サイバーセキュリティ最前線:
Talos 脅威インテリジェンスが示す、今求められる対策とは

GSSO Account Executive ID Security Sales Cisco Systems G.K.
Hiroki Hata, Takashi Yamamoto

April 2025

自己紹介

秦　寛樹　Hiroki Hata
Account Executive Identity Security

日系企業にてSE、コンサルタント、マーケティングに従事した後、2020年にシスコ（Duo）へ入社

入社以来一貫してIdentity Security分野のセールス代表として日本の市場をリード

山本　剛之　Takashi Yamamoto
Solutions Engineer

日米露のセキュリティベンダーにてテクニカルサポート、営業、SEなどに従事した後、2021年にシスコへ入社

アイデンティティセキュリティとSSEソリューションを主に担当

ID管理

再掲

機能領域	カテゴリ	カテゴリ
ガバナンス(GV)		
識別(ID)	ID.AM	資産管理
防御(PR)	PR.AA	資産へのアクセス
検知(DE)	⋮	⋮
対応(RS)		
復旧(RC)		

資産管理は、セキュリティの一丁目一番地

IDを管理することも、資産管理の一部

IDの管理も、範囲(網羅性)と深さ(成熟度)を上げましょう。

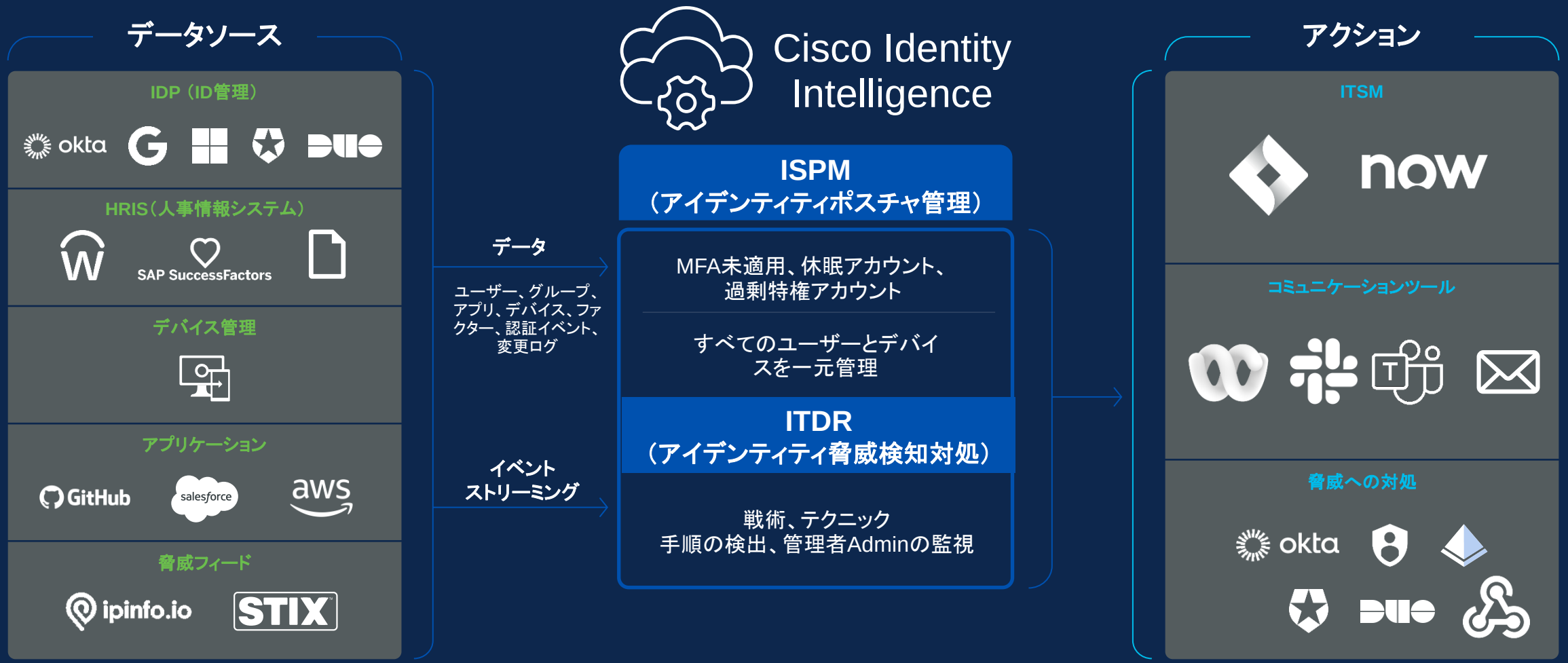
- 休眠アカウントありませんか？
- IDに関するLogを取得していますか？
- 多要素認証実施していますか？

アジェンダ

1) Cisco Identity Intelligence によるIDリスクの管理
2) デモ: IDリスクの可視化
3) アイデンティティセキュリティ アセスメント事例
4) Cisco XDR 最新アップデート
5) デモ: Cisco Identity Intelligence と Cisco XDR 連携で実現するレスポンスオートメーション
6) 本日のまとめ

