Leitfaden zu den wichtigsten Funktionen von Tenable Identity Exposure

Letzte Überarbeitung: 2. Juli 2025

Inhalt

Willkommen beim Leitfaden zu den wichtigsten Funktionen von Tenable Identity Exposure

Willkommen bei Tenable Identity Exposure, früher bekannt als Tenable AD. Dieses Dokument soll Ihre Arbeit erleichtern, indem es einen umfassenden Überblick über die Merkmale und Funktionen des Produkts bietet, unabhängig davon, ob es On-Premises oder über SAAS bereitgestellt wird. Diese Ressource soll Sie unterstützen, unabhängig davon, ob Sie ein Neuling sind, der nach Anleitung sucht, oder ein erfahrener Benutzer, der sein Verständnis vertiefen möchte.

In diesem Dokument finden Sie verschiedene Abschnitte, die eine Reihe von Themen behandeln, darunter die Optimierung der Produktnutzung und die Verwaltung von Indicators of Attack und Indicators of Exposure. Es ist wichtig zu beachten, dass dieses Dokument zwar wertvolle Erkenntnisse liefert, aber nicht als starres Regelwerk für die Verwendung von Tenable Identity Exposure gedacht ist. Stattdessen bietet es Empfehlungen für eine nahtlose und effektive Nutzung der Plattform.

Über diesen Leitfaden

Dieser Leitfaden basiert auf dem **Tenable Identity Exposure SaaS-Benutzerhandbuch**, in dem Sie umfassende Informationen finden.

Die in diesem Leitfaden gezeigten Beispiele sollen die Möglichkeiten von Tenable Identity Exposure hervorheben; sie stellen keine vollständige Liste dar und können nicht direkt auf jede Umgebung übertragen werden. Für optimale Sicherheitsvorkehrungen empfehlen wir Ihnen, unsere offizielle Dokumentation oder unsere Professional Services für weitere Details und Anleitungen zu konsultieren.

Wichtige Stakeholder

Die einzelnen Stakeholder in Tenable Identity Exposure unterscheiden sich je nach Größe, Struktur, Sicherheitsrichtlinien und den geplanten Anwendungsfällen Ihres Unternehmens. Durch die Festlegung präziser Rollen und Zuständigkeiten für jeden Stakeholder wird die effiziente Einführung und Nutzung des Produkts ermöglicht.

Bei der Arbeit mit Tenable Identity Exposure ist es wichtig, die verschiedenen beteiligten Interessengruppen (Stakeholder) zu verstehen. Diese Einzelpersonen und Gruppen übernehmen

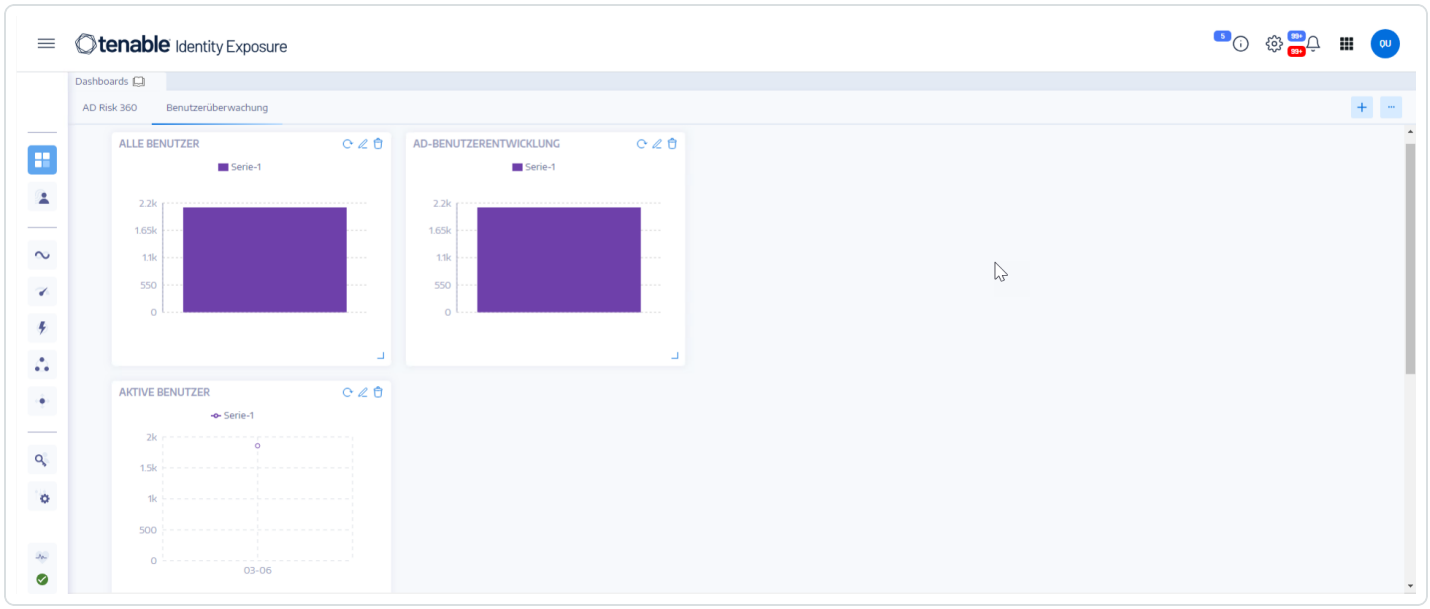
unterschiedliche Rollen bei der Identifizierung, Risikominderung und Meldung von identitätsbasierten Sicherheitsrisiken. Hier finden Sie eine umfassende Aufschlüsselung:

- **Sicherheitsteam**: Beaufsichtigt und verwaltet die Tenable-Lösung und nutzt Datenanalysen, um Schwachstellen und Risiken zu identifizieren und sofort darauf zu reagieren.
- **IT-Operations-Team**: Sorgt für den Infrastruktur- und Integrationssupport für die Tenable-Lösung und stellt eine nahtlose Konnektivität mit anderen Sicherheitstools und Benutzerverzeichnissen sicher.
- **Anwendungsentwicklungsteams**: Sind damit beauftragt, Anwendungen abzusichern und alle von Tenable gemeldeten gefährderten Identitäten umgehend zu beheben.
- **Identity and Access Management (IAM)-Team**: Verwaltet Benutzerkonten, Berechtigungen und Zugriffskontrollen und arbeitet eng mit Kollegen aus dem IT-Sicherheitsbereich zusammen, um Probleme zu beseitigen, die von Tenable Identity Exposure identifiziert wurden.
- **Geschäftsbereichsleiter**: Tragen die oberste Verantwortung für die Sicherheitslage ihrer Teams und Anwendungen. Sie überprüfen Berichte, priorisieren Risikominderungsstrategien und weisen Ressourcen zu, um die Sicherheitsmaßnahmen von Active Directory zu verbessern.

Dashboards

Mit Dashboards können Sie Daten und Trends visualisieren, die die Sicherheit Ihres Active Directory betreffen. Sie können sie mit Widgets anpassen, um Diagramme und Zähler nach Ihren Wünschen anzuzeigen.

Das Tenable Identity Exposure-Dashboard fungiert als Echtzeit-Befehlszentrale für die Active Directory (AD)-Sicherheit Ihres Unternehmens. Es bietet einen umfassenden Überblick (z. B. eine zentrale Echtzeitansicht) Ihrer Identitätsumgebung, indem sie kritische Schwachstellen hervorhebt, potenzielle Angriffsvektoren ausfindig macht und eine proaktive Risikominderung ermöglicht.



Wichtige Dashboard-Funktionen

- **Übersicht auf einen Blick**: Bietet Ihnen einen schnellen Überblick über Ihren Sicherheitsstatus. Dabei werden wichtige Kennzahlen wie Konformitätsbewertung, Hauptrisiken und Trends der Benutzeraktivität gut sichtbar angezeigt.
- **Aufschlüsseln von Details**: Mit interaktiven Widgets, die Risikofaktoren nach Schweregrad, Benutzerkategorie und anderen relevanten Kriterien aufschlüsseln, können Sie bestimmte Bereiche genauer untersuchen.
- **Anpassbarer Fokus**: Erstellen Sie personalisierte Dashboards, die auf Ihre Prioritäten zugeschnitten sind, indem Sie vorgefertigte Vorlagen verwenden oder Ihre eigenen Layouts

erstellen. So erstellen Sie beispielsweise ein Dashboard für eine weit verbreitete Fehlkonfiguration bei häufigen wiederkehrenden IoEs:

  - SDProp-Konsistenz sicherstellen
  - Domänencontroller werden von nicht legitimen Benutzern verwaltet
  - Gefährliche Kerberos-Delegierung

- **Echtzeitüberwachung**: Mit kontinuierlichen Updates und Warnungen bleiben Sie über aufkommende Bedrohungen und verdächtige Aktivitäten informiert.
- **Umsetzbare Einblicke**: Erhalten Sie praktische Empfehlungen für Behebungsmaßnahmen, priorisiert nach Schweregrad und potenziellen Auswirkungen.

Siehe auch

- Dashboards
- Videotutorial zu Dashboards

Trail Flow

Im Trail Flow in Tenable Identity Exposure wird die Echtzeitüberwachung und Analyse der Ereignisse angezeigt, die Ihre AD-Infrastruktur betreffen. Sie können damit kritische Schwachstellen und die empfohlenen Behebungsmaßnahmen identifizieren.

Auf der Seite **Trail Flow** können Sie in der Zeit zurückgehen und frühere Ereignisse laden oder nach bestimmten Ereignissen suchen. Sie können auch das Suchfeld oben auf der Seite verwenden, um nach Bedrohungen zu suchen und bösartige Muster zu erkennen.

Der Trail Flow verfolgt die folgenden Ereignisse:

- **Benutzer- und Gruppenänderungen**: Umfasst die Erstellung, Löschung und Änderung von Konten und Gruppen.
- **Berechtigungsänderungen**: Umfasst Änderungen an der Zugriffssteuerung für Objekte wie Dateien, Ordner und Drucker.
- **Anpassungen der Systemkonfiguration**: Umfasst Änderungen an Gruppenrichtlinienobjekten (GPOs) und anderen kritischen Einstellungen.
- **Verdächtige Aktivitäten**: Umfasst nicht autorisierte Versuche, Rechteausweitungen und andere Ereignisse, die Warnhinweise auslösen.

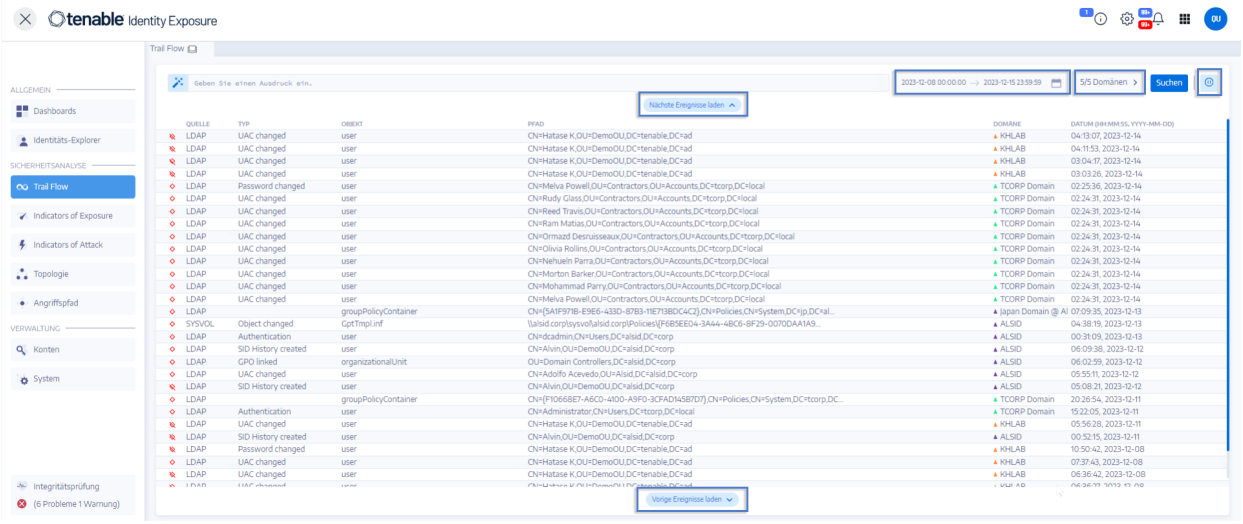
Tenable Identity Exposure bietet die folgenden Funktionen zur Nutzung der Trail Flow-Daten:

- **Durchsuchbar und filterbar**: Benutzer können mithilfe von Schlüsselwörtern oder bestimmten Kriterien mühelos durch den Ereignisstrom navigieren. So können sie ihre Aufmerksamkeit auf relevante Aktivitäten konzentrieren und gleichzeitig irrelevante Informationen Iminimieren.
- **Detaillierte Ereignisinformationen**: Jeder Ereigniseintrag liefert umfassende Details, darunter das betroffene Objekt, den für die Änderung verantwortlichen Benutzer, das verwendete Protokoll und die zugehörigen Indicators of Exposure (IoEs).
- **Visualisierte Beziehungen**: Das Tool bietet die Möglichkeit, die Beziehungen zwischen Ereignissen zu veranschaulichen und so aufzuzeigen, dass auch scheinbar nicht im Zusammenhang stehende Aktivitäten ggf. zu einer umfassenderen Angriffskampagne beitragen.

