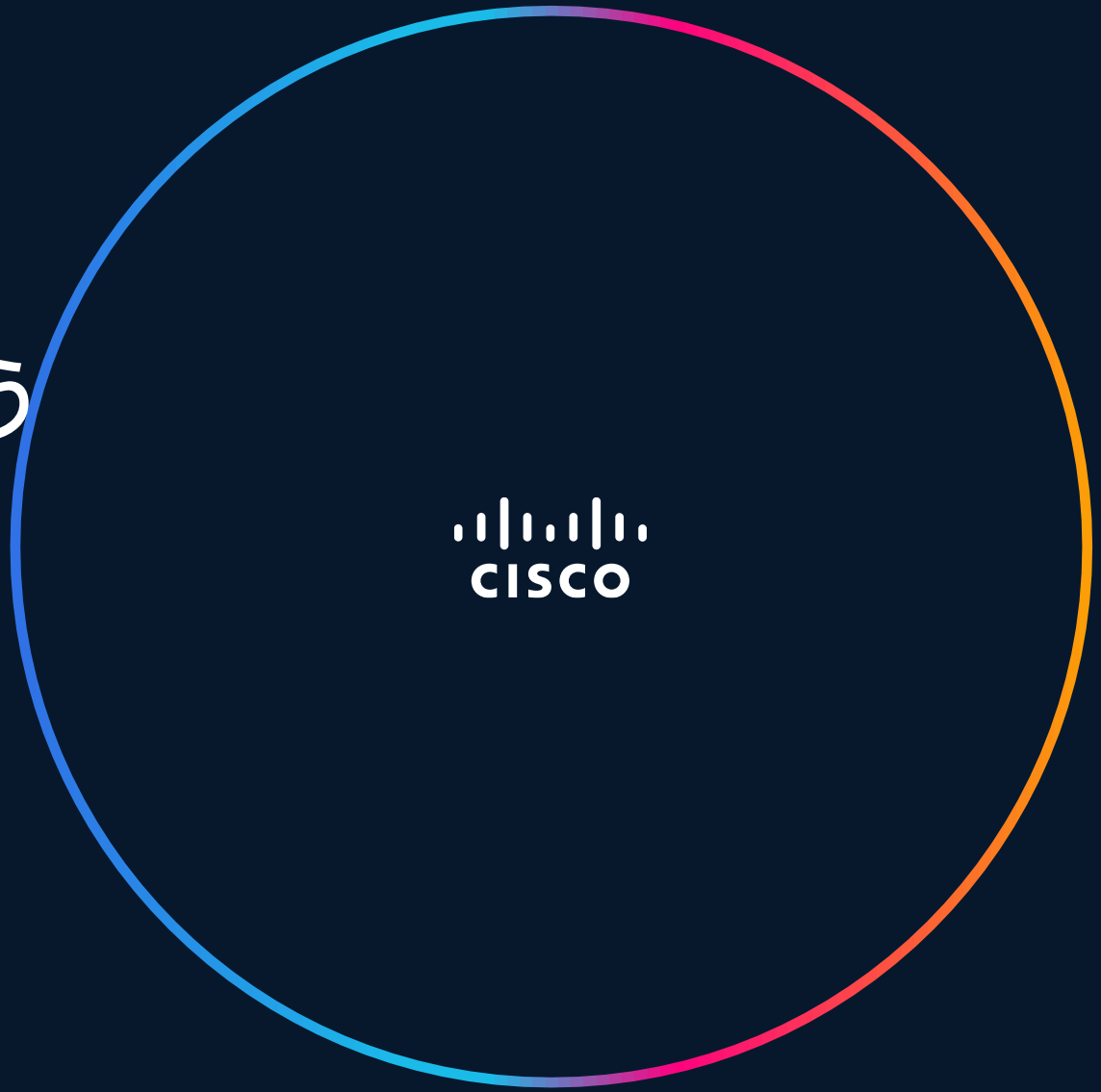
ランサムウェア攻撃者が狙う Active Directoryの弱点

Duoで実現するAD Defense



Tatsuhiro Hihraoka

Duo Sales Lead, Cisco Systems

2026年6月24日

アイデンティティが重要な要素として利用された侵害の割合

Cisco Talos インシデント対応チーム | 2025 年版『一年の総括』

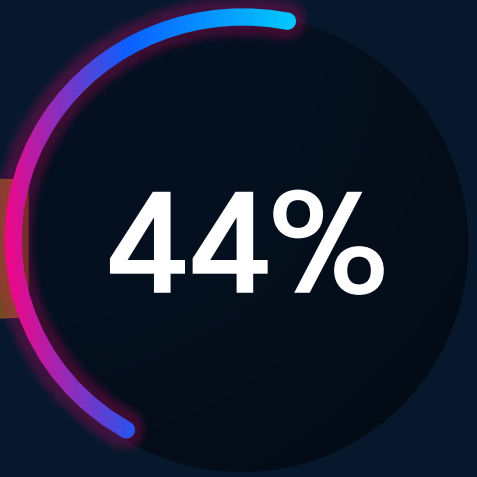
Active Directory が依然として基盤となっている

90% of Fortune 1000 企業

ADを使用してユーザーとリソースを管理している

ADは攻撃者にとって優先度の高い標的となっている

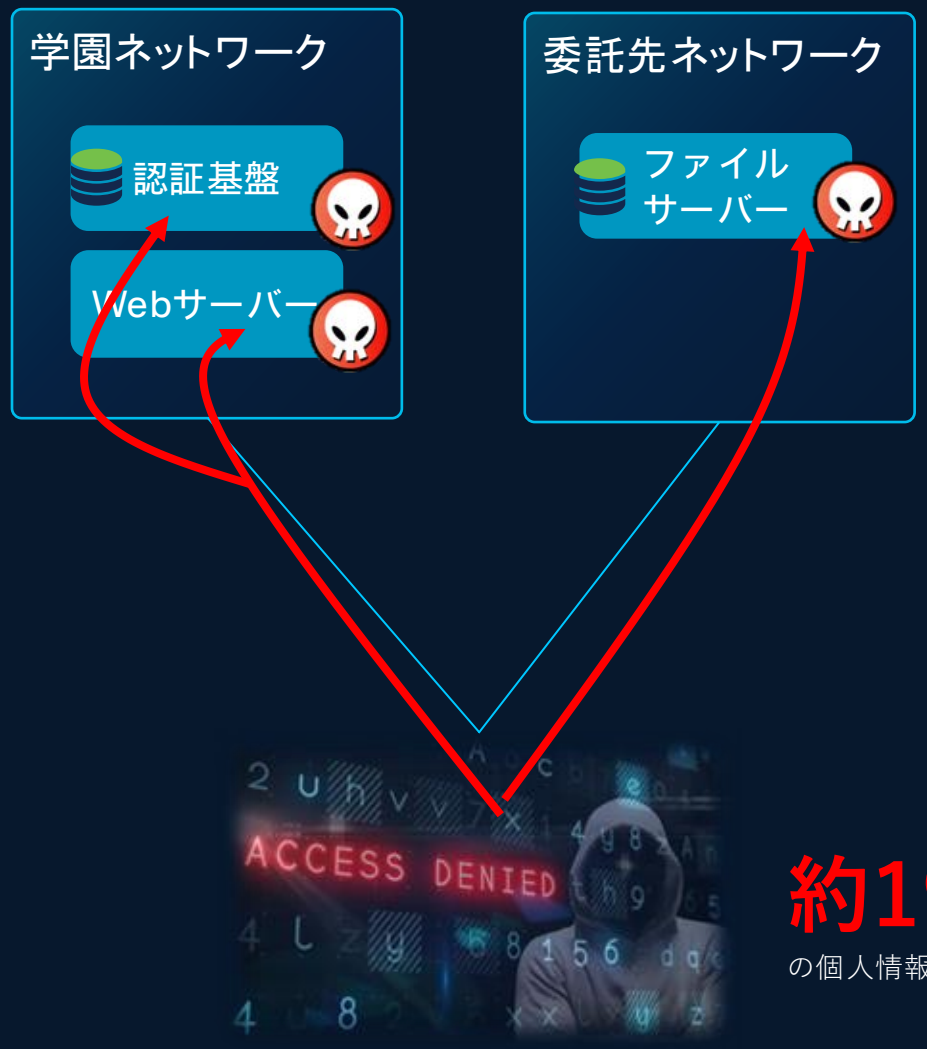
- **Active Directory**
  - *カスタム設定*
  - *複数ドメイン管理*
  - *レガシーシステムの設定*
  - *管理者および特権アカウントの管理*
  - *一時的なユーザー、サービスアカウント、NHIの管理*



