

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

セッション ID : BRKSEC-1029

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する犯罪

デジタル空間に潜むロッガー

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

ロックされていない
ドアや窓を見つける



侵入

家を探し、
潜むのに最適な場所を探す



環境の検出

拠点を設営し、
家にあるものを利用する



環境寄生

詳細を集め、
完璧な強奪計画を立てる



強奪の計画



010110
110010
001011

脆弱なアプリやデバイスを
エクスプロイトして侵入する



脆弱な
アセット

システム/サービスを
検出してマッピングする



検出と
マッピング

Web シェルのインストール、
構成の変更、ネイティブ/
管理ツールの操作



環境寄生

エスカレーション、移動、
DC 侵害、検出回避



防御と漏洩



010110
110010
001011

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

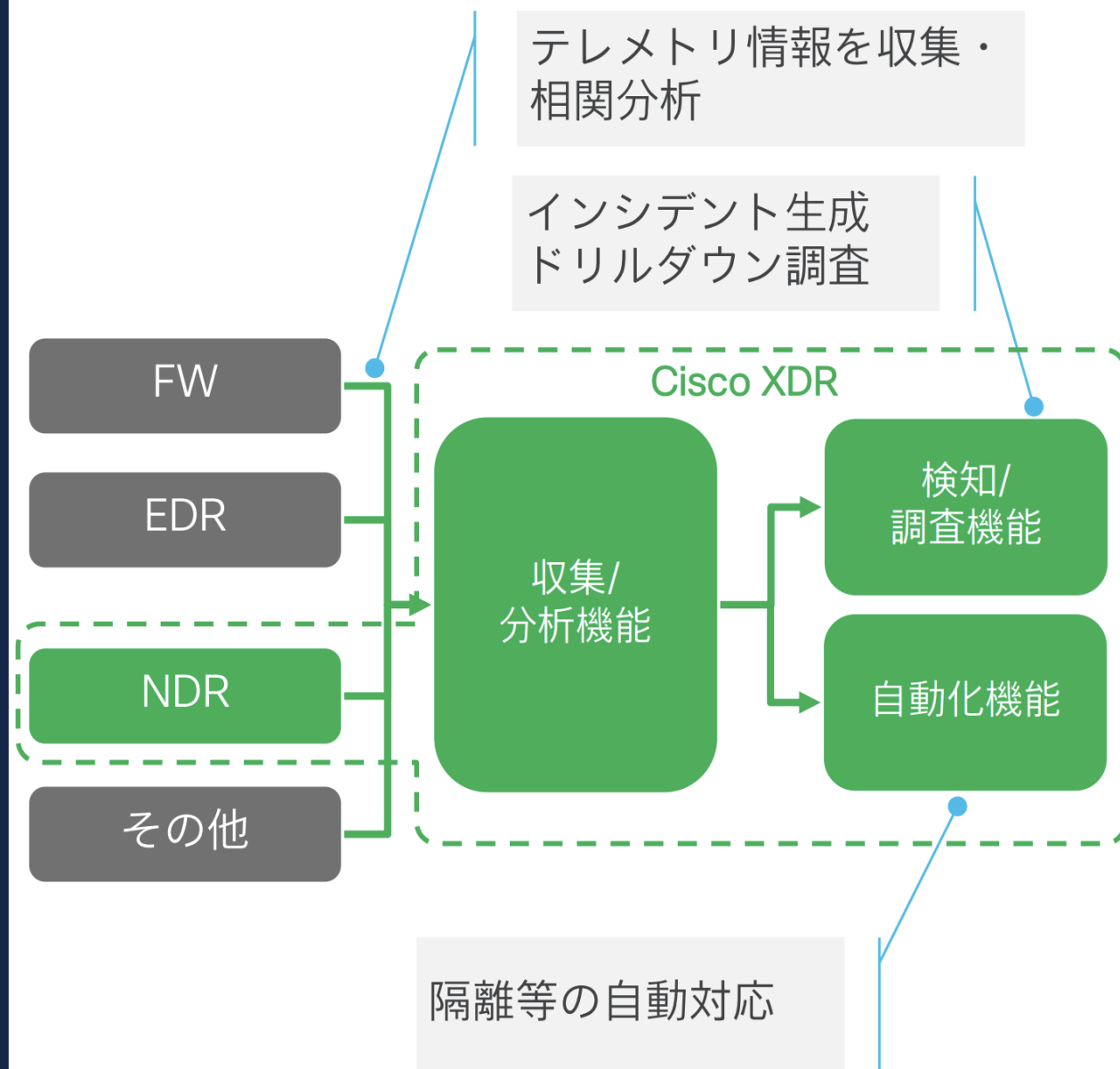
Detection

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

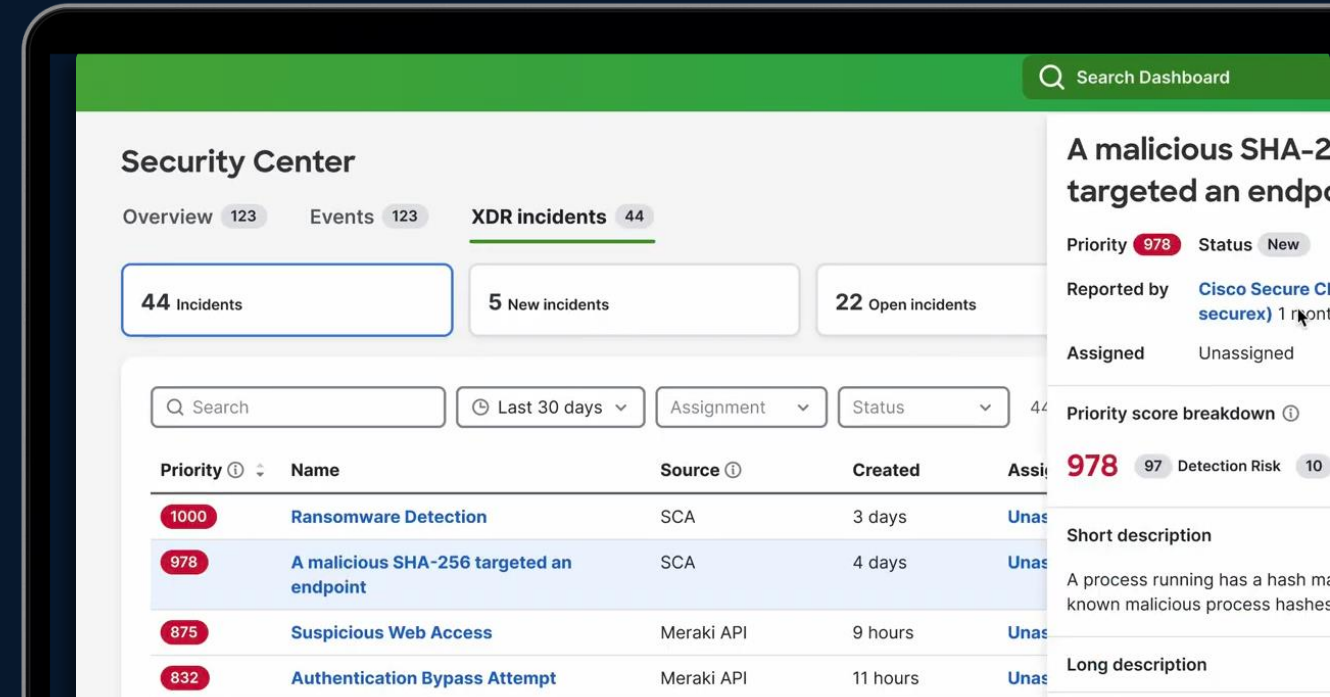
セキュリティ運用するうえで役に立つ
さまざまなツールのセット



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

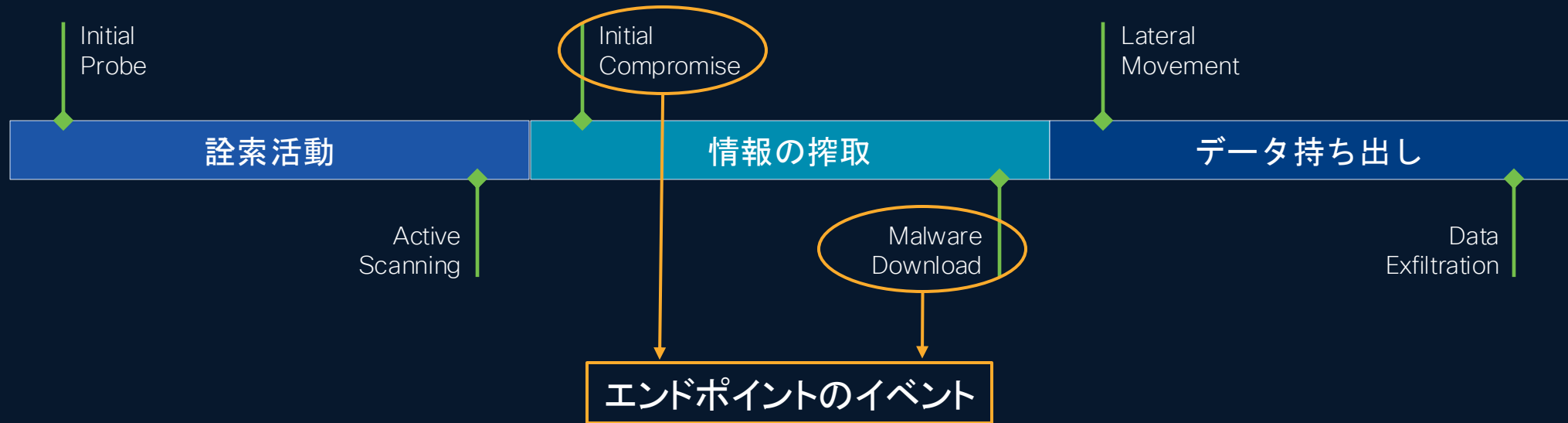


中小規模の
組織に最適化

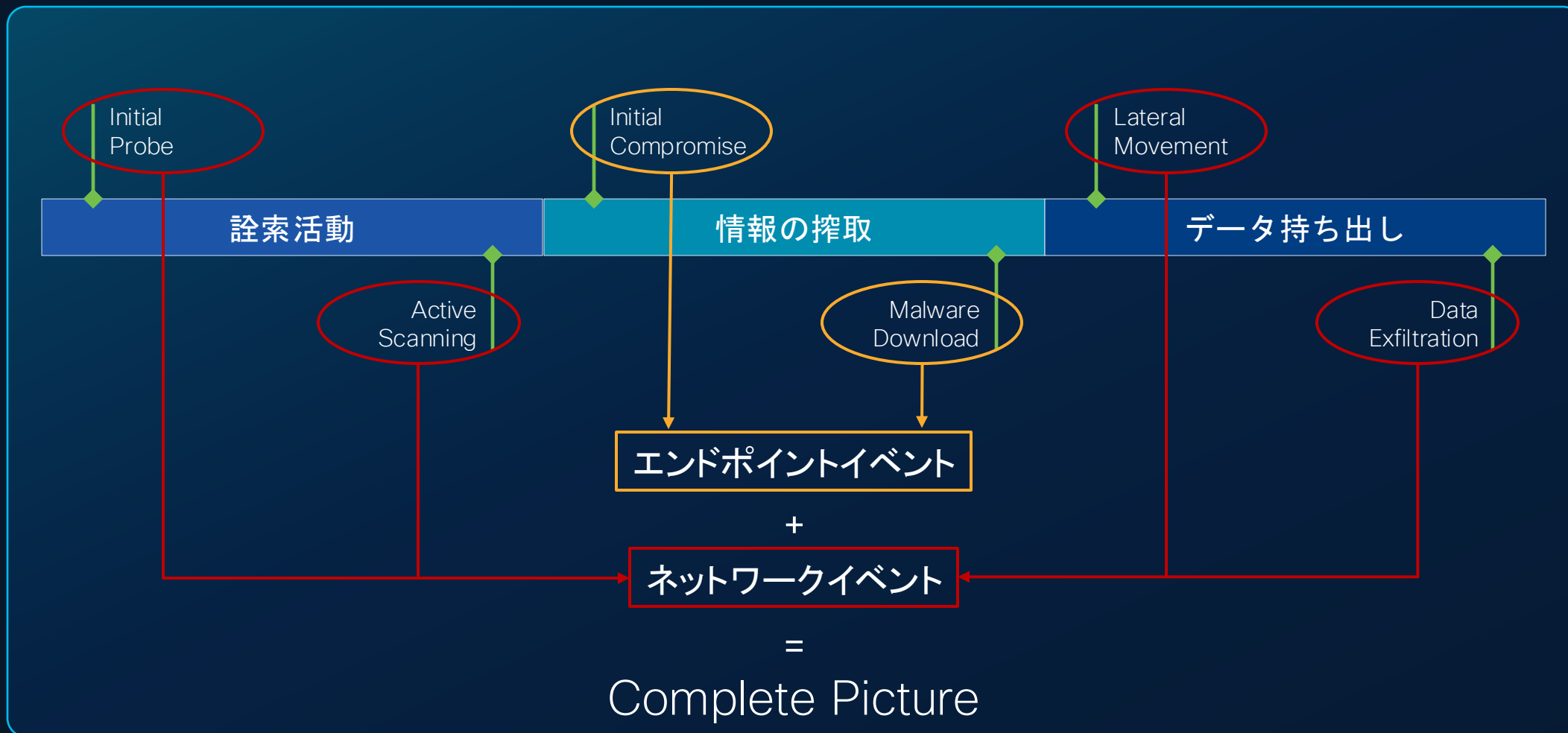
成果を迅速に提供

ネットワークと
深く統合

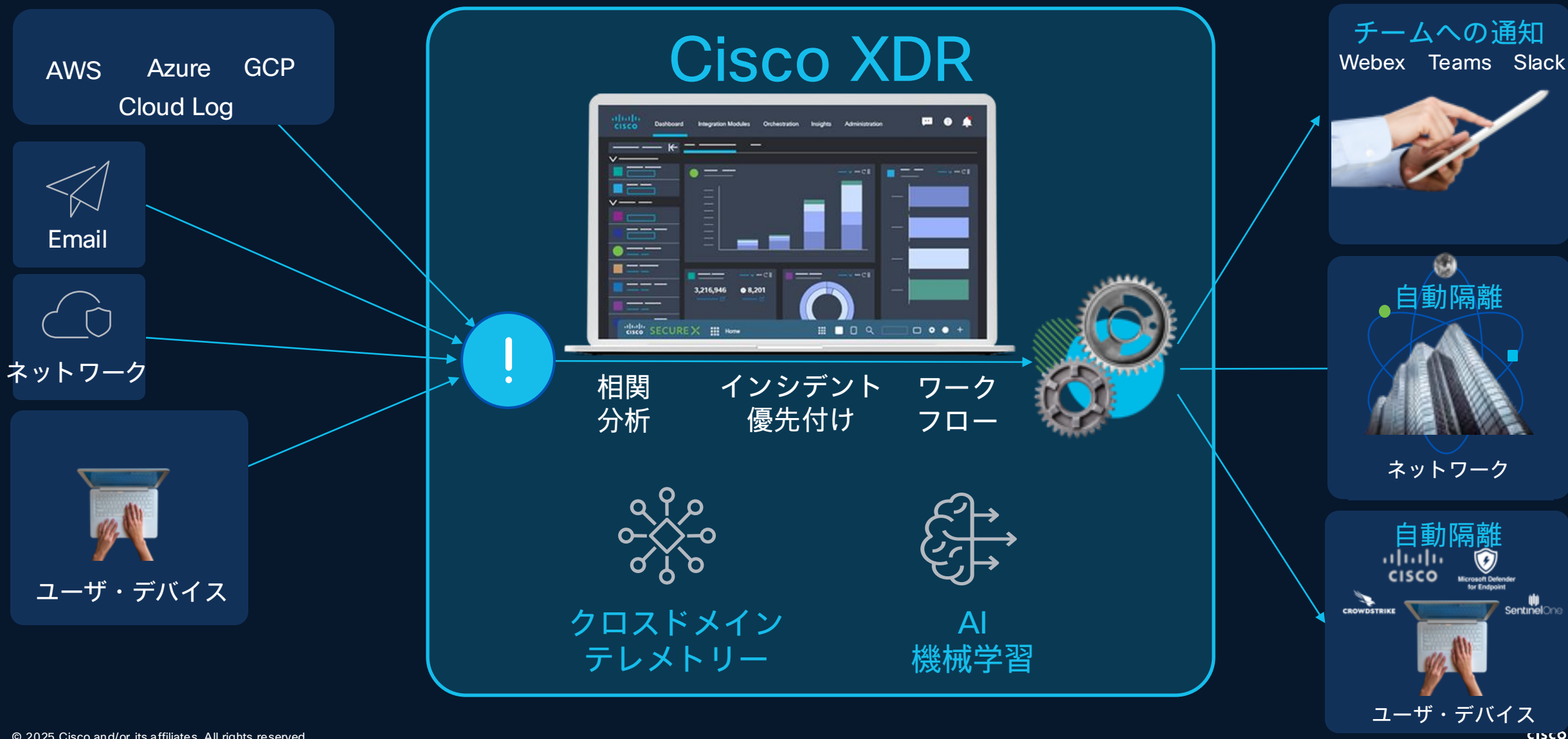
