



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？

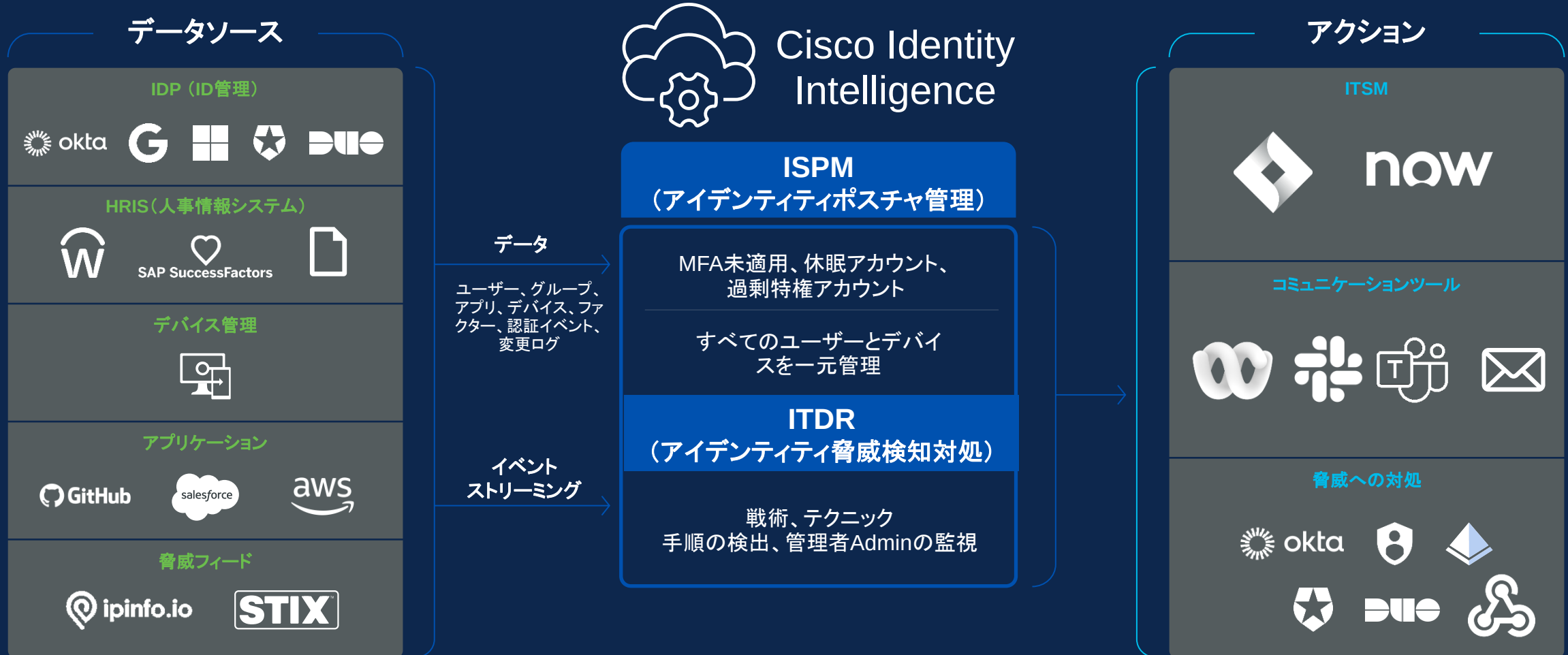
多要素認証実施していますか？

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

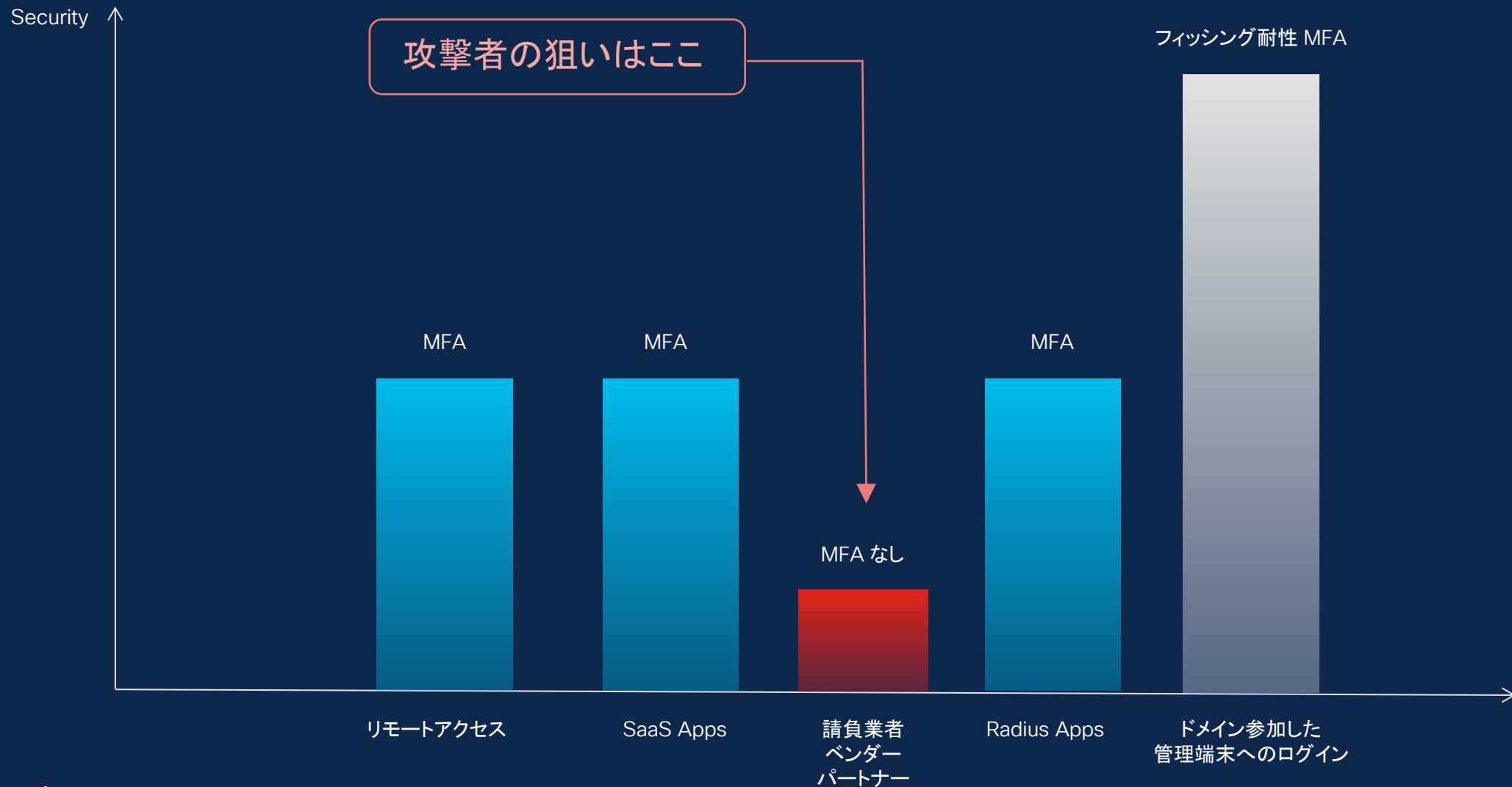
デモ: Cisco Identity IntelligenceによるID リスクの可視化

- 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





Compatibility All

- ☐ AWS 1
- ☐ Duo 11
- ☐ GitHub 2
- ☐ Google Workspace 4
- ☐ Microsoft Entra ID 13
- ☐ Okta 9
- ☐ Salesforce 2

Compliance All

- ☐ Full 1
- ☐ Partial 14

Severity All



mfa



All Checks

Check	# Failing	
34% No MFA Configured Critical End Users - Compliance, Identity Posture Insight	162	→ No change since last week → No change since last month
91% Weak MFA Was Used To Successfully Si... Critical End Users - Identity Posture Insight	22	→ No change since last week → No change since last month
91% No Strong MFA Configured Moderate End Users - Compliance, Identity Posture In...	21	→ No change since last week → No change since last month

162 failing users

User	First Reported (UTC) ↑	Last Reported (UTC) ↑
service.account@simubi...	Apr 14, 2025 16:14:19	Apr 14, 2025 16:25:01
simone.briggs@simubiz...	Apr 14, 2025 16:16:09	Apr 14, 2025 16:25:01
staller.fohey@gmail.com	Apr 14, 2025 16:14:19	Apr 14, 2025 16:25:01
stockburger.tronco@sim...	Apr 14, 2025 16:14:19	Apr 14, 2025 16:25:01

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



Compatibility

All

- ☐  AWS 1
- ☐  Duo 2
- ☐  GitHub 2
- ☐  Google Workspace 2
- ☐  Microsoft Entra ID 4
- ☐  Okta 4
- ☐  Salesforce 1
- ☐  Slack 1
- ☐  Workday 1

Compliance

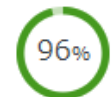
All

 inactive 

All Checks

Check

Failing



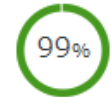
Inactive Users

Moderate

End Users - Compliance, Identity Posture In...

