HOJA DE DATOS

SEGURIDAD PREVENTIVA PARA LA EXPOSICIÓN DE IDENTIDADES

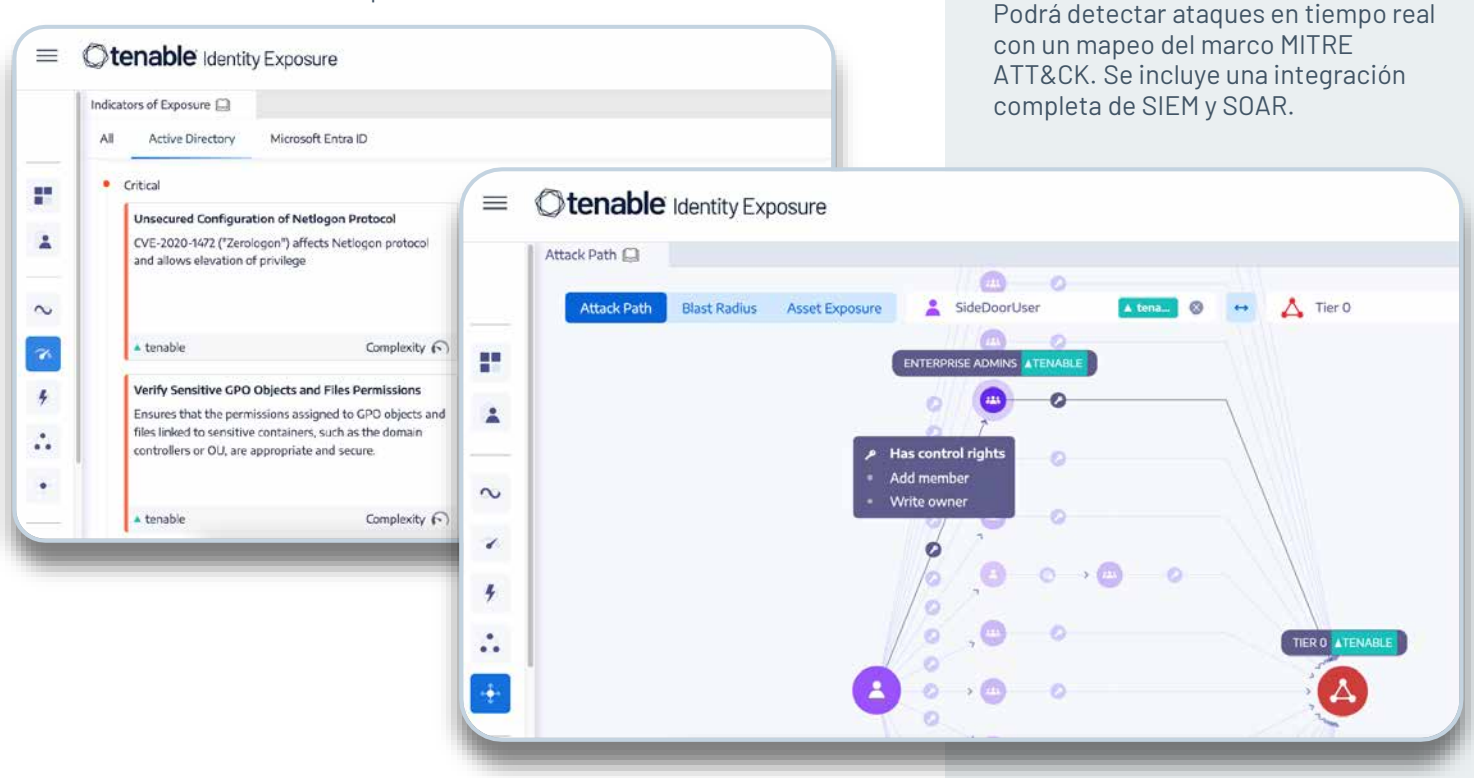
tenable Identity Exposure

Las identidades en riesgo son la base de casi todos los ataques a la ciberseguridad que llegan a concretarse. Active Directory y Entra ID (antes conocidos como Azure AD) son objetivos comunes para los atacantes que logran el control del dominio mediante herramientas comerciales para explotar las relaciones complejas entre los objetos, los permisos y las entidades.

Los cambios constantes en los servicios de directorio también limitan la visibilidad hacia toda la superficie de ataque y, continuamente, crean nuevas rutas de ataque. Pocos equipos de seguridad tienen la visibilidad y el contexto suficientes para proteger la superficie de ataque completa de los servicios de directorio, y las herramientas que suelen utilizar solo proporcionan un snapshot; por eso, la seguridad se vuelve un objetivo en movimiento.

Aún peor, según el informe sobre el costo de una filtración de datos de IBM de 2022, el tiempo promedio en el que se detecta una filtración que involucra credenciales en riesgo es 243 días y el tiempo promedio para contenerla es 84 días. Esto significa que un atacante exitoso puede tener alrededor de un año para desestabilizar el servicio más crítico de las empresas modernas.

Tenable Identity Exposure es una solución de seguridad sin agentes que continuamente evalúa la postura de seguridad de sus servicios de directorio y lo alerta de inmediato cuando estos están bajo ataque. Además, esta solución proporciona una guía de mitigación paso a paso que establece prioridades, califica sus identidades de mayor riesgo con una puntuación del riesgo impulsada por IA y ofrece una visualización de la ruta de ataque.