エンドポイントのテレメトリだけでは不十分



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



TalosのインテリジェンスでCisco XDRを強化

TALOS



500

脅威リサーチャーの数



AI

アルゴリズム



5,500億

1日のセキュリティイベント数

Meraki

Search Dashboard

Global Overview

Organization
ExplorCorp

Network
atl-tme-campus-networks

Network-wide

Switching

Insight

Organization

Find in Menu

Security Center

MX SummaryMX EventsXDR Incidents

56 Incidents8 New incidents26 Open incidents13 Un

Last year

Status

Assignment

56 incidents

Priority	Name	Source	Created	Assigned
1000	Data Loss and Suspicious Activities on Multiple Devices	Cisco XDR Analytics	5 days	HJASAS
913	Multiple Defense Evasion and Credential Theft Attempts Detected	Cisco XDR Analytics	6 days	AS
813	Multiple LiveCredential Theft Detection on User Laptop	Cisco XDR Analytics	7 days	AS / S / AS
783	[Terminated] Malicious File Activities Detected by CrowdStrike	Cisco XDR Analytics	8 days	RR
523	SuspiciousFileWritten	Cisco XDR Analytics	8 days	AS
392	Multiple Defense Evasion and Credential Theft Attempts Were Terminated	Cisco XDR Analytics	8 days	RR

Data Loss and Suspicious Activities on Multiple Devices

Priority1000StatusOpen

Reported byCisco XDR Analytics1 few seconds ago

Assigned toHJASAS+1

Priority score breakdown

1000100Detection Risk10Asset Value at Risk

Short description

The incident occurred between Oct 23 2024 and Oct 24 2024. A suspect data loss and hoarding were detected on device 320b5646-2d70-4f6d-9ffa-a26154f1e5df by SnaDetections. There were additional suspicious activities on the same and another device involving user obsidian by ScaDetections.

Long description

Assets2

Observables19

HelpView incident in XDR

© 2024 Cisco Systems, Inc.

Meraki MX を XDR に統合

© 2025 Cisco and/or its affiliates. All rights reserved.

CISCO

Global Overview

Organization Summary New

Organization
Acme Corp

Network
Acme Corp Branch 1 - DO NOT MODIFY

Secure Connect

Network-wide

Assurance New

Cellular Gateway