8

→ No change since last week
→ No change since last month



Inactive Guest Users

Critical

End Users - Compliance, Identity Posture Insight

2

→ No change since last week
→ No change since last month

Check Settings

 Custom Detection Settings

Number of days: 30

閾値はチューニング可能

 Edit

8 failing users

User

First Reported (UTC) ↑

zohra.anika@simubiz.com 

Apr 15, 2025 16:12:42

simone.briggs@simubiz.com 

Apr 15, 2025 16:15:46

 Identity Intelligence

☰



Compatibility

All

☐



AWS

1

☐



Duo

1

☐



GitHub

1

☐



Google Workspace

1

☐



Microsoft Entra ID

7

☐



Okta

6

☐



Salesforce

2

☰

All Checks

Check	# Failing
81% Unused Application for a User • LOW End Users - Compliance, Identity Posture Insight 46 → No change since last week → No change since last month	

Identity Intelligence

Checks > Unused Application for a User > staller.fohey@gmail.com

S

Staller Fohey

staller.fohey@gma

Active

Significant Change

Overview

Activi

Failing Checks

Name	Result	Times Excluded	Fi
Allow/Block Email Logins Critical	Failure	0	Ap

Unused Application for a User (Last reported: Less than 1 day ago)

Alert users about their unused applications or their managers before removing access. Removing access can save licensing costs, improve security posture, and reduce unnecessary access.

Applications

workday

User Trust Level

TRUSTED

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

Registered Location Mismatch Low

Details

Detects when an account's activity regularly comes from a location that differs from the registered location listed on the IDP or HRIS. Working locations are determined by evaluating an account's activity over the past 7 days.

Recommended Actions

Please consider updating the registered location within HRIS or IDP.



Automated notifications for this check are not configured. Please configure notifications if you wish to receive automated reports about users failing this check.

31 failing users

User	First Reported (UTC) ↑	Last Reported (UTC) ↑
clincy.bursi@simubiz.com 	May 5, 2024 04:28:34	May 5, 2024 04:28:34
cramblit.mitra@simubiz.com 	May 5, 2024 04:28:34	May 5, 2024 04:28:34
daymude.chiaravalle@simubiz.com 	May 5, 2024 04:28:34	May 5, 2024 04:28:34
deatrick.deroberts@simubiz.com 	May 5, 2024 04:28:34	May 5, 2024 04:28:34
deatrick.mcgurrin@simubiz.com 	May 5, 2024 04:28:34	May 5, 2024 04:28:34

Registered Location Mismatch (Last reported: Less than 1 day ago)

 [deatrick.mcgurrin@simubiz.com](#)

Please consider updating the registered location within HRIS or IDP.

Registered Location

Country: BE

Source: Demo Workday

Common Working Locations

User Location Prevalence: 84.314

Country: AU

State: NSW

Source: Demo Okta

Provider's Failing Check

Demo Workday

User Title

Partner Account Director - sw development eng/eng ii

Checks > Impossible Travel > kolluri.hofferber@simubiz.com

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

Overview

Failing Checks

Name	Result	Times Excluded	First Reported
Activity From Untrustworthy ISP • Moderate	Failure	0	Sep 24, 2024
Impossible Travel • Moderate	Failure	0	Sep 24, 2024
Weak MFA Was Used To Successfully Sign In • Critical	Failure	0	Sep 24, 2024
Registered Location Mismatch • Low	Failure	0	Sep 24, 2024
Unused Application for a User • Low	Failure	0	Sep 24, 2024
User in IDP but not in HRIS • Critical	Failure	0	Sep 24, 2024
No Strong MFA Configured • Moderate	Failure	0	Sep 24, 2024

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



- Compatibility** **All**
 - ☐  Duo 2
 - ☐  Microsoft Entra ID 2
 - ☐  Okta 3
 - ☐  Salesforce 1
- Compliance** **All**
 - ☐  Partial 3
- Severity** **All**
 - ☐  Moderate 3
- Topic** **All**
 - ☐ Devices 1
 - ☐ Identity Threat Insight 3
- Frameworks** **All**



 compromised



All Checks

Check

Failing



Impossible Travel 

 Moderate End Users - Identity Threat Insight

5

→ No change since last week
→ No change since last month



Authenticator Registration Anomalies 

 Moderate End Users - Devices, Identity Threat Insight

1

→ No change since last week
→ No change since last month



Compromised Session 

 Moderate End Users - Identity Threat Insight

1

→ No change since last week
→ No change since last month

Apr 13, 2025 20:04:41



user.authentication.sso

Type: WEB

fellmeth.emery@simubiz.com

Session: 102disvYQmOSb6SL...

 cisco asa vpn (saml)

User: fellmeth.emery@simu...

Success

77.9.12.3

Munich, Bavaria, DE

Apr 13, 2025 20:03:34



user.authentication.sso

Type: WEB

fellmeth.emery@simubiz.com

Session: 102disvYQmOSb6SL...

 cisco asa vpn (saml)

User: fellmeth.emery@simu...

