Cisco Security

Cisco XDR最新アップデートと Cisco Identity Intelligenceとの連携

Webinar

平岡 龍弘
APJC XDR Sales Lead
Cisco Systems

2025.4.17

免責事項

本日記載の内容はロードマップや開発段階のものが多く含まれます。

ロードマップはシスコの独断で変更されることがあり、シスコは本文書に記載された製品または機能の提供の遅延または提供の不履行について一切責任を負いません。

自己紹介

平岡　龍弘　Hiraoka Tatsuhiro

APJC XDR Sales Lead
Cisco Systems

大手SIerでネットワーク/セキュリティ領域のアーキテクトとして従事した後、2022年シスコへ入社。

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

Cisco XDR Overview

XDRとは

eXtended

複数のセキュリティツールからテレメトリを
自動的に収集して関連付けを実行

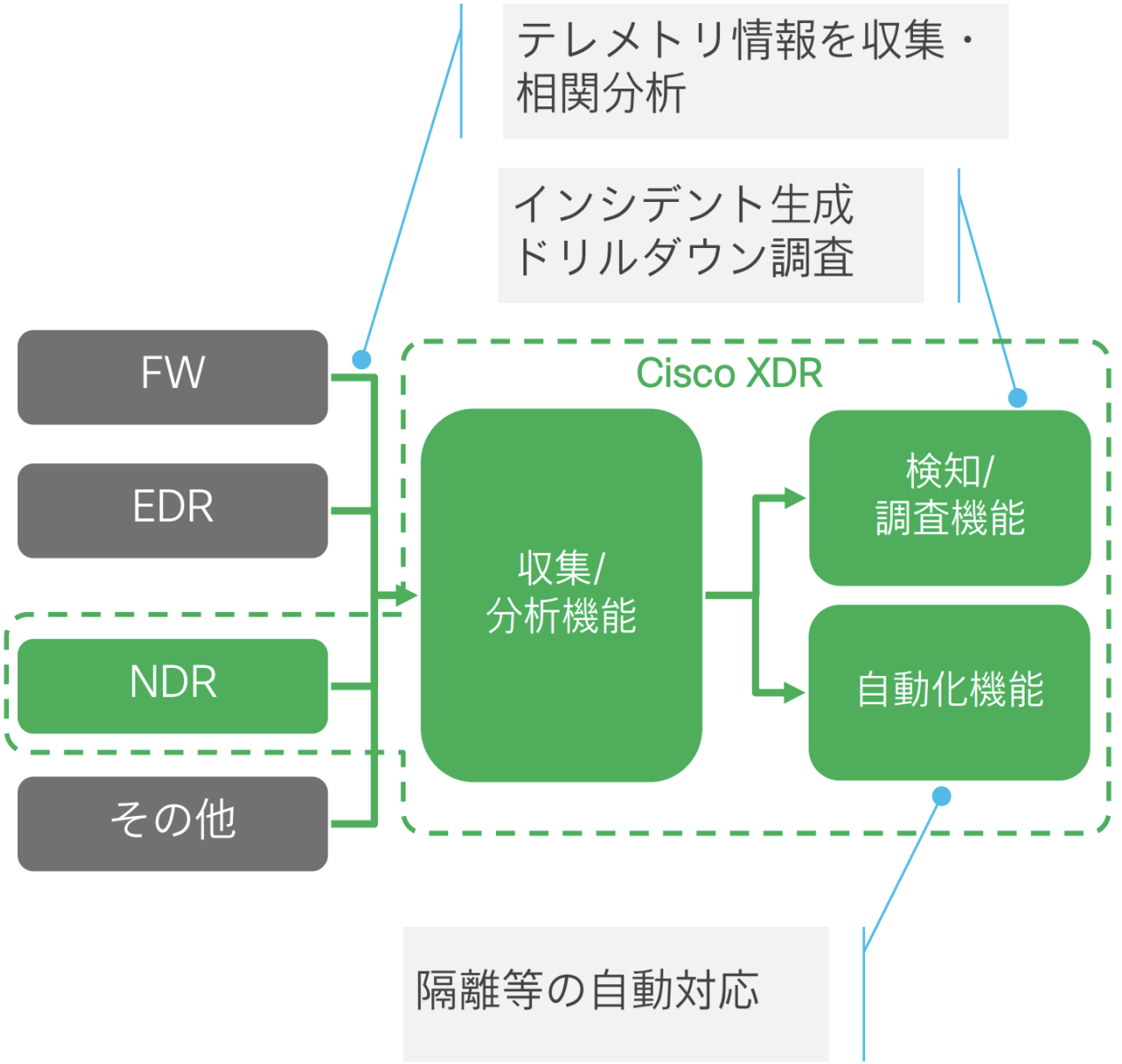
Detection

悪意のある活動を検出して分析を実行

Response

脅威への対応と修復を実行

**セキュリティ運用するうえで役に立つ
さまざまなツールのセット**



マルチレイヤのセキュリティリスクの検知対応・自動化

AWS Azure GCP
Cloud Log

Email

ネットワーク

テレメトリー情報

ユーザ・デバイス

Cisco XDR

相関関係を分析

インシデントの優先付け

対処のワークフロー

次世代セキュリティ施策に求められる2つの進化

クロスドメイン テレメトリー

AI 機械学習

チームへの通知
Webex Teams Slack

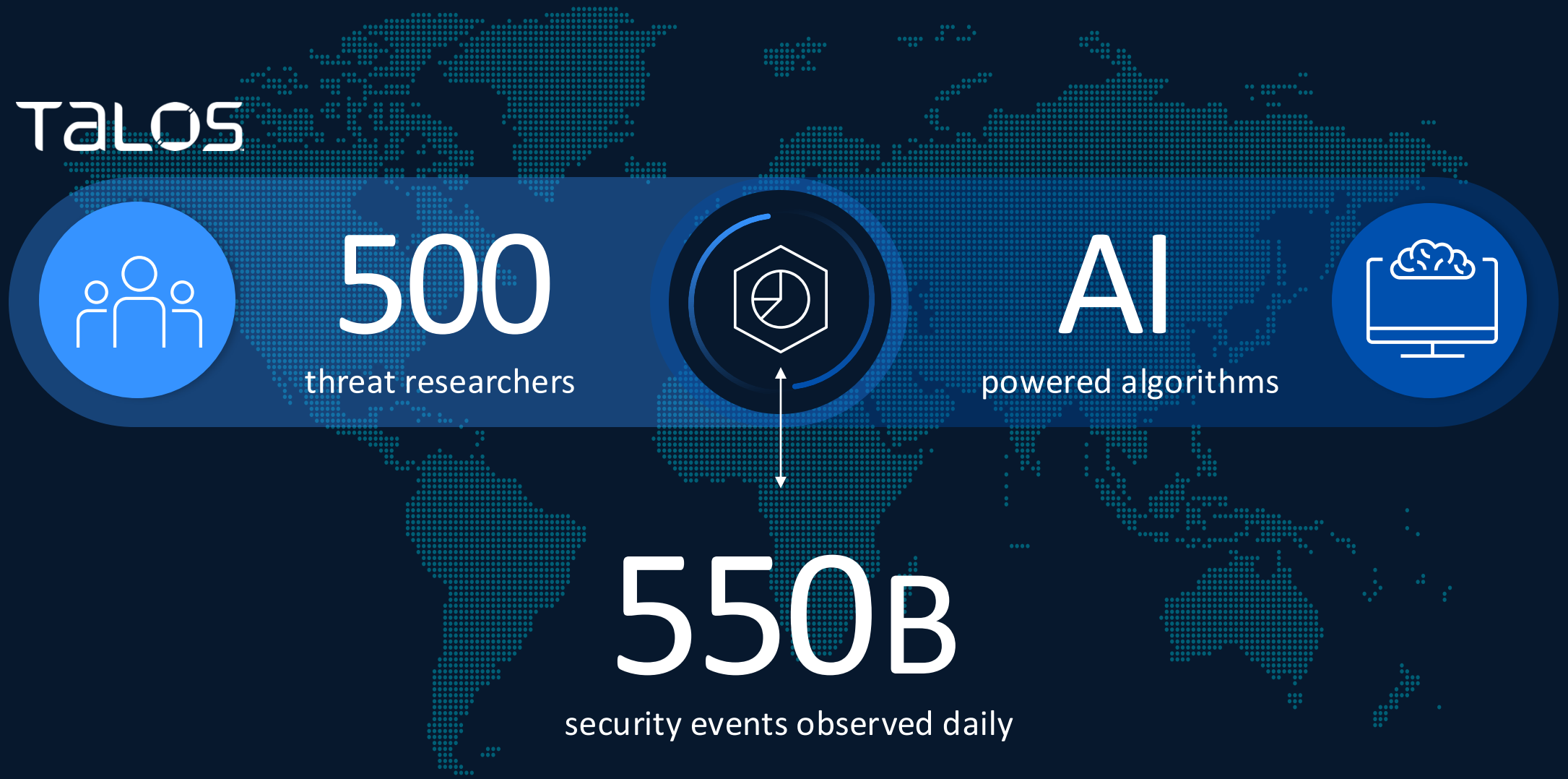
自動隔離

ネットワーク

自動隔離

ユーザ・デバイス

Talos powers the Cisco portfolio with intelligence



Cisco XDR 主要な戦略的パートナー

2025年4月現在

EDR
- CrowdStrike Falcon® Insight
- SentinelOne Singularity™
- Microsoft Defender for Endpoint
- Trend Micro Vision One
- Cybereason Endpoint Security
- Palo Alto Networks Cortex XDR

Email Threat Defense
- Proofpoint Email Protection
- Microsoft Defender for O365

Public Cloud Integrations
