

Cisco **Security**

Cisco XDR with Meraki

シスコ バーチャル イノベーション ツアー

APJC XDR Sales Lead

平岡 龍弘

Cisco Systems

2025.6.5

ご挨拶

自己紹介



■ 平岡 龍弘 Hiraoka Tatsuhiko
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、2025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 × Meraki MX

Network-Led
Security

Lean IT Outcomes

AI and Automations

今日攻撃を受けるのは運次第だろうか？
ゲームのように思える

セキュリティは重要ではある
が、仕事の一部ではない

インフラストラクチャ

IT

セキュリティ

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

セキュリティツール

A close-up, top-down view of a roulette wheel. The wheel is dark with a lighter-colored track around the edge. A central metal spindle with a cross-shaped handle is visible. The entire image is overlaid with a semi-transparent blue filter.

カジノで勝つのは常にカジノ運営側

別のアプローチがふさわしい

Meraki

Search Dashboard

Global Overview

Organization
ExplorCorp

Network
atl-tme-campus-networks

Network-wide

Switching

Insight

Organization

Find in Menu

Security Center

MX Summary

MX Events

XDR Incidents

56 Incidents

8 New incidents

26 Open incidents

13 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	HJ AS AS
974	Multiple Manuerialing and Credential Theft Attempts Detected	Cisco XDR Analytics	days	Assigned
873	Multiple LiveCredent Detection on Use of pgs 1	Cisco XDR Analytics	7 days	AS AS 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

Priority 1000

Status Open

Reported by

Cisco XDR Analytics

1 few seconds ago

Assigned to

HJ

AS

AS

+1

Priority score breakdown

1000

100

Detection Risk

10

Asset Value at Risk

Short description

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 ScaDetections. There were additional suspicious activities on the same and another device involving user obsidian by ScaDetections.

Long description

Assets

2

Observables

19

Help

View incident in XDR

© 2024 Cisco Systems, Inc.

すべての Meraki MX がセンサーになる

60 秒以内

Meraki

Search Dashboard

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 1 total
All Online

Sensors 16 total
All Online

Networks

Usage and clients over the last week

Search Networks Status Network Type Tags 36 networks

		Name	Usage	Clients	Tags	WAN Appliances	Switches	Access Points	Cameras	Cellular Gateways	Sensors
<input type="checkbox"/>	ⓘ	Acme Corp - India	50.16 GB	10	branch	1	—	1	—	—	—
<input type="checkbox"/>	✓	Acme Corp Branch 1 - DO NOT MODIFY	551.39 GB	37	azure branch	1	1	1	—	1	6
<input type="checkbox"/>	✓	Acme Corp - Branch 2	29.60 GB	7	branch	1	—	1	—	—	—
<input type="checkbox"/>	✓	Acme Corp - Branch 3	2.98 TB	49	branch	1	2	3	3	—	10
<input type="checkbox"/>	✓	AWS-Dragon-	5.51 GB	7	aws	1	—	—	—	—	—
<input type="checkbox"/>	✓	VM2-Dragon-	2.21 GB	1	aws	1	—	—	—	—	—
<input type="checkbox"/>	✓	3 Acme Corp - Branch	5.88 TB	48	branch	1	3	3	3	—	10

NetFlow データの価値を 解き放つ

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



~~XDR - EDR~~

Cisco XDR



同様の位置付け

すべてを Meraki ダッシュ
ボードで直接確認

[← 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](#)

[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 **obsd...** [AI-generated more](#)

HJ AS AS +1

Overview Detection Response Worklog Report

Expand

[Show timeline](#)

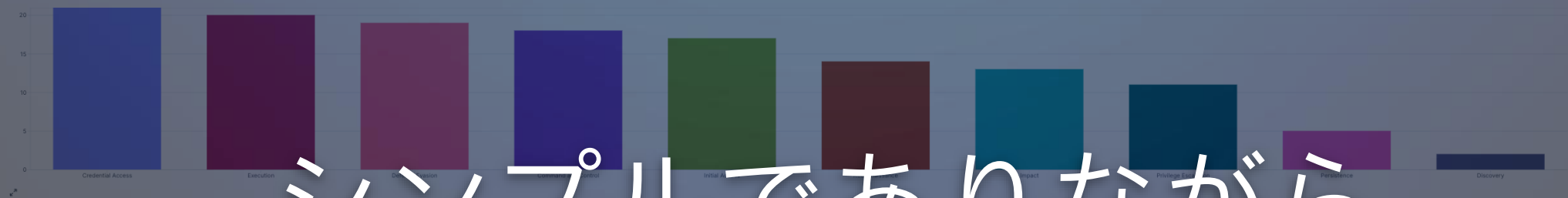
Malicious Suspicious Common Unknown Clean Asset

