シスコ エンタープライズ企業向け マンスリーウェビナー
ITDR のご紹介

～セキュリティインシデントの80%はIDから～

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

September 2024

ITDR (ID Threat Detection and Response) とは

2022年にGartnerによって提唱

侵入前の対策

侵入後の対策

IDに対する攻撃

ID管理・保護・予防対策

・MFA（Multi-Factor Authentication）
・IAM（Identity Access Management）
・PAM（Privileged Access Management）
・IGA（Identity Governance & Administration）
・CIEM（Cloud Infrastructure Entitlement Management）

侵入

検知(Detection)

・認証ソースのトラフィックの分析
・AD設定の監査
・不正なアクセス権限取得の検知
・異常な振舞いの検知
・脅威インテリジェンスやダークウェブ情報との合致
等

対応(Response)

・脅威の隔離
・IDの削除・無効化
・MFAのリセット
・ログアウトの強制
・脅威に応じた自動メッセージの送信
・レポート、報告
・XDRとの連携
等

ITDR の提供範囲

ITDRの主目的：ID・認証情報をモニタリングし、脅威や不正を検出・防御すること

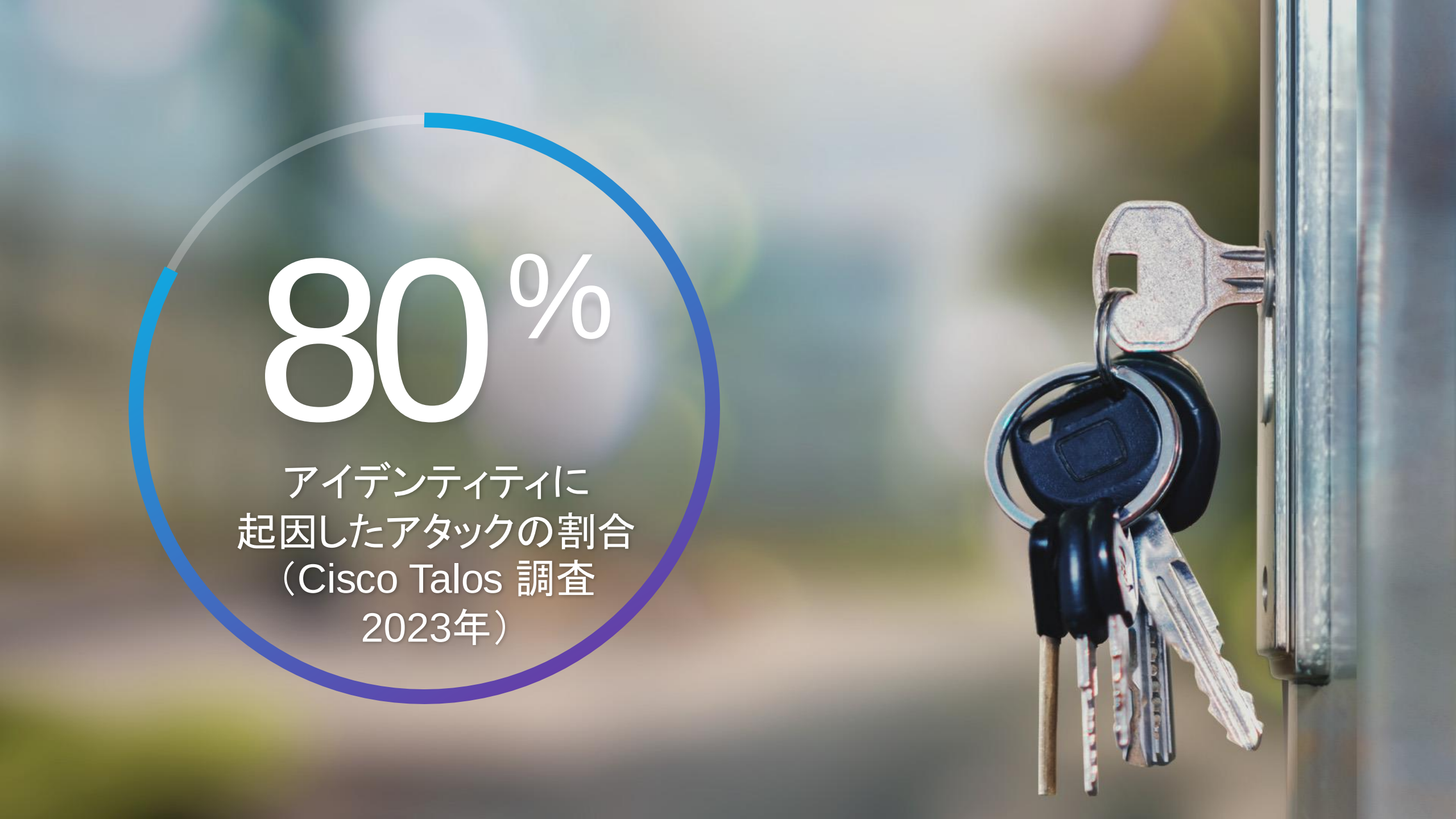
アジェンダ

1) ID攻撃の手法とフロー

2) Cisco ITDRのご紹介

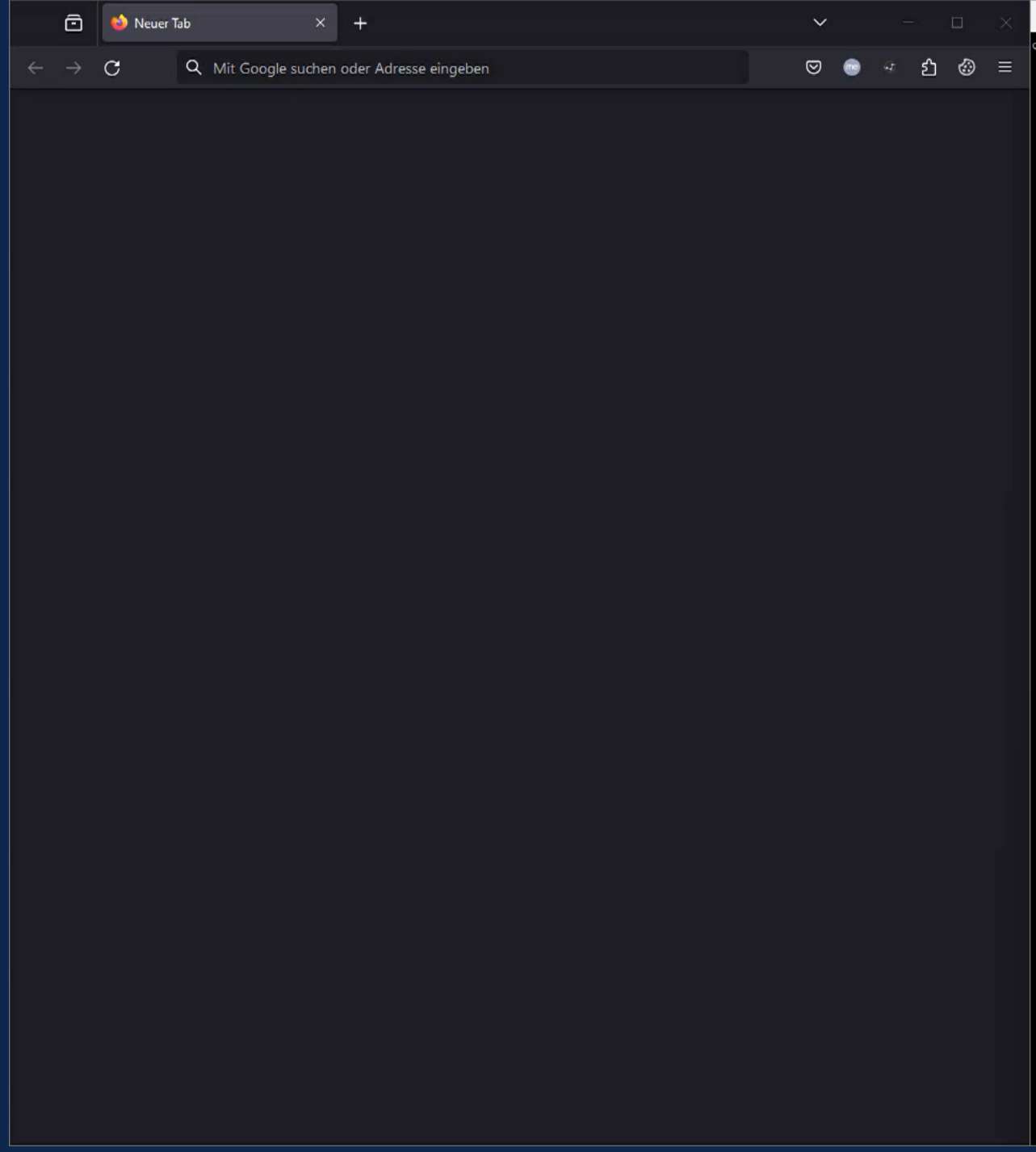
3) ITDR Demo

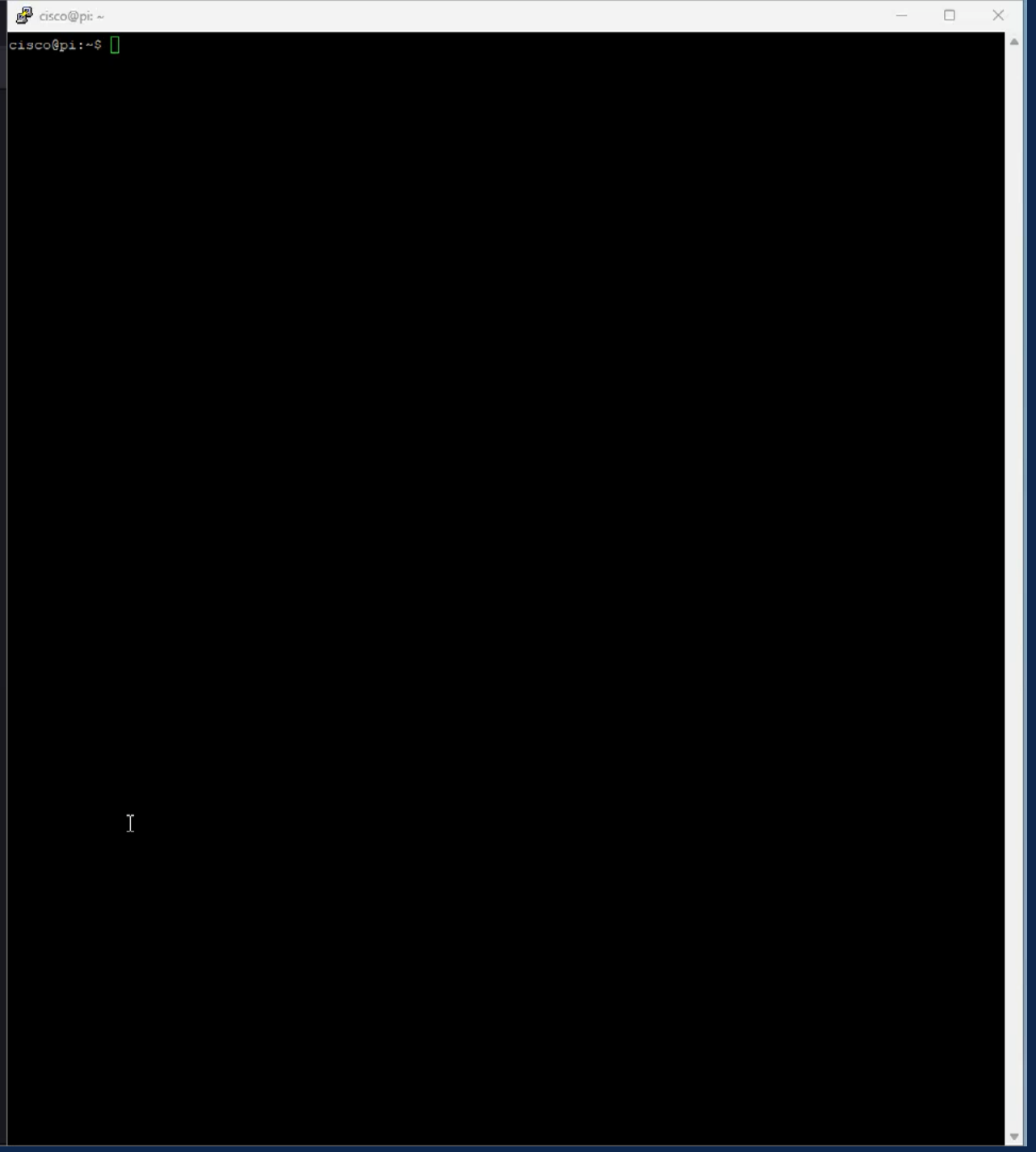
4) Q & A


80%
アイデンティティに
起因したアタックの割合
（Cisco Talos 調査
2023年）

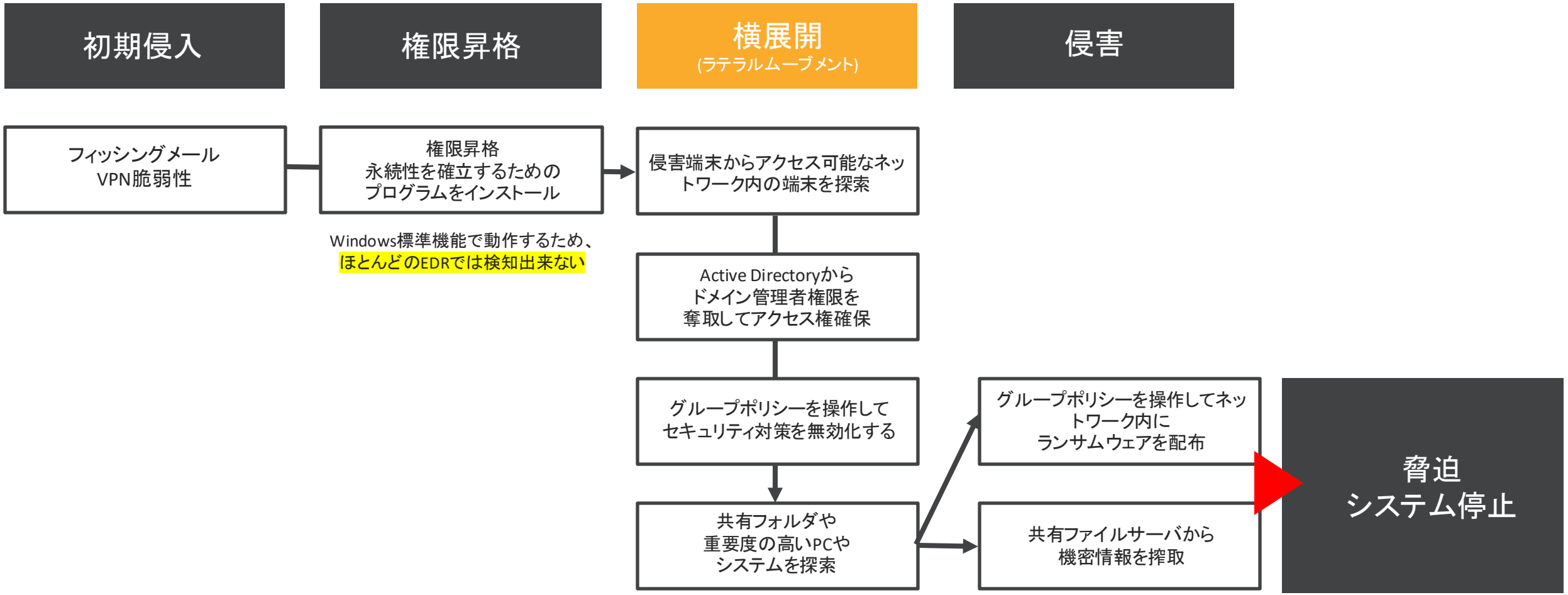
1）ID攻撃の手法とフロー

Demo：ハッカーによるフィッシング
簡単にID/Password・MFAを取得可能

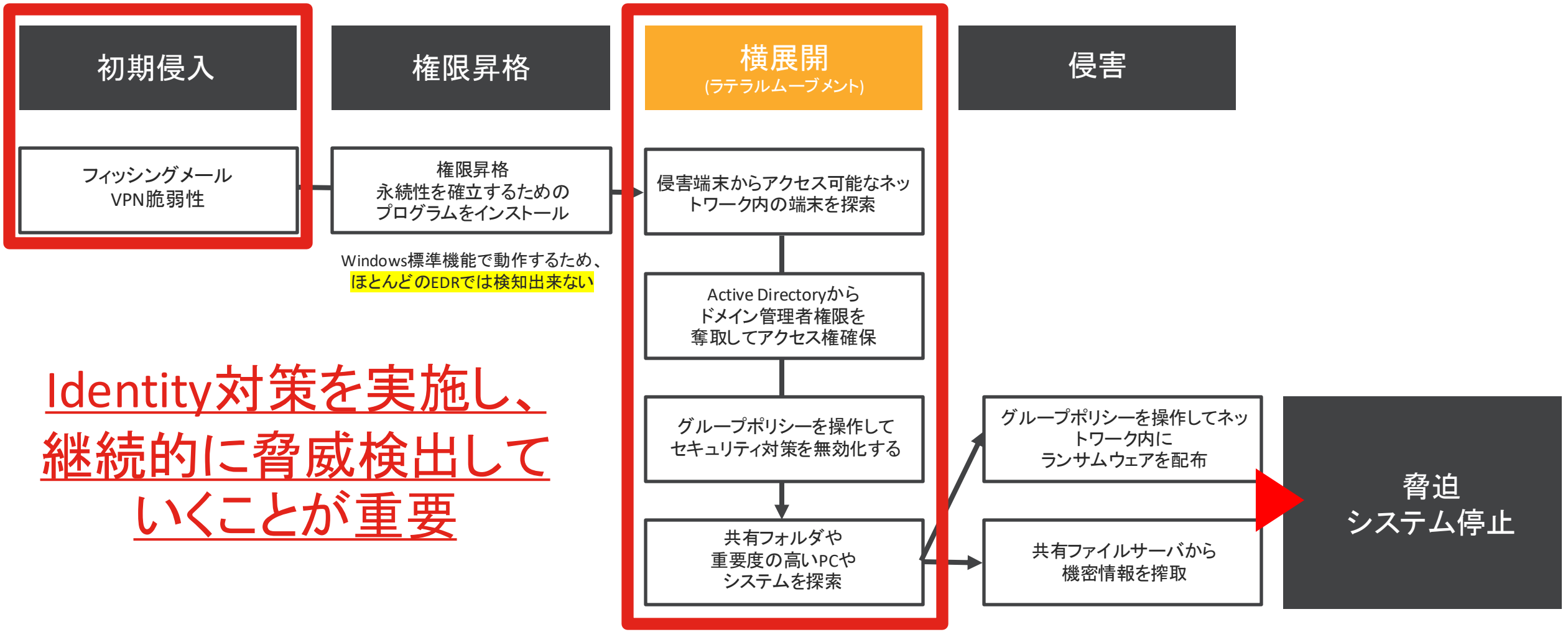

Neuer Tab