Cisco Identity Intelligence による ID リスクの管理

Identity Threat Detection & Response – Cisco Identity Intelligence



Cisco Duo（多要素認証･デバイス認証）Advantageに搭載してリリース

Cisco Identity Intelligence 画面デモ

Cisco Identity Intelligence のユースケース

ユーザ情報
一元管理

非従業員
アカウント
モニタリング

MFA
設定状況・
利用状況
モニタリング

IAM分析
レポート

ユーザ状況及
びセッション
状況
調査分析

継続的な
脅威検出

デモ: Cisco Identity IntelligenceによるID リスクの可視化

1) 非従業員アカウント モニタリング

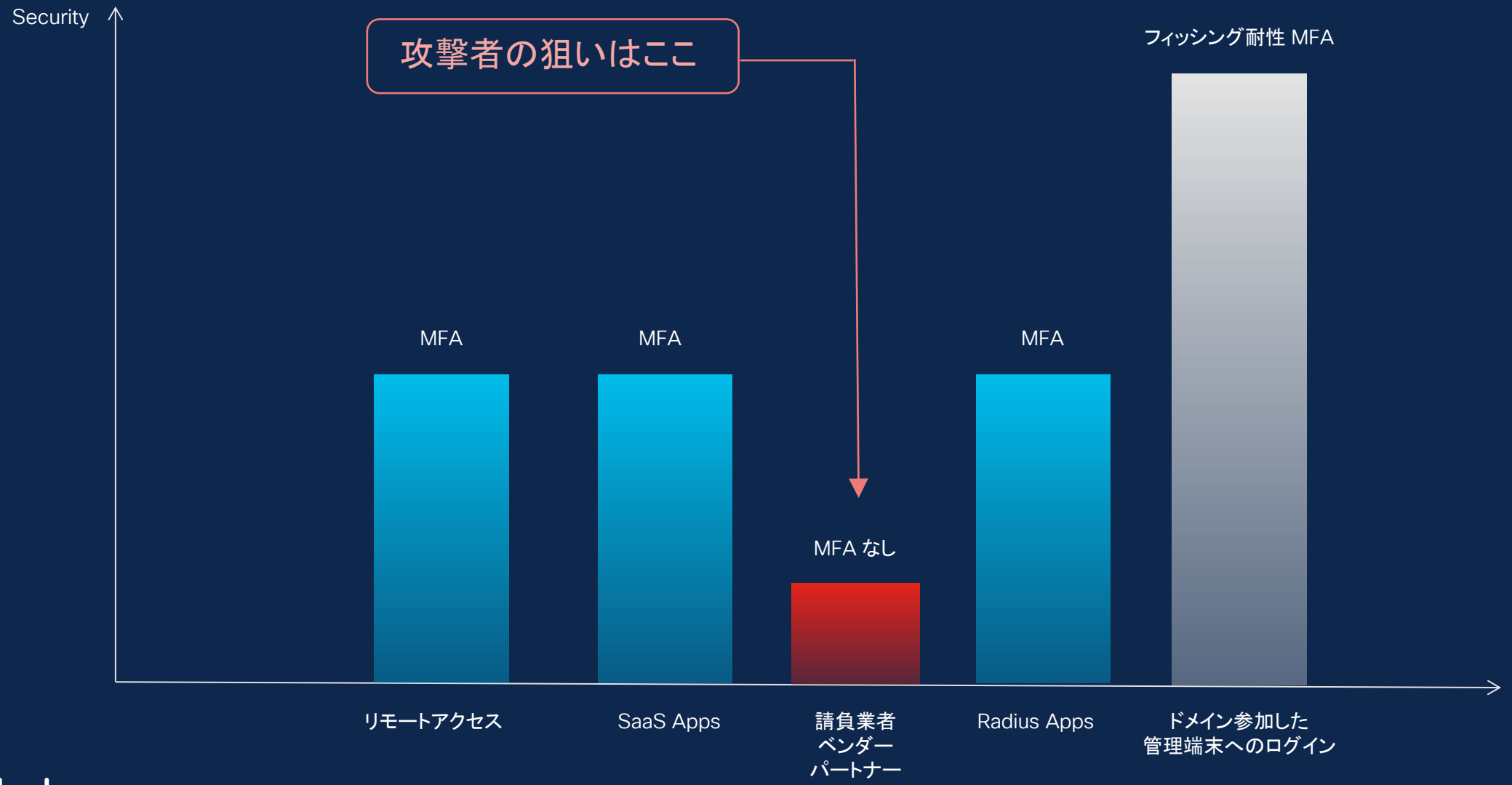
2) 休眠アカウントの管理

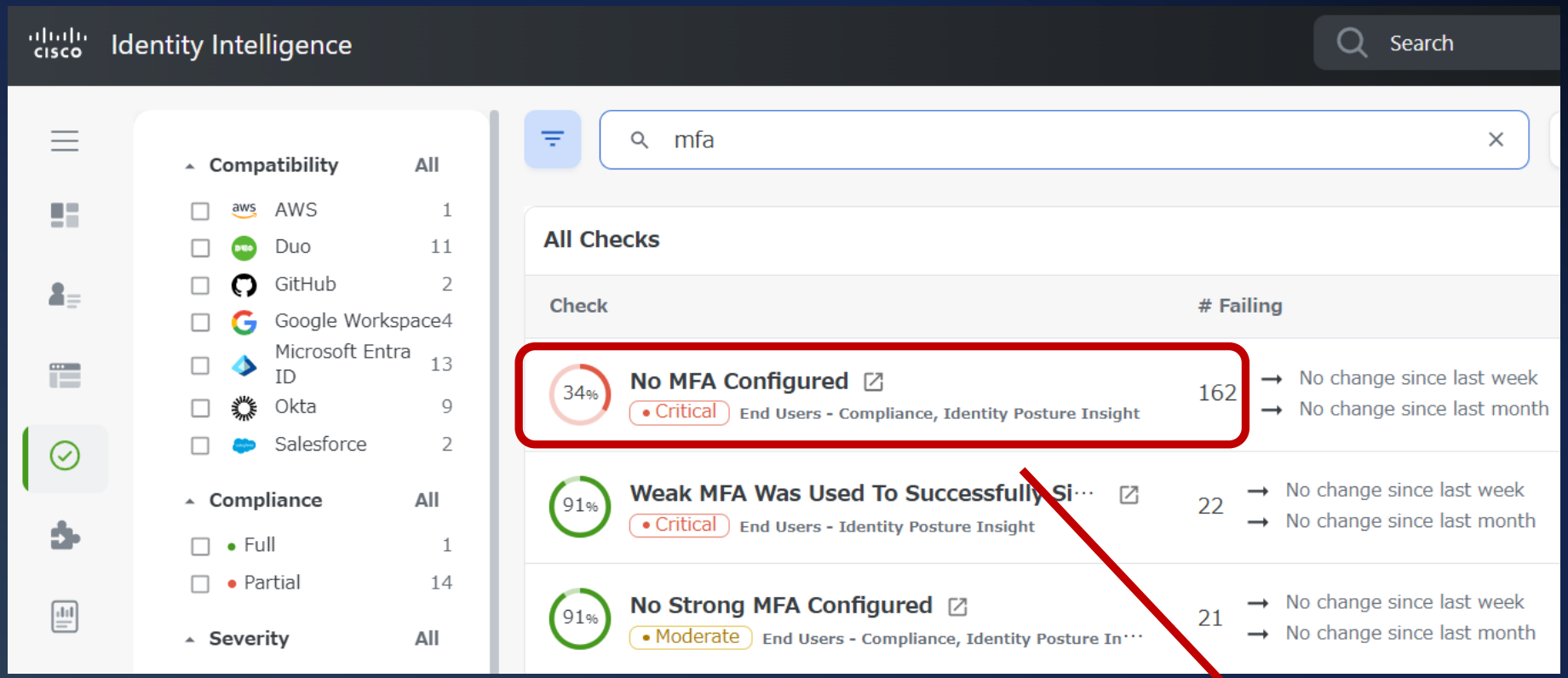
3) 継続的な脅威の管理　3パターン

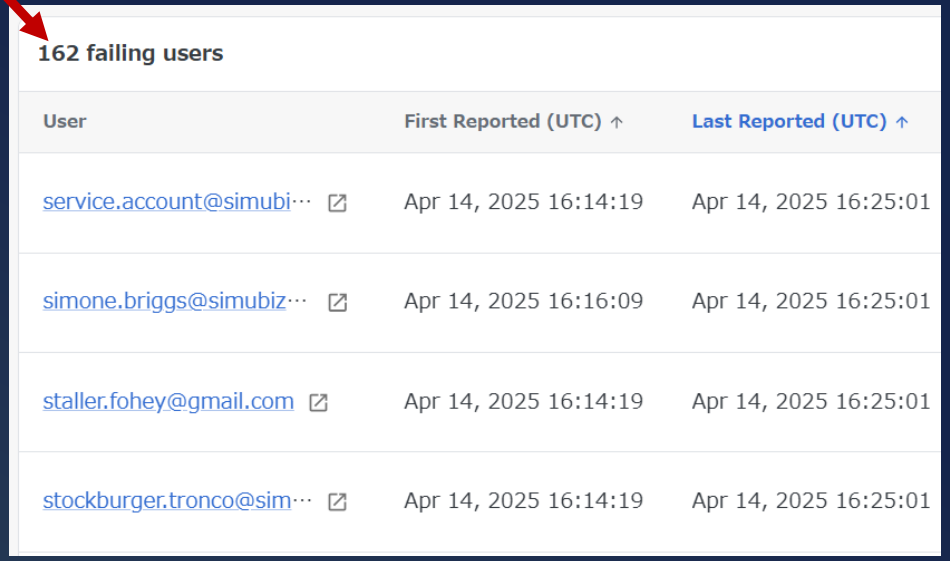
Cisco Identity Intelligence Demo

ユースケース①
非従業員アカウント
モニタリング

課題: ID のセキュリティ対策に差異がある







Cisco Identity Intelligence Demo

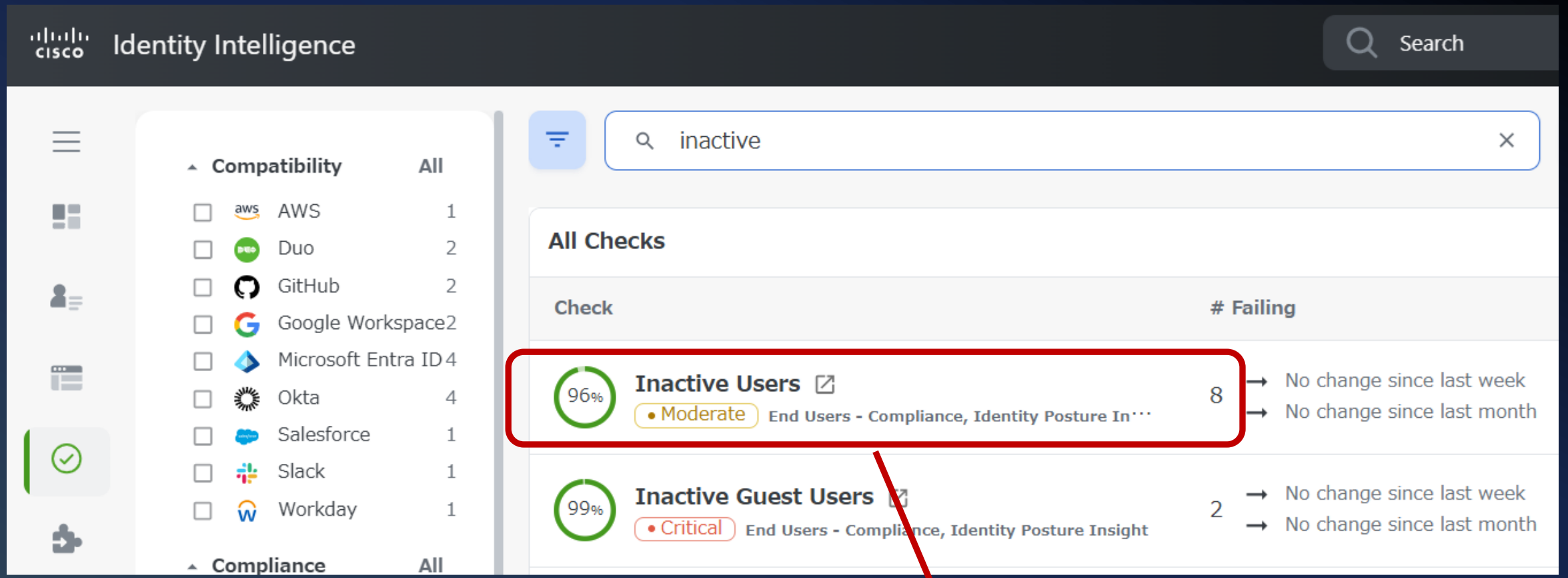
ユースケース②
休眠アカウントの管理

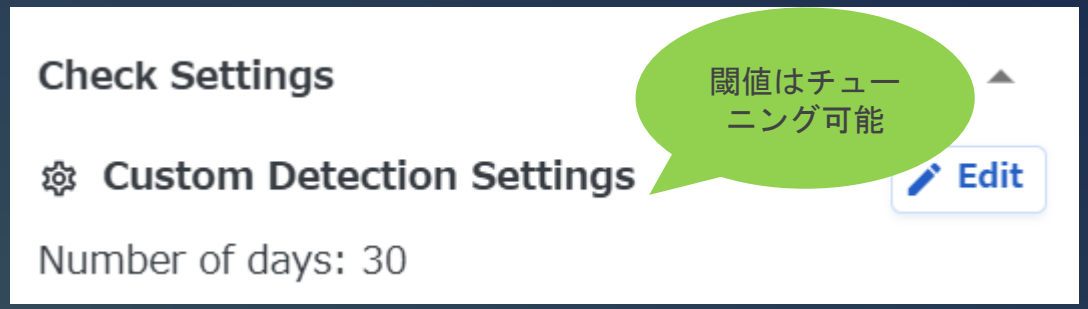
課題: 休眠アカウントの管理ができていない

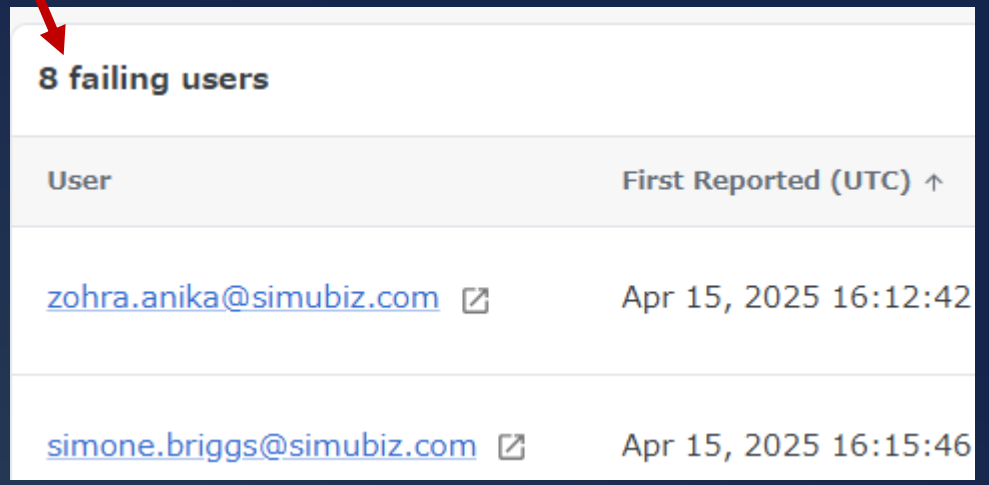
休眠アカウントが残っていることのリスク

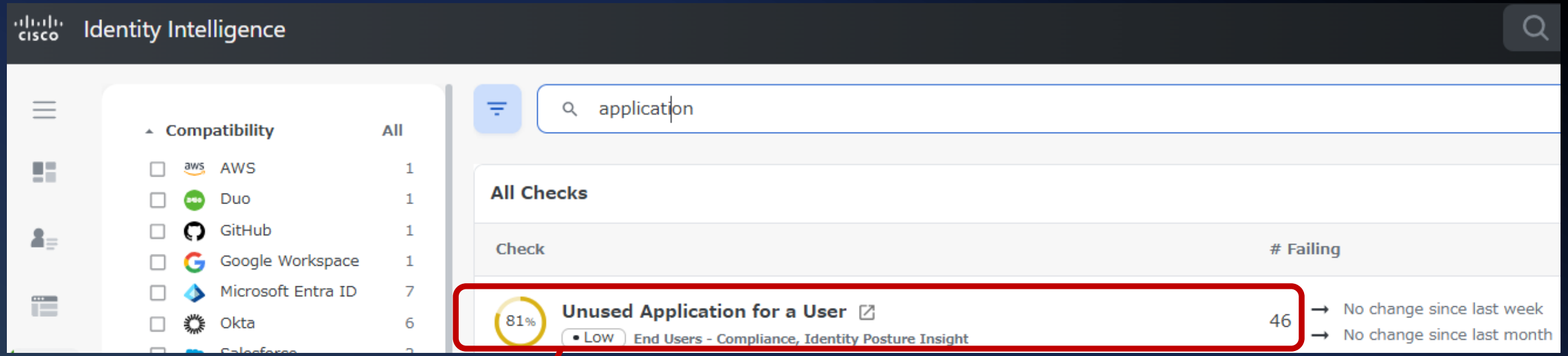
- **不正ログインのリスク**
  長期間利用されていないアカウントは、古いパスワードや再利用されたパスワードを使用している可能性が高く、悪意のある攻撃者に不正にログインされやすくなります。
- **個人情報漏洩のリスク**
  アカウントにログインされると登録されている氏名、メールアドレス、電話番号等の個人情報が漏洩する可能性があります。
- **なりすましによる悪用のリスク**
  不正にアクセスされたアカウントは、本来の利用者になりすまして犯罪行為やスパム配信、フィッシング詐欺などの悪意ある活動に利用される可能性があります。

