents** : une présentation unifiée des IoA affiche une chronologie en temps réel avec les trois principaux incidents qui ont affecté votre infrastructure AD, ainsi que la répartition des attaques, le tout au sein d'une interface unique.
- **Détails sur l'IoA** : au sein de Tenable Identity Exposure, le panneau de l'IoA fournit des informations sur les attaques qui ont eu lieu au sein de votre infrastructure AD.
- **Incidents impliquant l'IoA** : la liste des incidents IoA donne des détails complets sur des attaques spécifiques ciblant votre infrastructure AD. Ces informations vous permettent de répondre de manière appropriée en fonction du niveau de sévérité de l'IoA.

Les indicateurs d'attaque sont dotés d'une série de fonctionnalités conçues pour renforcer vos capacités d'investigation :

- **Recherche et filtrage** : explorez facilement l'IoA en utilisant la frise chronologique ou appliquez des filtres basés sur la forêt, le domaine et le niveau de criticité pour des résultats ciblés et efficaces.
- **Fonction d'exportation** : permet l'exportation des données d'IoA aux formats PDF, CSV ou PPTX.
- **Modifier le type de graphique :** donne la possibilité de modifier le type de graphique en permettant d'afficher soit la distribution de la sévérité des attaques, soit les trois principales attaques avec leurs nombres d'occurrences respectifs.
- **Action sur les incidents IoA** : permet de sélectionner un incident à fermer ou à rouvrir.

Niveau de sévérité

Tenable Identity Exposure détecte et attribue des niveaux de sévérité aux attaques :

Niveau	Description

Critique – Rouge	Détection d'une attaque post-exploitation prouvée dont la domination de domaine est une condition préalable.
Élevé – Orange	Détection d'une attaque majeure qui permet à un attaquant d'atteindre la domination de domaine.
Moyen – Jaune	L'IoA est liée à une attaque qui pourrait conduire à une élévation dangereuse des privilèges ou permettre l'accès à des ressources sensibles.
Faible – Bleu	Alertes sur les comportements suspects liés aux actions de reconnaissance ou aux incidents à faible impact.

Priorisation de la remédiation

Identifiez les IoA critiques et à fort impact qui correspondent à vos risques et problèmes de sécurité spécifiques.

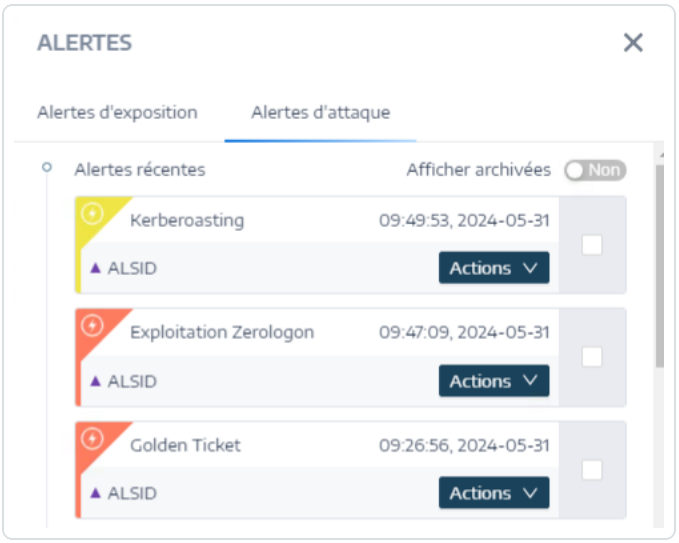
Pour atténuer le risque de faux positifs et éviter que des attaques légitimes soient ignorées, il est essentiel de calibrer les IoA en fonction de votre environnement. Cela implique les mesures suivantes :

- Ajustement des seuils : calibrez la sensibilité des IoA pour réduire les faux positifs en veillant à ce que les alertes soient significatives et exploitables.
- Ajout de comptes et d'activités à la liste blanche : excluez les activités légitimes découlant du déclenchement des IoA, améliorez la précision des alertes et simplifiez les investigations.
- Mise en corrélation des IoA : analysez les relations entre les différents IoA pour identifier des schémas d'attaque plus larges.

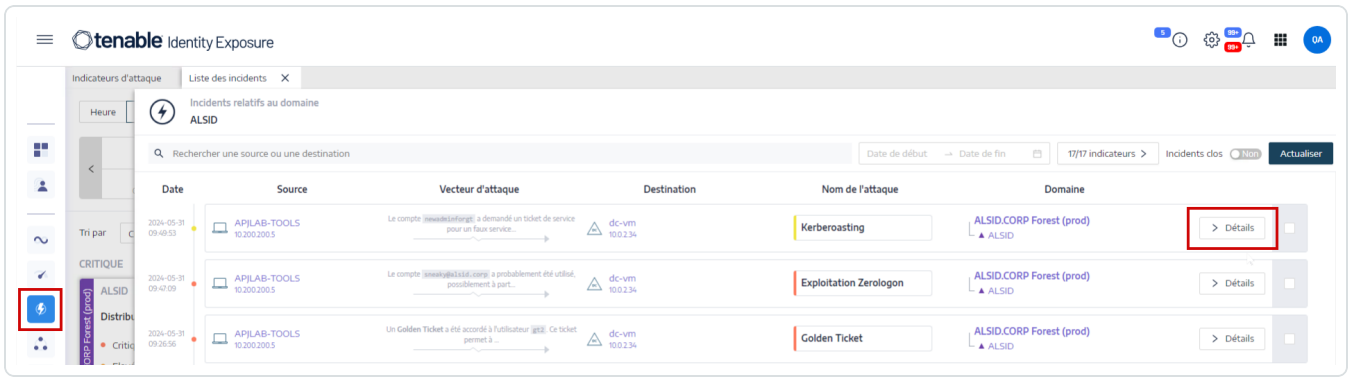
Conseil : pour plus de détails sur les options et les valeurs recommandées, référez-vous au guide Tenable Identity Exposure Indicators of Attack Reference Guide (disponible sur https://fr.tenable.com/downloads/identity-exposure). Appliquez ces options et ces valeurs à chaque IoA dans le profil de sécurité.

Cas d'utilisation

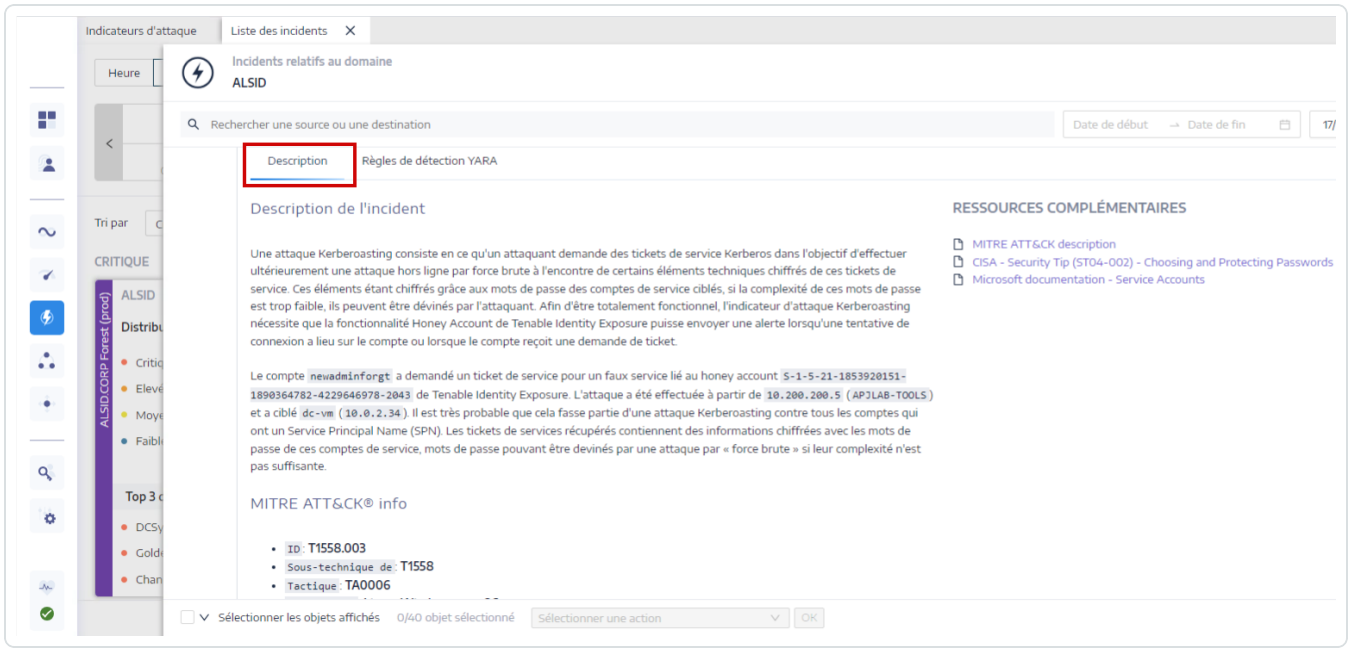
1. Lors de l'activation d'un IoA, sélectionnez « Indicateurs d'attaque » dans le volet de navigation ou cliquez sur l'icône de cloche située dans le coin supérieur droit de la page d'accueil.



