



Identityリスク・アセスメントサービス

XCOCKPIT IDENTITY

 CYCRAFT

株式会社アイティフォー
通信システム事業部

正規のユーザーアカウントによるADを介した不正アクセスへの対策が求められています

攻撃者は正規アカウントでログイン

- 攻撃者が正規アカウントとパスワードを使って侵入したケースが増加
- 攻撃者がどうやって有効なアカウント／パスワードを入手したかを知ることは困難

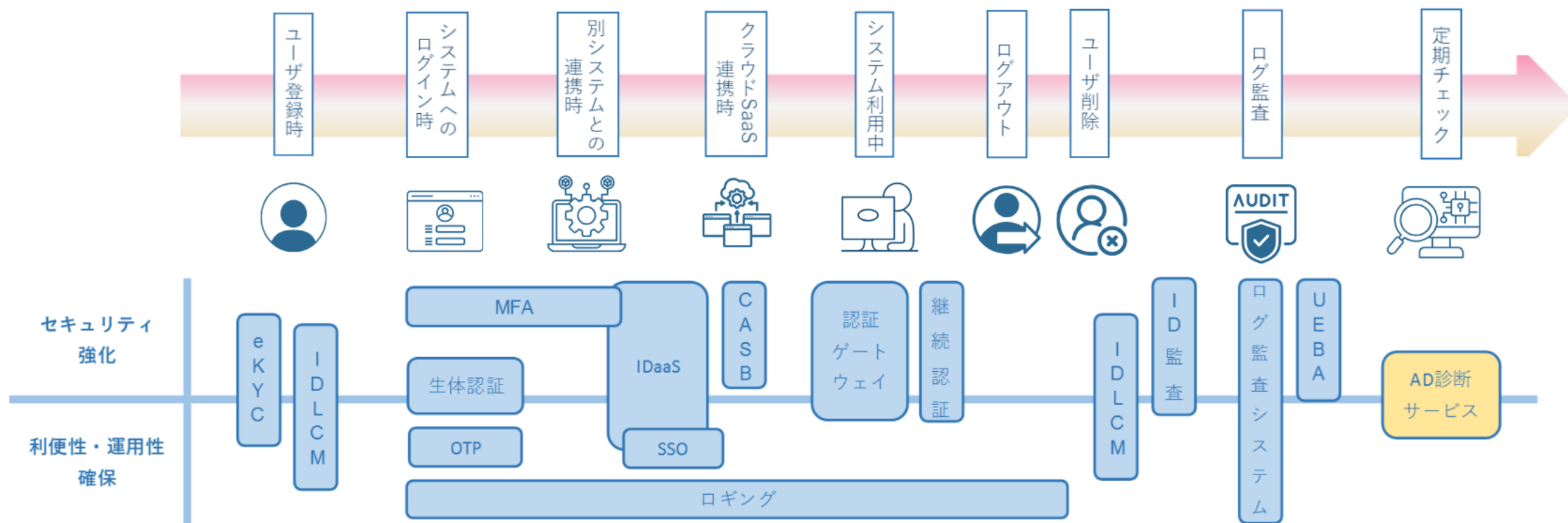
攻撃者から見たIdentity Threat

- なりすましで侵入し、特権を奪取する方がはるかに楽！
- なりすましであれば、セキュリティ対策ツールにひっかからずに侵入できる確率が高い
- 一般ユーザのアカウントが手に入れば、設定ミスを突いて権限昇格が可能
- ADのデフォルトポリシーをそのまま使っている組織が多いので、攻撃手法は確立されており、短時間で組織内の情報を調査できる

Identityリスクに関して

Identityリスクとは、他人によるなりすましのリスクであり、

「従来の入口対策、出口対策の経路を通らずに正規のユーザーとしてシステムに侵入するため、遠隔操作を行うための悪性プログラム（トロイの木馬等）を使わずに、Windows PowerShellなどの正規のツールを利用して情報窃取やランサムウェアの実行を行う」傾向が高まっている。



こんなActiveDirectoryとなっていないでしょうか？

- ☑ 組織変更や人事異動が多く設定や権限管理が追いついていない。
- ☑ 合併や組織変更によりドメインを統合したがたまにエラーが起きる
- ☑ 管理者がよく変わるため、どうしてこういう設定になっているか分からない
- ☑ 参照しているシステムが多く、下手に設定を変えられない



→一つでも当てはまる場合はアセスメントをお勧めします。

ADにおけるIdentityリスク

- **ADはとにかく難解**
ID管理の重要性は理解していても手が付けられない現状
- **ADの「アクセス権限の継承」は専門家でも把握が難しい**
大きな組織では複数組織の統廃合などが繰り返された結果で現在の設定となっており、過去の経緯がわかる人が減っている。
- **複雑な権限設定は触れてはいけないもの（アンタッチャブル）として扱われがち。**
- **権限付与の状態を俯瞰できるツールが存在しない。**