So greifen Sie auf den Trail Flow zu:

- Klicken Sie in Tenable Identity Exposure in der Navigationsleiste auf der linken Seite auf **Trail Flow**.

  Die Trail Flow-Seite wird mit einer Liste von Ereignissen geöffnet. Weitere Informationen finden Sie unter Trail Flow Table.



So wählen Sie einen Zeitrahmen aus:

So wählen Sie eine Domäne aus:

So zeigen Sie ein Ereignis an:

So halten Sie den Trail Flow an und starten ihn neu:

So laden Sie die nächsten oder vorherigen Ereignisse:

Wie werden die Daten im Trail Flow angezeigt?

1. Wenn Sie eine Aktion in Ihrer Active Directory (AD)-Oberfläche durchführen, wie z. B.:
   - Neues Benutzerkonto erstellen
   - Gruppenmitgliedschaft eines Benutzers ändern

- Passwort zurücksetzen
- Konto deaktivieren
- Konto aktivieren
- Konto löschen
- Objekt verschieben
- Berechtigungen ändern

2. Active Directory (AD) generiert automatisch einen Ereignisprotokolleintrag, der Details des Vorgangs erfasst, einschließlich:
    - Zeitstempel
    - Administrator, der die Aktion durchführt
    - Betroffene(s) Objekt(e)
    - Spezifische Änderungen
3. Tenable Identity Exposure erfasst und analysiert diese Ereignisprotokolle kontinuierlich und korreliert Ereignisse, identifiziert Muster und erkennt Anomalien.
4. Auf der Seite „Trail Flow" werden der Ablauf und die Auswirkungen des Vorgangs visualisiert:
    - Zeitleiste: Zeigt eine chronologische Abfolge von Ereignissen an und hebt den letzten Vorgang hervor.
    - Objektdetails: Bietet spezifische Informationen über die betroffenen Objekte, einschließlich ihrer Attribute und Beziehungen.
    - Änderungsverlauf: Zeigt einen Verlauf der Änderungen, die an den Objekten vorgenommen wurden, einschließlich des aktuellen Vorgangs.
    - Risk Insights: Identifiziert potenzielle Risiken im Zusammenhang mit dem Vorgang, wie z. B. übermäßige Berechtigungen oder Mitgliedschaft in sensiblen Gruppen.
    - Compliance-Informationen: Gibt alle Compliance-Verstöße im Zusammenhang mit dem Vorgang an.

Siehe auch

- Trail Flow-Übersicht
- Trail Flow Use Cases
- Trail Flow-Videotutorial

Reporting Center

Das **Reporting Center** in Tenable Identity Exposure bietet eine sehr nützliche Funktion, mit der Sie wichtige Daten als Berichte exportieren und an wichtige Stakeholder innerhalb einer Organisation weitergeben können. Das Reporting Center bietet die Möglichkeit, Berichte aus einer vordefinierten Liste zu erstellen und so einen effizienten und optimierten Prozess zu gewährleisten.

Es bietet folgende Funktionen:

- **Granulare Filterung**: Verfeinern Sie Berichte mit granularen Filtern basierend auf Datumsbereich, Domäne, Indicator of Attack (IoA), Indicator of Exposure (IoE) und weiteren Aspekten, um punktgenaue Einblicke zu erhalten.
- **Automatisierte Zustellung**: Planen Sie die automatische Generierung und Zustellung von Berichten in gewünschten Intervallen und optimieren Sie so die Sicherheitsüberwachung und Berichterstellung.
- **Flexibler Export**: Exportieren Sie Berichte in verschiedenen Formaten wie CSV, um sie weiter zu analysieren, mithilfe des Berichtszugriffsschlüssels zu teilen oder in vorhandene Reporting-Workflows zu integrieren.

Administratoren können verschiedene Arten von Berichten für verschiedene Benutzer mit einem flexiblen Berichtszeitraum von bis zu einem Quartal erstellen. Die Möglichkeit, kritische Identitätsdaten aus Tenable Identity Exposure gemeinsam zu nutzen, ermöglicht es dem Unternehmen, Risiken proaktiv zu mindern und potenzielle identitätsbasierte Angriffe zu identifizieren.

Um einen Bericht herunterzuladen, erhalten Benutzer eine E-Mail mit einer URL zu einer Seite, auf der sie einen Berichtszugriffsschlüssel eingeben, den sie von ihrem Administrator erhalten haben. Berichte stehen 30 Tage lang zum Herunterladen zur Verfügung. Danach sind sie veraltet und werden von Tenable Identity Exposure gelöscht. Benutzer müssen die Berichte herunterladen, bevor Tenable Identity Exposure einen neuen Bericht für den angegebenen Zeitrahmen generiert und den vorherigen überschreibt.

So greifen Sie auf das Reporting Center zu:

1. Wählen Sie in Tenable Identity Exposure **Systeme** > **Konfiguration**.
2. Klicken Sie unter **Berichterstellung** auf **Reporting Center**.

Es wird ein Fensterbereich mit einer Liste der konfigurierten Berichte und der zugehörigen Informationen geöffnet, wie z. B. Berichtsname, Berichtstyp, Domäne, Profil, Zeitraum, Wiederholung und E-Mail-Adressen der Empfänger.

Siehe auch

- Reporting Center
- Set Permissions for a Role

Indicators of Exposure

Tenable Identity Exposure misst den Sicherheitsreifegrad Ihrer AD-Infrastrukturen anhand von Indicators of Exposure (IoEs) und weist dem Strom von Ereignissen, der überwacht und analysiert wird, Schweregradestufen zu. Tenable Identity Exposure löst Warnungen aus, wenn es Sicherheitsmängel feststellt.

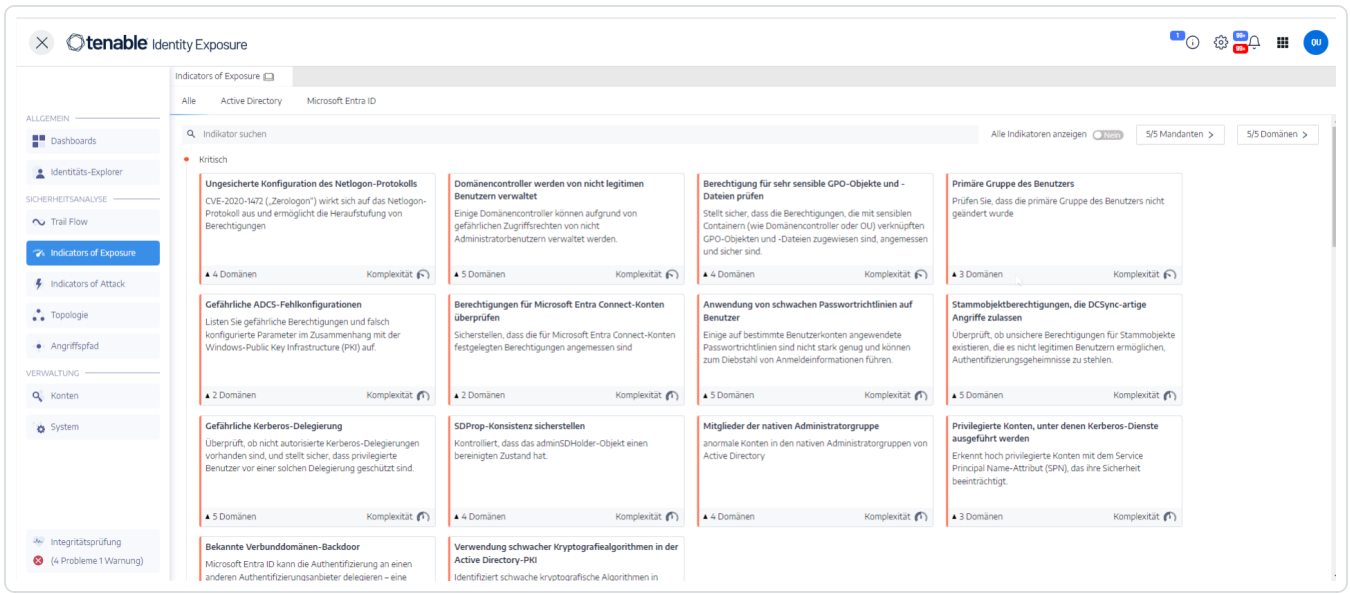
Diese IoEs sind vorkonfiguriert, und Abweichungen von den festgelegten Normen lösen entsprechende Warnungen aus.

So zeigen Sie IoEs an:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Exposure**.

   Der Fensterbereich **Indicators of Exposure** wird geöffnet. Standardmäßig zeigt Tenable Identity Exposure nur die IoEs an, die Abweichungen enthalten.

2. (Optional) Wenn Sie alle IoEs anzeigen möchten, stellen Sie den Schalter **Alle Indikatoren anzeigen** auf **Ja**.



Tenable Identity Exposure IoEs verfügen über eine Reihe von Funktionen, die Ihre Untersuchungsmöglichkeiten verbessern:

- **Durchsuchbar und filterbar**: Wenden Sie Filter auf Grundlage von Gesamtstruktur und Domäne an, um den IoE mühelos zu erkunden.
- **Exportfunktion**: Das Abweichungsobjekt ermöglicht es Ihnen, die IoEs im CSV-Format zu exportieren.
- **Maßnahme bei IoE-Vorfällen**: Entfernen Sie eine Exposition von der Zulassungsliste oder aktivieren Sie diese erneut.

Zu den Daten aus IoEs gehören:

- **Informationsabschnitt**: Dieser Abschnitt bietet eine Kurzzusammenfassung zu jedem Indicator of Exposure (IoE), einschließlich bekannter Angriffstools, betroffener Domänen und relevanter Dokumentation.
- **Details zum Sicherheitsrisiko**: Dieser Abschnitt enthält ausführlichere Informationen über die Fehlkonfiguration in Active Directory.
- **Abweichende Objekte**: In diesem Abschnitt werden Fehlkonfigurationen in Active Directory hervorgehoben, die die Angriffsoberflächen vergrößern können.
- **Empfehlung**: Dieser Abschnitt führt Sie durch effektive Konfigurationsstrategien, um Ihre Angriffsoberfläche zu minimieren.

Schweregrad

Anhand der Schweregrade können Sie den Schweregrad der entdeckten Schwachstellen beurteilen beurteilen und Prioritäten für Behebungsmaßnahmen setzen.

Im Fensterbereich **Indicators of Exposure** werden die IoEs wie folgt angezeigt:

- Nach Schweregrad unter Verwendung von Farbcodes.
- Vertikal: vom höchsten Schweregrad bis zum niedrigsten (rot für höchste Priorität und blau für niedrigste Priorität).
- Horizontal: vom komplexesten zum am wenigsten komplexen. Tenable Identity Exposure berechnet den Komplexitätsindikator dynamisch, um den Schwierigkeitsgrad der Behebung des abweichenden IoE anzuzeigen.

Schweregrad	Beschreibung

Kritisch – Rot	Zeigt, wie man Angriffe und Kompromittierungen des Active Directory durch bestimmte unprivilegierte Benutzer verhindern kann.
Hoch – Orange	Befasst sich entweder mit Techniken nach der Ausnutzung, die zum Diebstahl von Anmeldeinformationen oder zur Umgehung der Sicherheit führen, oder mit Ausnutzungstechniken, die eine Verkettung erfordern, um gefährlich zu sein.
Mittel – Gelb	Gibt ein begrenztes Risiko für die Active Directory-Infrastruktur an.
Gering – Blau	Zeigt gute Sicherheitspraktiken. In bestimmten geschäftlichen Zusammenhängen können Abweichungen mit geringen Auswirkungen zulässig sein, die die AD-Sicherheit nicht unbedingt beeinträchtigen. Diese Abweichungen wirken sich nur dann auf das AD aus, wenn ein Administrator einen Fehler macht, indem er beispielsweise ein inaktives Konto aktiviert.