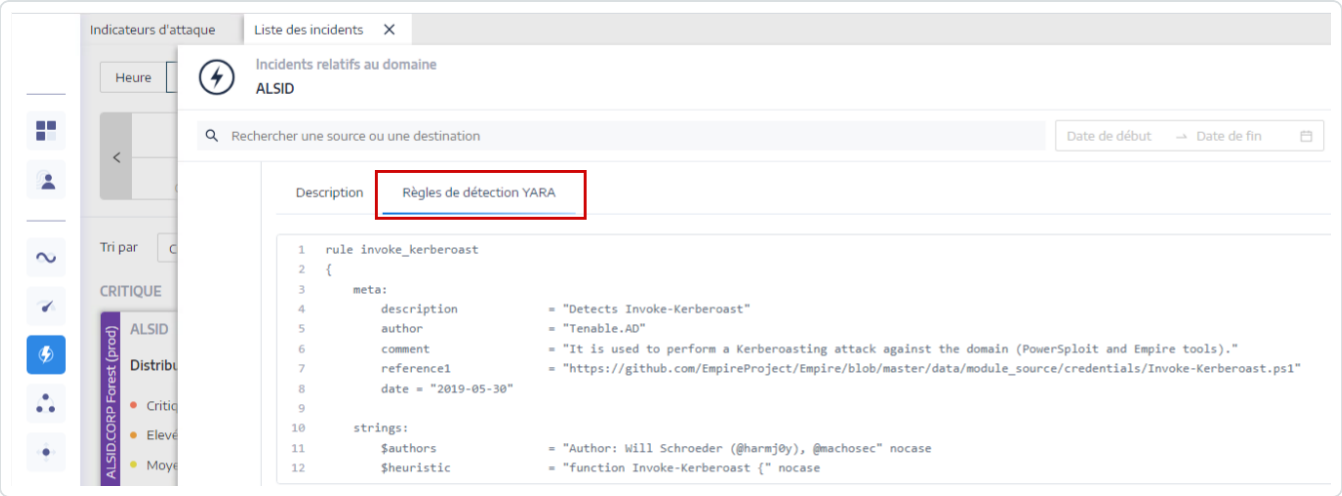
2. Chaque indicateur vous fournira des informations détaillées sur l'incident et vous permettra de prendre les mesures appropriées après examen des points suivants :
    - Moment de l'attaque
    - Description de l'attaque
    - Source de l'attaque
    - Cible de l'attaque
    - Informations MITRE ATT&CK®
    - Règles de détection YARA
    - Ressources complémentaires
3. Sélectionnez « Détails » pour accéder à la description, comme illustré dans cet exemple, qui porte sur l'énumération des administrateurs locaux.



4. L'onglet Description fournit des informations sur des attaques spécifiques contre votre infrastructure Active Directory (AD).



5. L'onglet Règles de détection YARA fournit des informations sur les règles YARA utilisées par Tenable Identity Exposure pour détecter les attaques Active Directory au niveau du réseau, améliorant ainsi les capacités de détection globales de Tenable Identity Exposure.



6. Collaborez avec l'administrateur Active Directory ou la partie prenante concernée pour examiner et résoudre l'incident, décider de le fermer ou de le rouvrir, et prendre des mesures pour empêcher qu'il se reproduise.
7. S'il s'agit d'une attaque reconnue ou autorisée, vous avez la possibilité de personnaliser l'IoA en conséquence pour éviter qu'il ne la signale à l'avenir.

Voir aussi

- Indicators of Attack
- Customize an Indicator
- Tutoriel vidéo portant sur les indicateurs d'attaque

Prise en charge de Microsoft Entra ID

Outre Active Directory, Tenable Identity Exposure prend en charge Microsoft Entra ID (anciennement Azure AD ou AAD) pour étendre la portée des identités dans une organisation. Cette fonctionnalité utilise de nouveaux indicateurs d'exposition qui se concentrent sur les risques spécifiques à Microsoft Entra ID.

Pour intégrer Microsoft Entra ID à Tenable Identity Exposure, suivez scrupuleusement ce processus d'intégration :

1. Respecter les Conditions préalables
2. Vérifier les Autorisations
3. Vérifier les Flux réseau
4. Configurer les paramètres Microsoft Entra ID
5. Activer la prise en charge de Microsoft Entra ID
6. Activer les scans de tenant

Conditions préalables

Vous avez besoin d'un compte Tenable Cloud pour vous connecter à « cloud.tenable.com » et utiliser la fonction de prise en charge de Microsoft Entra ID. Ce compte Tenable Cloud utilise la même adresse e-mail que celle de votre e-mail de bienvenue. Si vous ne connaissez pas l'adresse e-mail à utiliser pour « cloud.tenable.com », veuillez contacter le service d'assistance. Tous les clients disposant d'une licence valide (sur site ou SaaS) peuvent accéder à Tenable Cloud sur « cloud.tenable.com ». Ce compte vous permet de configurer des scans Tenable pour Microsoft Entra ID et de collecter les résultats de ces scans.

Remarque : vous n'avez pas besoin d'une licence **Tenable Vulnerability Management** valide pour accéder à Tenable Cloud. Une licence autonome Tenable Identity Exposure en cours de validité (sur site ou SaaS) est suffisante.

Remarque : Tenable Identity Exposure **ne prend pas en charge Microsoft Entra ID dans les clouds nationaux**, y compris les zones dédiées aux gouvernements chinois et américain. Microsoft Entra ID propose des clouds nationaux. Il s'agit d'instances d'Azure physiquement isolées, conçues pour des besoins spécifiques en matière de réglementation et de conformité. Tenable Identity Exposure ne prend en charge que l'environnement Microsoft Entra ID global, à l'exception du cloud national chinois et du cloud

national du gouvernement américain. Pour plus d'informations sur les clouds nationaux Microsoft Entra ID, voir Authentification de Microsoft Entra et clouds nationaux - Plateforme d'identités Microsoft.

Autorisations

La prise en charge de Microsoft Entra ID nécessite de collecter des données auprès de Microsoft Entra ID : utilisateurs, groupes, applications, principaux de service, rôles, autorisations, politiques, journaux, etc. Ces données sont collectées à l'aide de l'API Microsoft Graph et des identifiants des principaux de service conformément aux recommandations de Microsoft.

