Cisco XDR で
セキュリティ運用を簡素化

平岡 龍弘
Cisco Security、APJC XDR Sales Lead

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。

*AI 生成によるビデオ

Phrogger/フロッガー

Phrogger/フロッガー

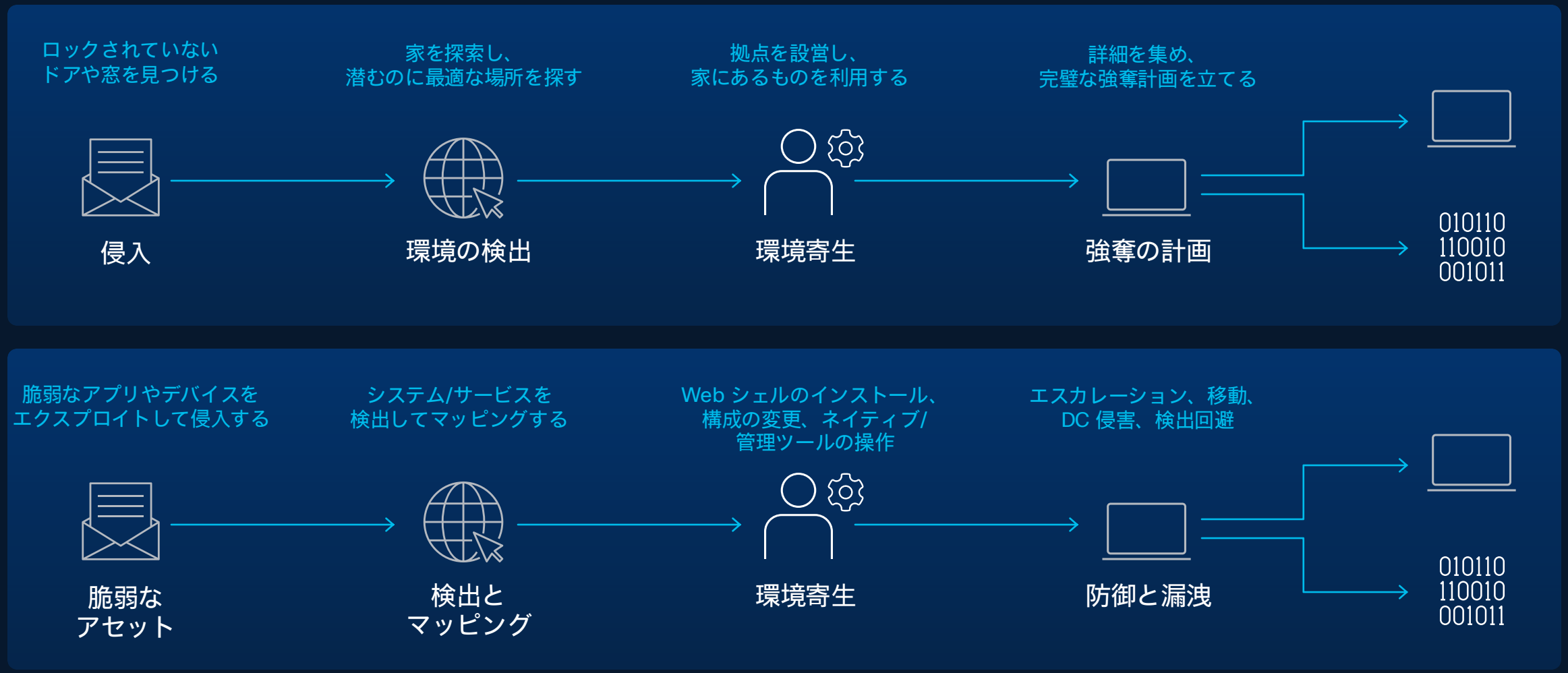
他人の家に忍び込んで家主に気づかれず生活を続ける犯罪

デジタル空間に潜むフロッガー

昨今の攻撃者の特徴

特徴	内容
“Living off the land”（既存ツール利用）	通常、未知のマルウェアを導入する代わりに、標的システムに元から備わっている正規ツール（PowerShell、WMIC、net shll、NTDSUtil など）を悪用することが多い。これにより、検知回避を図る。
ステルス性と持続性の追求	標準的なログ生成や異常検知を回避するように振る舞う。また、ルーター、VPN機器、ファイアウォールなどのネットワーク機器を中継点に使い、トラフィックの出どころを隠すことも確認されている。
横移動・認証情報取得	一度内部に侵入すると、ネットワーク内で他の端末やサーバーに展開しつつ、正規のアカウントや認証情報を収集・利用して拡張。
事前配置 (“pre-positioning”)	将来的な紛争や軍事的緊張時に備え、あらかじめ重要ネットワークに“根を張る”ような配置を行っておくという戦略的な動きがある。