Priorisierung der Behebung

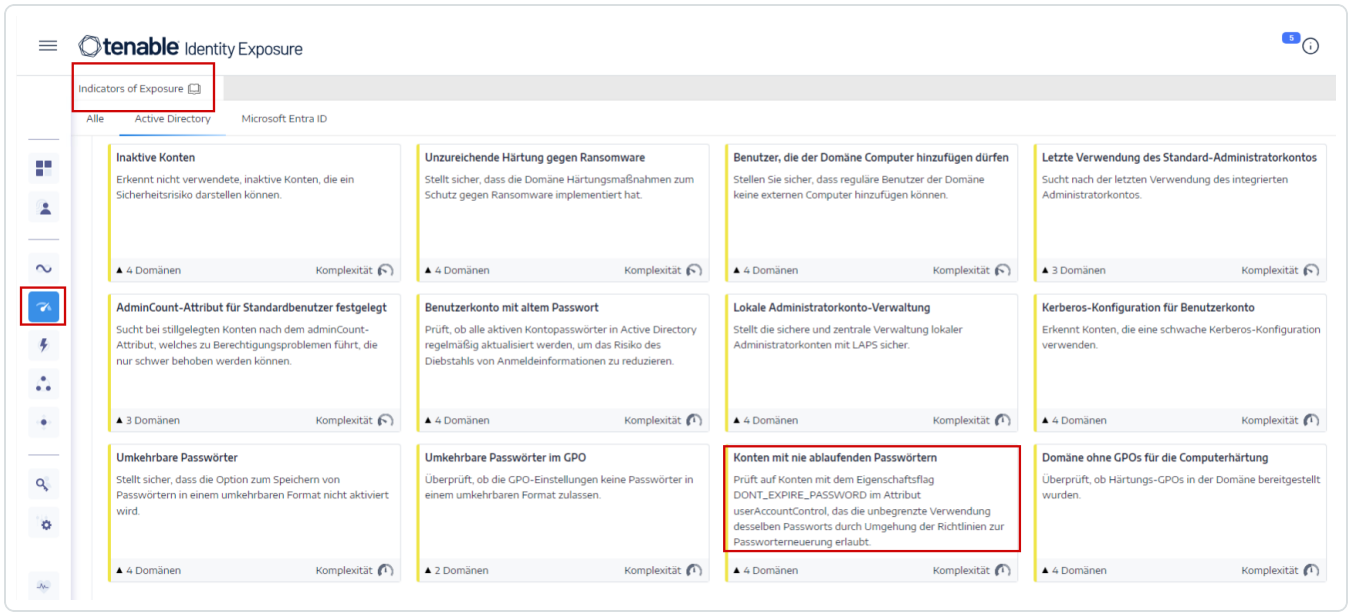
Sie priorisieren Behebungsmaßnahmen für IoEs mit hohem Schweregrad, die vom System identifiziert wurden. Darüber hinaus können Sie innerhalb der Kategorie „Kritisch“ eine weitere Priorisierung vornehmen, indem Sie die Risikoanzeige im IoE verwenden.

Wenn Sie der Meinung sind, dass der IoE in den Zuständigkeitsbereich oder den operativen Auftrag Ihrer Organisation fällt, können Sie ihn auf die Zulassungsliste setzen.

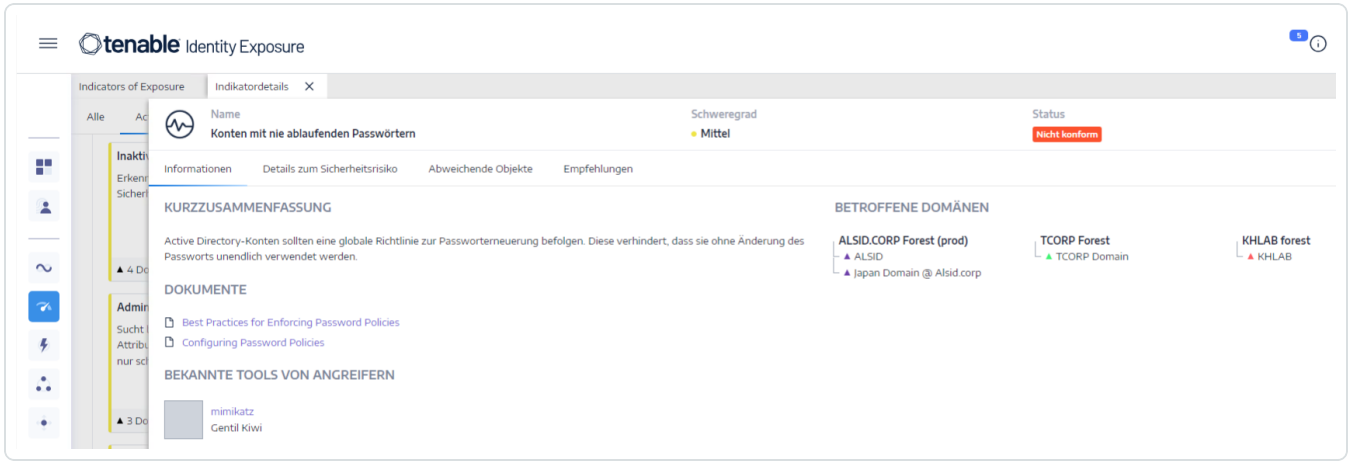
Anwendungsfall

Der folgende Anwendungsfall konzentriert sich auf den IoE „Konten mit nie ablaufenden Passwörtern“.

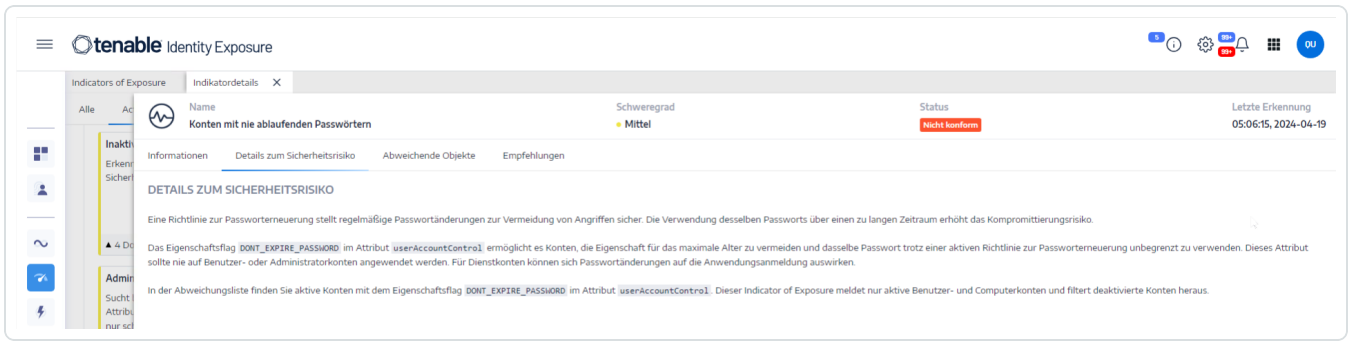
1. Wenn Tenable Identity Exposure einen IoE meldet, wird er im Fensterbereich „Indicators of Exposure“ angezeigt:



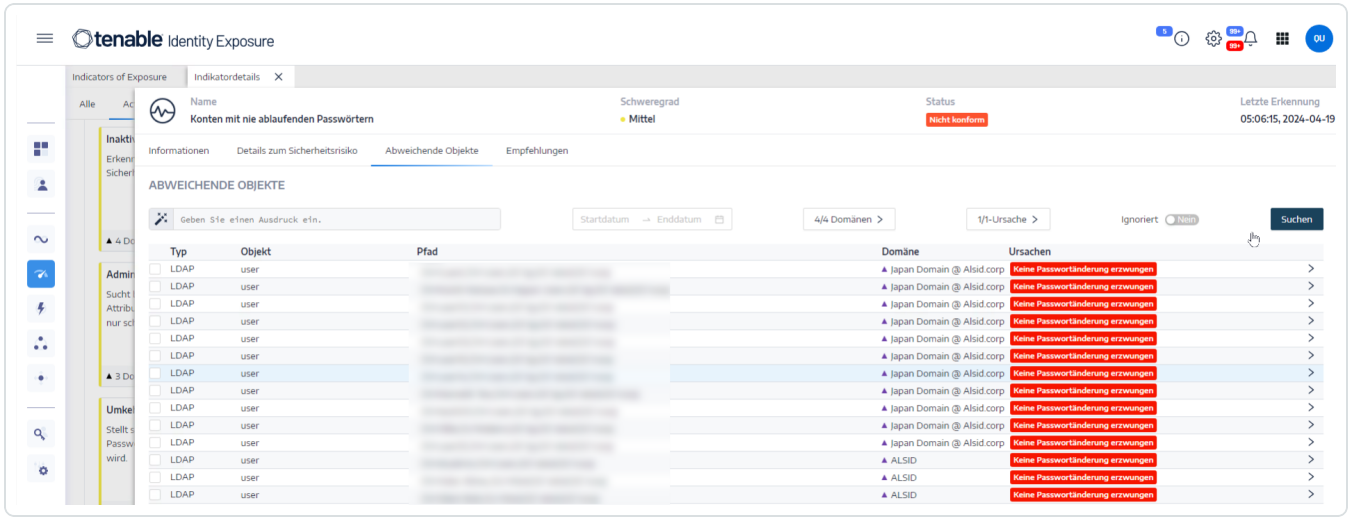
2. Wenn Sie weitere Informationen zum IoE erhalten möchten, klicken Sie auf den IoE, um weitere Details anzuzeigen. Auf der Informationsseite finden Sie eine Zusammenfassung, die einen kurzen Überblick, Details zu potenziellen Angriffstools im Zusammenhang mit dem IoE, die betroffenen Domänen sowie relevante Dokumentation enthält, damit Sie das Problem verstehen und effektiv beheben können.

3. 

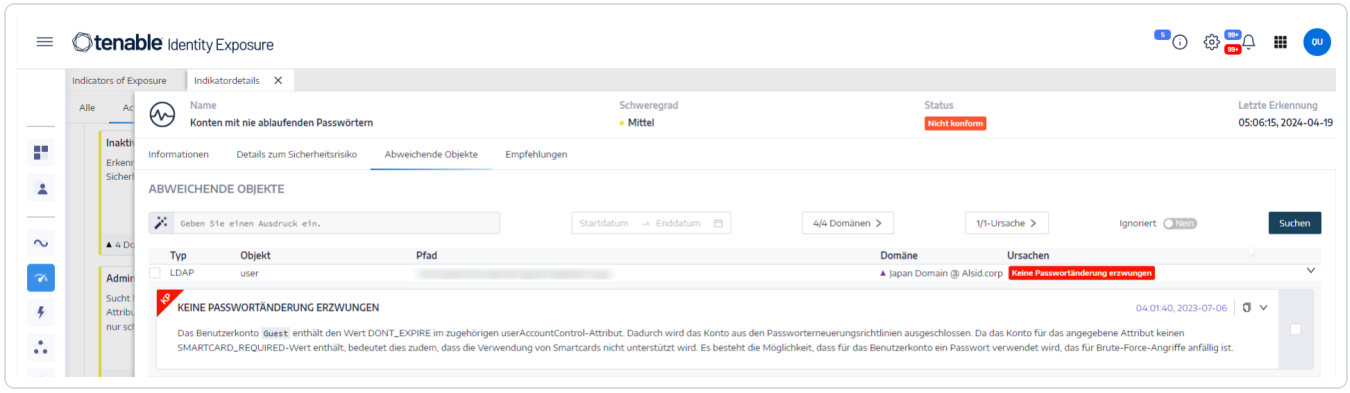
4. Weitere Informationen zum IoE erhalten Sie über die Registerkarte „Details zum Sicherheitsrisiko“.



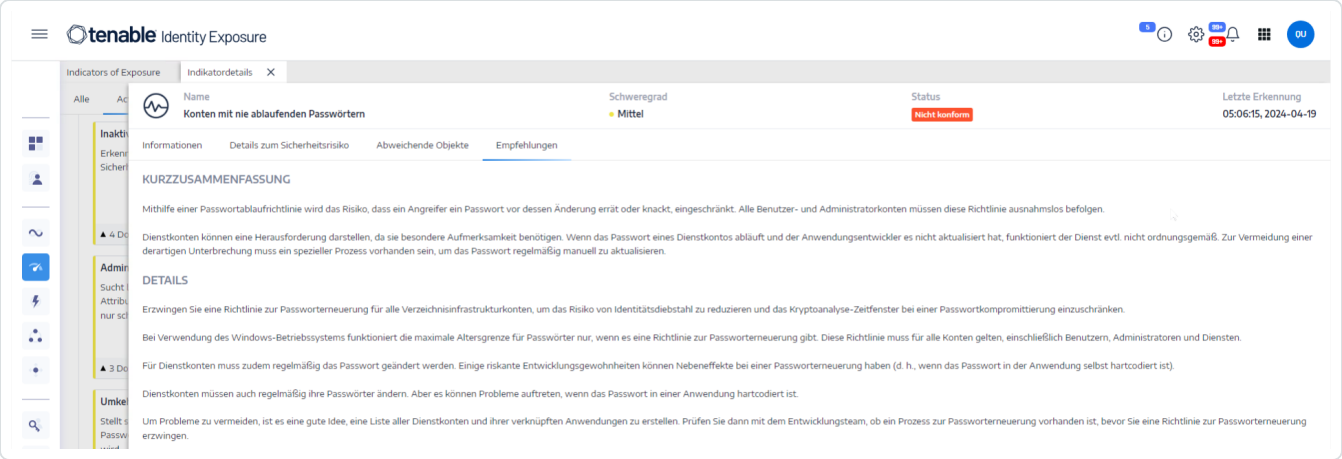
5. Um zu überprüfen, für welche Konten die Einstellung „Konto mit nie ablaufenden Passwörtern“ aktiviert ist, klicken Sie auf die Option „Abweichende Objekte“. Mit dieser Aktion können Sie auf eine Liste von Konten zugreifen, die in Ihrem System über diese Konfiguration verfügen.



6. Klicken Sie auf das abweichende Objekt, um die Konten anzuzeigen, die vom IoE gekennzeichnet wurden.



7. Wenden Sie sich an Ihren Active Directory-Administrator, um zu verstehen, warum für das betroffene Konto die Option „Konten mit nie ablaufenden Passwörtern“ aktiviert ist.
8. Auf der Grundlage der Antwort können Sie entweder das Konto auf die Zulassungsliste setzen oder Ihren Active Directory-Administrator dabei unterstützen, Empfehlungen zur Behebung des Problems zu geben.
9. Empfehlungen finden Sie im Abschnitt „Empfehlungen“ des IoE.