- AWS
- Microsoft Azure
- Google Cloud Platform

NGFW
- Check Point
- Fortinet FortiGate
- Palo Alto Networks NGFW

NDR
- Darktrace
- ExtraHop

SIEM
- Exabeam
- Google Chronicle
- LogRhythm
- Sumo Logic
- Elastic

Application and Identity
- Microsoft Azure AD
- Jamf Pro
- Vmware Workspace ONE UEM
- Microsoft Intune

Threat Intelligence and Hunting Integrations
- Recorded Future
- Virus Total
- Pulsedive
- Service Now Sec Ops
- Shodan
- IBM X-Force Exchange
- alphaMountain.ai
- Amazon GuardDuty

Data Cloud
- Cohesity
- Rubrik

2025年4月現在

Cisco製品のインテグレーション

User Endpoint
- Secure Endpoint
- Secure Client
- Email Threat Defence
- Cisco Orbital

Application and Identity
- Duo (Cisco Identity Intelligence)

Cloud
- Umbrella
- Secure Access
- Secure Workload
- Attack Surface Management

Network
- Secure Network Analytics
- Secure Firewall
- Meraki
- ISE
- Defense Orchestrator

VM
- Cisco Vulnerability Management

SIEM
- Splunk

Cisco XDR Updates

ついにSecure Accessの相関分析がスタート。完全な連携が可能に

表：投影限り

XDR主要機能

Detection & Correlation

テレメトリデータを関連づけ
インシデントとして抽出

Threat Hunting & Investigation

脅威の探索、クエリを実行して
脅威への可視性を強化

Asset Insights & Context

組織全体のユーザとデバイスを把握

Automation & Response

インシデントを迅速に封じ込め、
根絶するためのアクションを提供

5/1からCisco Identity Intelligenceの一部機能をCisco XDRユーザーに付与

