

SB C&S様 オンラインウェビナー

# Cisco XDR

ここが違う！ CiscoならではのXDR

Cisco Systems  
APJC XDR Sales Lead  
平岡 龍弘

2024.9.19

# 自己紹介

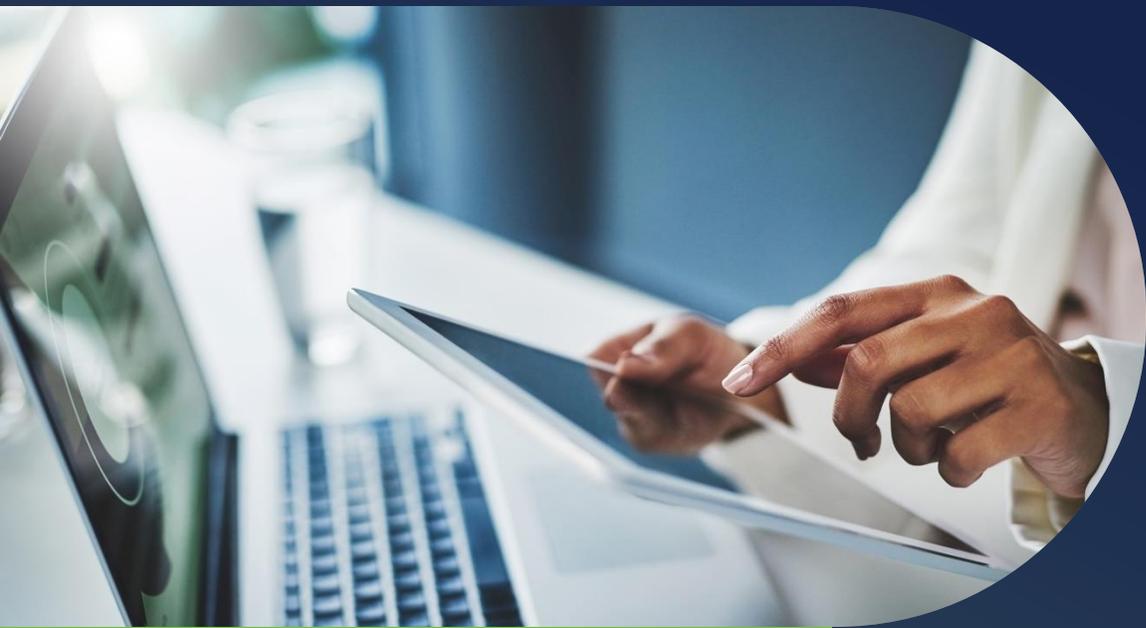


## 平岡 龍弘 Hiraoka Tatsuhiro

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。近年では特にセキュリティオペレーションへフォーカスし、セールス活動だけでなく、イベントや研究会を通じたセキュリティ対策の啓蒙活動に取り組む。



# Over View

# 防御領域のサイロ化



- T1566: Spear phishing
- T1055: Process Injection
- T1189: Drive-by Compromise
- T1570: Lateral Tool Transfer
- T1087: Account Discovery: Domain Account
- T1048: System Network Connections Discovery



# 各製品で検出したアラートすべてを対応することは難しい

TA0001: Initial Access	TA0002: Execution	TA0003: Persistence
T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1098: Account Manipulation
T1190: Exploit Public-Facing Application	T1203: Exploitation for Client Execution	T1197: BITS Jobs
T1133: External Remote Services	T1559: Inter-Process Communication	T1547: Boot or Logon Autostart Execution
T1200: Hardware Additions	T1106: Native API	T1037: Boot or Logon Initialization Scripts
T1566: Phishing	T1053: Scheduled Task/Job	T1176: Browser Extensions
T1566.001: Spearphishing Attachment	T1129: Shared Modules	T1554: Compromise Client Software Binaries
T1566.002: Spearphishing Link	T1072: Software Deployment Tools	T1136: Create Account
T1566.003: Spearphishing via Service	T1569: System Services	T1543: Create or Modify System Process
T1091: Replication Through Removable Media	T1204: User Execution	T1546: Event Triggered Execution
T1195: Supply Chain Compromise	T1047: Windows Management Instruments	T1133: External Remote Services
T1199: Trusted Relationship		T1574: Hijack Execution Flow
T1078: Valid Accounts		T1556: Modify Authentication Process
		T1137: Office Application Startup
		T1542: Pre-OS Boot
		T1053: Scheduled Task/Job
		T1505: Server Software Component

TA0006: Credential Access	TA0007: Discovery
T1557: Adversary-in-the-Middle	T1087: Account Discovery
T1110: Brute Force	T1087.002: Domain Accounts
	T1087.003: Email Accounts
	T1087.001: Local Accounts
	T1010: Application Window Discovery
	T1217: Browser Bookmark Discovery
T1555: Credential from Password Store	T1555.003: Credential from Web Browser
	T1555.005: Password Managers
	T1555.002: Security Memory
	T1555.004: Windows Credential Manager
T1212: Exploitation for Credential Access	T1482: Domain Trust Discovery
T1187: Forced Authentication	T1083: File and Directory Discovery
T1606: Forge Web Credentials	T1615: Group Policy Discovery
T1056: Input Capture	T1046: Network Service Discovery
	T1315: Network Share Discovery
	T1040: Network Sniffing
	T1201: Password Policy Discovery
	T1120: Peripheral Device Discovery
	T1069: Permission Groups Discovery
	T1069.002: Domain Groups
	T1069.001: Local Groups
T1556: Modify Authentication Process	T1057: Process Discovery
T1111: Multi-Factor Authentication Interception	T1012: Query Registry
T1621: Multi-Factor Authentication Request Generation	T1018: Remote System Discovery
T1040: Network Sniffing	T1518: Software Discovery
T1003: OS Credential Dumping	T1120: System Information Discovery
	T1614: System Location Discovery
	T1016.001: Internet Connection Discovery
	T1003.008: /etc/passwd and /etc/shadow
	T1003.006: CACHEDomain Credentials
	T1003.009: DC Sync
	T1003.004: LSA Secrets
	T1003.001: LSAS: Memory
	T1003.003: NTDS
	T1003.007: Proc filesystem
	T1003.002: Security Account Manager
T1558: Steal or Forge Kerberos Tickets	T1497: Virtualization/Sandbox Evasion
T1539: Steal Web Session Cookie	
T1552: Unsecured Credentials	
	T1552.003: Bash History
	T1552.001: Credential in Files
	T1552.002: Credential in Registry
	T1552.006: Group Policy Preferences
	T1552.004: Private Keys