10. Wenn das Konto eine Ausnahme aufweist oder bekanntermaßen erwartungsgemäß funktioniert, können Sie den IoE ignorieren, indem Sie zu **Abweichungsobjekt** > Entsprechende Abweichung auswählen > Ausgewähltes Objekt **ignorieren** (oder) das ausgewählte Objekt nicht mehr ignorieren (je nach Anforderung).

Siehe auch

- Indicators of Exposure
- Videotutorial zu Indicators of Exposure
- Customize an Indicator

Indicators of Attack

Tenable Identity Exposure Die Indicators of Attack (IoA) helfen Ihrer Organisation, Angriffe mit den neuesten Exploit-Techniken auf Ihre Active Directory-Infrastrukturen zu erkennen und umgehend Maßnahmen zu ergreifen. Dazu gehören:

- **Top 3-Vorfälle**: Eine einheitliche Darstellung von IoAs zeigt eine Echtzeitzeitleiste zusammen mit den Top drei Vorfällen, von denen Ihr AD betroffen war, sowie der Verteilung der Angriffe – alles innerhalb einer einzigen Oberfläche.
- **Details zu IoA**: Innerhalb von Tenable Identity Exposure bietet der IoA-Bereich Informationen zu Angriffen, die in Ihrem AD stattgefunden haben.
- **Vorfälle mit IoA**: Die Liste der IoA-Vorfälle bietet umfassende Details zu bestimmten Angriffen auf Ihr AD. Diese Informationen ermöglichen es Ihnen, basierend auf dem Schweregrad des IoA angemessen zu reagieren.

Die Funktion „Indicators of Attack“ verfügt über eine Reihe von Merkmalen, die Ihre Untersuchungsmöglichkeiten verbessern:

- **Durchsuchbar und filterbar**: Sie können den IoA mühelos über die Zeitleiste untersuchen oder Filter auf der Grundlage von Gesamtstruktur, Domäne und Kritikalitätsstufe anwenden, um effiziente und gezielte Ergebnisse zu erzielen.
- **Exportfunktion**: Ermöglicht den Export von IoA-Daten in den Formaten PDF, CSV oder PPTX.
- **Diagrammtyp ändern:** Bietet die Möglichkeit, den Diagrammtyp zu ändern, so dass Sie entweder die Verteilung des Schweregrads der Angriffe oder die Top-3-Angriffe und deren jeweilige Anzahl an Vorkommnissen anzeigen können.
- **Aktion bei IoA-Vorfällen**: Ermöglicht es Ihnen, einen Vorfall auszuwählen, den Sie schließen oder erneut öffnen möchten.

Schweregrad

Tenable Identity Exposure erkennt Angriffe und weist ihnen einen Schweregrad zu:

Schweregrad	Beschreibung
Kritisch – Rot	Es wurde ein nachweislicher Post-Exploitation-Angriff erkannt, für den

	Domänendominanz eine Voraussetzung ist.
Hoch – Orange	Es wurde ein größerer Angriff erkannt, über den ein Angreifer Domänendominanz erlangen kann.
Mittel – Gelb	Der IoA hängt mit einem Angriff zusammen, der zu einer gefährlichen Rechteausweitung führen oder den Zugriff auf sensible Ressourcen ermöglichen könnte.
Gering – Blau	Warnt vor verdächtigem Verhalten in Zusammenhang mit Auskundschaftung oder Vorfällen mit geringen Auswirkungen.

Priorisierung der Behebung

Erkennen Sie kritische IoAs mit großen Auswirkungen, die mit Ihren spezifischen Sicherheitsrisiken und -bedenken übereinstimmen.

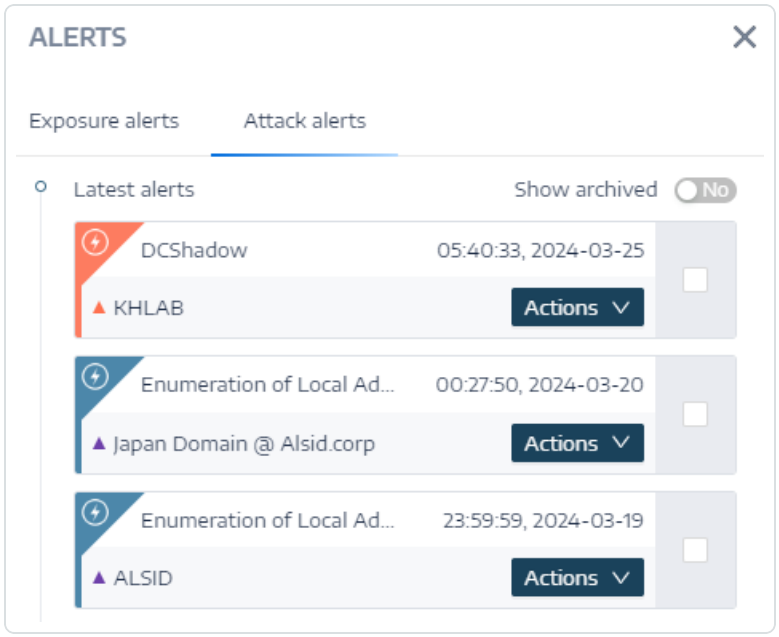
Um das Risiko von falsch positiven Meldungen oder das Übersehen legitimer Angriffe zu minimieren, ist es wichtig, die IoAs auf Ihre Umgebung abzustimmen. Dies beinhaltet:

- Anpassen von Schwellenwerten: Kalibrieren Sie die IoA-Empfindlichkeit, um falsch positive Ergebnisse zu reduzieren und sicherzustellen, dass Warnungen aussagekräftig und handlungsrelevant sind.
- Konten und Aktivitäten auf die Zulassungsliste setzen: Schließen Sie legitime Aktivitäten als Auslöser von IoAs aus, um die Warngenauigkeit zu erhöhen und Untersuchungen zu optimieren.
- Korrelieren von IoAs: Analysieren Sie die Beziehungen zwischen verschiedenen IoAs, um umfassendere Angriffsmuster zu erkennen.

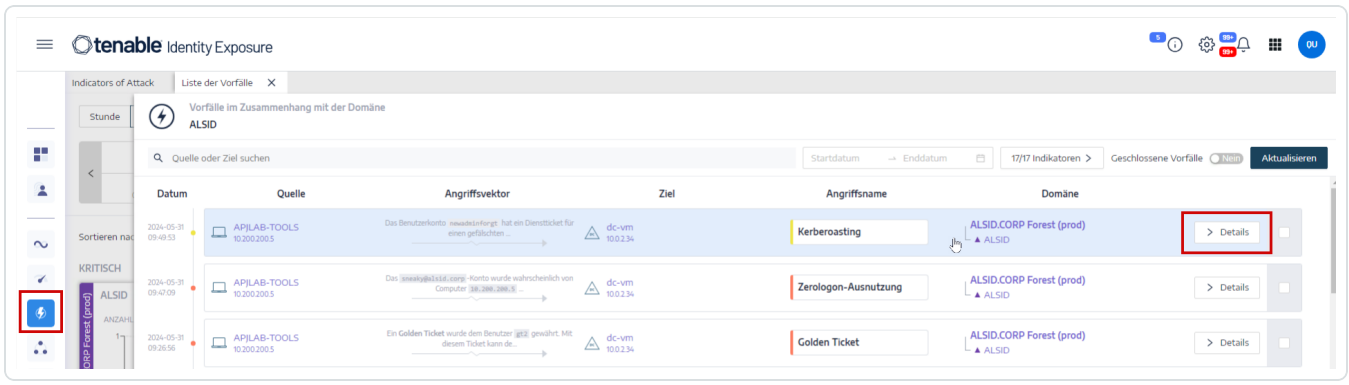
Tipp: Weitere Einzelheiten zu den Optionen und empfohlenen Werten finden Sie im Referenzhandbuch zu Tenable Identity Exposure Indicators of Attack (verfügbar unter https://de.tenable.com/downloads/identity-exposure). Wenden Sie diese Optionen und Werte auf jeden IoA im Sicherheitsprofil an.

Anwendungsfall

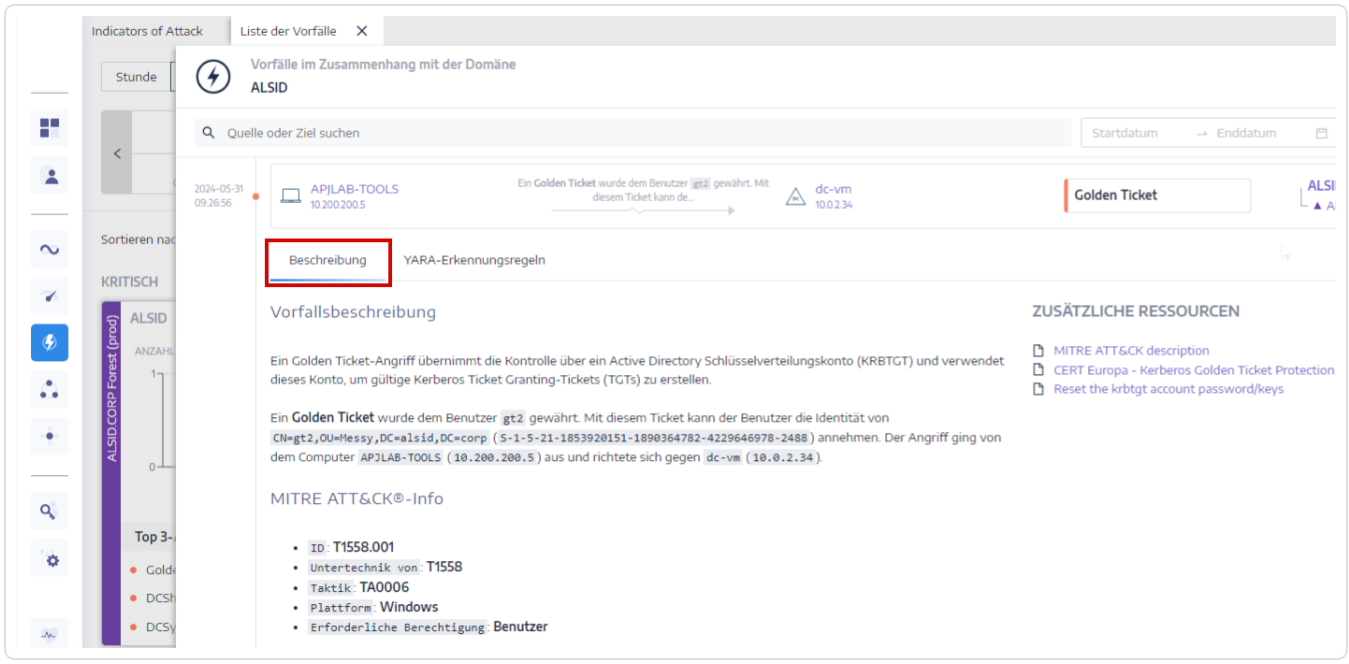
1. Wählen Sie nach der Aktivierung eines IoA im Navigationsbereich „Indicators of Attack“ aus, oder klicken Sie auf das Glockensymbol oben rechts auf der Startseite.



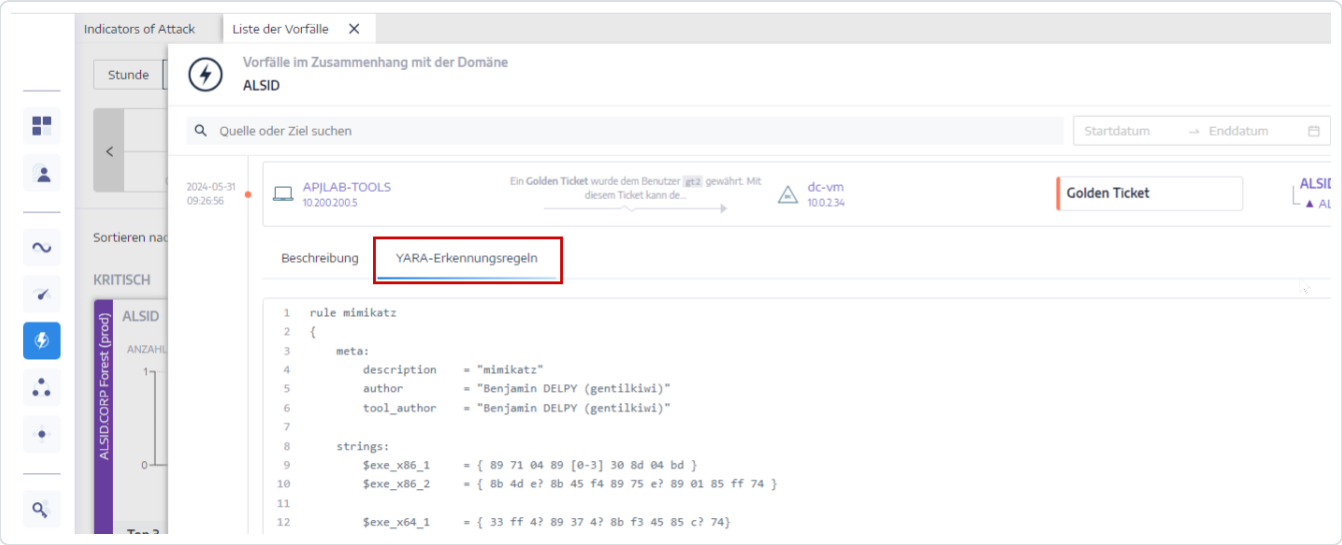
2. Jeder Indikator gibt Ihnen detaillierte Informationen über den Vorfall und ermöglicht es Ihnen, nach Überprüfung geeignete Maßnahmen zu ergreifen:
    - Wann der Angriff stattfand
    - Beschreibung des Angriffs
    - Quelle des Angriffs
    - Ziel des Angriffs
    - MITRE ATT&CK®-Informationen
    - YARA-Erkennungsregeln
    - Zusätzliche Ressourcen
3. Wählen Sie „Details“, um die Beschreibung aufzurufen, wie in diesem Beispiel dargestellt, das sich auf die Auflistung lokaler Administratoren konzentriert.