Success

77.9.98.7

Munich, Bavaria, DE

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

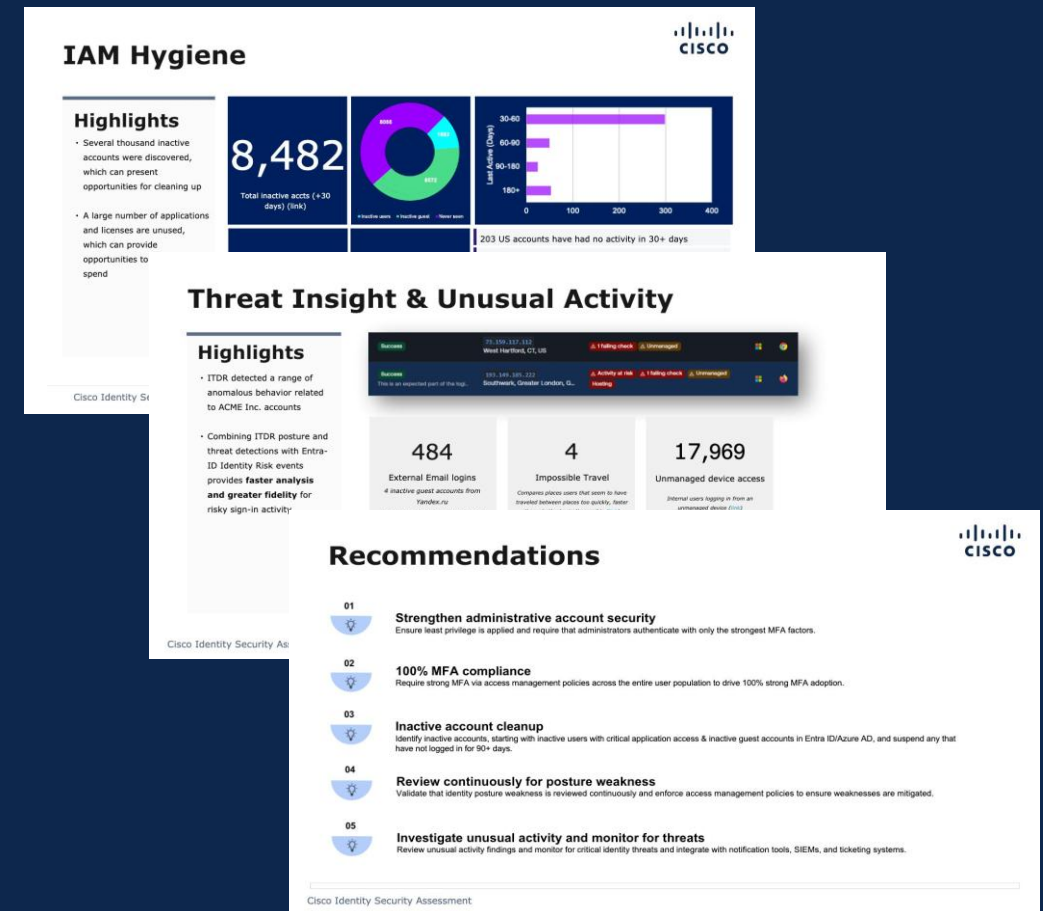
アイデンティティ関連攻撃の洞察

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

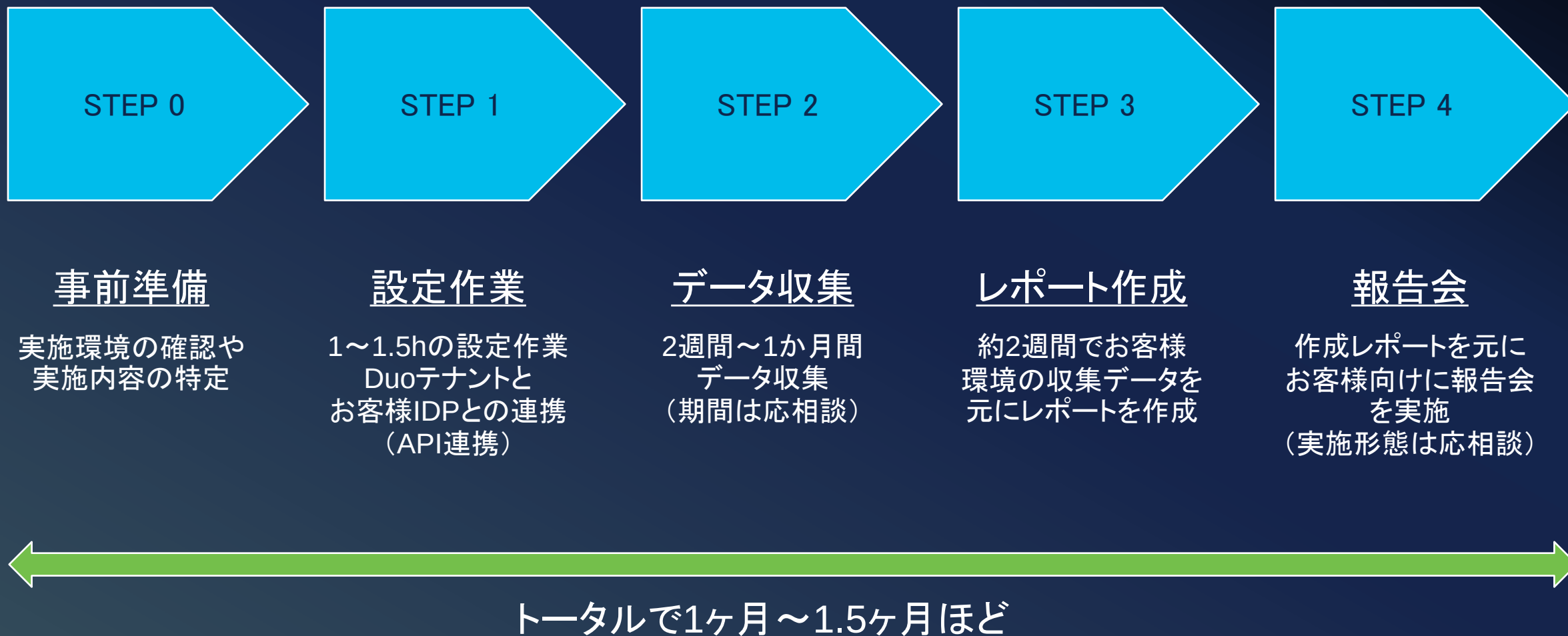
CIS, CMMC, MITRE, NIST, PCI, SOX標準の整合性を確認

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



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

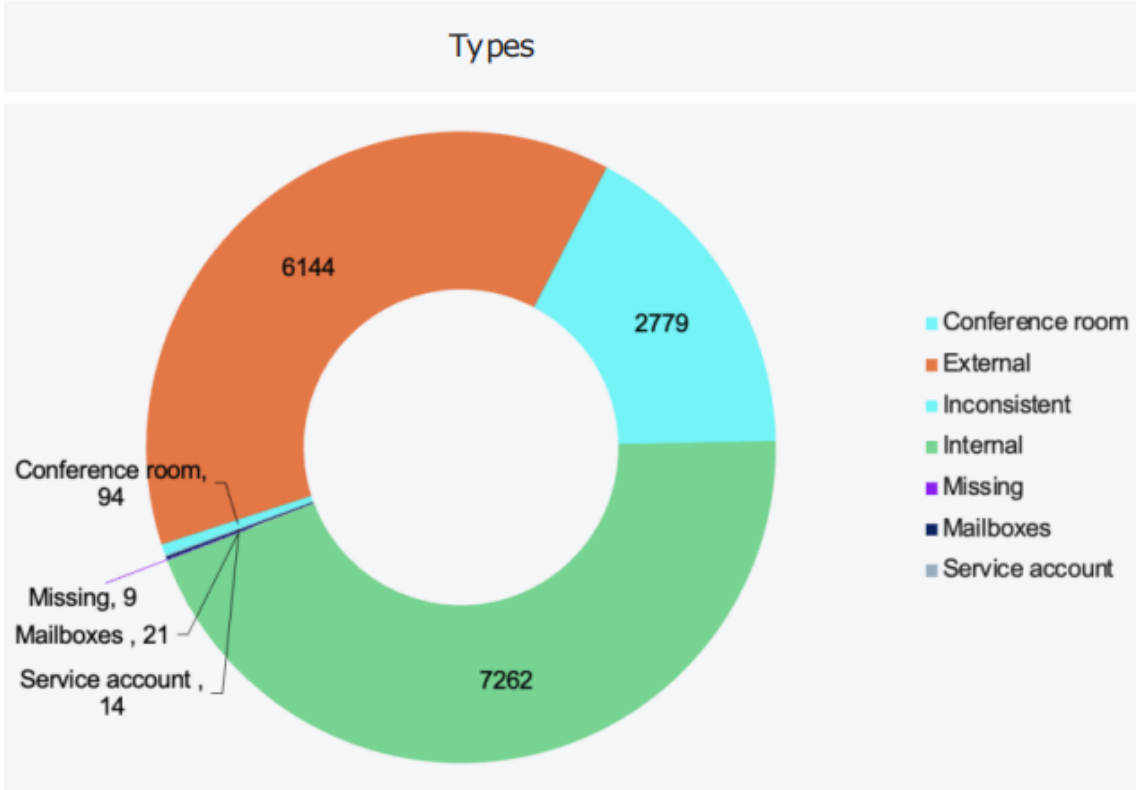
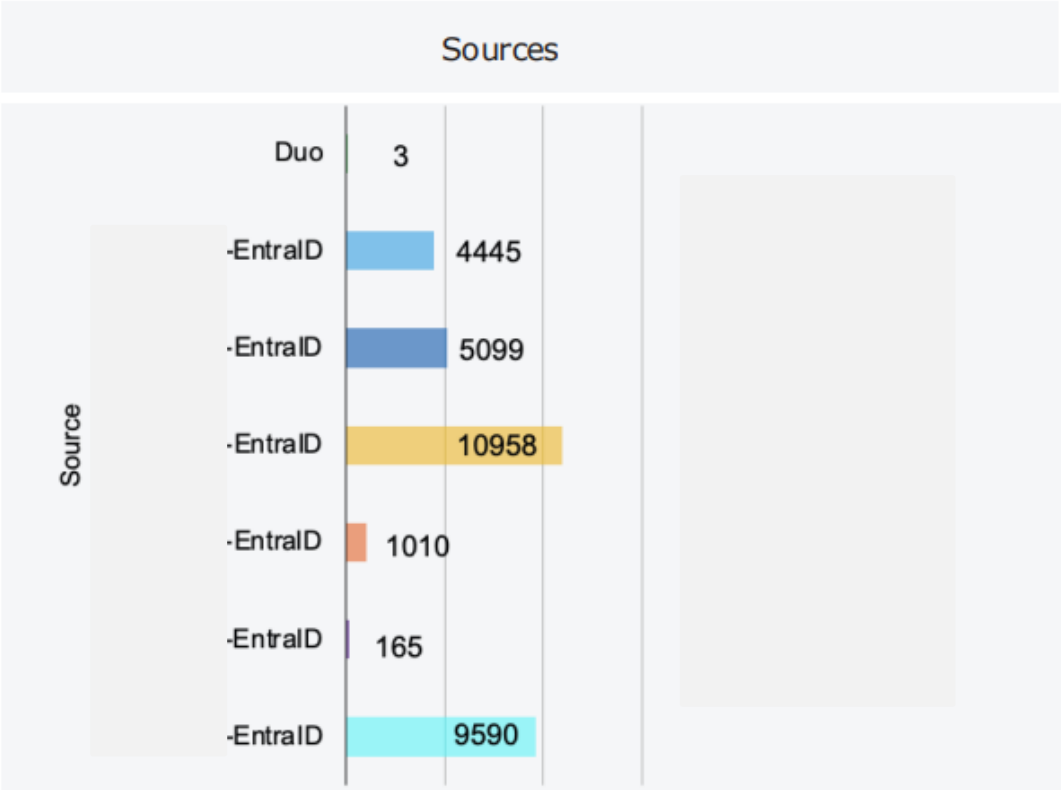
Last 30 Days