TA0011: Command and Control	TA0010: Exfiltration
T1071: Application Layer Protocol	T1071.004: DNS
	T1071.002: File Transfer Protocols
	T1071.003: Mail Protocols
	T1071.001: Web Protocols
T1092: Communication Through Removable Media	T1132.002: Non-Standard Encoding
T1132: Data Encoding	T1132.001: Standard Encoding
T1001: Data Obfuscation	T1001.001: Junk Data
	T1001.003: Protocol Impersonation
	T1001.002: Steganography
T1568: Dynamic Resolution	T1573.002: Asymmetric Cryptography
T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
T1008: fallback Channels	
T1105: Ingress Tool Transfer	
T1104: Multi-Stage Channels	
T1095: Non-Application Layer Protocol	
T1571: Non-Standard Port	
T1572: Protocol Tunneling	
T1090: Proxy	T1090.004: Domain Fronting
	T1090.002: External Proxy
	T1090.001: Internal Proxy
	T1090.003: Multi-hop Proxy
T1219: Remote Access Software	T1205.001: Port Knocking
T1205: Traffic Signaling	T1102.002: Bidirectional Communication
T1102: Web Service	T1102.001: Dead Drop Resolver
	T1102.003: One-Way Communication

TA0011: Command and Control	TA0010: Exfiltration
T1071: Application Layer Protocol	T1071.004: DNS
	T1071.002: File Transfer Protocols
	T1071.003: Mail Protocols
	T1071.001: Web Protocols
T1092: Communication Through Removable Media	T1132.002: Non-Standard Encoding
T1132: Data Encoding	T1132.001: Standard Encoding
T1001: Data Obfuscation	T1001.001: Junk Data
	T1001.003: Protocol Impersonation
	T1001.002: Steganography
T1568: Dynamic Resolution	T1573.002: Asymmetric Cryptography
T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
T1008: fallback Channels	
T1105: Ingress Tool Transfer	
T1104: Multi-Stage Channels	
T1095: Non-Application Layer Protocol	
T1571: Non-Standard Port	
T1572: Protocol Tunneling	
T1090: Proxy	T1090.004: Domain Fronting
	T1090.002: External Proxy
	T1090.001: Internal Proxy
	T1090.003: Multi-hop Proxy
T1219: Remote Access Software	T1205.001: Port Knocking
T1205: Traffic Signaling	T1102.002: Bidirectional Communication
T1102: Web Service	T1102.001: Dead Drop Resolver
	T1102.003: One-Way Communication

TA0008: Lateral Movement	TA0009: Collection
T1210: Exploitation of Remote Services	T1557: Adversary-in-the-Middle
T1534: Internal Spearphishing	T1560: Archive Collected Data
T1570: Lateral Tool Transfer	T1560.002: Archive via Library
T1563: Remote Service Session Hijacking	T1560.001: Archive via Utility
T1091: Remote Services	T1563.001: SSH Hijacking
	T1021.003: Distributed Component OS
	T1021.001: Remote Desktop Protocol
	T1021.002: SMB/Windows Admin Shares
	T1021.004: SSH
	T1021.005: VNC
	T1021.006: Windows Remote Management
T1091: Replication Through Removable Media	T1025: Data from Removable Media
T1072: Software Deployment Tools	T1074.001: Local Data Staging
T1080: Taint Shared Content	T1074.002: Remote Data Staging
T1550: Use Alternate Authentication Methods	T1114.003: Email Forwarding Rule
	T1114.002: Remote Email Collection
	T1056.004: Credential API Hooking
	T1056.001: Keylogging
	T1056.003: Web Portal Capture
	T1113: Screen Capture
	T1125: Windows Font Cache