Security & SD-WAN

Switching

Wireless

Cameras

Sensors

Insight

Organization

Adaptive Policy

Devices

View all devices

Uplinks 20 total

1 Offline

WAN Appliances 20 total

1 Offline

Switches 3 total

All Online

Access Points 6 total

1 Offline

Cameras 3 total

All Online

Cellular Gateways 0 total

All Online

Sensors 16 total

All Online

Networks

Usage and clients over the last week

Search Networks

Status

60 秒以内

Tags

36 networks

		Name	Usage	Clients	Tags	WAN Appliances	Switches	Access Points	Cameras	Cellular Gateways	Sensors
☐	ⓘ	Acme Corp - India	50.16 GB	10	branch	1	—	1	—	—	—
☐	✓	Acme Corp Branch 1 - DO NOT MODIFY	551.39 GB	37	azure branch	1	1	1	—	1	6
☐	✓	Acme Corp - Branch 2	29.60 GB	7	branch	1	—	1	—	—	—
☐	✓	Acme Corp - Branch 3	2.98 TB	49	branch	1	2	3	3	—	10
☐	✓	AWS-Dragon-	5.51 GB	7	aws	1	—	—	—	—	—
☐	✓	VM2-Dragon-	2.21 GB	1	aws	1	—	—	—	—	—
☐	✓	Acme Corp - group	5.88 TB	10	branch	1	3	3	3	—	10

© 2025 Cisco and/or its affiliates. All rights reserved.