IDを狙った攻撃のうち
ADを標的としている割合

Cisco Talos Incident Response | Active Directory-based Attacks

事例：某大学のランサムウェア攻撃



約19万人
の個人情報が外部へ流出

実際に起きたこと

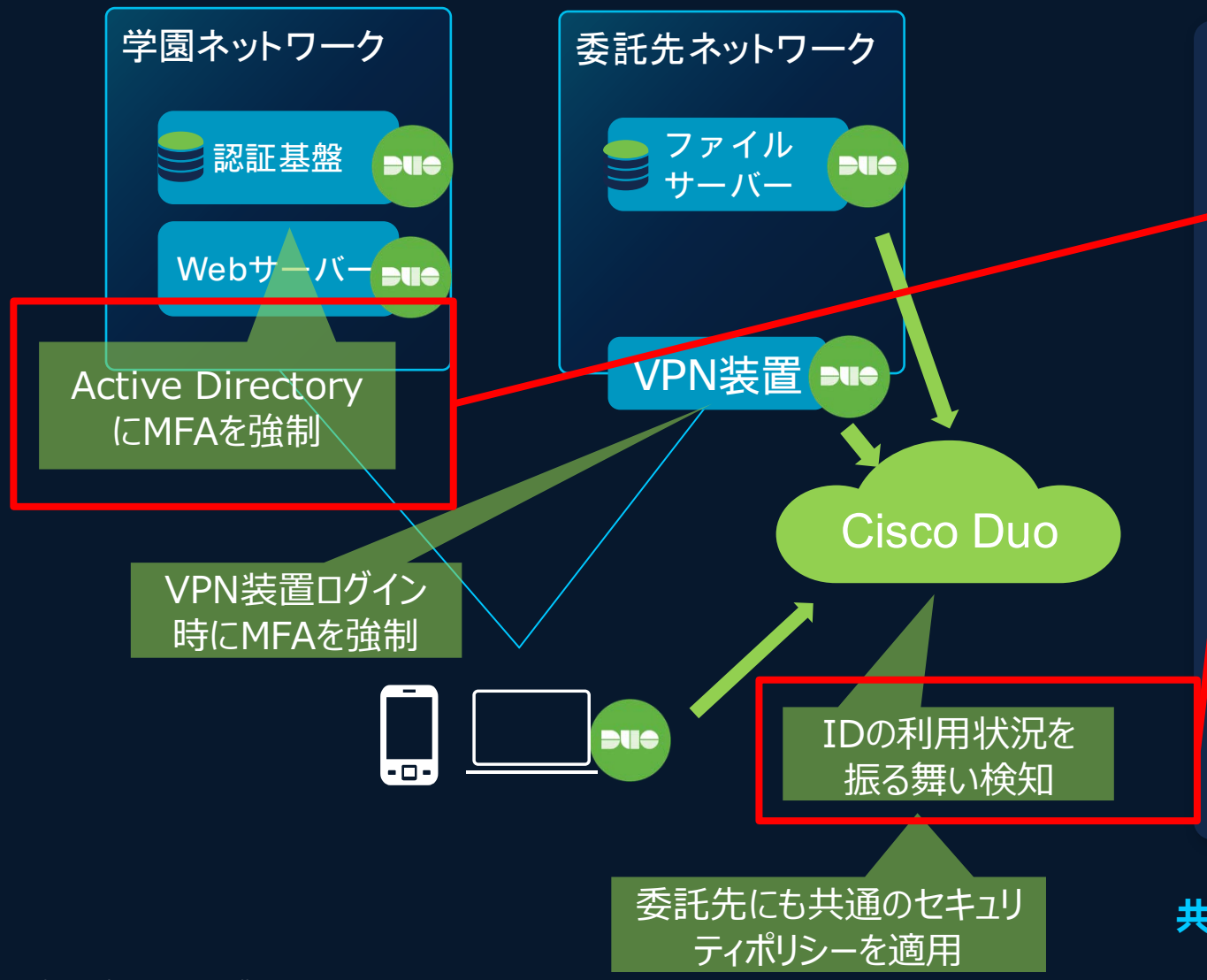
4月：フィッシングなど何らかの手段で、関係者のアカウント情報が窃取

IDを起点に学園内に侵入し、ランサムウェアで全6キャンパスに障害
認証情報 最大43,451件が暗号化、ポータル・公式サイト停止

11月：今度は委託先サーバーが被害
リモート保守の入口から、窃取した管理者アカウントで侵入

教職員・学生・保護者のID/パスワード漏洩の恐れ
MFA未実装サービスを緊急停止、全員パスワード一括リセット

事例：某大学のランサムウェア攻撃



Duo導入の効果

全サービスにMFAを強制
盗まれた認証情報だけでは侵入できない

Trusted Endpointsで端末を検証
未管理・不審な端末からの接続をブロック

ISPM / ITDRで常時監視
休眠アカウントや異常ログインを継続検知

委託先も含めた共通のセキュリティポリシーを適用
必要なアプリだけに最小権限でアクセス

共通のセキュリティポリシーでアイデンティティを保護

Cisco Duoが選ばれる理由

アイデンティティへの攻撃を阻止するセキュリティファーストIAM

フィッシング対策MFA

組織に合わせた柔軟なMFA

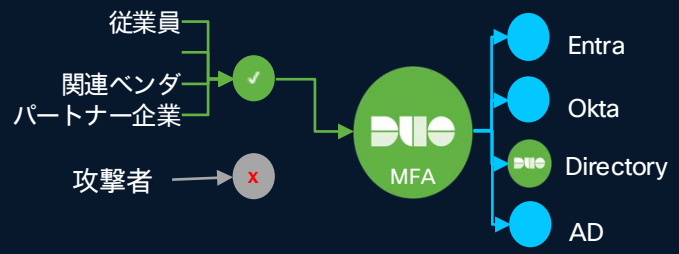
パスワードレス　近接認証

モバイルApp　Desktop

SMS　電話

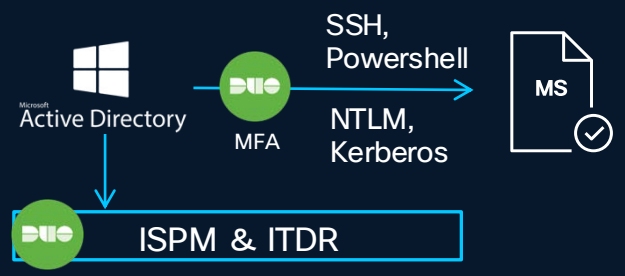
既存IdPを活かしたID統合

IdPをまとめない「ハブ型」認証基盤



Active Directory保護

Active Directoryを標的とした攻撃を阻止



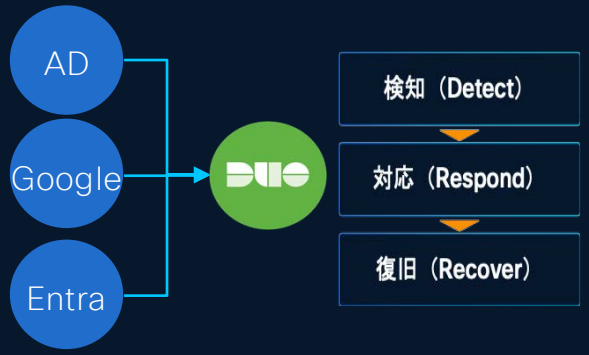
デバイスポスチャー

証明書に頼らない
安全なデバイスだけ認証を許可

PCの可視化

モバイルの可視化

ISPM & ITDR



ISPM　アイデンティティの健全性管理

MFA未適用、休眠ID、過剰特権アカウント

ITDR アイデンティティの振る舞い検知

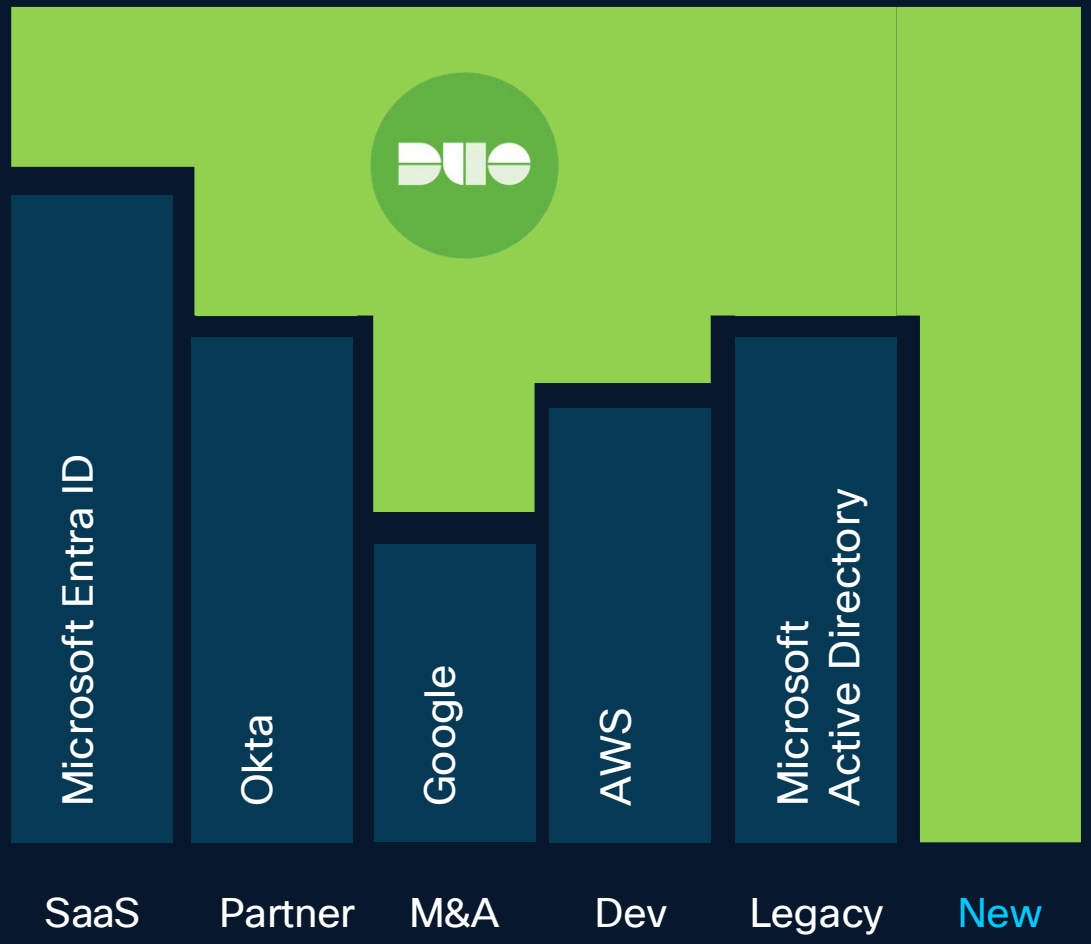
怪しい振る舞いのユーザーを即座に特定・隔離

Gartnerのレポート

Gartner® Peer Insights™ 2026 Voice of the Customerのアクセスマネジメント領域で「Customers Choice」に選出

https://www.gartner.com/doc/reprints?id=1-2NADO242&ct=260501&st=sb

DuoはIdentityのセキュリティにフォーカス



複雑なID環境へ強力なセキュリティを柔軟に安価に提供し、ギャップを埋める

ユーザーの快適性を損なわず、すべてのユーザーを守る

新 機 能

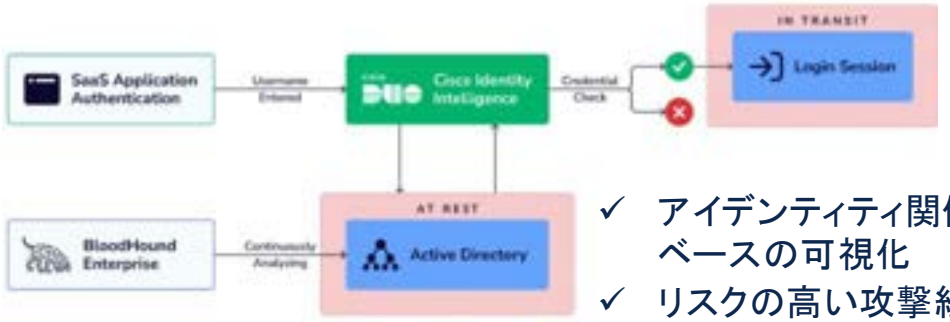
Active Directory Defense

Active Directory Defense の4つの機能

Active Directoryに存在するIDの可視化とリスク検出

- ✓ Identity Intelligenceと連携して、オンプレミスのActive Directoryの全ユーザー（管理者、ゲスト、サービスアカウントなど）を含むアイデンティティの完全なインベントリを提供
- ✓ 過剰権限や休眠アカウント、Kerberoasting攻撃などのリスクを可視化