4. Die Registerkarte „Beschreibung“ enthält Informationen zu spezifischen Angriffen auf Ihr Active Directory (AD).



5. Die Registerkarte „YARA-Erkennungsregeln“ enthält Informationen über die YARA-Regeln, die Tenable Identity Exposure zur Erkennung von Active Directory-Angriffen auf Netzwerkebene verwendet. Dies verbessert die Erkennungsfunktionen von Tenable Identity Exposure insgesamt.



6. Arbeiten Sie mit dem Active Directory-Administrator oder dem zuständigen Stakeholder zusammen, um den Vorfall zu untersuchen und zu beheben. Entscheiden Sie, ob der Vorfall geschlossen oder erneut geöffnet werden soll, und implementieren Sie Maßnahmen, um ein erneutes Auftreten zu verhindern.
7. Wenn es sich um einen erkannten oder autorisierten Angriff handelt, haben Sie die Möglichkeit, den IoA entsprechend anzupassen, um zu verhindern, dass der IoA ihn in zukünftigen Instanzen kennzeichnet.

Siehe auch

- Indicators of Attack
- Customize an Indicator
- Videotutorial zu Indicators of Attack

Microsoft Entra ID-Unterstützung

Zusätzlich zu Active Directory unterstützt Tenable Identity Exposure auch Microsoft Entra ID (früher Azure AD oder AAD), um den Geltungsbereich von Identitäten in einer Organisation zu erweitern. Diese Funktion nutzt neue Indicators of Exposure, die sich auf Microsoft Entra ID-spezifische Risiken konzentrieren.

Um Microsoft Entra ID in Tenable Identity Exposure zu integrieren, befolgen Sie diesen Onboarding-Prozess:

1. Voraussetzungen erfüllen
2. Berechtigungen prüfen
3. Netzwerkflüsse prüfen
4. Microsoft Entra ID-Einstellungen konfigurieren
5. Microsoft Entra ID-Unterstützung aktivieren
6. Mandantenscans aktivieren

Voraussetzungen

Sie benötigen ein Tenable Cloud-Konto, um sich bei „cloud.tenable.com“ einzuloggen und die Supportfunktion von Microsoft Entra ID zu nutzen. Dieses Tenable Cloud-Konto ist dieselbe E-Mail-Adresse, die für Ihre Begrüßungs-E-Mail verwendet wird. Wenn Sie Ihre E-Mail-Adresse für „cloud.tenable.com“ nicht kennen, wenden Sie sich an den Support. Alle Kunden mit einer gültigen Lizenz (On-Premises oder SaaS) können unter „cloud.tenable.com“ auf die Tenable Cloud zugreifen. Mit dem Konto können Sie Tenable-Scans für Ihre Microsoft Entra ID konfigurieren und die Ergebnisse der Scans erfassen.

Hinweis: Sie benötigen keine gültige **Tenable Vulnerability Management**-Lizenz, um auf die Tenable Cloud zuzugreifen. Eine aktuell gültige eigenständige Tenable Identity Exposure-Lizenz (On-Premises oder SaaS) ist ausreichend.

Hinweis: Tenable Identity Exposure **unterstützt Microsoft Entra ID nicht in den National Clouds**, einschließlich der dedizierten Bereiche für China und die US-Regierung. Microsoft Entra ID bietet National Clouds an, bei denen es sich um physisch isolierte Azure-Instanzen handelt, die im Hinblick auf bestimmte behördliche und Compliance-Anforderungen entwickelt wurden. Tenable Identity Exposure unterstützt nur die globale Microsoft Entra ID-Umgebung, mit Ausnahme der China National Cloud und der National Cloud

der US-Regierung. Weitere Informationen zu National Clouds für Microsoft Entra ID finden Sie unter Microsoft Entra-Authentifizierung und National Clouds - Microsoft Identity Platform.

Berechtigungen

Die Unterstützung von Microsoft Entra ID erfordert die Erfassung von Daten von Microsoft Entra ID, wie beispielsweise Benutzern, Gruppen, Anwendungen, Dienstprinzipalen, Rollen, Berechtigungen, Richtlinien, Protokollen usw. Diese Daten werden mithilfe der Microsoft Graph-API und Dienstprinzipal-Anmeldeinformationen gemäß den Empfehlungen von Microsoft erfasst.

- Sie müssen sich bei Microsoft Entra ID **als Benutzer mit der Berechtigung zum Erteilen einer mandantenweiten Administratoreinwilligung** für Microsoft Graph einloggen, der laut Microsoft über die Rolle „Globaler Administrator“ oder „Privilegierter Rollenadministrator“ (oder eine beliebige benutzerdefinierte Rolle mit entsprechenden Berechtigungen) verfügen muss.
- Um auf die Konfiguration und Datenvisualisierung für Microsoft Entra ID zuzugreifen, muss Ihre **Tenable Identity Exposure-Benutzerrolle** über die entsprechenden Berechtigungen verfügen. Weitere Informationen finden Sie unter Set Permissions for a Role.

Netzwerkflüsse

Erlauben Sie den folgenden Adressen an Port 443 ausgehend vom Security Engine Node-Server, die Entra ID-Unterstützung zu aktivieren:

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

Anzahl der Lizenzen

Tenable rechnet doppelte Identitäten **nur dann nicht auf die Lizenz an, wenn die Tenable Cloud-Synchronisierung aktiviert ist**. Ohne diese Funktion können Konten aus Microsoft Entra ID und Active Directory nicht abgeglichen werden, sodass jedes Konto separat gezählt wird.

- **Ohne Tenable Cloud-Synchronisierung**: Ein einzelner Benutzer mit sowohl einem AD-Konto als auch einem Entra ID-Konto zählt im Hinblick auf die Lizenz als zwei separate Benutzer.

- **Bei aktivierter Tenable Cloud-Synchronisierung**: Das System fasst mehrere Konten zu einer einzigen Identität zusammen und stellt so sicher, dass ein Benutzer mit mehreren Konten nur einmal gezählt wird.

Microsoft Entra ID-Einstellungen konfigurieren

Verwenden Sie die folgenden Verfahren (übernommen aus dem Artikel Schnellstart: Registrieren einer Anwendung bei Microsoft Identity Platform der Microsoft-Dokumentation), um alle erforderlichen Einstellungen in Microsoft Entra ID zu konfigurieren.

1. **Erstellen Sie eine Anwendung:**

   a. Öffnen Sie im Azure-Administratorportal die Seite **App-Registrierungen**.

   b. Klicken Sie auf **+ Neue Registrierung**.

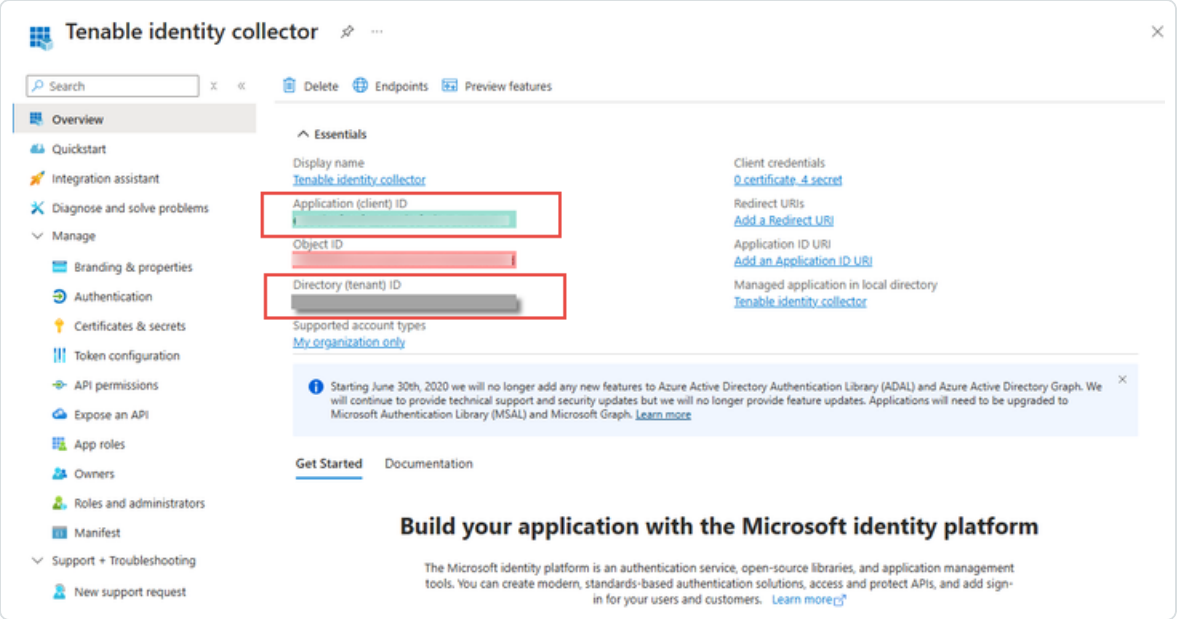
   c. Geben Sie der Anwendung einen Namen (Beispiel: „Tenable Identity Collector“). Für die anderen Optionen können Sie die Standardwerte unverändert lassen.

   d. Klicken Sie auf **Registrieren**.

   e. Notieren Sie sich auf der Übersichtsseite dieser neu erstellten App die „Anwendungs-ID (Client)“ und die „Verzeichnis-ID (Mandant)“, die Sie später in Schritt So fügen Sie einen neuen Microsoft Entra ID-Mandanten hinzu: benötigen.

   > **Achtung**: Achten Sie darauf, dass Sie die **Anwendungs-ID** und **nicht** die **Objekt-ID**

auswählen, damit die Konfiguration funktioniert.



2. **Fügen Sie Anmeldeinformationen zur Anwendung hinzu:**

   a. Öffnen Sie im Azure-Administratorportal die Seite App-Registrierungen.

   b. Klicken Sie auf die von Ihnen erstellte Anwendung.

   c. Klicken Sie im linken Menü auf **Zertifikate und Geheimnisse**.

   d. Klicken Sie auf **+ Neuer geheimer Clientschlüssel**.

   e. Geben Sie im Feld **Beschreibung** einen praktischen Namen für dieses Geheimnis und einen **Ablaufwert** ein, der Ihren Richtlinien entspricht. Denken Sie daran, dieses Geheimnis kurz vor Ablauf seines Ablaufdatums zu erneuern.

   f. Speichern Sie den Wert des geheimen Schlüssels an einem sicheren Ort, da Azure ihn nur einmal anzeigt und Sie ihn neu erstellen müssen, wenn Sie ihn verlieren.

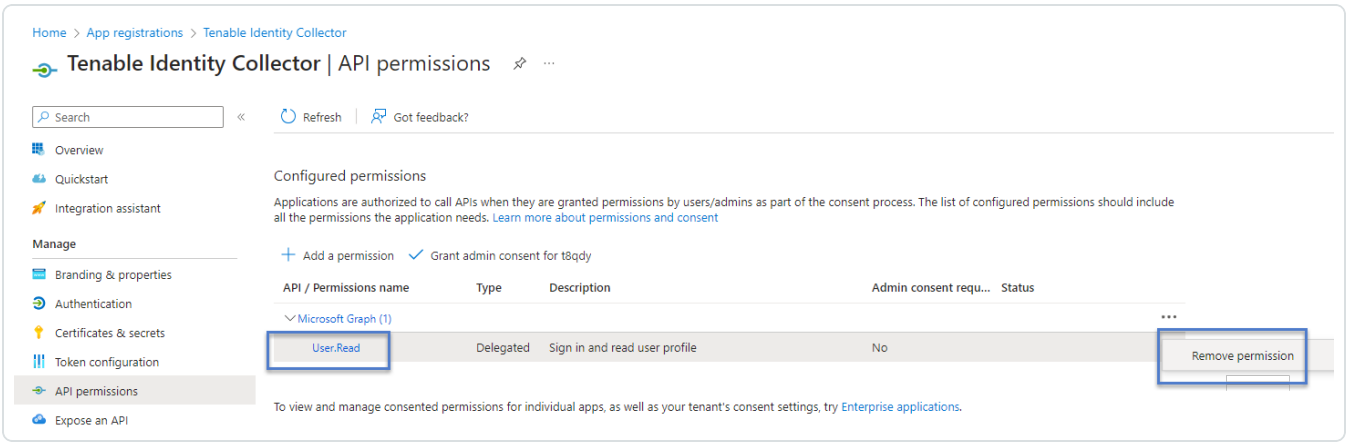
3. **Weisen Sie der Anwendung Berechtigungen zu:**

   a. Öffnen Sie im Azure-Administratorportal die Seite App-Registrierungen.