CISCO

NetFlow データの 価値を解放つ

- Control Center >
- Incidents**
- Investigate
- Intelligence >
- Automate >
- Assets >
- Client Management >
- Administration >

i Exciting enhancements are rolling out through October for Incident Generation, Incident Comprehension, Incident Prioritization, Integration Support, Response, Coverage Mapping, and Notifications. View our Cisco XDR release notes and email for full details! ×

← Incidents

1000
Open ▾
Data Loss and Suspicious Activities on Multiple Devices

Reported by **Cisco XDR Analytics** on 2024-10-24T13:47:49.348Z - [1 Linked Incident](#)

HJ AS AS +1

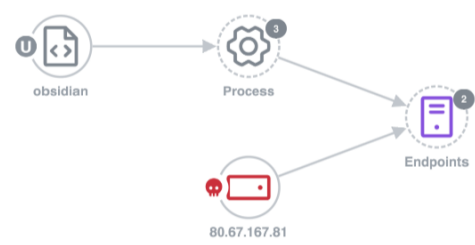
[View detailed description](#)

The incident occurred between Oct 23 2024 and Oct 24 2024. A suspect data loss and hoarding were detected on **device 320b5646-2d70-4f6d-9ffa-a26154f1e5df** by SnaDetections. There were additional suspicious activities on the same and another device involving **user **obsid...** AI-generated [more](#)

- Overview**
- Detection
- Response
- Worklog
- Report

↗ Expand

- +
- −
- ✕
- ↶
- 👉
- 🔍



Show timeline 

- Malicious
- Suspicious
- Common
- Unknown
- Clean
- Asset

Cisco XDR



電子メール



ネットワーク



クラウド



ファイアウォール



エンドポイント



アイデンティティ

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



Incident 453

Multi-Stage Malware Attack with Exfiltration

Overview Detection Response Worklog Report

Summary

On October 8th, 2024, user Darin received a phishing email, resulting in the IcedID malware installation on endpoint Darin-windows11 and subsequent communication with a suspicious IP.

By October 9th, 3.2 GB of data was exfiltrated from endpoint misty-windows to an external IP.

Next Steps

Verification

Review data transfer logs to confirm data exfiltration to IP 162.125.13.18.

Containment

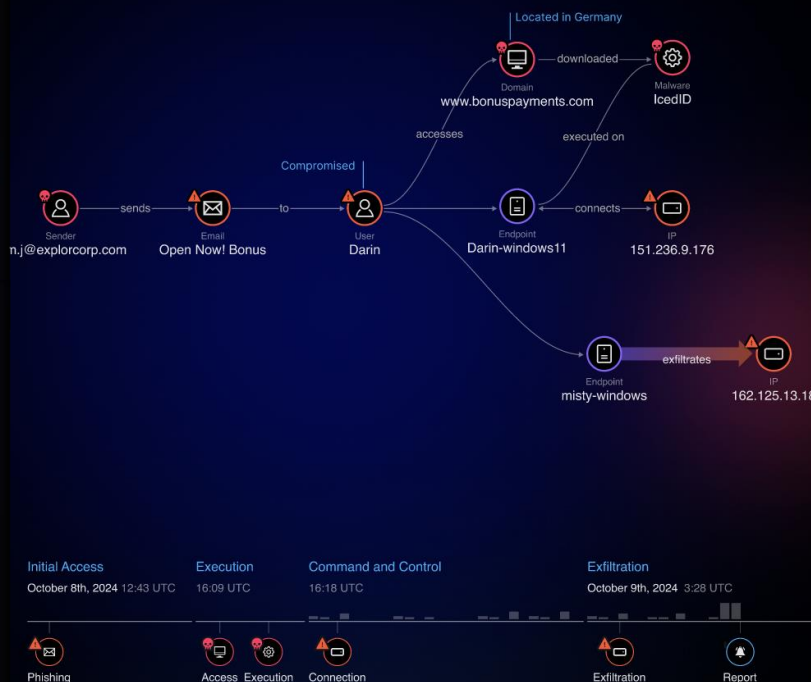
Isolate endpoints to prevent further damage.

Block malicious IPs and domains to stop communication.

Recovery

Reimage endpoints to restore a clean state.

Perform a full incident review and enhance email and network policies.