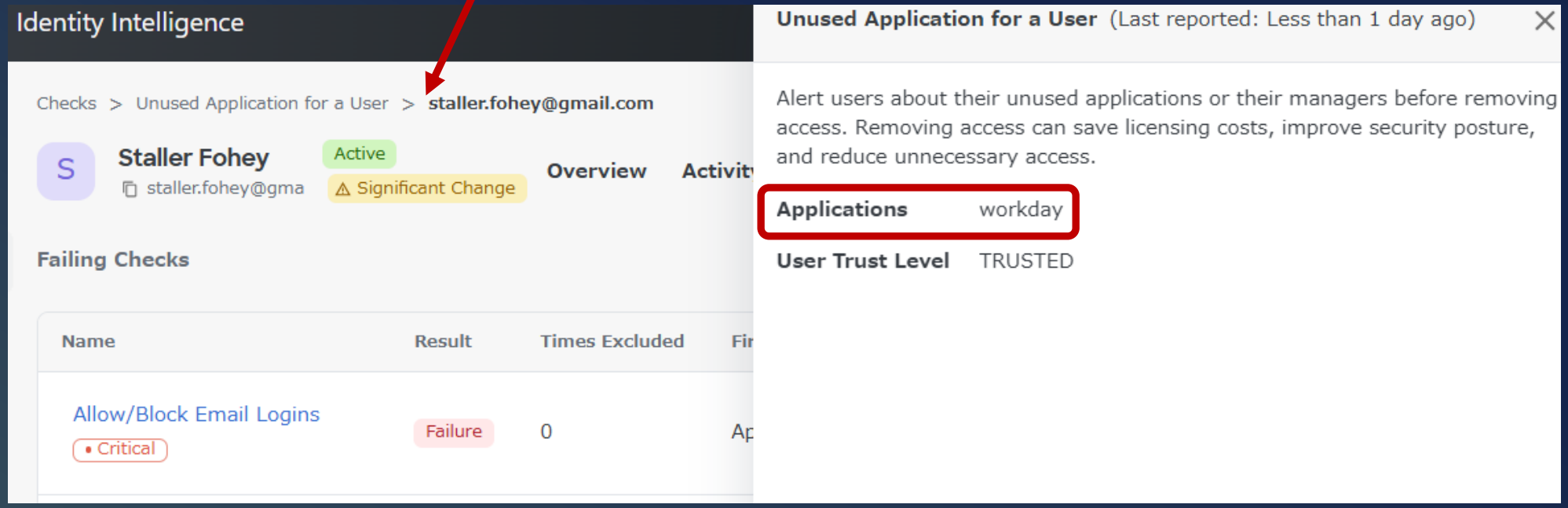
加えて、ライセンス費用も多く支払っている可能性が高い









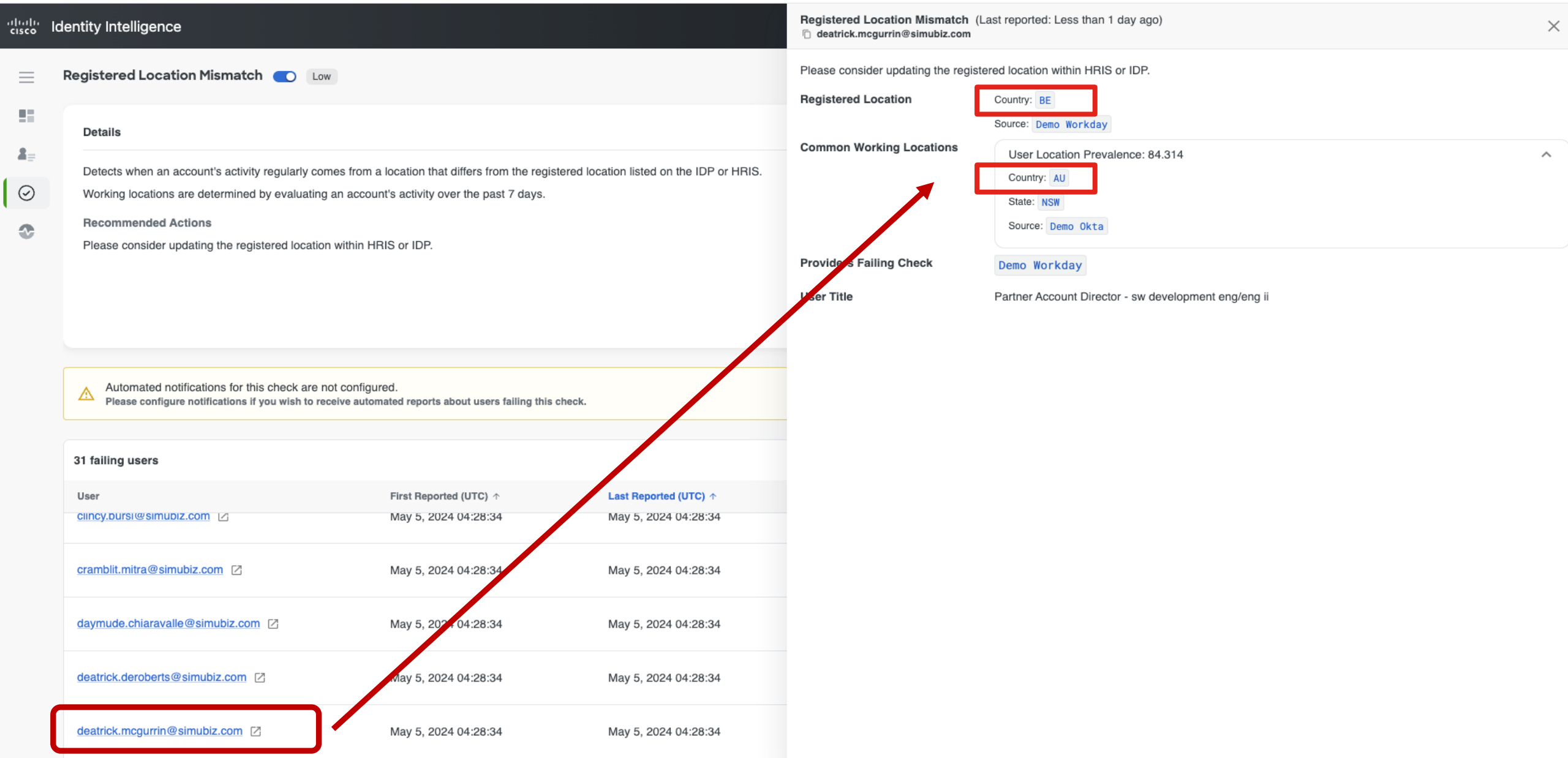


Cisco Identity Intelligence Demo

ユースケース③
継続的な脅威検出

課題: 継続的な脅威の管理

- 通常の勤務地以外の場所からのアクセス
- 移動が不可能な場所からのアクセス
- 同じユーザで複数セッションが発生



K **Kolluri Hofferber**
kolluri.hofferber@simubiz.com
Fremont, CA, US
Active

Overv

Failing Checks

Name	Result	Times Excluded	First Reporte
Activity From Untrustworthy ISP • Moderate	Failure	0	Sep 24, 202
Impossible Travel • Moderate	Failure	0	Sep 24, 202
Weak MFA Was Used To Successfully Sign In • Critical	Failure	0	Sep 24, 202
Registered Location Mismatch • Low	Failure	0	Sep 24, 202
Unused Application for a User • Low	Failure	0	Sep 24, 202
User in IDP but not in HRIS • Critical	Failure	0	Sep 24, 202
No Strong MFA Configured • Moderate	Failure	0	Sep 24, 202

Impossible Travel (Last reported: Less than 1 day ago)

Providers Failing Check Demo Okta

Travels

Distance: 8978208 m

First Event

⚠ VPN

Event Date: Sep 23, 2024 20:14:40 UTC

IP Address: 104.250.182.36

IP Prevalence: 0.042

Device Age: 0

User IP Age: 0

Country: GE

City: Tbilisi

State: Tbilisi

User Agent: mozilla(macintosh;intelmacosx__)applewebkit(khtml,likegecko…

OS: Mac os x

Browser: Unknown

Second Event

⚠ VPN

Event Date: Sep 23, 2024 23:59:59 UTC

IP Address: 46.3.27.137

IP Prevalence: 0.042

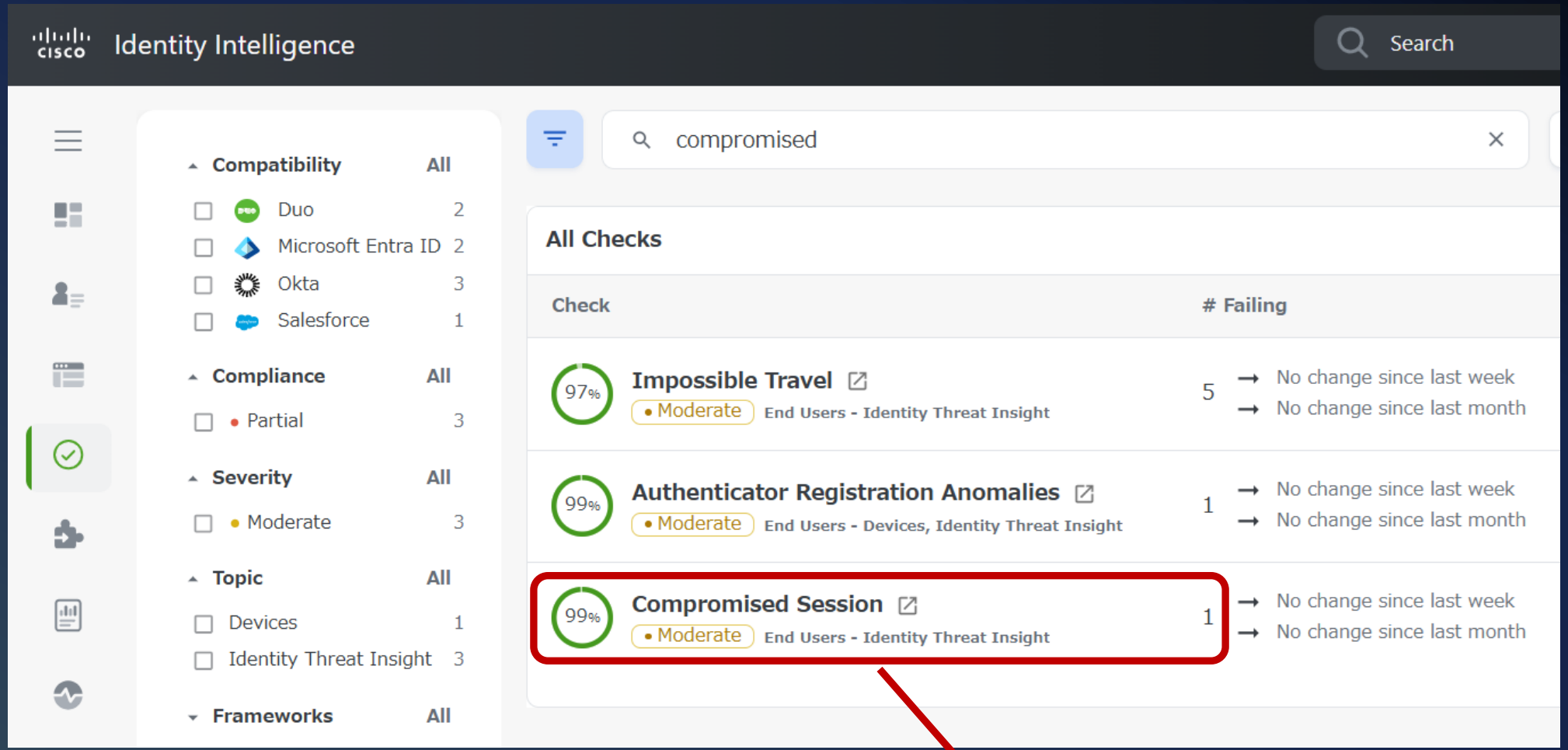
Device Age: 0

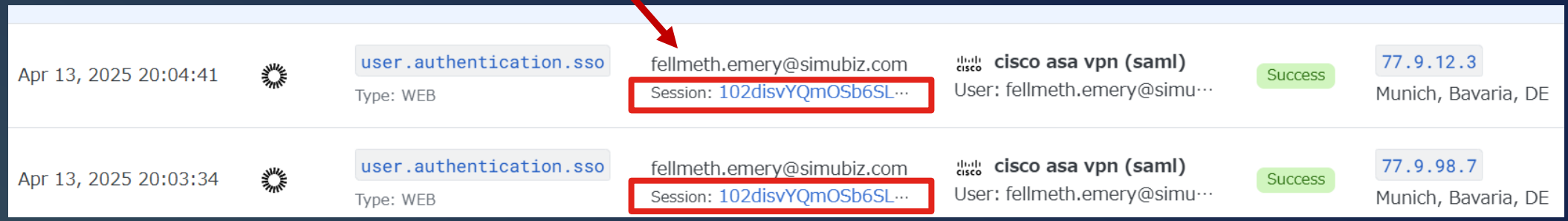
User IP Age: 0

Country: US

City: New York City

State: New York





Cisco Identity Intelligenceを使った Identity Security アセスメント事例

無償のCisco Identity セキュリティアセスメント

お客様のアイデンティティエコシステムに対する可視化レポートをご提供します

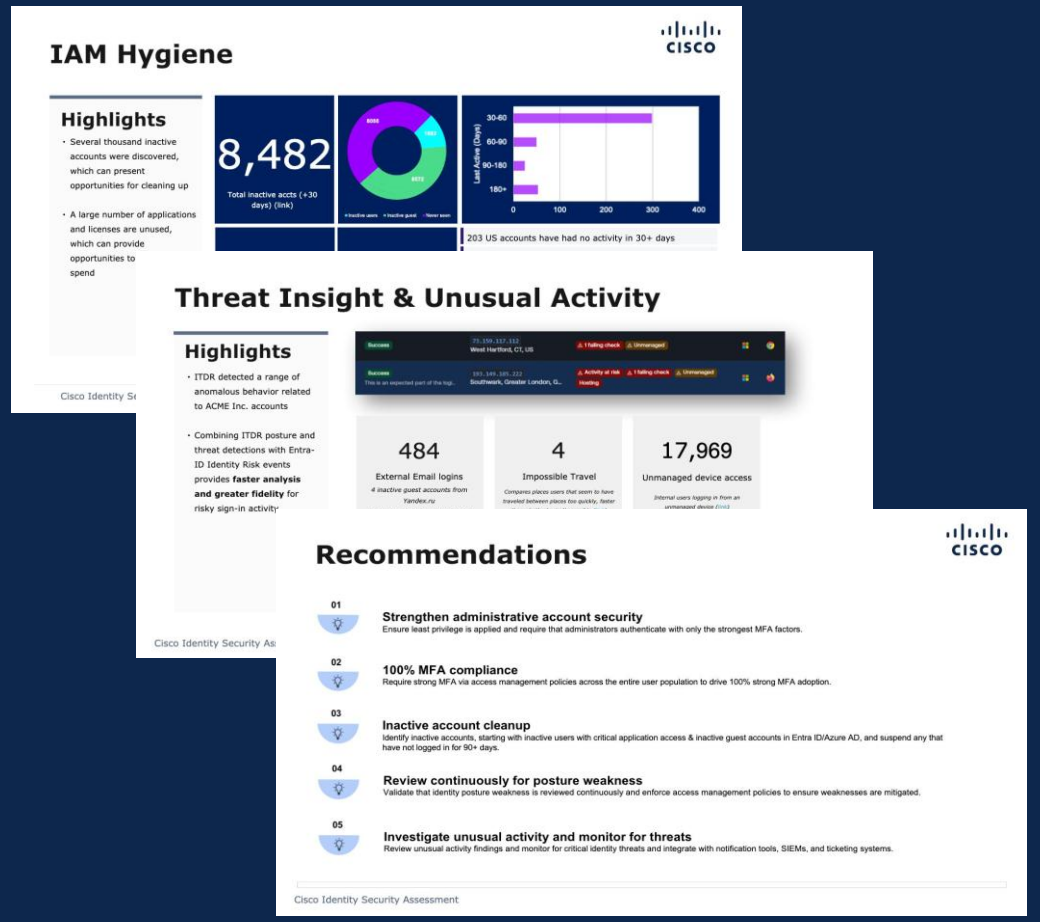
IAMポスチャ評価
MFAが設定されていない/弱い、休眠アカウント、過剰な特権ユーザなどを特定するIAMハイジーンのレビュー

