Zscaler ITDR™

Beneficios de Zscaler ITDR

Reducción de la superficie de ataque a la identidad
Consiga visibilizar las configuraciones erróneas de identidad que permiten a los adversarios escalar privilegios y moverse lateralmente.

Detección de los ataques a la identidad
Detenga las amenazas a la identidad como DCSync, DCShadow y kerberoasting que eluden las defensas existentes.

Mitigación del riesgo de identidad
Mida y supervise su postura ante la superficie de ataque de la identidad utilizando los avisos de riesgo generados por la evaluación de la seguridad de la identidad.

¿Qué es Zscaler ITDR?

Con la rápida adopción de un enfoque zero trust, los atacantes eligen a usuarios e identidades como punto de entrada y utilizan ese acceso para escalar privilegios y moverse lateralmente. Zscaler ITDR ofrece una visibilidad continua de las configuraciones erróneas de identidad y de los permisos que conllevan riesgo. Aumenta la visibilidad con una orientación en forma de tutoriales en video, scripts y comandos para solucionar dichos problemas y reducir su superficie de ataque interna.

Además de las capacidades preventivas, Zscaler ITDR también ofrece detecciones de alta fidelidad para ataques basados en la identidad como credenciales robadas, derivaciones de autenticación multifactor y técnicas de escalada de privilegios que normalmente traspasan las defensas existentes en casos de compromiso de identidad.

¿Por qué Zscaler ITDR?

Sin necesidad de agentes / máquinas virtuales adicionales
Zscaler ITDR está integrado en el Zscaler Client Connector y habilita nuevas capacidades y protecciones preparadas para usarse.

Integrado con la política de acceso
El Zscaler Zero Trust Exchange puede aplicar de forma dinámica controles de políticas de acceso para bloquear a los usuarios comprometidos cuando se detecta un ataque de identidad.

Integraciones con SOC
Refuerce la investigación y la respuesta con integraciones que incluyen EDR como CrowdStrike, Microsoft Defender, VMware CarbonBlack y todos los SIEM (Información sobre seguridad y control de eventos) líderes.

©2023 Zscaler, Inc. Todos los derechos reservados.

Capacidades clave

Identificación de los problemas que permiten a los atacantes sacar ventaja

Descubra configuraciones de riesgo como la exposición de contraseñas GPP, la delegación sin restricciones y las contraseñas obsoletas que posibilitan nuevos frentes de ataque.

Construcción de un estado saludable de la identidad, con orientaciones para su reparación

Comprenda el problema, el impacto y a quién afecta. Use la guía de reparación paso a paso junto con tutoriales en video, scripts y comandos.

Recepción de alertas cuando los cambios de configuración generen un riesgo

Los sistemas de identidad están en constante cambio por las constantes variantes de configuración y permisos. Supervise en tiempo real y reciba alertas acerca de nuevos riesgos y problemas.

Freno de la escalada de privilegios con la detección de amenazas a la identidad

No todas las configuraciones erróneas pueden remediarse. Detecte y detenga ataques como DCSync, DCShadow, kerberoasting y otros en caso de compromiso.

Casos de uso

Visibilidad de la superficie de ataque de identidad

- Puntuación del riesgo para la cuantificación y el seguimiento de la postura de identidad
- Reconocimiento de los principales problemas de identidad y los usuarios/hosts con mayor riesgo
- Mapeo de MITRE ATT&CK para lograr un gran visibilidad de los puntos ciegos de seguridad

Control del estado de la identidad

- Identificación de las nuevas configuraciones erróneas a medida que aparecen
- Alerta en tiempo real de nuevos riesgos en su almacén de identidades
- Orientación, comandos y scripts preparados para usarse en la reparación

Detección y respuesta a amenazas de identidad

- Detección de los ataques contra su almacén de identidades
- Prevención de ataques contra Kerberos, DCSync, la enumeración LDAP y más
- Contención integrada que emplea la política de acceso zero trust

Visite **nuestro sitio web** para obtener más información sobre zscaler ITDR.

zscaler™ | 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 contra los ciberataques y la pérdida de datos al conectar de manera segura a los usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com.mx** o síganos en Twitter **@zscaler**.

© 2023 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ y ZPA™ y otras marcas comerciales listadas en **zscaler.com.mx/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/u otros países. Toda otra marca comercial es propiedad de sus respectivos propietarios.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San José, CA 95134 zscaler.com.mx