- Vous devez vous connecter à Microsoft Entra ID en tant qu'**utilisateur disposant des autorisations nécessaires pour accorder le consentement d'administrateur à l'échelle du tenant** sur Microsoft Graph, qui doit avoir le rôle administrateur global ou d'administrateur de rôle privilégié (ou tout autre rôle personnalisé avec les autorisations appropriées), selon Microsoft.
- Pour accéder à la configuration et à la visualisation des données pour Microsoft Entra ID, votre **rôle utilisateur Tenable Identity Exposure** doit disposer des autorisations appropriées. Pour plus d'informations, voir Set Permissions for a Role.

Flux réseau

Autorisez les adresses suivantes sur le port 443 sortant du SEN (Security Engine Node) pour activer la prise en charge d'Entra ID :

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

Nombre de licences

Tenable ne compte pas les identités dupliquées dans la licence **uniquement lorsque la fonction Synchronisation de Tenable Cloud est activée**. Sans cette fonctionnalité, Tenable ne peut pas rapprocher les comptes de Microsoft Entra ID et d'Active Directory. Tenable compte donc chacun d'eux séparément.

- **Sans la synchronisation de Tenable Cloud**, un utilisateur unique possédant à la fois un compte AD et un compte Entra ID compte comme deux utilisateurs distincts du point de vue de la licence.
- **Lorsque la synchronisation de Tenable Cloud est activée**, le système regroupe plusieurs comptes en une seule identité, ainsi un utilisateur ayant plusieurs comptes n'est compté qu'une seule fois.

Configurer les paramètres Microsoft Entra ID

Utilisez les procédures suivantes (adaptées de la documentation Microsoft Démarrage rapide : Inscrire une application avec la plateforme d'identités Microsoft) pour configurer tous les paramètres requis dans Microsoft Entra ID.

1. **Créer une application :**

   a. Dans le portail d'administration Azure, ouvrez la page **Inscriptions d'application**.

   b. Cliquez sur **Nouvelle inscription**.

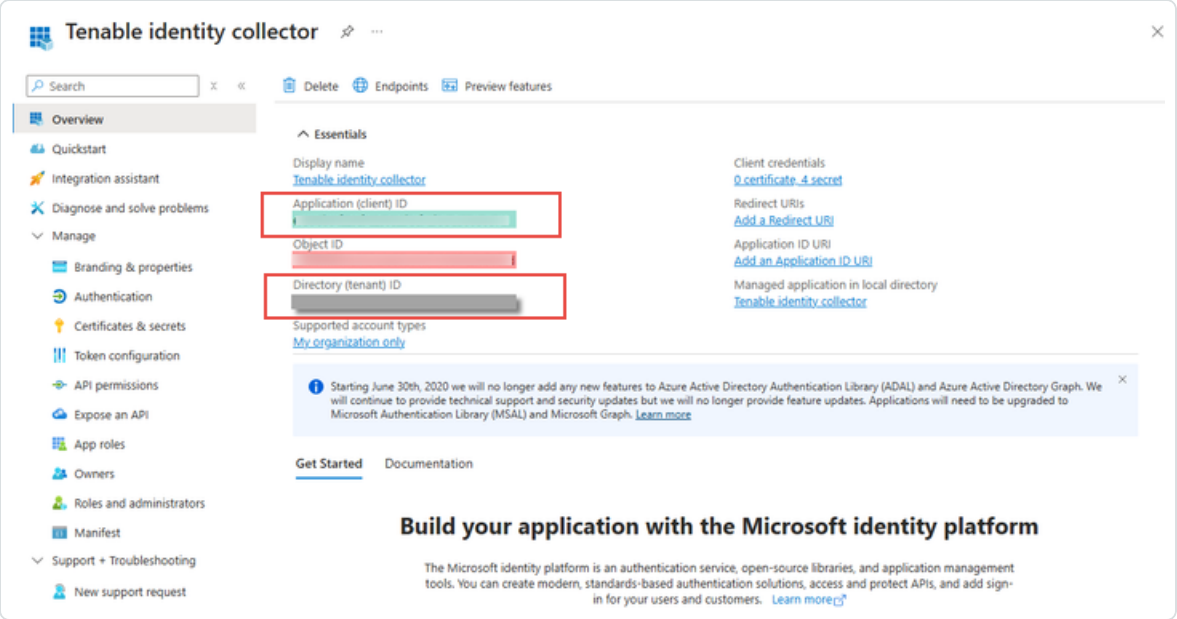
   c. Donnez un nom à l'application (par exemple, « Tenable Identity Collector »). Pour les autres options, vous pouvez laisser les valeurs par défaut telles qu'elles.

   d. Cliquez sur **Inscrire**.

   e. Sur la page Présentation de cette application nouvellement créée, notez l'« ID de l'application (client) » et l'« ID de l'annuaire (tenant) », qui vous serviront plus tard au cours de l'étape Pour ajouter un nouveau tenant Microsoft Entra ID :.

   > **Attention** : sélectionnez l'**ID de l'application** et **non** l'**ID d'objet** pour que la configuration

fonctionne.



2. **Ajouter des informations d'identification à l'application :**

   a. Dans le portail d'administration Azure, ouvrez la page **Inscriptions d'application**.

   b. Cliquez sur l'application que vous avez créée.

   c. Dans le menu de gauche, cliquez sur **Certificats et secrets**.

   d. Cliquez sur **Nouveau secret de client**.

   e. Dans la zone **Description**, donnez un nom pratique à ce secret et une valeur d'**expiration** conforme à vos politiques. N'oubliez pas de renouveler ce secret quand sa date d'expiration approche.

   f. Enregistrez la valeur secrète dans un emplacement sécurisé, car Azure ne l'affiche qu'une seule fois et vous devez la recréer si vous la perdez.

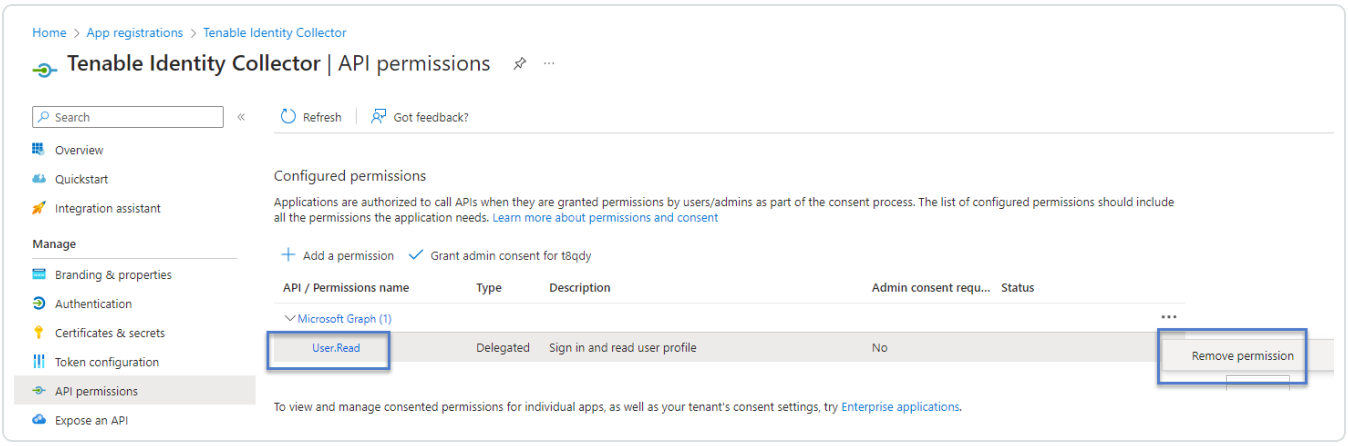
3. **Attribuer des autorisations à l'application :**

   a. Dans le portail d'administration Azure, ouvrez la page **Inscriptions d'application**.