Identityについての洞察
詳細なアクティビティとデバイスマッピングを含む、すべてのアイデンティティの統一ビュー

Identityの脅威
アイデンティティ関連攻撃の洞察

コンプライアンスとセキュリティフレームワークのモニタリング
CIS, CMMC, MITRE, NIST, PCI, SOX標準の整合性を確認

ライセンス使用状況
アイドルライセンスに関する洞察



Cisco Identity セキュリティアセスメントの進め方

事前準備	設定作業	データ収集	レポート作成	報告会
実施環境の確認や実施内容の特定	1～1.5hの設定作業 Duoテナントと お客様IDPとの連携 （API連携）	2週間～1か月間 データ収集 （期間は応相談）	約2週間でお客様 環境の収集データを 元にレポートを作成	作成レポートを元に お客様向けに報告会 を実施 （実施形態は応相談）

トータルで1ヶ月～1.5ヶ月ほど

Cisco Identity Assessment実施事例

①情報・通信業メーカー様 従業員規模グループ全体で1万人程度

②ヘルスケア関連企業様 従業員規模4000名程度

③電気機器メーカー様 従業員規模6万名程度

④情報処理 ソフトウェア企業様 従業員規模3000名程度

⑤化学/機械メーカー様 従業員規模5000名程度

Cisco Identity Assessment実施事例①

情報・通信業メーカー様

従業員規模グループ全体で1万人程度

セキュリティ アセスメントを実施した背景

- 多数のグループ会社、合併でID管理が複雑
- IDを統合したいが現実的ではない
- クラウド利用の増加に伴うアカウント管理に対し、多要素認証に対応していないSaaSなどへの対応が困難
- 複数のディレクトリを一元管理したい
- 社員外のIDの可視化ができていない

ID統合は長期的な施策としてまずは危険なアカウントを可視化

Identity Snapshot

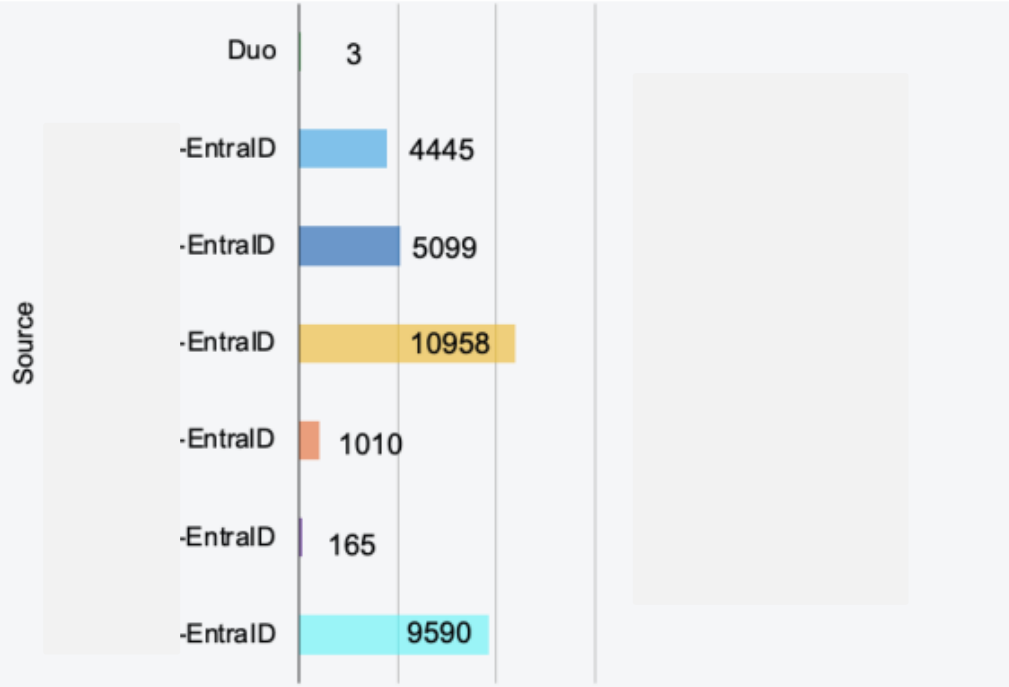
17,023
Total Identities

942 External Accounts
2,583 Inconsistent Accounts
Last 30 Days

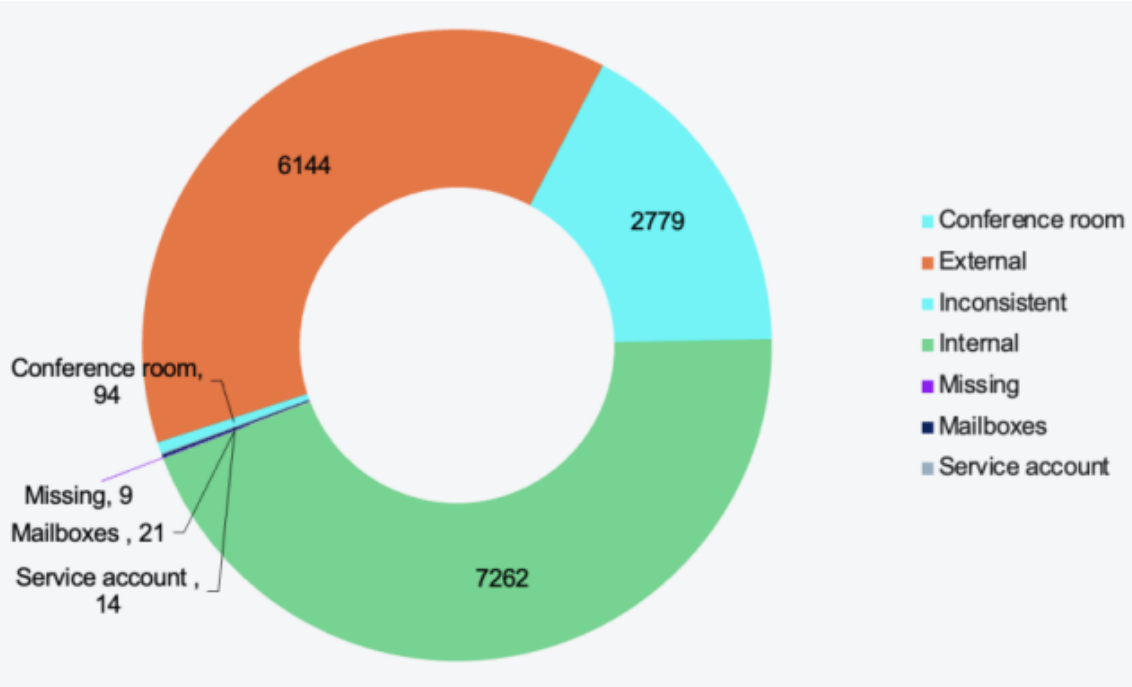
73
Administrators

73 Entra-ID Admins

Sources



Types



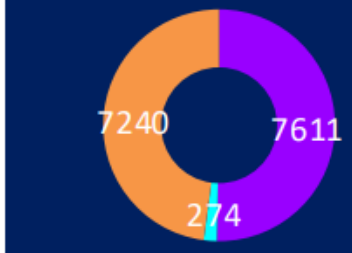
IAM Hygiene

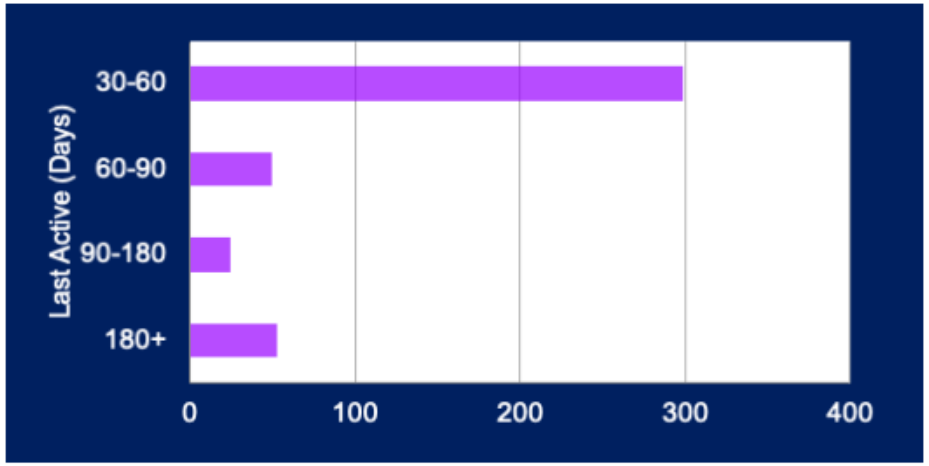
Highlights

- アクティブでは無いアカウントおよび、作成後７日経過しても利用されていないアカウント検出。長期間利用していないアカウントのクリーンアップを検討する。
- 2,899 の Inconsistent User を検知。同じアカウントで複数のIDPでのアクティビティを検出していることが要因と考えられ、High Severityのアクティビティは確認されていない。
- アカウント作成後、７日経過してもログインされていないゲストユーザの対応が必要。

441

Total inactive accts (+30 days)





2,899

Account Inconsistencies

4,993

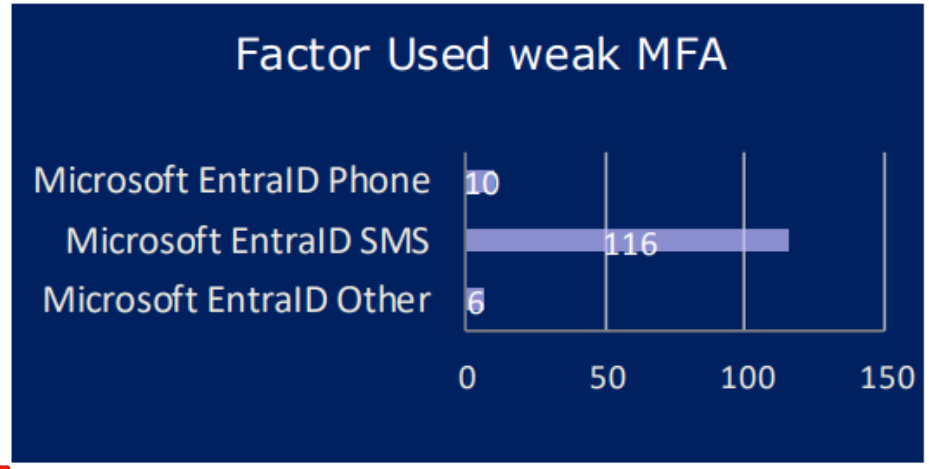
of guest users have never logged in

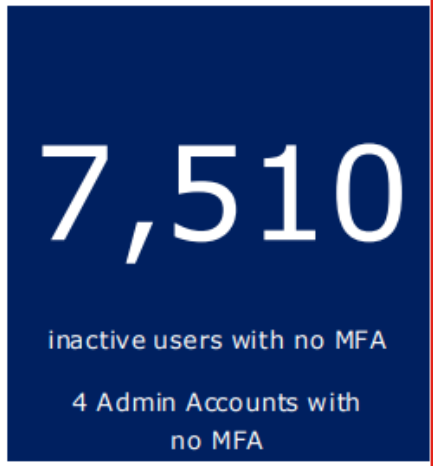
- 421 accounts have had no activity in 30+ days
- 7611 inactive users
- 274 inactive external **guest** users
- 14 service accounts identified, 2 with interactive logins
- 2,899 inconsistent users
- 4,993 never logged in **guest** users

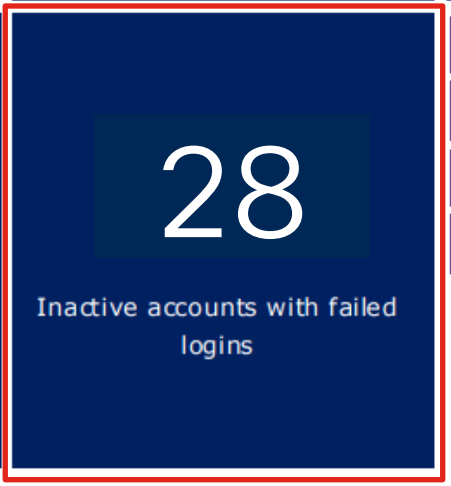
MFA Analysis

Highlights

- 9 ユーザがセキュリティ強度の弱いMFAを使ってログインに成功している
- 4,571 の中で、60の内部ユーザがセキュリティ強度の弱いMFAを利用している
- Phone calls, SMS のセキュリティ強度の弱いMFAが利用されており、その内SMSが多く利用されている
- 28 のアクティブで無いアカウントでログイン失敗が発生している







