



Zscaler ITDR™

Ventajas de Zscaler ITDR

Reduzca la superficie expuesta a ataques de identidad

Obtenga visibilidad de las configuraciones erróneas de identidad que permiten a los adversarios escalar privilegios y moverse lateralmente.

Detecte ataques de identidad

Detenga las amenazas de identidad sigilosas como DCSync, DCShadow y kerberoasting que eluden las defensas existentes.

Mitigue el riesgo de identidad

Mida y controle su postura de superficie de ataque de identidad utilizando puntuaciones de riesgo generadas por la evaluación de seguridad de identidad.

¿Qué es Zscaler ITDR?

Debido a la rápida adopción de la confianza cero, los atacantes centran su objetivo en los usuarios y las identidades para usarlos como puerta de entrada y emplear ese acceso para ampliar privilegios y moverse lateralmente. Zscaler ITDR brinda visibilidad continua de configuraciones incorrectas de identidad y permisos arriesgados. Aumenta esta visibilidad con orientación en forma de tutoriales en vídeo, scripts y comandos para remediar estos problemas y reducir su superficie de ataque interna.

Además de capacidades preventivas, Zscaler ITDR también proporciona detecciones de alta fidelidad para ataques basados en identidad, como credenciales robadas, desvíos de autenticación multifactor y técnicas de escalada de privilegios, que generalmente atraviesan las defensas existentes cuando se dan casos de compromiso de identidad.

¿Por qué Zscaler ITDR?

-  **No se requieren agentes/máquinas virtuales adicionales**
 Integrado en Zscaler Client Connector, Zscaler ITDR desbloquea nuevas capacidades y protecciones listas para usar.
-  **Integrado con la política de acceso**
 Zscaler Zero Trust Exchange puede aplicar dinámicamente controles de política de acceso para bloquear a los usuarios comprometidos cuando se detecta un ataque de identidad.
-  **Integraciones de SOC**
 Fortalezca la investigación y la respuesta con integraciones que incluyen EDR como CrowdStrike, Microsoft Defender, VMware CarbonBlack y todos los SIEM líderes.

Capacidades clave

... Descubre problemas que permiten a los atacantes ganar ventaja

Descubra configuraciones arriesgadas como exposición de contraseñas GPP, delegación sin restricciones y contraseñas obsoletas que abren nuevas rutas de ataque.

... Desarrolle una sólida higiene de identidad con orientación de remediación

Comprenda el problema, el impacto y quién se ve afectado. Aproveche la guía de corrección paso a paso junto con tutoriales en vídeo, scripts y comandos.

... Reciba alertas cuando los cambios de configuración presenten algún riesgo

Los sistemas de identidad se modifican constantemente con los cambios de configuración y permisos. Supervise en tiempo real y reciba alertas sobre nuevos riesgos y problemas.

... Detenga la escalada de privilegios con detección de amenazas de identidad

No todas las configuraciones incorrectas se pueden remediar. Detecte y detenga ataques como DCSync, DCShadow, kerberoasting y más en caso de compromiso.

Casos de uso

Visibilidad de la superficie de ataque de identidad

- Puntuación de riesgo para la cuantificación y el seguimiento de la postura de identidad
- Descubrimiento de los principales problemas de identidad y los usuarios/hosts de mayor riesgo
- Asignación de MITRE ATT&CK para obtener visibilidad de los puntos ciegos de seguridad

Gestión de la higiene de identidad

- Identificación de nuevas configuraciones erróneas a medida que surgen
- Alertas en tiempo real de nuevos riesgos en su almacén de identidad
- Orientación, comandos y scripts para la remediación listos para usarse

Detección y respuesta a amenazas de identidad

- Detección de ataques contra su almacén de identidades
- Detención de kerberoasting, DCSync, enumeración LDAP y más
- Contención integrada que emplea la política de acceso de confianza cero

Visite nuestra página web para obtener más información sobre Zscaler ITDR.

 | Experience your world, secured.™

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en zscaler.es o síganos en Twitter [@zscaler](https://twitter.com/zscaler).

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

© 2023 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas comerciales que aparecen en zscaler.es/legal/trademarks son (i) marcas comerciales o marcas de servicio registradas o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/o en otros países. Cualquier otra marca comercial es propiedad de sus respectivos propietarios.

zscaler.es