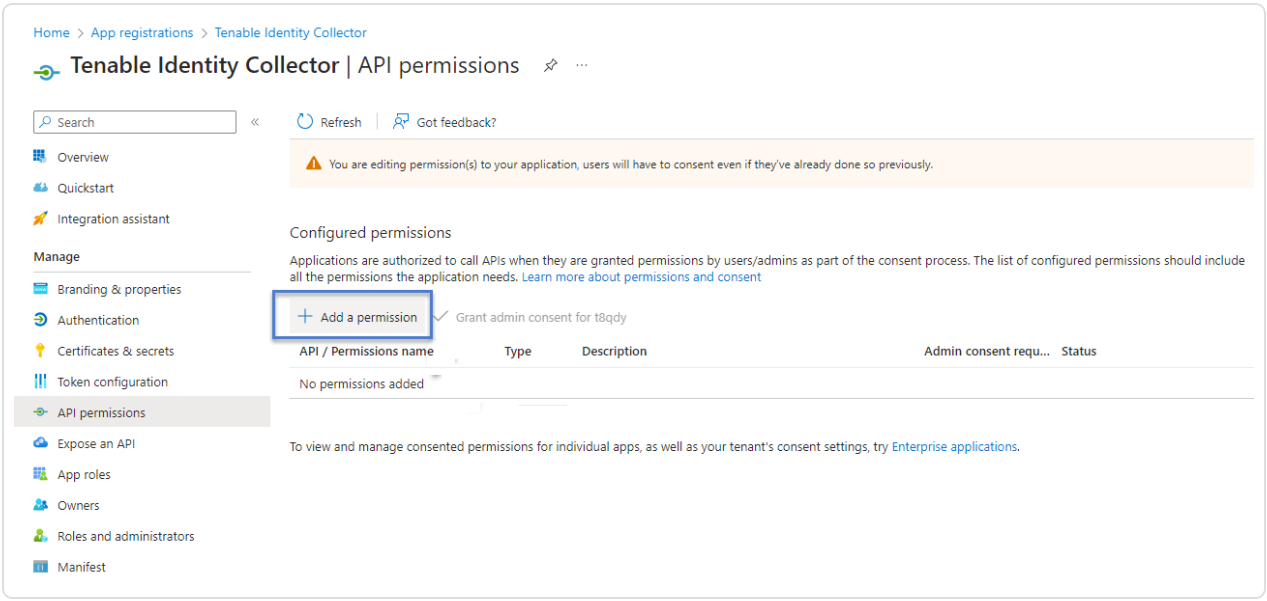
   b. Klicken Sie auf die von Ihnen erstellte Anwendung.

c. Klicken Sie im linken Menü auf **API-Berechtigungen**.

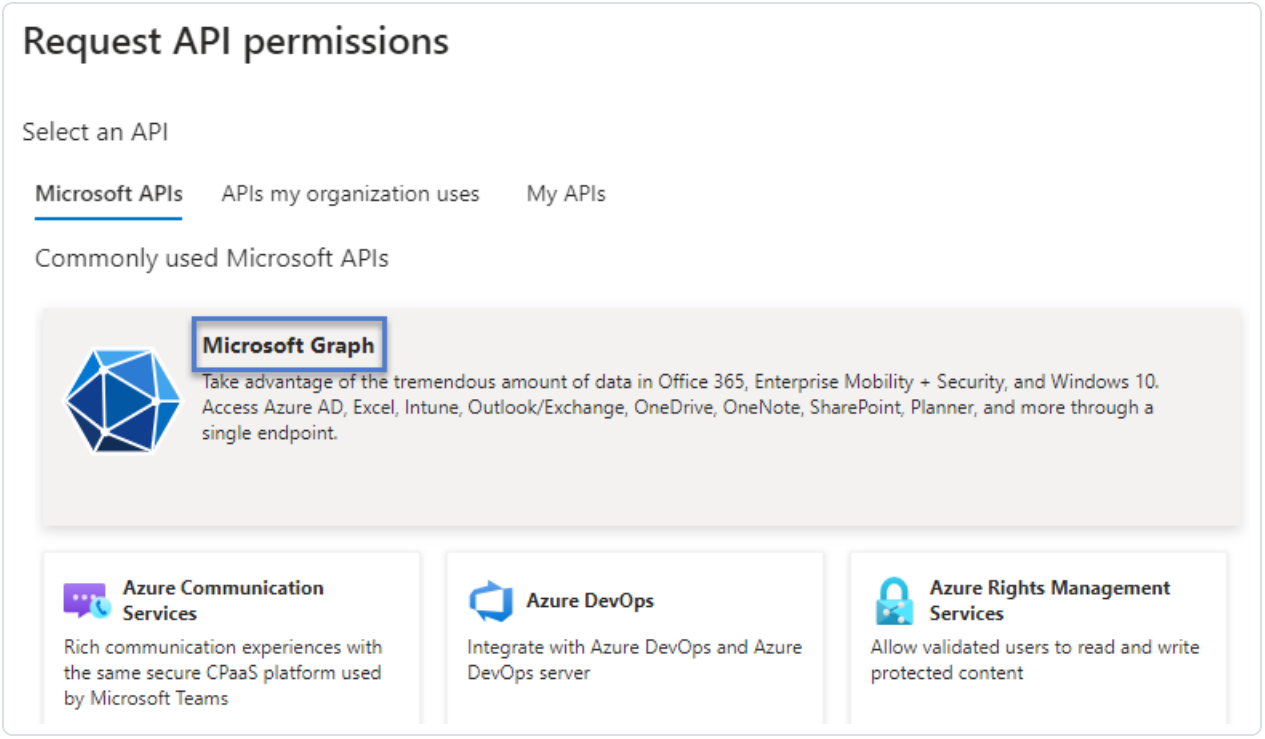
d. Entfernen Sie die vorhandene Berechtigung `User.Read`:



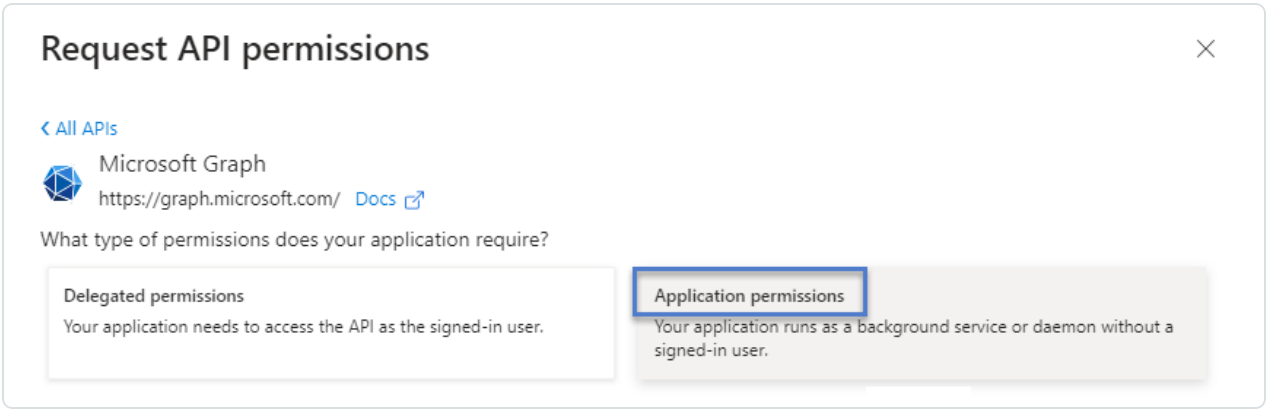
e. Klicken Sie auf **+ Berechtigung hinzufügen**:



f. Wählen Sie **Microsoft Graph** aus:



g. Wählen Sie **Anwendungsberechtigungen** aus (nicht „Delegierte Berechtigungen“).



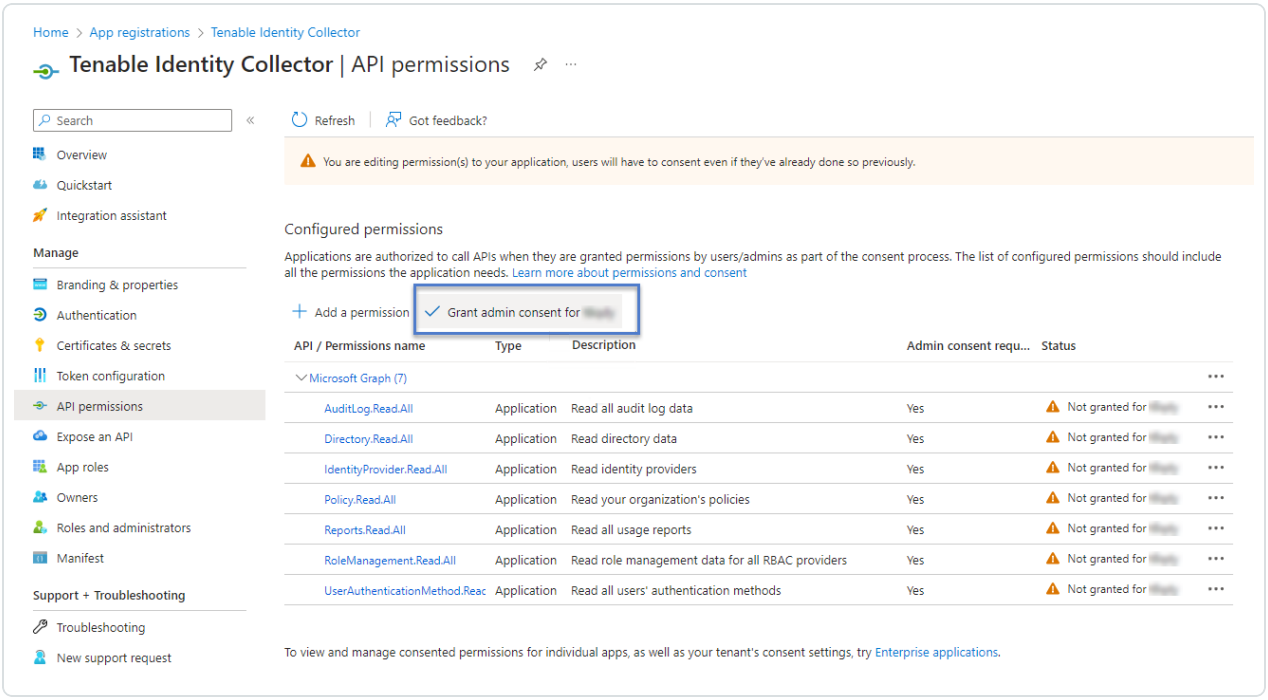
h. Verwenden Sie die Liste oder die Suchleiste, um alle folgenden Berechtigungen zu suchen und auszuwählen:

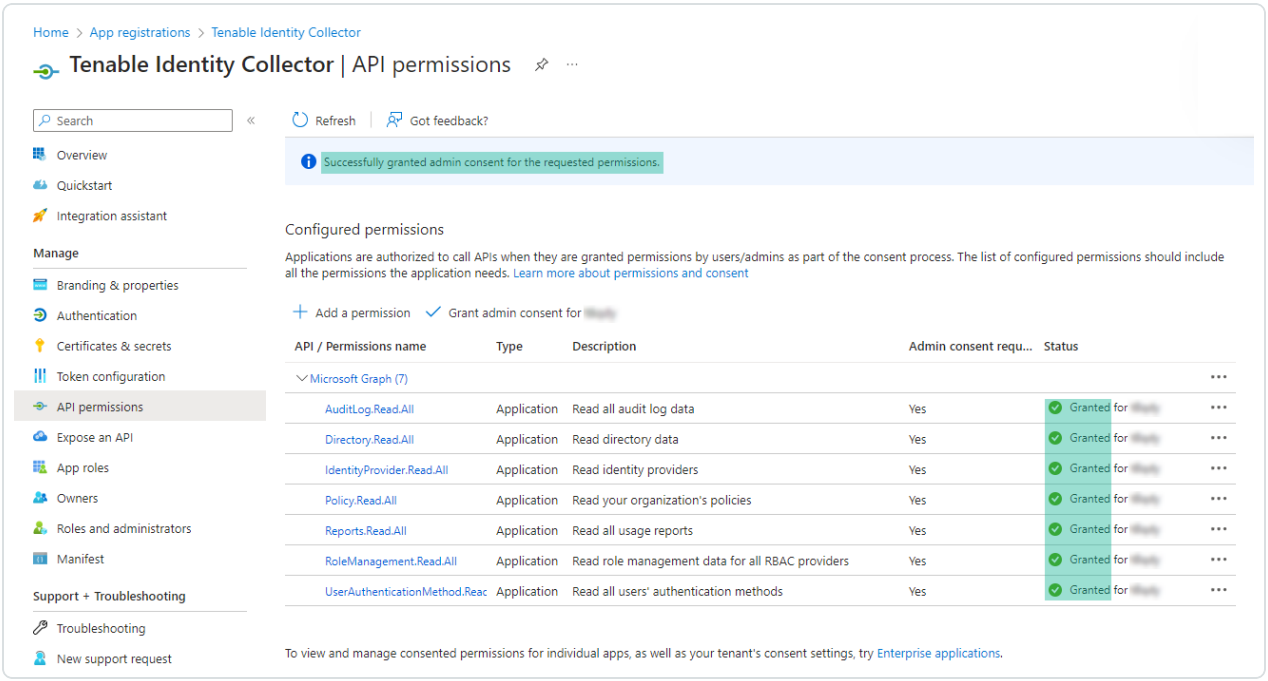
   - `AuditLog.Read.All`
   - `Directory.Read.All`
   - `IdentityProvider.Read.All`
   - `Policy.Read.All`

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

i. Klicken Sie auf **Berechtigungen hinzufügen**.

j. Klicken Sie auf **Administratoreinwilligung erteilen für <Mandantenname>** und klicken Sie zur Bestätigung auf **Ja**:





4. Nachdem Sie alle erforderlichen Einstellungen in Microsoft Entra ID konfiguriert haben, führen Sie die folgenden Schritte aus:

    a. Erstellen Sie in Tenable Vulnerability Management neue Anmeldeinformationen des Typs „Microsoft Azure“.

    b. Wählen Sie die Authentifizierungsmethode „Schlüssel“ und geben Sie die Werte ein, die Sie im vorherigen Verfahren abgerufen haben: Mandanten-ID, Anwendungs-ID und Client-Geheimnis.