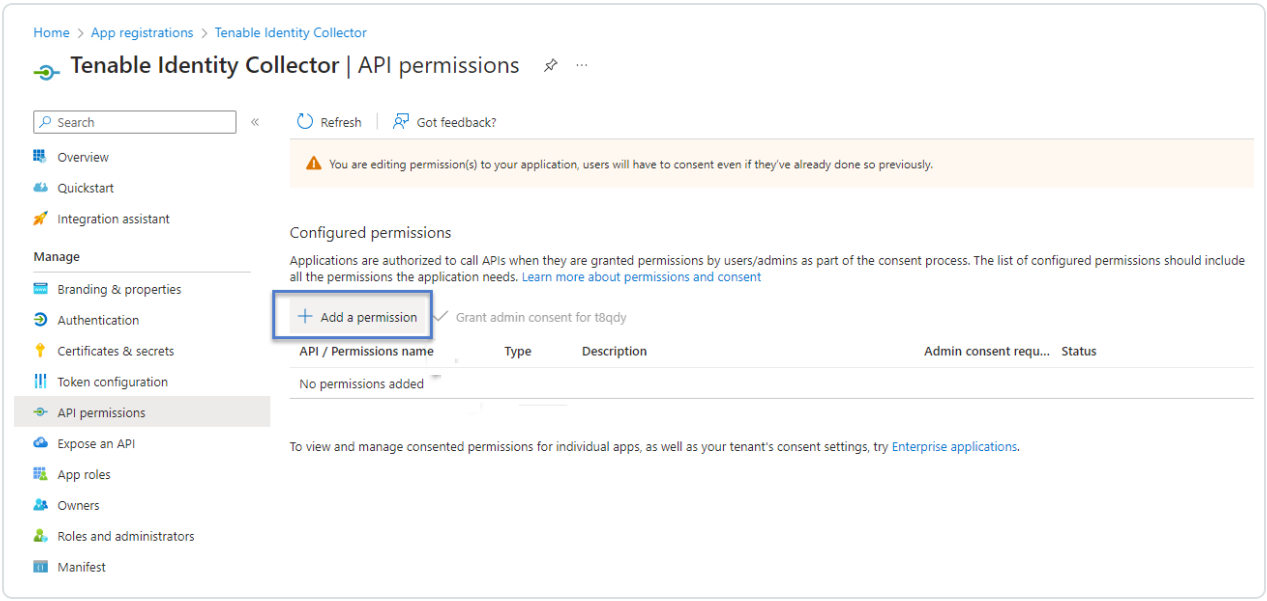
   b. Cliquez sur l'application que vous avez créée.

c. Dans le menu de gauche, cliquez sur **Autorisations des API**

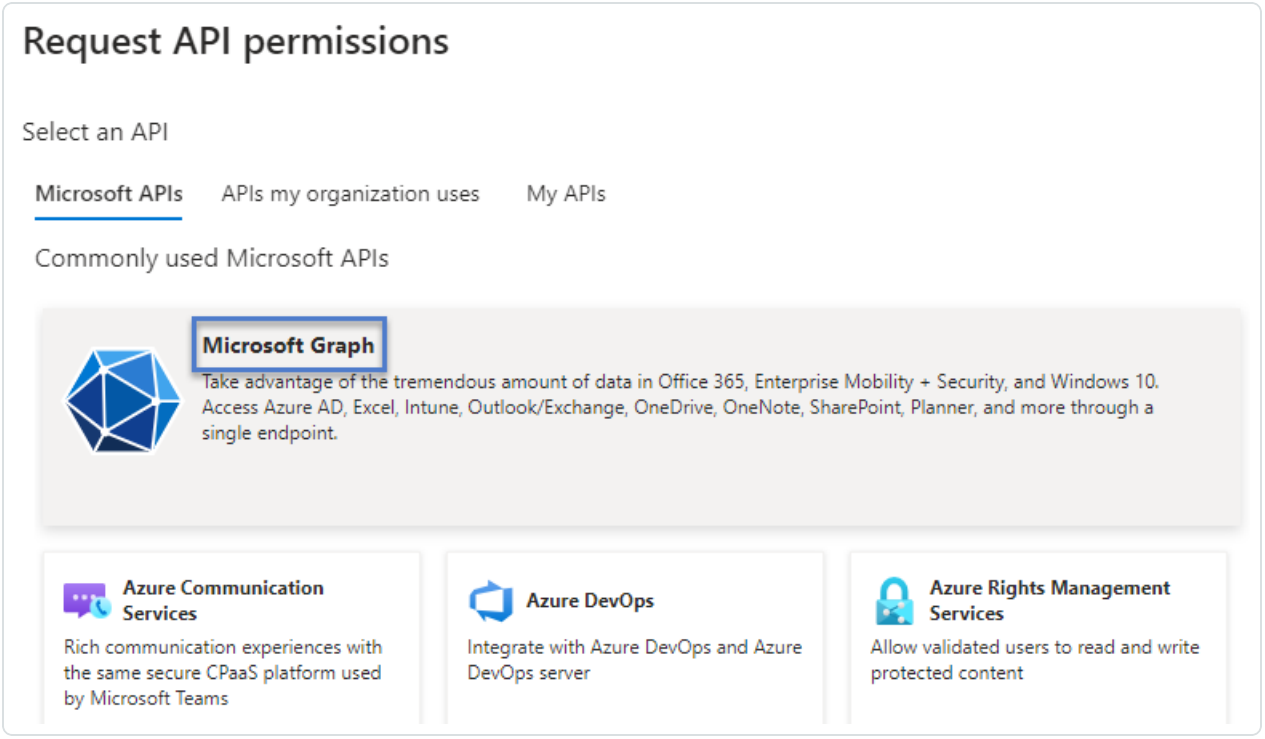
d. Supprimer l'autorisation existante `User.Read` :



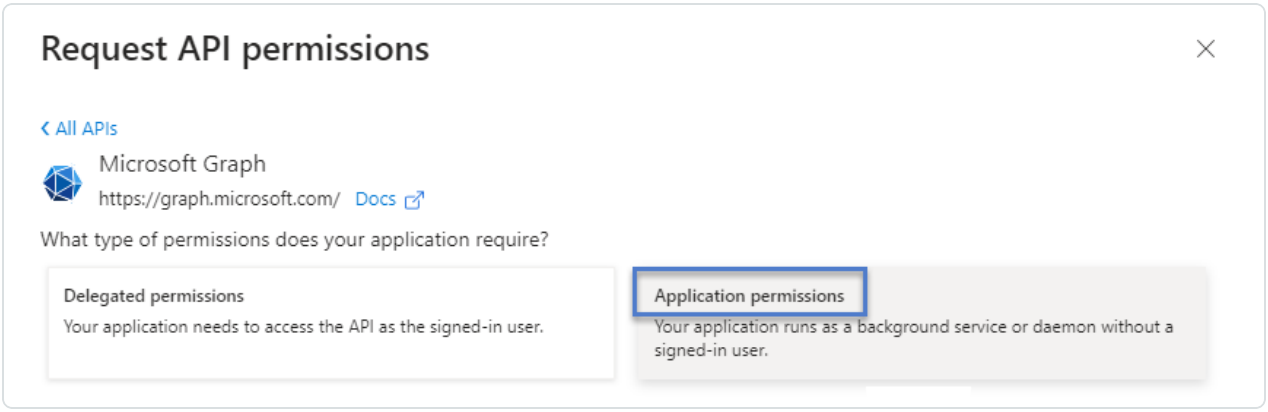
e. Cliquez sur **Ajouter une autorisation** :



f. Sélectionnez **Microsoft Graph** :



g. Sélectionnez **Autorisations de l'application** et non pas « Autorisations déléguées ».