Identity Intelligence now included within your Cisco XDR entitlement

Dear Cisco XDR Cyber Defender,

Cisco continues to enhance our XDR offering with capabilities that security operations teams need to defend their organizations. With the continued evolution of the Cisco Security Platform, Cisco XDR customers are now entitled to comprehensive identity user and security context from our Identity Intelligence service. This rich and critical context expands Asset Insights and incident correlation in Cisco XDR.

Cisco is enabling this functionality in waves for Cisco XDR customers beginning 31 March 2025.

Coming Soon: Stay tuned for an advisement on when your Cisco XDR tenant will be enabled with Identity Intelligence context.

Sincerely,
The Cisco XDR Team

まずはAsset InsightsとAutomationからスタート

XDR主要機能

Detection & Correlation

テレメトリデータを関連づけ
インシデントとして抽出

Threat Hunting & Investigation

脅威の探索、クエリを実行して
脅威への可視性を強化

Asset Insights & Context

組織全体のユーザとデバイスを把握

Automation & Response

インシデントを迅速に封じ込め、
根絶するためのアクションを提供

従来のCisco XDRとの連携

Secure Access

ZTNA | SWG | DLP

FWaaS | CASB | Browser Isolation

Integration

Cisco Identity Intelligence

ISPM
（アイデンティティポスチャ管理）

ITDR
（アイデンティティ脅威検知対処）

Integration

Cisco XDR

Detection
(相関分析・優先付け)

Response
(隔離/通知・自動化)

