Guía de funcionalidades clave de Tenable Identity Exposure

Última revisión: 2 de julio de 2025

Índice

Bienvenida a la Guía de funcionalidades clave de Tenable Identity Exposure

Le damos la bienvenida a Tenable Identity Exposure, anteriormente conocido como Tenable AD. Este documento se creó para mejorar su experiencia y en él se ofrece una descripción general completa de las características y funcionalidades del producto, ya sea que se implementen en el entorno local o como SaaS. Este recurso tiene como objetivo ayudarlo tanto si no está familiarizado con el producto y busca orientación como si es un usuario experimentado que busca profundizar sus conocimientos.

A lo largo de este documento, encontrará varias secciones que exploran una variedad de temas, incluidas la optimización del uso del producto y la gestión de indicadores de ataque e indicadores de exposición. Es importante tener en cuenta que, si bien este documento proporciona información valiosa, no pretende ser un libro de reglas rígido sobre el uso de Tenable Identity Exposure. Por el contrario, ofrece recomendaciones para lograr una utilización fluida y eficaz de la plataforma.

Acerca de esta guía

Esta guía se basa en la **Guía del usuario de Tenable Identity Exposure SaaS**, que puede consultar para obtener detalles completos.

Los ejemplos que se muestran en esta guía para destacar las capacidades de Tenable Identity Exposure no representan una lista exhaustiva y es posible que no se puedan traducir directamente a cada entorno en particular. Para adoptar medidas de seguridad óptimas, se recomienda consultar nuestra documentación oficial o acudir a Professional Services para obtener más detalles y orientación.

Principales partes interesadas

Las partes interesadas individuales en Tenable Identity Exposure difieren según el tamaño, la estructura, las políticas de seguridad y los casos de uso previstos de su organización. Establecer roles y responsabilidades precisos para cada parte interesada permite la adopción y utilización eficiente del producto.

Al trabajar con Tenable Identity Exposure, es fundamental comprender las diferentes partes interesadas que participan. Estas personas y grupos asumen distintos roles en la detección,

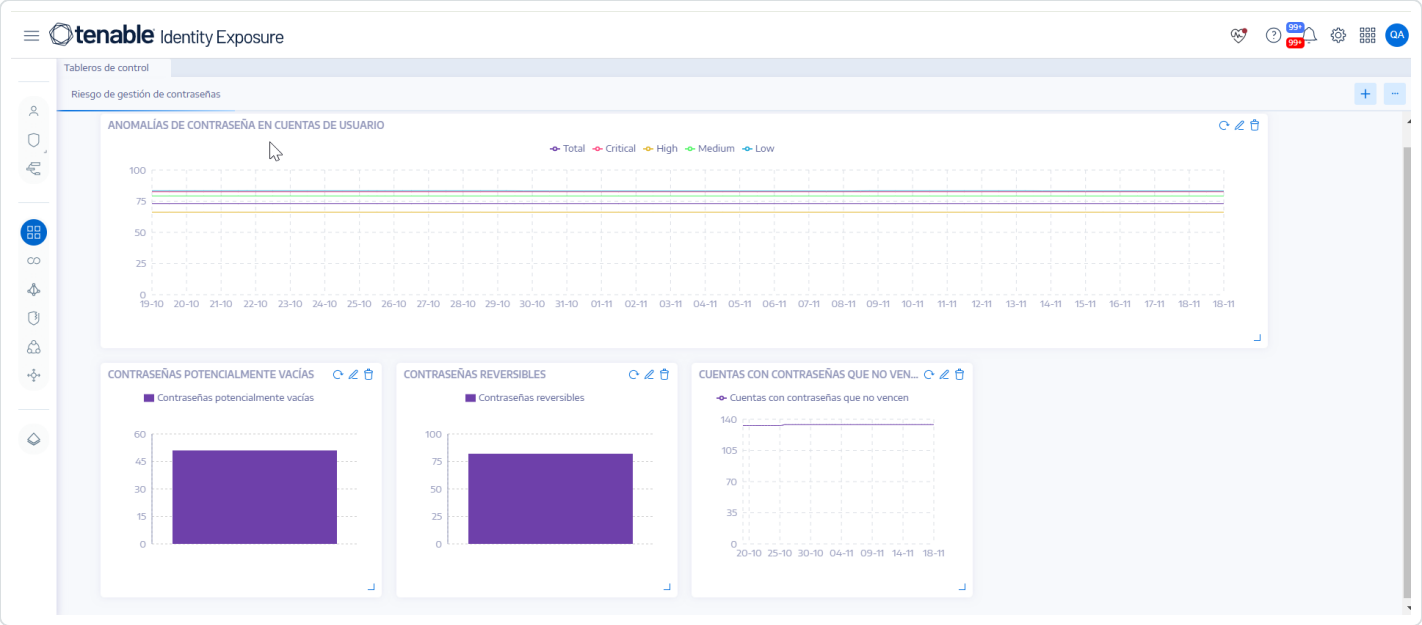
mitigación y notificación de riesgos de seguridad basados en la identidad. A continuación se muestra un desglose completo:

- **Equipo de seguridad**: supervisa y administra la solución Tenable, y aprovecha el análisis de datos para rápidamente detectar las vulnerabilidades y los riesgos y responder a ellos.
- **Equipo de operaciones de TI**: facilita la infraestructura y el soporte de integración para la solución Tenable, y garantiza una conectividad continua con otras herramientas de seguridad y directorios de usuarios.
- **Equipos de desarrollo de aplicaciones**: se encargan de proteger las aplicaciones y abordar rápidamente cualquier identidad expuesta que Tenable señale.
- **Equipo de gestión de identidades y acceso** (IAM): gestiona cuentas de usuario, permisos y controles de acceso, y colabora estrechamente con sus homólogos de seguridad de TI para abordar los problemas detectados por Tenable Identity Exposure.
- **Líderes de unidades de negocio**: tienen la máxima responsabilidad por la posición de seguridad de sus equipos y aplicaciones. Revisan informes, priorizan las estrategias de mitigación de riesgos y asignan recursos para mejorar las medidas de seguridad de Active Directory.

Tableros de control

Los tableros de control le permiten visualizar datos y tendencias que afectan la seguridad de su instancia de Active Directory. Puede personalizarlos con widgets para mostrar gráficos y contadores según sus requisitos.

El tablero de control de Tenable Identity Exposure sirve como centro de comando en tiempo real para la seguridad de Active Directory (AD) de su organización. Ofrece una descripción general completa (por ejemplo, una vista centralizada en tiempo real) de su panorama de identidades, donde se destacan vulnerabilidades críticas, se detectan posibles vectores de ataque y se permite la mitigación proactiva de riesgos.



Funcionalidades clave de los tableros de control

- **Generalidades de un vistazo**: conozca rápidamente su estado de seguridad con métricas clave que se muestran de manera destacada, como la puntuación de cumplimiento, los principales riesgos y las tendencias de actividad de los usuarios.
- **Análisis de los detalles**: profundice en áreas específicas con widgets interactivos que desglosan los factores de riesgo por gravedad, categoría de usuario y otros criterios pertinentes.

- **Enfoque personalizable**: cree tableros de control personalizados adaptados a sus prioridades; para ello, puede usar plantillas prediseñadas o crear sus propios diseños. Por ejemplo, para crear un tablero de control de los errores de configuración más comunes frente a los IoE recurrentes más comunes:
    - Asegurar la coherencia de SDProp.
    - Controladores de dominio administrados por usuarios ilegítimos.
    - Delegación peligrosa de Kerberos.
- **Supervisión en tiempo real**: manténgase al tanto de las amenazas emergentes y la actividad sospechosa por medio de actualizaciones y alertas continuas.
- **Información accionable**: obtenga recomendaciones prácticas para la corrección, priorizadas según la gravedad y el posible impacto.

Consulte también

- Tableros de control
- Tutorial en video sobre tableros de control

Trail Flow

Trail Flow de Tenable Identity Exposure muestra la supervisión y el análisis en tiempo real de los eventos que afectan su infraestructura de AD. Le permite detectar vulnerabilidades críticas y las acciones de corrección recomendadas.

Con la página **Trail Flow**, puede retroceder en el tiempo y cargar eventos anteriores o buscar eventos específicos. También puede usar el cuadro de búsqueda situado al principio de la página para buscar amenazas y detectar patrones malintencionados.

Trail Flow hace un seguimiento de los siguientes eventos:

- **Cambios de usuarios y grupos**: incluye la creación, la eliminación y la modificación de cuentas y grupos.
- **Modificaciones de permisos**: incluye las modificaciones a los controles de acceso en objetos, como archivos, carpetas e impresoras.
- **Ajustes en la configuración del sistema**: involucra cambios en los objetos de política de grupo (GPO) y otras opciones críticas.
- **Actividades sospechosas**: incluye intentos no autorizados, escalamientos de privilegios y otros eventos que generan señales de alerta.

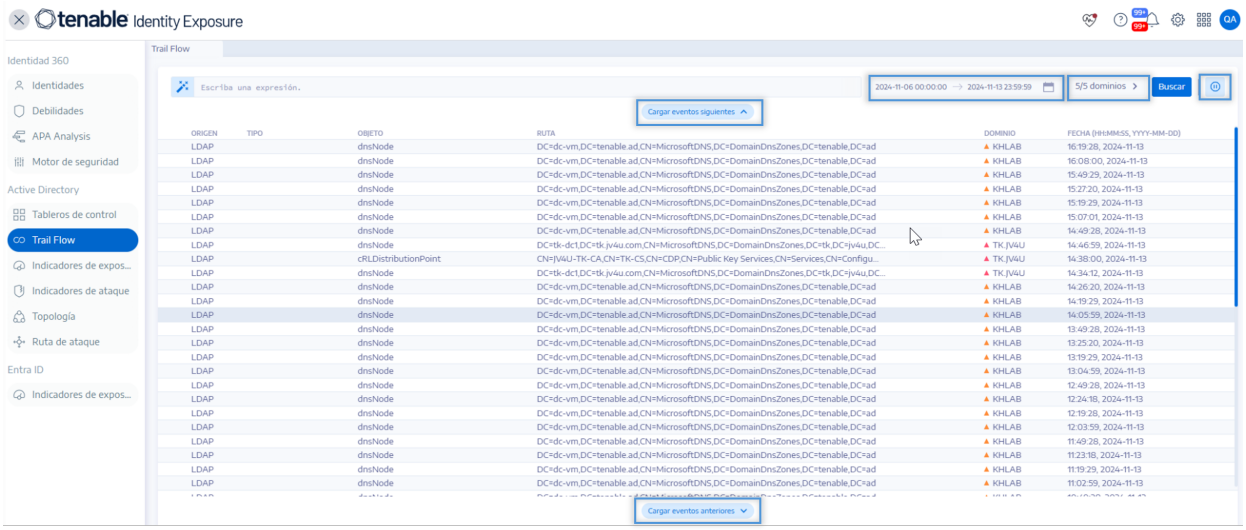
Tenable Identity Exposure ofrece estas funcionalidades para aprovechar los datos de Trail Flow:

- **Búsquedas y filtros**: es posible navegar de manera sencilla por el flujo de eventos mediante palabras clave o criterios específicos, lo que permite centrar la atención en las actividades pertinentes y minimizar el ruido externo.
- **Información detallada del evento**: cada entrada de evento ofrece detalles exhaustivos, que abarcan el objeto afectado, el usuario responsable del cambio, el protocolo utilizado y los indicadores de exposición (IoE) asociados.
- **Relaciones visualizadas**: refiere a la capacidad de ilustrar las relaciones entre los eventos, donde se destaca cómo actividades aparentemente no relacionadas pueden contribuir a una campaña de ataque más amplia.

Para acceder a Trail Flow:

- En Tenable Identity Exposure, haga clic en **Trail Flow** en la barra de navegación de la izquierda.

  Se abre la página “Trail Flow” con una lista de eventos. Para obtener más información, consulte Trail Flow Table.



Para seleccionar un período de tiempo:

Para seleccionar un dominio:

Para ver un evento:

Para pausar o reiniciar Trail Flow:

Para cargar los eventos siguientes o anteriores:

¿Cómo aparecen los datos en Trail Flow?

1. Cuando realiza una acción dentro de la interfaz de Active Directory (AD), por ejemplo:
   - Crear una nueva cuenta de usuario.
   - Modificar la pertenencia a un grupo de un usuario.