Volt Typhoon のような APT が「デジタル空間」に存在



攻撃の阻止が難しい理由

正規の方法でログイン

ツールの乱立、アラート疲れ

明確さの欠如

攻撃を阻止するために必要なもの

可視性の向上

明確な判断

迅速なアクション

セキュリティは重要ではあるが、仕事の一部でしかない

インフラストラクチャ

IT

セキュリティ

Cisco XDR

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

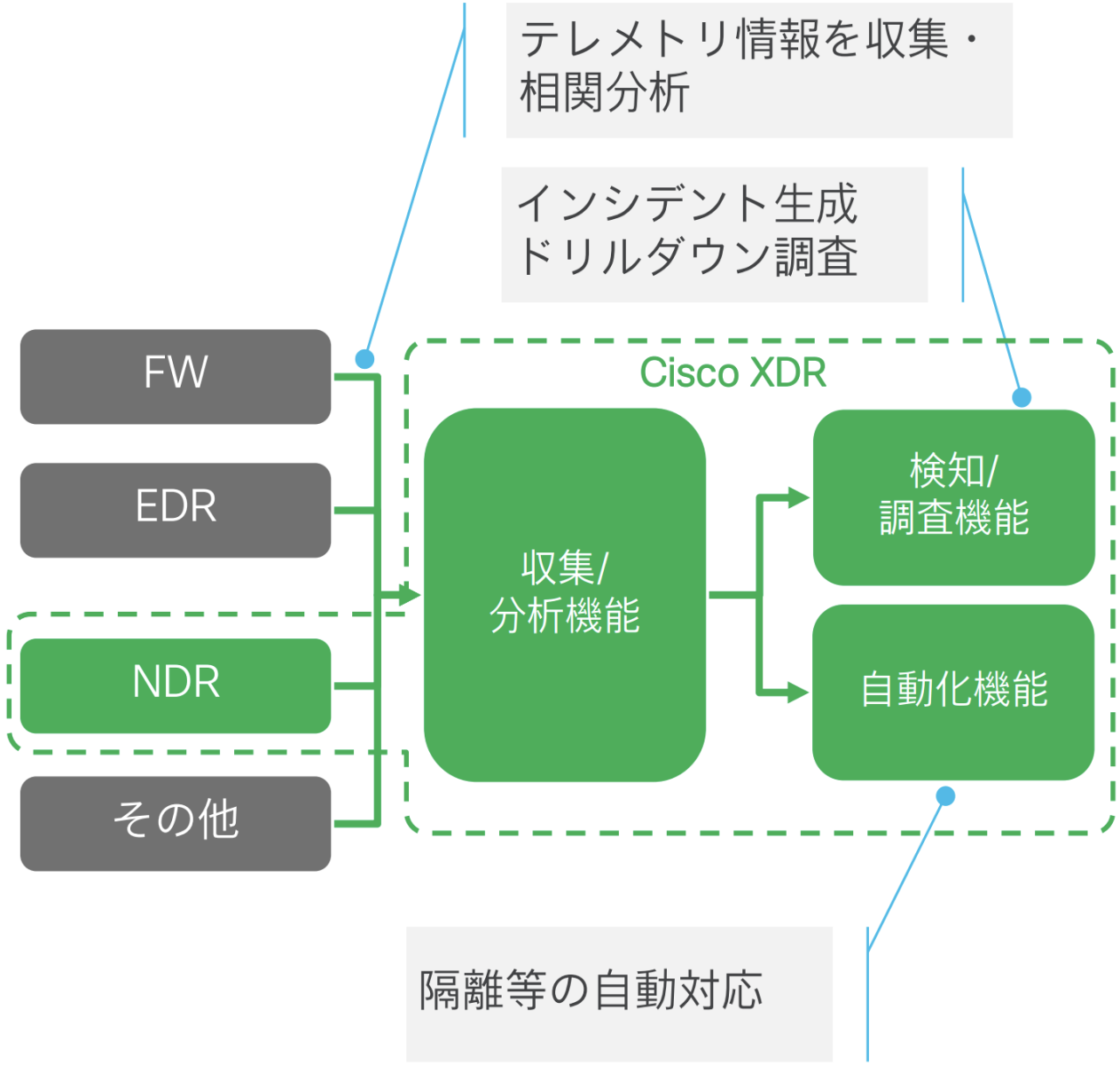
Detection

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**



Cisco XDRによる成果

Easy to Use

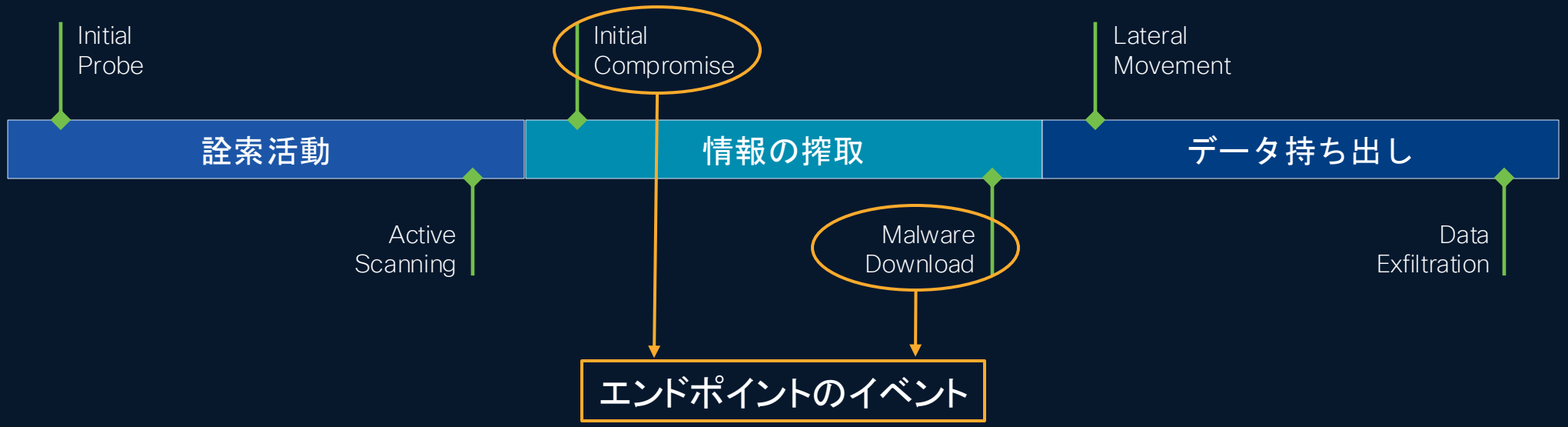