これからのCisco XDR連携

Secure Access

ZTNA | SWG | DLP

FWaaS | CASB | Browser Isolation

Integration

Cisco XDR

Detection
(相関分析・優先付け)

Response
(隔離/通知・自動化)

Cisco Identity Intelligence

ISPM
（アイデンティティポスチャ管理）

ITDR
（アイデンティティ脅威検知対処）

XDRの中に一部CIIの機能が内包*

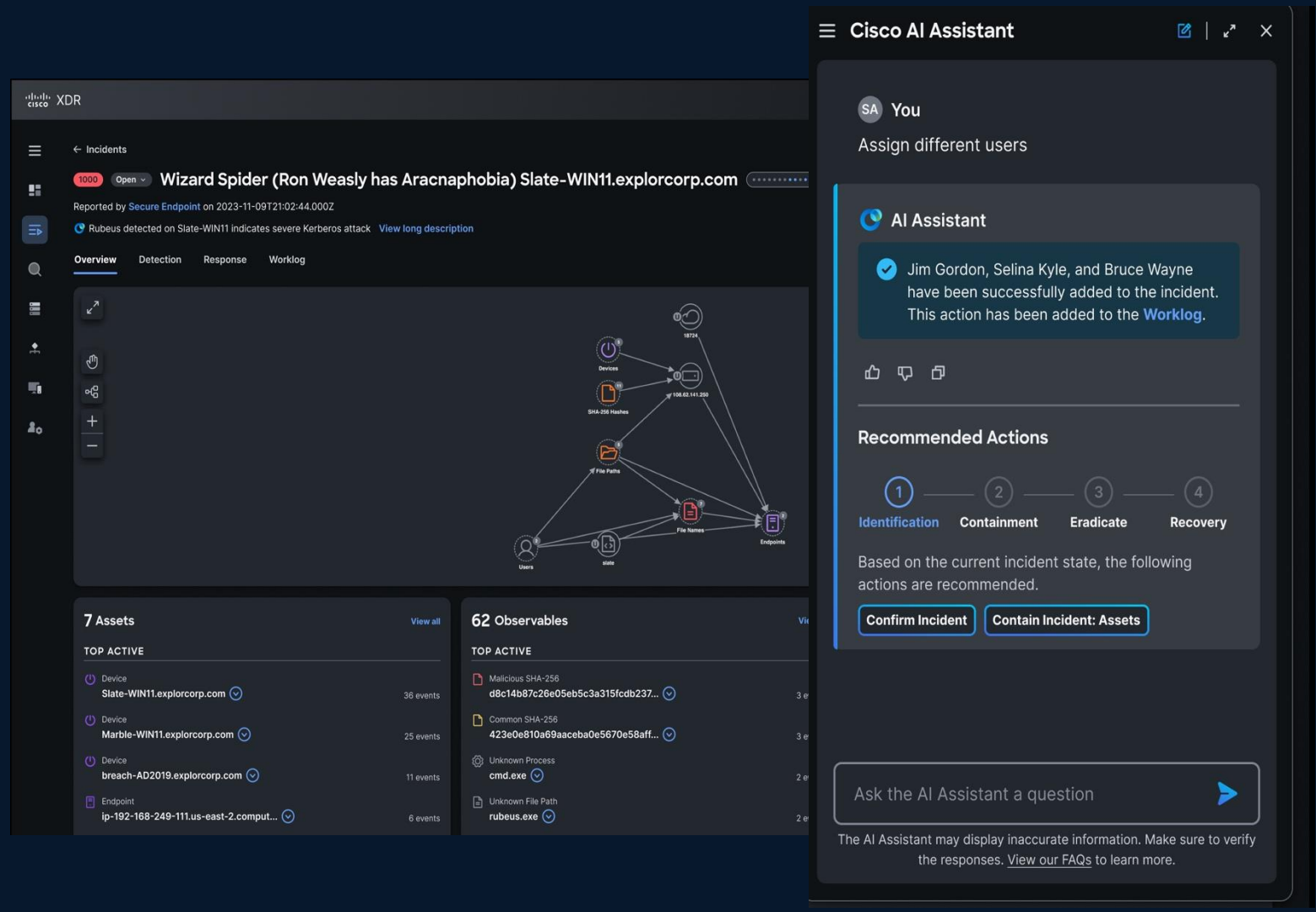
*詳細は後日アナウンス

Cisco AI Assistant for Cisco XDR

2025年リリース予定

あらゆるレベルのSOCアナリストにとって、より良い情報に基づいた意思決定を迅速に行えるように支援

- コンテキストに基づいた洞察
- レスポンスのガイド
- 最適な次のステップ
- 自動化されたワークフロー



Cisco Identity Intelligence Integration

Why hack in…

…when you can login?

