cisco SECURE

cisco The bridge to possible

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

標的型
メール

疑わしいサイト
へのアクセス

ユーザー端末へ
プロセスを作成

リモート
アクセス

T1566: Spear phishing

T1055: Process Injection

T1189: Drive-by Compromise

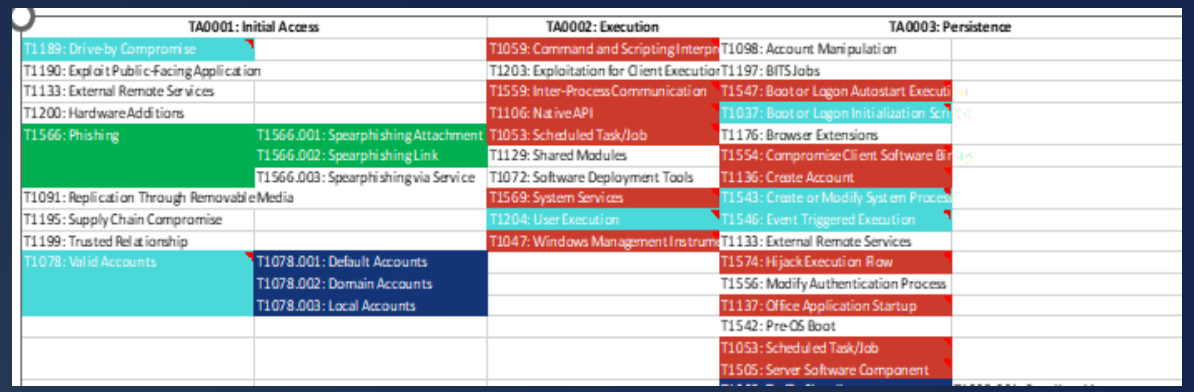
T1087: Account Discovery: Domain Account

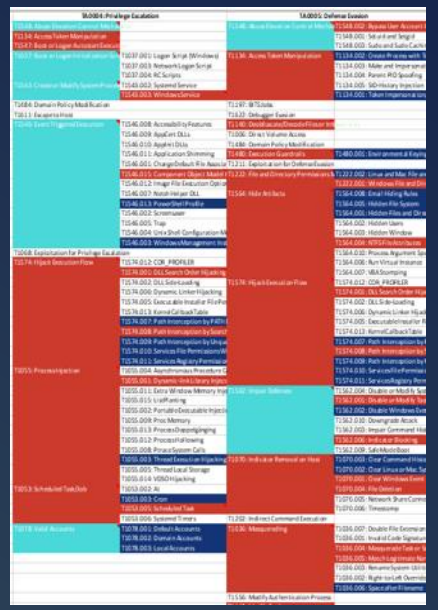
T1570: Lateral Tool Transfer

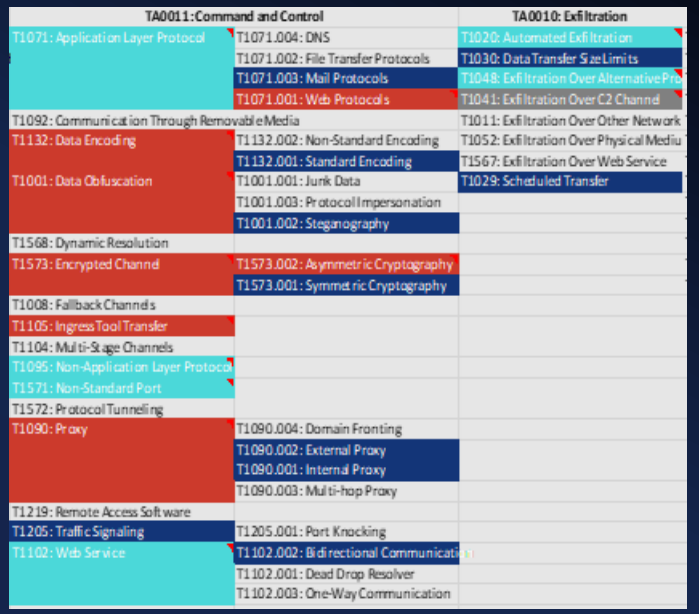
T1048: System Network Connections Discovery