いかに簡単に早く脅威を検知してアクションできるか

中小規模の組織に最適化

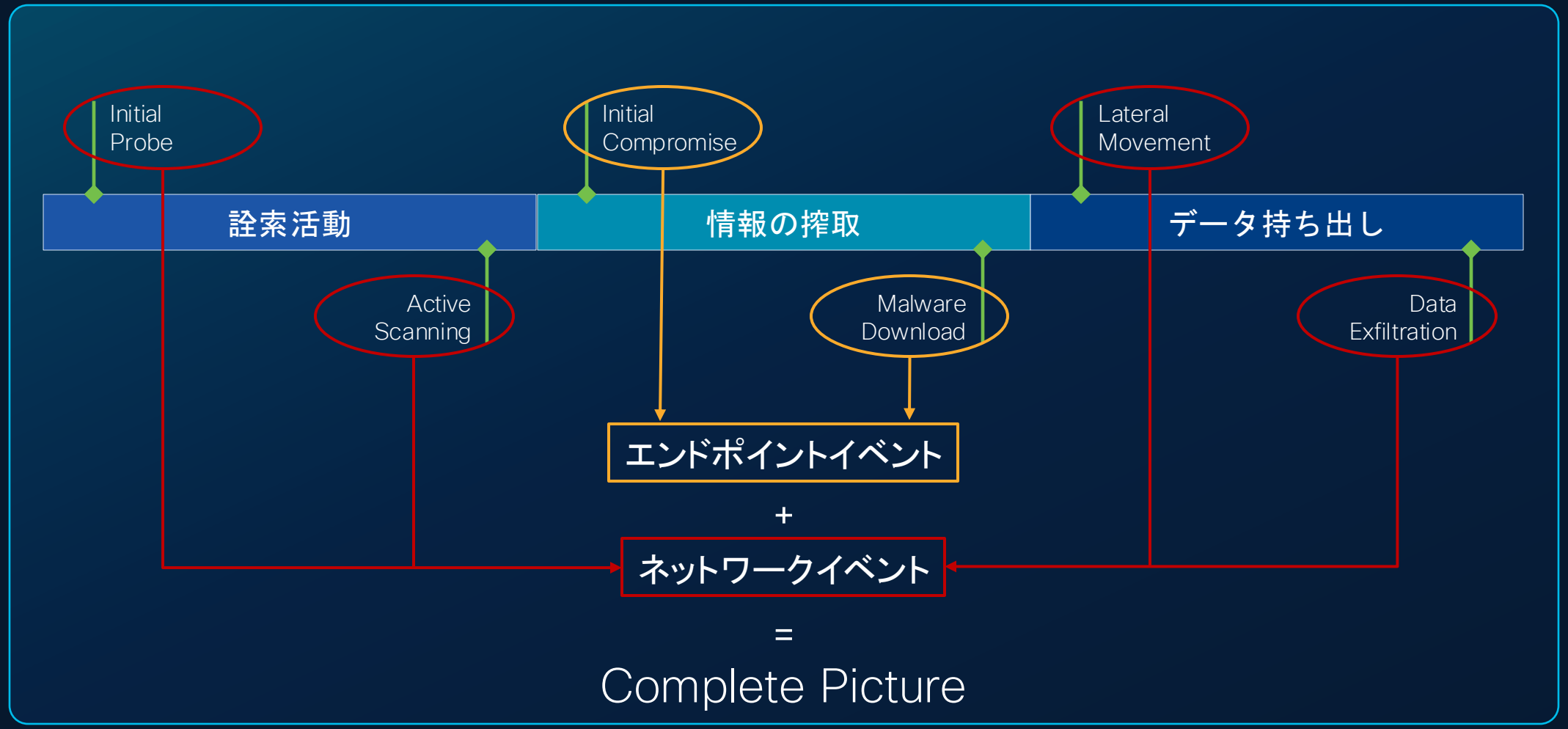
成果を迅速に提供

ネットワークと深く統合

エンドポイントのテレメトリーだけでは不十分



完全な可視化のためには、ネットワークが必要



セキュリティ検知対応・自動化のプラットフォーム

AWS Azure GCP
Cloud Log

Email

ネットワーク

ユーザ・デバイス

Cisco XDR

相関
分析

インシデント
優先付け

ワーク
フロー

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

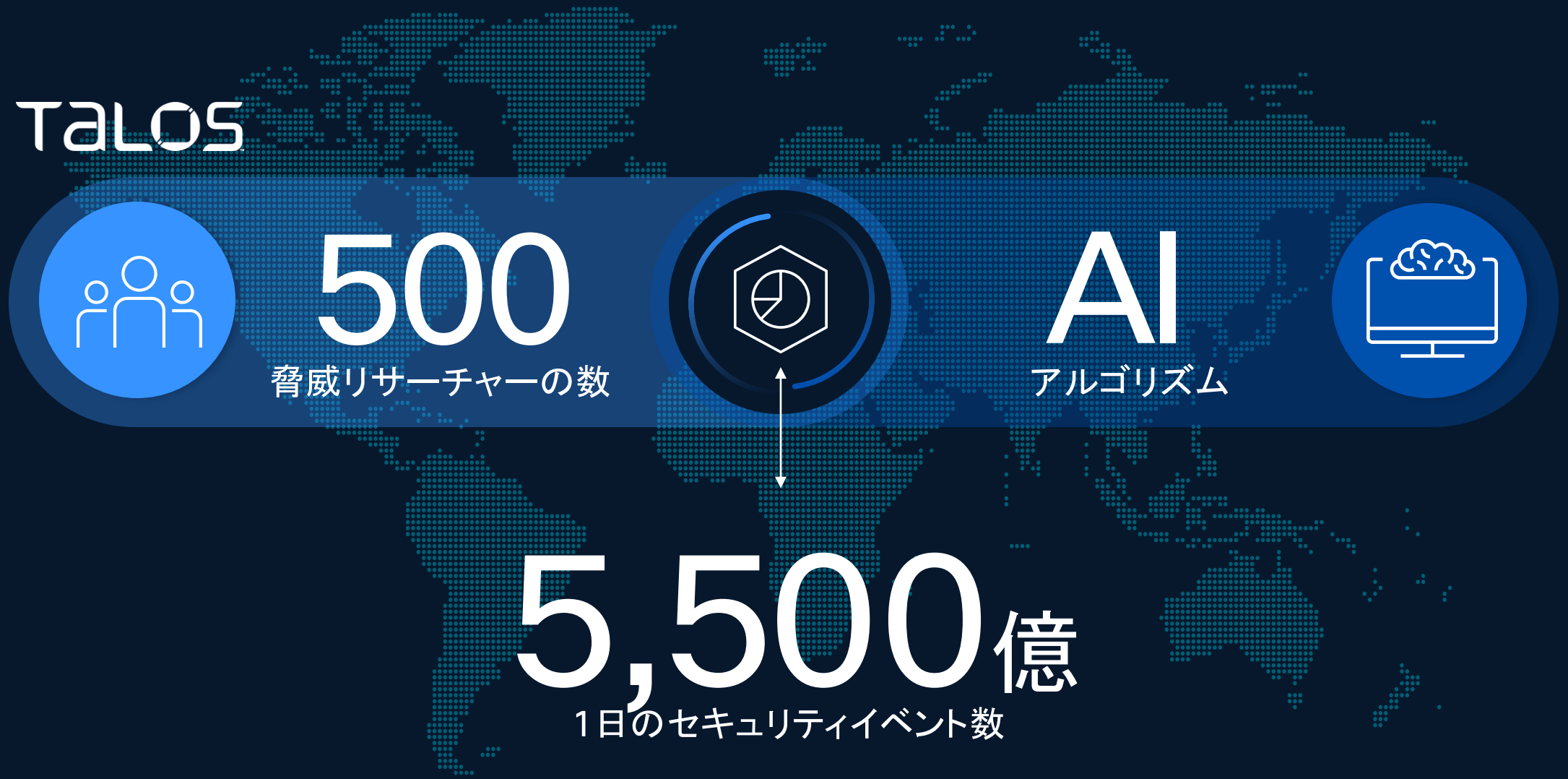
自動隔離

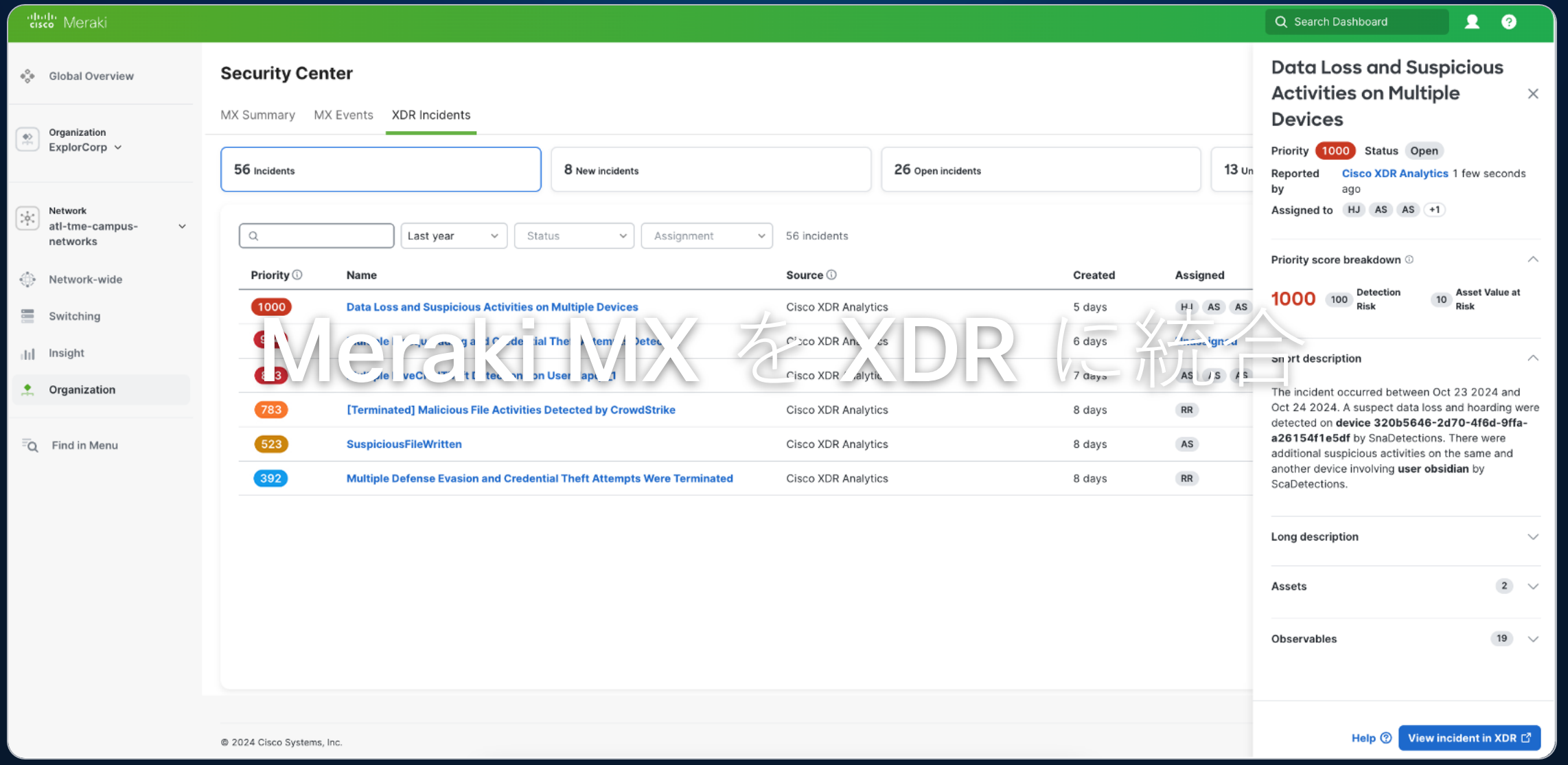
ネットワーク

自動隔離

ユーザ・デバイス