73

Administrators

73

Entra-ID Admins



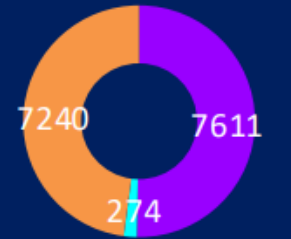
IAM Hygiene

Highlights

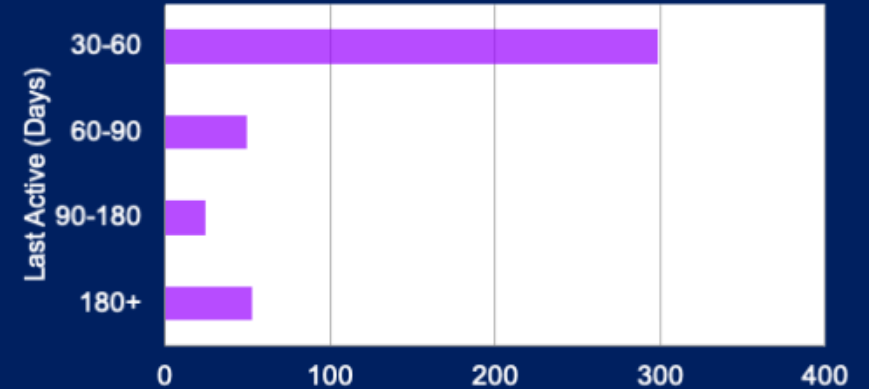
- アクティブでは無いアカウント
および、作成後7日経過しても利用されていないアカウント検出。
長期間利用していないアカウント
のクリーンアップを検討する。
- 2,899 の Inconsistent User を
検知。同じアカウントで複数の
IDPでのアクティビティを検出し
ていることが要因と考えられ、
High Severityのアクティビティ
は確認されていない。
- アカウント作成後、7日経過して
もログインされていないゲストユ
ーザの対応が必要。

441

Total inactive accts (+30
days)



Inactive users Inactive guest
Never logged in



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

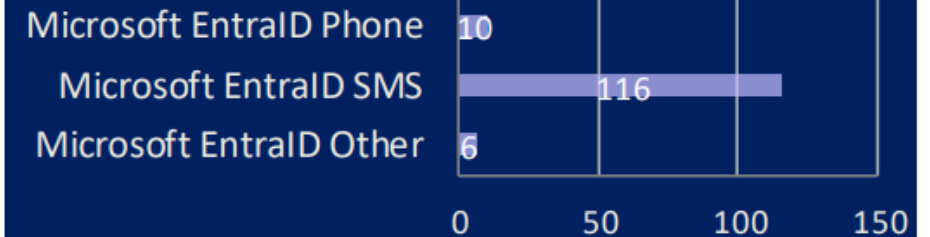
9

users successfully signed in using weak MFA
1,777 users have strong MFA

4,571

accounts with no MFA that actively log in to the system

Factor Used weak MFA



7,510

inactive users with no MFA
4 Admin Accounts with no MFA

28

Inactive accounts with failed logins

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多いため、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ト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。

Inactive Account Probing 31 24.91% decrease since last week 2.26% increase since last month
Critical End Users - Identity Threat Insight

Accounts With Unusually High Activity 8 124% increase since last week 56.7% increase since last month
Critical End Users - Identity Threat Insight

Threat: Critical

9

Accounts With Unusually High Activity

毎日のサインインイベントが多いため、悪意のある活動があるかどうか調査が必要。
(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あるいは一般的な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 Authenticator/Phone