# アタックチェーン全体を見渡せて優先付けできるソリューションが必要



Cisco XDR



Built on the Cisco Security Cloud platform

# XDR ≠ SIEM

## XDR

ニアリアルタイム

相関

より高度な検出・対処

人の介在（低）

## SIEM

数時間、日～週（後日評価）

集約

イベント監視・ログ監視

人の介在（高）

# 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



インシデントの優先付け  
相関関係を分析  
対応のワークフロー

### 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

TALOS



500

調査員



AI

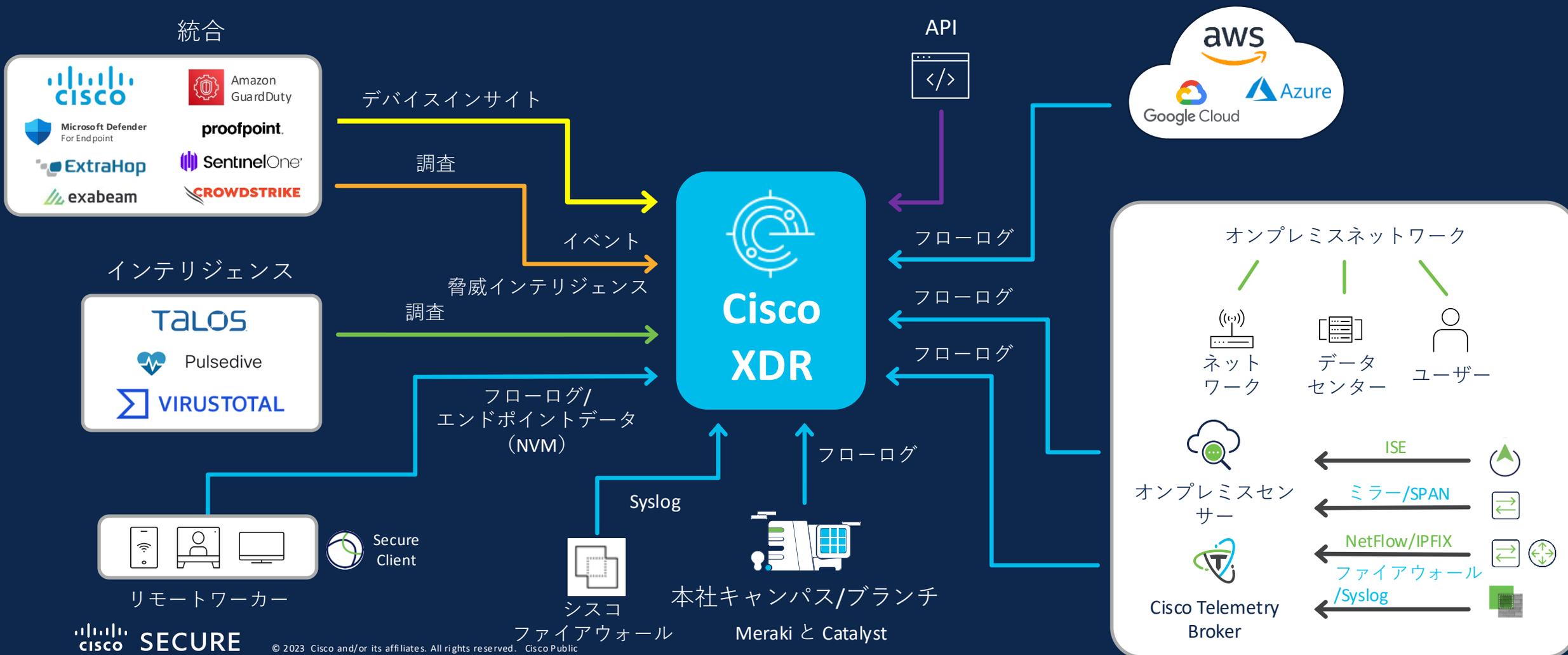
powered algorithms



5500億/1日

分析対象のセキュリティイベント

# テレメトリソースの特徴



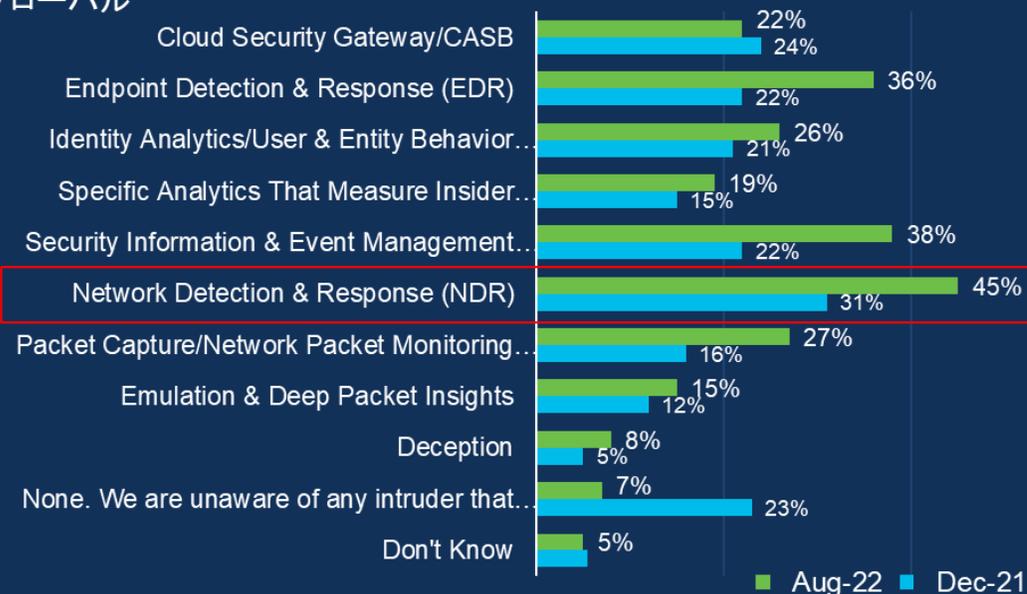
# ネットワークを監視することの重要性

## お客様が重要視するテレメトリデータソース

	カウント	シェア
 Endpoint	255	85.0%
 Network	226	75.3%
 Firewall	207	69.0%
 Identity	191	63.7%
 Email	179	59.7%
 DNS	140	46.7%
 Public Cloud	137	45.7%
 Non-Security Sources	36	12.0%

## ランサムウェアを実行する前に、検出/対処できるセキュリティ技術は・・・？

グローバル



IDC #US49731922 (September 2022)  
 Source: Future Enterprise Resiliency & Spending Survey – Wave 7,  
 IDC, August 2022, n=241; December 2021, n=361