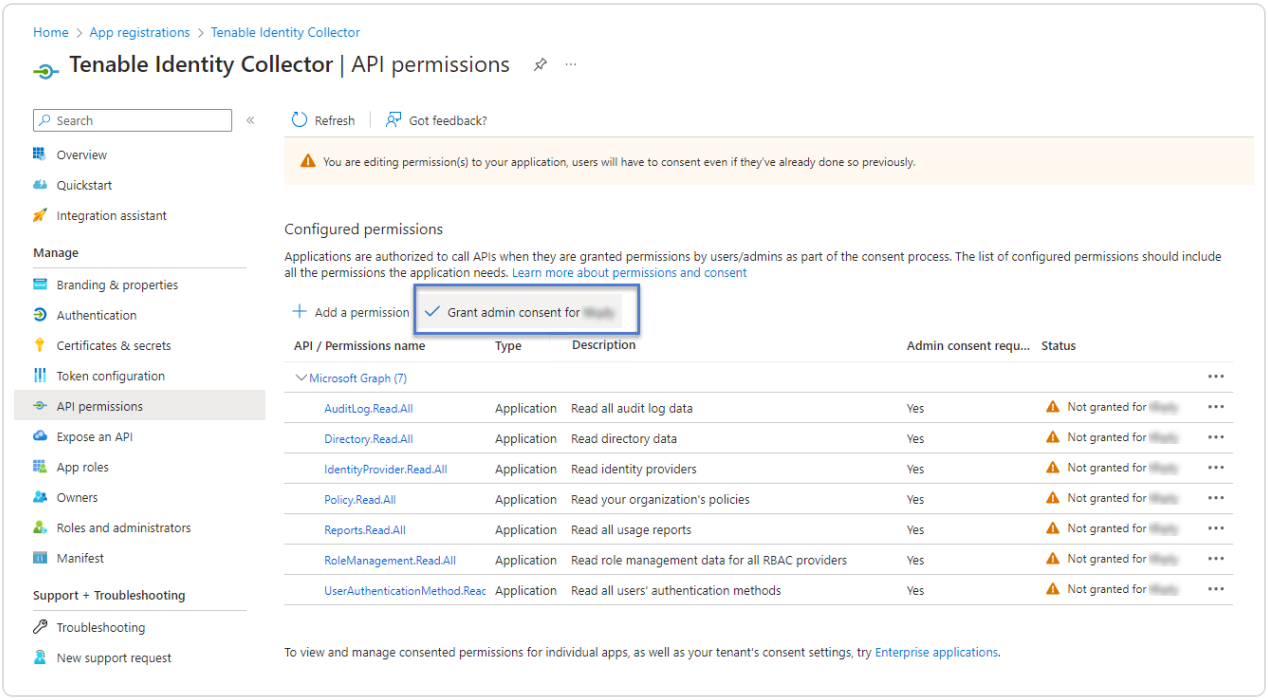
h. Utilisez la liste ou la barre de recherche pour rechercher et sélectionner toutes les autorisations suivantes :

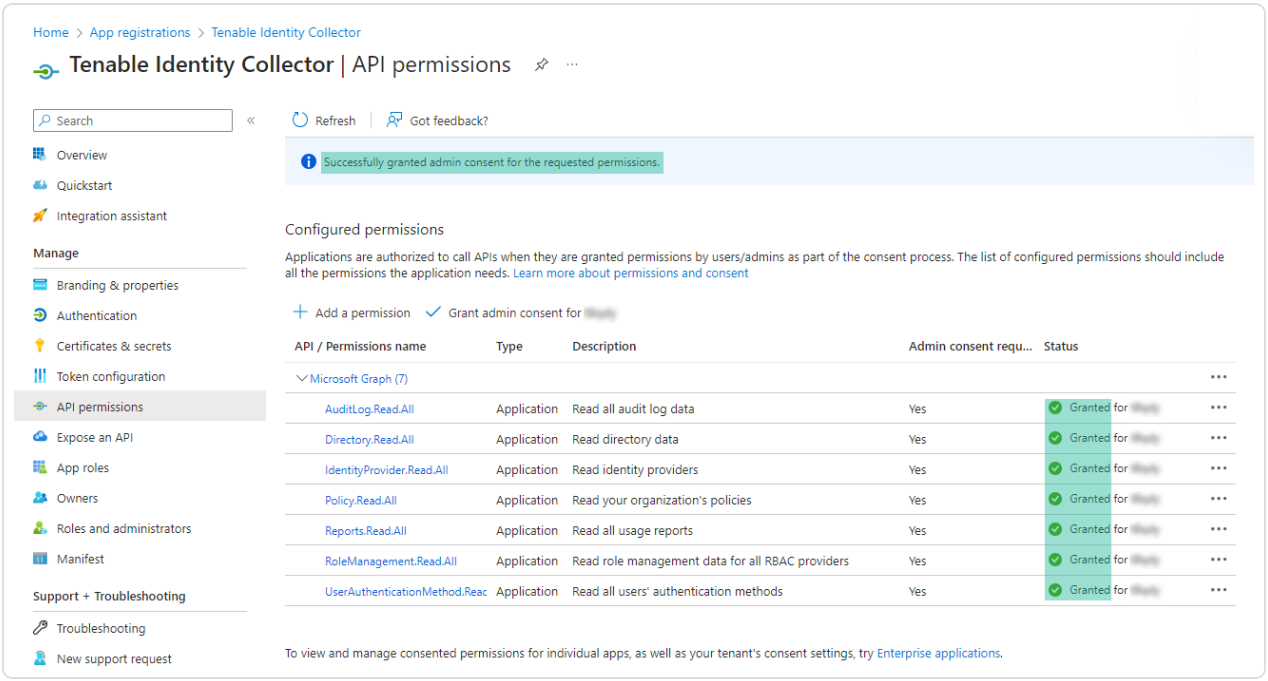
   - `AuditLog.Read.All`
   - `Directory.Read.All`
   - `IdentityProvider.Read.All`
   - `Policy.Read.All`

- `Reports.Read.All`
- `RoleManagement.Read.All`
- `UserAuthenticationMethod.Read.All`

i. Cliquez sur **Ajouter des autorisations**.

j. Cliquez sur **Accorder le consentement administrateur <nom du tenant>** et cliquez sur **Oui** pour confirmer :





4. Après avoir configuré tous les paramètres requis dans Microsoft Entra ID :
    a. Dans Tenable Vulnerability Management, créez un nouvel identifiant de type « Microsoft Azure ».
    b. Sélectionnez la méthode d'authentification « Clé » et saisissez les valeurs que vous avez récupérées dans la procédure précédente : ID de tenant, ID d'application et Secret de client.

Activer la prise en charge de Microsoft Entra ID

- Pour utiliser **Microsoft Entra ID**, vous devez activer la fonctionnalité dans les paramètres Tenable Identity Exposure.
- Voir Identity 360, Exposure Center, and Microsoft Entra ID Support Activation pour obtenir des instructions.