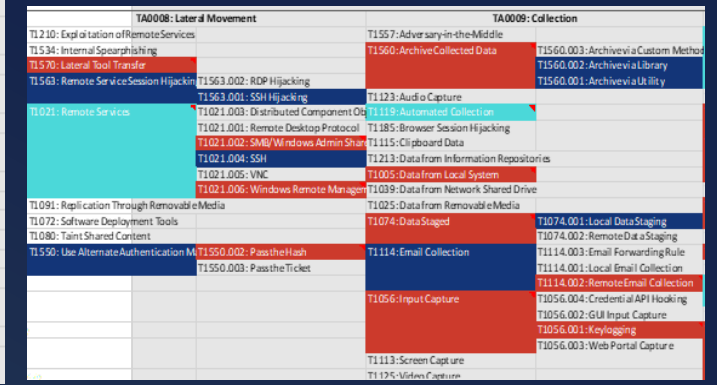
Vendor A	Vendor B	Vendor C	Vendor D	Vendor E

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

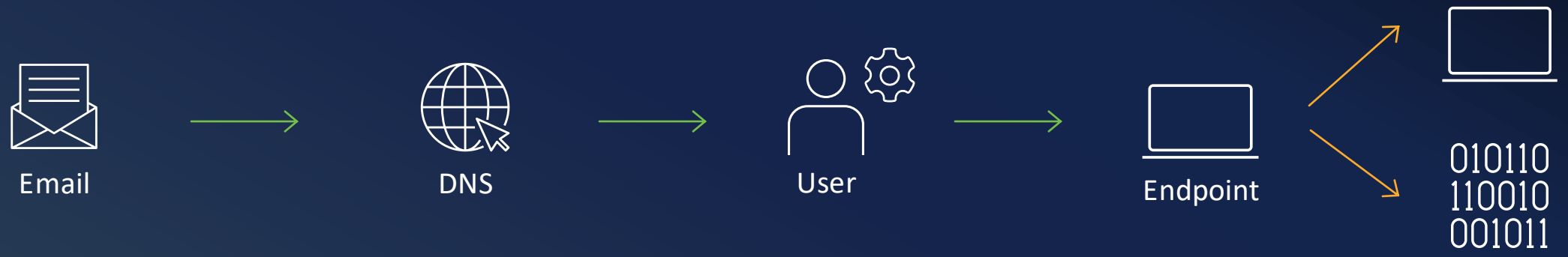








アタックチェーン全体を見渡せて優先付けできるソリューションが必要



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

ユーザ・デバイス

テレメトリー情報

Cisco XDR

インシデントの優先付け

相関関係を分析

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

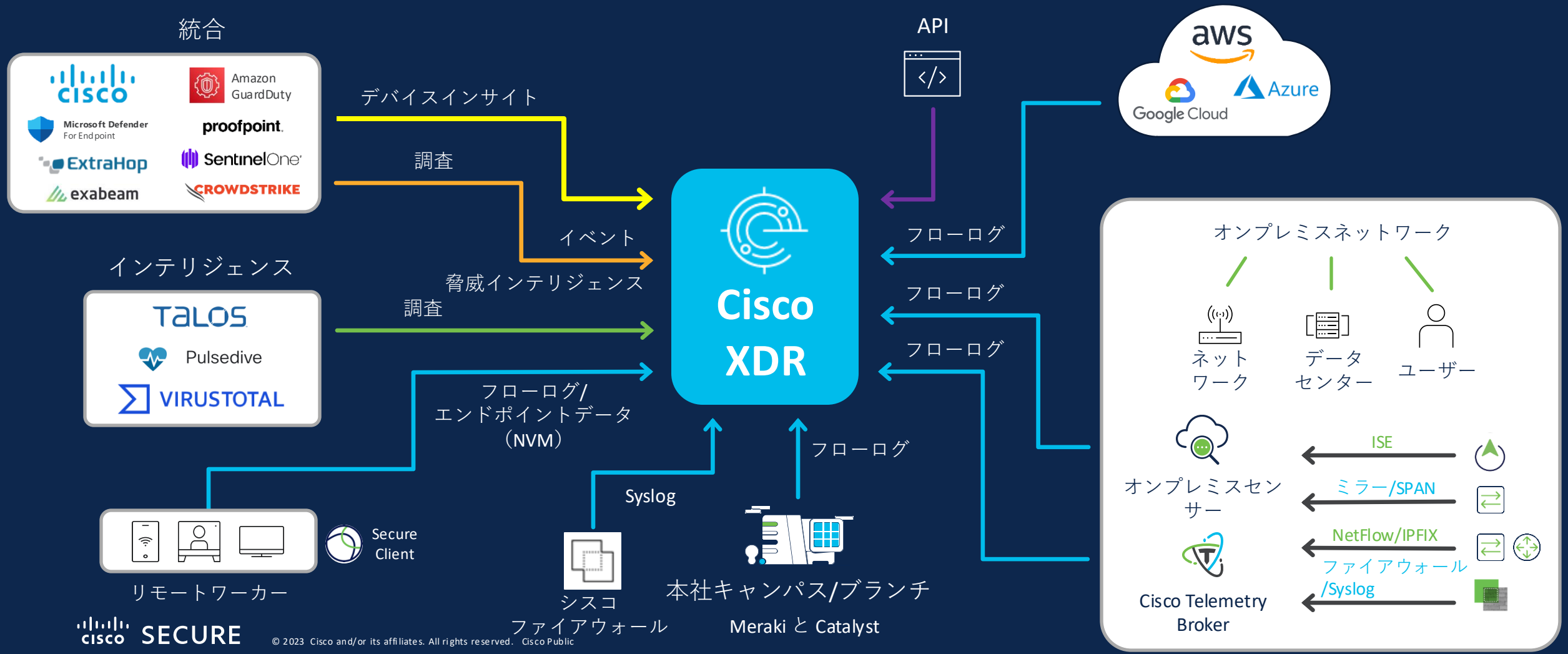
ネットワーク

自動隔離