ランサムウェア攻撃のシナリオ

初期侵入	権限昇格	横展開 (ラテラルムーブメント)	侵害

フィッシングメール
VPN脆弱性

Password Spraying Attack

権限昇格
永続性を確立するためのプログラムをインストール

侵害端末からアクセス可能なネットワーク内の端末を探索

Active Directoryからドメイン管理者権限を奪取してアクセス権確保

RDP Brute Force Attack

グループポリシーを操作してセキュリティ対策を無効化

共有フォルダや重要度の高いPCやシステムを探索

グループポリシーを操作してネットワーク内にランサムウェアを配布

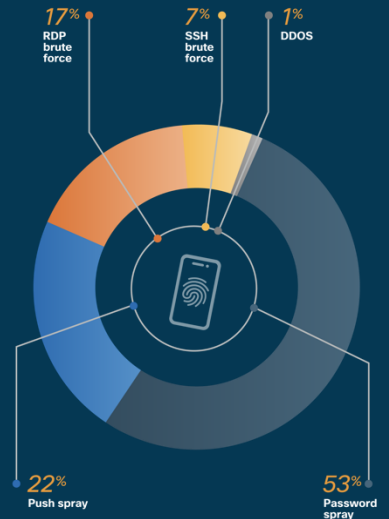
共有ファイルサーバから機密情報を搾取

情報漏えい
脅迫

～Talos Year in Review 2024～

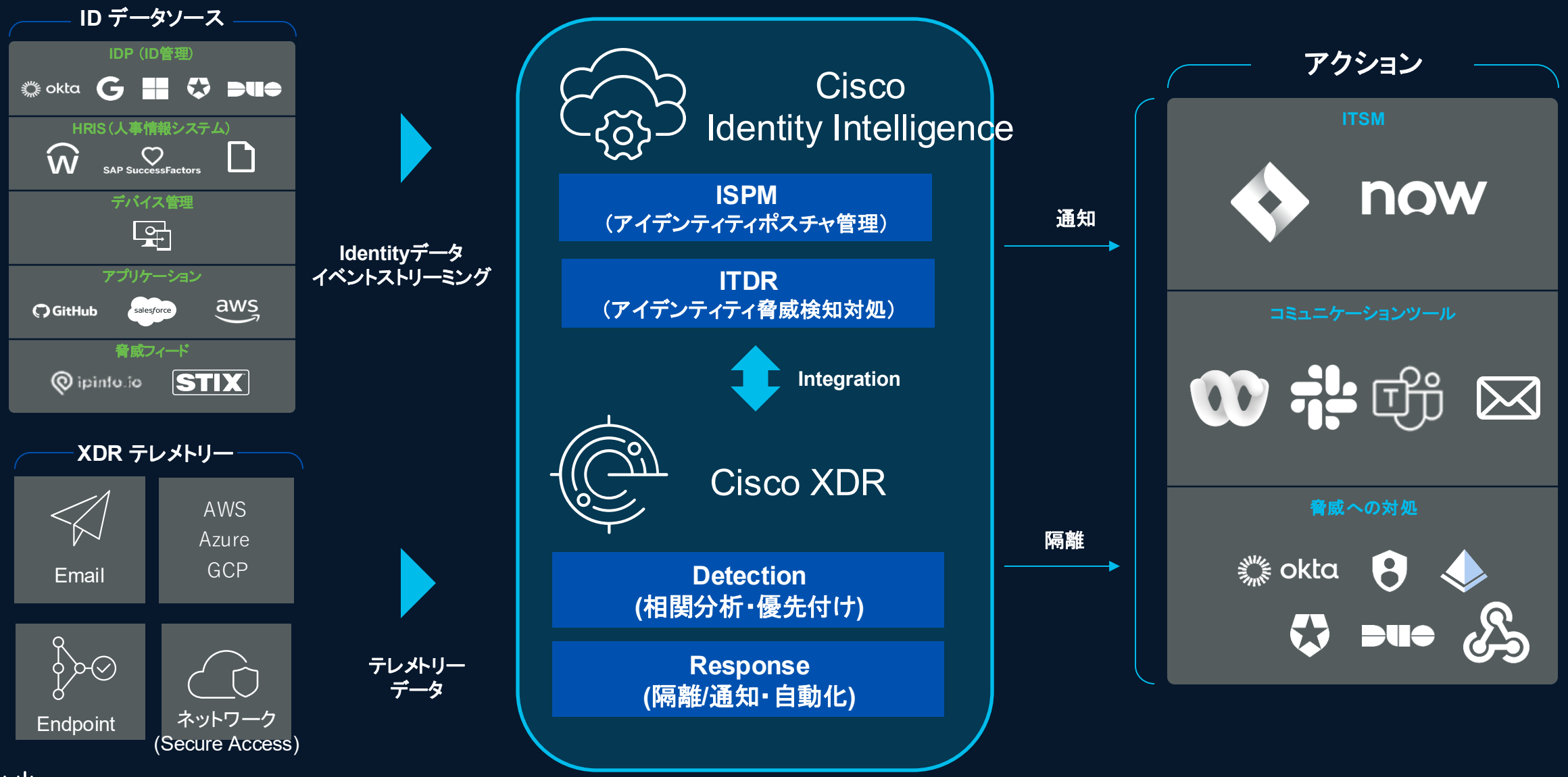
攻撃者はMFAがない組織やMFAが正しく設定されていない組織を探る。

既知の脆弱性や設定ミスを悪用してアクセスを試みる。



Cisco XDRでEnd to Endの脅威を検出

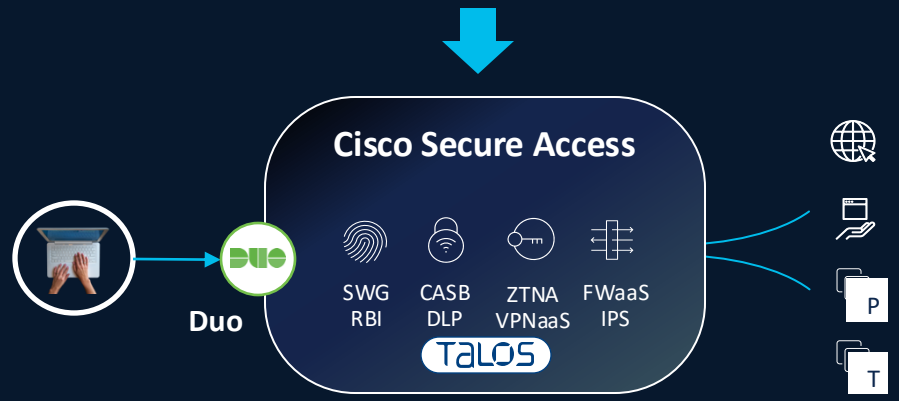
全体像：Cisco XDR w/ Cisco Identity Intelligence



Why Cisco XDR w/ Cisco Identity Intelligence

Cisco Identity Intelligence

- アイデンティティの可視化
- 強固な認証の展開