TalosのインテリジェンスでCisco XDRを強化



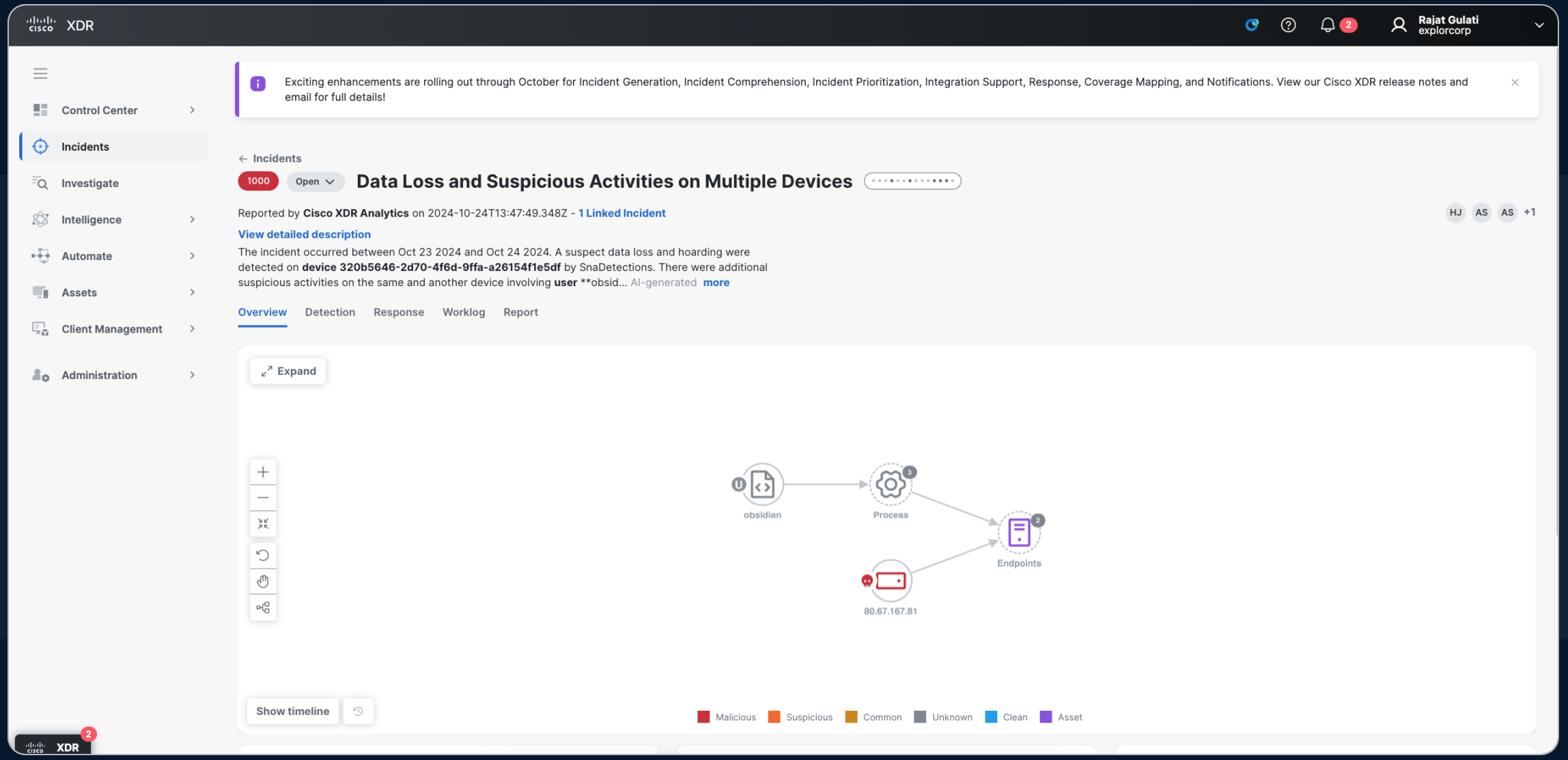


Meraki MX を XDR に統合

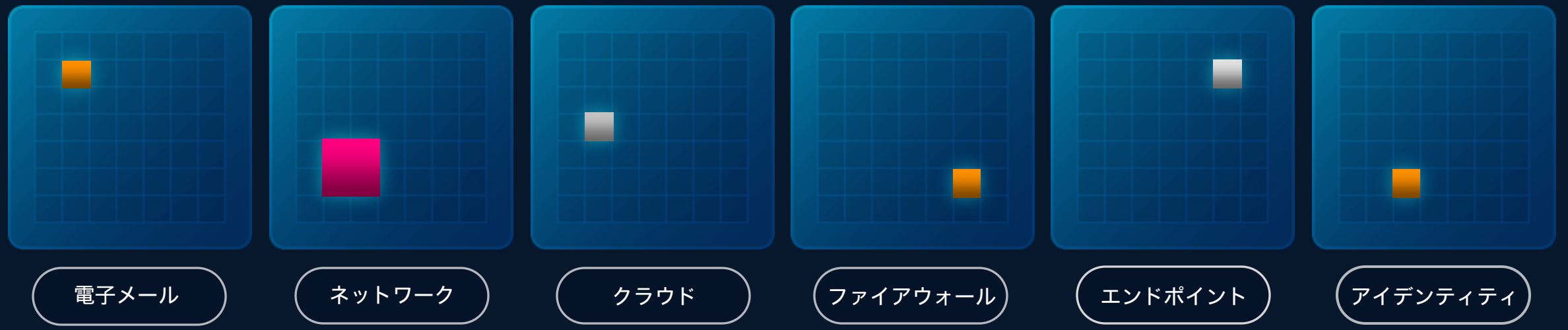
すべての Meraki MX がセンサーになる

60 秒以内

NetFlow データの価値を解き放つ



Cisco XDR



自社のペースで拡張

Cisco XDR

1つのコンソールで相関分析

Cisco XDR Update

Cisco XDR 2.0の進化

	成熟度：Low / Mid	成熟度：Mid / High
Cisco XDR	**Easy to Use** いかに簡単に早く脅威を検知してアクションできるか	-
Cisco XDR 2.0	**Confidence** 明確なアラートの判断基準 誤検知の抑止	**Forensic** エンドポイントの侵害根拠を350種類以上収集