Posture: Low

20

Personal VPN Usage

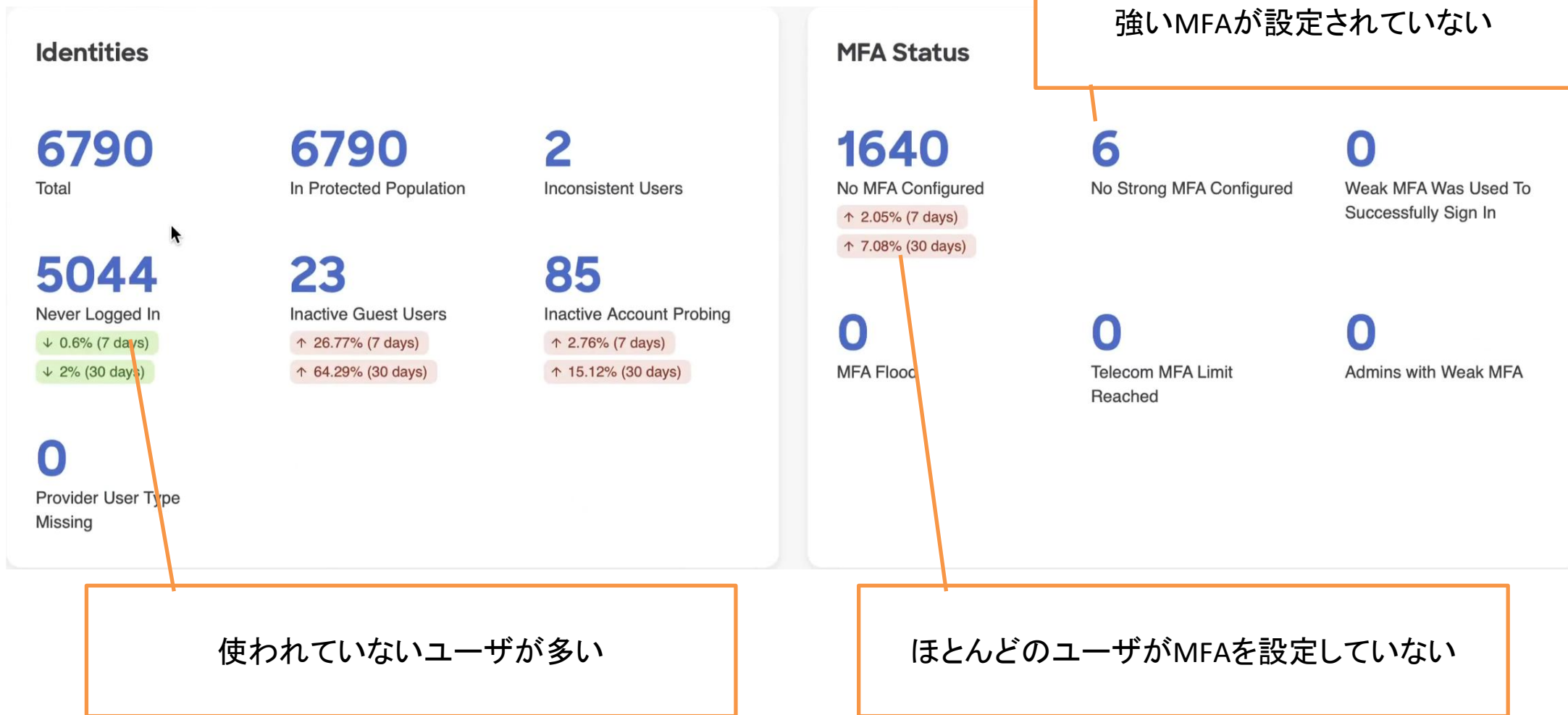
社内リソースへのアクセスにパーソナルVPNを
5回以上利用したユーザ

Cisco Identity Assessment実施事例②

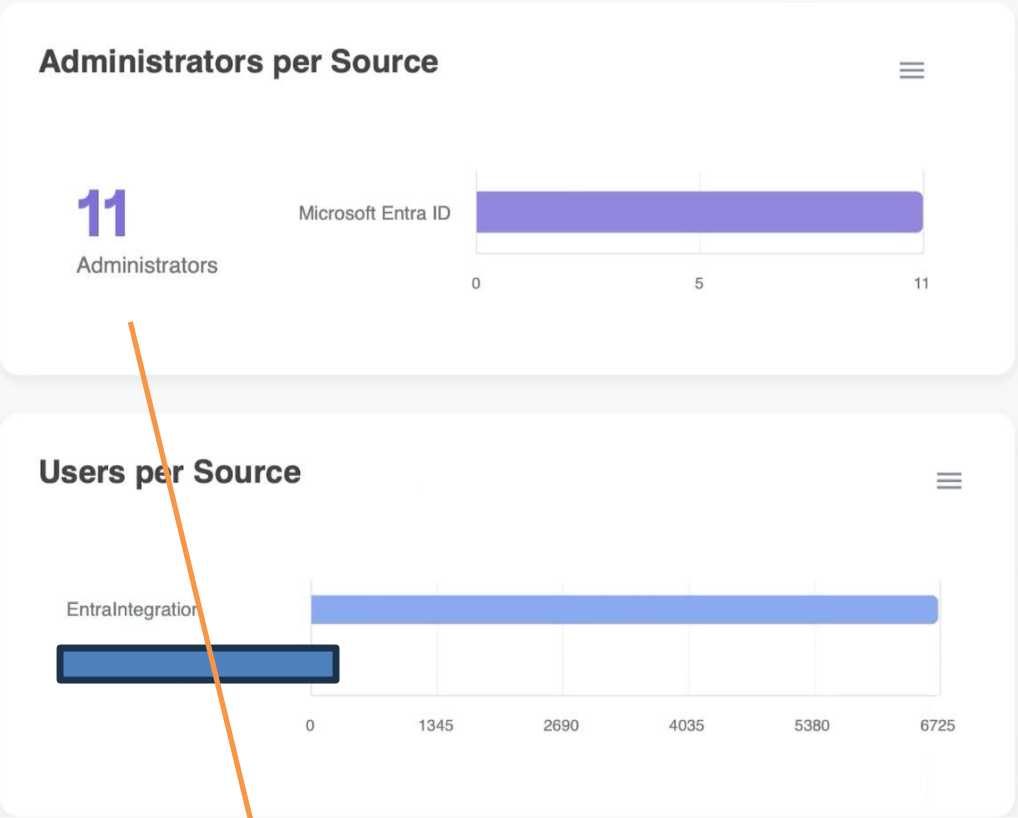
ヘルスケア関連企業様

従業員規模4000名程度

アイデンティティ・MFA



管理者アカウント



管理者ユーザの数

Administrators Logins

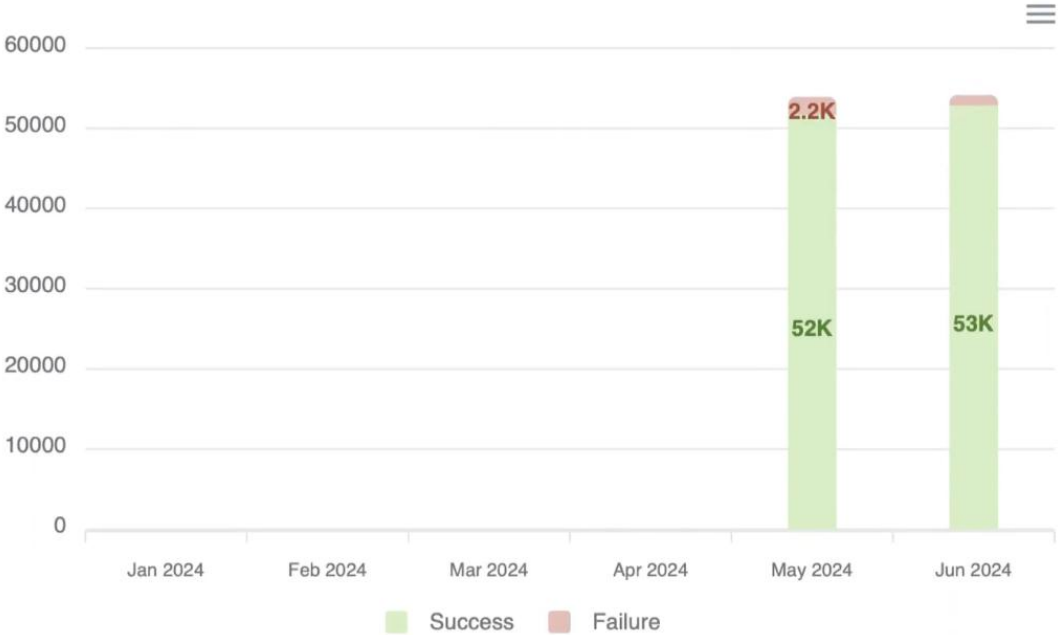
※サンプル

User	Last IP Address	Tags
Thrudi Brown	2.21.2.5 Moscow, Moscow, RU	New ISP Hosting
Brian Hayes	3.21.2.5 Reykjavik, IE	New ISP Hosting
Aalto Helmig	209.6.171.113 Burlington, MA, US	New ISP
Karsch Heuck	2600:1017:b808:d190:46... New York, NY, US	
Chanza Rosser	89.64.102.153 Gdansk, Pomerania, PL	New ISP
Daymude Sheiman	78.192.202.246 Paris, Île-de-France, FR	New ISP
Ayo Ganin	134.238.180.49 Ashburn, VA, US	New ISP Hosting