ADの攻撃パスの検出（BloodHound Enterprise連携）

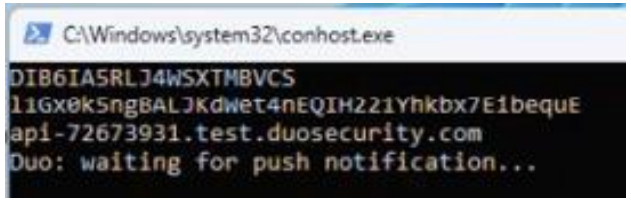


- ✓ アイデンティティ関係のグラフベースの可視化
- ✓ リスクの高い攻撃経路の検出とスコア化、修復方法の示唆
- ✓ 検出イベントのCIIへの連携

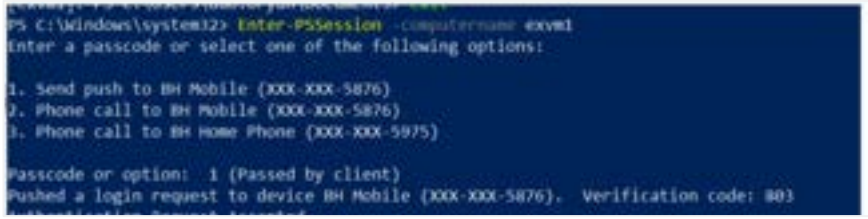
MFAの挿入によるレガシー認証の保護

- ✓ Active Directoryの認証プロトコル（KerberosやNTLM）に対して、MFAをシームレスに挿入し、不正アクセスを防止
- ✓ アプリ側ではなく、ドメインコントローラー（DC）に軽量なフィルターを1つ導入するだけ
- ✓ 特定グループや端末への適用も可能