# 究極の統合エージェント

## Secure Client

ユニファイドエージェント



### ネットワーク セキュリティ

- Secure Firewall & IPS
- ISE
- Secure Network Analytics

### ユーザ・エンドポイント セキュリティ

- Secure Endpoint

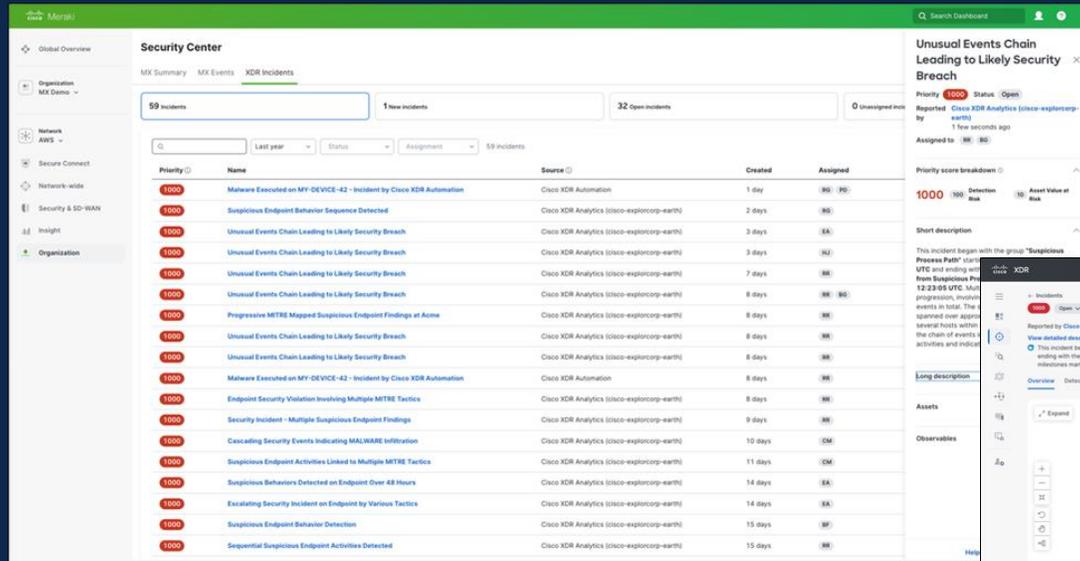
### クラウドアクセスセキュリティ

- Umbrella
- Secure Access

### セキュリティオペレーション

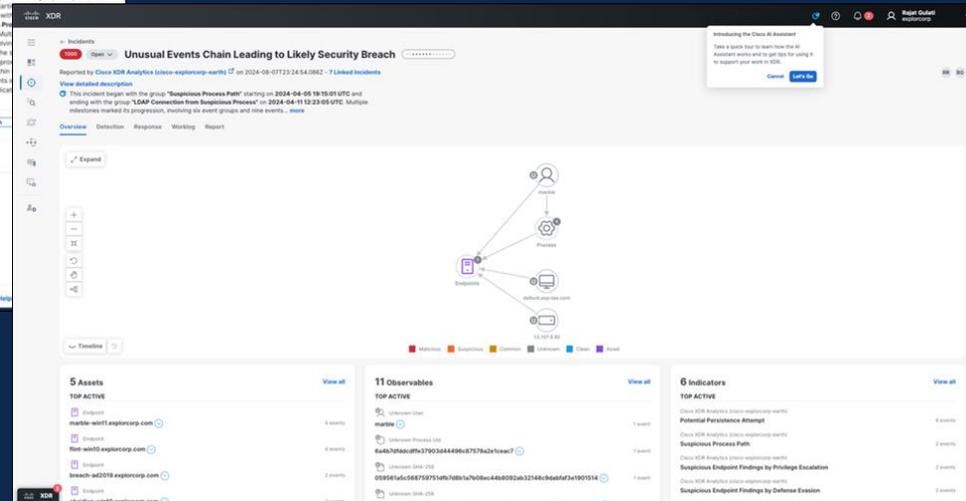
- Cisco XDR
- Thousand Eyes

## ワンタッチでMerakiのログデータをシームレスにXDRへ統合



Cisco XDR 内のインシデントビューに直感的に移動

管理者は Meraki ダッシュボード内で Cisco XDR インシデントに直接アクセス



# Cisco XDR 主要な戦略的パートナー

緑字の製品が対応済み  
2024年8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

- Microsoft Sentinel
- Exabeam
- Google Chronicle
- LogRhythm
- Sumo Logic
- Splunk
- 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

# Cisco製品 of インテグレーション

## User Endpoint

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

## Application and Identity

- Duo

## Cloud

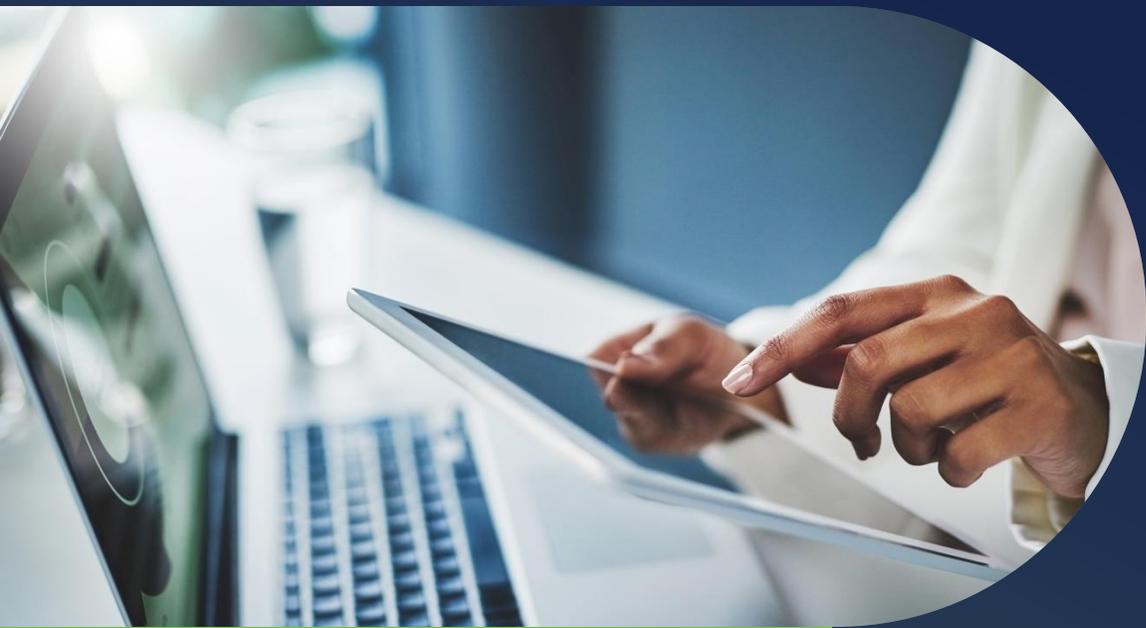
- Umbrella
- Secure Access
- Secure Workload
- Attack Surface Management

## Network

- Secure Network Analytics
- Secure Firewall
- Meraki
- ISE
- Defense Orchestrator
- Cisco Catalyst Center