- Restablecer una contraseña.
- Deshabilitar una cuenta.
- Habilitar una cuenta.
- Eliminar una cuenta.
- Mover un objeto.
- Modificar permisos.

2. Active Directory (AD) genera automáticamente una entrada del registro de eventos que captura detalles de la operación, entre otras cosas:
    - Marca de tiempo.
    - Administrador que se encarga de la acción.
    - Objetos afectados.
    - Cambios específicos que se hicieron.
3. Tenable Identity Exposure recopila y analiza de manera continua estos registros de eventos y correlaciona los eventos, identifica patrones y detecta anomalías.
4. En la página “Trail Flow” se visualizan el flujo y el impacto de la operación:
    - Línea de tiempo: muestra una secuencia cronológica de eventos, donde se resalta la operación reciente.
    - Detalles del objeto: ofrece información específica sobre los objetos afectados, incluidos sus atributos y relaciones.
    - Historial de cambios: muestra un historial de modificaciones hechas en los objetos, incluida la operación actual.
    - Información sobre riesgos: identifica riesgos potenciales asociados a la operación, como permisos excesivos o la pertenencia a grupos confidenciales.
    - Información sobre cumplimiento: indica cualquier infracción de cumplimiento relacionada con la operación.

Consulte también

- Información general de Trail Flow
- Trail Flow Use Cases
- Tutorial en video de Trail Flow

Centro de informes

El **Centro de informes** en Tenable Identity Exposure proporciona una funcionalidad valiosa que le permite exportar datos importantes como informes a las partes interesadas clave dentro de una organización. El Centro de informes ofrece un medio para crear informes a partir de una lista predefinida, lo que garantiza un proceso eficiente y optimizado.

Ofrece las siguientes funciones:

- **Filtrado detallado**: ajuste los informes mediante filtros detallados basados en rangos de fechas, dominios, indicadores de ataque (IoA), indicadores de exposición (IoE) y más, lo que garantiza información muy precisa.
- **Entrega automatizada**: programe informes para su generación y entrega automáticas en los intervalos deseados, lo que agiliza los procesos de supervisión y generación de informes de seguridad.
- **Exportación flexible**: exporte informes en varios formatos, como CSV, para su posterior análisis, y compártalos mediante una clave de acceso a los informes o intégrelos en flujos de trabajo de informes existentes.

Los administradores pueden crear distintos tipos de informes para distintos usuarios con plazos de informes flexibles de hasta un trimestre. La capacidad de compartir datos de identidad críticos desde Tenable Identity Exposure permite a la organización mitigar de forma proactiva los riesgos e identificar posibles ataques basados en la identidad.

Para descargar un informe, los usuarios reciben un correo electrónico con una dirección URL a una página en la que ingresan una clave de acceso al informe que recibieron del administrador. Los informes están disponibles para su descarga durante 30 días, después de los cuales vencen y Tenable Identity Exposure los elimina. Los usuarios deben descargar los informes antes de que Tenable Identity Exposure genere uno nuevo para el período de tiempo especificado y sobrescriba el anterior.

Para acceder al Centro de informes:

1. En Tenable Identity Exposure, seleccione **Sistema** > **Configuración**.
2. En **Informes**, haga clic en **Centro de informes**.

Se abre un panel con una lista de informes configurados y su información asociada, como el nombre del informe, el tipo, el dominio, el perfil, el período, la periodicidad y los correos electrónicos de los destinatarios.

Consulte también

- Centro de informes
- Set Permissions for a Role

Indicadores de exposición

Tenable Identity Exposure usa indicadores de exposición (IoE) para medir la madurez de la seguridad de las infraestructuras de AD y asigna niveles de gravedad al flujo de eventos que supervisa y analiza. Tenable Identity Exposure desencadena alertas cuando detecta regresiones de seguridad.

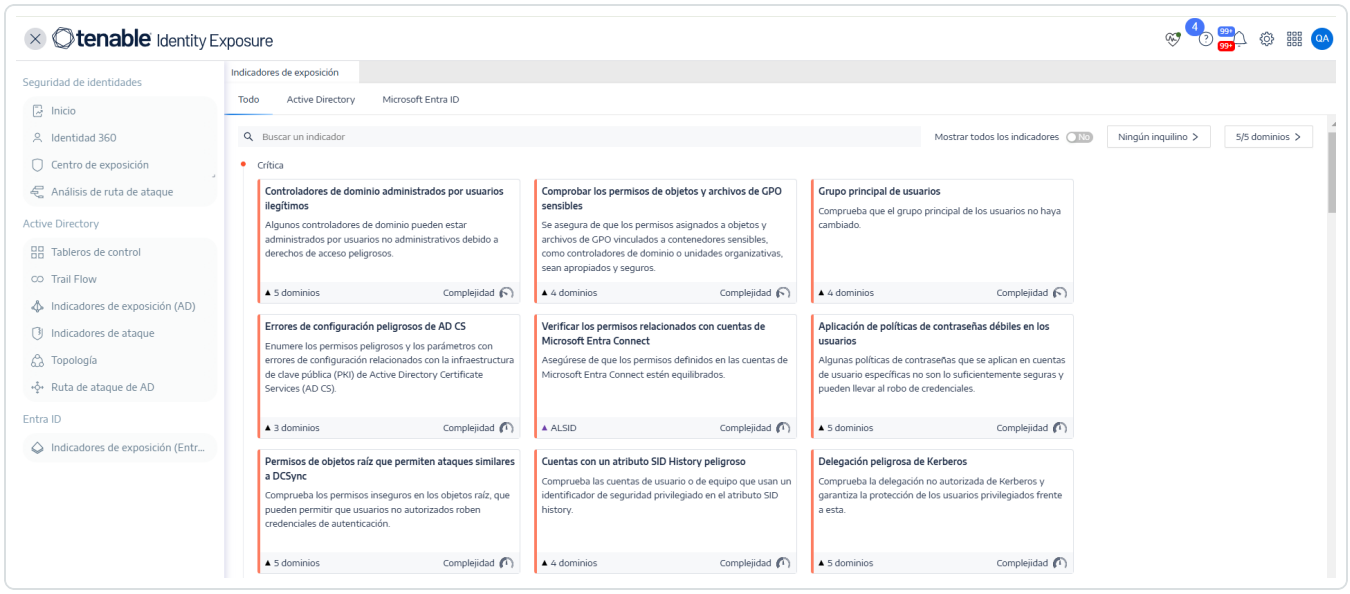
Estos IoE están preconfigurados y cualquier desviación de las normas establecidas desencadena las alertas correspondientes.

Para mostrar los IoE:

1. En Tenable Identity Exposure, haga clic en **Indicadores de exposición** en el panel de navegación.

   Se abre el panel **Indicadores de exposición**. De manera predeterminada, Tenable Identity Exposure muestra solo los IoE que contienen anomalías.

2. (Opcional) Para mostrar todos los IoE, haga clic en el conmutador **Mostrar todos los indicadores** para establecerlo en **Sí**.



Los IoE de Tenable Identity Exposure vienen con una variedad de funcionalidades diseñadas para mejorar las capacidades de investigación:

- **Búsqueda y filtros**: aplique filtros basados en el bosque y el dominio para explorar los IoE sin esfuerzo.
- **Funcionalidad de exportación**: el objeto anómalo le permitirá exportar los IoE en formato CSV.
- **Acción ante incidentes de IoE**: quite una exposición de la whitelist o vuelva a habilitarla.

Los datos de los IoE incluyen:

- **Sección de información**: en esta sección encontrará un resumen ejecutivo sobre cada indicador de exposición (IoE), incluidas las herramientas de ataque conocidas, los dominios afectados y la documentación pertinente.
- **Detalles de la vulnerabilidad**: en esta sección se ofrece información más detallada sobre el error de configuración de Active Directory.
- **Objetos anómalos**: en esta sección se destacan los errores de configuración de Active Directory que pueden contribuir a superficies de ataque más amplias.
- **Recomendación**: esta sección lo guía por las estrategias de configuración efectivas para minimizar la superficie de ataque.

Nivel de gravedad

Los niveles de gravedad le permiten evaluar la gravedad de las vulnerabilidades detectadas y priorizar las acciones de corrección.

En el panel **Indicadores de exposición**, los IoE se muestran de la siguiente manera:

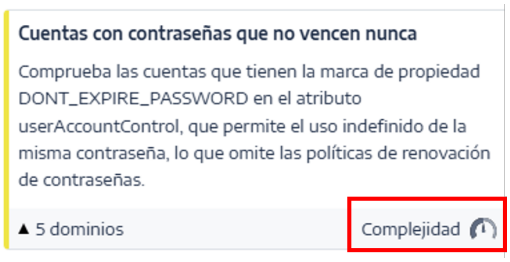
- Por nivel de gravedad con códigos de colores.
- En dirección vertical: del más grave al menos grave (rojo para la prioridad máxima y azul para la prioridad mínima).
- En dirección horizontal: del más complejo al menos complejo. Tenable Identity Exposure calcula el indicador de complejidad de forma dinámica para indicar el nivel de dificultad para corregir el IoE anómalo.

Gravedad	Descripción

Crítica: rojo	Muestra cómo prevenir los ataques y el riesgo de Active Directory por parte de ciertos usuarios sin privilegios.
Alta: naranja	Se ocupa de técnicas posteriores a la explotación que conducen al robo de credenciales o a la evasión de la seguridad, o de técnicas de explotación que requieren encadenamiento para ser peligrosas.
Media: amarillo	Indica un riesgo limitado para la infraestructura de Active Directory.
Baja: azul	Muestra prácticas recomendadas de seguridad. Ciertos contextos empresariales pueden permitir anomalías de bajo impacto que no necesariamente afecten la seguridad de AD. Estas anomalías tienen un impacto en la instancia de AD solo si un administrador comete un error, como activar una cuenta inactiva.

Priorización de la corrección

Los esfuerzos de corrección se centran en los IoE de alta gravedad que el sistema detectó. Además, puede priorizar aún más dentro de la categoría crítica por medio del medidor de riesgo incluido en el IoE.

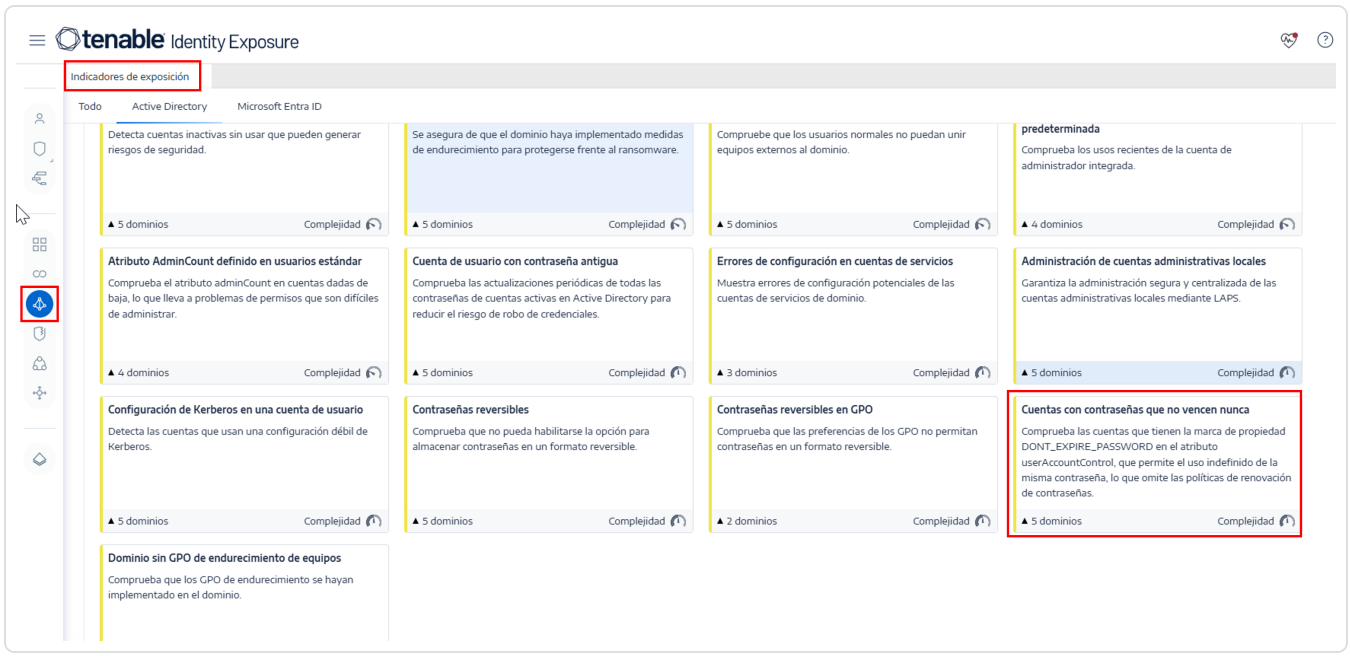


Si cree que el IoE se ubica dentro del ámbito de competencia o mandato operativo de su organización, puede incluirlo en la lista de permitidos.

