Zscaler ITDR™

I vantaggi di Zscaler ITDR

Riduzione della superficie di attacco delle identità
Ottieni la massima visibilità sugli errori di configurazione delle identità che consentono agli aggressori di elevare i propri privilegi e di muoversi lateralmente.

Rilevamento degli attacchi alle identità
Blocca le minacce avanzate alle identità, come DCSync, DCShadow e kerberoasting, che sono in grado di aggirare le difese esistenti.

Mitigazione del rischio relativo alle identità
Misura e monitora il profilo di sicurezza della superficie di attacco delle identità utilizzando il punteggio di rischio generato dalla valutazione della loro sicurezza.

Che cos'è Zscaler ITDR?

Con la rapida adozione dello zero trust, gli aggressori prendono di mira utenti e identità per riuscire a penetrare nel sistema, e sfruttano l'accesso che riescono a ottenere per elevare i propri privilegi e muoversi lateralmente. Zscaler ITDR fornisce una visibilità continua sugli errori di configurazione delle identità e sulle autorizzazioni a rischio. È inoltre in grado di supportare tale visibilità fornendo linee guida sotto forma di video tutorial, script e comandi, che consentono di risolvere queste problematiche e ridurre la superficie di attacco interna.

Oltre alle funzionalità preventive, Zscaler ITDR fornisce anche un rilevamento ad alta fedeltà per individuare gli attacchi diretti alle identità, come il furto delle credenziali, l'elusione dell'autenticazione a più fattori e le tecniche di escalation dei privilegi, che, in caso di compromissione dell'identità, sono solitamente in grado di oltrepassare le difese esistenti.

Perché scegliere Zscaler ITDR?

Non sono necessari ulteriori agenti/VM
Zscaler ITDR è un servizio integrato in Zscaler Client Connector che consente di usufruire da subito di nuove funzionalità e protezioni.

Integrazione con le policy di accesso
Quando viene rilevato un attacco alle identità, Zscaler Zero Trust Exchange è in grado di applicare dinamicamente i controlli delle policy di accesso per bloccare gli utenti compromessi.

Integrazioni con il SOC
Rafforza le indagini e le azioni di risposta sfruttando integrazioni che includono strumenti di EDR come Crowdstrike, Microsoft Defender, VMware CarbonBlack e tutti i principali SIEM.

Funzionalità principali

Individua i problemi che consentono agli aggressori di avere la meglio

Rileva le configurazioni a rischio, come l'esposizione delle password GPP, la delega illimitata e le password obsolete che aprono nuovi percorsi di attacco.

Sviluppa una solida igiene digitale delle identità usufruendo di linee guida per la correzione

Comprendi il problema, l'impatto e i soggetti interessati, quindi segui le nostre dettagliate linee guida per procedere alla correzione, usufruendo di video tutorial, script e comandi.

Ricevi avvisi quando vengono apportare modifiche alle configurazioni che introducono rischi

I sistemi di gestione delle identità sono in costante evoluzione, e configurazioni e autorizzazioni cambiano frequentemente. Effettua il monitoraggio in tempo reale e ricevi avvisi sui nuovi rischi e sui problemi rilevati.

Blocca l'escalation dei privilegi con Identity Threat Detection

Non tutti gli errori di configurazione possono essere corretti. In caso di compromissione, rileva e blocca attacchi DCSync, DCShadow, kerberoasting e altri.

Casi d'uso

Visibilità sulla superficie di attacco dell'identità

- Punteggio di rischio per la quantificazione e il monitoraggio del profilo di sicurezza delle identità
- Rilevamento dei principali problemi relativi alle identità e degli utenti/host maggiormente a rischio
- Mappatura MITRE ATT&CK per la visibilità sui punti ciechi nella sicurezza

Gestione dell'igiene digitale delle identità

- Rilevamento dei nuovi errori di configurazione non appena emergono
- Segnalazione in tempo reale dei nuovi rischi introdotti nell'archivio delle identità
- Procedure guidate, comandi e script pronti all'uso per le attività di correzione

Identity Threat Detection and Response

- Rileva gli attacchi diretti all'archivio delle identità
- Blocco di kerberoasting, DCSync, enumerazione LDAP e altro
- Contenimento integrato con policy di accesso zero trust

Visita **la nostra pagina web** per scoprire di più su Zscaler ITDR.

zscaler™ | Experience your world, secured.™

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it