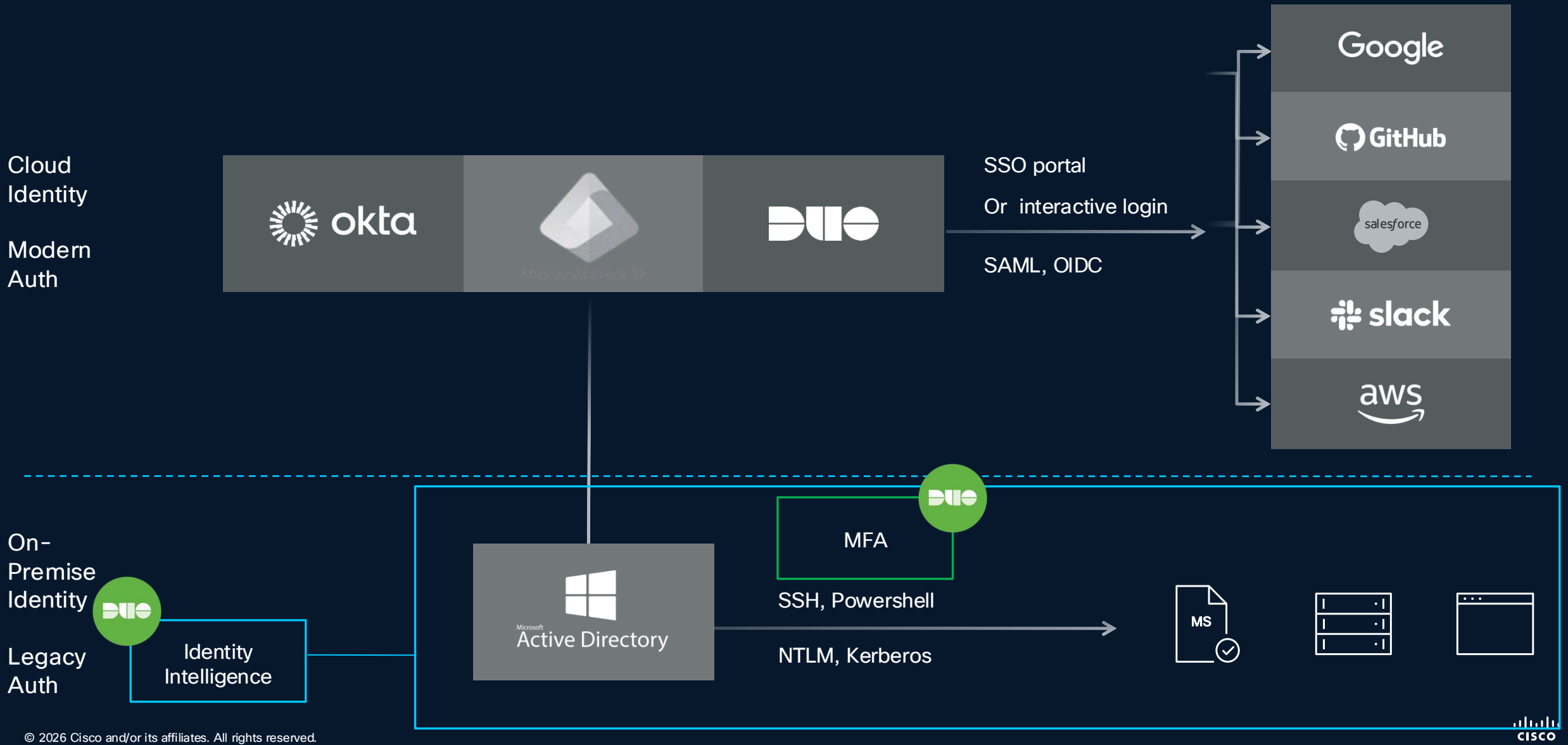
Windows Command Line Protection



- ✓ SSHやリモートPowerShellへのログイン時にMFAを適用する機能も提供



Active Directory Defenseの構成



Active Directoryに存在するIDの可視化とリスク検出

ユーザ毎にアクティビティを監視し、異常なふるまいを早期に発見

User 360 View

ユーザの詳細は「ユーザ 360 ビュー」と呼ばれます。

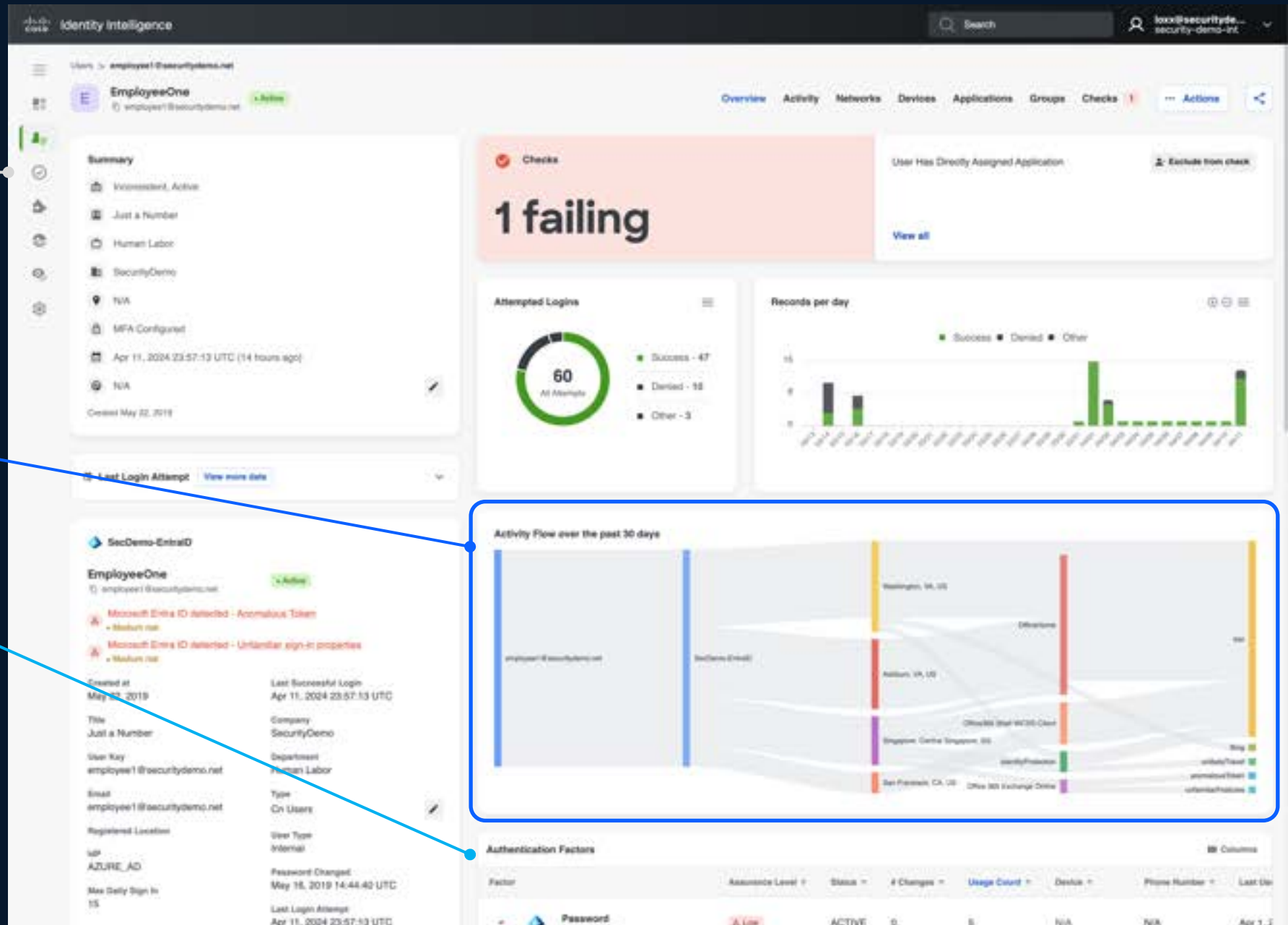
ユーザーのアイデンティティ関連のセキュリティ、アクティビティ、その他の重要なプロパティを表示します。

Activity Flow

ユーザーのアクティビティパターンがわかるビュー。

Combined Auth Log

各IDPからのユーザー認証と要素がわかるビュー。



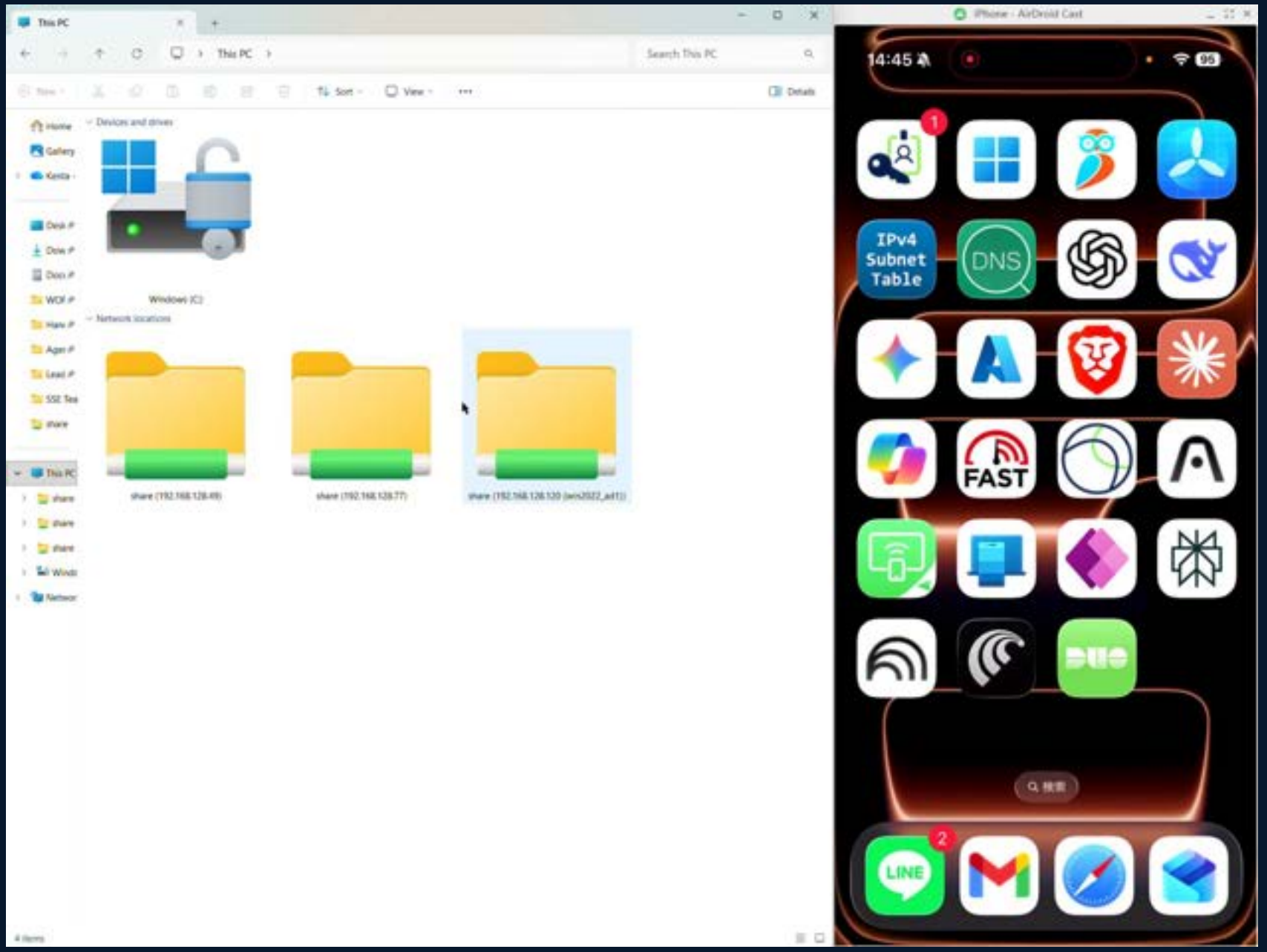
Active Directoryへの攻撃を可視化

Check	# Failing	# Excluded	Report Channels
42% NHI with No Owners Assigned • Critical Non-Human Identities - Identity Posture Insight, Non-···	11 → No change since last week → No change since last month	N/A	+ Add
94% NHI with Deprovisioned Owners • Critical Non-Human Identities - Identity Posture Insight, Identi···	1 → No change since last week → No change since last month	N/A	+ Add
96% User Password Expiration Failure • Moderate End Users - Identity Posture Insight	35 → No change since last week → No change since last month	0	+ Add
97% Inactive Users • Moderate End Users - Compliance, Identity Posture Insight	21 → No change since last week → No change since last month	0	+ Add
99% Provider User Type Missing • Moderate End Users - Compliance, Identity Posture Insight	5 → No change since last week → No change since last month	0	+ Add
99% Never Logged In • Critical End Users - Compliance, Identity Posture Insight	4 → No change since last week → No change since last month	0	+ Add
99% User Trust Level Alert • Critical End Users - Identity Threat Insight	4 → No change since last week → No change since last month	0	+ Add
99% Non-Human Identity Password Expiration Fai··· • Moderate End Users - Identity Posture Insight, Non-Human Id···	3 → No change since last week → No change since last month	0	+ Add
99% Kerberoastable Accounts • Moderate End Users - Identity Posture Insight	1 → No change since last week → No change since last month	0	+ Add
99% Attack Path Alert • Moderate End Users - Identity Posture Insight	2 → No change since last week → No change since last month	0	+ Add