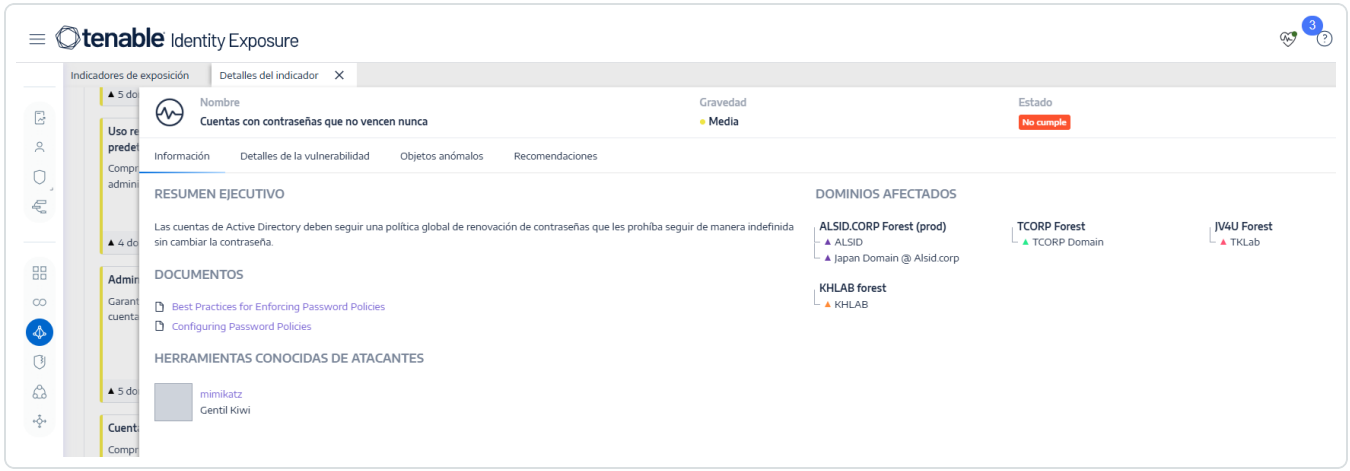
Caso de uso

El siguiente caso de uso se centra en el IoE denominado “Cuentas con contraseñas que no vencen nunca”.

1. Cuando Tenable Identity Exposure marca un IoE, aparece en el panel “Indicadores de exposición”:

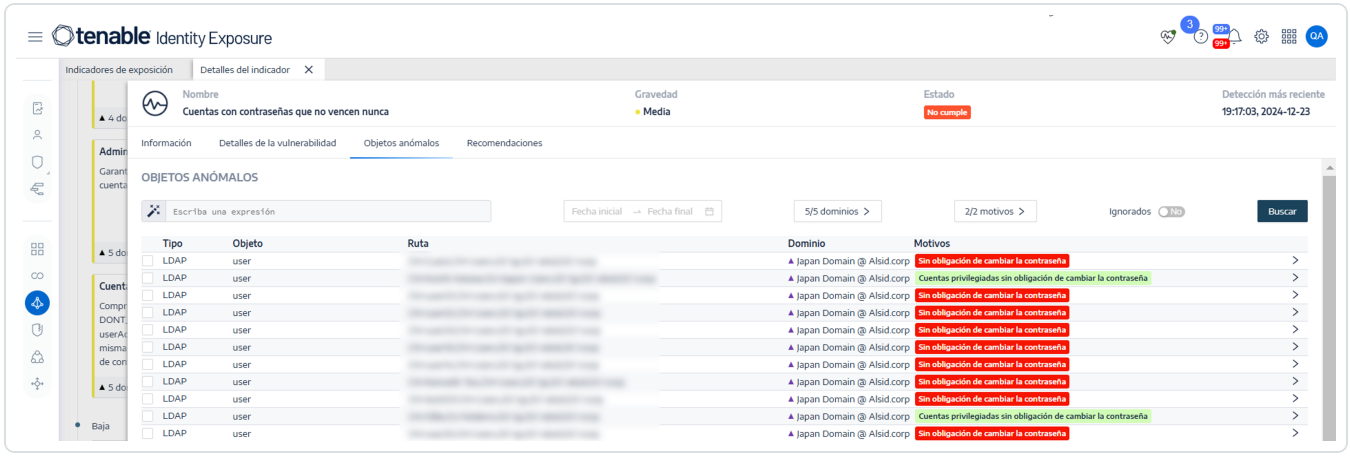


2. Para obtener más información sobre el IoE, haga clic en él para acceder a detalles adicionales. Dentro de la página de información, encontrará un resumen ejecutivo con una descripción general concisa, detalles sobre posibles herramientas de ataque asociadas con el IoE, los dominios afectados y documentación pertinente para ayudarlo a comprender y abordar el problema de manera eficaz.

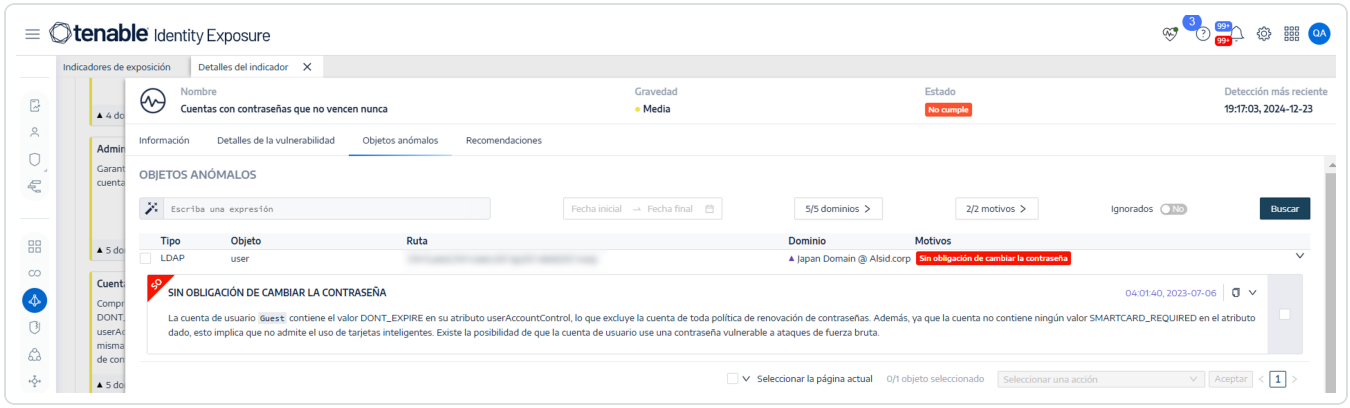
3. 

4. Para obtener más detalles sobre el IoE, haga clic en la pestaña “Detalles de la vulnerabilidad”.

5. Para verificar qué cuentas tienen habilitada la opción “Cuentas con contraseñas que no vencen nunca”, haga clic en “Objetos anómalos”. Esta acción le permitirá acceder a una lista de cuentas que tienen esta configuración dentro de su sistema.

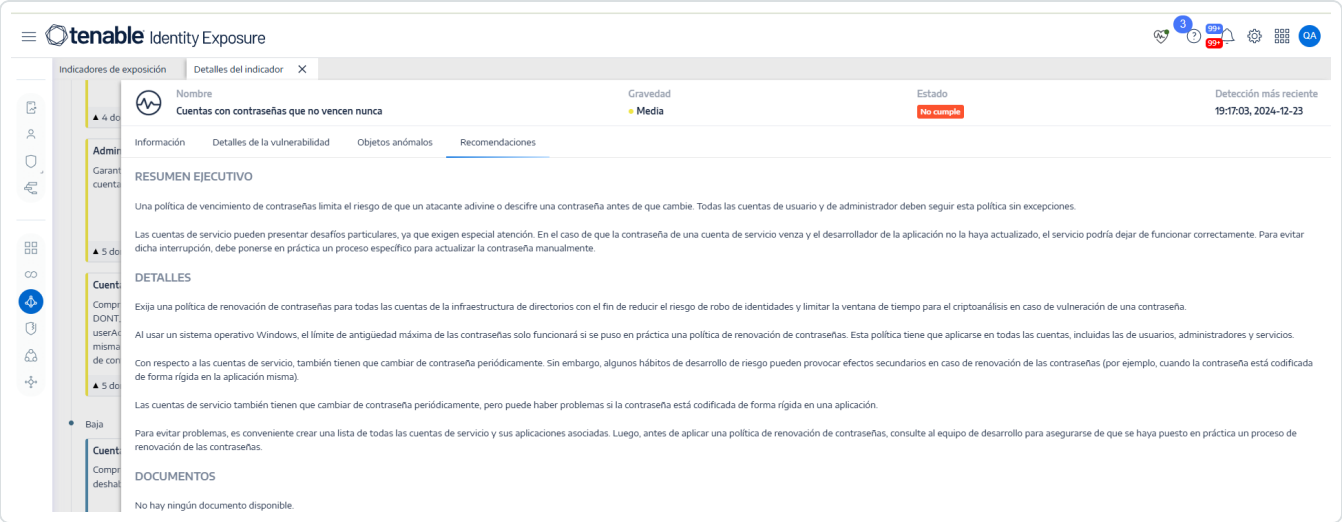


6. Haga clic en el objeto anómalo para ver las cuentas que el IoE marcó.



7. Consulte a su administrador de Active Directory para comprender por qué la cuenta afectada tiene habilitada la opción “Cuentas con contraseñas que no vencen nunca”.

8. Según la respuesta, puede elegir incluir la cuenta en la whitelist o ayudar a su administrador de Active Directory a hacer recomendaciones para solucionar el problema.
9. Para obtener recomendaciones, puede consultar la sección de recomendaciones del IoE.



10. Si la cuenta tiene una excepción o se sabe que funciona según lo esperado, puede ignorar el IoE; para ello, vaya a **Objeto anómalo** > seleccione la anomalía correspondiente > **Ignorar** el objeto seleccionado o dejar de ignorar el objeto seleccionado, según el requisito.

Consulte también

- Indicators of Exposure
- Tutorial en video sobre indicadores de exposición
- Customize an Indicator

Indicadores de ataque

Los indicadores de ataque (IoA) de Tenable Identity Exposure ayudan a su organización a detectar y adoptar medidas inmediatas cuando las técnicas de explotación más avanzadas intentan poner en peligro sus infraestructuras de Active Directory (AD), entre ellas:

- **Tres incidentes principales**: una presentación unificada de IoA muestra una línea temporal en tiempo real junto con los tres principales incidentes que han afectado a su instancia de AD, así como la distribución de los ataques, todo dentro de una única interfaz.
- **Detalles sobre el IoA**: dentro de Tenable Identity Exposure, el panel de IoA brinda información sobre los ataques que han tenido lugar dentro de su instancia de AD.
- **Incidentes que involucran a IoA**: la lista de incidentes de IoA ofrece detalles completos sobre ataques específicos dirigidos a su instancia de AD. Esta información le permitirá responder de manera adecuada según el nivel de gravedad del IoA.

Los indicadores de ataque vienen con una variedad de funcionalidades diseñadas para mejorar sus capacidades de investigación:

- **Búsqueda y filtros**: explore sin esfuerzo el IoA mediante la línea temporal o aplique filtros basados en bosques, dominios y nivel de criticidad para obtener resultados eficientes y segmentados.
- **Capacidad de exportación**: permite la exportación de datos de los IoA en formatos PDF, CSV o PPTX.
- **Modificar el tipo de gráfico**: ofrece la opción de cambiar el tipo de gráfico, lo que le permite mostrar la distribución de la gravedad del ataque o los tres ataques principales junto con el número correspondiente de veces que ocurrieron.
- **Acción sobre incidentes de IoA**: le permite seleccionar un incidente para cerrarlo o reabrirlo.