Microsoft Entra ID-Unterstützung aktivieren

- Um **Microsoft Entra ID**verwenden zu können, müssen Sie die Funktion in den Einstellungen von Tenable Identity Exposure aktivieren.
- Entsprechende Anweisungen finden Sie unter Identity 360, Exposure Center, and Microsoft Entra ID Support Activation .

Mandantenscans aktivieren

So fügen Sie einen neuen Microsoft Entra ID-Mandanten hinzu:

Durch das Hinzufügen eines Mandanten wird Tenable Identity Exposure mit dem Microsoft Entra ID-Mandanten verknüpft, um Scans für diesen Mandanten durchzuführen.

1. Klicken Sie auf der Seite „Konfiguration“ auf die Registerkarte **Mandantenverwaltung**.

    Die Seite **Mandantenverwaltung** wird geöffnet.

2. Klicken Sie auf **Mandanten hinzufügen**.

    Die Seite **Mandanten hinzufügen** wird geöffnet.

3. Geben Sie im Feld **Name des Mandanten** einen Namen ein.
4. Klicken Sie im Feld **Anmeldeinformationen** auf die Dropdown-Liste, um Anmeldeinformationen auszuwählen.
5. Wenn Ihre Anmeldeinformationen nicht in der Liste angezeigt werden, haben Sie diese beiden Möglichkeiten:
    - Erstellen Sie Anmeldeinformationen in Tenable Vulnerability Management (Tenable Vulnerability Management > **Settings** (Einstellungen) > **Credentials** (Anmeldeinformationen)). Weitere Informationen finden Sie im Verfahren zum Erstellen von Azure-Anmeldeinformationen in Tenable Vulnerability Management.
    - Überprüfen Sie, ob Sie über die Berechtigung „Can use“ (Verwendung erlaubt) oder „Can edit“ (Bearbeitung erlaubt) für die Anmeldeinformationen in Tenable Vulnerability

Management verfügen. Sofern Sie nicht über diese Berechtigungen verfügen, zeigt Tenable Identity Exposure die Anmeldeinformationen nicht in der Dropdown-Liste an.

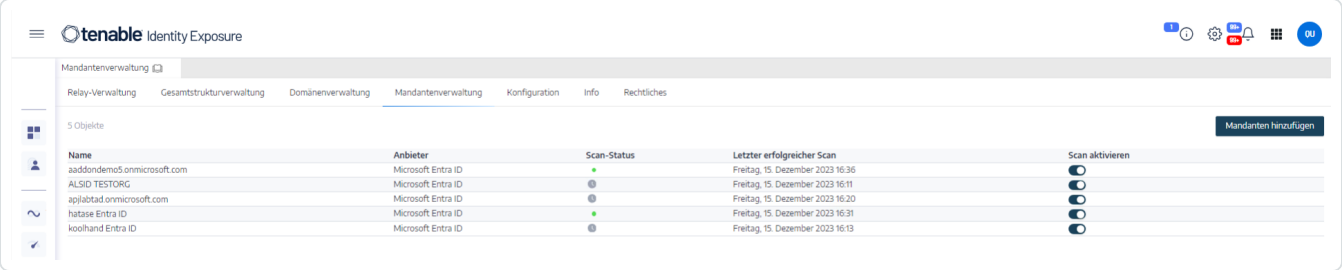
6. Klicken Sie auf **Aktualisieren**, um die Dropdown-Liste der Anmeldeinformationen zu aktualisieren.
7. Wählen Sie die von Ihnen erstellten Anmeldeinformationen aus.
8. Klicken Sie auf **Hinzufügen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure den Mandanten hinzugefügt hat, der nun in der Liste auf der Seite „Mandantenverwaltung“ angezeigt wird.

So aktivieren Sie Scans für den Mandanten:

Hinweis: Mandantenscans erfolgen nicht in Echtzeit und erfordern mindestens 45 Minuten, bis Microsoft Entra ID-Daten im Identitäts-Explorer sichtbar sind.

- Wählen Sie einen Mandanten in der Liste aus und stellen Sie den Schalter auf **Scan aktiviert**.



Tenable Identity Exposure fordert einen Scan des Mandanten an und die Ergebnisse werden auf der Indicator of Exposure-Seite angezeigt.

Hinweis: Die obligatorische Mindestzeitspanne zwischen zwei Scans beträgt **30 Minuten**.

Angriffspfad

Tenable Identity Exposure bietet mehrere Möglichkeiten, die potenzielle Schwachstelle eines Assets durch grafische Darstellungen zu visualisieren.

- **Angriffspfad**: Zeigt die möglichen Angriffspfade, die ein Angreifer nehmen kann, um ein Asset von einem Einstiegspunkt aus zu kompromittieren.
- **Angriffsradius**: Zeigt die möglichen lateralen Bewegungen (Lateral Movements) in das Active Directory von jedem Asset aus an.
- **Asset-Exposure**: Zeigt alle Pfade, die potenziell die Kontrolle über ein Asset übernehmen können.

Wenn Sie den Angriffspfad verstehen, können Sie die notwendigen Schritte zur Risikominderung bestimmen, um Angreifer an der Ausnutzung von Schwachstellen zu hindern. Dazu können das Patchen von Systemen, die Härtung von Konfigurationen, die Implementierung strengerer Zugriffskontrollen oder die Sensibilisierung von Benutzern gehören.

Vorteile der Verwendung von „Angriffspfad“ in Tenable Identity Exposure:

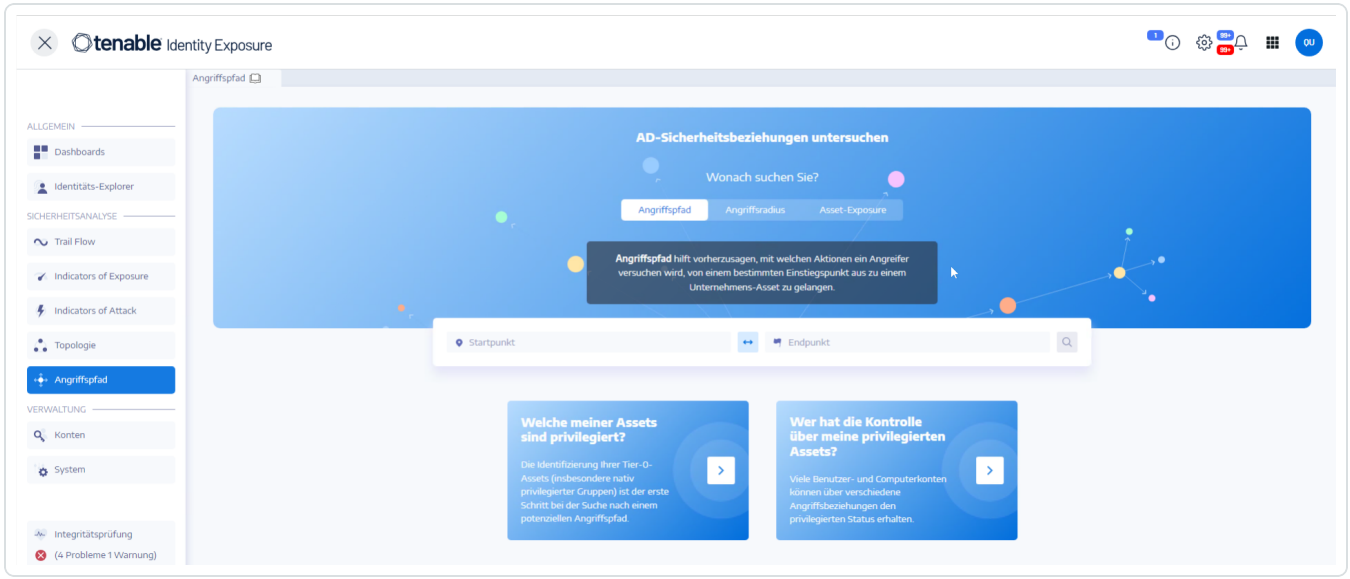
- **Proaktive Sicherheit**: Potenzielle Angriffsvektoren können leichter vorhergesehen und abgewehrt werden, bevor sie ausgenutzt werden.
- **Priorisierung**: Benutzer können ihre Sicherheitsbemühungen gezielter auf die kritischsten Schwachstellen und Angriffspfade konzentrieren.
- **Visualisierung**: Komplexe Sicherheitsbeziehungen im AD werden klar und leicht verständlich dargestellt.
- **Kommunikation**: Stakeholder werden durch visuelle Darstellung potenzieller Angriffsszenarien besser über Sicherheitsrisiken informiert.

So zeigen Sie den Angriffspfad an:

Geben Sie den Startpunkt an, der ein beliebiges Asset in Ihrem AD sein kann (z. B. ein Benutzerkonto, ein Computer, eine Gruppe). Definieren Sie den Zielpunkt, der das Asset darstellt, das der Angreifer letztendlich kompromittieren will (z. B. ein Domänencontroller, Server für sensible Daten).

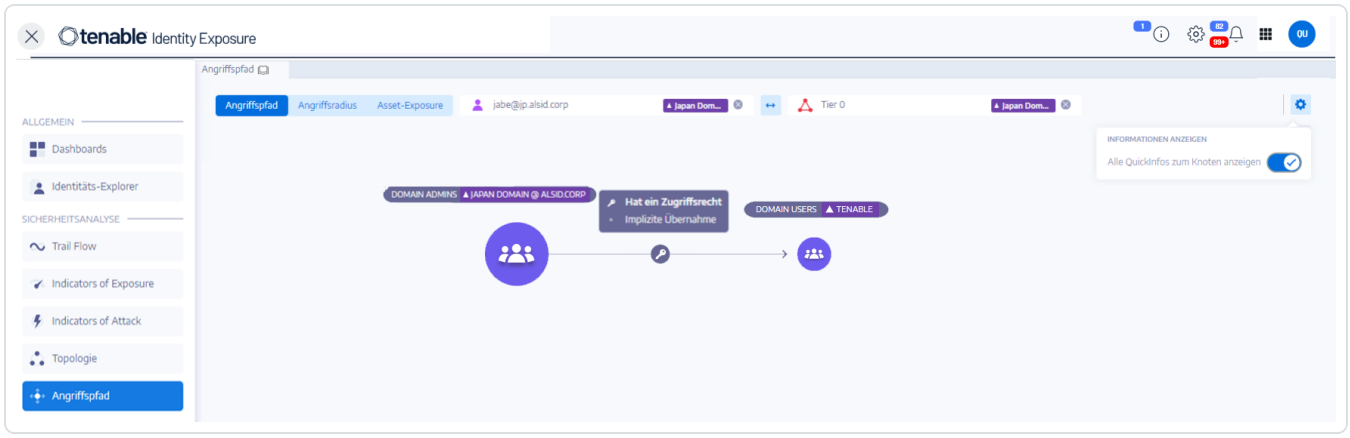
1. Klicken Sie in Tenable Identity Exposure im Menü der Seitenleiste auf **Angriffspfad**.

   Der Fensterbereich **Angriffspfad** wird angezeigt.



2. Klicken Sie im Banner auf **Angriffspfad**.
3. Geben Sie im Feld **Startpunkt** das Asset am Einstiegspunkt ein.
4. Geben Sie im Feld **Endpunkt** das Asset am Ende des Pfades ein.
5. Klicken Sie auf das Symbol  .

   Tenable Identity Exposure zeigt den Angriffspfad zwischen den beiden Assets an.



6. Optional können Sie auf das Symbol  klicken, um Folgendes zu tun:

- Klicken Sie auf den **Zoom**-Schieberegler, um die Vergrößerung der grafischen Darstellung einzustellen.
- Klicken Sie auf die Schaltfläche **Alle QuickInfos zum Knoten anzeigen**, um Informationen über die Assets anzuzeigen.