ユーザ・デバイス

Talos powers the Cisco portfolio with intelligence

テレメトリソースの特徴



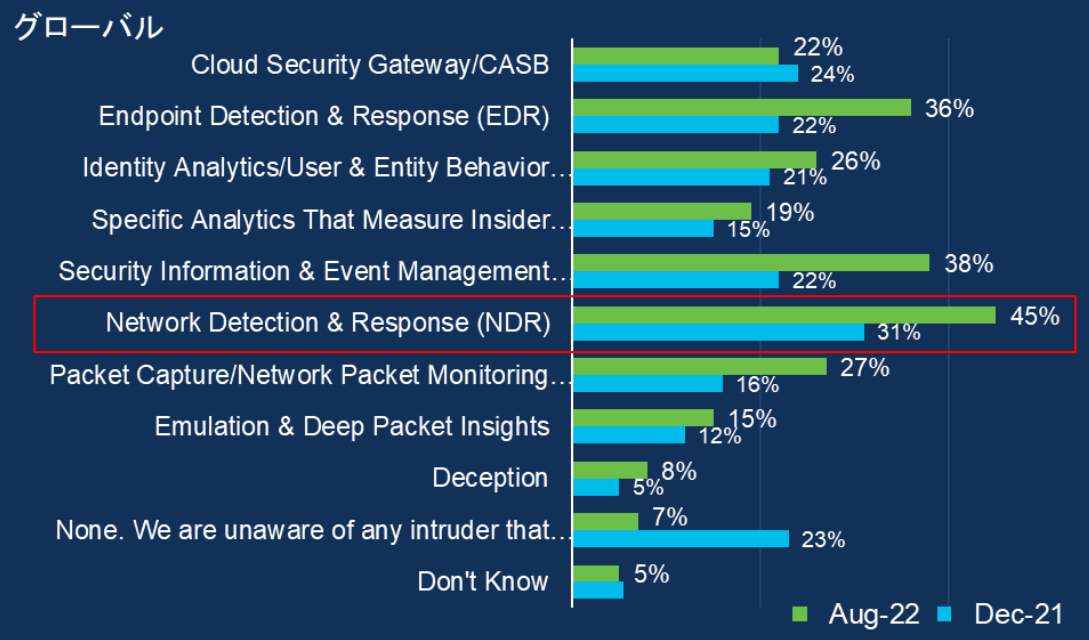
cisco SECURE

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ーデータソース

	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・・・？

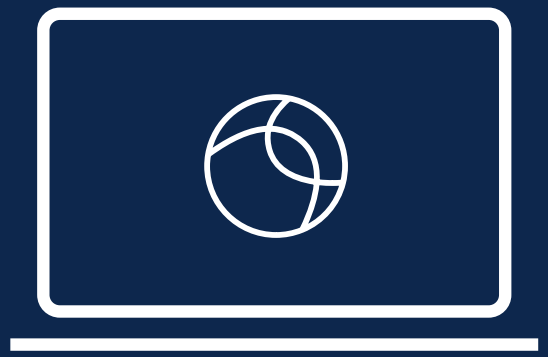


IDC #US49731922 (September 2022)
Source: Future Enterprise Resiliency & Spending Survey – Wave 7, IDC, August 2022, n=241; December 2021, n=361