CyCraft XCOCKPITは、

AIを活用したアセスメントサービスを提供します。

- ① AD内を探索し、保有するID、割り当てられた権限、アクセス可能なリソースなどの情報を収集
- ② AD内の設定ミス、過大な権限を付与されているアカウントの特定、管理者特権を使えるアカウント等を自動で発見
- ③ AIを活用し、大量のIDの保有権限を調査し、関係性を可視化
- ④ 机上で攻撃シミュレーションを行いAttack Pathsを洗い出し
- ⑤ IDと権限の複雑な設定を理解できるよう、AIを用いて自然言語で説明

他セキュリティ製品の空白部分をカバーします。



ADアセスメントサービスの利用STEP

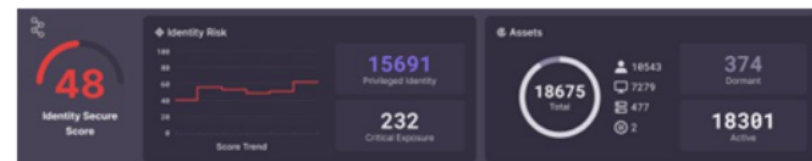
STEP 01 ドメインに参加している端末を1台用意いただき、その端末で検査プログラムを実行。

STEP 02 スキャン結果をCyCraftの分析クラウドサイトにアップロード

STEP 03 ADの設定ミス、意図しない管理者権限への昇格要因、過大な権限付与ID等を見つける攻撃シミュレーションを分析クラウド上で行い、**Attack Paths**を洗い出す。

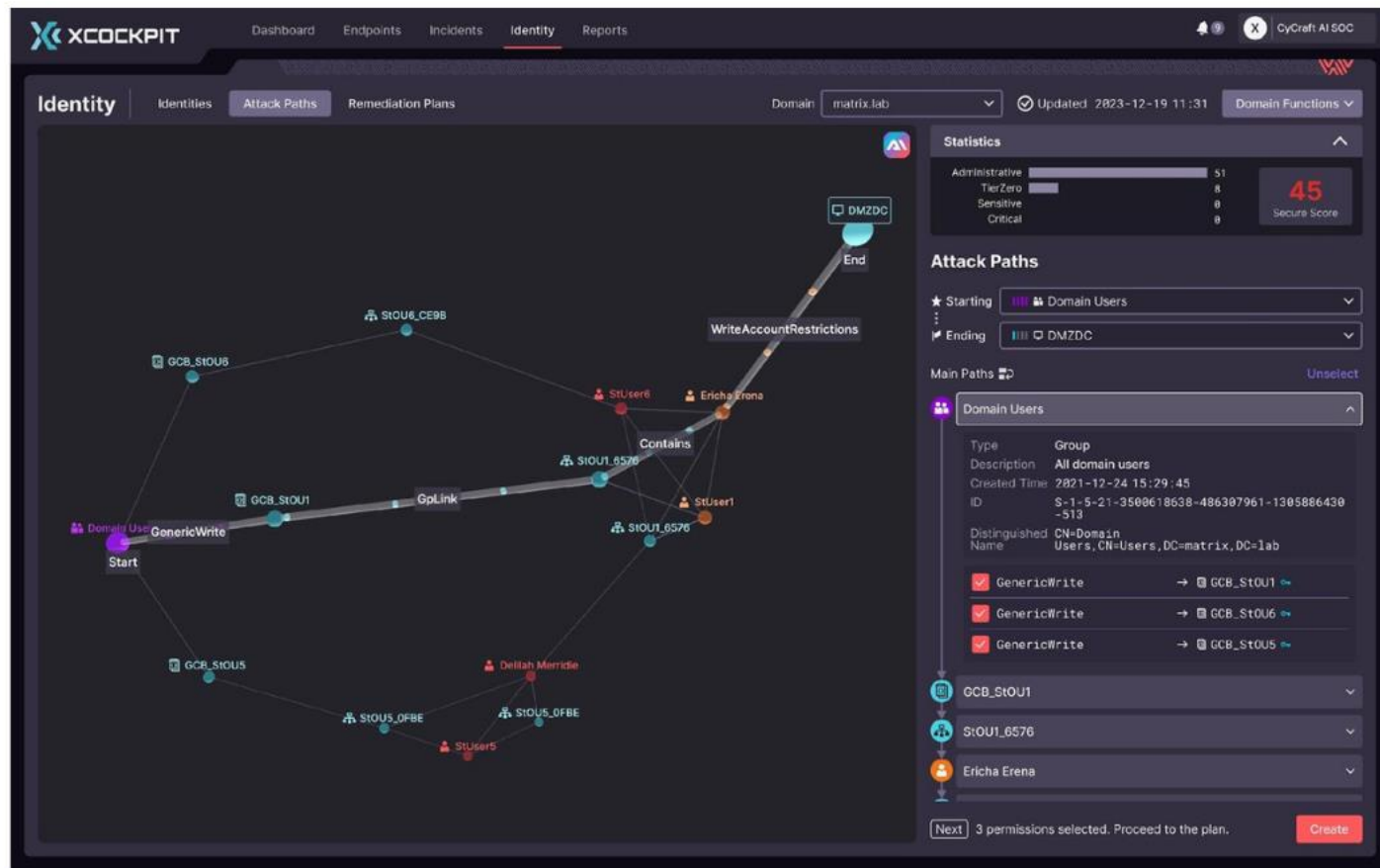
STEP 04 分析レポート画面からドメイン内の不要な設定を確認し、ADサーバー上で削除・修正するプログラムを必要に応じ実行。