4つの新機能をアナウンス

Instant Attack Verification

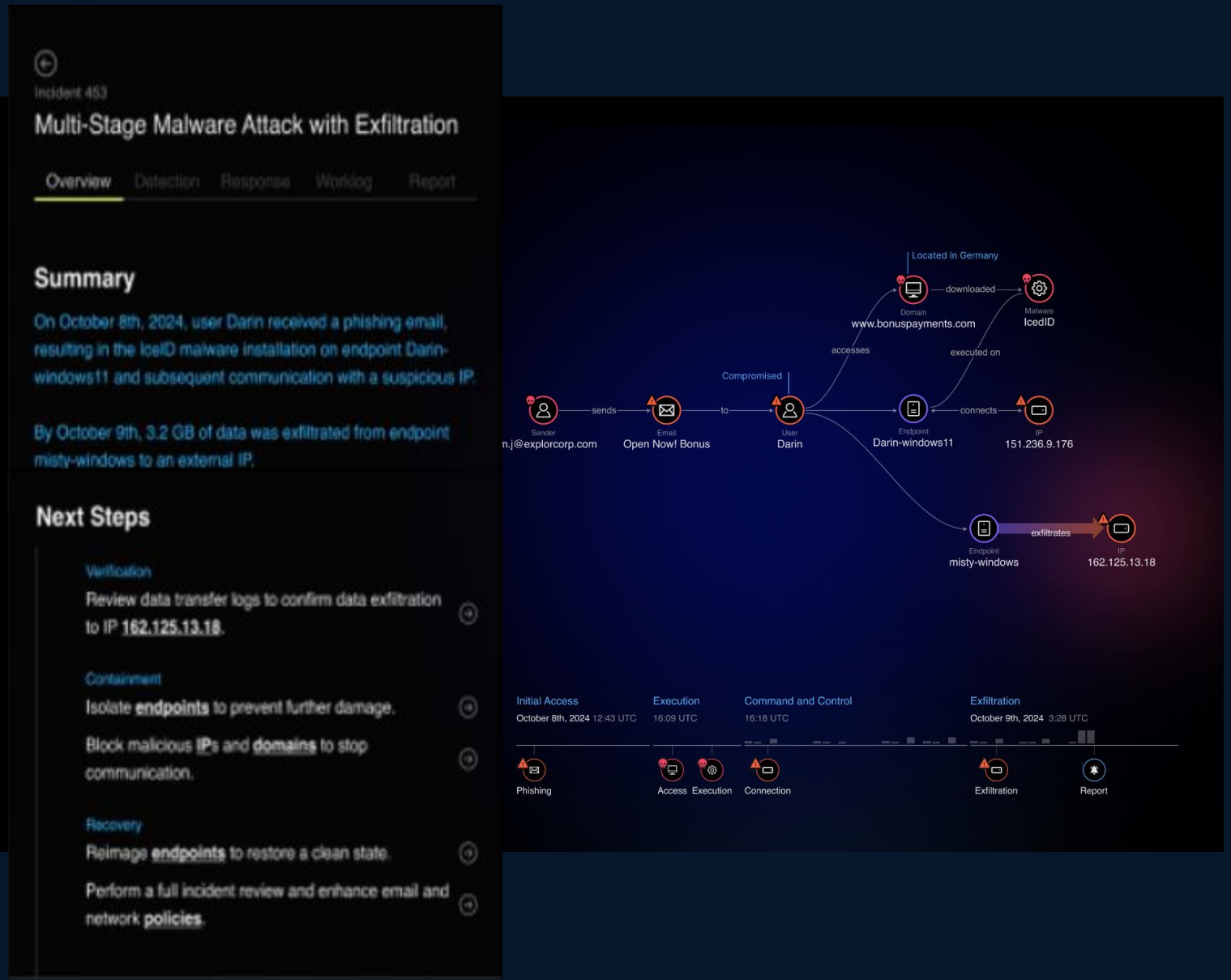
Attack Storyboard

Automated Forensics

OCSF Format

Instant Attack Verification

2025.冬 リリース



Agentic AIによるインシデントの自律的評価機能。

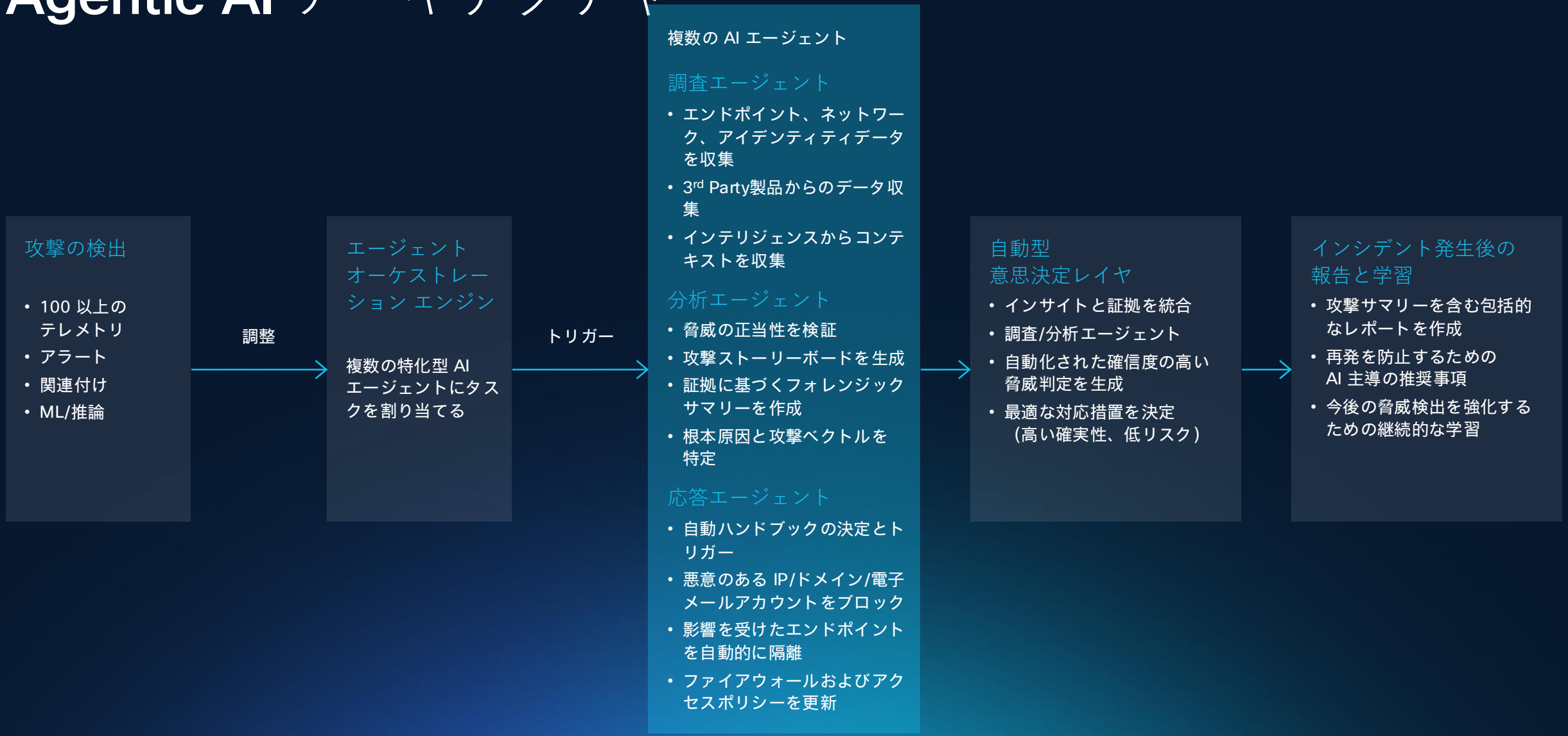
アラートの信頼度を定量的に判断し、真の脅威 or 誤検知を自動判定。

具体的な影響、調査プランの立案、**推奨アクション**を提示。

AI AssistntとAgentic AIの定義

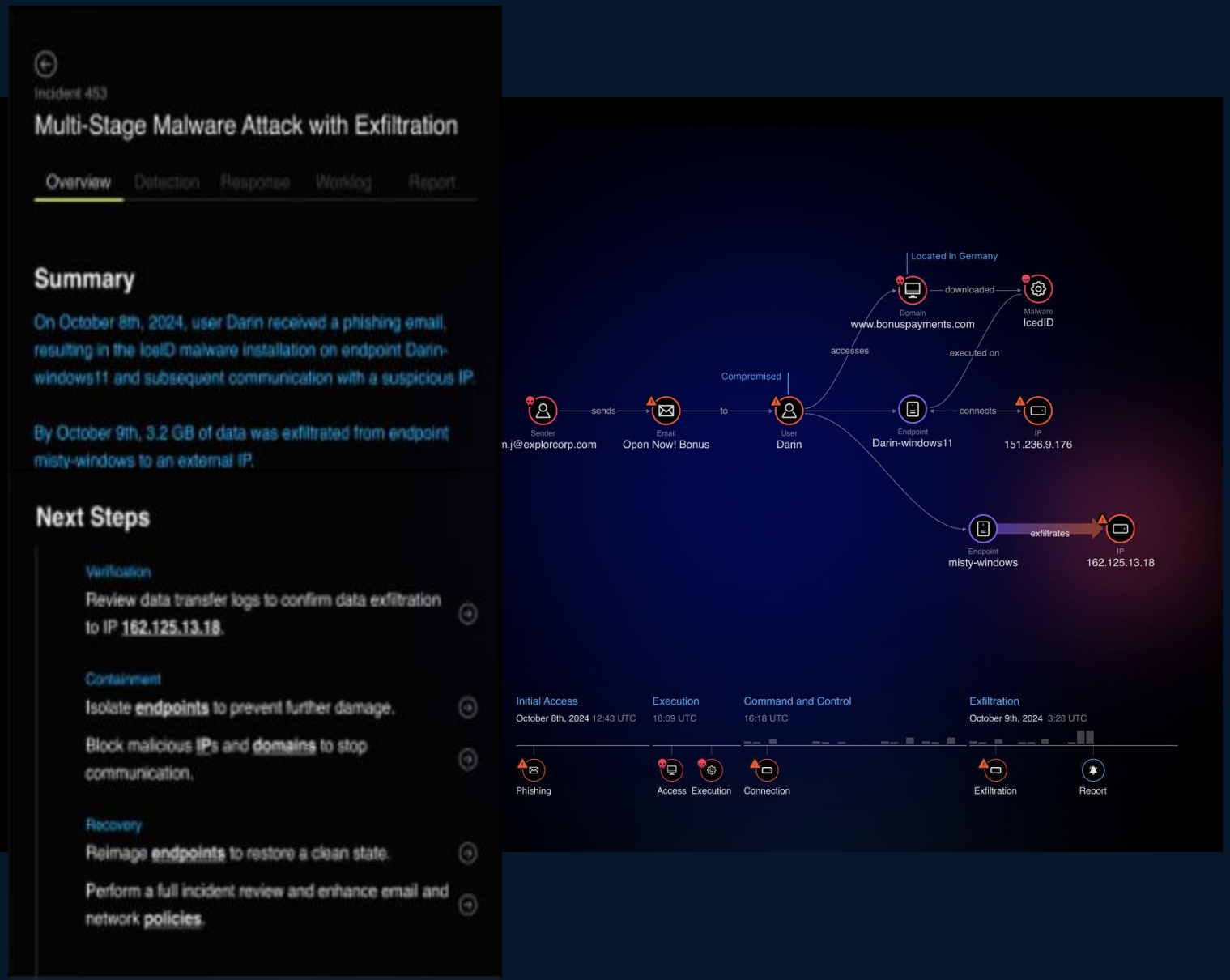
	AI Assistant	Agentic AI
主体	人間	AI
動作モデル	指示待ち型（受動的）	自律実行型（能動的）
役割	作業の補助・サポート	業務プロセスの自動化
得意なこと	単発のタスク処理、情報検索	複数のタスク処理・複雑な業務
関係性	優秀な「パートナー」	自律的に働く「パートナー」

