Zscaler Identity Protection™

概要

Zscaler Identity Protection のメリット

アイデンティティー攻撃対象領域の削減
権限昇格とラテラル ムーブメントを可能にする設定ミスを可視化します。

アイデンティティー攻撃の検知
既存の防御策を回避する DCSync、DCShadow、Kerberoasting などのステルス性の高いアイデンティティー脅威を阻止します。

アイデンティティー リスクの軽減
アイデンティティー セキュリティ評価によって生成されたリスク スコアを使用して、アイデンティティー攻撃対象領域のポスチャーを測定しモニタリングします。

Zscaler Identity Protection とは

Zscaler Identity Protection は、オンプレミスの Active Directory、Entra、ハイブリッドのアイデンティティー ストアにおける設定ミスや脆弱性を可視化することで、攻撃対象領域の削減を支援します。また、特権、デバイスの資格情報、リスクの高い権限付与を悪用して水平に移動するアイデンティティーベースの攻撃を検知します。

Zscaler Identity Protection は Active Directory をモニタリングして、権限昇格やラテラル ムーブメントのリスクを高める設定ミスや脆弱性を確認するとともに、アイデンティティーを保護しながら、アイデンティティーの攻撃対象領域を広範囲に可視化することで、アイデンティティーベースの攻撃をリアルタイムで通知します。資格情報の窃取、多要素認証の迂回、権限昇格戦術といったアイデンティティーベースの攻撃を検知して阻止することが可能です。

Zscaler Identity Protection を採用する理由

追加のエージェントや VM は不要

Zscaler Client Connector に組み込まれた Zscaler Identity Protection は、追加設定なしで新たな機能および保護を提供します。

アクセス ポリシーとの統合

Zscaler Zero Trust Exchange は、ID 攻撃が検出された場合、アクセス ポリシー制御を動的に適用して侵害されたユーザーをブロックします。

SOC の統合

CrowdStrike、Microsoft Defender、VMware CarbonBlack などの EDR、およびすべての主要な SIEM を含む統合により、調査と対応を強化します。

主な機能

攻撃者優位につながる問題を検知

GPP パスワードの漏洩、制約のない委任、古いパスワードなど、新しい攻撃経路になり得る危険な構成を検出します。

修復ガイダンスで強力なアイデンティティー保護を構築

問題点、影響度、影響を受けるユーザーを把握し、動画チュートリアル、スクリプト、コマンドを利用したステップバイステップの修復ガイダンスを活用できます。

構成の変更に伴うリスクをアラートで通知

アイデンティティー システムでは、構成や権限の変更が常に行われます。リアルタイムのモニタリングで新たなリスクや問題に関するアラートを受信できます。

アイデンティティー脅威の検知で権限昇格を阻止

設定ミスをすべて修復することはほぼ不可能です。侵害が発生した場合に、DCSync、DCShadow、Kerberoasting などの攻撃を検出して阻止します。

資格情報における攻撃対象領域の範囲の削減

安全でない方法で保存されている資格情報をエンドポイント全体にわたって検出し、すでに侵害されているものや簡単に解読されるものを可視化し、ワンクリックでそれらを削除します。

こちらの Web ページをご確認ください。

ユース ケース

アイデンティティーの攻撃対象領域の可視化

- アイデンティティー態勢の定量化と追跡のためのリスク スコア
- アイデンティティーに関する最も重大な課題と最もリスクの高いユーザーやホストを検出
- MITRE ATT&CK マッピングでセキュリティの死角を可視化

アイデンティティー保護の管理

- 新たな設定ミスを特定
- アイデンティティー ストア内の新しいリスクに対するリアルタイムのアラート
- 修復のための既製のガイダンス、コマンド、およびスクリプト

アイデンティティー脅威の検知と対応

- アイデンティティー ストアに対する攻撃を検知
- Kerberoasting、DCSync、LDAP 列挙などを阻止
- ゼロトラスト アクセス ポリシーを使用した組み込みの封じ込め

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange™ は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/jp**

zscaler™

Zero Trust Everywhere