Datenblatt

Zscaler ITDR™

Identitätsorientierte Sicherheit für Zero-Trust-Architekturen

Zscaler ITDR (Identity Threat Detection and Response) stellt leistungsstarke Funktionen zum Erkennen von und Schutz vor identitätsbezogenen Angriffen bereit. Damit verhindern Sie Bedrohungen wie Diebstahl von Anmeldedaten, Missbrauch von Rechten, Active-Directory-Angriffe, riskante Berechtigungen usw.

Identität als neue Angriffsfläche

Cyberkriminelle nutzen zunehmend raffinierte Methoden für Angriffe auf Identitätsspeicher und Systeme zur Identitätsverwaltung. Angesichts der steigenden Anzahl identitätsbezogener Angriffe und Bedrohungen benötigen Unternehmen zuverlässige Methoden zur Aufdeckung von Versuchen, identitätsbezogene Daten auszunutzen un kömmliche Techniken zur Bedrohungs-erkennung und Legay-Identitätssysteme können unter heutigen Vorzeichen keinen ausreichenden Schutz mehr gewährleisten. Zscaler ITDR unterstützt die Bekämpfung von Cyberbedrohungen für Identitätssysteme und -daten bzw. die einschlägige Infrastruktur (sprich: Ihr lokales Active Directory).

Zscaler ITDR

Zscaler ITDR unterstützt die Überwachung Ihres Active Directory auf Fehlkonfigurationen und Sicherheitslücken, die das Risiko unbefugter Zugriffe mit erweiterten Berechtigungen bzw. der lateralen Ausbreitung von Bedrohungen im Netzwerk erhöhen. Die Software schützt Ihre Identitäten und liefert umfassende Informationen zur identitätsbezogenen Angriffsfläche sowie Echtzeit-Warn-meldungen über einschlägige Bedrohungen. Damit steht Ihnen ab sofort eine zuverlässige Methode zur Erkennung und Abwehr identitätsbezogener Angriffe (Diebstahl von Anmeldedaten, Umgehung der Multifaktorauthentifi-zierung, unbefugte Rechteerhöhung usw.) zur Verfügung.

Vorteile

- **Echtzeiterkennung identitätsbezogener Bedrohungen:** Identitätssysteme unterliegen einem ständigen Wandel mit laufenden Konfigurations- und Berechtigungsände-rungen. Unsere Lösung unterstützt die Überwachung in Echtzeit, damit Sie sofort über neue Schwachstellen, Sicherheitsrisiken und Probleme informiert werden.
- **Reduzierung der identitätsbezogenen Angriffsfläche:** Sie profitieren von transparenten Einblicken in Fehlkonfigura-tionen und riskante Berechtigungen, die Ihre Organisation anfällig für Angriffe machen.
- **Geringeres Risiko identitätsbezogener Angriffe:** Sie erhalten Informationen über riskante Konfigurationen wie Exposition von GPP-Passwörtern, uneingeschränkte Weitergabe von Berechtigungen und veraltete Passwörter, die neue Angriffspfade eröffnen.
- **Beschleunigte Untersuchung und Reaktion:** Risk Scores aus identitätsbezogenen Risikobewertungen unterstützen Sicherheitsbeauftragte bei der Priorisierung von Untersuchungen und Behebungsmaßnahmen.
- **Optimierte Vorfallbehebung:** Zscaler ITDR stellt detaillierte Anleitungen zur Fehlerbehebung mitsamt Videoanleitungen, Skripts und Befehlen bereit, um eine möglichst zügige Reaktion auf Sicherheitsvorfälle zu ermöglichen.
- **Einfache Bereitstellung:** Keine zusätzlichen VMs erforderlich. Über den vorhandenen Client Connector von Zscaler kann eine zusätzliche Sicherheitsebene zur Abwehr identitätsbezogener Bedrohungen bereitgestellt werden.