- 9 users successfully signed in using weak (Phone, SMS)
- 7,510 inactive users with No MFA
- 4 Admin Accounts with No MFA
- 28 inactive accounts with failed logins

Threat Insight & Unusual Activity

Highlights

- 毎日のサインインイベントが非常に多いアカウントを検出しているため、悪意のある活動かどうか調査が必要。
- アクティブでは無いアカウンからのログインを検知しており、攻撃リスク低減のために、無効化可能な非アクティブアカウントの精査が必要。

Threat: Critical

9

Accounts With Unusually High Activity

毎日のサインインイベントが非常に多い（1000回以上）アカウントを検出
悪意のある活動あるいはサービスアカウント

Threat: Critical

7/41

Inactive/Active

Inactive Account Probing

7日以上Inactiveで、その後1回以上のログイン失敗を検知

Threat: Moderate

12

Activity From Untrustworthy ISP

過去90日間に信頼性が低いISPあるいは一般的ではないISPからのアクティビティを検出
Uusima, Stockholms, Hong Kong, SG

Threat: Low

13

Registered Location Mismatch

IDPに登録されたロケーション以外からのアクティビティを検出
Uusima, Somerset,London

Threat: Moderate

3

Access From Dormant Account

7日以内にログインが発生し、それ以前に30日以上休眠状態のアカウント

Threat: Moderate

38

Users With Defined Email Forward Rules

Email転送ルールを定義したユーザを検出

Posture: Critical

624

Allow/Block Email Logins

7日間に5回未満のパーソナルあるいはレアなEmailドメインでのログインを検知

Posture: Critical

39

Users Sharing Authenticators

共有されたAuthenticotor/Phone

Posture: Low

20

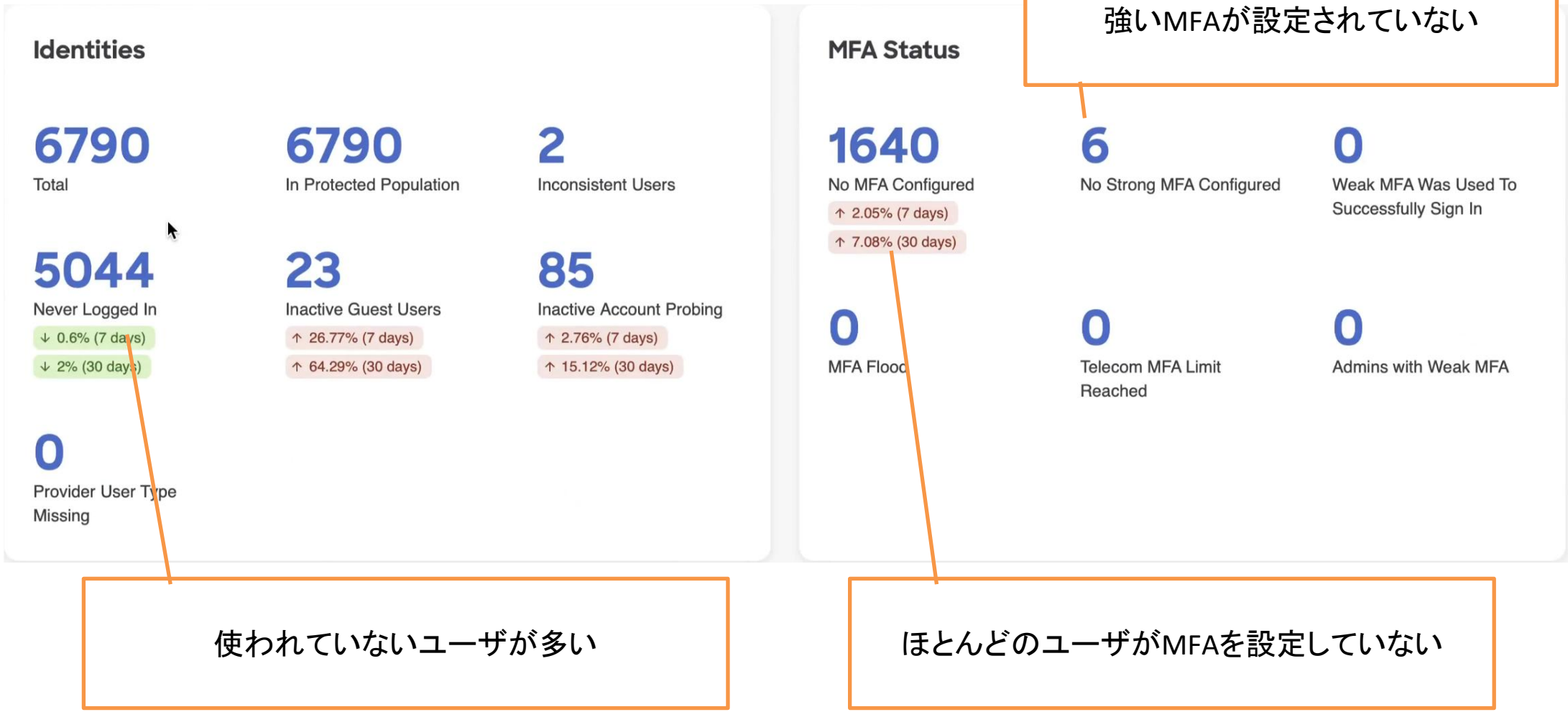
Personal VPN Usage

社内リソースへのアクセスにパーソナルVPNを5回以上利用したユーザ

Cisco Identity Assessment実施事例②
ヘルスケア関連企業様

従業員規模4000名程度

アイデンティティ・MFA

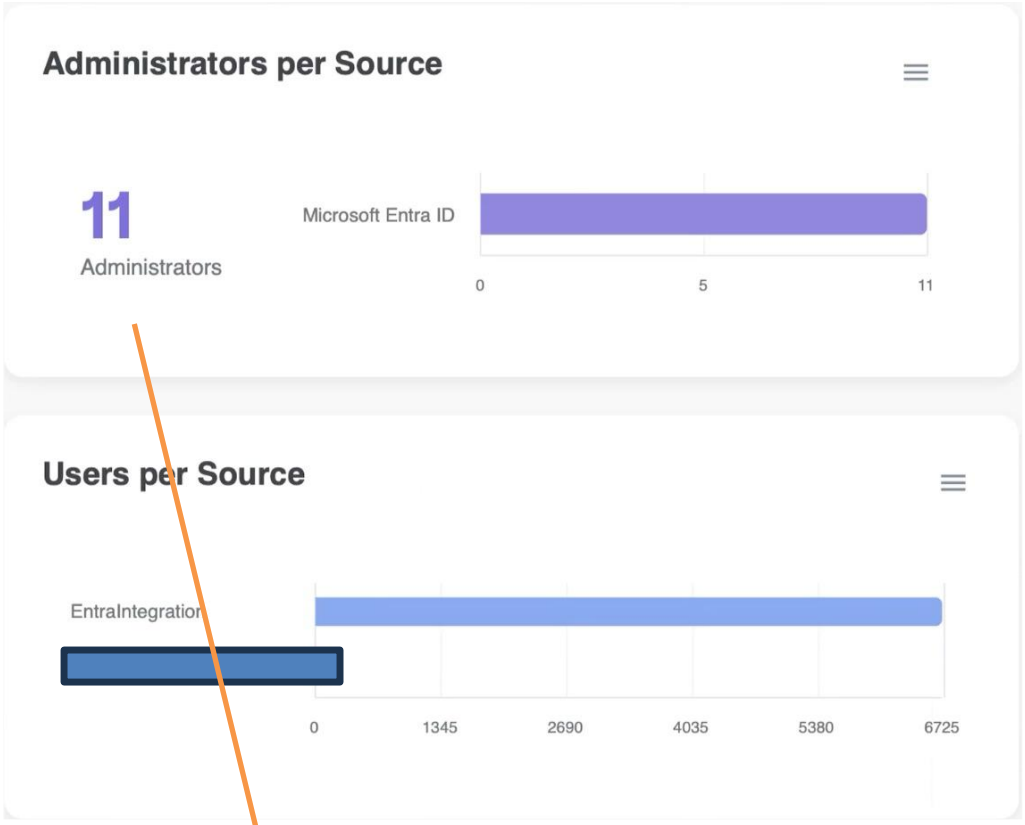


強いMFAが設定されていない

使われていないユーザが多い

ほとんどのユーザがMFAを設定していない

管理者アカウント



管理者ユーザの数

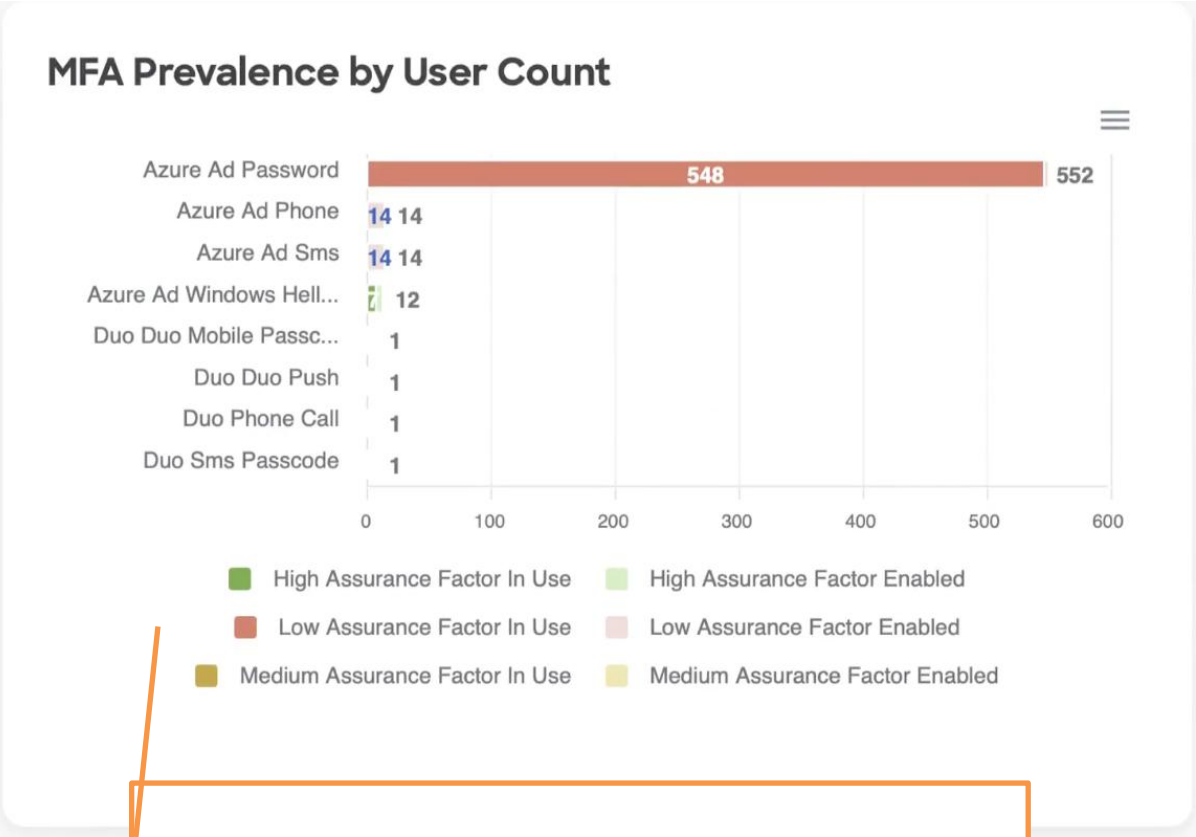
※サンプル

Administrators Logins

User	Last IP Address	Tags
Thrudi Brown thrudi.brown@simubiz.com	2.21.2.5 Moscow, Moscow, RU	New ISP, Hosting
Brian Hayes brian.hayes@simubiz.com	3.21.2.5 Reykjavik, IE	New ISP, Hosting
Aalto Helmig helmig@simubiz.com	209.6.171.113 Burlington, MA, US	New ISP
Karsch Heuck karsch.heuck@simubiz.com	2600:1017:b808:d190:46… New York, NY, US	
Chanza Rosser santos.rosser@simubiz.com	89.64.102.153 Gdansk, Pomerania, PL	New ISP
Daymude Sheiman daymude.chiaravalle@simubiz.c…	78.192.202.246 Paris, Île-de-France, FR	New ISP
Ayo Ganin ayo.ganin@simubiz.com	134.238.180.49 Ashburn, VA, US	New ISP, Hosting