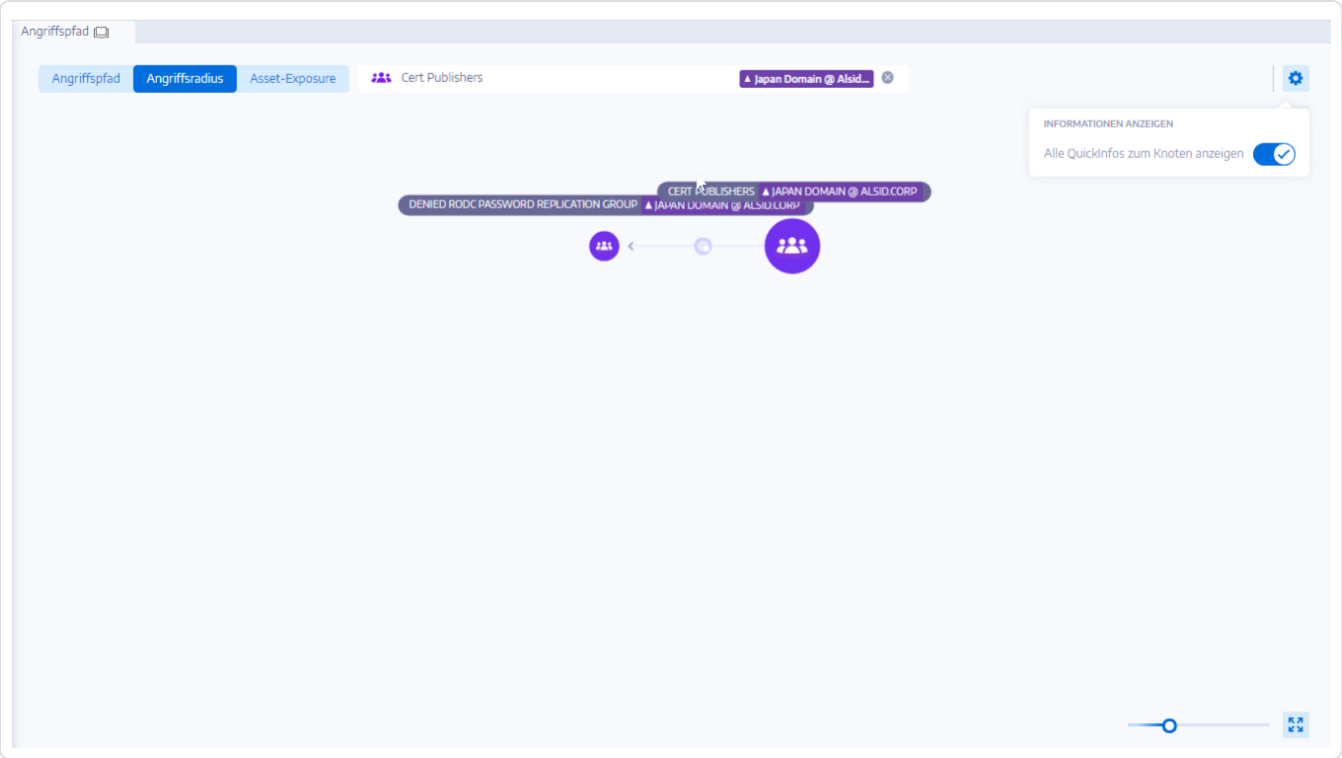
So zeigen Sie den Angriffsradius an:

Tenable Identity Exposure zeigt eine grafische Darstellung des potenziellen Angriffspfads an und hebt die Verbindungen zwischen Assets hervor. Jede Verbindung stellt eine potenzielle Schwachstelle oder Fehlkonfiguration dar, die der Angreifer ausnutzen könnte, um sich lateral in Ihrem AD zu bewegen. Sie können die Ansicht vergrößern und verkleinern, um sich die Details des Pfads genauer anzusehen.

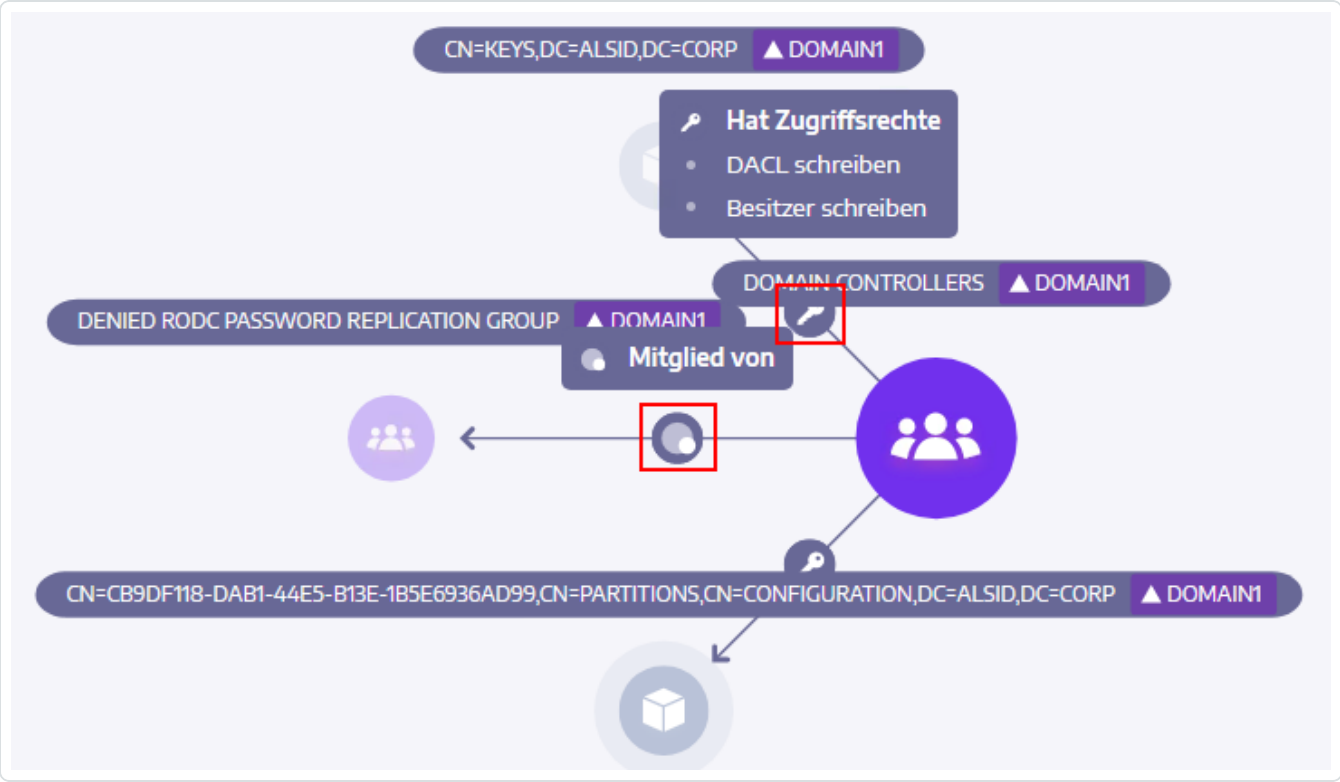
1. Klicken Sie in Tenable Identity Exposure im Menü der Seitenleiste auf **Angriffspfad**.

   Der Fensterbereich **Angriffspfad** wird angezeigt.
2. Klicken Sie im Banner auf **Angriffsradius**.
3. Geben Sie im Feld **Objekt suchen** den Namen eines Assets ein.
4. Klicken Sie auf das Symbol .

   Tenable Identity Exposure zeigt die lateralen Verbindungen an, die von diesem Asset ausgehen:



5. Klicken Sie auf die Symbole auf den Pfeilen zwischen den Assets, um die Beziehungen zwischen ihnen anzuzeigen.



So zeigen Sie die Asset-Exposure an:

Jeder Schritt im Angriffspfad ist mit einem Risikowert verbunden, der den Schweregrad der Schwachstelle angibt. Dies hilft Ihnen dabei, Prioritäten zu setzen, da sie besser erkennen können, welche Pfade die größte Bedrohung darstellen und sofortiges Handeln erfordern. Sie können auch auf einzelne Verbindungspunkte klicken, um weitere Details zu der spezifischen Schwachstelle oder Fehlkonfiguration zu erhalten.

1. Klicken Sie in Tenable Identity Exposure im Menü der Seitenleiste auf **Angriffspfad**.

   Der Fensterbereich **Angriffspfad** wird angezeigt.

2. Klicken Sie im Banner auf **Asset-Exposure**.

3. Geben Sie im Feld **Objekt suchen** den Namen eines Assets ein.

4. Klicken Sie auf das Symbol .

   Tenable Identity Exposure zeigt die Pfade, die zu dem Asset führen, und die Beziehungen zwischen den Assets an.

5. Klicken Sie auf die Symbole auf den Pfeilen zwischen den Assets, um die Beziehungen zwischen ihnen anzuzeigen.

So stecken Sie einen Angriffspfad ab:

Siehe auch

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

Benutzerverwaltung

Schwerpunkte

- **Rollen**: Zu den Standardrollen gehören Administrator, Sicherheitsanalyst, Benutzer und Gast, jeweils mit unterschiedlichen Berechtigungen. Benutzerdefinierte Rollen ermöglichen eine granulare Kontrolle für spezifische Anforderungen.
- **Berechtigungen**: Berechtigungen legen fest, worauf Benutzer in Tenable Identity Exposure Zugriff haben und was sie dort tun können. Dies reicht von der Anzeige von Berichten und Dashboards über die Verwaltung von Benutzern, das Konfigurieren von Indikatoren und das Durchführen von Aktionen wie der Deaktivierung von Konten.
- Die **Festlegung des Geltungsbereichs** für Tenable Identity Exposure ermöglicht die Zuweisung von Berechtigungen für bestimmte Domänen, Gruppen oder sogar einzelne Objekte innerhalb von Active Directory. Dadurch wird sichergestellt, dass Benutzer nur auf relevante Daten zugreifen, die ihrer Rolle und ihren Verantwortlichkeiten entsprechen.

Vorteile

- **Verbesserte Active Directory-Sicherheit**: Die granulare Zugriffssteuerung minimiert das Risiko eines nicht autorisierten Zugriffs auf sensible Identitätsdaten.
- **Verbesserte Effizienz und verbesserte Workflows**: Benutzer haben Zugriff auf die benötigten Tools und Daten, wodurch Untersuchungen und Vorfallsreaktion effizienter werden.
- **Compliance-Einhaltung**: Die rollenbasierte Zugriffssteuerung hilft bei der Erfüllung von Compliance-Anforderungen für die Identitäts- und Zugriffsverwaltung in Active Directory.

Siehe auch

- User Roles

Tenable Identity Exposure-Integration

Integrieren Sie Tenable Identity Exposure mit Ihrer SIEM-, SOC- oder SOAR-Lösung, um Echtzeitüberwachung, automatisierte Reaktionen und ein verbessertes Warnungsmanagement zu erzielen.

Echtzeitüberwachung mit Syslog-Integration

Erhalten Sie sofortige Warnungen für kritische IoEs (Indicators of Exposure) durch nahtlose Syslog-Integration.

Wichtige Vorteile

- **Zentrale Protokollierung**: Aggregieren Sie Tenable Identity Exposure-Ereignisse mit anderen Sicherheitslösungen, um umfassende Analysen durchzuführen.
- **Echtzeitbenachrichtigungen**: Erhalten Sie sofortige Benachrichtigungen über potenzielle Expositionen von Identitäten und Angriffe.
- **Verbessertes Sicherheitsmanagement**: Korrelieren Sie Ereignisse aus verschiedenen Quellen, um komplexe Bedrohungen schneller zu identifizieren.
- **Verbesserte SIEM-Sichtbarkeit**: Integrieren Sie Tenable Identity Exposure-Daten nahtlos in Ihr SIEM-SystemSIEM, um Lageerkennung und Korrelationsanalyse zu verbessern.
- **Optimierter Workflow**: Automatisieren Sie die Einordnung von Warnungen und den entsprechenden Reaktionsmaßnahmen auf der Grundlage von Syslog-Daten, um Sicherheitsabläufe zu optimieren.

Beispiel für IoEs für die Echtzeitüberwachung

- **Gefährliche ADCS-Fehlkonfigurationen**: Erkennen/Identifizieren von Änderungen an AD-Zertifikatservern, die möglicherweise auf „Certified Pre-Owned”-Angriffe (CPO-Angriffe) hinweisen.
- **GPO-Ausführungsintegrität**: Erkennt/identifiziert Versuche, Backdoors durch Skriptausführung innerhalb von Gruppenrichtlinien zu installieren.

- **Benutzer, die der Domäne Computer hinzufügen dürfen**: Erkennen nicht autorisierter Hinzufügungen von Domänencomputern, eine typische Angriffsvorbereitung von „RBCD“-Backdoor-Angriffen.

Automatisierung von Reaktionsmaßnahmen mit SOAR-Plattformen

Nutzen Sie vorhandene SOAR-Plattformen (Security Orchestration, Automation and Response), um automatisierte Behebungsmaßnahmen auf der Grundlage von TIE-Daten auszuführen. Die wichtigsten Vorteile sind:

- **Schnelle Risikominderung**: Minimieren Sie Ausfallzeiten und Auswirkungen, indem Sie Reaktionen auf kritische IoEs automatisieren.
- **Verbesserte Effizienz**: Entlasten Sie Sicherheitsteams von repetitiven Aufgaben, sodass sie sich auf strategische Sicherheitsinitiativen konzentrieren können.
- **Verbesserte Sicherheitsmaßnahmen**: Beheben Sie proaktiv erkannte Fehlkonfigurationen, und stärken Sie Ihren Sicherheitsstatus insgesamt.

Wichtig: Fehlerbehebung oder Unterstützung bei Automatisierungsskripten fallen nicht in den Aufgabenbereich von Tenable Support. Bitte wenden Sie sich an unser Professional Services-Team, um Unterstützung zu erhalten.