Nivel de gravedad

Tenable Identity Exposure detecta y asigna niveles de gravedad a los ataques:

Nivel	Descripción
Crítico: rojo	Se detectó un ataque posterior a la explotación probado que requiere la

	dominación del dominio como requisito previo.
Alto: naranja	Se detectó un ataque importante que permite que un atacante logre la dominación del dominio.
Medio: amarillo	El IoA se relaciona con un ataque que podría conducir a un escalamiento peligroso de privilegios o permitir el acceso a recursos confidenciales.
Bajo: azul	Alerta sobre comportamientos sospechosos relacionados con acciones de reconocimiento o incidentes de bajo impacto.

Priorización de la corrección

Reconozca los IoA críticos y de alto impacto que se alinean con sus inquietudes y riesgos de seguridad específicos.

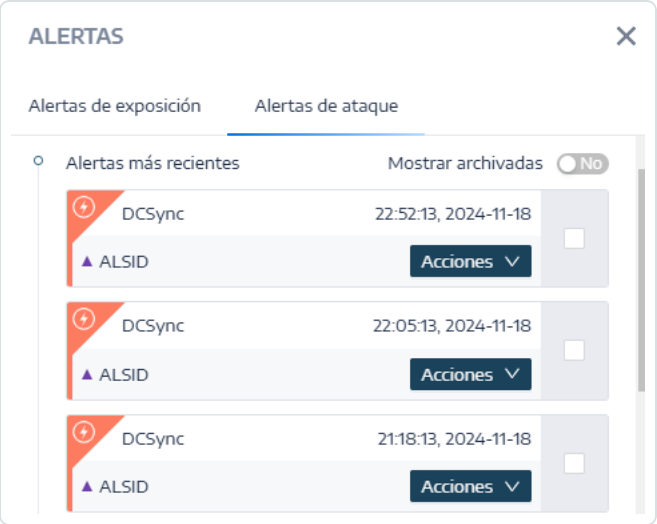
Para mitigar el riesgo de falsos positivos o de pasarse por alto ataques legítimos, es fundamental calibrar los IoA en función del entorno en particular. Esto implica:

- Ajustar los umbrales: calibre la sensibilidad de los IoA para reducir los falsos positivos y garantizar así que las alertas sean pertinentes y puedan atenderse.
- Agregar cuentas y actividades a whitelists: excluya las actividades legítimas para que no activen los IoA, lo que mejora la precisión de las alertas y agiliza las investigaciones.
- Correlacionar los IoA: analice las relaciones entre los distintos IoA para detectar patrones de ataque más amplios.

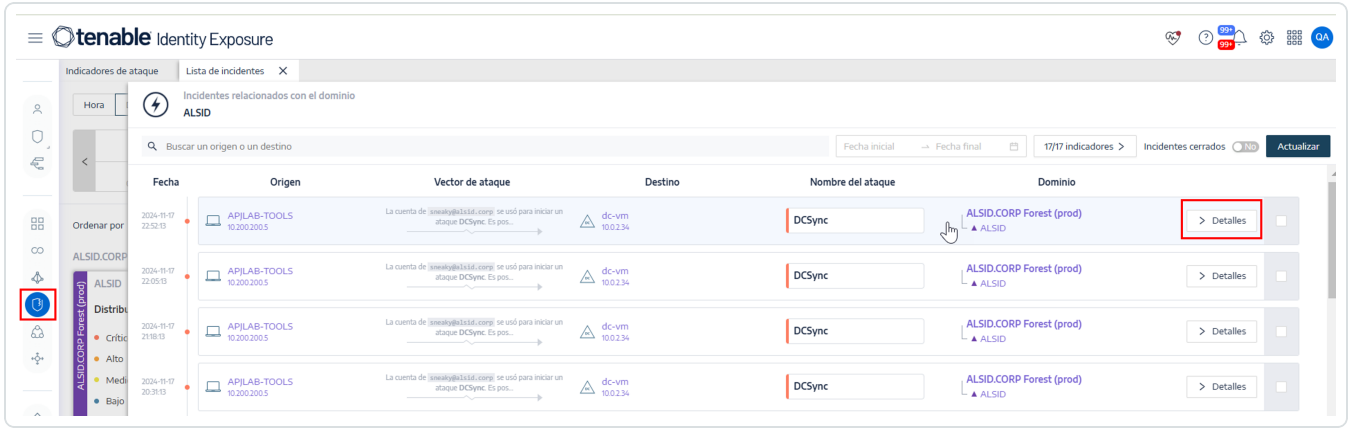
Sugerencia: Consulte Tenable Identity Exposure Indicators of Attack Reference Guide (Guía de referencia de indicadores de ataque de Tenable Identity Exposure) (disponible en https://es-la.tenable.com/downloads/identity-exposure) para obtener más detalles sobre las opciones y los valores recomendados. Aplique estas opciones y valores a cada IoA del perfil de seguridad.

Caso de uso

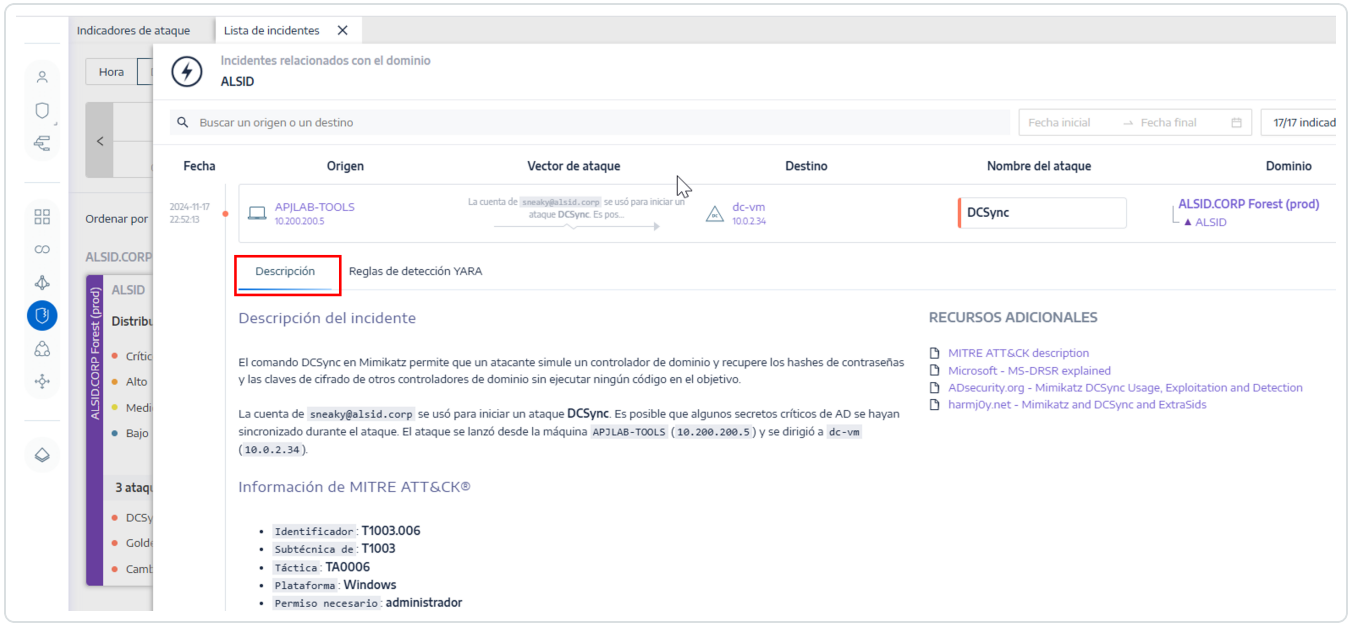
1. Tras activar un IoA, seleccione “Indicadores de ataque” en el panel de navegación o haga clic en el ícono de la campana ubicado en la parte superior derecha de la página de inicio.



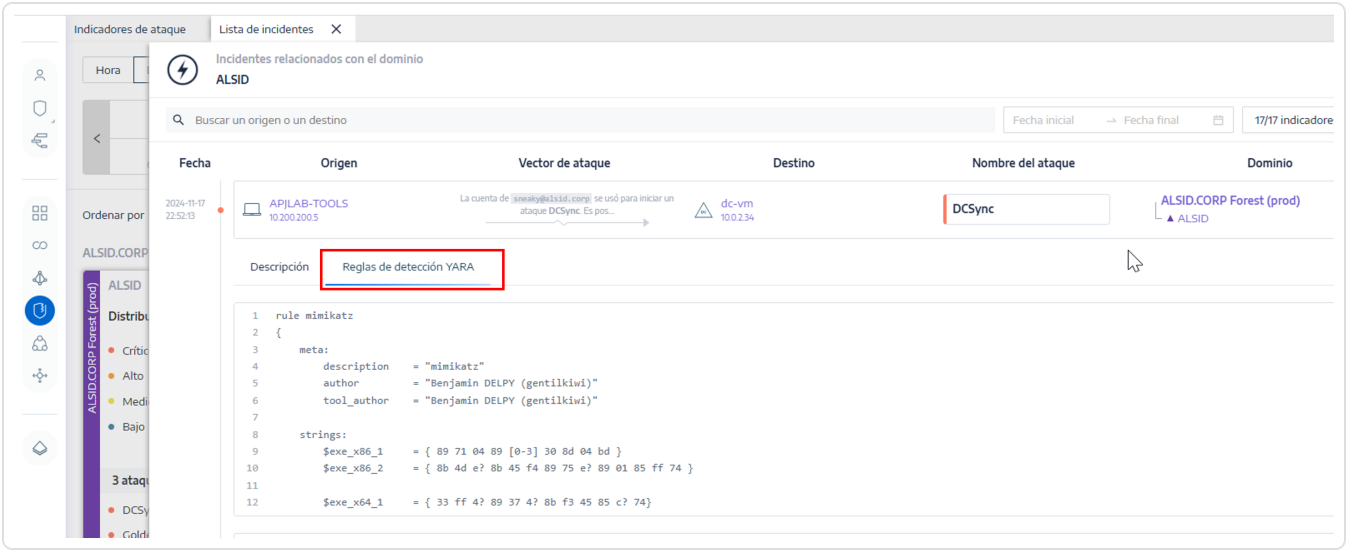
2. Cada indicador le brindará información detallada sobre el incidente y le permitirá tomar las medidas adecuadas después de la revisión:
    - Cuándo tuvo lugar el ataque.
    - Descripción del ataque.
    - Origen del ataque.
    - Objetivo del ataque.
    - Información de MITRE ATT&CK®.
    - Reglas de detección YARA.
    - Recursos adicionales.
3. Seleccione “Detalles” para acceder a la pestaña “Descripción”, como se ilustra en este ejemplo, centrándose en “Enumeración de Administradores locales”.



4. En la pestaña “Descripción” se proporciona información sobre ataques específicos a su instancia de Active Directory (AD).



5. En la pestaña “Reglas de detección YARA” se brinda información sobre las reglas YARA empleadas por Tenable Identity Exposure para detectar ataques a Active Directory en el nivel de red, lo que mejora las capacidades de detección generales de Tenable Identity Exposure.



6. Colabore con el administrador de Active Directory o la parte interesada pertinente para examinar y resolver el incidente, decidir si cerrarlo o reabrirlo e implementar medidas para evitar que vuelva a ocurrir.
7. Si se trata de un ataque reconocido o autorizado, tiene la opción de personalizar el IoA en consecuencia para evitar que este lo marque en instancias futuras.

Consulte también

- Indicators of Attack
- Customize an Indicator
- Tutorial en video sobre indicadores de ataque

Compatibilidad con Microsoft Entra ID

Además de Active Directory, Tenable Identity Exposure admite Microsoft Entra ID (anteriormente, Azure AD o AAD) para ampliar el ámbito de las identidades en una organización. Esta funcionalidad aprovecha nuevos indicadores de exposición que se centran en los riesgos específicos de Microsoft Entra ID.