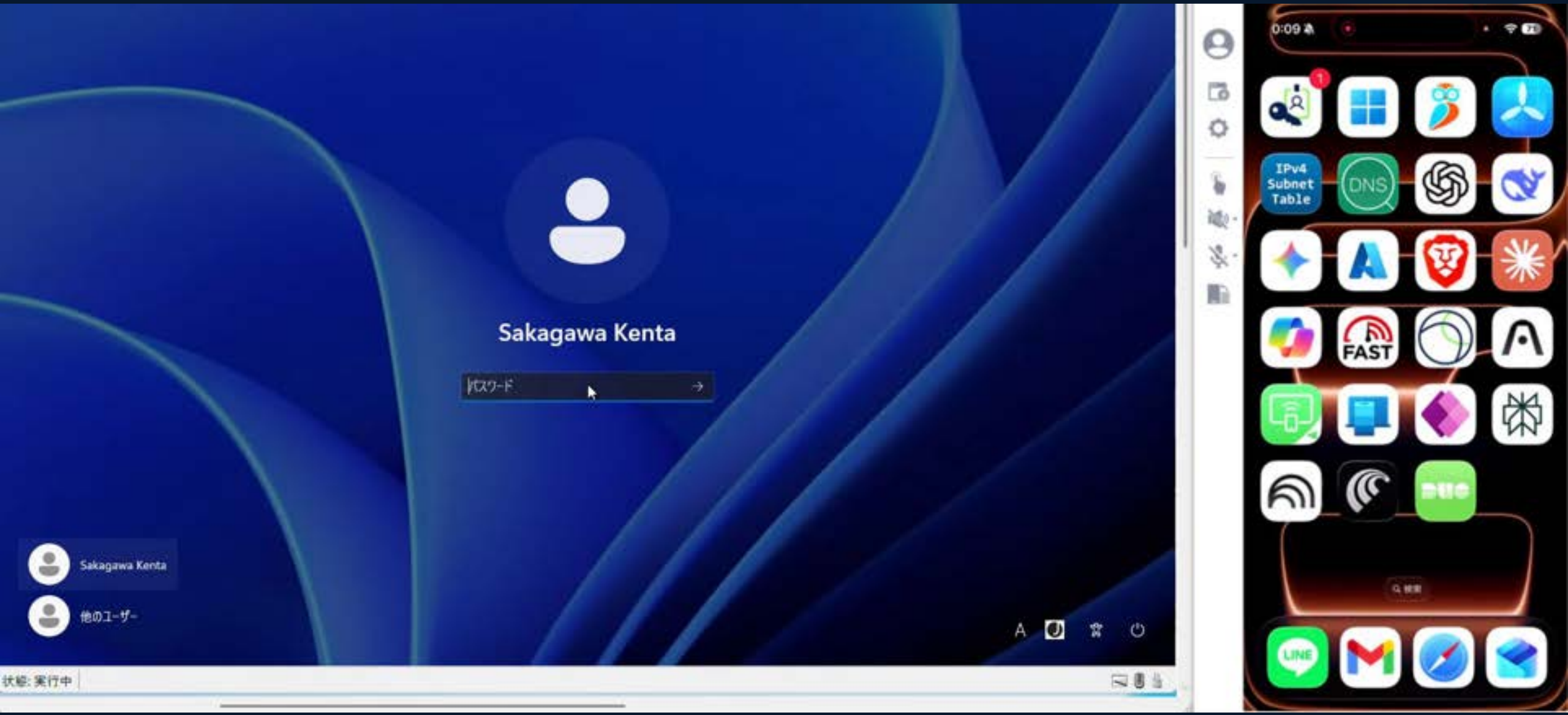
MFAの挿入によるレガシー認証の保護

デモ動画 ① NTLM 認証：共有フォルダへのアクセス例

これは、共有フォルダにアクセスする際に、通常のユーザー名とパスワードに加えてMFA（多要素認証）を使用する方法のデモ動画です。

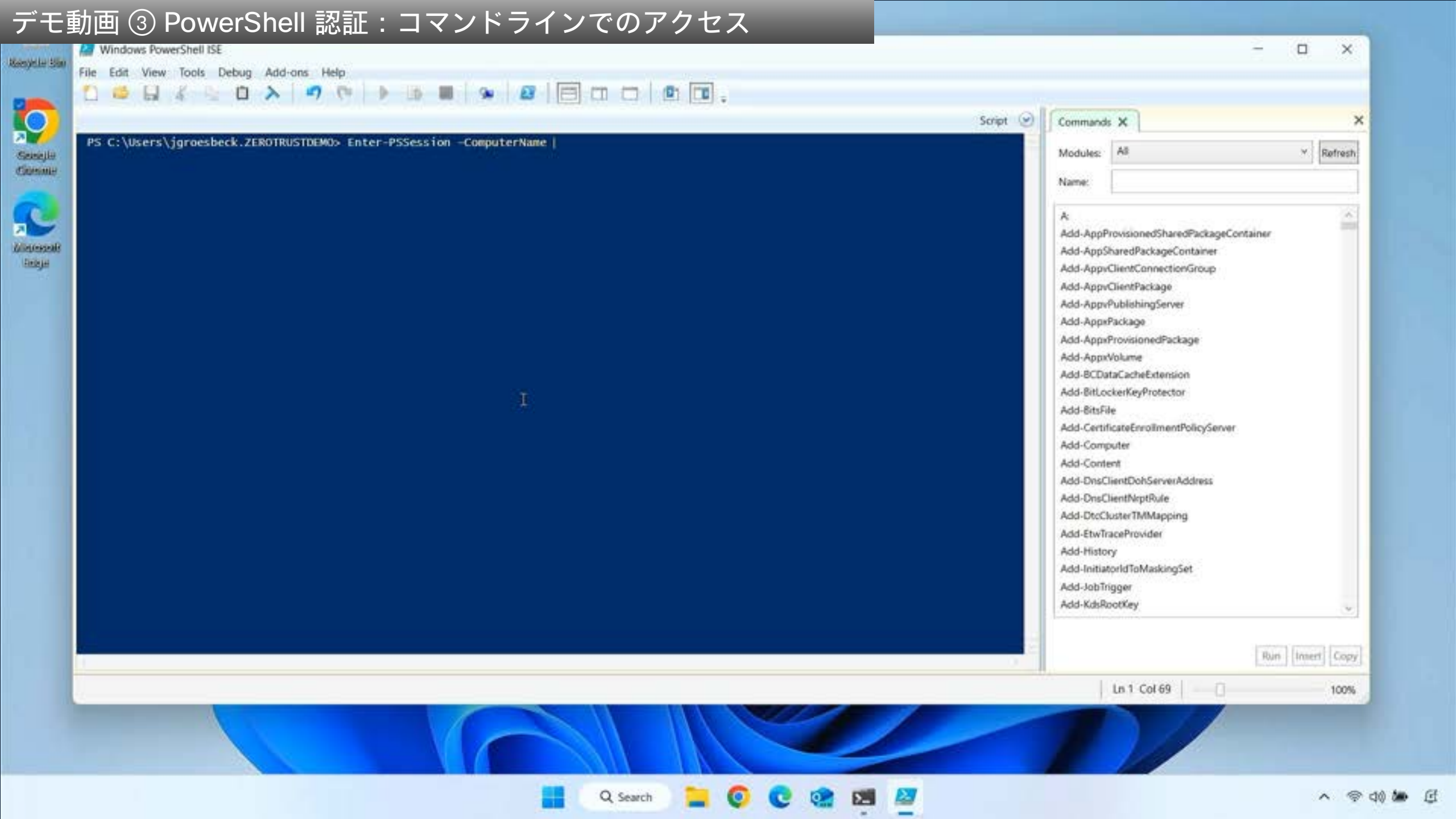


デモ動画 ② Kerberos 認証：ドメインユーザでのOSログイン



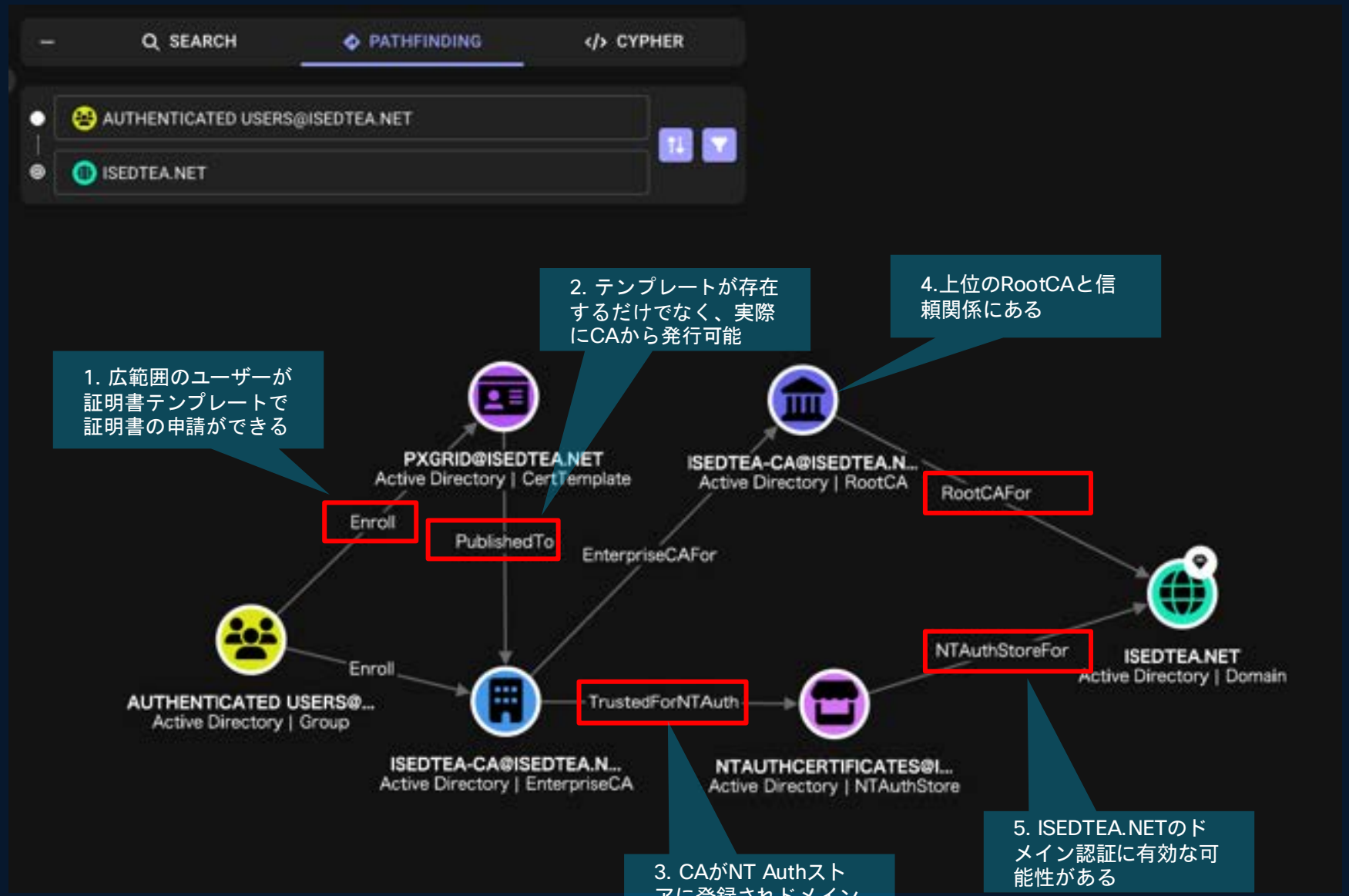
Windows Command Line Protection

デモ動画 ③ PowerShell 認証：コマンドラインでのアクセス



ADの攻撃パスの検出
（BloodHound Enterprise連携）

攻撃パスの可視化



ADCSESC1

関係情報

ソースノード: 認証済みユーザー@ISEDTEA.NET

ターゲットノード: ISDTEA.NET

ブラッドハウンドによる最終目撃情報：
2026-06-05 12:14 GMT+9 (GMT+0900)

一般的な

グループAUTHENTICATED USERS@ISEDTEA.NETのメンバーは、ターゲットドメインに対してADCS ESC1攻撃を実行する権限を持っています。

プリンシパルは、1つ以上の証明書テンプレートに登録する権限を持ち、代替のサブジェクト名を指定して証明書を認証に使用できます。また、必要なテンプレートが公開されているエンタープライズCAへの登録権限も持っています。このエンタープライズCAは、ルートCA証明書までの証明書チェーンとともに、フォレスト内のNT認証で信頼されています。この設定により、プリンシパルは任意のADフォレストユーザーまたはコンピューターの証明書を登録でき、資格情報なしで任意のADフォレストユーザーまたはコンピューターの認証となりすましが可能になります。