Activer les scans de tenant

Pour ajouter un nouveau tenant Microsoft Entra ID :

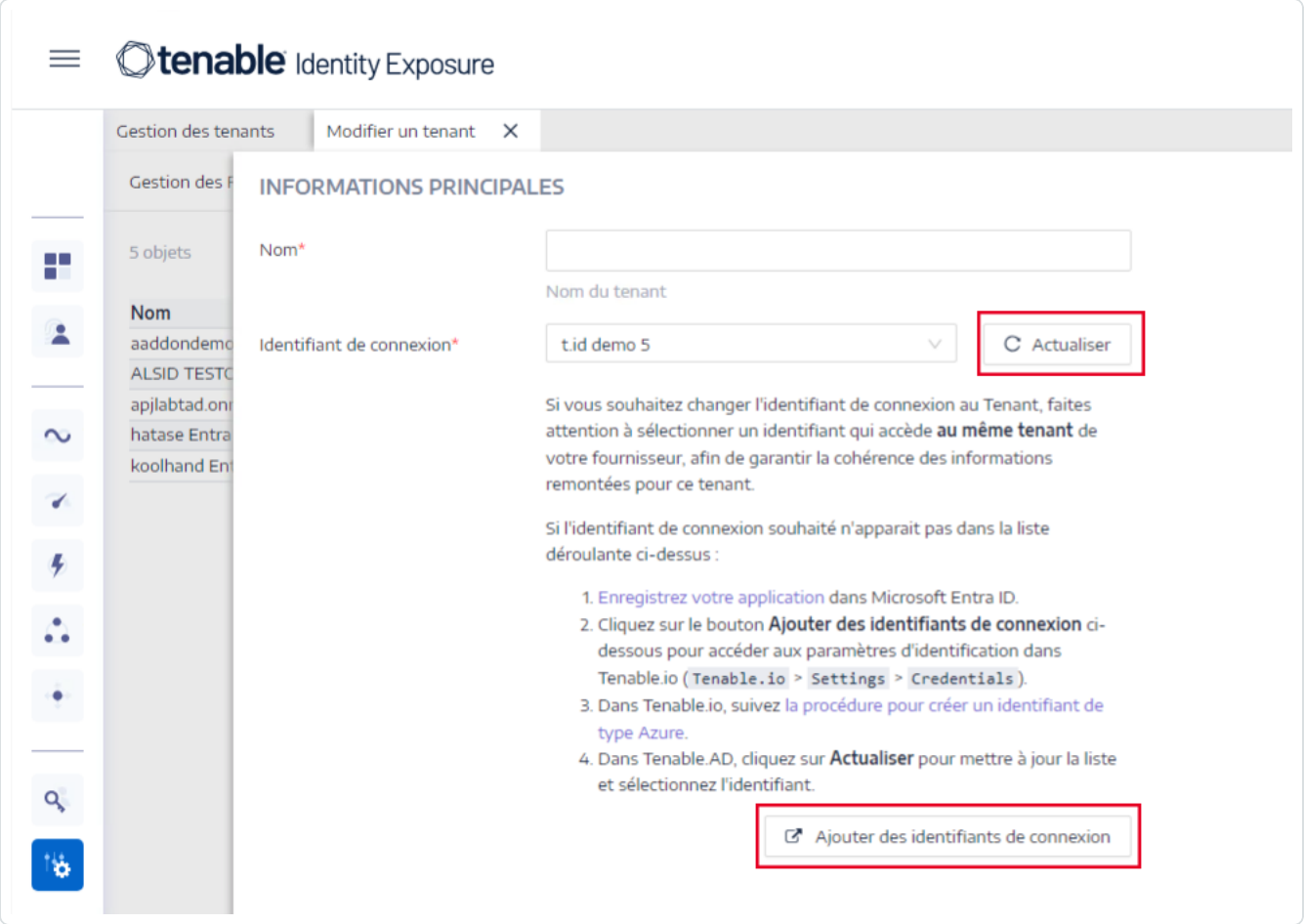
L'ajout d'un tenant lie Tenable Identity Exposure au tenant Microsoft Entra ID pour effectuer des scans sur le tenant.

1. Sur la page de configuration, cliquez sur l'onglet **Gestion des tenants**.

    La page **Gestion des tenants** apparaît.

2. Cliquez sur **Ajouter un tenant**.

    La page **Ajouter un tenant** apparaît.



3. Dans la zone **Nom du tenant**, saisissez un nom.
4. Dans la zone **Identifiants**, cliquez sur la liste déroulante pour sélectionner un identifiant.
5. Si votre identifiant ne figure pas dans la liste, vous pouvez effectuer l'une ou l'autre des opérations suivantes :
    - Créez un identifiant dans Tenable Vulnerability Management (Tenable Vulnerability Management > **Paramètres** > **Identifiants**). Pour plus d'informations, voir la procédure de création d'un identifiant de type Azure dans Tenable Vulnerability Management.
    - Vérifiez que vous disposez de l'autorisation « Peut utiliser » ou « Peut modifier » pour l'identifiant dans Tenable Vulnerability Management. Si vous ne disposez pas de ces

autorisations, Tenable Identity Exposure n'affiche pas l'identifiant dans la liste déroulante.

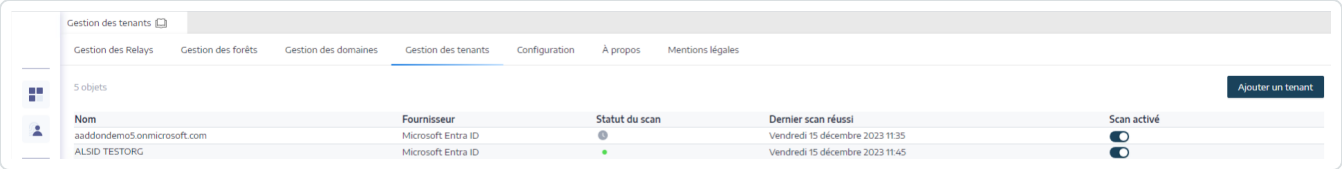
6. Cliquez sur **Actualiser** pour mettre à jour la liste déroulante des identifiants.
7. Sélectionnez l'identifiant que vous avez créé.
8. Cliquez sur **Ajouter**.

   Un message confirme que Tenable Identity Exposure a ajouté le tenant qui apparaît désormais dans la liste de la page Gestion des tenants.

Pour activer les scans pour le tenant :

Remarque : les scans de tenant ne sont pas exécutés en temps réel et il faut compter au moins 45 minutes avant que les données Microsoft Entra ID soient visibles dans l'Explorateur d'identités.

- Sélectionnez un tenant dans la liste et cliquez sur le curseur pour activer l'option **Scan activé**.



Tenable Identity Exposure demande un scan sur le tenant ; les résultats apparaissent sur la page Indicateur d'exposition.

Remarque : le délai minimum obligatoire entre deux scans est de **30 minutes**.

Chemin d'attaque

Tenable Identity Exposure offre plusieurs façons de visualiser la vulnérabilité potentielle d'un asset opérationnel à l'aide de représentations graphiques.

- **Chemin d'attaque** : affiche les chemins qu'un attaquant peut emprunter pour compromettre un asset à partir d'un point d'entrée.
- **Blast Radius** : affiche les mouvements latéraux possibles dans l'infrastructure Active Directory à partir de n'importe quel asset.
- **Exposition d'un asset** : affiche tous les chemins pouvant potentiellement prendre le contrôle d'un asset.

Comprendre le chemin d'attaque vous permet d'identifier les mesures d'atténuation nécessaires pour empêcher les attaquants d'exploiter les vulnérabilités. Cela peut impliquer de corriger les systèmes, de durcir les configurations, de mettre en œuvre des contrôles d'accès plus stricts ou de sensibiliser les utilisateurs.