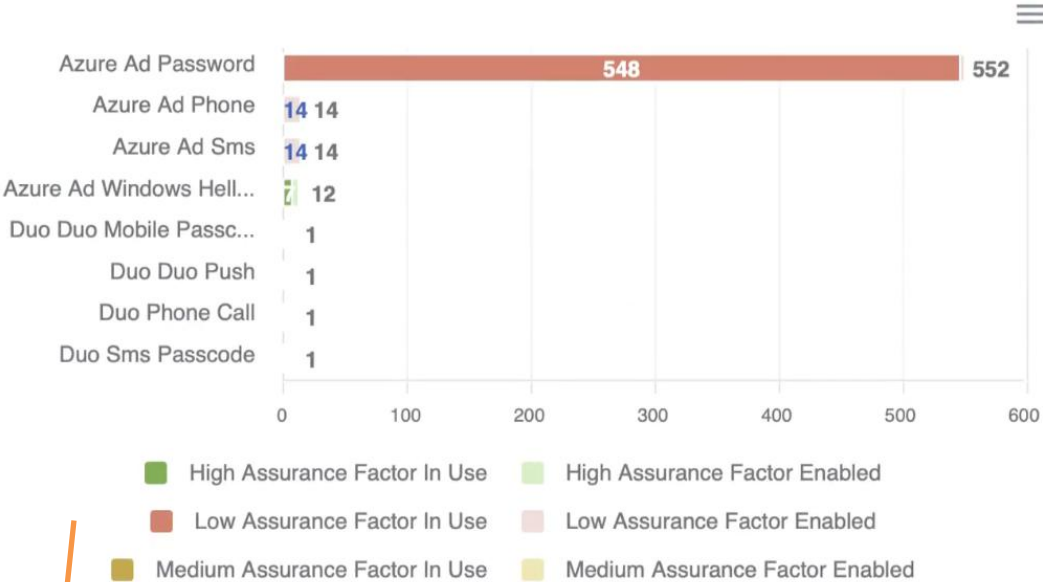
ありえないロケーション、IPからのアクセス等を
チェックしていくことを推奨

MFAの利用状況

Monthly Sign-Ins



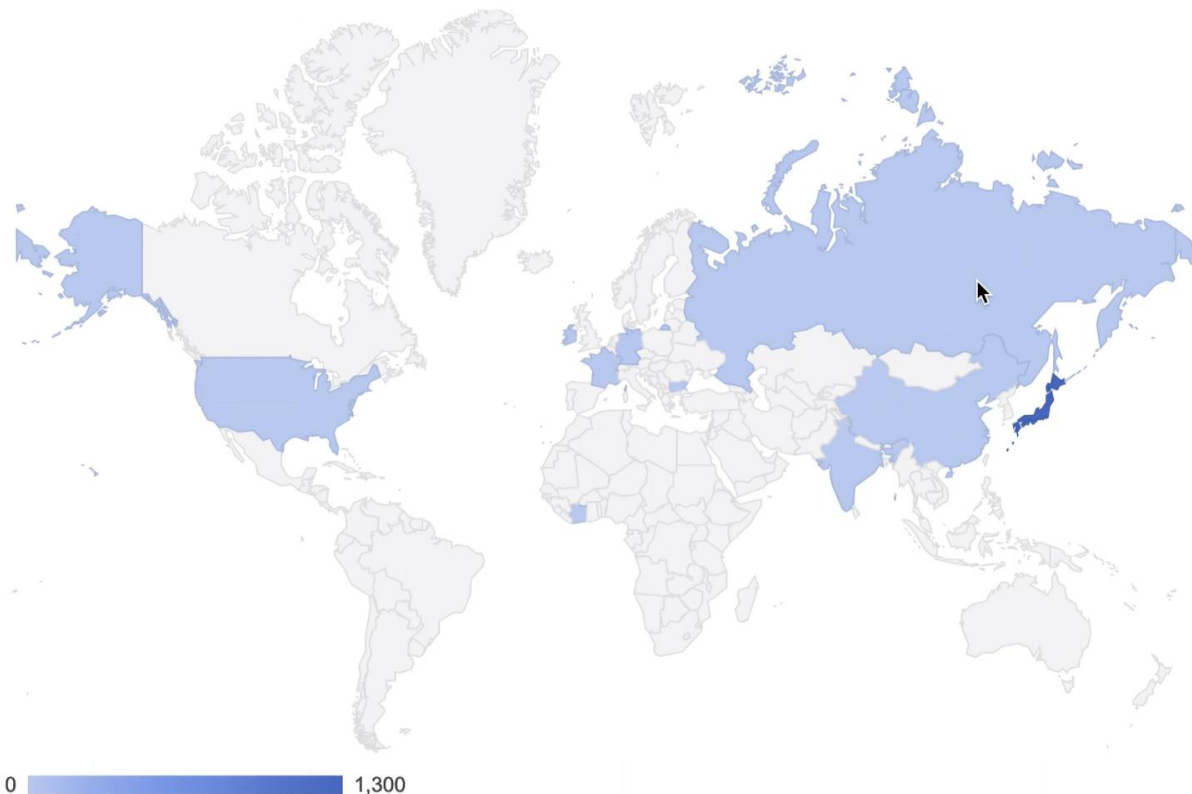
MFA Prevalence by User Count



より強度の強いMFAの設定を推奨

国別のアクセス状況

Last Sign In Attempts over the past 30 days



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

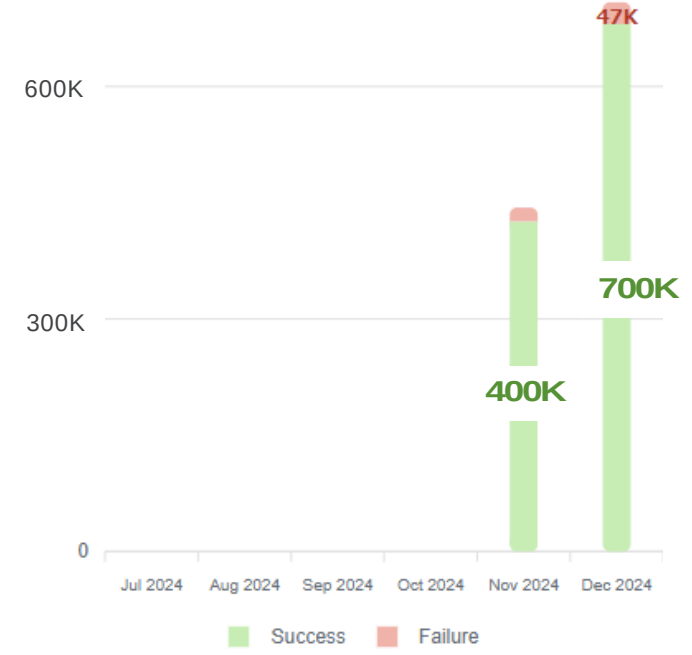
61,797

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ーが確認されました。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

Last Sign In Attempts over the past 30 days



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

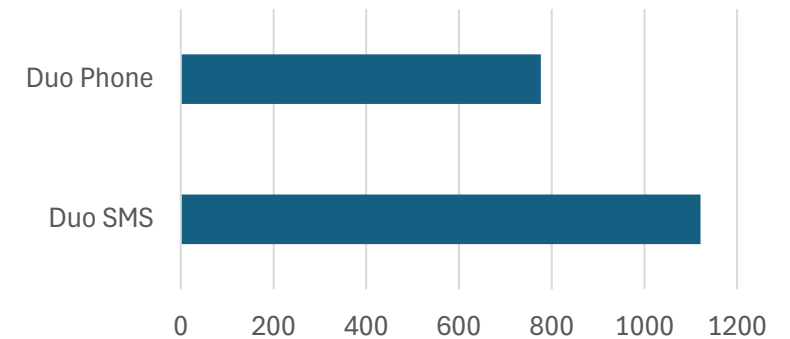
0

No Strong MFA Configured

0

Admins with weak MFA

Factor usec weakMFA



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 Failing 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