Para integrar Microsoft Entra ID en Tenable Identity Exposure, siga de cerca este proceso de incorporación:

1. Cumplir con los Requisitos previos.
2. Comprobar los Permisos.
3. Comprobar los Flujos de red.
4. Configurar las opciones de Microsoft Entra ID
5. Activar la compatibilidad con Microsoft Entra ID
6. Habilitar escaneos de inquilinos

Requisitos previos

Necesita una cuenta de Tenable Cloud para iniciar sesión en “cloud.tenable.com” y usar la funcionalidad de compatibilidad con Microsoft Entra ID. Esta cuenta de Tenable Cloud es la misma dirección de correo electrónico usada para el correo electrónico de bienvenida. Si no conoce su dirección de correo electrónico para “cloud.tenable.com”, póngase en contacto con Soporte. Todos los clientes que tengan una licencia válida (local o SaaS) pueden acceder a Tenable Cloud en “cloud.tenable.com”. Esta cuenta le permite configurar los escaneos de Tenable para su instancia de Microsoft Entra ID y recopilar los resultados de los escaneos.

Nota: No necesita una licencia de **Tenable Vulnerability Management** válida para acceder a Tenable Cloud, alcanza con una licencia de Tenable Identity Exposure (local o SaaS) independiente actualmente válida.

Nota: Tenable Identity Exposure **no es compatible con Microsoft Entra ID en las nubes nacionales**, incluidas las áreas dedicadas de los Gobiernos de EE. UU. y China. Microsoft Entra ID ofrece nubes nacionales, que son instancias físicamente aisladas de Azure diseñadas para necesidades normativas y de cumplimiento específicas. Tenable Identity Exposure solo es compatible con el entorno global de Microsoft Entra ID, excluida la nube nacional de China y la nube nacional del Gobierno de EE. UU. Para

obtener más información sobre las nubes nacionales de Microsoft Entra ID, consulte Autenticación Microsoft Entra y nubes nacionales- Microsoft Identity Platform.

Permisos

La compatibilidad de Microsoft Entra ID requiere la recopilación de datos de Microsoft Entra ID, como usuarios, grupos, aplicaciones, entidades de servicio, roles, permisos, políticas, registros, etc. Recopila estos datos mediante Microsoft Graph API y las credenciales de la entidad de servicio siguiendo las recomendaciones de Microsoft.

- Debe iniciar sesión en Microsoft Entra ID como **usuario con permisos para conceder el consentimiento del administrador para todo el inquilino** en Microsoft Graph, que debe tener el rol de Administrador global o Administrador de roles privilegiados (o cualquier rol personalizado con los permisos adecuados), según Microsoft.
- Para acceder a la configuración y a la visualización de datos de Microsoft Entra ID, su **rol de usuario de Tenable Identity Exposure** debe tener los permisos adecuados. Para obtener más información, consulte Set Permissions for a Role.

Flujos de red

Permita las siguientes direcciones en el puerto 443 saliente del servidor de Security Engine Node para activar la compatibilidad con Entra ID:

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

Recuento de licencias

Tenable no cuenta las identidades duplicadas para la licencia **solo cuando la funcionalidad de sincronización de Tenable Cloud está habilitada**. Sin esta funcionalidad, no puede hacer coincidir las cuentas de Microsoft Entra ID y Active Directory, lo que hace que cuente cada cuenta por separado.

- **Sin sincronización de Tenable Cloud**: un único usuario que tenga tanto una cuenta de AD como una cuenta de Entra ID se cuenta como dos usuarios independientes en lo que respecta

a la licencia.

- **Con la sincronización de Tenable Cloud habilitada**: el sistema consolida varias cuentas en una única identidad, lo que garantiza que un usuario que tenga varias cuentas se cuente solo una vez.

Configurar las opciones de Microsoft Entra ID

Siga los procedimientos a continuación (adaptados a partir de la documentación de Microsoft Inicio rápido: Registro de una aplicación en la plataforma de identidad de Microsoft) para configurar todas las opciones necesarias en Microsoft Entra ID.

1. **Crear una aplicación:**

    a. En el portal de administración de Azure, abra la página **Registros de aplicaciones**.

    b. Haga clic en **+ Nuevo registro**.

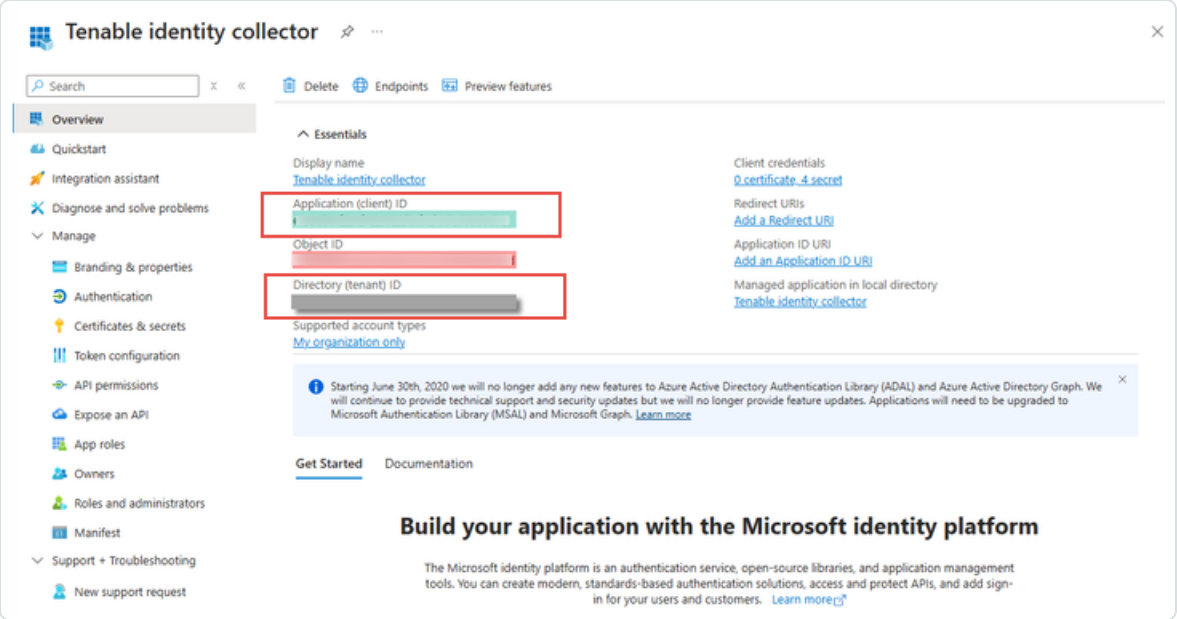
    c. Asigne un nombre a la aplicación (ejemplo: “Tenable Identity Collector”). Para las demás opciones, puede dejar los valores predeterminados tal como están.

    d. Haga clic en **Registrar**.

    e. En la página “Descripción general” de esta aplicación recién creada, anote el “Id. de la aplicación (cliente)” y el “Id. del directorio (inquilino)”, que necesitará más adelante en el paso Para agregar un nuevo inquilino de Microsoft Entra ID:.

    > **Precaución**: Para que la configuración funcione, asegúrese de seleccionar el **Id. de la**

aplicación y no el Id. del objeto.



2. **Agregar credenciales a la aplicación:**

   a. En el portal de administración de Azure, abra la página **Registros de aplicaciones**.

   b. Haga clic en la aplicación que creó.

   c. En el menú de la izquierda, haga clic en **Certificados y secretos**.

   d. Haga clic en **+ Nuevo secreto de cliente**.

   e. En el cuadro **Descripción**, asigne un nombre práctico a este secreto y un valor de **Vencimiento** que cumpla con sus políticas. Recuerde renovar este secreto cerca de su fecha de vencimiento.

   f. Guarde el valor secreto en una ubicación segura, ya que Azure solo lo muestra una vez y debe volver a crearlo si lo pierde.

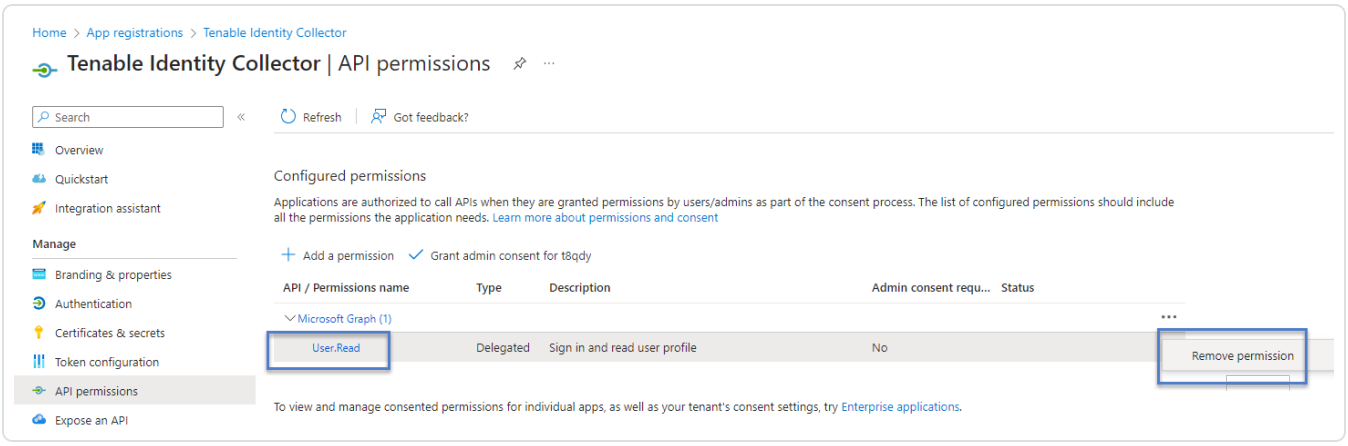
3. **Asignar permisos a la aplicación:**

   a. En el portal de administración de Azure, abra la página **Registros de aplicaciones**.

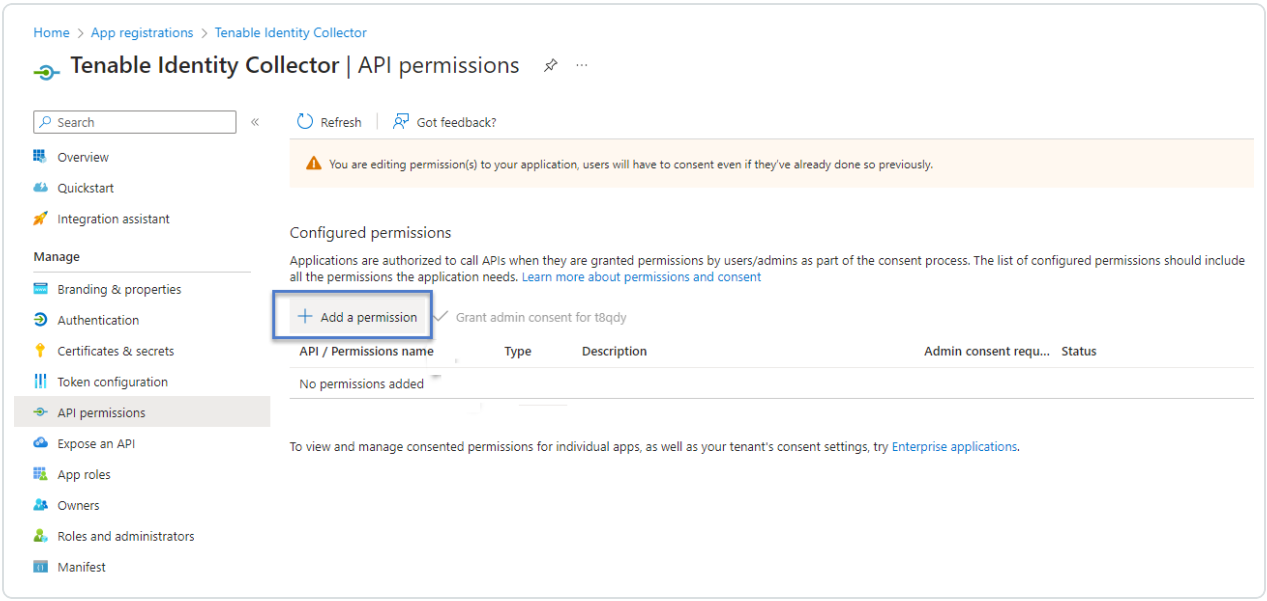
   b. Haga clic en la aplicación que creó.

c. En el menú de la izquierda, haga clic en **Permisos de API**.