Mit Google suchen oder Adresse eingeben


cisco@pi: ~
cisco@pi:~$

攻撃のフローとラテラルムーブメント

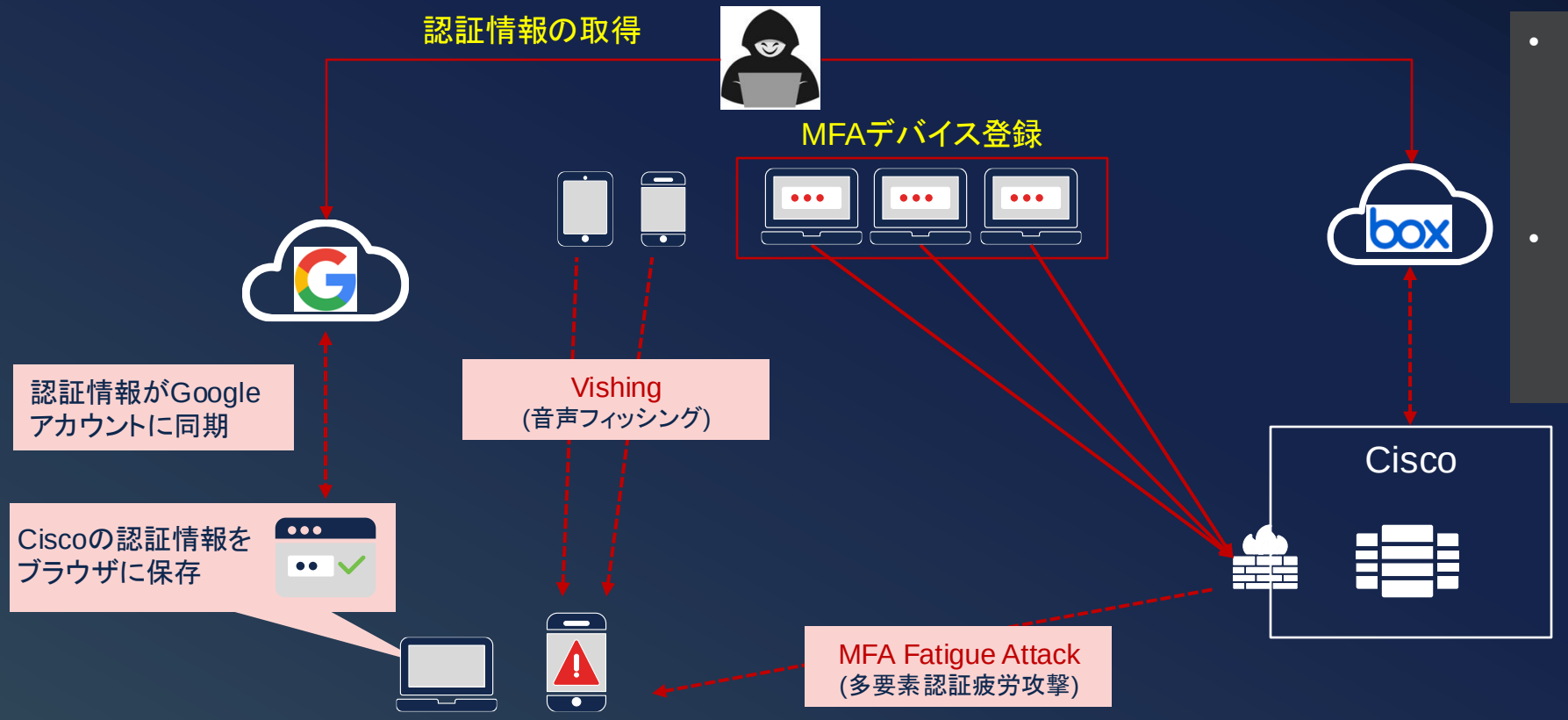


攻撃のフローとラテラルムーブメント



Identity対策を実施し、継続的に脅威検出していくことが重要

2022年5月：シスコに対するサイバー攻撃



- 最初のアクセスを取得した後、脅威行為者は、アクセスを維持し、フォレンジックアーティファクトを最小限に抑え、環境内のシステムへのアクセスレベルを上げるために、様々な活動を実施
- この脅威アクターを環境から排除することに成功し、攻撃後の数週間、繰り返しアクセスを回復しようとする粘り強さを見せたが、これらの試みは失敗

ユーザーの認証情報を入手した後、ボイスフィッシング（別名「ビッシング」”vishing”）やMFA疲労攻撃 “MFA fatigue”（誤って、あるいは単に繰り返し受信するプッシュ通知を黙らせるために、ユーザーが承諾するまでターゲットのモバイルデバイスに大量のプッシュ要求を送信するプロセス）など、さまざまな手法を用いて多要素認証（MFA）をバイパスしようと試みた