Windowsの悪用

攻撃者は、以下の手順でこの攻撃を実行する可能性があります。

ステップ 1：Certify (2.0) を使用して、影響を受けるテンプレートへの登録を要求し、影響を受ける認証局となりすます対象プリンシパルを指定します。

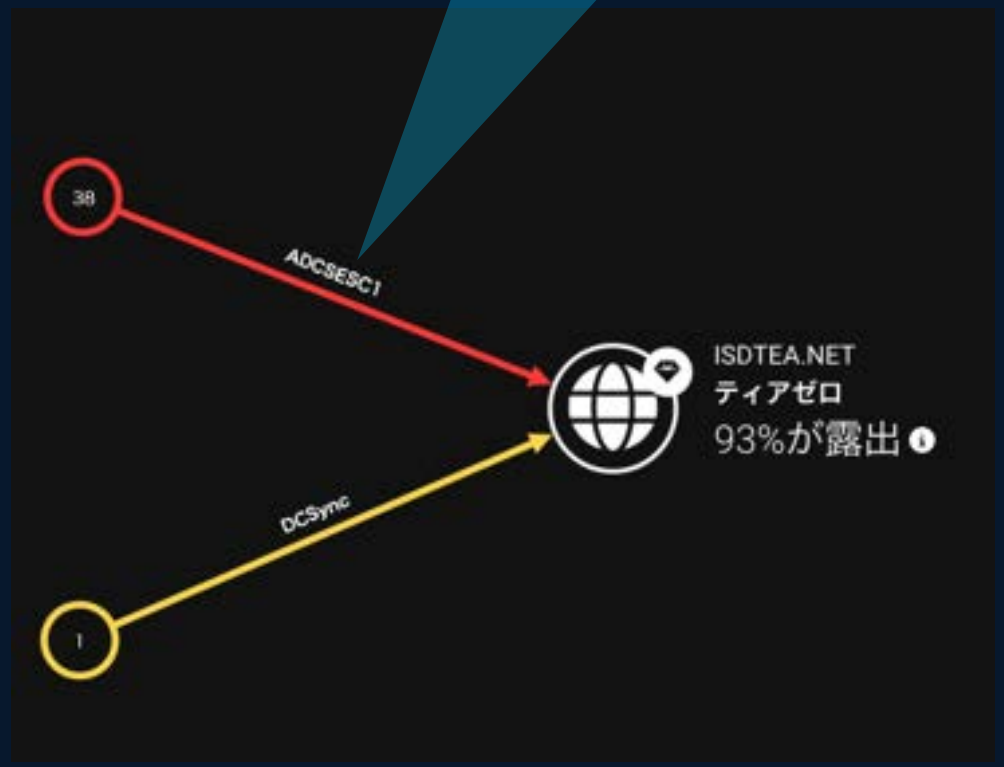
```
Certify.exe request --ca rootdomaindc.forestroot.com\forestroot-RootDomainDC-CA --template ESC1 --upn Administrator --sid S-1-5-21-976219687-1556195986-4104514715-500
```

証明書のPFXファイルは、base64エンコードされた形式でコンソールに表示されます。

ステップ2：Rubeusを使用して、証明書を使ってドメインへの認証を行い、なりすます予定のIDを指定してTGTを要求します。

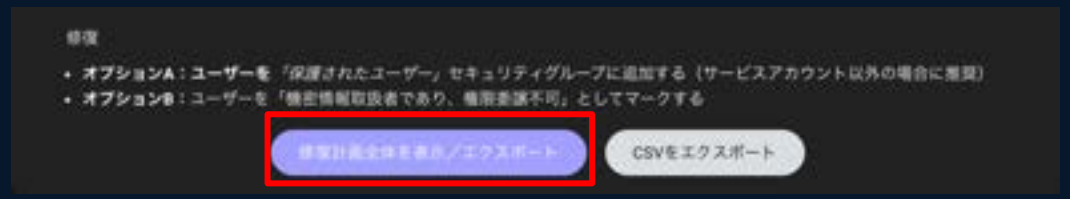
リスクの可視化・優先順位付け

チョークポイント：
これを改善することで、配下の攻撃パスの本数を大幅に減らすことができる。



優先度ごとにチョークポイントを明確化して、
対応すべき脅威を特定

修復支援



具体的な推奨手順を表示

オプションA：保護対象ユーザーセキュリティグループにティアゼロユーザーを追加する

1. ティアゼロのアカウント（例えば、*ドメイン管理者*グループのメンバー）を使用して、Active Directoryユーザーとコンピューター（ADUC）を開きます。
2. *PROTECTED USERS*セキュリティ グループを探します（このグループのデフォルトの場所は、デフォルトの「Users」コンテナの直下です）。
3. 「*保護されたユーザー*」グループを右クリックし、「プロパティ」をクリックします。
4. 「プロパティ」ウィンドウの「メンバー」タブをクリックします。
5. 各ティアゼロユーザーについて、「追加...」をクリックし、該当するティアゼロユーザーを見つけて、「OK」をクリックします。
6. すべてのティアゼロユーザーがグループに追加されたら、「適用」をクリックし、「OK」をクリックします。

オプションB：ユーザーを「機密情報取扱者であり、権限委譲不可」としてマークする

「機密情報であり、委任不可」としてマークする必要があるユーザーごとに、以下の手順を実行してください。

1. ADUCにログインするには、 Tier Zeroアカウント（例： *DOMAIN ADMINS*グループのメンバー）を使用してください。
2. 検索機能を使用するか、組織単位（OU）ツリーでユーザーに移動して、ユーザーを見つけます。
3. ユーザーを右クリックして「プロパティ」をクリックします。
4. 「ユーザープロパティ」ウィンドウの「アカウント」タブをクリックします。
5. 「アカウントオプション」リストで、「アカウントは機密情報であり、委任できません」という項目までスクロールします。
6. 「アカウントは機密情報が含まれているため、委任できません」というリスト項目の横にあるチェックボックスをクリックし、「OK」をクリックします。

ライセンス

Pricing & Packaging

Duo Essentials

従業員のアイデンティティ保護を強化するために、シンプルかつ効果的なツールを導入する。

$3 | User | Month

- Duo Directory
- Complete Passwordless
- 近接認証
- AI Assistant
- Multi-Factor authentication
- Single Sign-On
- Trusted Endpoints
- 登録アプリ制限なし

Duo Advantage

ログイン前、ログイン中、ログイン後の全段階で機能する継続的なアイデンティティセキュリティへアップグレード

$6 | User | Month

- Duo Passport
  - Session Protection
- Cisco Identity Intelligence
- Adaptive authentication
- Risk-based authentication
- Active Directory Defense
  - \+ Attack Path Management: Partnership with SpecterOps

Duo Premier

クラウド、オンプレミス、およびプライベートなアプリケーションやリソースに対する保護を強化し、シームレスなアクセスを可能にします。

$9 | User | Month

- Secure VPN-less remote access
- 3rd party EDR agent check

Seamless Identity Verification: Partnership with Persona

まとめ

オンプレADを守るAD Defenseとは

背景：
なぜ今、オンプレADなのか

✓ 攻撃は 高度化・自動化 し、**オンプレADを起点に特権アカウントを奪う攻撃 が主流**になっている。これを 未然に防ぐ ため、Cisco Duo はオンプレAD向けの防御機能（Active Directory Defense） を開発

お客様の課題：
ADは「残り続け、狙われ続けている」

1. ADは今もビジネスの中核：80%以上の企業 がオンプレADまたはハイブリッド環境に依存
2. ADは常に攻撃の起点 （Cisco Talos（2024）アイデンティティ起点攻撃の 約50%がADを標的）
   ⇨悪用されるのは過剰な権限 / 弱いパスワード / MFA未導入
3. 可視性が足りない ：ハイブリッドなアイデンティティ環境を一元的に把握できていない「見えていないから、守れない」
4. レガシーアプリが最大の穴 ：AD認証のレガシーアプリは最新の認証・セキュリティ制御に非対応
   ⇨攻撃者にとって最も狙いやすいポイント

Cisco Duoの対策：
オンプレADを「3層」で守る

1. 可視化（見える化） オンプレAD内の 全アカウント（人・サービス） を一元管理
   ⇨非アクティブユーザ、ゲスト、パスワード不備を検知、Identity Intelligence に統合してユーザ可視化
2. 認証強化（止める） ：オンプレADログインに MFAを強制
   ⇨Windows Logon、Kerberos、NTLM、Windows Powershell CLI認証時にレガシー環境でも MFAを後付け可能
3. 攻撃パスの可視化・管理（防ぐ） ：AD上の 攻撃パスを可視化 権限構造のリスクを把握し、是正へつなげる


CISCO