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。

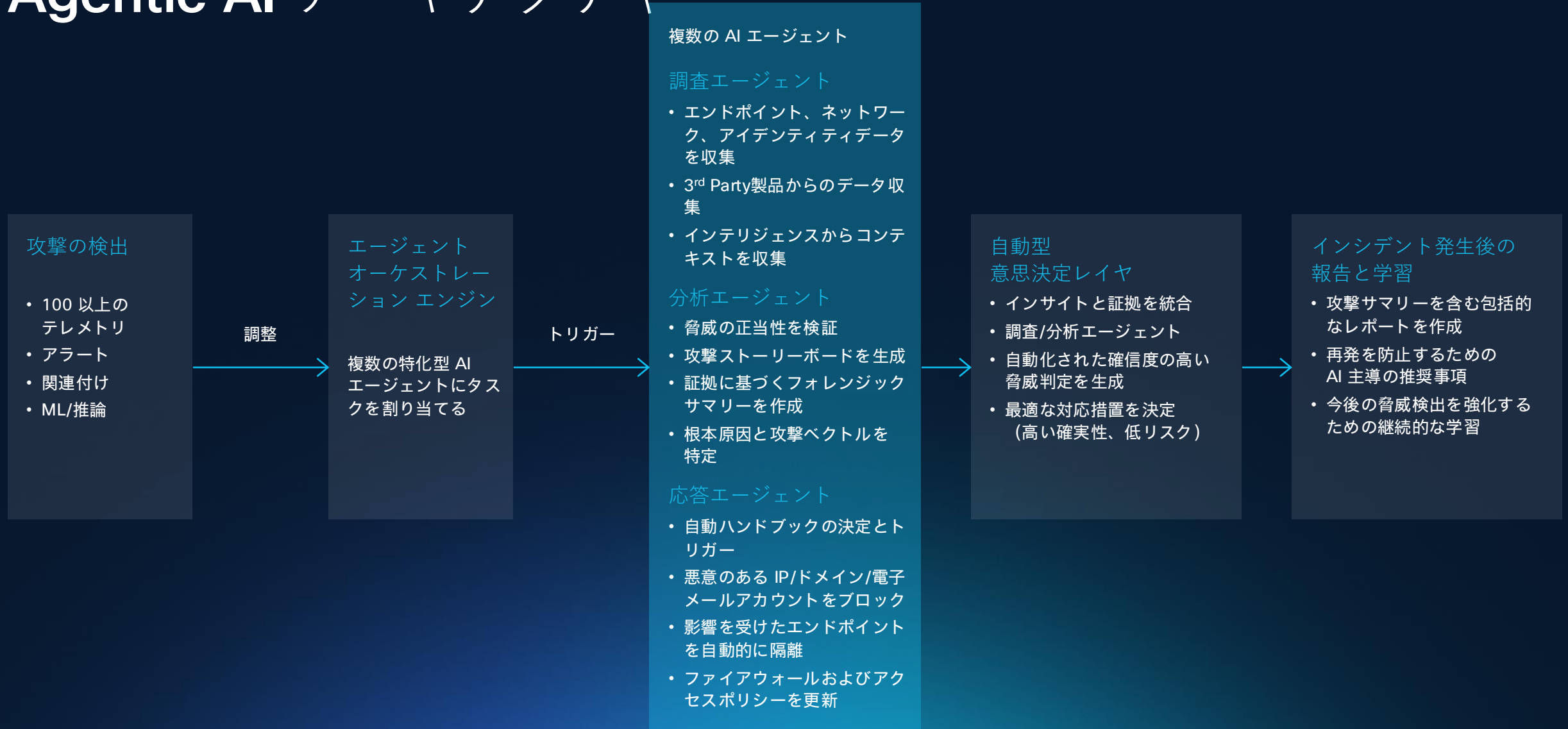
AI AssistantとAgentic AIの定義

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



Incident 453

Multi-Stage Malware Attack with Exfiltration

Overview Detection Response Worklog Report

Summary

On October 8th, 2024, user Darin received a phishing email, resulting in the IcedID malware installation on endpoint Darin-windows11 and subsequent communication with a suspicious IP.

By October 9th, 3.2 GB of data was exfiltrated from endpoint misty-windows to an external IP.

Next Steps

Verification

Review data transfer logs to confirm data exfiltration to IP 162.125.13.18.

Containment

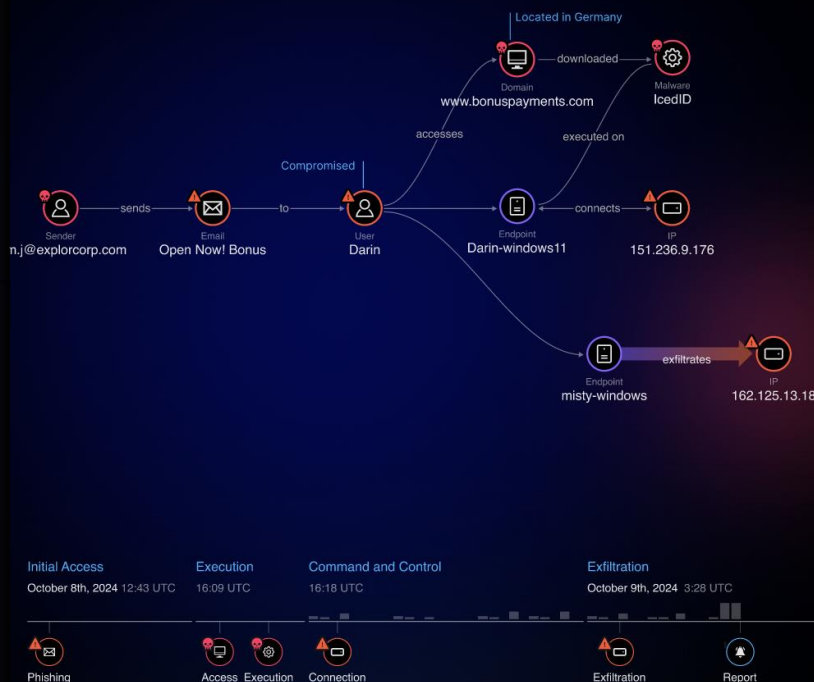
Isolate endpoints to prevent further damage.

Block malicious IPs and domains to stop communication.

Recovery

Reimage endpoints to restore a clean state.

Perform a full incident review and enhance email and network policies.