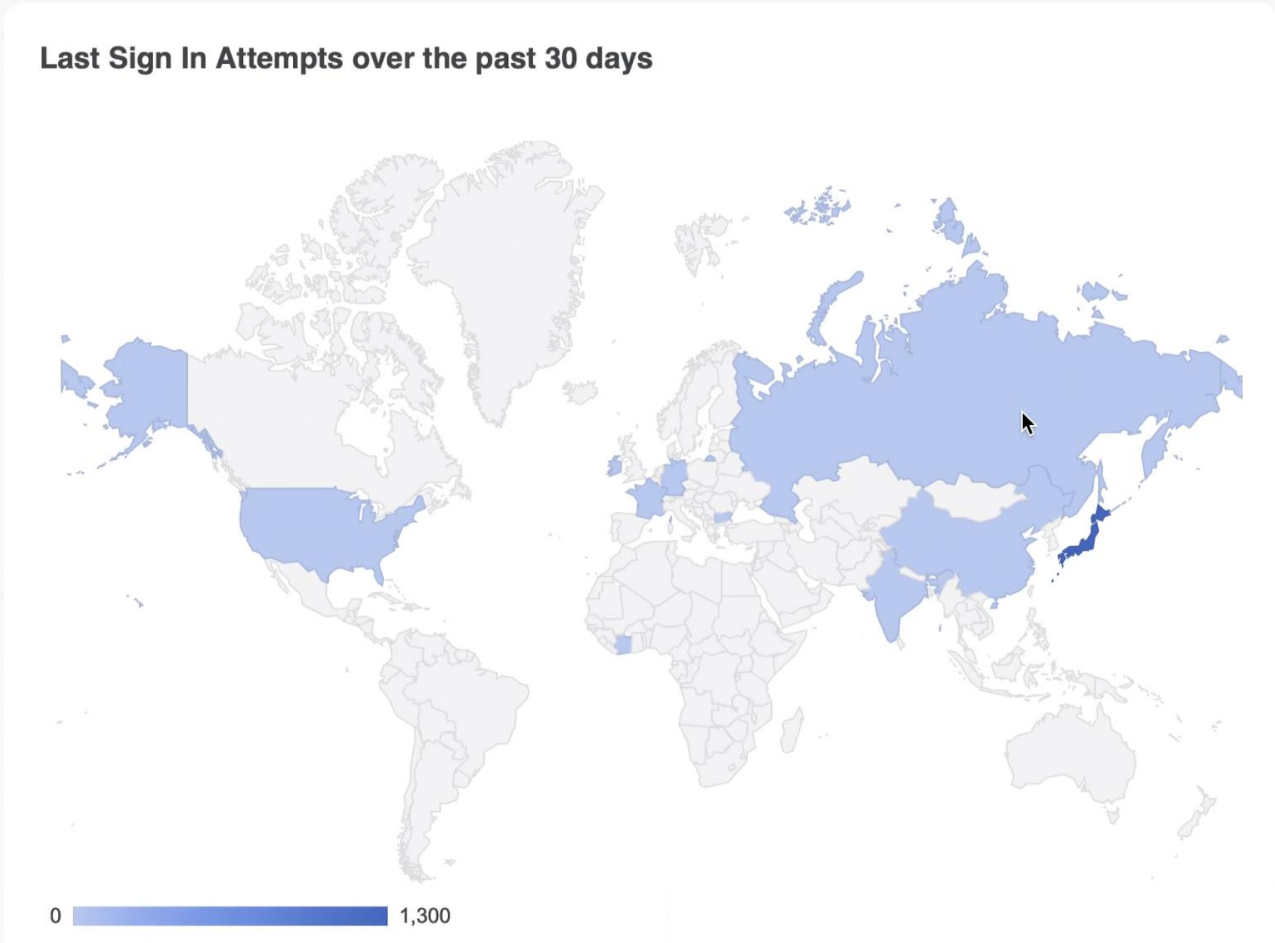
ありえないロケーション、IPからのアクセス等をチェックしていくことを推奨

MFAの利用状況



より強度の強いMFAの設定を推奨

国別のアクセス状況



Login Attempts from New Countries

Country ↑	Success ↑	Failure ↑	Other ↑
Ireland	4	21	0
South Korea	2	23	0
India	2	14	0
China	1	0	0

ありえない国からのアクセスが合った場合には、ハッカーに乗っ取られている可能性があるため、アカウントの削除等の対策が必要

Cisco Identity Assessment実施事例③

電気機器メーカー様

従業員規模6万名程度

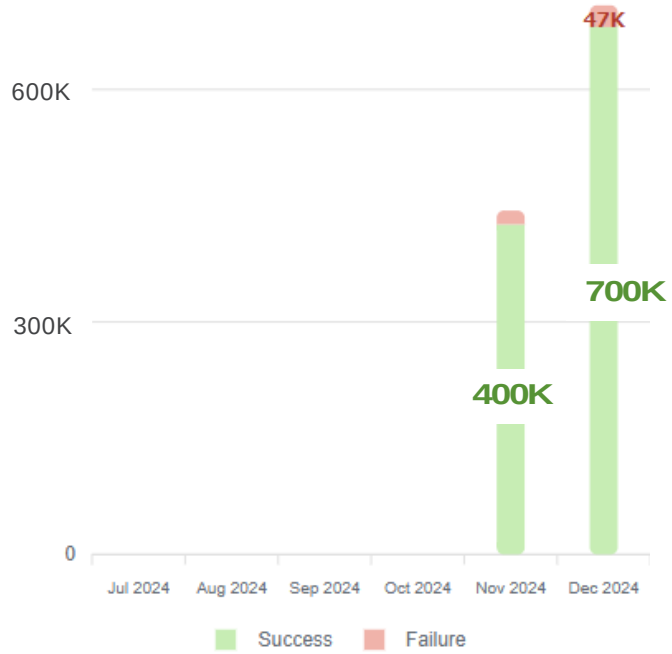
Identity Snapshot

61,797

総アイデンティティ数

ソース

月間ログイン



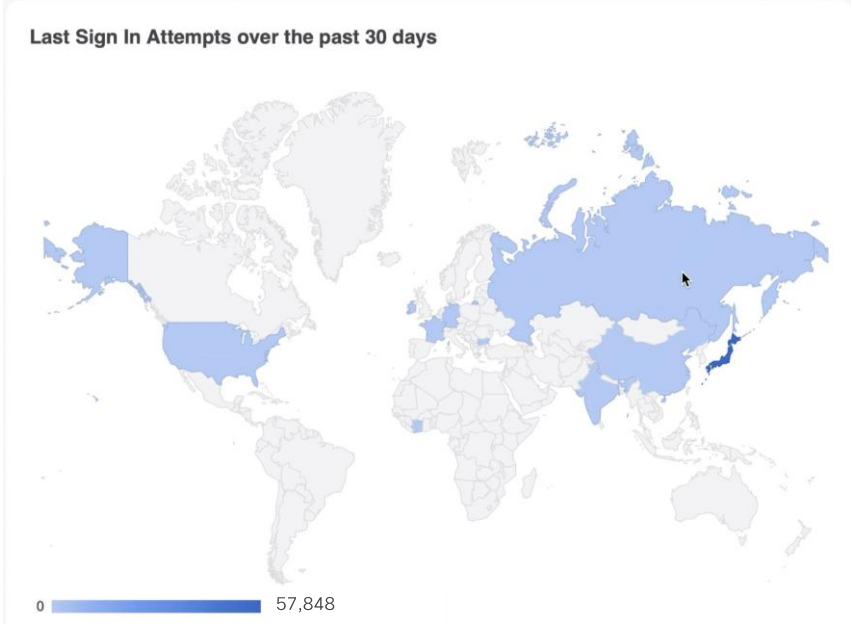
IAM Hygiene

Highlights

- 8,312名の非アクティブなユーザが確認されました。３０日間以上ログインしていないため、狙われる休眠アカウントのリスクがあります。またライセンスを過剰に消費をしている可能性もあります。
- 10名のユーザーがバイパスコードを利用してログインに成功しています。
- 51回の信頼できないISPからのアクセスがあります。
- ２回のアクセスが拒否された国からのアクセスがあります。

8,312 Inactive users	10 A Bypass Code Was Used To Successfully Sign In
51 Activity from Untrustworthy ISP	2 Access from Denied Countries

国別ログインソース

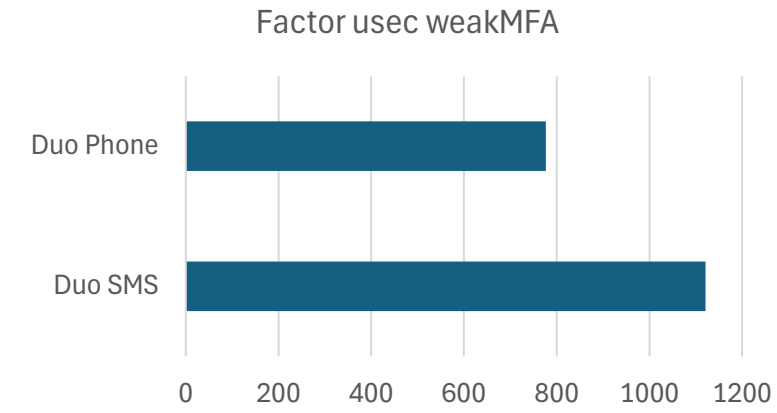


MFA Analysis

Highlights

- 1,898のアカウントが弱いMFAを使ってログインしています。
- 53のアカウントで強いMFAが設定されていません。
- 弱いMFAを設定しているユーザーはありません。
- 弱いMFAを設定している管理者アカウントはありません。

1,898 Weak MFA Was Used To Successfully Sign In	53 No MFA Configured
0 No Strong MFA Configured	0 Admins with weak MFA



Threat Insight & Unusual Activities

Highlights

- 4のアカウントで、エンドユーザーから不審なアクティビティが報告されています。
- 5のアカウントが以前に認証失敗していたIPからアクセス成功しています。
- 50のアカウントで、信頼できないISPからのアクセスが確認されています。
- 8のアカウントはテナントへ新しい国からアクセスしています。

Threat: Critical

4

Suspicious Activity Reported by End User

エンドユーザーから報告された不審なアクティビティ

Threat: Moderate

5

Successful Access from a Previously Only Falling IP

以前は失敗していたIPからのアクセス成功

Threat: Moderate

50

Activity From Untrustworthy ISP

過去９０日間に信頼性が低いISPあるいは一般的ではないISPからのアクティビティを検出

Posture: Moderate

8

New Country for Tenant

テナントへ新しい国からアクセスが検出

Posture: Low

832

Personal VPN Usage

アクセス時に個人向けVPNサービスを５回以上利用したユーザ

Cisco Identity Assessment実施事例④
情報処理 ソフトウェア企業様

従業員規模3000名程度

Identity Snapshot

9,300

総アイデンティティ数

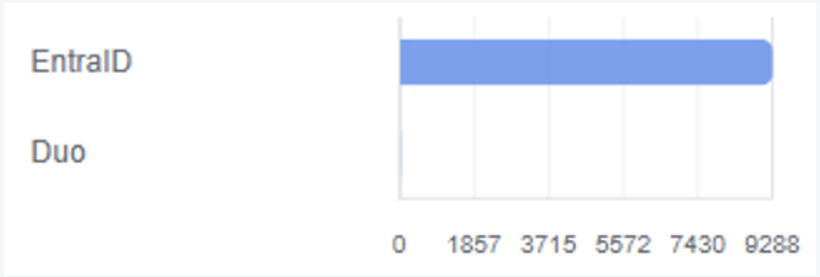
70

管理者数

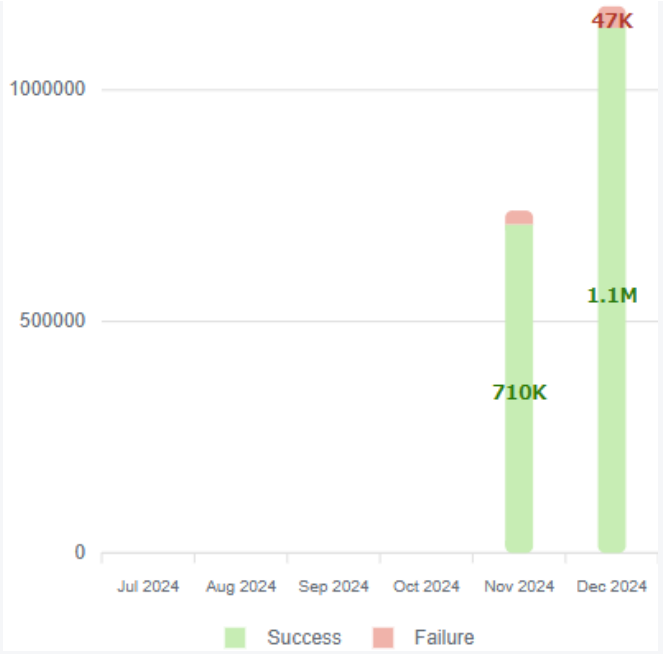
68 EntraID

2 Duo

ソース



月間ログイン



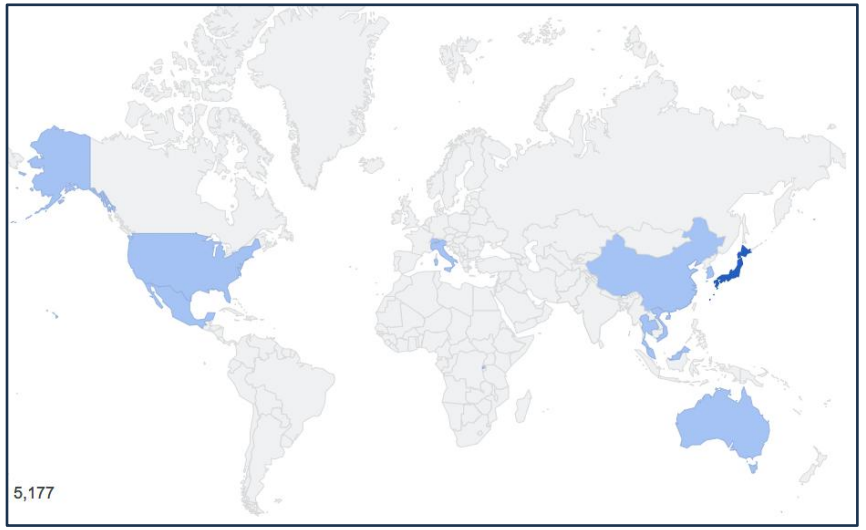
IAM Hygiene

Highlights

- 35の非アクティブアカウント。過去30日間ログインアクティビティがありません。
- 18のサービスアカウントでinteractiveログインが確認されました。
- 390の非アクティブゲストアカウント。過去30日間ログインアクティビティがありません。
- 3,800のアカウントは一度もログインしていません。