Cisco IT 侵害からの教訓

アイデンティティ・認証においてすべきこと

1

アイデンティティの可視化

多様なアイデンティティの可視化

一元化された洞察

アラート情報の統合とノイズ除去

2

強固な認証の展開

MFA（多要素認証）の徹底

フィッシング耐性MFA

デバイス健全性の確認（検疫）

3

ガバナンスの強化

動的なアクセスポリシー

ブロックポリシーの柔軟な選択肢

リスクに対する迅速な対応

加えて、ユーザ利便性を下げないこと

2024年2月27日

Gartner、2024年のサイバーセキュリティのトップ・トレンドを発表

ガートナージャパン株式会社 (本社：東京都港区、以下Gartner) は、2024年のサイバーセキュリティのトップ・トレンドを発表しました。本トップ・トレンドの推進要因には、ジェネレーティブAI (生成AI)、セキュリティ意識の低い従業員の行動、サードパーティのリスク、継続的な脅威エクスポージャ、取締役会でのコミュニケーション・ギャップ、セキュリティに対するアイデンティティ・ファーストなアプローチの6つが挙げられます (グローバルでは2024年2月22日に発表しています)。

トレンド6：サイバーセキュリティの成果向上における役割拡大を支えるアイデンティティ／アクセス管理 (IAM) の進化

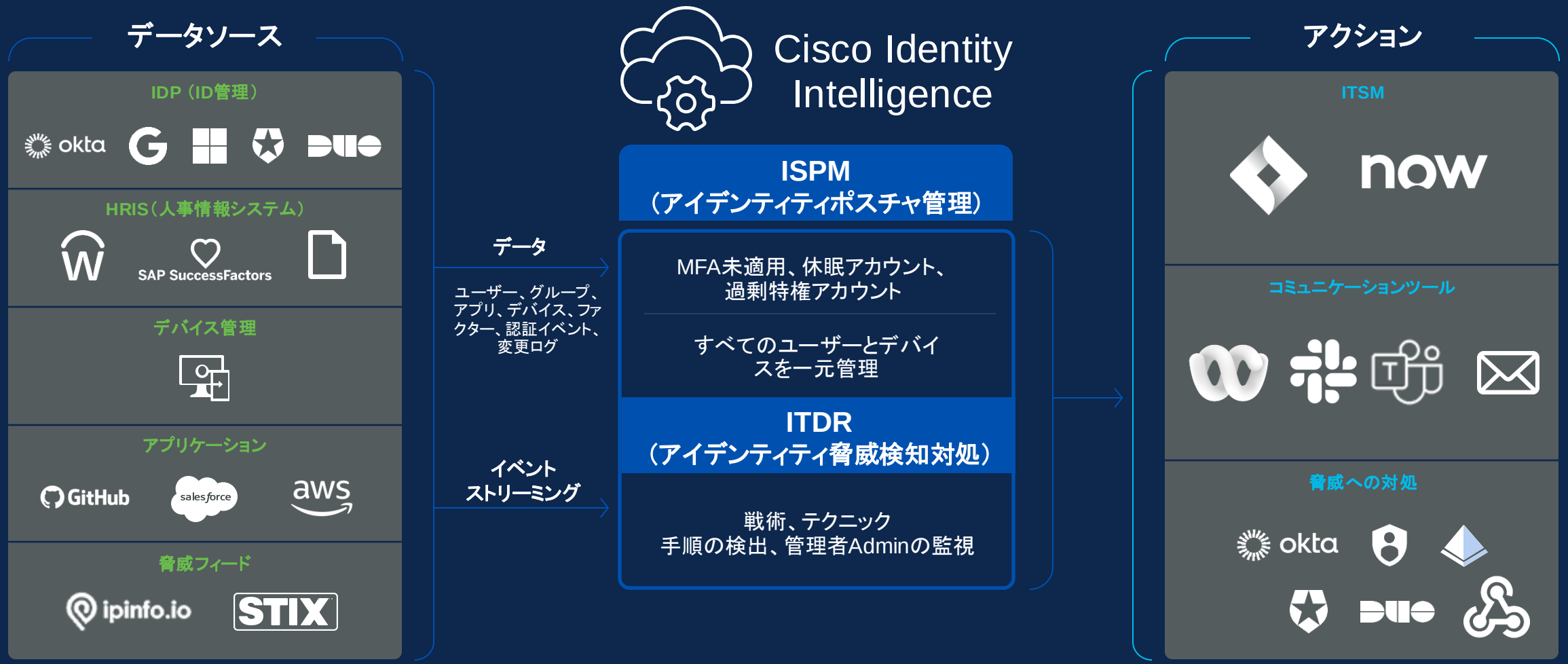
より多くの組織がアイデンティティ・ファーストのセキュリティ・アプローチを採用するにつれて、セキュリティの重点は、ネットワーク・セキュリティやその他の従来型コントロールから、アイデンティティ・アクセス管理 (IAM) に移行しています。IAMは、組織のサイバーセキュリティ成果、ひいてはビジネス成果に寄与する重要な要素となっています。Gartnerはセキュリティ・プログラムにおけるIAMの役割が拡大する一方で、基本的なIAMのハイジーン (衛生) とレジリエンス向上に向けたIAMシステムの強化に注力する必要があるとみています。

セキュリティ・リーダーは、アイデンティティ・ファブリックの強化と活用に重点を置き、アイデンティティ脅威検知／対応 (ITDR) を活用して、IAMのケイパビリティがセキュリティ・プログラム全体を幅広くサポートする取り組みを推進することが重要です。