Le chemin d'attaque dans Tenable Identity Exposure offre plusieurs avantages :

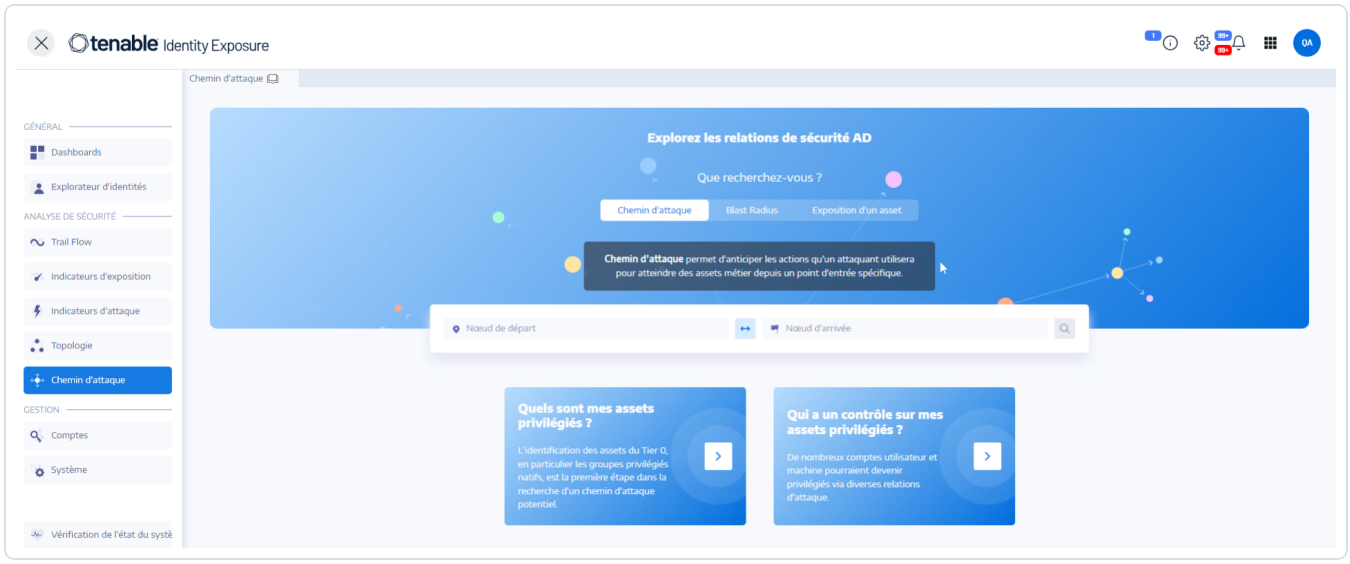
- **Sécurité proactive** : il permet d'anticiper et de traiter les vecteurs d'attaque potentiels avant qu'ils ne soient exploités.
- **Priorisation** : il oriente les efforts de sécurité vers les vulnérabilités et les chemins d'attaque les plus critiques.
- **Visualisation** : il fournit une représentation claire et facile à comprendre des relations de sécurité complexes au sein de votre infrastructure AD.
- **Communication** : il facilite la communication des risques de sécurité aux parties prenantes en fournissant des preuves visuelles des scénarios d'attaque potentiels.

Pour afficher le chemin d'attaque :

Vous spécifiez le point de départ, qui peut être n'importe quel asset de votre infrastructure AD (par exemple, un compte utilisateur, un ordinateur ou un groupe). Vous définissez le point d'arrivée, qui représente l'asset que l'attaquant vise à compromettre (par exemple, un contrôleur de domaine ou un serveur de données sensible).

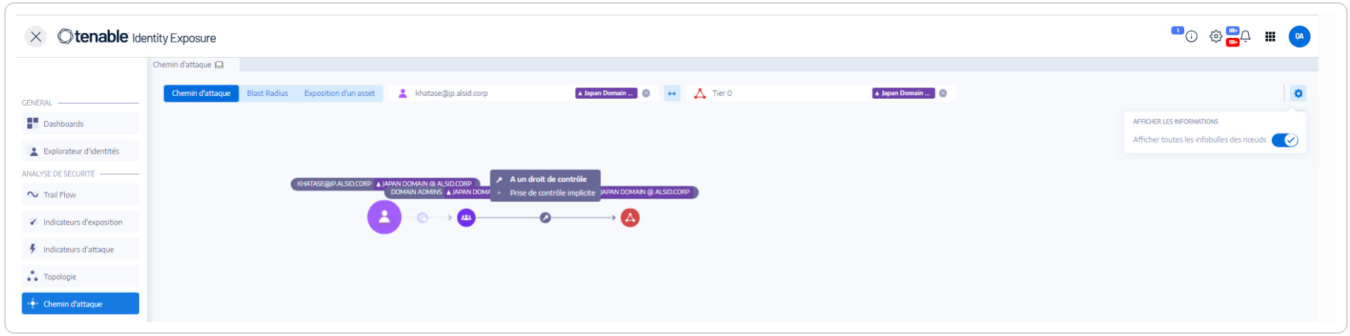
1. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

   Le volet **Chemin d'attaque** apparaît.



2. Dans la bannière, cliquez sur **Chemin d'attaque**.
3. Dans la zone **Point de départ**, saisissez l'asset au point d'entrée.
4. Dans la zone **Point d'arrivée**, saisissez l'asset à la fin du chemin.
5. Cliquez sur l'icône .

   Tenable Identity Exposure affiche le chemin d'attaque entre les deux assets.



6. Éventuellement, vous pouvez cliquer sur l'icône pour effectuer les actions suivantes :

- Cliquer sur le curseur **Zoom** pour ajuster le niveau de grossissement des graphiques.
- Cliquer sur le curseur **Afficher toutes les infobulles des nœuds** pour afficher des informations sur les assets.

Pour afficher le Blast Radius (rayon d'impact) :

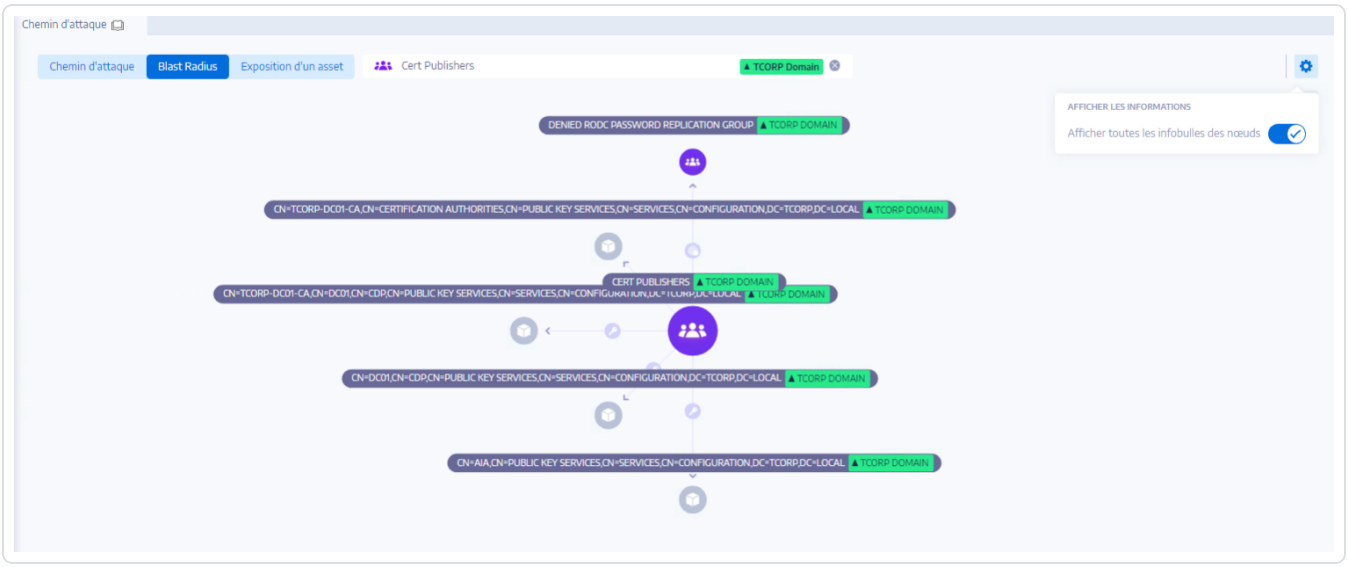
Tenable Identity Exposure affiche une représentation graphique du chemin d'attaque potentiel, mettant ainsi en évidence les connexions entre les assets. Chaque connexion représente une vulnérabilité ou une mauvaise configuration potentielle que l'attaquant pourrait exploiter pour se déplacer latéralement au sein de votre infrastructure AD. Vous pouvez zoomer et dézoomer pour mieux comprendre les détails du chemin.

1. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

   Le volet **Chemin d'attaque** apparaît.