Agentic AI アーキテクチャ



Attack Storyboard

2025.冬 リリース



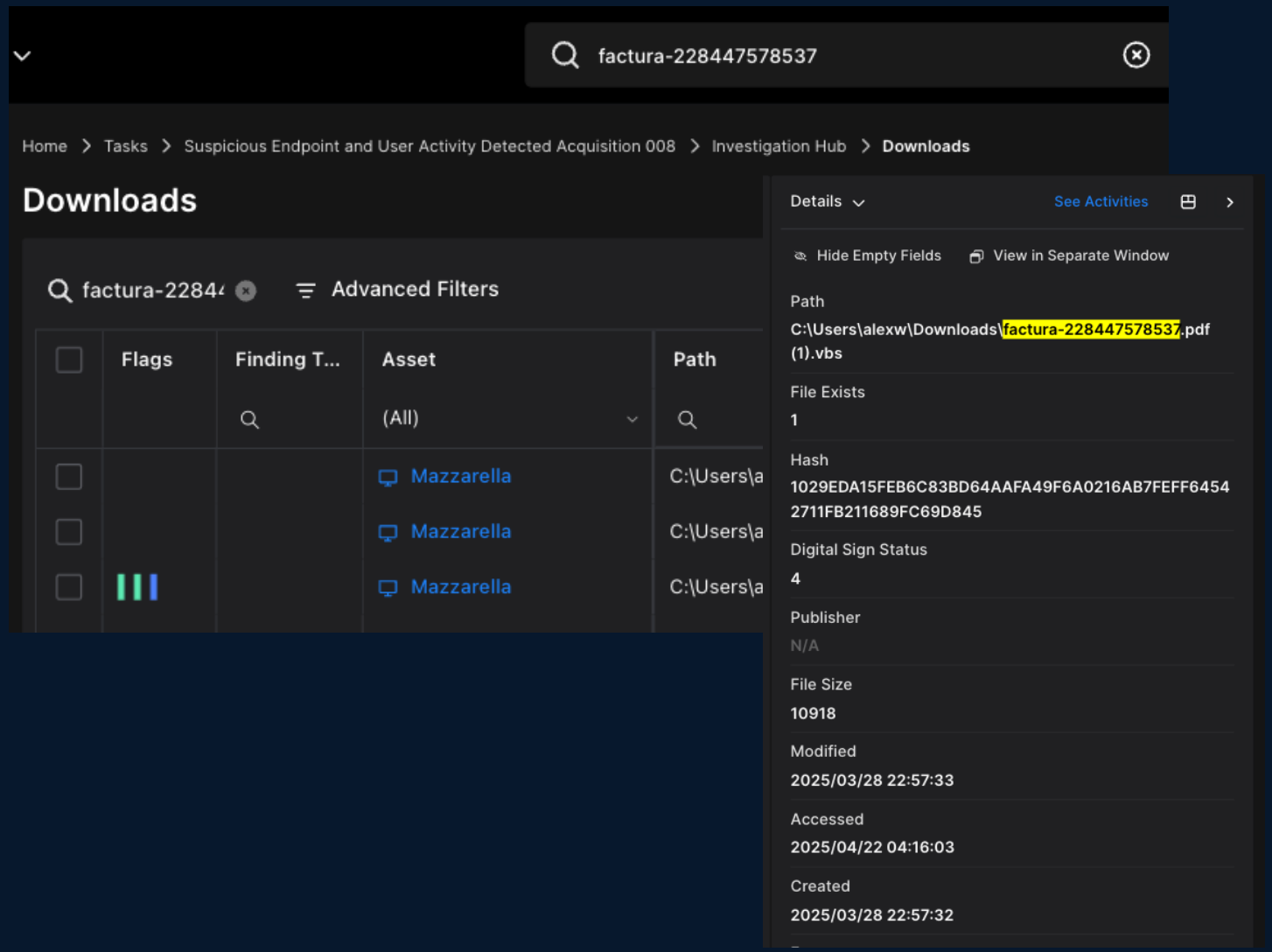
攻撃の全体像を30秒以内に把握できる可視化機能。

Agentic AIが得た情報をもとに、攻撃のタイムラインや経路をMITRE ATT&CKに沿ってグラフィカルに表示。

各ステップには簡易な説明を付加し、専門知識がなくても「何が起きたか」を直感的に理解でき、迅速な原因分析と対応判断が可能。

Automated Forensics

2025.冬 リリース



SOCアナリスト向けの自動フォレンジック機能。

インシデント検知時に350種類以上のエンドポイントデータを即座に収集して時系列で提示。

専門スキルや手間をかけずにマルウェア感染時の原因特定と被害範囲の把握が可能となり、迅速かつ高品質な対応を実現。

OCSFサポート

リリース済み

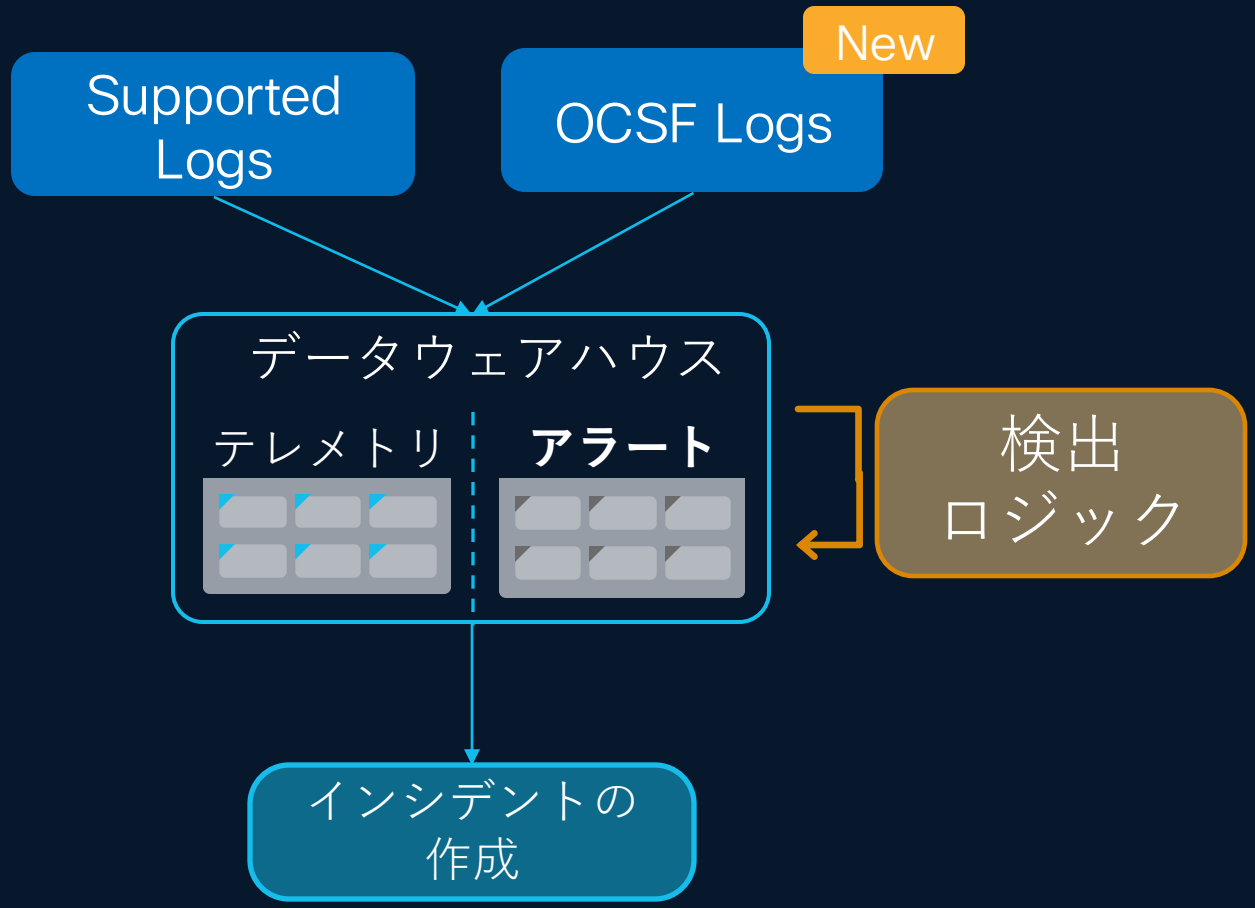
OCSFとは

複数のIT企業によって創設されログの統合プロジェクト。

ログの共通スキーマ（フォーマット）を提供して異なるツール間でのデータ連携や分析を容易にする。

Full List of contributors

Cisco XDRの検出ロジック



Zero Trust with Cisco XDR

Secure Access ・Duo連携

Released

Secure Access

ZTNA | SWG | DLP

FWaaS | CASB | Browserl solation

Integration

Cisco XDR

Detection
(相関分析・優先付け)