2） Cisco ITDRのご紹介

Cisco IT 侵害からの教訓

ITDR用途でOortの利用→買収→Cisco Identity Intelligenceのリリース



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

Cisco Identity Intelligence Demo

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

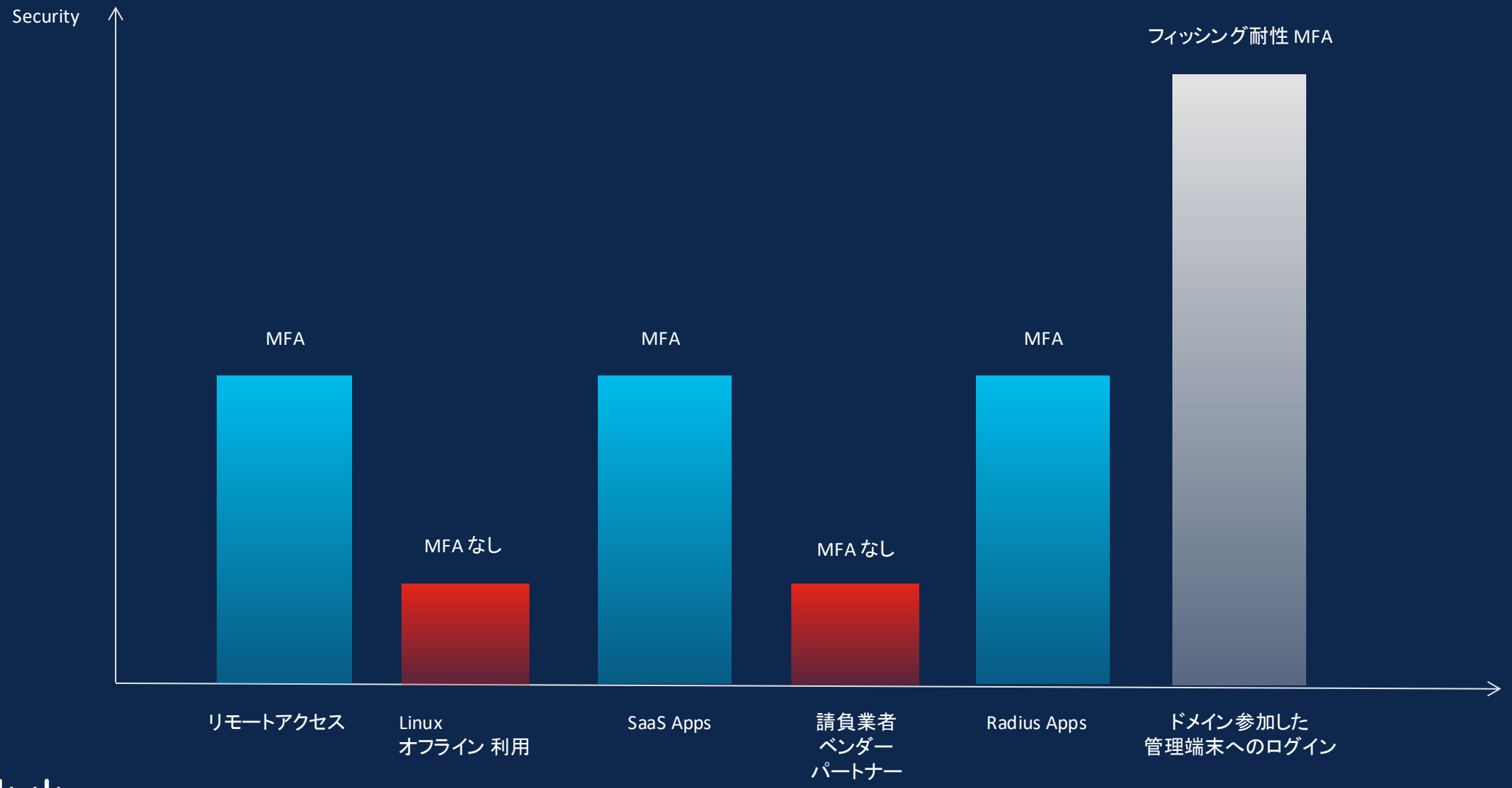
（ユーザ状況及びセッション状況調査分析）

3) 継続的な脅威の管理　3パターン

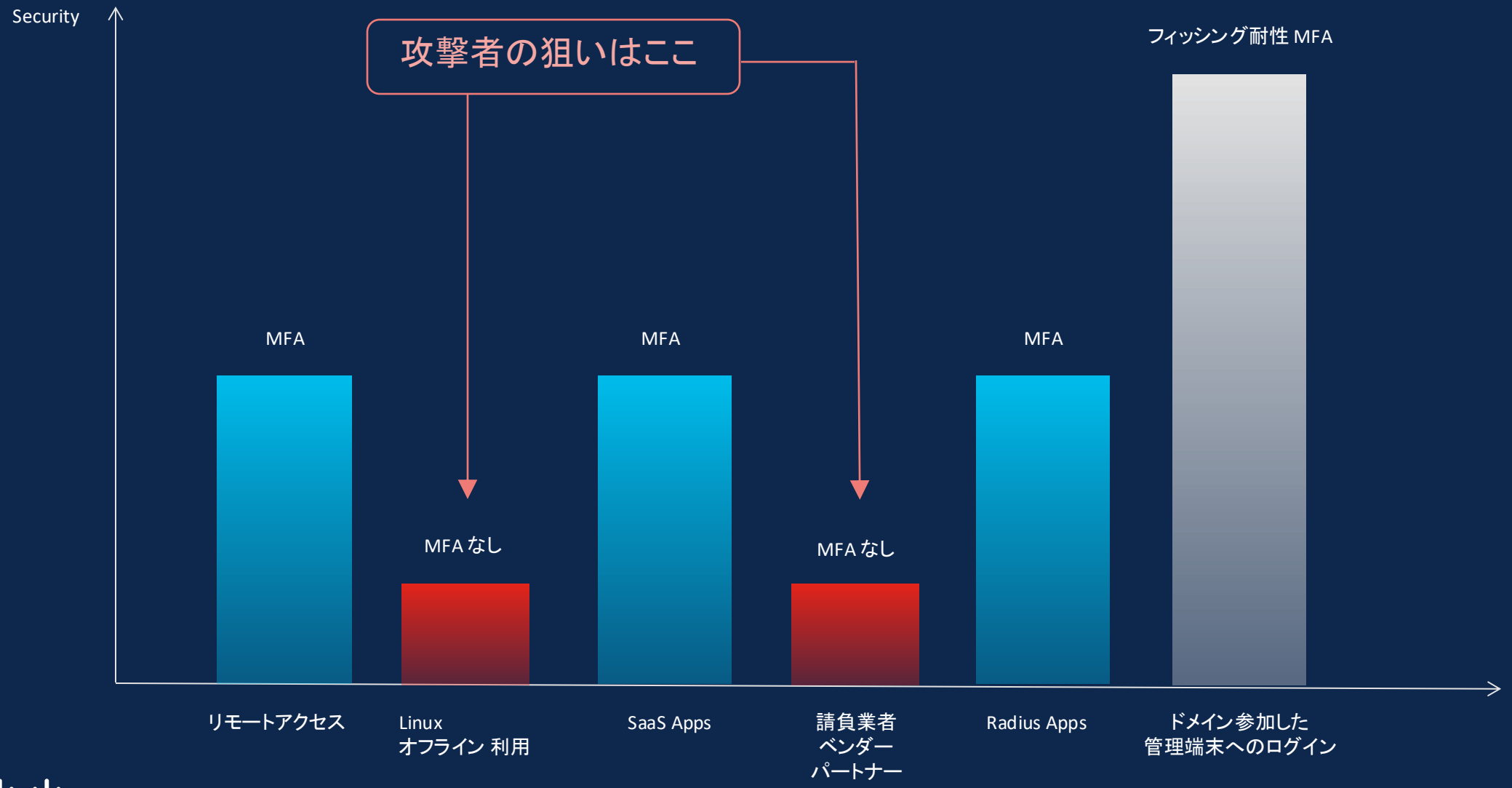
Cisco Identity Intelligence Demo

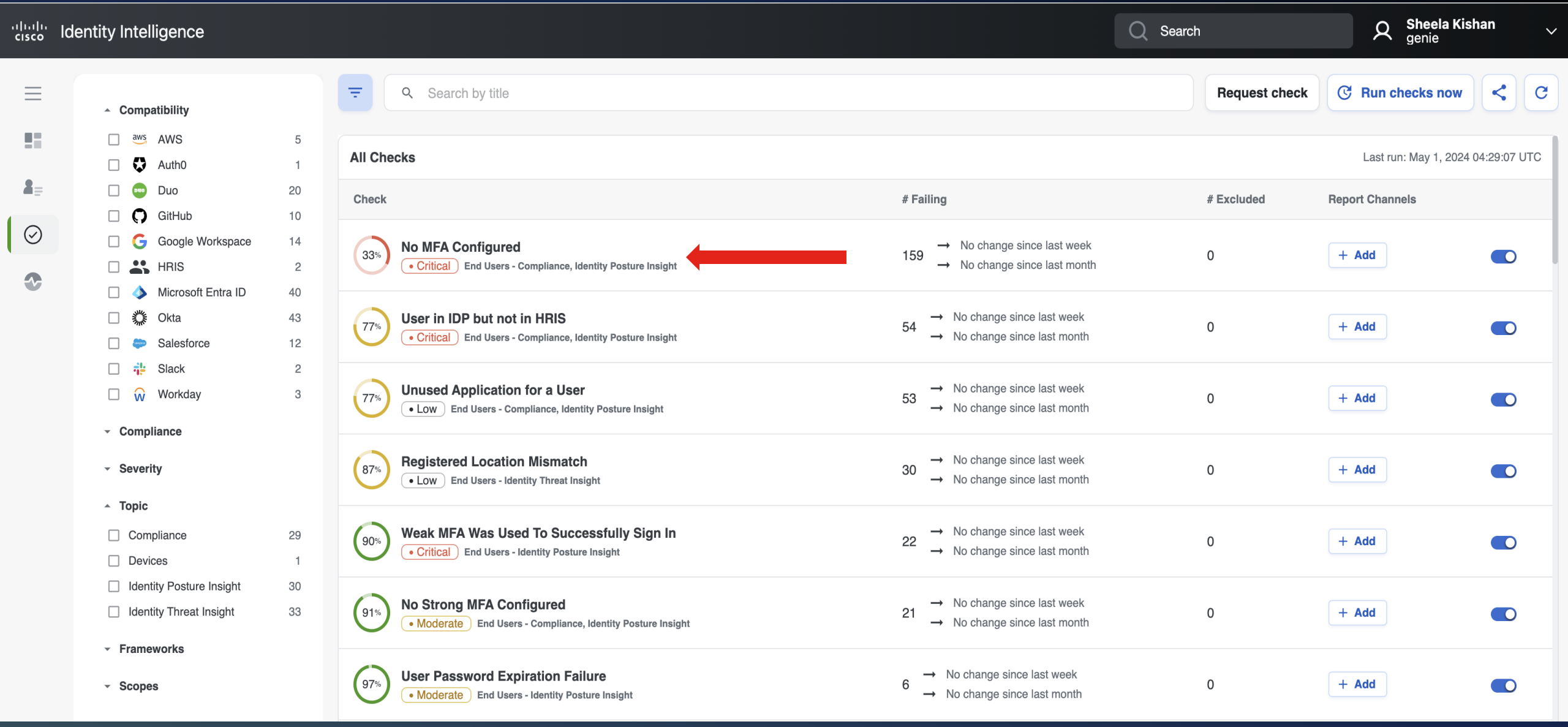
ユースケース①
非従業員アカウント
モニタリング

課題: Identityに対する対策に差異がある



課題: Identityに対する対策に差異がある





Details

Detects users with no Multi-Factor Authentication (MFA) enabled.