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。

factura-228447578537

Home > Tasks > Suspicious Endpoint and User Activity Detected Acquisition 008 > Investigation Hub > Downloads

Downloads

factura-228447578537 Advanced Filters

☐	Flags	Finding T...	Asset	Path
		Q	(All)	Q
☐			Mazzarella	C:\Users\alexw\Downloads\factura-228447578537.pdf
☐			Mazzarella	C:\Users\alexw\Downloads\factura-228447578537.pdf
☐	III		Mazzarella	C:\Users\alexw\Downloads\factura-228447578537.pdf

Details

Hide Empty Fields View in Separate Window

Path
C:\Users\alexw\Downloads\factura-228447578537.pdf

File Exists
1

Hash
1029EDA15FEB6C83BD64AAFA49F6A0216AB7FEFF6454
2711FB211689FC69D845

Digital Sign Status
4

Publisher
N/A

File Size
10918

Modified
2025/03/28 22:57:33

Accessed
2025/04/22 04:16:03

Created
2025/03/28 22:57:32

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。

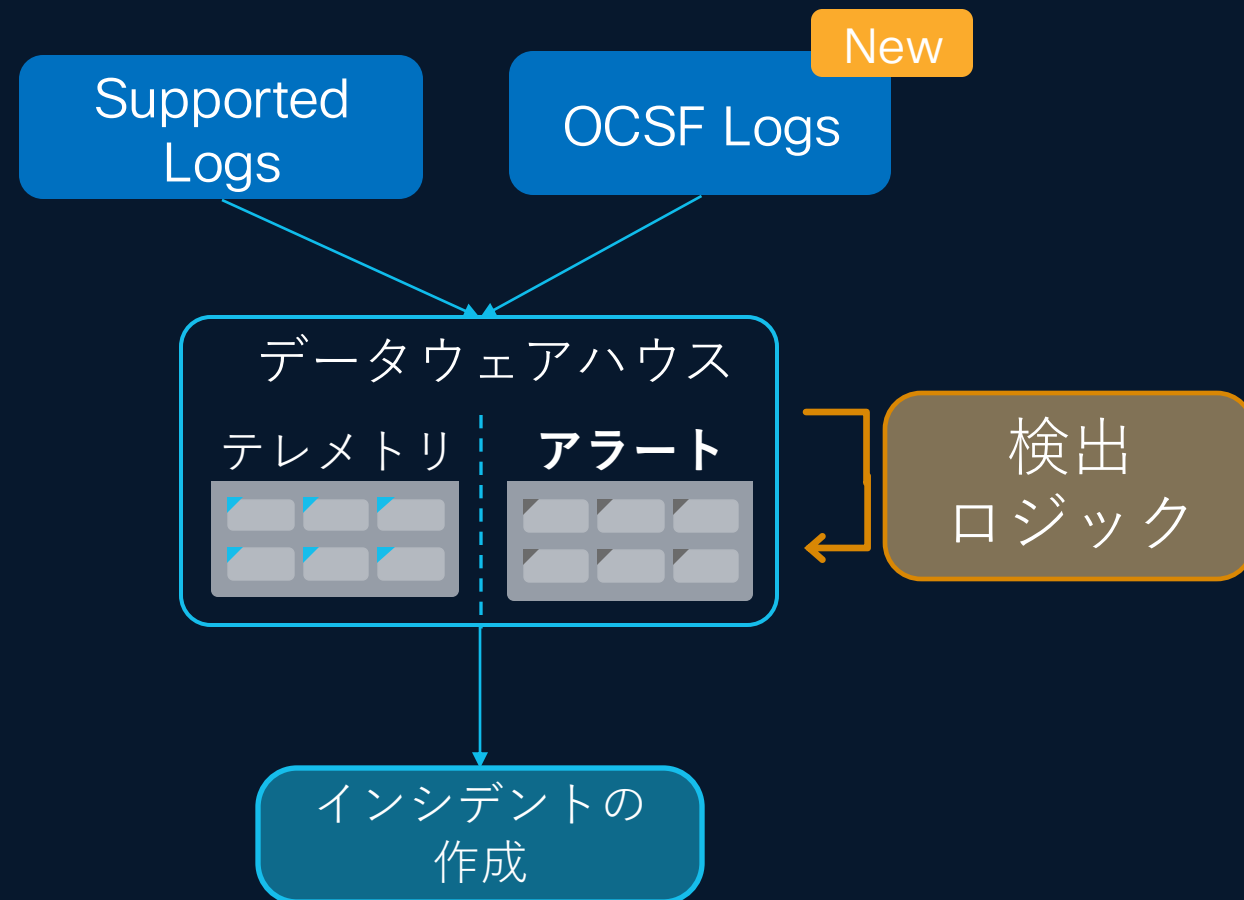
OCSFとは

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](#)

