Zscaler ITDR™

Avantages de Zscaler ITDR

Réduire la surface d'attaque des identités
Acquérir une visibilité sur les erreurs de configuration des identités qui permettent aux adversaires d'élever leurs privilèges et de se déplacer latéralement.

Détecter les attaques d'identité
Arrêter les menaces d'identité furtives telles que DCSync, DCShadow et le kerberoasting qui contournent les défenses en place.

Atténuer les risques liés à l'identité
Mesurez et surveillez votre posture de surface d'attaque d'identité à l'aide des scores de risque générés par l'évaluation de la sécurité de l'identité.

Qu'est-ce que Zscaler ITDR ?

Du fait de l'adoption rapide de Zero Trust, les hackers ciblent les utilisateurs et les identités comme point d'entrée et utilisent cet accès pour escalader les privilèges et se déplacer latéralement.Zscaler ITDR offre une visibilité permanente sur les erreurs de configuration des identités et les autorisations à risque.Il complète cette visibilité par des conseils sous forme de tutoriels vidéo, de scripts et de commandes pour remédier à ces problématiques et réduire votre surface d'attaque interne.

Outre ses capacités préventives, Zscaler ITDR fournit également des fonctions de détection haute fidélité pour les attaques basées sur l'identité, telles que le vol d'informations d'identification, le contournement de l'authentification multifacteur et les techniques d'élévation des privilèges qui échappent généralement aux défenses en place en cas de compromission de l'identité.

Pourquoi Zscaler ITDR ?

Aucun agent/VM supplémentaire n'est nécessaire
Intégré à Zscaler Client Connector, Zscaler ITDR débloque de nouvelles capacités et protections prêtes à l'emploi.

Intégré à la politique d'accès
Zscaler Zero Trust Exchange peut appliquer dynamiquement les contrôles de la politique d'accès pour bloquer les utilisateurs compromis lorsqu'une attaque d'identité est détectée.

Intégrations SOC
Renforce l'investigation et la réponse avec des intégrations qui incluent des EDR tels que CrowdStrike, Microsoft Defender, VMware CarbonBlack, et tous les principaux SIEM.

Capacités principales

Découverte des problèmes qui permettent aux hackers de prendre le dessus

Découvrez les configurations à risque telles que l'exposition des mots de passe GPP, la délégation sans contrainte et les mots de passe périmés qui ouvrent de nouvelles voies d'attaque.

Construire une hygiène d'identité forte grâce à des conseils de correction

Comprenez le problème, l'impact et les personnes affectées. Tirez parti des conseils de correction étape par étape, ainsi que des tutoriels vidéo, des scripts et des commandes.

Recevoir des alertes lorsque des changements de configuration introduisent des risques

Les systèmes d'identité sont en constante évolution du fait des changements de configuration et d'autorisation. Surveillez en temps réel et soyez alerté des nouveaux risques et problèmes.

Arrêter l'élévation des privilèges avec Identity Threat Detection

Toutes les erreurs de configuration ne peuvent pas être corrigées. Détectez et arrêtez les attaques de type DCSync, DCShadow, Kerberoasting, et bien d'autres en cas de compromission.

Cas d'utilisation

Visibilité de la surface d'attaque de l'identité

- Score de risque pour la quantification et le suivi de la posture d'identité
- Découvrir les principaux problèmes d'identité et les utilisateurs/hôtes les plus risqués
- Cartographie MITRE ATT&CK pour une visibilité sur les zones d'ombre de la sécurité

Gestion de l'hygiène de l'identité

- Identifier les nouvelles erreurs de configuration à mesure qu'elles apparaissent
- Alerte en temps réel sur les nouveaux risques dans votre magasin d'identité
- Conseils, commandes et scripts de remédiation prêts à l'emploi

Détection des menaces et réponses en matière d'identité

- Détecter les attaques contre votre magasin d'identités
- Arrêter l'énumération kerberoasting, DCSync, LDAP, etc.
- Confinement intégré à l'aide d'une politique d'accès Zero Trust

Visitez **notre page web** pour en savoir plus sur Zscaler ITDR.

zscaler™ | Experience your world, secured.™

Zscaler (NASDAQ : ZS) accélère la transformation digitale des entreprises pour les rendre plus agiles, productives, résilientes et sécurisées. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les appareils et les applications, quelle que soit leur localisation. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange basé sur le SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.fr