MFA requires users to provide something you know, like a password or PIN, or something you have, like an out-of-band device or a one-time password provider. All users should be using MFA to gain access to the system.

Users will not fail this check if they fall within the grace period of 14 days.

You can add known domains to either ignore or include list.

Learn More About the Risk

Recommended Actions

Some system accounts may not have MFA. We recommend categorizing those for easy detection. Consider using solutions like expired passwords to block access to these accounts.

Last Report Update
May 2, 2024 04:33:03 UTC

Topics
Compliance, Identity Posture Insight

Frameworks
NIST 800-63-3, CIS 6.3, CIS 6.4, CIS 6.5, NIST CSF PR.AC-7, ASD Essential 8, CMMC IA.3.083, PCI DSS 8.2, Mitre Mitigation M1032

Compatibility
Microsoft Entra ID, Okta, Duo, Google Workspace, GitHub

Tags
+ Add tag

Check Settings

- Custom Detection Settings
- Notification Settings
- List Settings

Failing Users

159

No change (7 days)
No change (30 days)

66% of Users failing

Failing Users Per Integration

- Demo Okta - 154 — 96.86% of Failing Users
- Demo Azure AD - 2 — 1.26% of Failing Users
- Demo Workday - 2 — 1.26% of Failing Users
- Demo GitHub - 1 — 0.63% of Failing Users
- Demo Salesforce - 1 — 0.63% of Failing Users

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

159 failing users

View users | Download List

User	First Reported (UTC) ↑	Last Reported (UTC) ↑	User/Manager Notified	Admin Notified
service.account@simubiz.com	May 2, 2024 04:29:30	May 2, 2024 04:32:45	Not notified	Not notified
staller.fohey@gmail.com	May 2, 2024 04:29:30	May 2, 2024 04:32:45	Not notified	Not notified

Excluded Users

0

Unprotected users failing

0

Cisco Identity Intelligence Demo

ユースケース②
ユーザ状況及びセッション状況調査分析
→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 6
- Auth0 1
- Duo 21
- GitHub 11
- Google Workspace 15
- HRIS 2
- Microsoft Entra ID 42
- Okta 44
- Salesforce 13
- Slack 2
- Workday 3

Compliance All

- Full 7
- Partial 56
- Not Enabled 1

Severity All

- Critical 20
- Low 16
- Moderate 28

Topic All

- Compliance 30

Search by title

Request check | Run checks now

All Checks

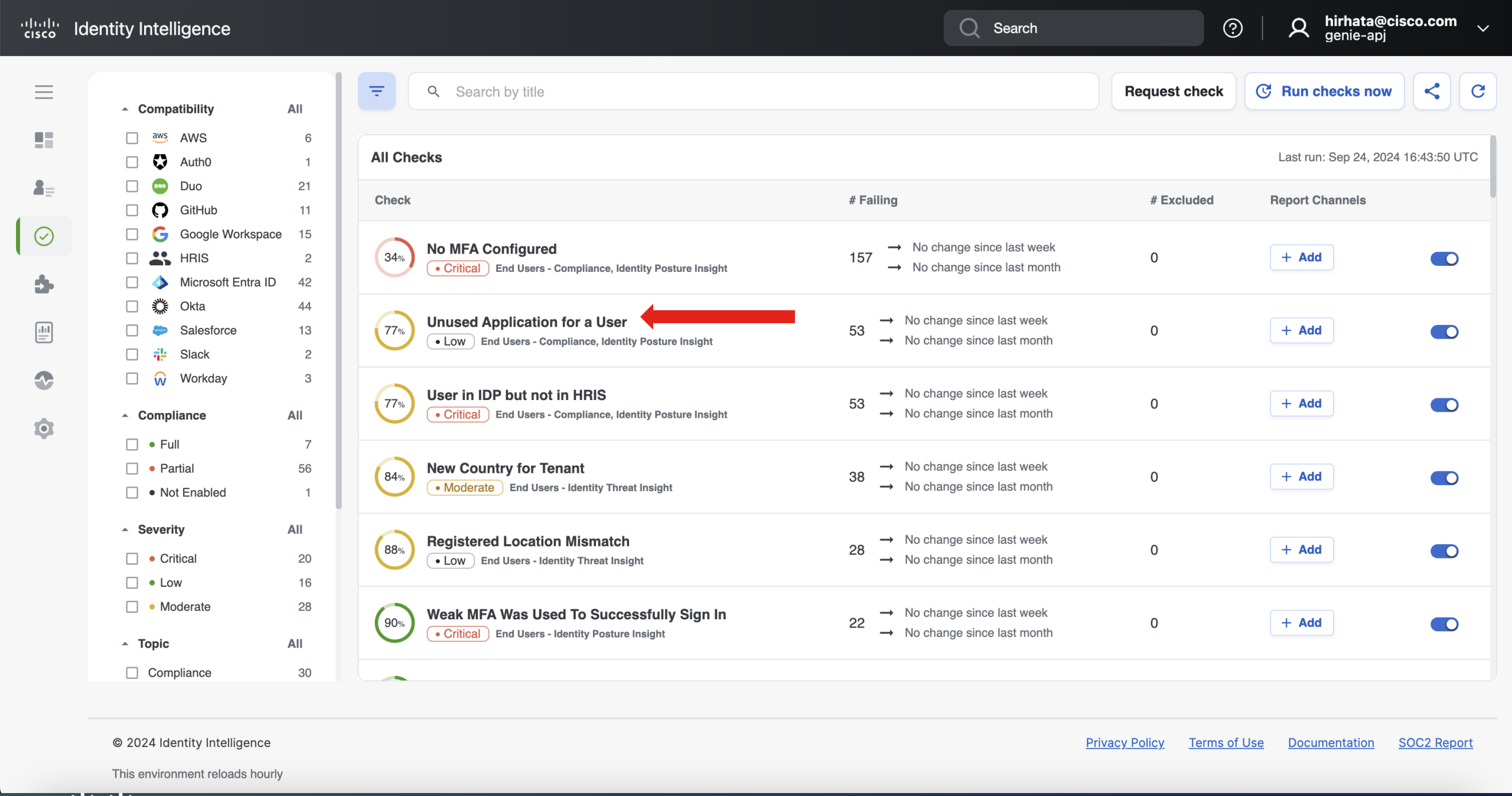
Last run: Sep 24, 2024 16:43:50 UTC

Check	# Failing	# Excluded	Report Channels
• Low End Users - Identity Posture Insight	→ No change since last month		
98% **Inactive Users** • Moderate End Users - Compliance, Identity Posture Insight	4 → No change since last week → No change since last month	0	+ Add
98% **Never Logged In** • Critical End Users - Compliance, Identity Posture Insight	4 → No change since last week → No change since last month	0	+ Add
98% **Allow/Block Email Logins** • Critical End Users - Compliance, Identity Posture Insight	3 → No change since last week → No change since last month	0	+ Add
98% **Provider User Type Missing** • Moderate End Users - Compliance, Identity Posture Insight	3 → No change since last week → No change since last month	0	+ Add
99% **Rare Browser Activity** • Moderate End Users - Compliance, Identity Threat Insight	2 → No change since last week → No change since last month	0	+ Add
99% **Role Assigned to Azure Cloud Only Account** • Moderate End Users - Identity Posture Insight	2 → No change since last week → No change since last month	0	+ Add