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

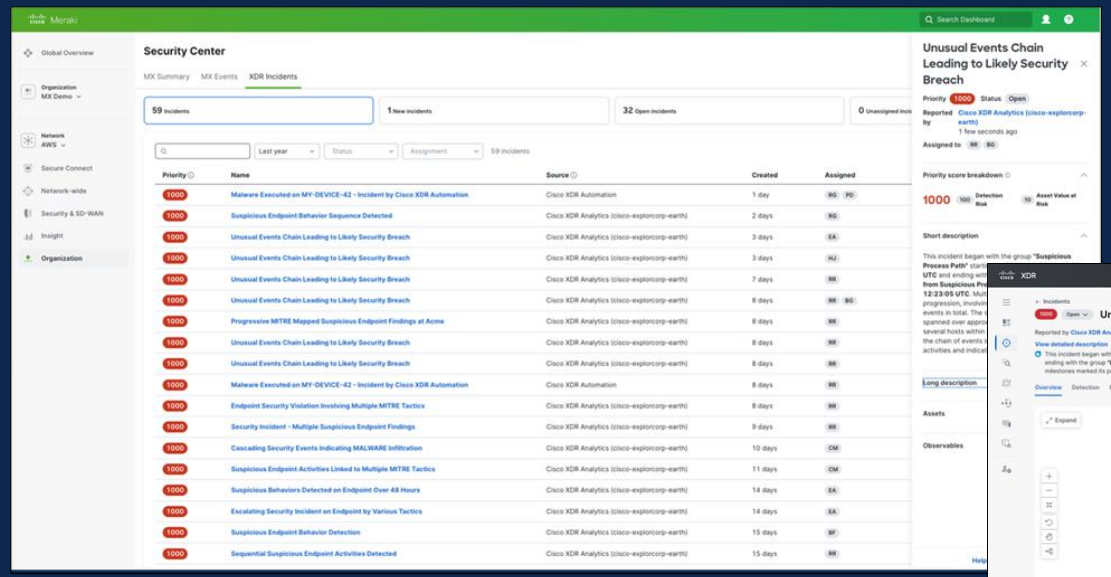
セキュリティオペレーション

- Cisco XDR
- Thousand Eyes

Cisco XDR with Meraki

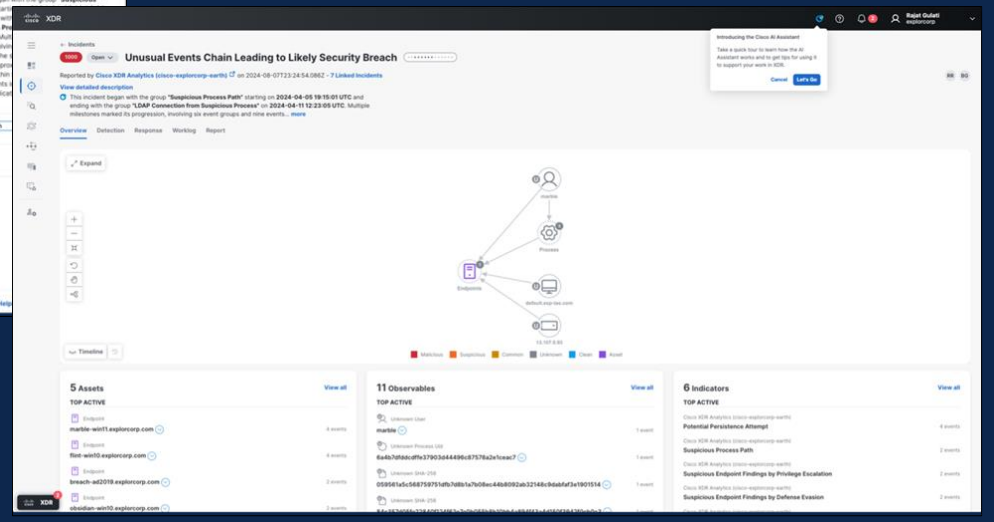
Beta

ワンタッチでMerakiのログデータをシームレスにXDRへ統合



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 内のインシデントビューに直感的に移動



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-Forece Exchange
- alphaMountain.ai
- Amazon GuradDuty

Data Cloud
- Cohesity
- Rubrik

Cisco製品のインテグレーション

緑字の製品が対応済み
2024年8月現在

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	Cisco XDR Advantage	Cisco XDR Premier
Full featured XDR	Full featured XDR	Full featured XDR
	+3rd Party Telemetry	+3rd Party Telemetry
		+Managed Services