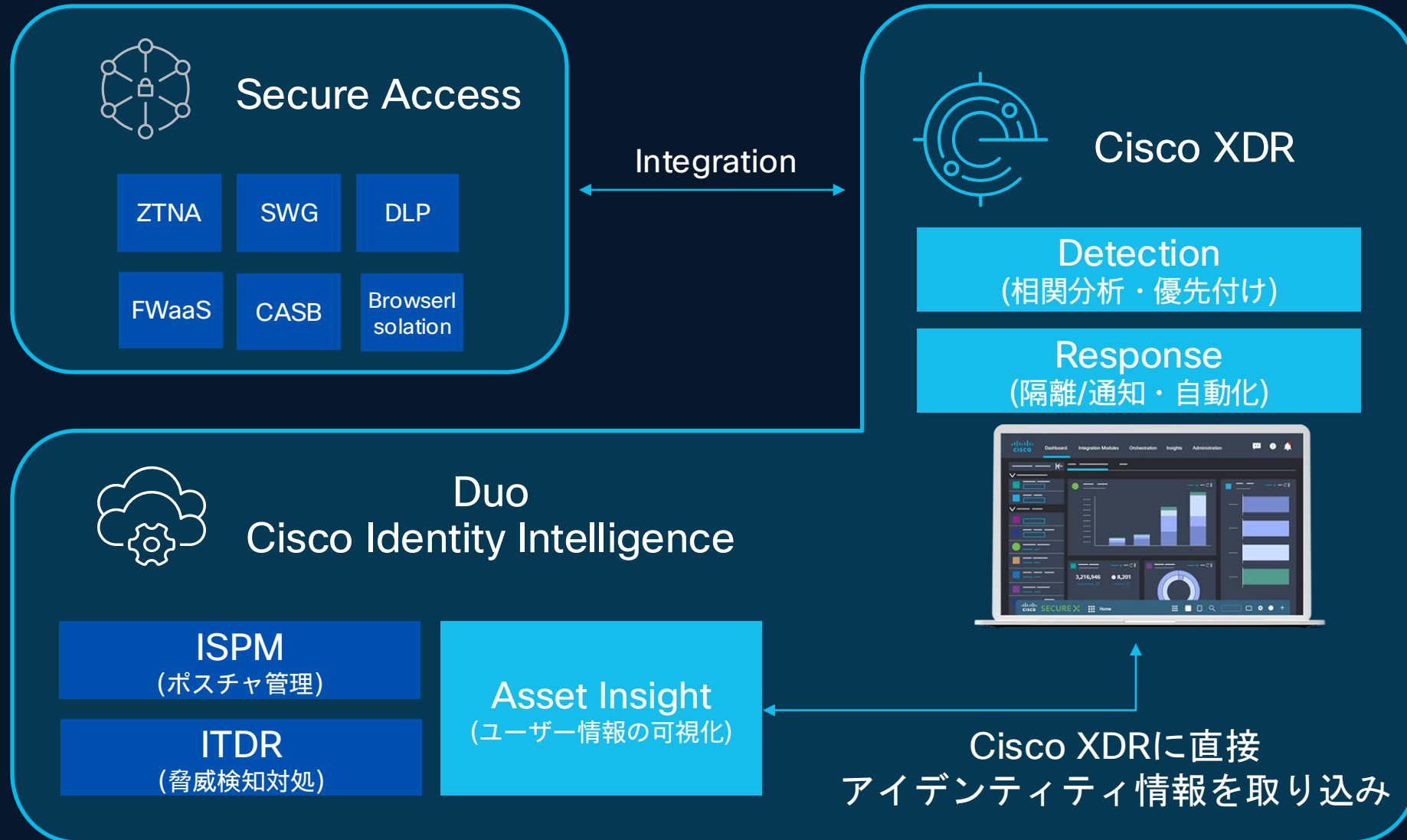
Cisco XDRの検出ロジック



Zero Trust with Cisco XDR

Secure Access ・ Duo連携

Released



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

Q 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)

← Users

User - Admin

Jon Doe

User TagMedi sg-ca-clientservicesUser TagMedi sg-ca-clientservices

User Identity / Credentials

Email	user@email.com	Company	Company Name	Account Status	Active
User ID	user@email.com	Office Location	New York, USA	Account Created Date	2024-09-13
Login Name	user@email.com	Department	Corporate Services	Account Type	Admin
Phone Number	+1 (123) 456-7890	Manager	Homer simpson	Groups	sg-duo-domo-userssg-gsuite-enduserssg-ca-clientservices
Sources	Duo, AWS, Azure	Job Title	User Experience Designer		

Access / Authentication

MFA Status	Enabled
Used Factor	5 hours ago
Last Login	4 days ago
Last Active	4 days ago
Last Location	New York, USA
Password last changed	6 months ago

Applications

Application Type	Application Name	45 minutes ago
Application Type	Application Name	45 minutes ago
Application Type	Application Name	45 minutes ago
Application Type	Application Name	45 minutes ago
Application Type	Application Name	45 minutes ago

Trust Level

Trusted

The level changed to Trusted because of the following factors:

- Account signed in using weak MFA, but this occurred from known device and known ISP

Login Attempts

New York, USA

2 minutes ago

New York, USA

7 hours ago

IP Address

10.167.241.134

Used Factor

MFA

Device

Endpoint

Device 1234

Paris, France

Incorrect Password

5 days ago

New York, USA

10 days ago

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

エンドポイント



XDR



Meraki
アクセスポイント

Actions taken

[View Notes](#)

[Download](#) ▾

- May 12, 2025 @ 9:12 PM PDT **DU** [View run](#) 
Executed Workflow for Contain Incident:
Assets (Devices)
- May 12, 2025 @ 9:11 PM PDT **DU**
Added note for Review Incident
- May 12, 2025 @ 7:41 AM PDT **OS** [View run](#) 
Executed Workflow for Contain Incident:
Assets (Devices)
- May 1, 2025 @ 12:04 PM PDT **DU** [View run](#) 
Executed Workflow for Confirm Incident
- Apr 29, 2025 @ 1:13 PM PDT **DU** [View run](#) 
Executed Workflow for Contain Incident:
Assets (Devices)

*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

| 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 Acc
- ・ 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 の失敗原因の調査に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](https://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