Response
(隔離/通知・自動化)

Duo
Cisco Identity Intelligence

ISPM
(ポスチャ管理)

ITDR
(脅威検知対処)

Asset Insight
(ユーザー情報の可視化)

Cisco XDRに直接
アイデンティティ情報を取り込み

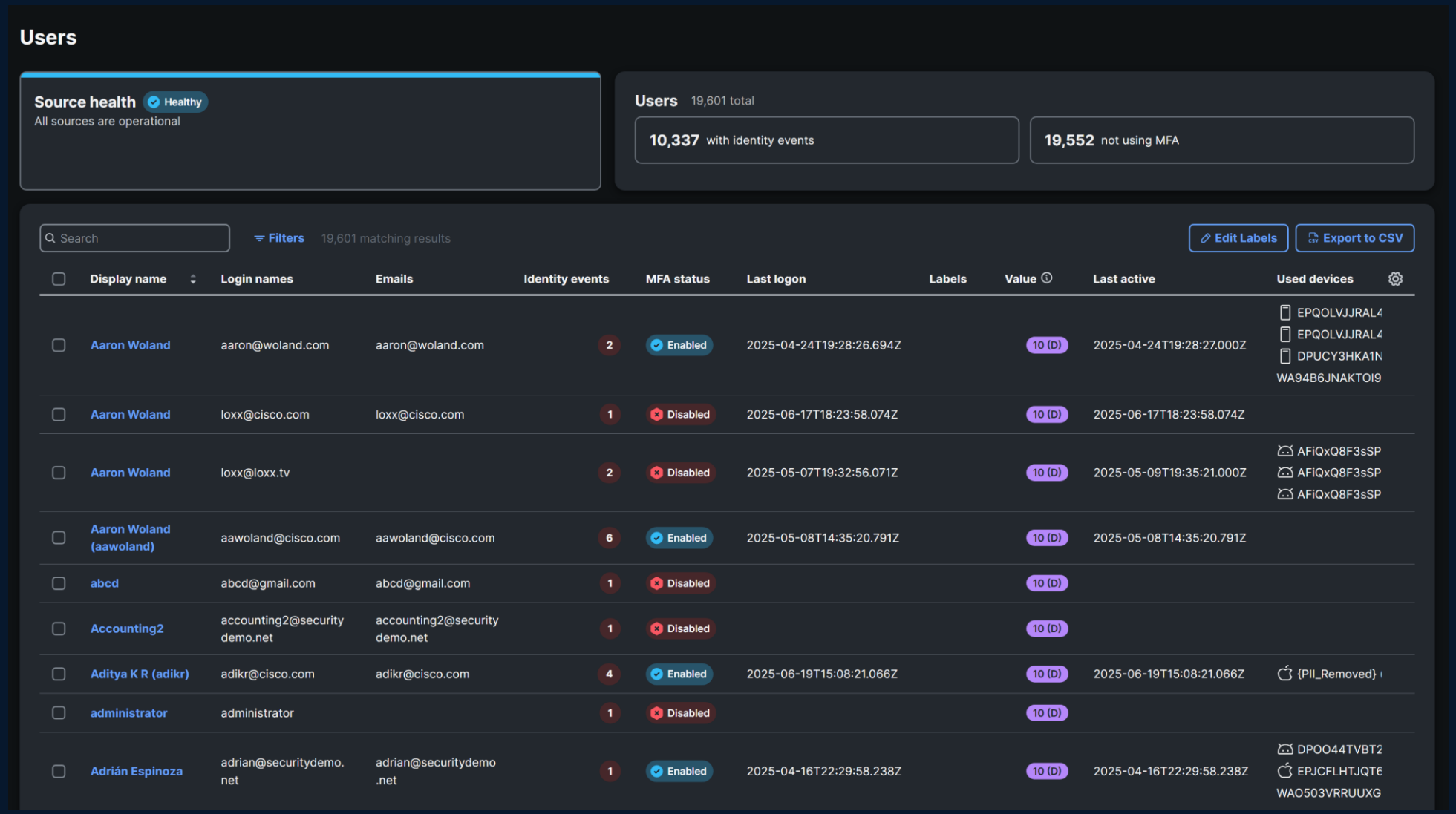
ゼロトラストの脅威を包括管理

Released

ゼロトラストの脅威を包括管理

Released

Duo連携の成果



Users

Source health Healthy
All sources are operational

Users 19,601 total

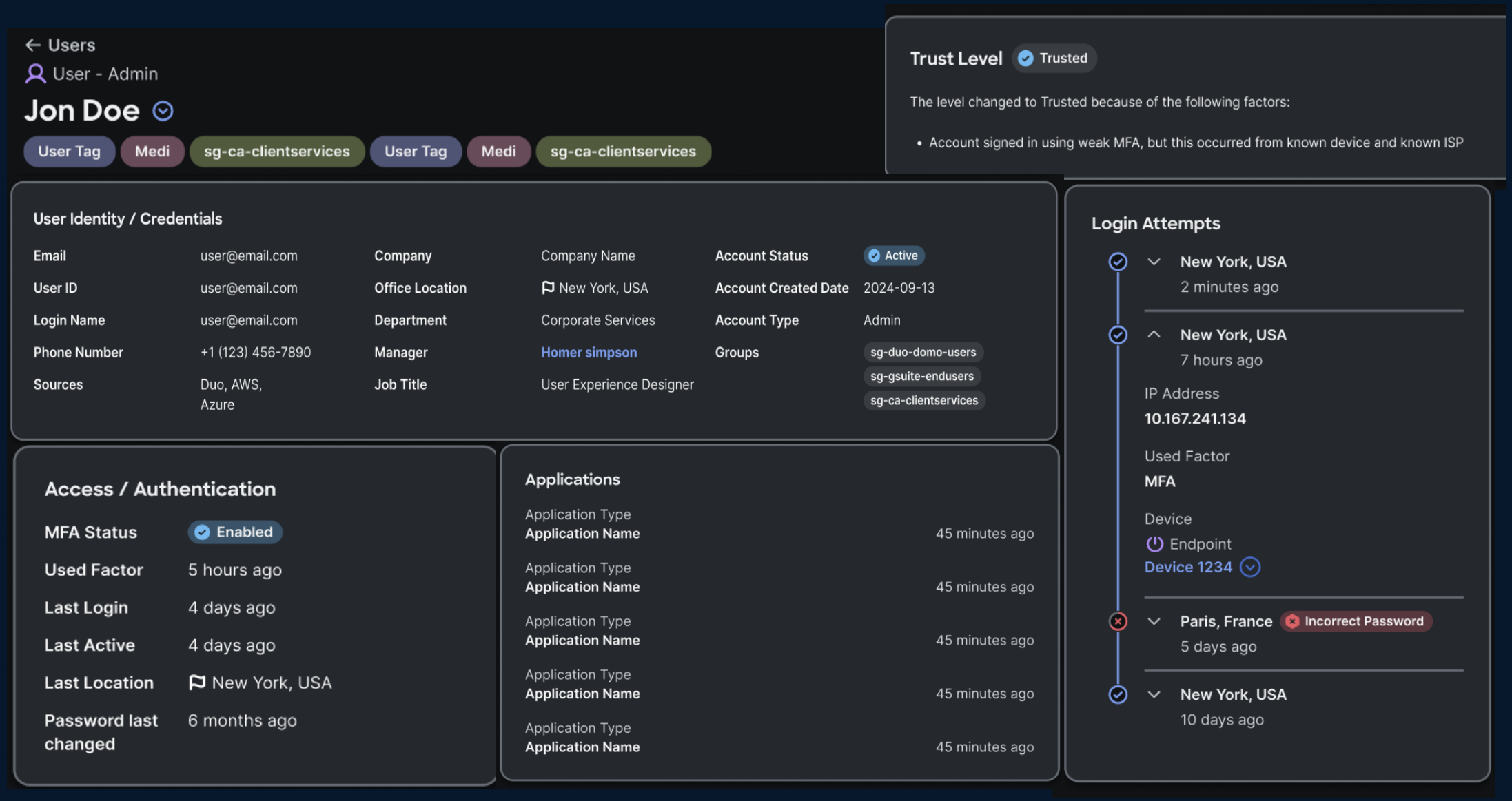
10,337 with identity events

19,552 not using MFA

Search | Filters | 19,601 matching results | Edit Labels | Export to CSV

Display name	Login names	Emails	Identity events	MFA status	Last logon	Labels	Value	Last active	Used devices
Aaron Woland	aaron@woland.com	aaron@woland.com	2	Enabled	2025-04-24T19:28:26.694Z		10 (D)	2025-04-24T19:28:27.000Z	EPQOLVJJRAL4 EPQOLVJJRAL4 DPUCY3HKA1N WA94B6JNAKTOI9
Aaron Woland	loxx@cisco.com	loxx@cisco.com	1	Disabled	2025-06-17T18:23:58.074Z		10 (D)	2025-06-17T18:23:58.074Z	
Aaron Woland	loxx@loxx.tv		2	Disabled	2025-05-07T19:32:56.071Z		10 (D)	2025-05-09T19:35:21.000Z	AFiQxQ8F3sSP AFiQxQ8F3sSP AFiQxQ8F3sSP
Aaron Woland (aawoland)	aawoland@cisco.com	aawoland@cisco.com	6	Enabled	2025-05-08T14:35:20.791Z		10 (D)	2025-05-08T14:35:20.791Z	
abcd	abcd@gmail.com	abcd@gmail.com	1	Disabled			10 (D)		
Accounting2	accounting2@securitydemo.net	accounting2@securitydemo.net	1	Disabled			10 (D)		
Aditya K R (adikr)	adikr@cisco.com	adikr@cisco.com	4	Enabled	2025-06-19T15:08:21.066Z		10 (D)	2025-06-19T15:08:21.066Z	{PII_Removed}
administrator	administrator		1	Disabled			10 (D)		
Adrián Espinoza	adrian@securitydemo.net	adrian@securitydemo.net	1	Enabled	2025-04-16T22:29:58.238Z		10 (D)	2025-04-16T22:29:58.238Z	DPOO44TVBT2 EPJCFLHTJQT6 WAO503VRRUUXG

Duo連携の成果　(将来像)



XDR の実例

予兆検知

検出

不審なユーザーアクティビティと、そのエンドポイントからの不審なトラフィック、不審な IP への長時間の接続

調査

対応

Agentic AIによる調査・明確な判断

検出

調査

関連付けられたアラートを調査し、85% の確率で攻撃であると判定

対応

ハンドブックを活用した確実な対応

検出
調査

対応

隔離されたエンドポイント
ブロックされた悪意のある IP
無効化されたプロセス
UserTrigger フォレンジック向けに MFA をトリガー

*AI 生成によるビデオ

明確な判断と確固たるアクションで
デジタル「空間」を整理

Cisco XDR事例 前橋赤十字病院様

医療

AIを活用し止まらない医療を実現。前橋赤十字病院

医療用システム・機器の制約や体制面の課題にも対応

事例を読む　ビデオを見る（1:58）

お客様の声

セキュリティ担当者の負担を大きく高めることなく、高度なセキュリティを実現できた

"これで被害に遭うのなら他の対策でも防ぐのは難しい。そう評価しています"

前橋赤十字病院
病院長
中野 実氏

追加のアップデート

Cisco XDR How to サイト

リリース済み

提案 / 販売

■ XDR紹介資料
- [NEW!] ざっくりCisco XDR（パートナー様向け）
- [Cisco Japan Blog] Cisco XDRのご紹介