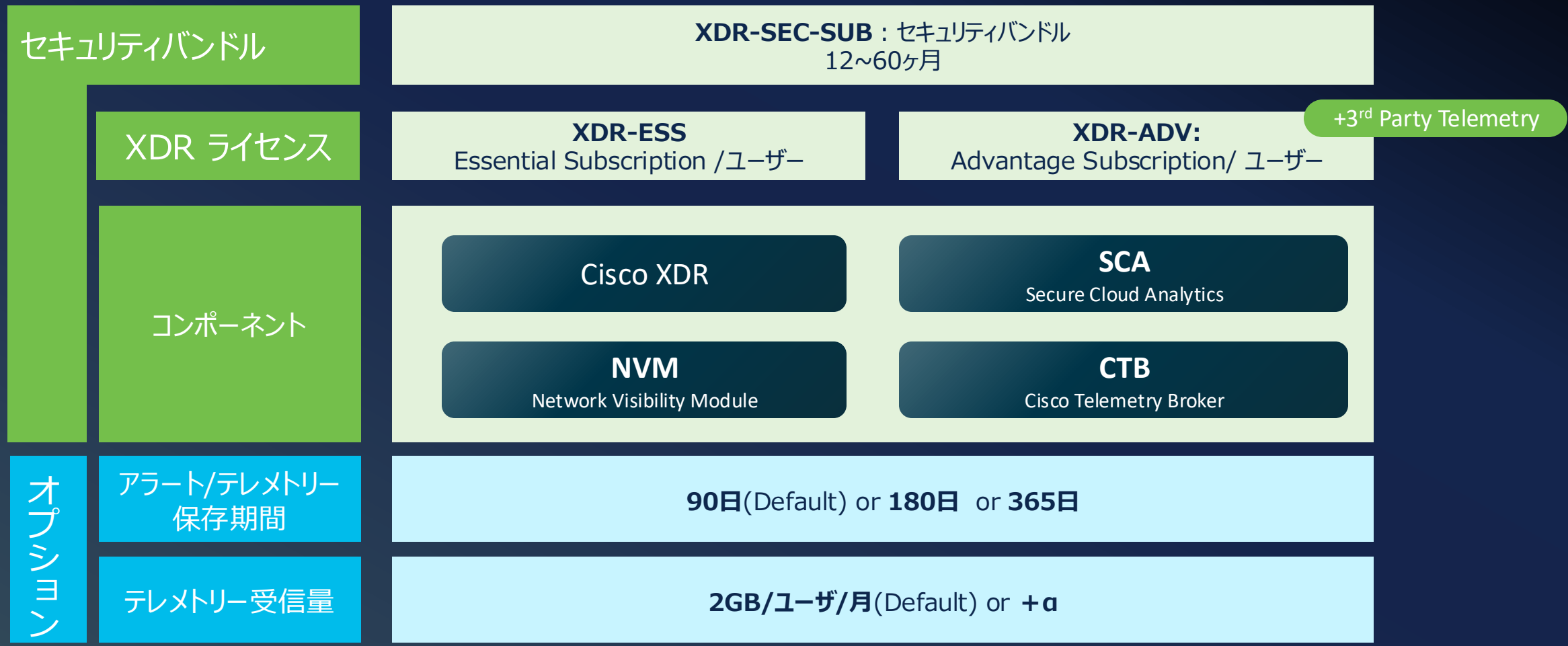
Cisco XDR Premier

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

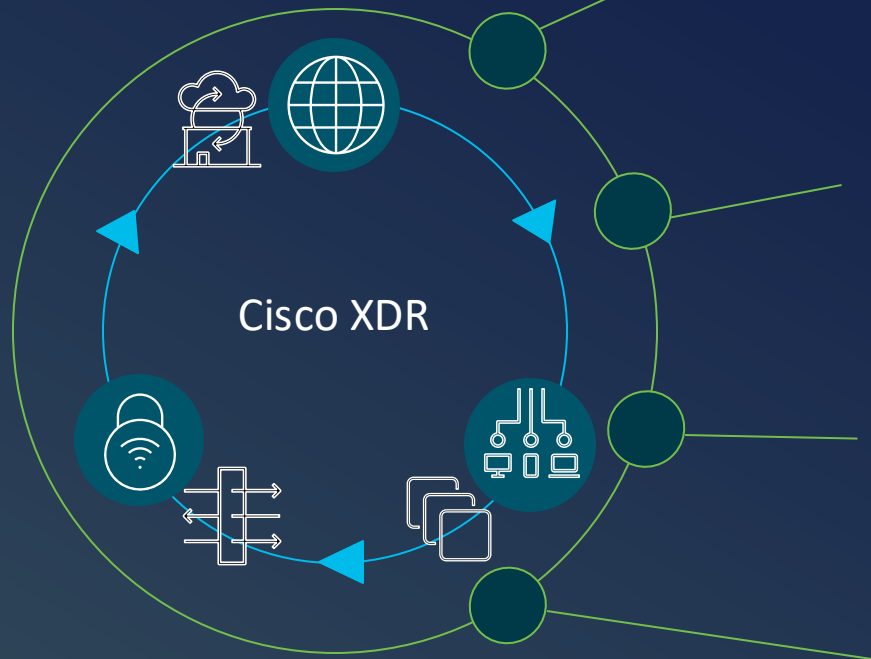
製造業

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