STEP 05 AD設定を見直し後、再度スキャンを行いリスクが軽減されているかを確認する。この作業を周期的に繰り返すことでADリスクの改善を行う。



ユーザIDが権限昇格できる経路を可視化

- ✓ 組織内に存在するIDを見つける。
- ✓ 攻撃シミュレーションにより、特権ユーザに権限昇格が可能なルートを見つける。
- ✓ ユーザ、デバイス、グループ、オブジェクトなどの関係性を可視化
- ✓ 難解なADの権限設定を日本語で説明



攻撃事例

委託業者アカウントが設定ミスについてドメインコントローラ権限奪取



委託業者向けアカウントは制限され、スクリーンロックの設定変更機能を与えられましたが、その機能を悪用するとTier-0権限（ドメイン管理者権限）を入手できることが判明しました。

アカウントの権限が制限されていても、管理者権限を取得するための迂回経路は頻繁に存在します。ただし、現在の状況では全体像を把握することが難しいです。



CyCraftGTP：日本語で有効な対応を提示します！

2023 年 10 月 6 日 11:01:57, CyCraft AI 仮想アナリストは、MATRIX.LAB AD ドメインのアカウント分析をして、特権アカウント他への攻撃経路分析をしました。結果、総合セキュリティ評価スコアは42点でした。この分析では、合計で2374のオブジェクトが検査され、12のユーザーアカウント、6のコンピュータアカウント、68のグループ、およびその他の2288のオブジェクトが含まれていました。アカウント関係を分析した結果、62の特権アカウントが存在することが判明し、その中には15のTierZero アカウントと47の管理アカウントが含まれていました。最小権限の原則に基づいて、アカウント全体とリソースの関係や構造を分析することで、次項のアカウントセキュリティの強化提案がまとめられました：

<アカウントセキュリティの強化提案>

アセット権限の調整：潜在的な脅威を減らすための権限の変更

- ・ オブジェクトのフォルダリダイレクション (GPO)、デフォルトドメインコントロールポリシー (GPO)、暗号化キーエスクロー (AD CS テンプレート)、Internet Explorer Setting (GPO)、matrixlab (DOMAIN)、JPsec、¥¥matrix.lab¥SYSVOL¥matrix.lab¥Policies{C7920CB3-673A-4C6C-8955-2692EFAF4CCA}¥Machine¥Scripts¥scripts.ini (SHAREFILES)、パスワードポリシー (GPO)、SecureEmail (AD CS Template)、EnciphermentKeyEscrowNew (AD CS Template)、デフォルトドメインポリシー (GPO)、SecureVPN (AD CS Template)、署名、Tainan-ADMIN、アカウントログアウトポリシー (GPO)、Office 365 設定、Windows ファイアウォール設定 (GPO)、ソフトウェアインストール (GPO) の権限設定を確認してください。これらのオブジェクトには明らかな設定エラーが存在し、多数の低特権アカウントに特権アセットを制御させており、セキュリティポリシーに違反しています。特に特別な理由がない限り、関連する権限設定を変更して、最小限の権限原則に合致するようにすることをお勧めします。
- ・ アカウント Mei Ishikawa (USER) の必要性を確認してください。アカウント Mei Ishikawa (USER) は特権アセットを直接または間接的に制御できます。これらのアカウントが長期間使用されていない場合および使用されなくなった場合、アクセス権の範囲を制限するために無効にすることをお勧めします。

アイデンティティの強化：ネットワークセキュリティポリシーに基づいたアカウントセキュリティの向上

- ・ アカウント Daniel Cooper (USER) のパスワード設定を確認してセキュリティを強化してください。アカウント Daniel Cooper (USER) には現在、直接的なリスクはないかもしれませんが、パスワードが簡単に破られる可能性があるため、セキュリティを強化する必要があります。パスワードポリシーを強化するか、破られるリスクを回避するために Microsoft MSA メカニズムを検討してください。
- ・ アカウント matrix.lab (DOMAIN)、EnciphermentKeyEscrow (AD CS Template)、EnciphermentKeyEscrowNew (AD CS Template)、SecureVPN (AD CS Template) のアクセス権限や設定が過度に高いかどうかを確認してください。これらは他の一般的な特権アカウントに比べてセキュリティリスクがある可能性があります。これらは管理要件の専用アカウントかもしれません。これらのアカウントの目的を確認し、必要に応じてアクセス権限の範囲を調整してセキュリティを向上させてください。



株式会社アイティフォー

<http://www.itfor.co.jp>

通信システム事業部

(東京本社)

〒102-0082 東京都千代田区一番町 2 1 番地
一番町東急ビル

TEL : 03-5275-7909 FAX : 03-5275-7921
E-mail : telecom@itfor.co.jp