## VM

- Cisco Vulnerability Management



# ライセンス

# ライセンス

Cisco XDR  
Essentials

Full featured XDR

Cisco XDR  
Advantage

Full featured XDR

+3<sup>rd</sup> Party Telemetry

Cisco XDR  
Premier

Full featured XDR

+3<sup>rd</sup> Party Telemetry

+Managed Services

# Cisco XDR Premier



24H365Dの  
モニタリング

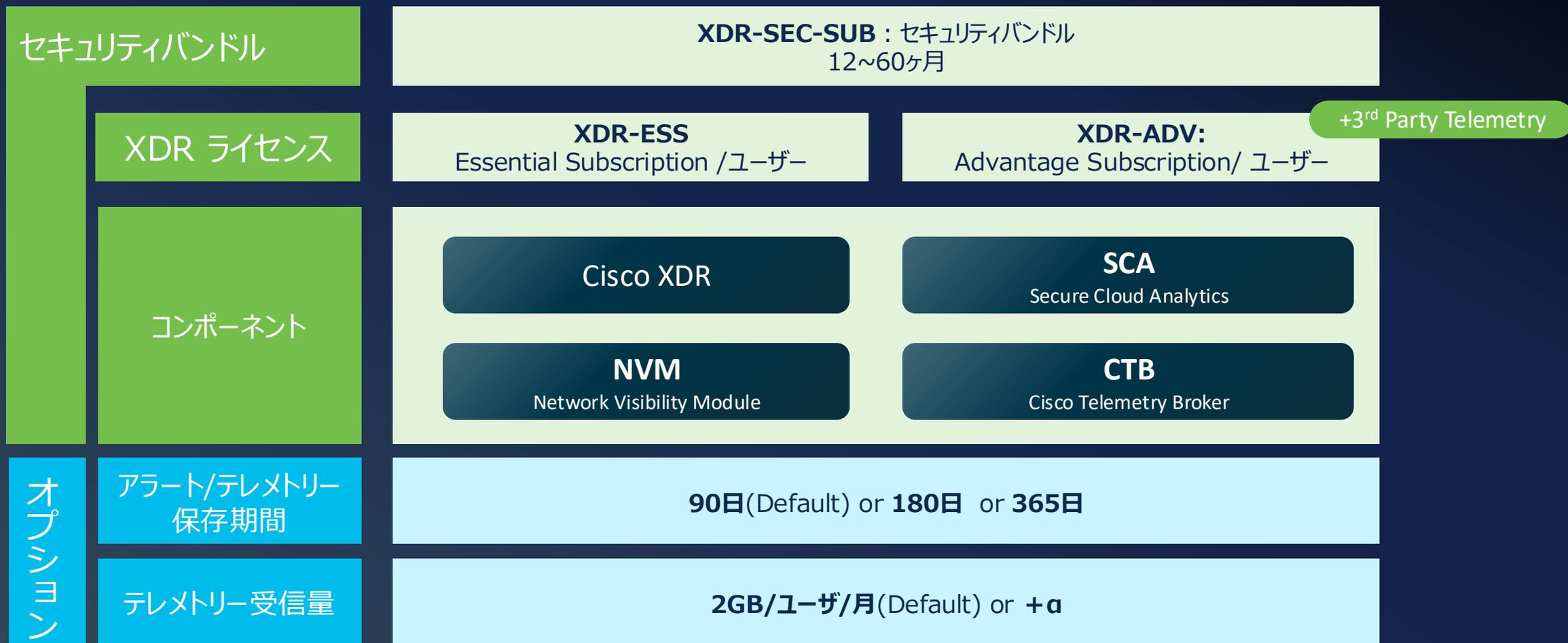


インシデント  
レスポンス



セキュリティ  
アセスメント

# Cisco XDR ライセンス体系



# 業界別のライセンス

ヘルスケア

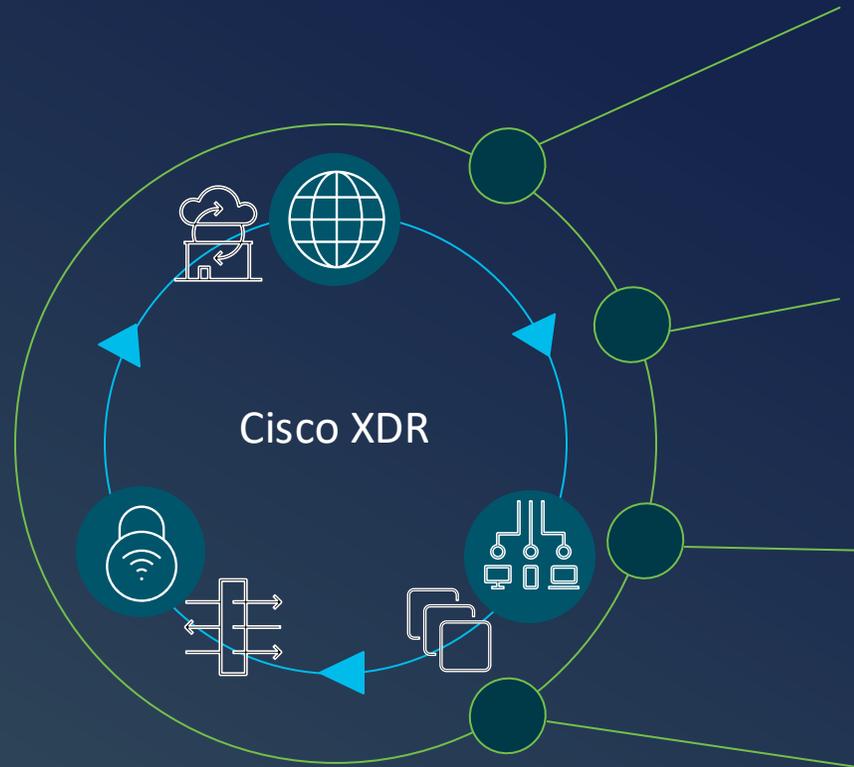
製造業

文教/大学

小売業

Cisco 営業担当へご相談ください！

# Why Cisco XDR ?



## 相関分析

自動相関によるチューニングレス  
アラートチェーンやリレーションマップなどの卓越した可視性  
優れた操作性

## インシデントの優先付け

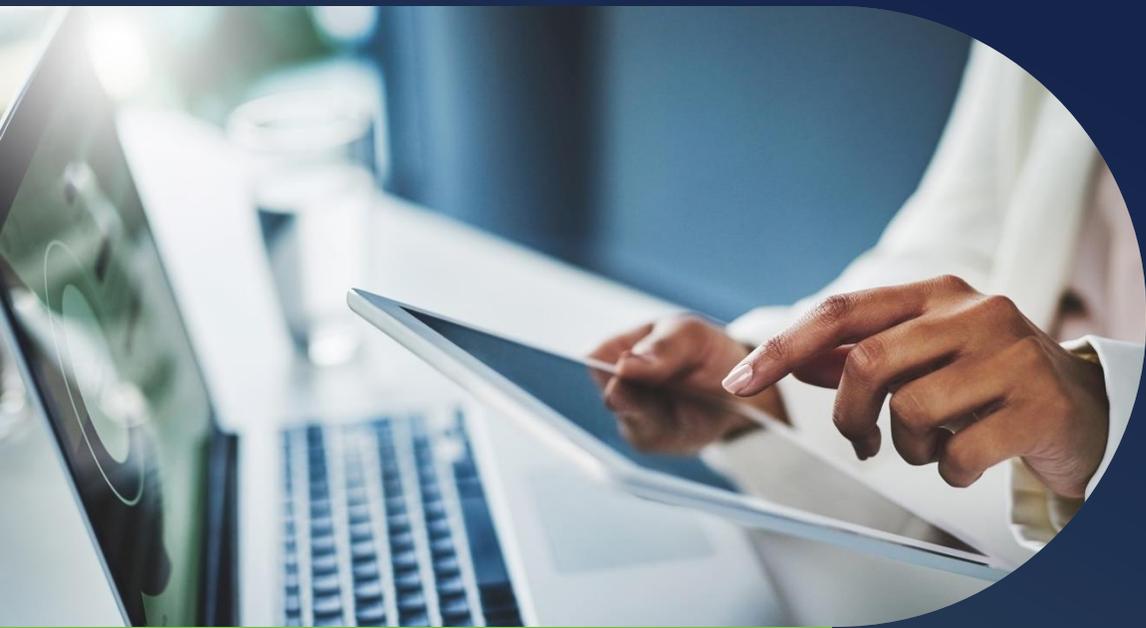
Financial Impact をベースにした独自の優先アルゴリズム\*  
無償でのTalos Feed活用  
\*4つの特許を申請中

## 対処のワークフロー

無償でのSOAR活用  
実際の現場で必要とされた即効性の高いプリセットワークフロー

## 広範囲なテレメトリ収集

NDR機能を標準装備  
端末から直接ネットワークテレメトリを収集可能 (Secure Client利用時)  
ネイティブなサードパーティーテレメトリ



# Cisco XDR事例



# 前橋赤十字病院様

## Cisco XDR with Cohesity

2024年9月13日

[Leave a Comment](#)