- ガバナンス強化



ゼロトラストに基づく継続的かつ安全なアクセスを実現

脅威検知

Cisco XDR

- 脅威の相関分析・優先付け
- TalosインテリジェンスのFeed
- オートメーションによる自動応答

脅威の相関分析とリスクの高いユーザー/端末の自動隔離やアクセス制御

Why Cisco XDR w/ Cisco Identity Intelligence

Identity Intelligence

アイデンティティの可視化

強固な認証の展開

ガバナンスの強化

×

Cisco XDR

相関分析
優先付け

Talos Intelligence

Automation

安全なゼロトラストの実現

インシデント対応

自動防御

可視化

本日のデモシナリオ

Identity Intelligence

アイデンティティの可視化

強固な認証の展開

ガバナンスの強化

×

Cisco XDR

相関分析 優先付け

Talos Intelligence

Automation

安全なゼロトラストの実現

インシデント対応

自動防御

可視化

本日のデモシナリオ

Cisco Identity Intelligence

- アイデンティティの可視化
- 強固な認証の展開
- ガバナンス強化

✓ Identity のアタック検知
✓ リスクに対する迅速な対応

連携

Cisco XDR

- 脅威のリアルタイム検知
- TalosインテリジェンスのFeed
- オートメーションによる自動応答

リスクの高いユーザーのMS365アカウントを自動隔離して通知

Demo


CISCO