35 Inactive	390 Inactive Guests
18 Service Account Successful Sign In	3,800 Never Logged In

国別ログインソース



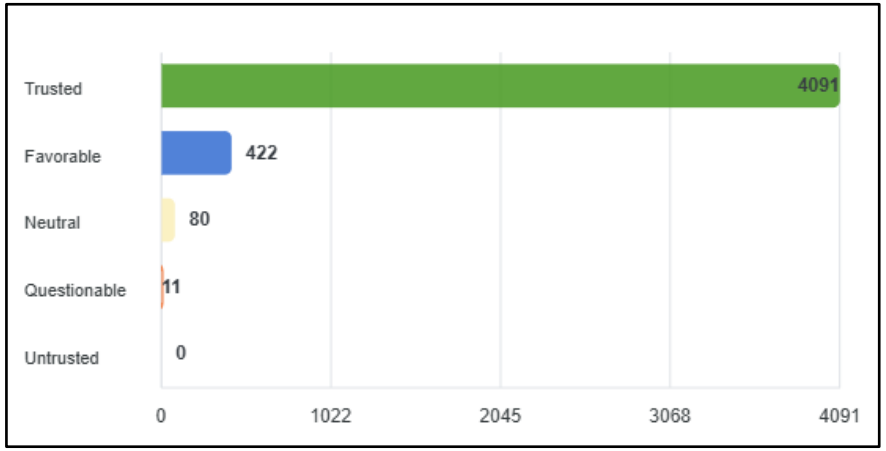
MFA Analysis

Highlights

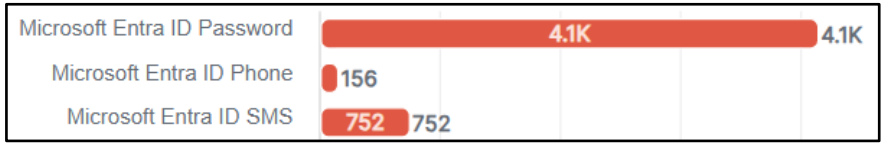
- 30のアカウントが弱いMFAを使ってログインしています。
- 630のアカウントで強いMFAが設定されていません。
- 1,399のアカウントがMFA未設定です。
- 268のアカウントで認証要素の共有が発生しています。

30 Weak MFA Was Used To Successfully Sign In	1,399 No MFA Configured
630 No Strong MFA Configured	268 Users Sharing Authenticators

アカウントトラストレベル



弱い認証要素を使用しているアカウント



Threat Insight & Unusual Activities

Highlights

- 3のアカウントで、1日に1000件以上のログインアクティビティが確認されています。
- 5のアカウントがMFAフラッド攻撃を受けている可能性があります。
- 90のアカウントで、7日以上アクティビティが無い状態が続いたのちにログインを試みて失敗しています。
- 590のアカウントは個人向けメールプロバイダーや使用頻度の低いドメインが設定されています

Threat: Critical

3

Accounts With Unusually High Activity

1日あたりのログインアクティビティが非常に多い (1000回以上) アカウントを検出

Threat: Critical

90

Inactive Account Probing

7日以上ログインアクティビティがなく、その後1回以上のログイン失敗を検知

Threat: Moderate

5

Activity From Untrustworthy ISP

過去90日間に信頼性が低いISPあるいは一般的ではないISPからのアクティビティを検出

Threat: Critical

5

MFA Flood

MFAフラッド攻撃を受けている可能性

Posture: Critical

590

Allow/Block Email Logins

7日間で使用された回数が5回未満のドメイン、または個人向けのメールサービスドメインなどを持つアカウント

Posture: Low

60

Personal VPN Usage

アクセス時に個人向けVPNサービスを5回以上利用したユーザ

Cisco Identity Assessment実施事例⑤

化学/機械メーカー様

従業員規模5000名程度

Identity Snapshot

2,720

総アイデンティティ数

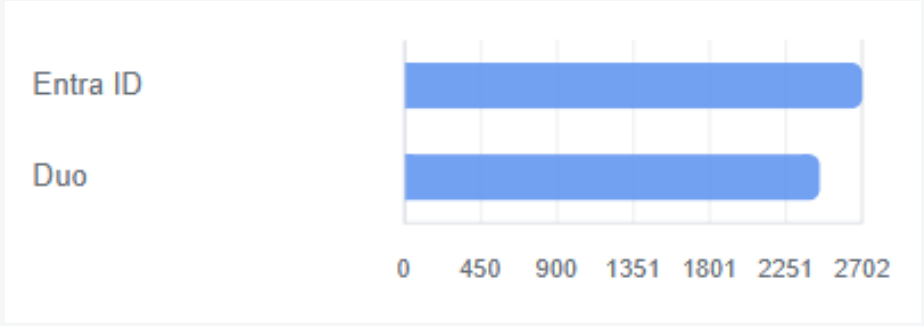
6

管理者数

4 EntraID

2 Duo

ソース



月間ログイン

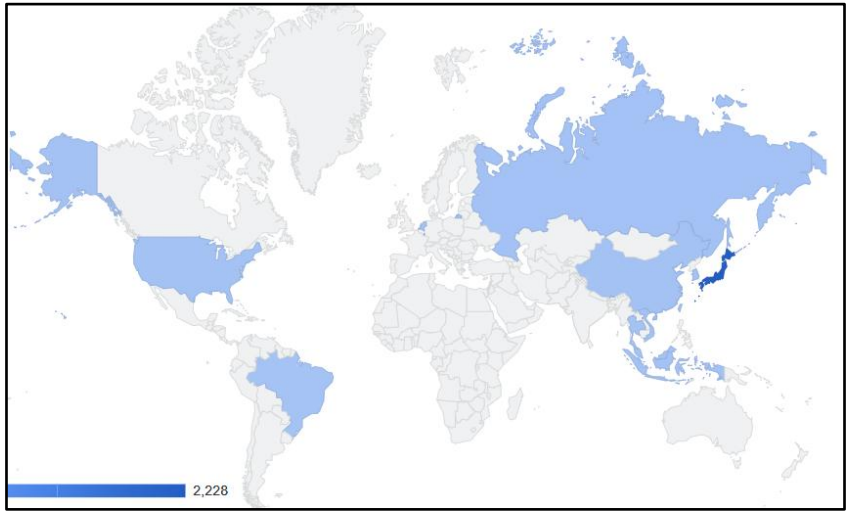
IAM Hygiene

Highlights

- 170の非アクティブアカウント。過去30日間ログインアクティビティがありません。
- 3のサービスアカウントでinteractiveログインが確認されました。
- 350の非アクティブゲストアカウント。過去30日間ログインアクティビティがありません。
- 290のアカウントは一度もログインしていません。

170 Inactive	350 Inactive Guests
3 Service Account Successful Sign In	290 Never Logged In

国別ログインソース



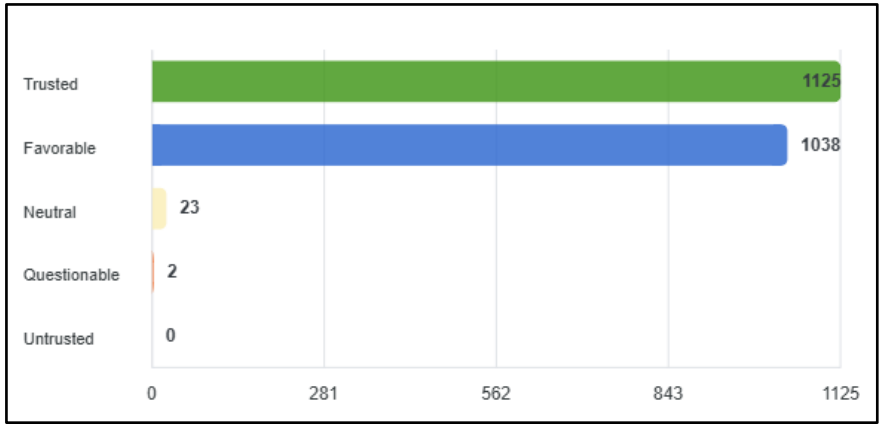
MFA Analysis

Highlights

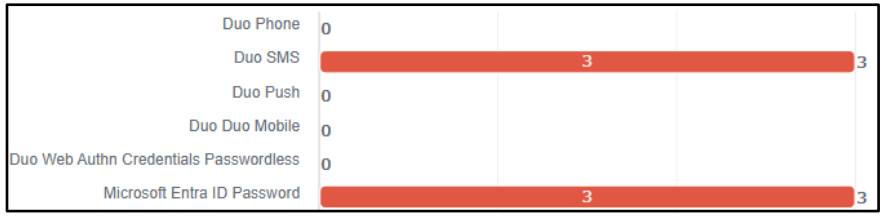
- 5のアカウントが弱いMFAを使ってログインしています。
- 68のアカウントで強いMFAが設定されていません。
- 1483のアカウントがMFA未設定です。
- 8のアカウントで認証要素の共有が発生しています。

5 Weak MFA Was Used To Successfully Sign In	1483 No MFA Configured
68 No Strong MFA Configured	8 Users Sharing Authenticators

アカウントトラストレベル



弱い認証要素を使用しているアカウント



再掲：無償のCisco Identity セキュリティアセスメント

お客様のアイデンティティエコシステムに対する可視化レポートをご提供します

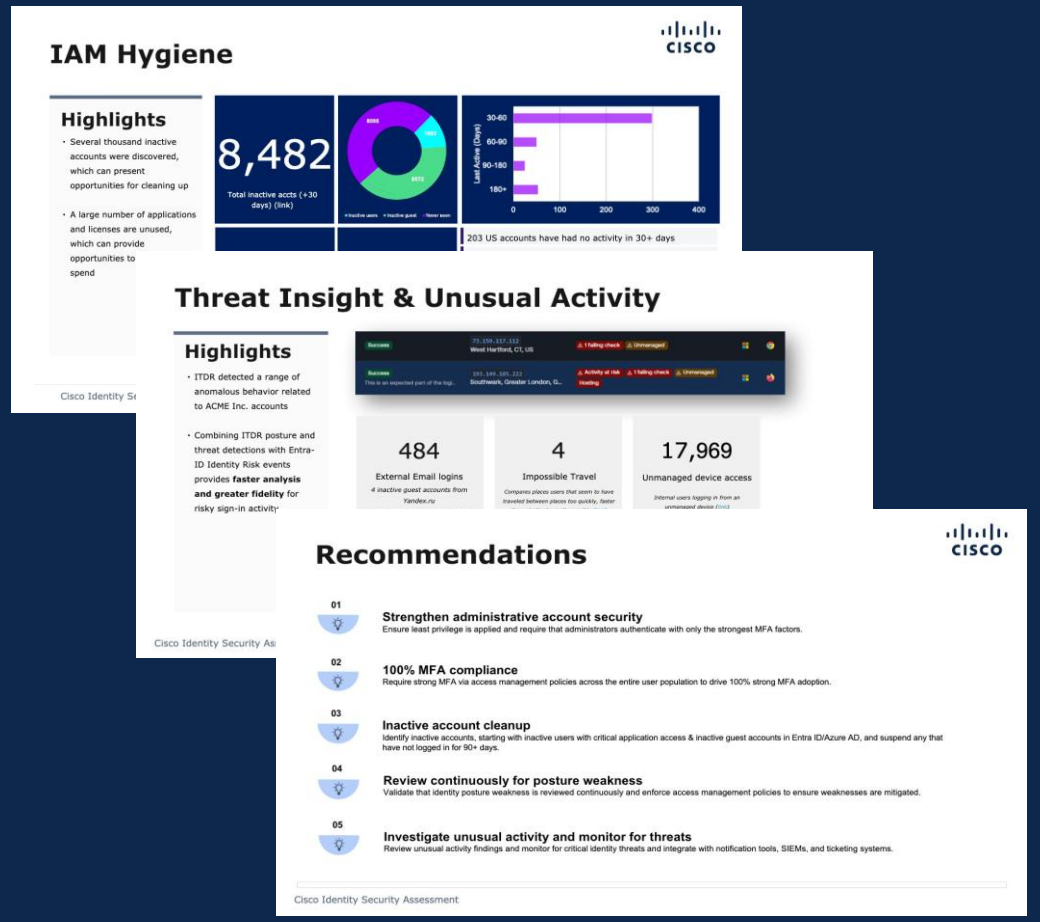
IAMポスチャ評価
MFAが設定されていない/弱い、休眠アカウント、過剰な特権ユーザなどを特定するIAMハイジーンのレビュー