5/10

Organisationen sind Opfer eines Active-Directory-Angriffs

Quelle: EMA

80 %

aller heutigen Angriffe sind identitätsbezogen

Quelle: CrowdStrike

90 %

der von Mandiant beobachteten Cybersicherheitsvorfälle betreffen Active Directory

Quelle: Dark Reading

Wie funktioniert das?

Zscaler ITDR gewährleistet unkomplizierten Identitätsschutz ohne Zusatzaufwand. Die Lösung ist in den Zscaler Client Connector integriert, einen Agent zur sicheren Vermittlung von Verbindungen zwischen Usern und Anwendungen/Ressourcen.

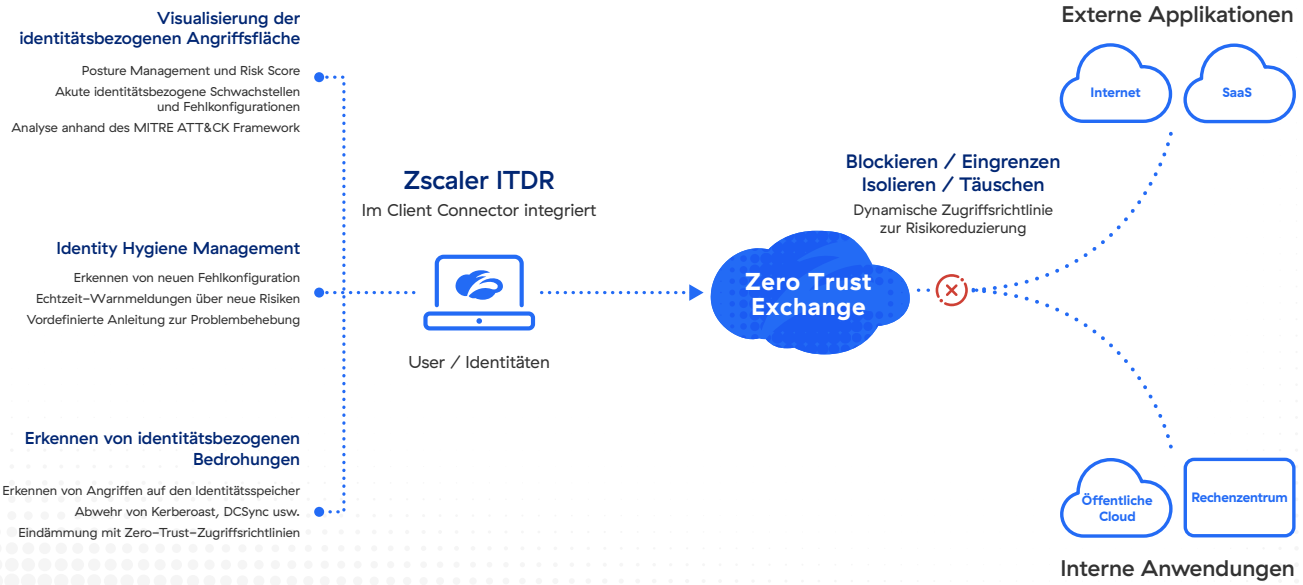
Zscaler ITDR kombiniert drei Funktionen:

- Identity Attack Surface Visibility (Visualisierung der identitätsbezogenen Angriffsfläche)
- Identity Change Detection (Erkennen von Identitätsänderungen)
- Identity Threat Detection (Erkennen von identitätsbezogenen Bedrohungen)

Identity Attack Surface Visibility

Zscaler ITDR prüft das Active Directory mithilfe von LDAP-Abfragen und visualisiert Schema, User, Computer, Organisationseinheiten und andere Objekte in Ihrem Identitätsspeicher. Anschließend werden diese Objekte überprüft, um Fehlkonfigurationen und Sicherheitsrisiken im Active Directory zu identifizieren.