2. Dans la bannière, cliquez sur **Blast Radius**.
3. Dans la zone **Rechercher un objet**, saisissez le nom d'un asset.
4. Cliquez sur l'icône .

   Tenable Identity Exposure affiche les connexions latérales qui partent de l'asset :



5. Cliquez sur les icônes des flèches qui relient les assets pour afficher leurs relations.

Pour afficher l'exposition d'un asset :

Chaque étape du chemin d'attaque est associée à un score de risque indiquant la sévérité de la vulnérabilité. Cela vous aide à traiter en priorité les chemins qui constituent la menace la plus importante et requièrent une attention immédiate. Vous pouvez également cliquer sur des points de connexion individuels pour obtenir plus de détails sur la vulnérabilité ou la mauvaise configuration impliquée.

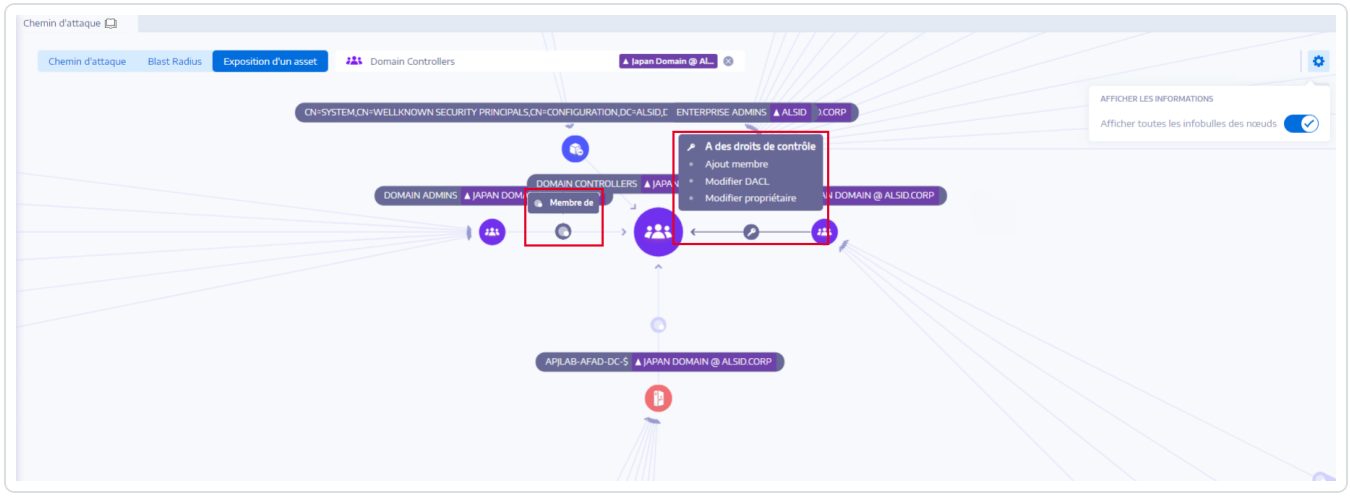
1. Dans Tenable Identity Exposure, cliquez sur **Chemin d'attaque** dans le menu de la barre latérale.

   Le volet **Chemin d'attaque** apparaît.

2. Dans la bannière, cliquez sur **Exposition de l'asset**.
3. Dans la zone **Rechercher un objet**, saisissez le nom d'un asset.
4. Cliquez sur l'icône .

   Tenable Identity Exposure affiche les chemins vers l'asset et les relations entre les assets.

5. Cliquez sur les icônes des flèches qui relient les assets pour afficher leurs relations.



Pour épingler un chemin d'attaque :

Voir aussi

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

Gestion des utilisateurs

Aspects clés

- **Rôles** : les rôles par défaut sont Administrateur, Analyste sécurité, Utilisateur et Invité, chacun disposant d'autorisations différentes. Les rôles personnalisés permettent d'exercer un contrôle granulaire pour répondre à des besoins spécifiques.
- **Autorisations** : les autorisations permettent de définir ce à quoi les utilisateurs peuvent accéder et ce qu'ils peuvent faire dans Tenable Identity Exposure. Cela va de la visualisation des rapports et des dashboards à la gestion des utilisateurs, en passant par la configuration des indicateurs et par des opérations telles que la désactivation de comptes.
- **Établissement de la portée** : Tenable Identity Exposure permet d'étendre les autorisations à des domaines, des groupes spécifiques ou même des objets individuels au sein d'Active Directory. Les utilisateurs n'ont ainsi accès qu'à des données pertinentes en fonction de leur rôle et de leurs responsabilités.

Avantages

- **Renforcement de la sécurité de l'infrastructure Active Directory** : un contrôle d'accès granulaire minimise le risque d'accès non autorisé à des données sensibles sur l'identité.
- **Amélioration de l'efficacité et des workflows** : les utilisateurs ont accès aux outils et aux données dont ils ont besoin, ce qui simplifie les investigations et la réponse aux incidents.
- **Respect de la conformité** : le contrôle d'accès basé sur le rôle permet de répondre aux exigences de conformité qui encadrent la gestion des identités et des accès au sein d'Active Directory.

Voir aussi

- User Roles

Intégration de Tenable Identity Exposure

Intégrez Tenable Identity Exposure à votre solution SIEM, SOC ou SOAR pour profiter d'une surveillance en temps réel, d'une réponse automatisée et d'une gestion améliorée des alertes.

Surveillance en temps réel avec intégration Syslog

Bénéficiez d'alertes instantanées pour les indicateurs d'exposition (IoE) critiques grâce à l'intégration Syslog transparente.

Principaux avantages

- **Journalisation centralisée** : agrégez les événements Tenable Identity Exposure avec d'autres solutions de sécurité pour une analyse complète.
- **Notifications en temps réel** : recevez des notifications immédiates concernant les expositions et attaques potentielles liées à l'identité.
- **Gestion améliorée de la sécurité** : établissez des corrélations entre les événements de différentes sources pour identifier plus rapidement les menaces complexes.
- **Amélioration de la visibilité du SIEM** : intégrez les données Tenable Identity Exposure en toute transparence dans votre SIEM afin de renforcer la connaissance de la situation et l'analyse des corrélations.
- **Workflow rationalisé** : automatisez le tri et le traitement des alertes en fonction des données Syslog afin d'optimiser les opérations de sécurité.

Exemples d'IoE pour la surveillance en temps réel

- **Paramétrages dangereux sur des serveurs ADCS** : détecte/identifie les modifications apportées aux serveurs de certificats AD lesquelles peuvent annoncer des attaques « Certified Pre-owned ».
- **Intégrité des stratégies de groupe** : détecte/identifie les tentatives d'installation de portes dérobées par le biais de l'exécution de script au sein des stratégies de groupe.
- **Utilisateurs autorisés à joindre des ordinateurs au domaine** : reconnaît les ajouts non

autorisés d'ordinateurs de domaine, une pré-attaque caractéristique des attaques par porte dérobée dans le « RBCD ».

Automatiser la réponse avec les plateformes SOAR

Tirez parti des plateformes d'orchestration, d'automatisation et de réponse de sécurité (SOAR) existantes pour exécuter des actions de remédiation automatisées basées sur les données TIE. Les principaux avantages :

- **Atténuation rapide** : minimisez les temps d'arrêt et leur impact en automatisant les réponses aux IoE critiques.
- **Efficacité améliorée** : libérez les équipes de sécurité des tâches répétitives pour leur permettre de se concentrer sur des initiatives de sécurité stratégiques.
- **Mesures de sécurité renforcées** : corrigez de manière proactive les mauvaises configurations détectées et renforcez votre niveau de sécurité global.

Important : la résolution des problèmes affectant les scripts d'automatisation ne fait pas partie des attributions de l'assistance Tenable. Veuillez contacter notre équipe de service professionnel pour obtenir de l'aide.