BENEFICIOS PRINCIPALES

Predicción y priorización

Califique a cada identidad con una puntuación del riesgo y priorice la corrección de configuraciones inseguras donde más importa.

Visibilidad completa

Elimine las configuraciones riesgosas de hace mucho tiempo. Visualice el dominio complejo y las relaciones de bosques.

Visualización de rutas de ataque

Elimine las rutas de ataque con un mapeo en tiempo real de las rutas que dan lugar al control de dominio.

No intrusivo

Obtenga resultados instantáneos con una implementación rápida y sin inconvenientes que no requiere agentes ni privilegios administrativos.

Detección de ataques instantánea

Podrá detectar ataques en tiempo real con un mapeo del marco MITRE ATT&CK. Se incluye una integración completa de SIEM y SOAR.

CAPACIDADES PRINCIPALES

Unificación de identidades y puntuación del riesgo impulsada por IA

Unifique las cuentas híbridas, de Active Directory y de Entra ID en una única vista. Controle las identidades dispersas entre varios servicios de directorio, dominios y bosques desde un único lugar. Nuestro motor de IA y ciencia de datos califica cada identidad, y las puntúa según el nivel de riesgo en el que se pueden encontrar.

Evaluación continua de la seguridad de los servicios de directorio en tiempo real

Evalúe la postura de seguridad de sus servicios de directorio y descubra las vulnerabilidades, las configuraciones riesgosas y los permisos.
Tenable Identity Exposure ofrece una guía táctica paso a paso en la que se identifican los objetos afectados, que elimina la necesidad de consultar guiones o informes manuales que requieren mucho tiempo.

Eliminación de las rutas de ataque que dan lugar al control de dominio

Comprenda las interrelaciones complejas entre los objetivos, las entidades de seguridad y los permisos, y elimine las rutas de ataque que dan lugar al control del dominio. Attack Path Analysis (Análisis de ruta de ataque) cubre todos los posibles pasos de los atacantes para moverse lateralmente, escalar privilegios y controlar sus servicios de directorios de empresas.

Detección de ataques en tiempo real

Reciba alertas instantáneas cuando ocurra un ataque, incluyendo el volcado de credenciales, Kerberoasting, DCSync, ZeroLogon y muchas más. Responda a ataques en tiempo real mediante la integración de Tenable Identity Exposure con su SIEM y SOAR. El equipo de investigación de Tenable actualiza con regularidad los indicadores de ataque a medida que se detectan nuevos exploits basados en identidades.

Investigación e información

Reduzca el tiempo de respuesta ante incidentes y registre todos los cambios en Active Directory con el flujo de registros. Informe a sus equipos de respuesta ante incidentes y refuerce los procesos de operaciones de seguridad con una priorización en tiempo real y pasos de corrección detallados.

Tenable One: gestión de exposición con reconocimiento de identidad

Tenable Identity Exposure permite la gestión de exposición con reconocimiento de identidad y es una parte fundamental de la plataforma de gestión de exposición Tenable One. La gestión de exposición con reconocimiento de identidad lo ayuda a comprender dónde centrar sus esfuerzos de prevención para reducir el riesgo de que una filtración tenga éxito. Descomponga los silos entre los sistemas de datos de empresas y relacione la información sobre el riesgo de la identidad y la vulnerabilidad en toda la empresa con el poder de Tenable.

Respaldado por Tenable Research

Con regularidad, nuestro equipo de investigación de primer nivel agrega nuevos indicadores de exposición y detecciones de ataques a Tenable Identity Exposure. Se detectan vulnerabilidades de día cero, se desarrollan pasos de corrección y boletines de seguridad, y se publican resúmenes e información sobre la inteligencia.

Acerca de Tenable

Tenable® es la empresa de Exposure Management. Aproximadamente 43 000 organizaciones de todo el mundo confían en que Tenable ayuda a comprender el riesgo cibernético y a reducirlo. Como creador de Nessus®, Tenable amplió su conocimiento sobre vulnerabilidades para ofrecer la primera plataforma del mundo para ver y proteger los activos digitales en cualquier plataforma de cómputo. Entre los clientes de Tenable, se incluye aproximadamente al 60 % de las compañías de la lista Fortune 500, aproximadamente el 40 % de las compañías de la lista Global 2000 y grandes instituciones gubernamentales. Para obtener más información, visite es-la.tenable.com.

COPYRIGHT 2023 TENABLE, INC. TODOS LOS DERECHOS RESERVADOS. TENABLE, TENABLE.IO, NESSUS, ALSID, INDEGY, LUMIN, ASSURE Y LOG CORRELATION ENGINE SON MARCAS REGISTRADAS DE TENABLE, INC. O SUS FILIALES. TENABLE.SC, TENABLE.OT, TENABLE.AD, EXPOSURE.AI Y TENABLE.ASM SON MARCAS REGISTRADAS DE TENABLE, INC. O SUS FILIALES. EL RESTO DE LOS PRODUCTOS O SERVICIOS SON MARCAS REGISTRADAS DE SUS RESPECTIVOS PROPIETARIOS.