Zscaler ITDR™

Vorteile von Zscaler ITDR

Reduzierung der identitätsbezogenen Angriffsfläche
Verschaffen Sie sich einen Überblick über identitätsbezogene Fehlkonfigurationen, durch die Angreifer ihre Zugriffsrechte ausweiten und sich lateral fortbewegen können.

Erkennung identitätsbasierter Angriffe
Wehren Sie verborgene identitätsbasierte Bedrohungen wie DCSync, DCShadow und Kerberoasting ab, die bestehende Schutzmaßnahmen umgehen.

Verringerung identitätsbasierter Risiken
Messen und überwachen Sie die identitätsbezogene Angriffsfläche anhand von Risk Scores aus entsprechenden Risikobewertungen.

Was ist Zscaler ITDR?

Aufgrund der raschen Einführung von Zero Trust konzentrieren sich Angreifer mittlerweile auf User und Identitäten, um in Ihr Netzwerk zu gelangen, ihre Zugriffsrechte auszuweiten und sich lateral fortzubewegen.Zscaler ITDR bietet kontinuierlichen Einblick in identitätsbezogene Fehlkonfigurationen und riskante Berechtigungen. Zudem erhalten Sie Zugriff auf Videotutorials, Skripte und Befehle, die Sie bei der Behebung identitätsbezogener Probleme und der Reduzierung der internen Angriffsfläche unterstützen.

Zscaler ITDR verfügt nicht nur über präventive Funktionen, sondern erkennt auch identitätsbasierte Angriffe wie gestohlene Anmeldedaten, Umgehung der Multifaktorauthentifizierung und unbefugte Rechteerhöhung, die im Fall einer Kompromittierung von vorhandenen Abwehrmechanismen nicht entdeckt werden.

Warum Zscaler ITDR?

Keine zusätzlichen Agents/VMs erforderlich
Zscaler ITDR ist in Zscaler Client Connector integriert und bietet Ihnen sofort einsatzbereite neue Funktionen und Schutzmechanismen.

Integrierte Zugriffsrichtlinien
Die Zscaler Zero Trust Exchange kann Richtlinienkontrollen dynamisch anwenden, um kompromittierte User zu blockieren, wenn ein identitätsbasierter Angriff erkannt wird.

SOC-Integrationen
Integrationen mit EDRs wie CrowdStrike, Microsoft Defender, VMware CarbonBlack und allen führenden SIEMs unterstützen die Untersuchung und Behebung von Vorfällen.

Kernfunktionen

Frühzeitige Erkennung kritischer Probleme

Sie erhalten Informationen über riskante Konfigurationen wie Exposition von GPP-Passwörtern, uneingeschränkte Weitergabe von Berechtigungen und veraltete Passwörter, die neue Angriffspfade eröffnen.

Umfassende identitätsbezogene IT-Hygiene mit Anleitungen zur Problembehebung

Sie gewinnen Einblick in das bestehende Problem, die Auswirkungen und betroffene User. Zudem erhalten Sie Schritt-für-Schritt-Anleitungen zur Problembehebung sowie Videotutorials, Skripte und Befehle.

Echtzeit-Benachrichtigungen bei riskanten Konfigurationsänderungen

Identitätssysteme unterliegen einem ständigen Wandel mit laufenden Konfigurations- und Berechtigungsänderungen. Unsere Lösung unterstützt die Überwachung in Echtzeit, damit Sie jederzeit sofort über neue Sicherheitsrisiken und Probleme informiert sind.

Unterbindung unbefugter Rechteerhöhung mit Identity Threat Detection

Nicht alle Fehlkonfigurationen können behoben werden. Deshalb ist es besonders wichtig, Angriffe wie DCSync, DCShadow oder Kerberoasting im Falle einer Kompromittierung zu erkennen und abwehren zu können.

Anwendungsfälle

Identity Attack Surface Visibility (Visualisierung der identitätsbezogenen Angriffsfläche)

- Risk Score zur Quantifizierung und Erfassung des Identitätsstatus
- Anzeige akuter identitätsbezogener Probleme und besonders riskanter User/Hosts
- MITRE ATT&CK-Zuordnung für Einblick in Sicherheitslücken

Identity Hygiene Management

- Sofortige Identifizierung neuer Fehlkonfigurationen
- Echtzeitwarnungen bei neuen Risiken für Ihren Identitätsspeicher
- Vorgefertigte Anleitungen, Befehle und Skripte zur Problembehebung

Identity Threat Detection and Response

- Erkennung von Angriffen auf den Identitätsspeicher
- Unterbindung von Kerberoast-, DCSync- und LDAP-Enumerationsangriffen
- Integrierte Eindämmung mit Zero-Trust-Zugriffsrichtlinien

Weitere Informationen zu Zscaler ITDR finden Sie auf **unserer Webseite.**

zscaler™ | Experience your world, secured.™

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.de** oder auf Twitter unter **@zscaler**.

+1 408 533 0288

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

zscaler.de