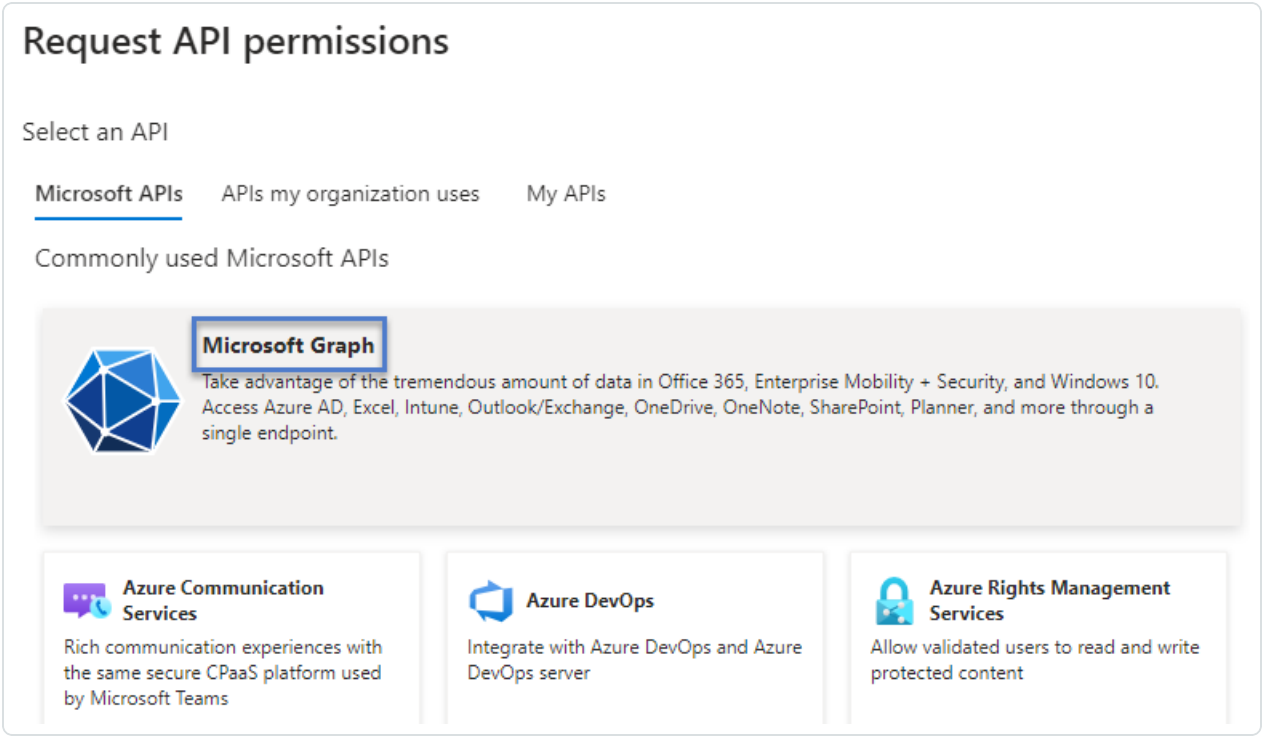
d. Elimine el permiso `User.Read` existente:



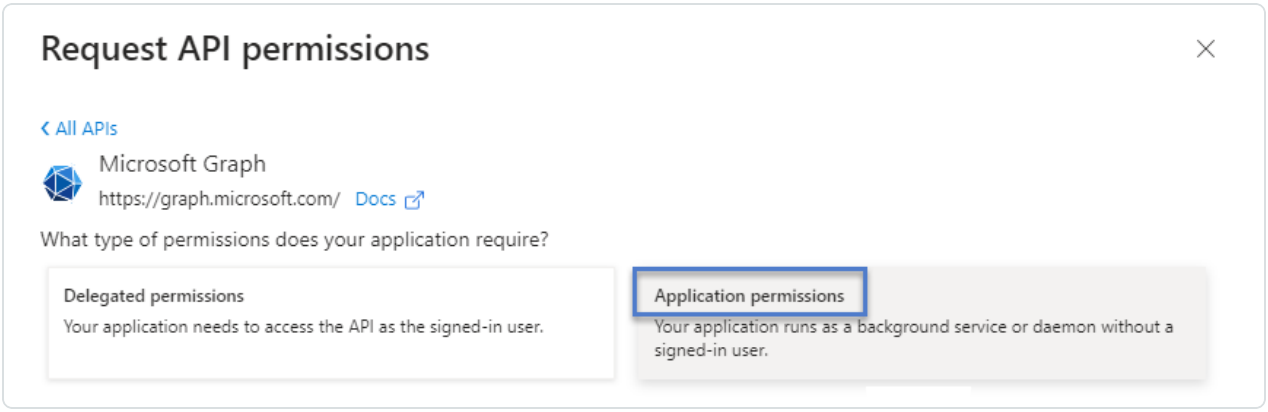
e. Haga clic en **+ Agregar un permiso**:



f. Seleccione **Microsoft Graph**:



g. Seleccione **Permisos de aplicación** (no “Permisos delegados”).



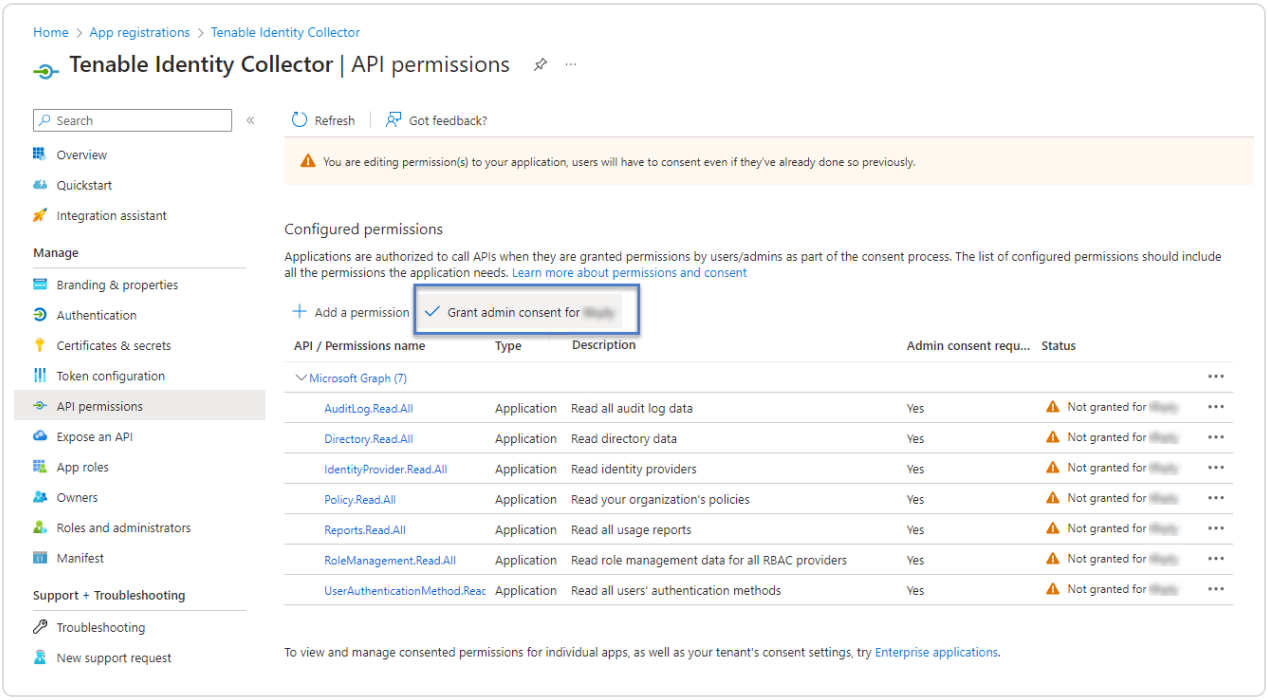
h. Use la lista o la barra de búsqueda para buscar y seleccionar todos los permisos siguientes:

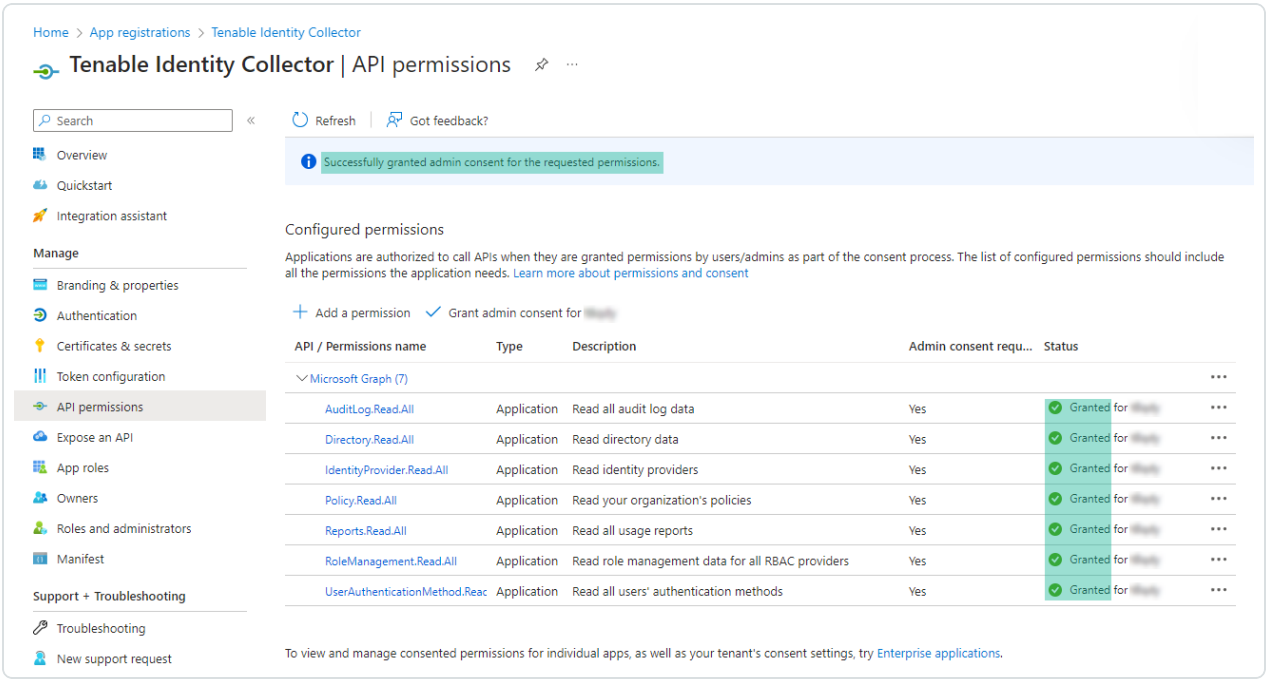
   - `AuditLog.Read.All`
   - `Directory.Read.All`
   - `IdentityProvider.Read.All`
   - `Policy.Read.All`

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

i. Haga clic en **Agregar permisos**.

j. Haga clic en **Otorgar consentimiento de administrador a <nombre del inquilino>** y haga clic en **Sí** para confirmar:





4. Después de configurar todas las opciones obligatorias en Microsoft Entra ID:
    a. En Tenable Vulnerability Management, cree una nueva credencial de tipo “Microsoft Azure”.
    b. Seleccione el método de autenticación “Clave” e ingrese los valores que recuperó en el procedimiento anterior: ID de inquilino, ID de aplicación y Secreto de cliente.

Activar la compatibilidad con Microsoft Entra ID

- Para usar **Microsoft Entra ID**, tiene que activar la funcionalidad en la configuración de Tenable Identity Exposure.
- Para obtener instrucciones, consulte Identity 360, Exposure Center, and Microsoft Entra ID Support Activation .