- Zur Risikobewertung des Active Directory muss Zscaler ITDR auf einem Client Connector ausgeführt werden, der auf einem in die Domain eingebundenen Windows-Rechner installiert ist.
- Das Sicherheitsteam gibt an, welche Active-Directory-Domain gescannt werden soll, und wählt den Rechner aus, auf dem der Scan ausgeführt wird. Auf diesem Computer muss der Client Connector installiert sein.
- Abhängig von der Größe des Active Directory dauert die Bewertung 15 bis 30 Minuten.
- Nach Abschluss der Bewertung können die Ergebnisse sofort im Dashboard abgerufen werden.
- In der Bewertung sind folgende Informationen inbegriffen: Risk Score für die gescannte Domain, Schwerpunktbereiche zur Priorisierung von Behebungsmaßnahmen, Liste der am stärksten gefährdeten User und Computer, Analyse des Schweregrads und der Risikokategorisierung, Analyse der Kill Chain anhand des MITRE-ATT&CK-Frameworks sowie eine vollständige Liste aller erkannten Fehlkonfigurationen.



Für jede erkannte Fehlkonfiguration werden folgende Angaben bereitgestellt:

- Risikokategorisierung
- Schweregrad
- Maßnahmen zur Fehlerbehebung
- ID und Taktik gemäß MITRE-ATT&CK-Framework
- Problembeschreibung
- Potenzielle Auswirkungen
- Liste der betroffenen User, Computer und Objekte
- Anleitung zur Fehlerbehebung
- Videoanleitungen
- Skripts
- Befehle

Identity Change Detection

Nachdem eine Bewertung konfiguriert wurde, besteht die Möglichkeit, Identity Change Detection für die betreffende AD-Domain zu aktivieren, um identitätsbezogene Konfigurationsänderungen zu erkennen, die sich auf den Sicherheitsstatus des Active Directory auswirken. Die Erkennung erfolgt nahezu in Echtzeit, sodass Sicherheitsteams und Directory-Administratoren sofort reagieren können.

- Zscaler ITDR führt eine Reihe wichtiger Konfigurationsprüfungen des Active Directory durch.
- Dadurch lassen sich Probleme identifizieren, bei denen das höchste Risiko eines Missbrauchs durch Angreifer besteht.
- Diese Prüfungen werden alle 15 Minuten auf dem ausgewählten Endgerät mit installiertem Client Connector für die betreffende Domain ausgeführt.
- Alle erkannten Veränderungen werden je nach ihren Auswirkungen als positiv oder negativ gekennzeichnet.
- Veränderungen mit positiver Auswirkung deuten darauf hin, dass ein Problem behoben wurde.
- Veränderungen mit negativer Auswirkung deuten auf ein potenzielles neues Problem hin.

Identity Threat Detection in Echtzeit

Zscaler ITDR stellt eine Funktion zur Bedrohungserkennung bereit, die SOC-Teams und Bedrohungsexperten in Echtzeit über schädliche bzw. verdächtige identitätsbezogene Aktivitäten informiert.

Die Bedrohungserkennung kann als Richtlinie zur Überprüfung von Endgeräten auf Computern aktiviert werden, auf denen der Client Connector installiert ist.

- Durch Aktivieren der Richtlinie zur Bedrohungserkennung wird die Überwachung von Events im System sowie die Analyse von Mustern zur Erkennung von Indikatoren für die jeweils ausgewählten Bedrohungsvektoren ermöglicht.
- Dabei stehen verschiedene Indikatoren zur Auswahl, u. a. DCSync, DCShadow, Kerberoasting, Sitzungsenumerationen, Zugriffe auf Konten mit erweiterten Berechtigungen und LDAP-Enumerationen.
- Diese können in beliebiger Kombination auf den betreffenden Endgeräten aktiviert werden.
- Wenn ein Muster erkannt wird, übermittelt der Client Connector ein entsprechendes Warnsignal an Zscaler ITDR.
- Die Plattform ergänzt dieses Signal mit relevanten Informationen, damit eine Untersuchung eingeleitet werden kann.
- Durch Konfigurieren von Orchestrierungsfunktionen in Zscaler ITDR können Warnmeldungen, Weiterleitungen und Maßnahmen zur Problembehebung automatisiert werden.