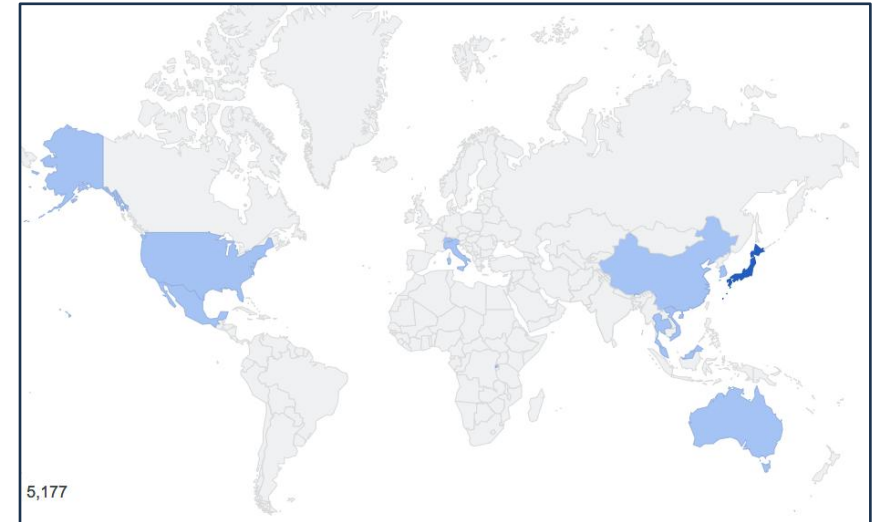
18

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

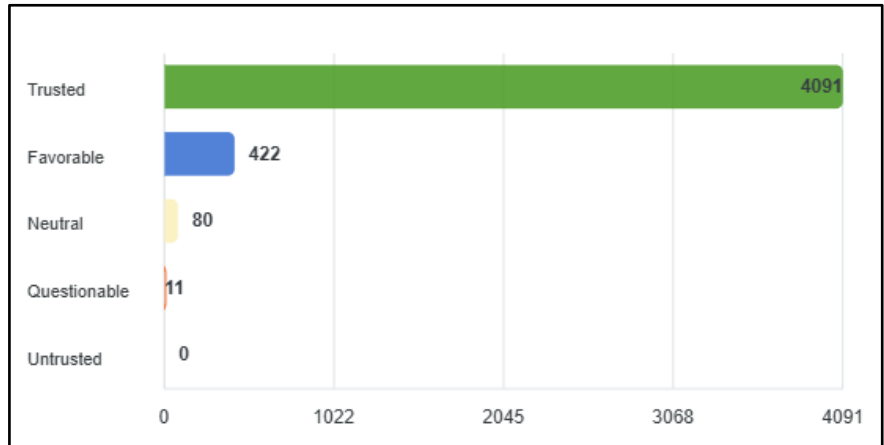
630

No Strong MFA Configured

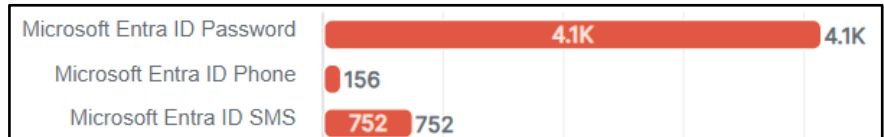
268

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ー

Cisco Identity Assessment実施事例⑤

化学/機械メーカ一様

従業員規模5000名程度

Identity Snapshot

2,720

総アイデンティティ数

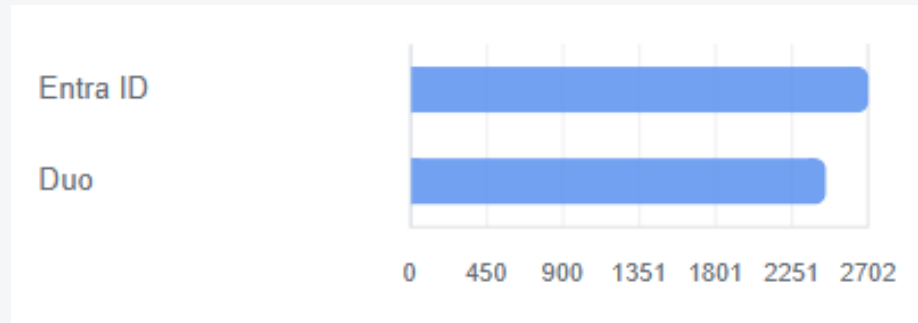
6

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

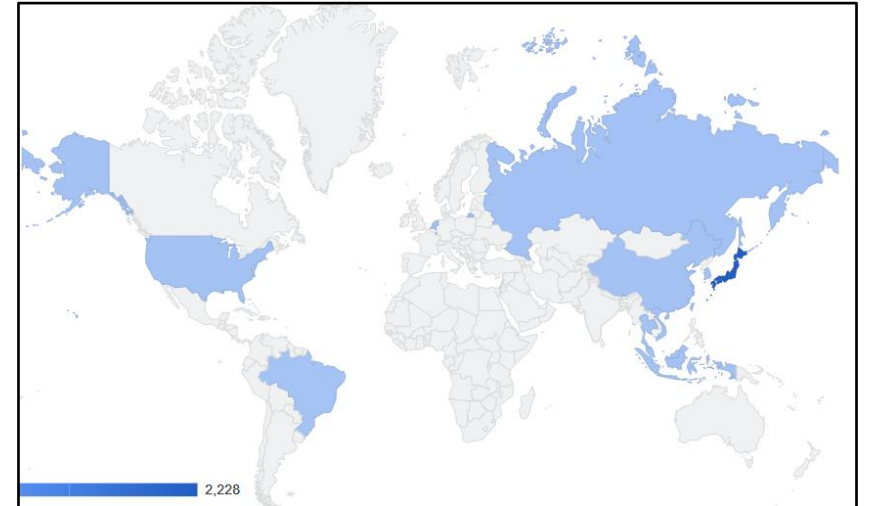
3

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

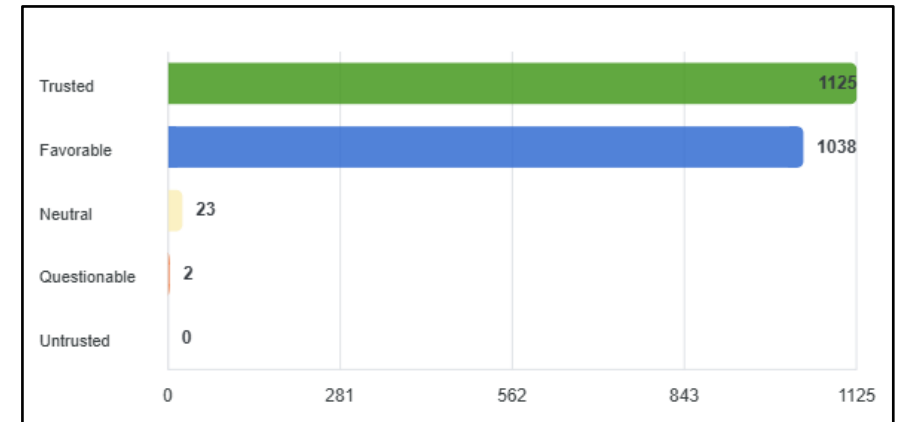
68

No Strong MFA Configured

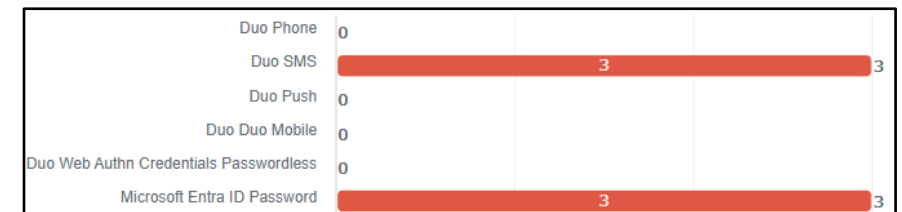
8

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ハイジーンのリビュー

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

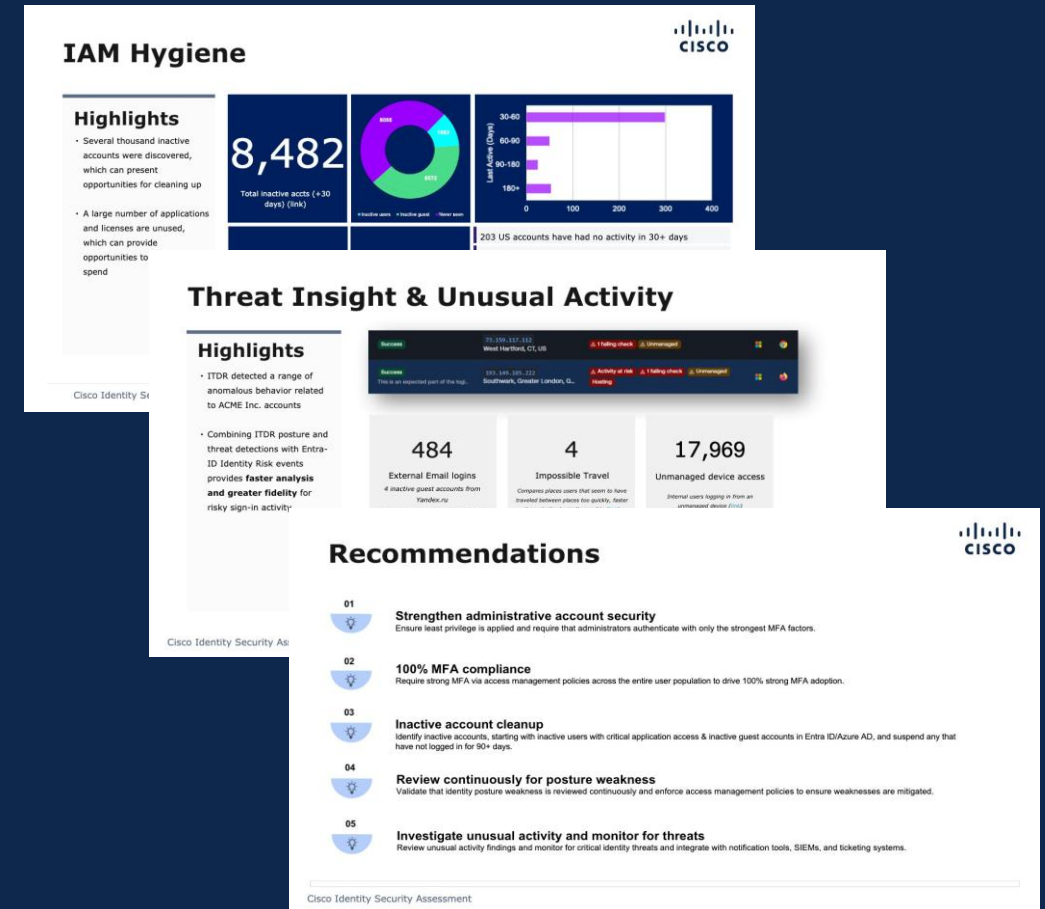
アイデンティティ関連攻撃の洞察

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

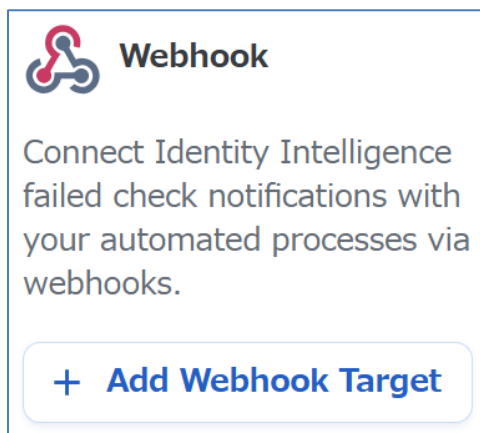


Cisco XDR 最新アップデート

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

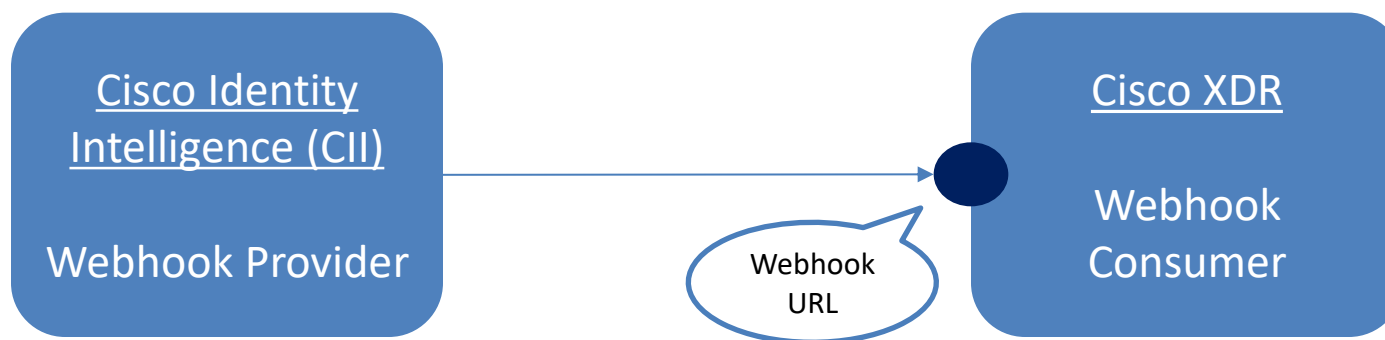
Webhookによる外部通知



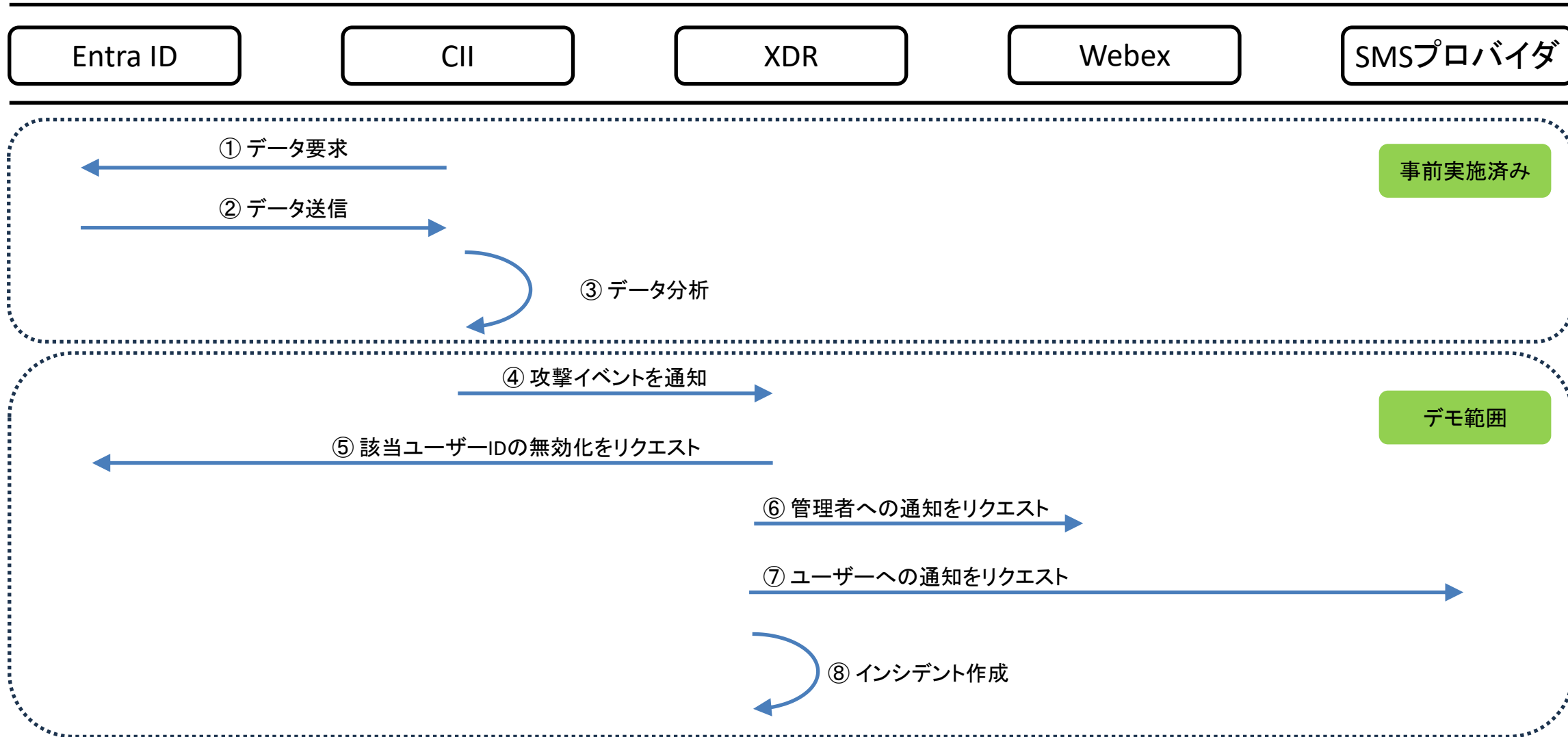