Habilitar escaneos de inquilinos

Para agregar un nuevo inquilino de Microsoft Entra ID:

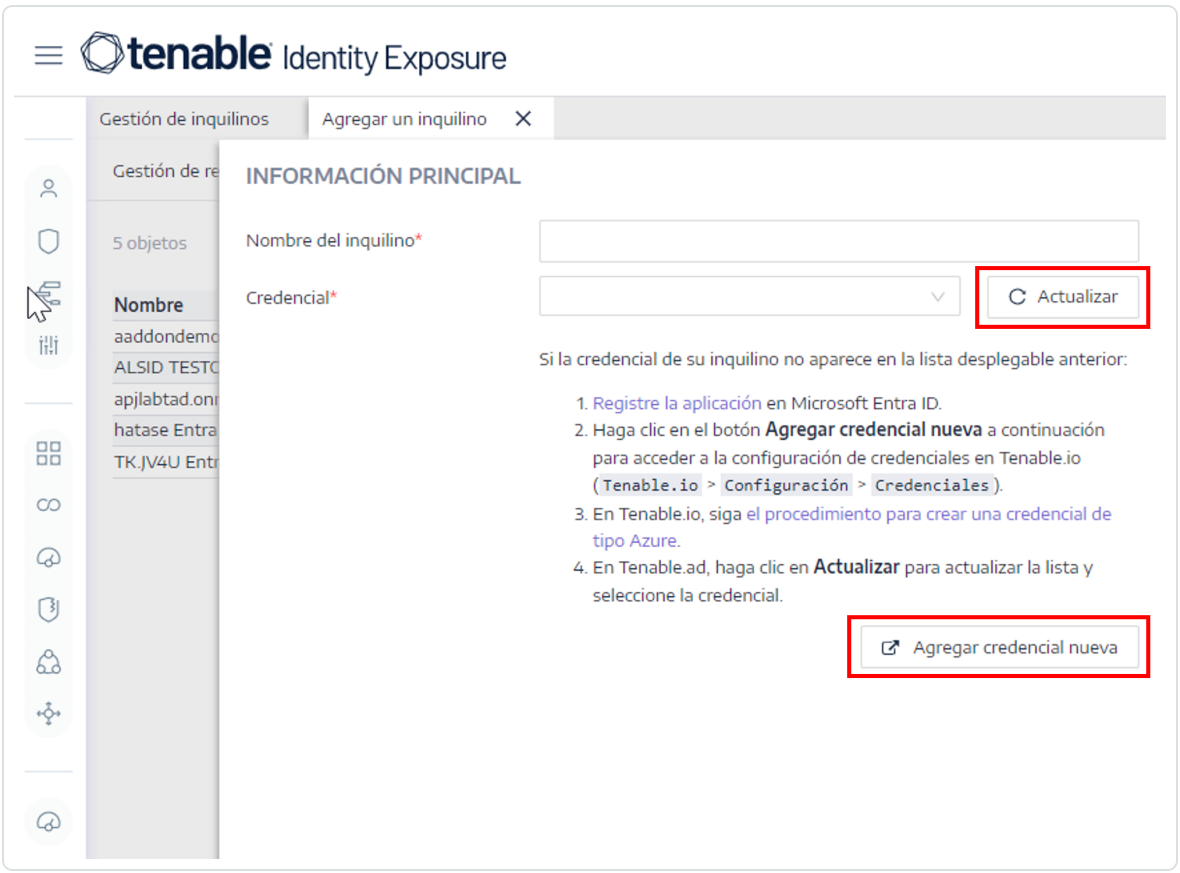
Al agregar un inquilino, se vincula Tenable Identity Exposure con el inquilino de Microsoft Entra ID para realizar escaneos en ese inquilino.

1. En la página “Configuración”, haga clic en la pestaña **Gestión de inquilinos**.

    Se abre la página **Gestión de inquilinos**.

2. Haga clic en **Agregar un inquilino**.

    Se abre la página **Agregar un inquilino**.



3. En el cuadro **Nombre del inquilino**, escriba un nombre.
4. En el cuadro **Credenciales**, haga clic en la lista desplegable para seleccionar una credencial.
5. Si la credencial no aparece en la lista, puede:
    - Crear una en Tenable Vulnerability Management (Tenable Vulnerability Management > **Configuración** > **Credenciales**). Para obtener más información, consulte el procedimiento para crear una credencial de tipo Azure en Tenable Vulnerability Management.
    - Comprobar que tiene el permiso “Puede usar” o “Puede editar” para la credencial en Tenable Vulnerability Management. A menos que tenga estos permisos, Tenable Identity Exposure no muestra la credencial en la lista desplegable.
6. Haga clic en **Actualizar** para actualizar la lista desplegable de las credenciales.
7. Seleccione la credencial que creó.
8. Haga clic en **Agregar**.

Un mensaje confirma que Tenable Identity Exposure agregó el inquilino, que ahora aparece en la lista de la página “Gestión de inquilinos”.

Para habilitar escaneos para el inquilino:

Nota: Los escaneos de inquilinos no se producen en tiempo real y necesitan al menos 45 minutos para que los datos de Microsoft Entra ID se puedan ver en el Explorador de identidades.

- Seleccione un inquilino de la lista y haga clic en el conmutador para **Escaneo habilitado**.

Tenable Identity Exposure solicita un escaneo del inquilino, y los resultados aparecen en la página “Indicador de exposición”.

Nota: El tiempo mínimo obligatorio de retraso entre dos escaneos es de **30 minutos**.

Ruta de ataque

Tenable Identity Exposure ofrece varias maneras de visualizar la vulnerabilidad potencial de un activo empresarial a través de representaciones gráficas.

- **Ruta de ataque**: muestra las posibles rutas que puede tomar un atacante para poner en riesgo un activo desde un punto de entrada.
- **Radio de ataque**: muestra los posibles movimientos laterales en la instancia de Active Directory desde cualquier activo.
- **Exposición de los activos**: muestra todas las rutas que potencialmente pueden tomar el control de un activo.

Comprender la ruta de ataque le permitirá detectar los pasos de mitigación necesarios para evitar que los atacantes exploten las vulnerabilidades. Esto podría implicar la colocación de parches en los sistemas, el endurecimiento de las configuraciones, la implementación de controles de acceso más estrictos o la generación de conciencia entre los usuarios.

Beneficios de utilizar las rutas de ataque en Tenable Identity Exposure:

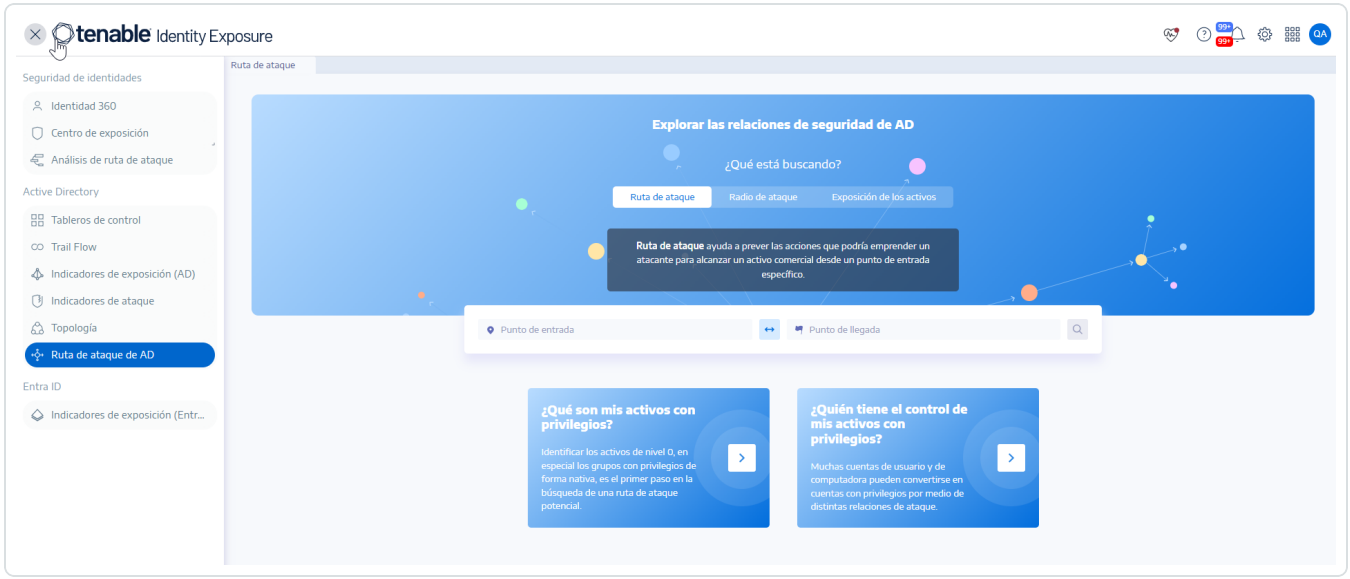
- **Seguridad proactiva**: ayuda a prever y abordar posibles vectores de ataque antes de que se exploten.
- **Priorización**: orienta a centrar los esfuerzos de seguridad en las vulnerabilidades y rutas de ataque más críticas.
- **Visualización**: ofrece una representación clara y fácil de entender de las relaciones de seguridad complejas dentro de la instancia de AD.
- **Comunicación**: facilita la comunicación de los riesgos de seguridad a las partes interesadas al ofrecer evidencia visual de posibles escenarios de ataque.

Para mostrar la ruta de ataque:

Especifique el punto de entrada, que podría ser cualquier activo de la instancia de AD (por ejemplo, una cuenta de usuario, un equipo o un grupo). Defina el punto de llegada, que representa el activo que el atacante pretende poner en peligro en última instancia (por ejemplo, un controlador de dominio o un servidor de datos confidenciales).

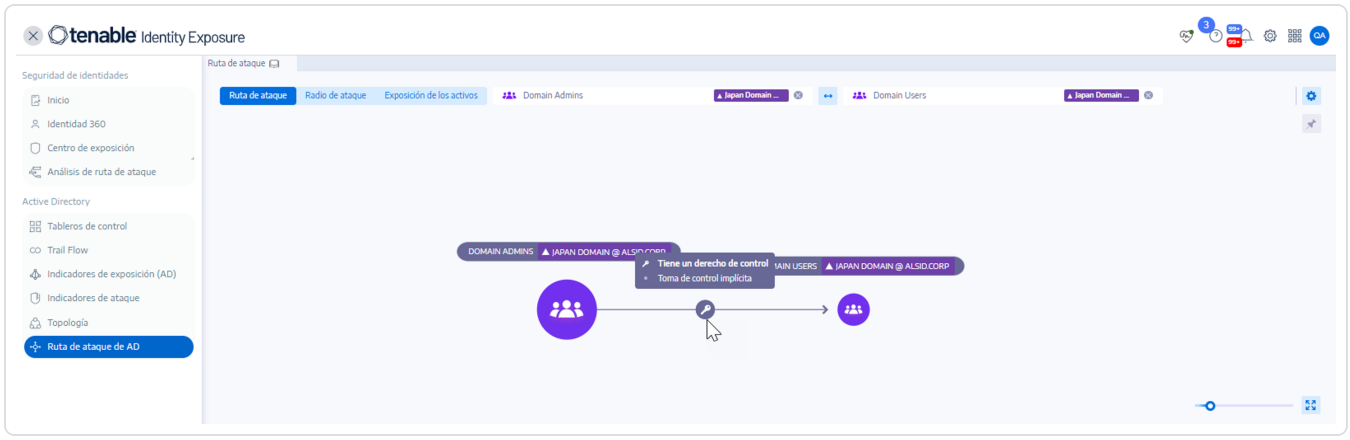
1. En Tenable Identity Exposure, haga clic en **Ruta de ataque** en el menú de la barra lateral.

   Aparece el panel **Ruta de ataque**.



2. En el banner, haga clic en **Ruta de ataque**.
3. En el cuadro **Punto de entrada**, escriba el activo del punto de entrada.
4. En el cuadro **Punto de llegada**, escriba el activo del final de la ruta.
5. Haga clic en el ícono  .

   Tenable Identity Exposure muestra la ruta de ataque entre los dos activos.



6. De manera opcional, puede hacer clic en el ícono  para lo siguiente:

- Hacer clic en el control deslizante **Zoom** para ajustar la ampliación de los gráficos.
- Hacer clic en el conmutador **Mostrar toda la información sobre herramientas de nodos** para ver la información sobre los activos.