セキュリティ

シスコと前橋赤十字病院とユニアデックス  
が病院内ネットワークで連携

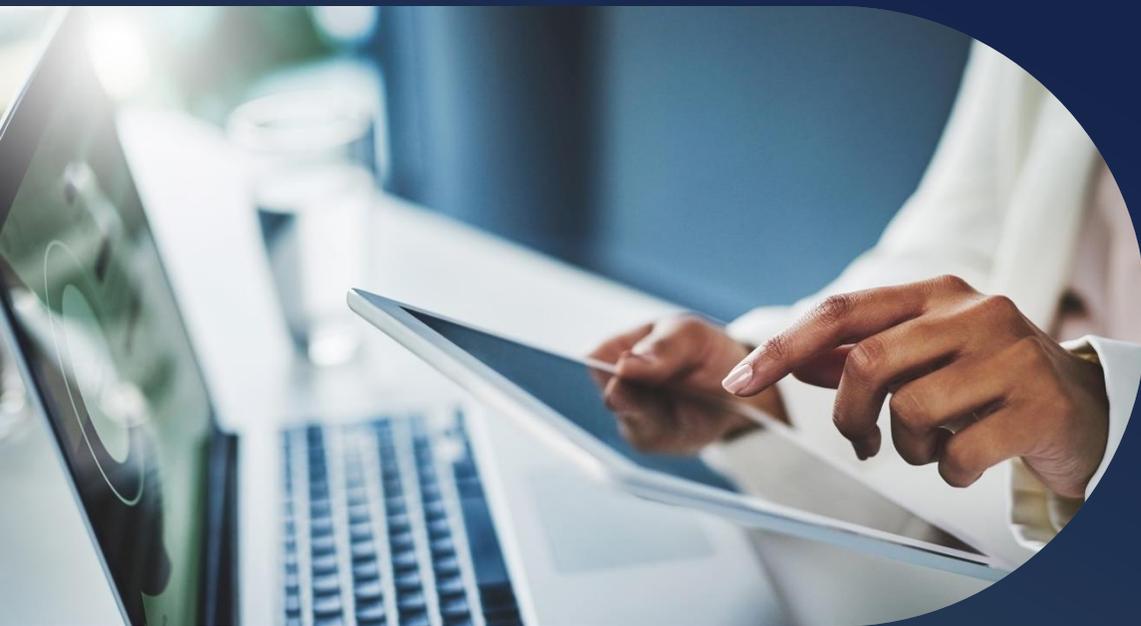
[Press Release](#)

病院内ネットワークのセキュリティ対策・SOC実現に取り組む  
— Cisco XDR導入により、ランサムウェア等の脅威の早期検知を実現 —

概要

[シスコと前橋赤十字病院とユニアデックスが病院内ネットワークで連携](#)





# Update New Feature



# Cisco AI Assistant for Security

NEW: XDR

## Secure Access

**Let's create some access rules today, shall we?**

Choose from a suggestion below or use the text field to create access rules by telling me a source, destination, and rule action. Rules added using the assistant include the default security settings and are disabled by default.

**Create a single rule**  
Allow <User> and <User Group> access to <Private Resource>

**Create multiple rules**  
Allow <User Group> and Block <User> access to <Content Category>

Type your rule here

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

## Firewall

How do I schedule a recurring backup?

To schedule a recurring backup, follow the steps below:

1. In the **Frequency** field, select daily, weekly, or monthly backup.
2. Select the time of day, in 24-hour time, you want the backup to occur. Note that you schedule the time in Coordinated Universal Time (UTC).
  - For weekly backups: Check the days of the week on which you want the backup to occur.
  - For monthly backups: Click in the **Days of Month** field and add whichever days of the month you want to schedule the backup. Note: If you enter day 31 but a month doesn't have 31 days in it, the backup will not take place.
3. Give the scheduled backup time a name and a description.
4. Click **Save**.

Please note that changing the default recurring backup schedule does not change any existing scheduled backups or recurring backup schedules.

**Sources**

1. [Configure a Default Recurring Backup Schedule](#)

Which countries are the access control policies blocking traffic to?

The **Close Incident** action is in progress. You can check on the status of this action by viewing it in [Workflow](#).

**AI Assistant**

The **Close Incident** action started by **sam@explorcorp.com** was completed successfully and the incident status changed to **Closed**. This action has been added to the [Worklog](#).

**Recommended Actions**

Identification   Containment   Eradicate (3)   Recovery

Based on the current incident state, the following actions are recommended.

## Hypershield

Prove the Distributed Exploit Shield is working

This Distributed Exploit Shield will block **httpd** from executing a script in **/tmp**, thereby precluding remote code execution.

We've tested this in the shadow dataplane and no deviations within the thresholds were found.

[View test results](#)

**Are there public exploits available for the CVE?**

[View More](#)

Ask a question

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

**Common connections**

# Cisco AI Assistant for Cisco XDR

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

The screenshot displays the Cisco XDR console. At the top, it shows the incident name 'Wizard Spider (Ron Weasley has Aracnaphobia) Slate-WIN11.explorcorp.com' with a severity of 1000. Below this, there's a network diagram showing connections between various entities like 'Devices', 'File Paths', and 'Endpoints'. At the bottom, there are two summary panels: '7 Assets' with a 'TOP ACTIVE' list including 'Slate-WIN11.explorcorp.com' (36 events) and 'Marble-WIN11.explorcorp.com' (25 events); and '62 Observables' with a 'TOP ACTIVE' list including 'Malicious SHA-256' and 'Common SHA-256'.

The screenshot shows the 'Cisco AI Assistant' chat interface. It features a header with a menu icon, the title 'Cisco AI Assistant', and window controls. The chat area shows a message from 'SA You' with the text 'Assign different users'. Below this, a confirmation message from the AI Assistant states: 'Jim Gordon, Selina Kyle, and Bruce Wayne have been successfully added to the incident. This action has been added to the Worklog.' Underneath, there are 'Recommended Actions' with a progress indicator showing four steps: 1. Identification, 2. Containment, 3. Eradicate, and 4. Recovery. Two buttons are visible: 'Confirm Incident' and 'Contain Incident: Assets'. At the bottom, there is a text input field 'Ask the AI Assistant a question' with a blue arrow button.

# AI help for the SOC analystst

## クリアでシンプルなDescription

- インシデントのShort DescriptionとLong Descriptionを自動生成
- 複数のイベントソースから関連付けられた攻撃の内容理解を補助

The screenshot displays a security incident response interface. At the top, there is a user profile for 'Remi Business Corp, Inc' and a notification bell. The incident details include: Priority 10, Status Closed, Reported by Secure Endpoint, Assigned SB, and MITRE N/A. The main title is 'Malicious Email sent to Multiple Users'. A 'Description' section contains two paragraphs: one detailing the AWS CloudTrail event on May 24, 2023, and another summarizing the incident as high priority. A 'Short Description' section contains the text 'CloudTrail Watchlist Hit for Cis Lab (Earth)'. A 'Long Description' section is present but empty. An 'Assets' section is also present but empty. A callout box states 'This description was generated by Cisco AI'. A 'Close' button is located at the bottom right.