Identityについての洞察
詳細なアクティビティとデバイスマッピングを含む、すべてのアイデンティティの統一ビュー

Identityの脅威
アイデンティティ関連攻撃の洞察

コンプライアンスとセキュリティフレームワークのモニタリング
CIS, CMMC, MITRE, NIST, PCI, SOX標準の整合性を確認

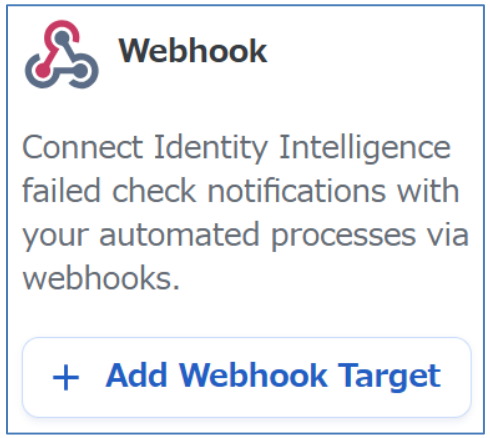
ライセンス使用状況
アイドルライセンスに関する洞察



Cisco XDR 最新アップデート

デモ:
Cisco Identity Intelligence, Cisco XDR 連携で実現するレスポンスオートメーション

Webhookによる外部通知

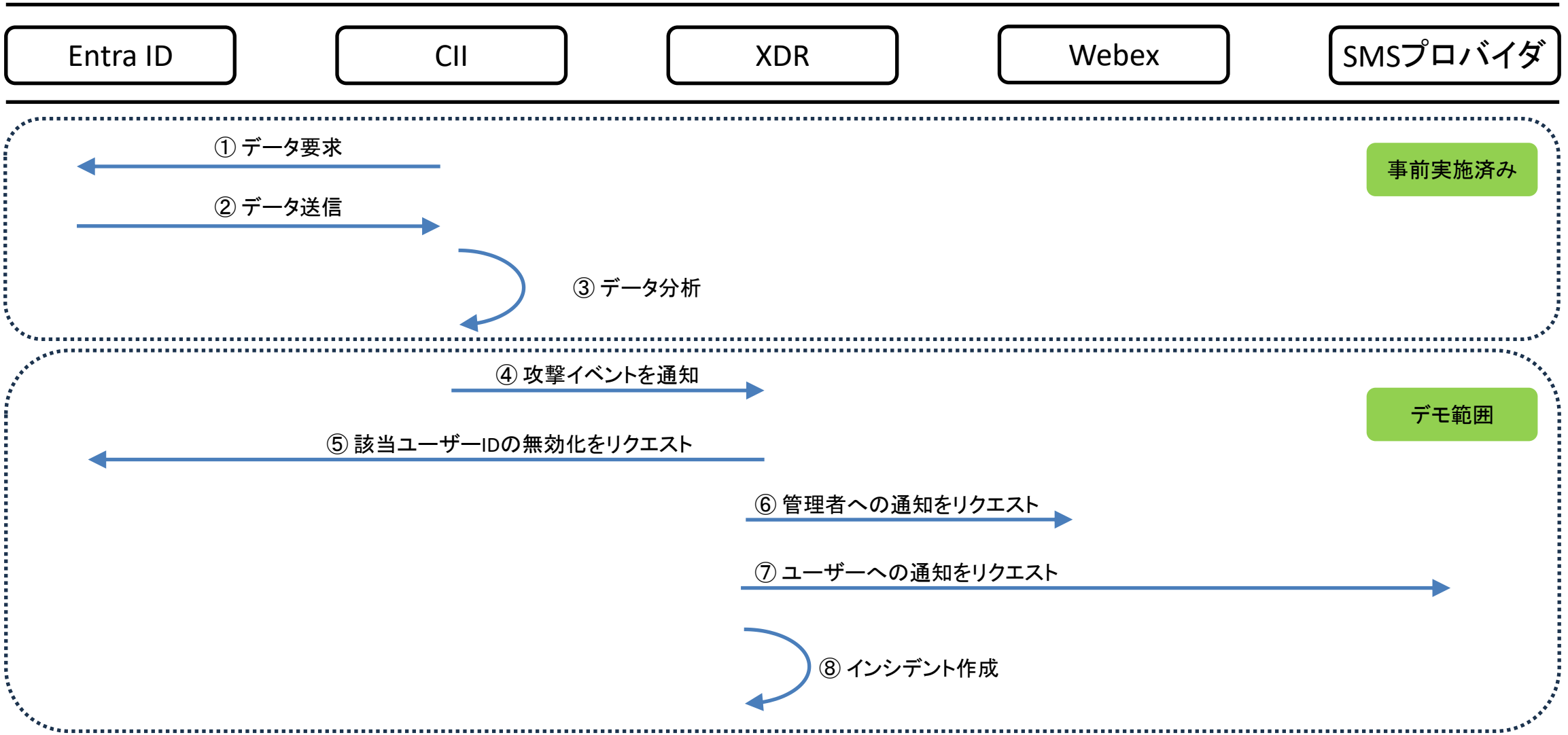


重大なイベントが発生した場合、Webhook Provider から Webhook Consumer へ通知を送信 (HTTP POST による JSON や XML 形式データの送信が一般的)

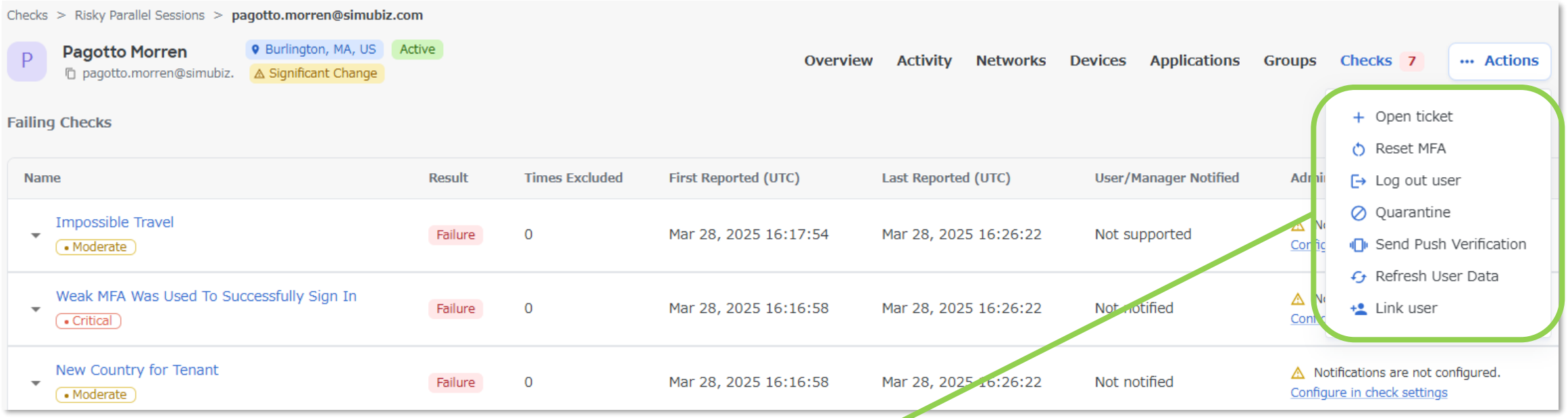
Consumerはデータ受信後に任意の処理を実施

CII は Provider として、XDR は Consumer として動作させることが可能

デモシナリオ


Entra ID
CII
XDR
Webex
SMSプロバイダ
① データ要求
② データ送信
③ データ分析
事前実施済み
④ 攻撃イベントを通知
⑤ 該当ユーザーIDの無効化をリクエスト
⑥ 管理者への通知をリクエスト
⑦ ユーザーへの通知をリクエスト
⑧ インシデント作成
デモ範囲

リスク検知後の手動レスポンス

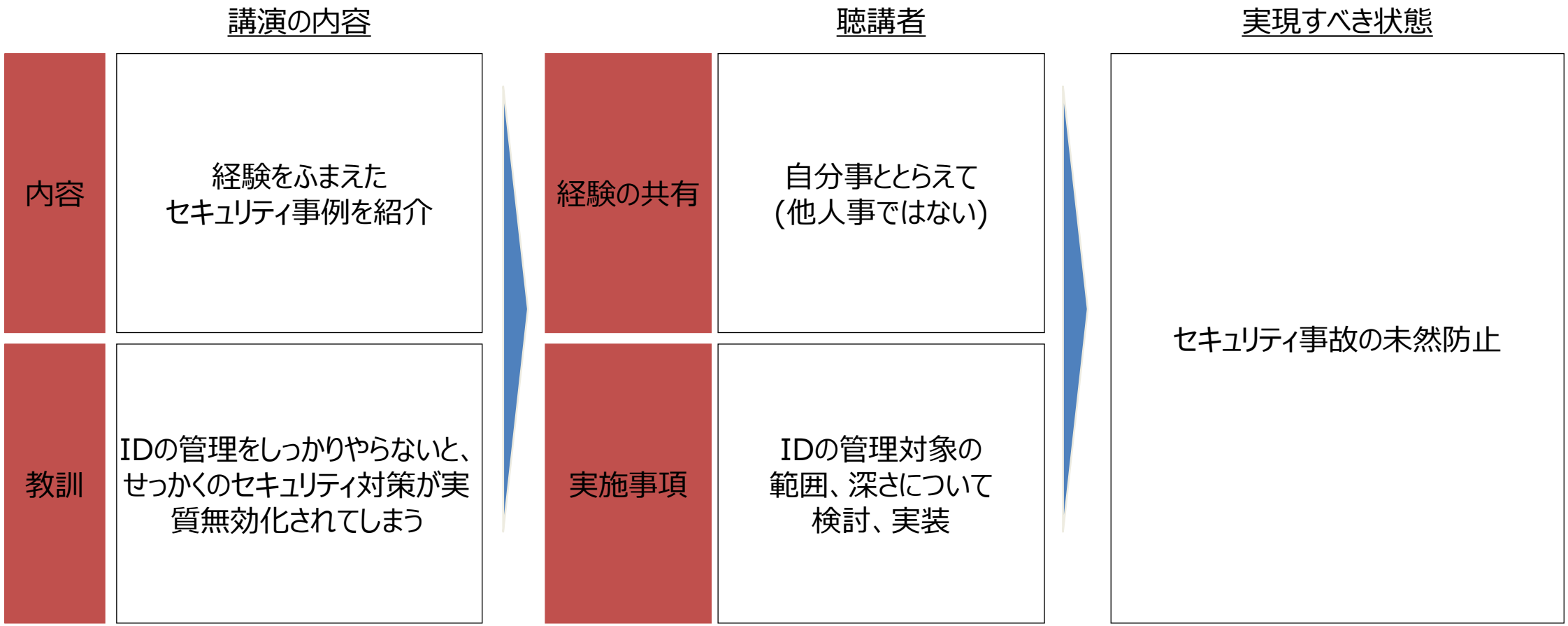


管理者の操作によりチケット作成や
ユーザー隔離などを実施可能

本日のまとめ

本日のまとめ

再掲


講演の内容
聴講者
実現すべき状態
内容
経験をふまえた
セキュリティ事例を紹介
教訓
IDの管理をしっかりやらないと、
せっかくのセキュリティ対策が実
質無効化されてしまう
経験の共有
自分事ととらえて
(他人事ではない)
実施事項
IDの管理対象の
範囲、深さについて
検討、実装
セキュリティ事故の未然防止

本日のまとめ

- Cisco Identity Intelligence によるIDリスクの管理と事例のご紹介
- Cisco XDR 最新アップデート
- Cisco Identity Intelligence と Cisco XDR の連携によるID脅威へのレスポンスオートメーション例のご紹介


CISCO