Die wichtigsten Anwendungsfälle

Identity Attack Surface Visibility

Anhand der laufenden Bewertung des Active Directory wird ein Risk Score erstellt. Außerdem erhalten Sie eine Liste der erkannten Fehlkonfigurationen und Sicherheitsrisiken sowie Anleitungen zu ihrer Behebung.

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

Identity Hygiene Management

Bei Erkennen neuer Risiken für das Active Directory werden Echtzeit-Warnmeldungen und Benachrich-tigungen ausgegeben. Ihre Organisation profitiert ebenfalls von Echtzeit-Informationen über riskante Konfigurationen und Berechtigungsänderungen.

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

Identity Threat Detection and Response

Echtzeit-Erkennung für akute identitätsbezogene Bedrohungen

- Erkennung von Angriffen auf den Identitätsspeicher
- U. a. werden Kerberoast, DCSync und LDAP-Enumeration erkannt
- Integrierte Eindämmung mit Zero-Trust-Zugriffsrichtlinien

Wichtige Unterscheidungsmerkmale

In den Client Connector integriert

Zscaler ITDR ist in den Client Connector von Zscaler integriert und erschließt unmittelbar neue Kapazitäten und Schutzfunktionen. Derselbe Endgerät-Client, der User sicher mit dem Internet und Anwendungen verbindet, stellt jetzt zusätzliche Sicherheitsfunktionen bereit und verringert das Risiko identitätsbezogener Angriffe.

Integriert mit der Zero Trust Exchange

Zscaler Identity lässt sich nahtlos mit der Zero-Trust-Exchange-Plattform von Zscaler integrieren, um eine bessere Erkennung und Reaktion auf identitätsbezogene Bedrohungen zu ermöglichen. Bei Erkennen eines identitätsbezogenen Angriffs kann die Zero Trust Exchange kompromittierte User durch dynamische Anwendung von Zugriffsrichtlinien blockieren.

Nahtlose Integrationen

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

Zscaler ITDR: Leistungsstarke Funktionen zur Verbesserung Ihres Sicherheitsstatus

Schutz vor identitätsbezogenen Bedrohungen.

Die zuverlässige Erkennung identitätsbezogener Bedrohungen setzt lückenlose Transparenz voraus. Zscaler ITDR liefert umfassende Informationen zu identitätsbezogenen Vorfällen und Anomalien in Ihrer gesamten IT-Umgebung und gewährleistet so eine rechtzeitige Erkennung und Abwehr identitätsbezogener Angriffe.

Erkennung von Angriffen auf das Active Directory

Active Directory ist ein beliebtes Ziel für identitätsbezogene Angriffe. Zscaler ITDR überwacht AD/AZURE AD kontinuierlich auf Sicherheitsrisiken und Fehl- bzw. riskante Konfigurationen.

Verhindern des Missbrauchs/Diebstahls von Anmeldedaten

Angreifer nutzen gestohlene Anmeldedaten sowie Angriffe auf das Active Directory zur unbefugten Rechteerhöhung, um die laterale Ausbreitung im Netzwerk zu ermöglichen. Zscaler ITDR unterstützt Sie beim Erkennen verdächtiger Aktivitäten und verhindert so den Missbrauch/Diebstahl von Anmeldedaten.

Schutz vor lateraler Ausbreitung

Zscaler ITDR erkennt Fehlkonfigurationen und exponierte Anmeldedaten, die Angriffspfade für laterale Bewegungen öffnen. Dadurch wird verhindert, dass Angreifer, die perimeterbasierte Sicherheitskontrollen erfolgreich unterlaufen haben, sich lateral in Ihrer Umgebung bewegen.

Zscaler ITDR erschließt leistungsstarke neue Funktionen, die ohne zusätzlichen Betriebs- oder Ressourcenaufwand die Möglichkeiten Ihres Zero-Trust-Programms erweitern.

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, zuverlässiger und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an beliebigen Standorten vor Cyberangriffen und Datenverlust. Die SSE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.

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