- [Cisco Blog] 経営幹部向けXDRのROI（英語）
- XDR入門書 （For Dummiesシリーズ）

■ 提案資料（パートナー様向け）
- [NEW!] Japan Partner Community:セキュリティ
- [NEW!] Cisco XDRのご紹介（PPT）
- [NEW!] Cisco XDRのご紹介（動画）
- [NEW!] 第1回 次世代セキュリティ対策の教科書セミナー:フレームワーク編
- [NEW!] 第2回 次世代セキュリティ対策の教科書セミナー:ツールミックス編
- [NEW!] 第3回 次世代セキュリティ対策の教科書セミナー:基本設計編
- [NEW!] 第1回 XDRで拓く 次世代セキュリティ運用へのロードマップセミナー:SOC
- [NEW!] 第2回 XDRで拓く 次世代セキュリティ運用へのロードマップセミナー:XDR
- [NEW!] 第3回 XDRで拓く 次世代セキュリティ運用へのロードマップセミナー:モダ

■ 導入事例
- 前橋赤十字病院様
- 国内事例一覧
- 海外事例一覧

設計 / 構築

■ マニュアル
- XDR Help Center
- XDR 技術情報TOP
- XDR Analytics(SCA) 技術情報TOP
- CTB 技術情報TOP

■ ガイド
- [NEW!] Cisco XDR 初期設定ガイド （パートナー様向け）
- SNAとの連携手順
- Umbrella APIの種類とできること

■ デモ / ハンズオン環境
- dCloud XDRコンテンツ一覧
- Cisco Breach Protection Suite v1 - Instant Demo (XDR)
- Cisco XDR with Cohesity Data Protection - Automated Ransomware Response and Acce
- Breach Defense and Security Operations: XDR and Splunk

■ ツール
- Flows Per Second (FPS) Estimator
- NetFlow Config Generation Tool for Security Analytics!

■ Deep Dive
- [Cisco Live] Making Sense of all the Parts & Pieces
- [CIsco Live]Incident Response with Cisco XDR
- [Cisco Live]Automating detection and response outcomes using Cisco XDR and Generati
- [Cisco U.] New Cisco XDR Alerts
- [Cisco U.] Network Visibility Module (NVM) Telemetry and Detections

運用 / 開発

■ トラブルシューティング
- Cisco XDR TAC Troubleshooting Knowledge Base
- [Cisco Live]Troubleshoot Cisco Secure Client Network Visibility Module with XDR
- XDRの新規SRオープン時に取得する情報
- XDR: Automation Remote が Disconnected になる問題で取得すべき情報 （version 2.4 まで）
- XDR: Automation Remote が Disconnected になる問題で取得すべき情報（Version 2.5 以降）
- XDR: Workflow の失敗原因の調査で必要な情報について
- XDR: NVM モジュールからのフローデータ送信先について
- XDR: NVM モジュールにおける Proxy サポートについて
- XDR: HAR ファイルの取得方法
- SAML Tracer利用方法
- XDR: SNA との連携手順と確認方法
- SCC: [事象] No verified domain exists for the organizationと表示しMFAリセットが失敗
- SCC: Security Cloud Control での Organization ID の確認方法

■ トレーニングコンテンツ
- Ask the Experts（ATX） 過去セッション 録画と資料
- Rapid Incident Response with Cisco XDR
- Automation Labs

■ 開発
- XDR APIガイド
- カスタムインテグレーションガイド
- Workflow ベストプラクティス
- Important Notes and Limits
- Thresholds and Limits
- [NEW!] デモ動画：[AI×MCP×XDR] Experience AI-Powered Incident Response with MCP!

次のステップ

ライブデモ
ウェビナー

防御の手法の
ワークショップ

cisco.com/site/jp/ja/products/security/xdr にアクセスする

ありがとうございました