重大なイベントが発生した場合、Webhook Provider から Webhook Consumer へ通知を送信 (HTTP POST による JSON や XML 形式データの送信が一般的)

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



リスク検知後の手動レスポンス

Checks > Risky Parallel Sessions > pagotto.morren@simubiz.com

Pagotto Morren Burlington, MA, US Active
pagotto.morren@simubiz. Significant Change

Overview Activity Networks Devices Applications Groups Checks 7 ... Actions

Failing Checks

Name	Result	Times Excluded	First Reported (UTC)	Last Reported (UTC)	User/Manager Notified	Admin
Impossible Travel Moderate	Failure	0	Mar 28, 2025 16:17:54	Mar 28, 2025 16:26:22	Not supported	⚠ No Config
Weak MFA Was Used To Successfully Sign In Critical	Failure	0	Mar 28, 2025 16:16:58	Mar 28, 2025 16:26:22	Not notified	⚠ No Config
New Country for Tenant Moderate	Failure	0	Mar 28, 2025 16:16:58	Mar 28, 2025 16:26:22	Not notified	⚠ Notifications are not configured. Configure in check settings

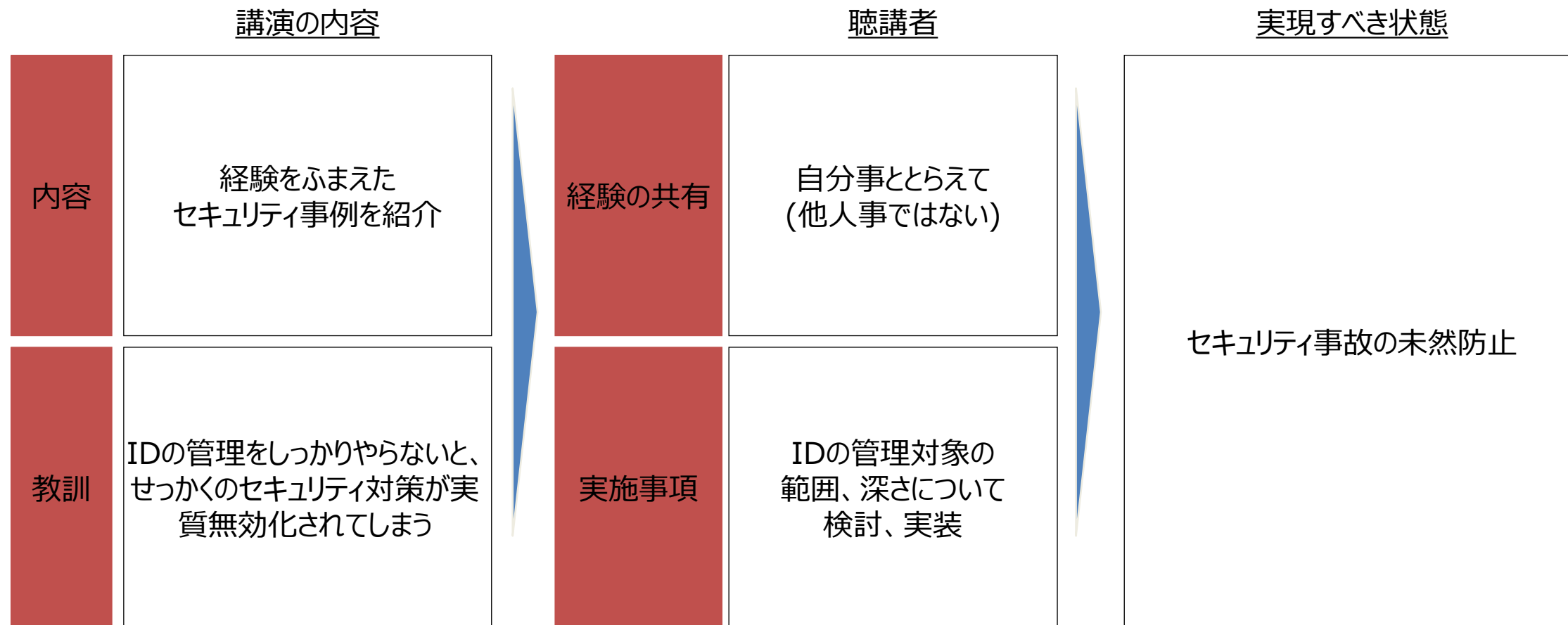
- + Open ticket
- 🔄 Reset MFA
- 🚪 Log out user
- 🔒 Quarantine
- 📱 Send Push Verification
- 🔄 Refresh User Data
- 👤 Link user

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



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