# AI help for the SOC analystst

## Incident Summary Reporting

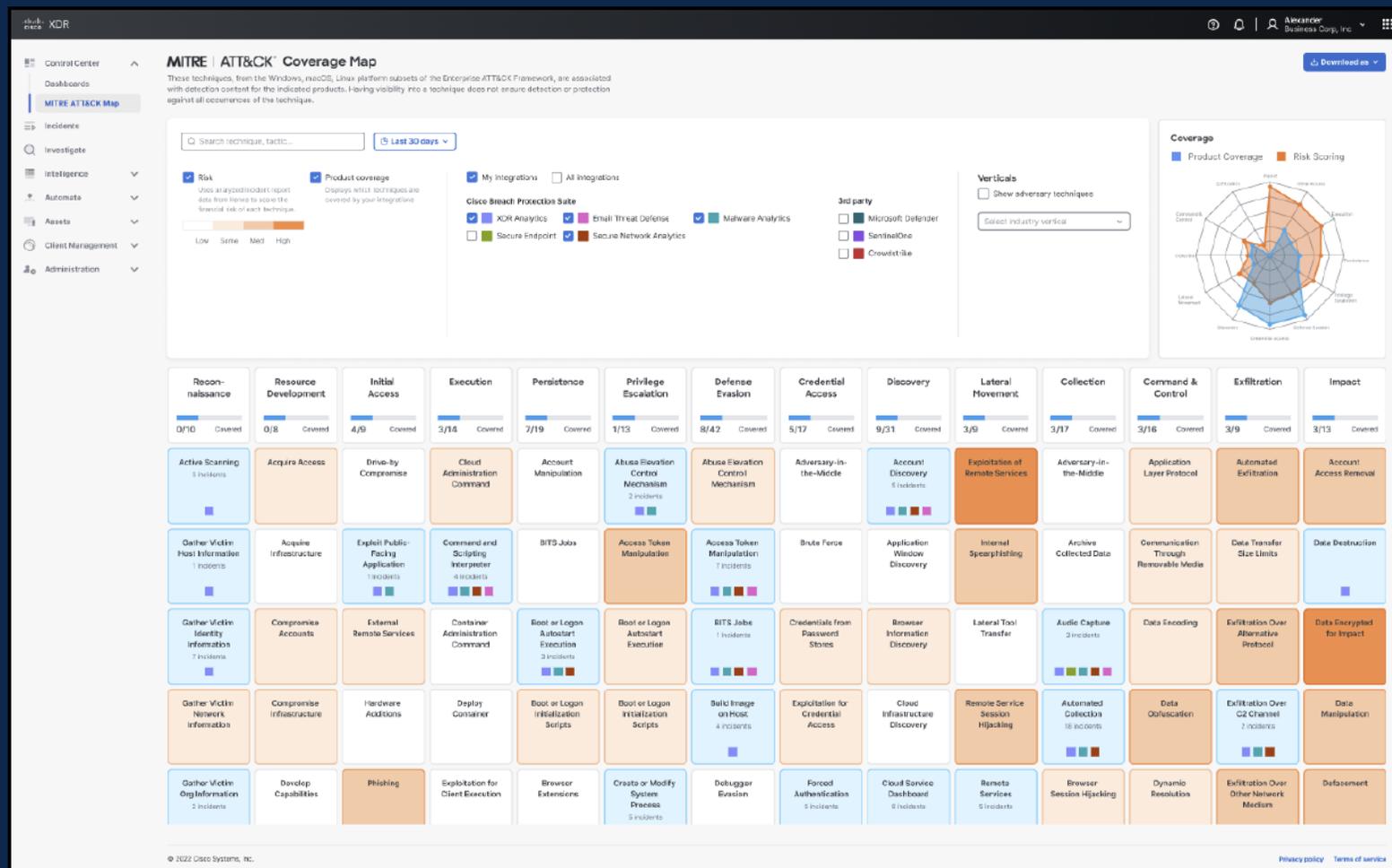
- インシデントが解決されると、生成AIがインシデント要約レポートを作成
- 関係者と共有するためにpdfにエクスポートも可能

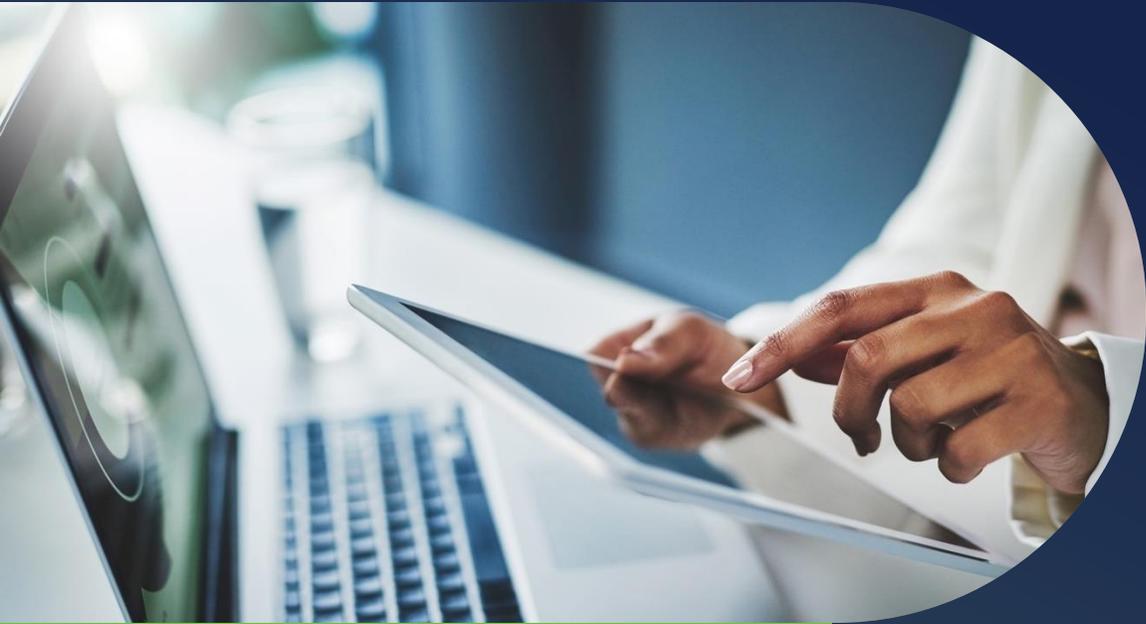
The screenshot displays a SOC dashboard interface. At the top right, there is a user profile for 'Remi Business Corp, Inc'. The main content area shows an incident titled 'Malicious Email Sent to Multiple Users' with a status of 'New' and a count of '990'. Below the title, it indicates the incident was 'Created via Umbrella 2m ago - Linked Incidents' and provides a link to 'View long description'. The dashboard has tabs for 'Overview', 'Detection', 'Response', and 'Worklog', with 'Response' currently selected. A sidebar on the left lists incident stages: Identification, Containment, Eradication, and Recovery. A central modal window titled 'Incident Report' is open, showing a 'Preview' of a report for the selected incident. The report includes an 'Executive Summary' and an 'Investigation Summary'. The 'Executive Summary' describes the execution of a PowerShell script on thirteen systems, identifying the use of Metasploit and a compromised service account. The 'Investigation Summary' outlines the primary concern of containing and remediating a Ryuk ransomware infection. At the bottom of the modal, there are 'Close' and 'Create PDF' buttons. The background dashboard also shows a list of recent incidents with 'View' and 'Export' options.