Back to top

Privacy Policy | Terms of Use | Documentation | SOC2 Report

This environment reloads hourly



Compatibility All

- AWS 6
- Auth0 1
- Duo 21
- GitHub 11
- Google Workspace 15
- HRIS 2
- Microsoft Entra ID 42
- Okta 44
- Salesforce 13
- Slack 2
- Workday 3

Compliance All

- Full 7
- Partial 56
- Not Enabled 1

Severity All

- Critical 20
- Low 16
- Moderate 28

Topic All

- Compliance 30

Search by title

Request check | Run checks now

All Checks

Last run: Sep 24, 2024 16:43:50 UTC

Check	# Failing	# Excluded	Report Channels
34% **No MFA Configured** • Critical End Users - Compliance, Identity Posture Insight	157 → No change since last week → No change since last month	0	+ Add
77% **Unused Application for a User** • Low End Users - Compliance, Identity Posture Insight	53 → No change since last week → No change since last month	0	+ Add
77% **User in IDP but not in HRIS** • Critical End Users - Compliance, Identity Posture Insight	53 → No change since last week → No change since last month	0	+ Add
84% **New Country for Tenant** • Moderate End Users - Identity Threat Insight	38 → No change since last week → No change since last month	0	+ Add
88% **Registered Location Mismatch** • Low End Users - Identity Threat Insight	28 → No change since last week → No change since last month	0	+ Add
90% **Weak MFA Was Used To Successfully Sign In** • Critical End Users - Identity Posture Insight	22 → No change since last week → No change since last month	0	+ Add

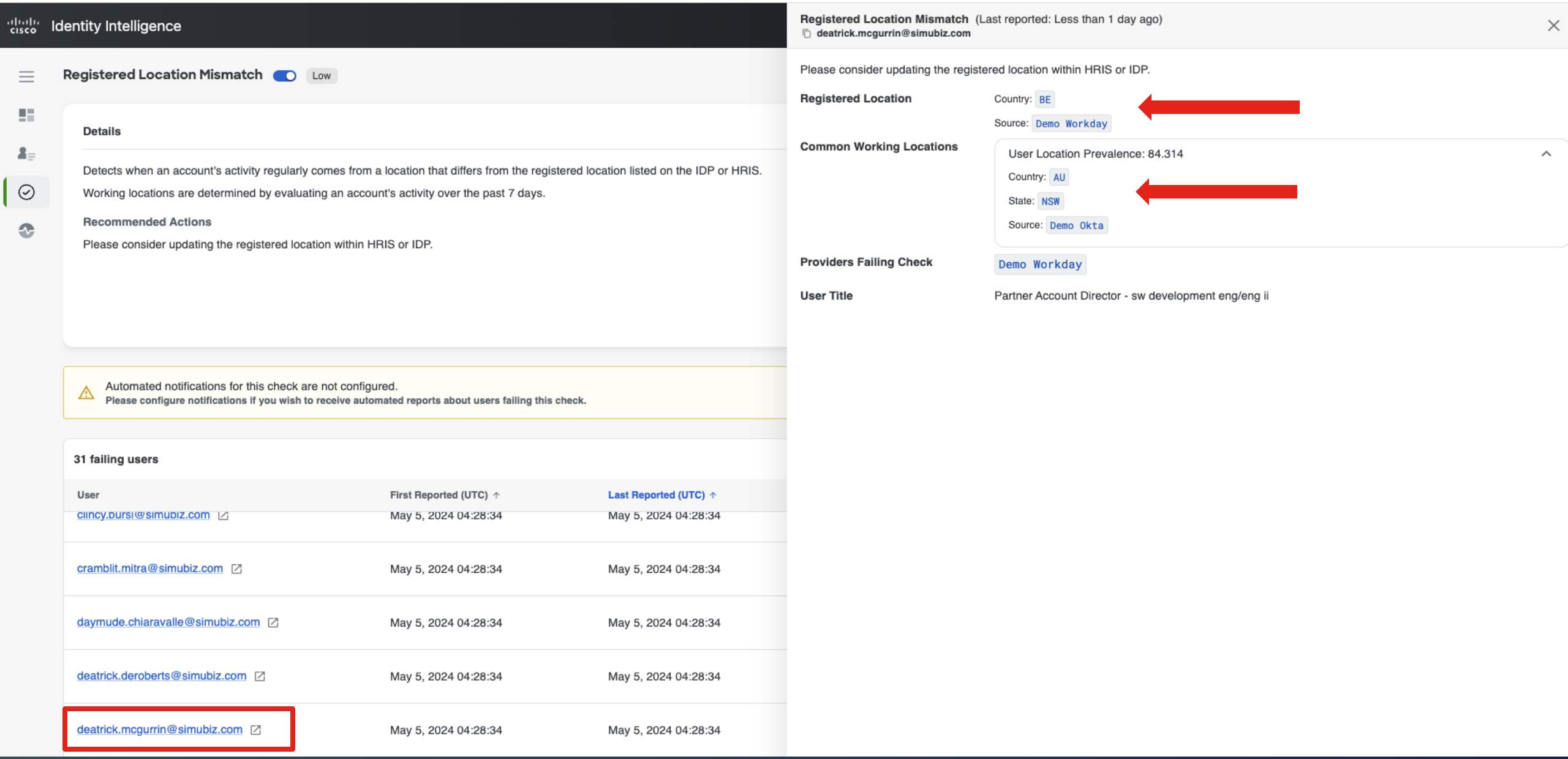
This environment reloads hourly

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

P **Pagotto Morren** Burlington, MA, US Active

pagotto.morren@simubiz.com

Overv

Failing Checks

Name	Result	Times Excluded	First Reporte
Weak MFA Was Used To Successfully Sign In • Critical	Failure	0	Sep 24, 202
New Country for Tenant • Moderate	Failure	0	Sep 24, 202
Registered Location Mismatch • Low	Failure	0	Sep 24, 202
Risky Parallel Sessions • Critical	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

Risky Parallel Sessions (Last reported: Less than 1 day ago) View activity from all sessions

Please verify the users with sessions running in parallel are from IT/InfoSec teams.

Providers Failing Check `Demo Okta`

External Session Ids `102z0f8ZaV8QR66X2M3_drYBB`

`102cmxHllJUSdW1J8sZ_9PPBB`

User Title senior site reliability engineer

User Level Of Trust QUESTIONABLE

Activity targets

App `palo alto networks - prisma access`

User `Pagotto morren`

App `cisco asa vpn (saml)`

User `Pagotto morren`

2 events found View in activity

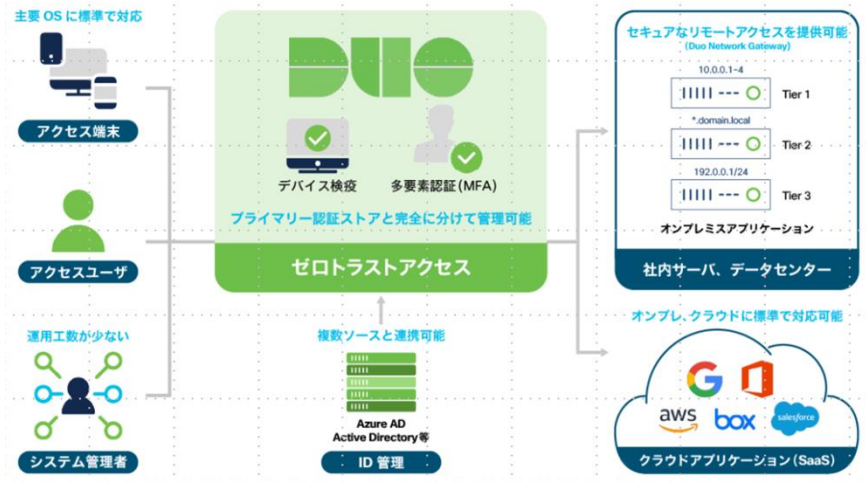
Date (UTC)	Source	Event	Result	
Sep 23, 2024 23:59:59		`user.authentication.sso`	Success	See in context
Sep 23, 2024 23:59:59		`user.authentication.sso`	Success	See in context