Para mostrar el radio de ataque:

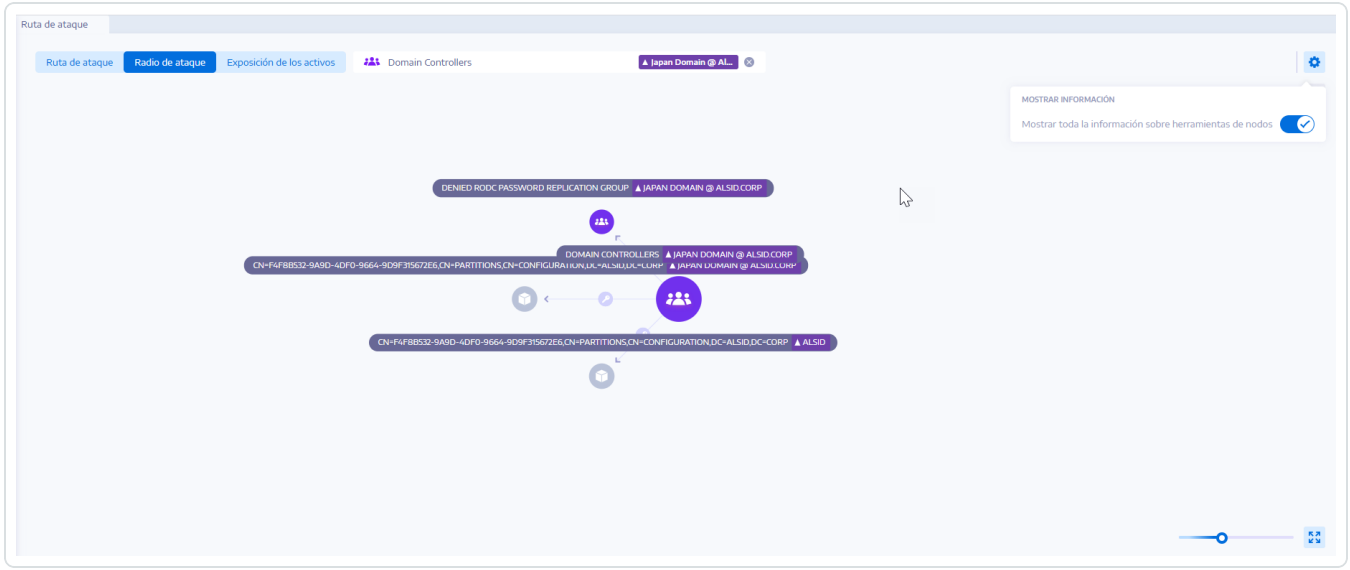
Tenable Identity Exposure muestra una representación gráfica de la ruta de ataque potencial, donde se resaltan las conexiones entre los activos. Cada conexión representa una vulnerabilidad potencial o un error de configuración que un atacante podría aprovechar para moverse lateralmente dentro de la instancia de AD. Puede acercar o alejar la imagen para comprender mejor los detalles de la ruta.

1. En Tenable Identity Exposure, haga clic en **Ruta de ataque** en el menú de la barra lateral.

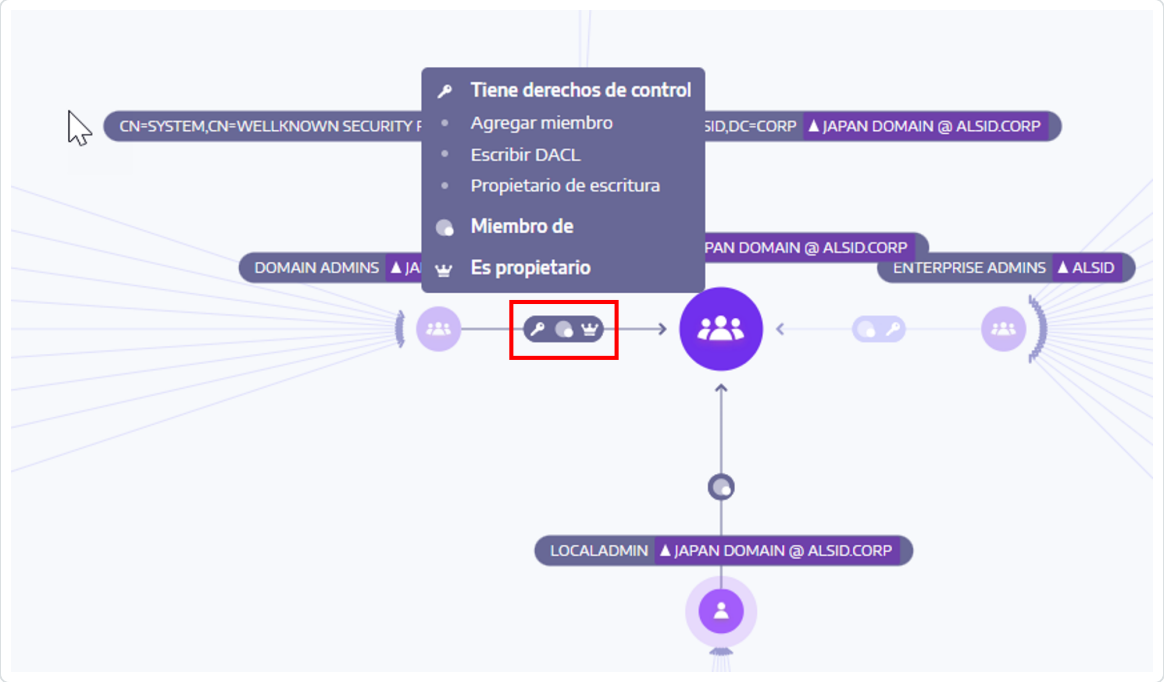
   Aparece el panel **Ruta de ataque**.

2. En el banner, haga clic en **Radio de ataque**.
3. En el cuadro **Buscar un objeto**, escriba el nombre de un activo.
4. Haga clic en el ícono .

   Tenable Identity Exposure muestra las conexiones laterales que salen de ese activo:



5. Haga clic en los íconos en las flechas entre los activos para mostrar las relaciones entre ellos.



Para visualizar la exposición de los activos:

Cada paso en la ruta de ataque se asocia a una puntuación de riesgo, que indica la gravedad de la vulnerabilidad. Esto lo ayuda a priorizar qué rutas representan la amenaza más importante y requieren atención inmediata. También puede hacer clic en puntos de conexión individuales para obtener más detalles sobre la vulnerabilidad o el error de configuración específicos relacionados.

1. En Tenable Identity Exposure, haga clic en **Ruta de ataque** en el menú de la barra lateral.

   Aparece el panel **Ruta de ataque**.

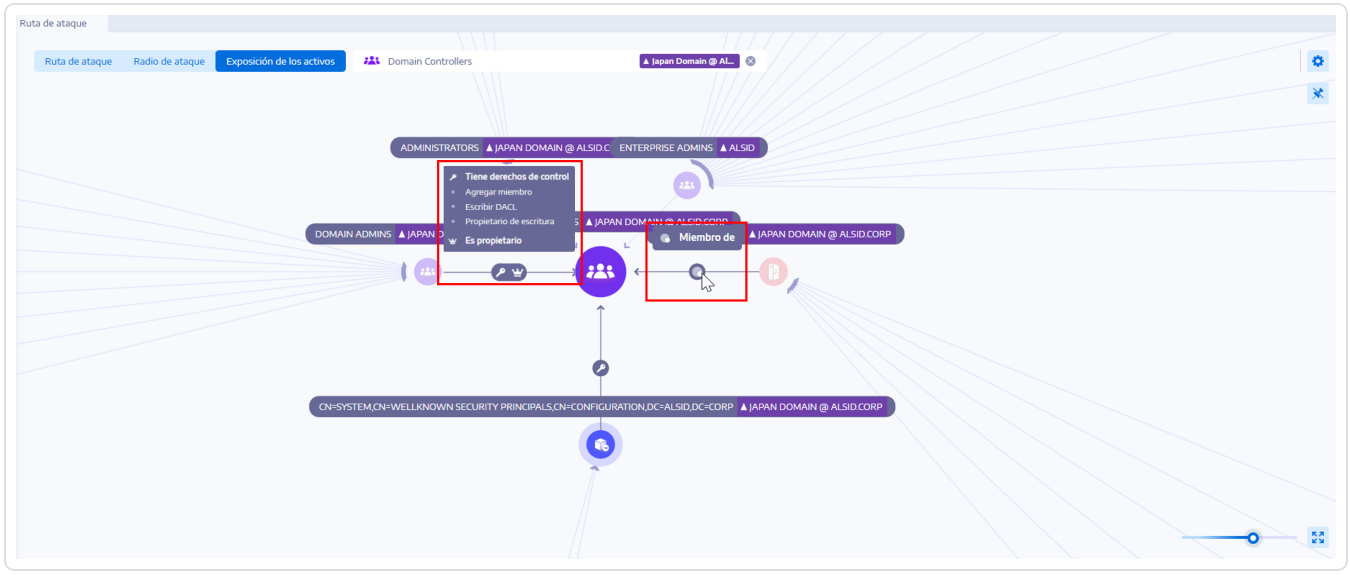
2. En el banner, haga clic en **Exposición de los activos**.

3. En el cuadro **Buscar un objeto**, escriba el nombre de un activo.

4. Haga clic en el ícono .

   Tenable Identity Exposure muestra las rutas que conducen al activo y las relaciones entre los activos.

5. Haga clic en los íconos en las flechas entre los activos para mostrar las relaciones entre ellos.



Para anclar una ruta de ataque:

Consulte también

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

Gestión de usuarios

Aspectos clave

- **Roles**: los roles predeterminados incluyen Administrador, Analista de seguridad, Usuario e Invitado, cada uno con diferentes permisos. Los roles personalizados permiten un control detallado para satisfacer necesidades específicas.
- **Permisos**: los permisos definen qué pueden hacer los usuarios dentro de Tenable Identity Exposure, así como a qué partes pueden acceder. Van desde la visualización de informes y tableros de control, pasando por la gestión de usuarios y la configuración de indicadores, hasta la realización de acciones, como deshabilitar cuentas.
- **Ámbito**: Tenable Identity Exposure permite delimitar permisos para dominios o grupos específicos o, incluso, objetos individuales dentro de Active Directory. Esto garantiza que los usuarios solo accedan a datos pertinentes en función de su rol y responsabilidades.

Beneficios

- **Seguridad mejorada de Active Directory**: el control de acceso detallado minimiza el riesgo de acceso no autorizado a datos de identidad confidenciales.
- **Eficiencia y flujos de trabajo mejorados**: los usuarios tienen acceso a las herramientas y los datos que necesitan, lo que agiliza las investigaciones y la respuesta ante incidentes.
- **Cumplimiento de normas**: el control de acceso basado en roles ayuda a satisfacer los requisitos de cumplimiento para la gestión de identidades y acceso dentro de Active Directory.

Consulte también

- User Roles

Integración de Tenable Identity Exposure

Integre Tenable Identity Exposure en su solución de SIEM, SOC o SOAR para lograr supervisión, respuestas automatizadas y una mejor gestión de las alertas en tiempo real.

Supervisión en tiempo real con la integración de SYSLOG

Obtenga alertas instantáneas para indicadores de exposición (IoE) críticos a través de la integración fluida de SYSLOG.

Beneficios clave

- **Registro centralizado**: agrupe eventos de Tenable Identity Exposure con otras soluciones de seguridad para un análisis integral.
- **Notificaciones en tiempo real**: reciba notificaciones inmediatas sobre posibles exposiciones de identidad y ataques.
- **Gestión de seguridad mejorada**: correlacione eventos de diferentes orígenes para identificar amenazas complejas más rápidamente.
- **Visibilidad de SIEM mejorada**: integre los datos de Tenable Identity Exposure sin problemas en su SIEM para mejorar el conocimiento de la situación y el análisis de correlaciones.
- **Flujo de trabajo optimizado**: automatice la clasificación y la respuesta de alertas en función de los datos de SYSLOG para optimizar las operaciones de seguridad.

Ejemplo de IoE para supervisión en tiempo real

- **Errores de configuración peligrosos de AD CS**: detecta o identifica cambios en los servidores de certificados de AD que puedan indicar ataques “Certified Pre-owned”.
- **Sanidad de la ejecución de GPO**: detecta e identifica intentos de instalar puertas traseras a través de la ejecución de scripts dentro de políticas de grupo.
- **Usuarios con permiso para unir equipos al dominio**: reconozca la adición de equipos no autorizados al dominio, un ataque previo característico de los ataques de puerta trasera “RBCD”.

Automatización de la respuesta con plataformas de SOAR

Aproveche las plataformas de orquestación, automatización y respuesta de seguridad (SOAR) existentes para ejecutar acciones de corrección automatizadas en función de los datos de TIE. Los principales beneficios son los siguientes:

- **Mitigación rápida**: minimice el tiempo de inactividad y los efectos al automatizar las respuestas a los IoE críticos.
- **Eficiencia mejorada**: libere a los equipos de seguridad de tareas repetitivas, lo que les permite centrarse en iniciativas de seguridad estratégicas.
- **Medidas de seguridad mejoradas**: aborde de forma proactiva los errores de configuración detectados y fortalezca su estado de seguridad general.

Importante: La resolución de problemas o la asistencia en el script de automatización están fuera del alcance del soporte de Tenable. Para obtener asistencia, comuníquese con nuestro equipo de Professional Services.