# Accelerate MITRE ATT&CK Coverage

## Heatmap & Prioritization

- ヒートマップでMITRE ATT&CKのカバー範囲を素早く把握
- フィルタリングにより、最も広いカバー範囲と最も大きなギャップのある場所を把握
- カバレッジを最適化するために必要なツールやテレメトリのタイプを推奨





# Cisco XDR with Splunk

# Splunkの買収を合意

280億ドル = 約4兆円

- 2023年 9月 21日にCiscoはSplunkの買収意向を発表
- 現時点での買収完了は2024年後半目処（2024年 第三四半期見込み）
- 買収が完了するまでは、Cisco と Splunk は独立した企業として事業を継続（現在のオファーを提供）
- 詳細は買収完了後に発表

## 本買収による狙い

デジタルレジリエントの実現

セキュリティとオブザーバビリティ機能の拡張

# Cisco XDR with Splunk

行動分析、脅威インテリジェンス、拡張検知・対応（XDR）、SOARなどの機能を統合することで、従来のSIEMの機能を超えて、包括的なSOCプラットフォームを提供

## TDIR

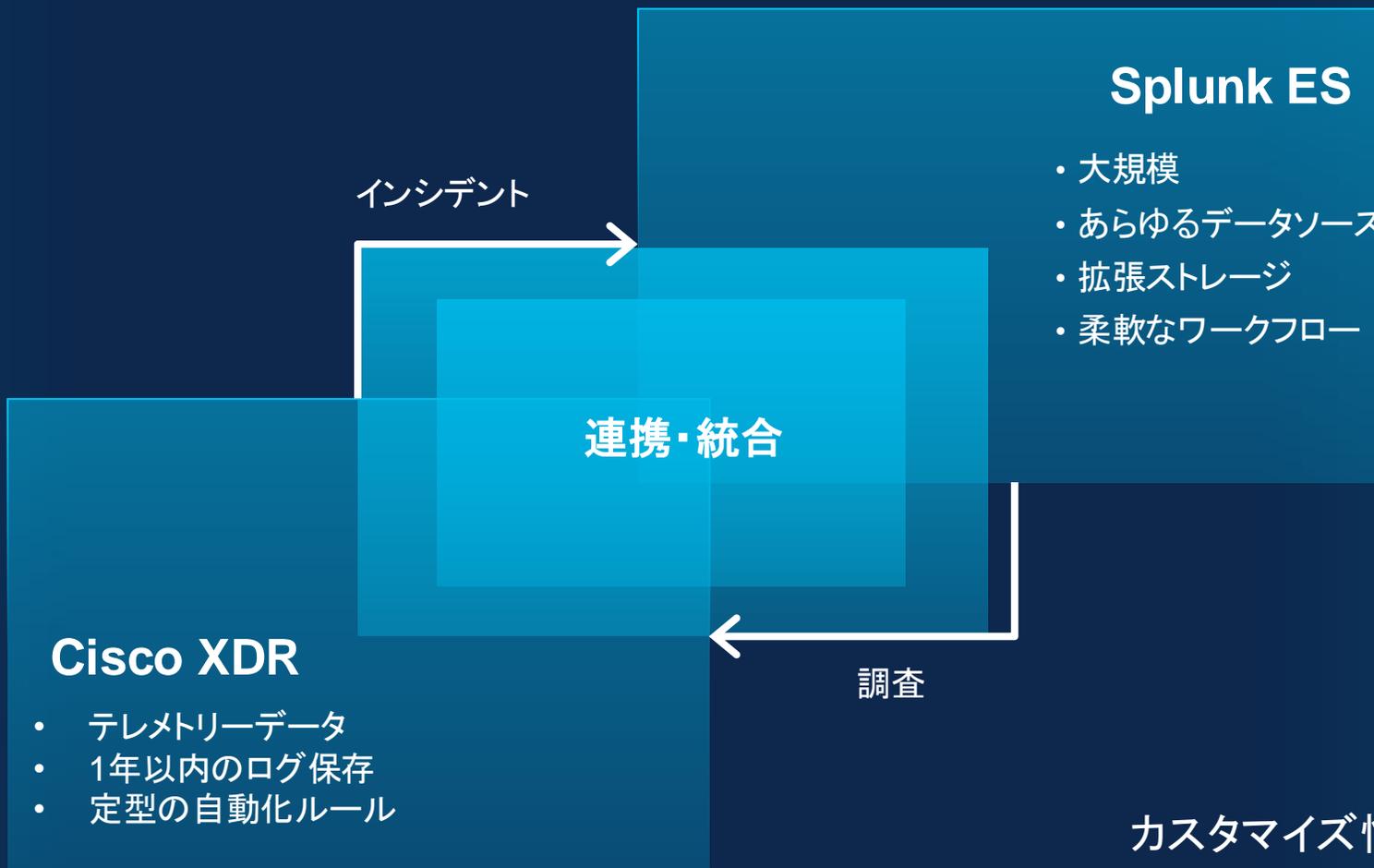
### Threat Detection, Investigation, and Response



# Cisco XDR + Splunk ES 連携を発表

## 多様なセキュリティオペレーションの形態に対応

規模・拡張性



# セキュリティ成熟度による使い分け

要素	成熟度: Low / Mid	成熟度: Mid / High
SOCメンバーの数	10人以下	10人以上
カスタムの要素	雛形を利用	カスタム
主なユースケース	インシデント レスポンス	スレット ハンティング
提案プロダクト	Cisco XDR	Splunk ES (Main) Cisco XDR (Join)

The Cisco logo, consisting of a stylized signal icon above the word "CISCO" in a sans-serif font.

CISCO SECURE