Dashboards

Overview XDR - Copy CLUS2024 email ExplorCorp - Copy

MITRE ATT&CK® Incidents

Private Intelligence



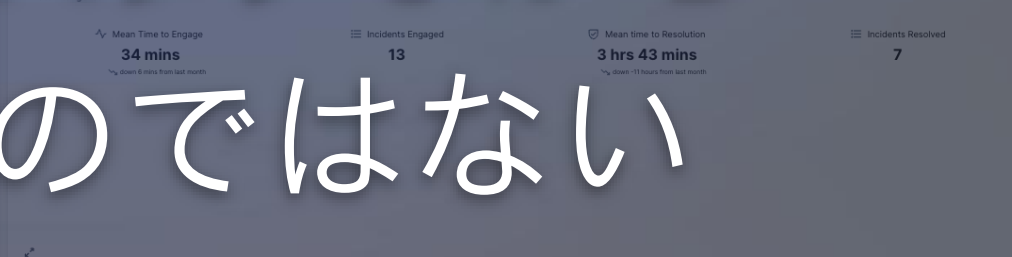
Unassigned Incidents

Private Intelligence

Priority	Name	Created
930	HiveCredTheft	8 days ago
920	HiveCredTheft	8 days ago
920	HiveCredTheft and Unexpected Svchost	8 days ago
880	(Not Terminated, Not Blocked) Malicious	8 days ago
850	(Not Blocked, Not Terminated) Detected	8 days ago
850	SuspiciousFileWritten	6 days ago
850	(Not Terminated, Partially Quarantined) Custom IO	6 days ago
850	(Terminated) Suspicious Files Written Detected on Device	6 days ago

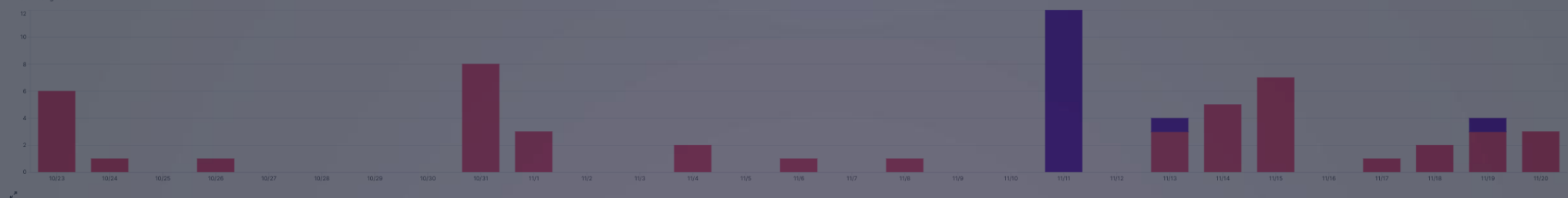
Team Metrics

Private Intelligence



Detection Sources

Private Intelligence



The AI Assistant has identified 2 new incidents. The incident has a minimum priority score of 700. Immediate investigation and mitigation is recommended.

[View incident](#)

シンプルでありながら
単純なものではない

Cisco XDR

AI

AI で強化された
検出

脅威ハンティング、調査、
フォレンジック

対応

Cisco XDR | オーケストレーション

TALOS

500 人の脅威研究者 + AI を活用したアルゴリズム

シスコのテレメトリ



ネットワーク



エンドポイント



電子メール



クラウド



アプリケーション



アイデン
ティティ

サードパーティの
テレメトリ

サードパーティの
インターフェイス

お客様のインフラストラクチャ



サードパーティのツール



インテリジェンス




SIEM/SOAR



その他



マネージドサービス

A man with a beard and glasses is working at a computer in a server room. He is looking at a monitor displaying a network diagram. Another person is visible in the background, also working at a computer. The room is dimly lit with blue light from the monitors.

- SNOC -

Cisco XDR でセキュリティ、 ネットワーク、IT を連携

戦略で勝負が決まるゲーム

セキュリティとネットワークの統合



XDR



Meraki

A man in a military uniform with pilot wings is seated at a desk in a dimly lit control room. He is wearing glasses and looking at a computer monitor. The monitor displays a map with a yellow line. In the background, another person is visible working at a similar station. The overall atmosphere is professional and focused.

Video