Identity Protection + Identity Intelligence = Cisco Duo

New

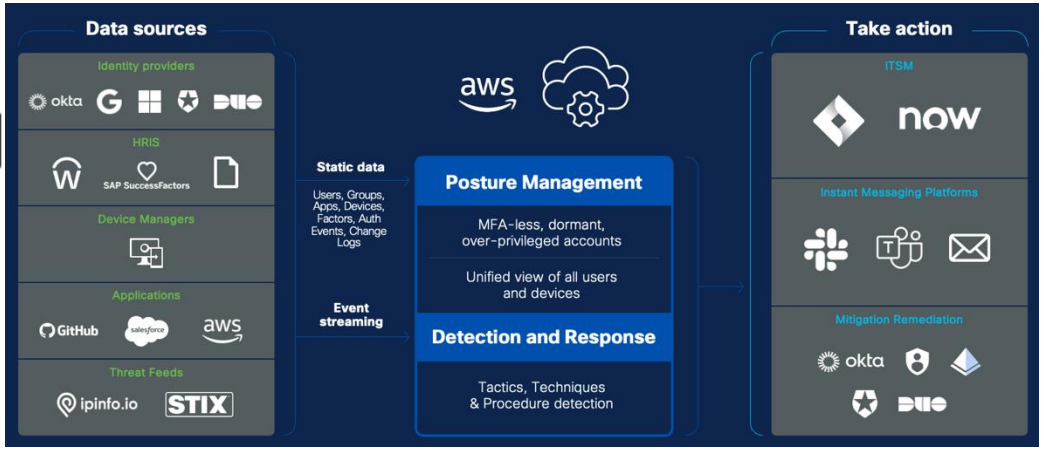
Identity Protection

全てのアプリケーションに対し、安全なアクセスとエンドユーザ及び管理者の生産性向上を提供



Identity Intelligence

全てのIdentityとアクセスを可視化し、危険なIdentityを排除して、継続的に安全なアクセスを提供



強固な認証を
管理者に簡単に、ユーザに優しく提供可能

全てのIdentityを可視化し、
管理者に簡単に、ガバナンスを強化

Cisco Duo

Cisco Identity セキュリティアセスメントのご提案

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

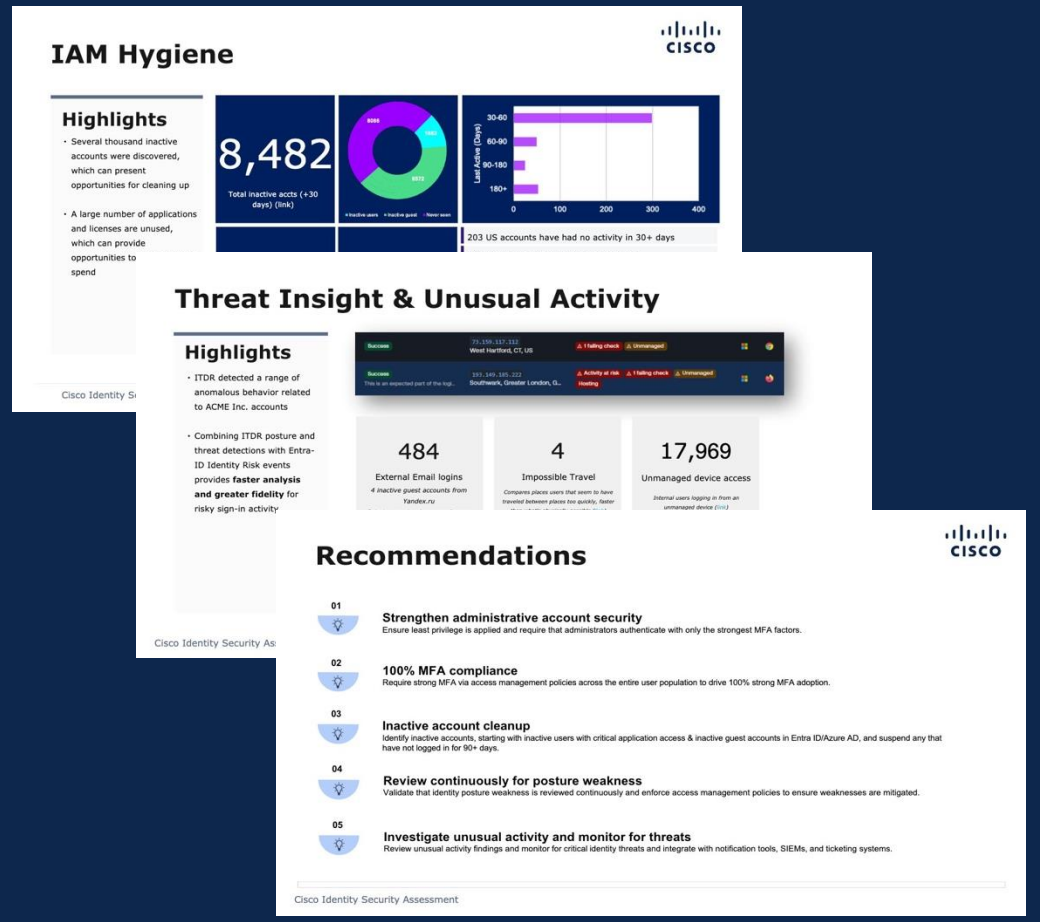
IAMポスチャ評価
MFAが設定されていない/弱い、休眠アカウント、過剰な特権ユーザなどを特定するIAMハイジーンのレビュー

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例

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

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

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

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

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

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

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

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

Users Sharing Authenticators

共有されたAuthenticotor/Phone

Posture: Low

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

ご希望のお客様はCisco担当営業までご連絡ください

Cisco Identity セキュリティアセスメントのご提案

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

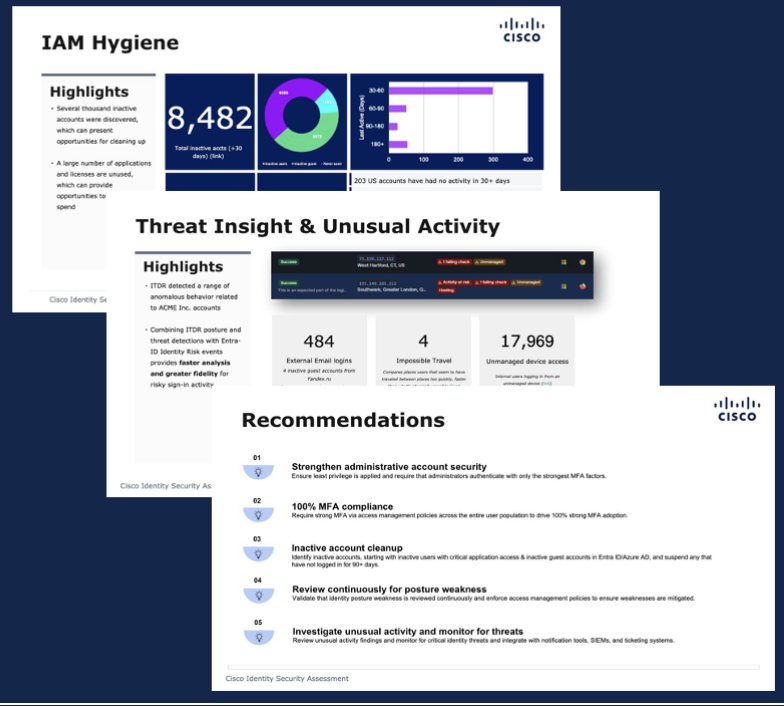
IAMポスチャ評価
MFAが設定されていない/弱い、休眠アカウント、過剰な特権ユーザなどを特定するIAMハイジーンのレビュー

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