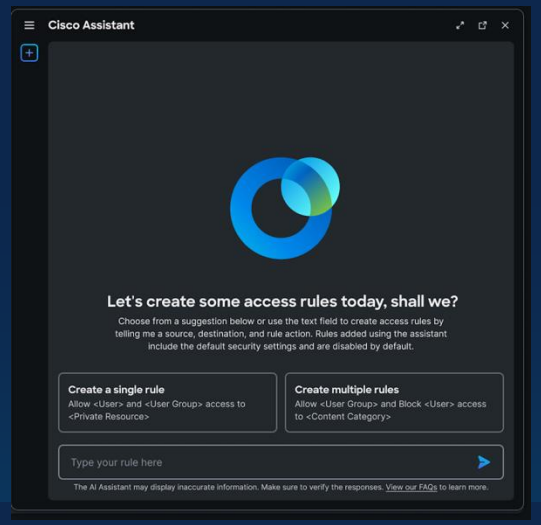
シスコと前橋赤十字病院とユニアデックスが病院内ネットワークで連携

Update

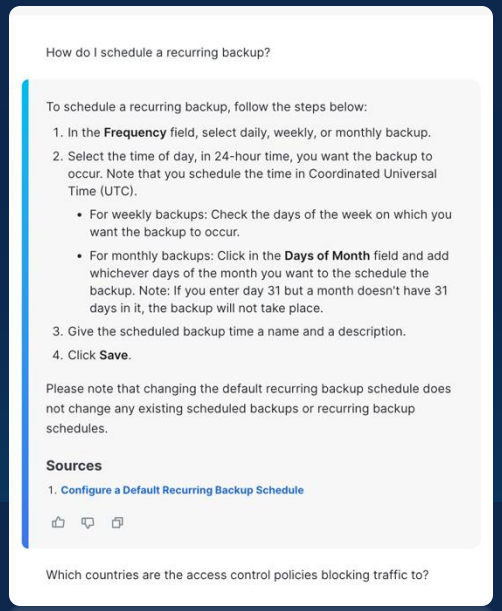
New Feature

Cisco AI Assistant for Security

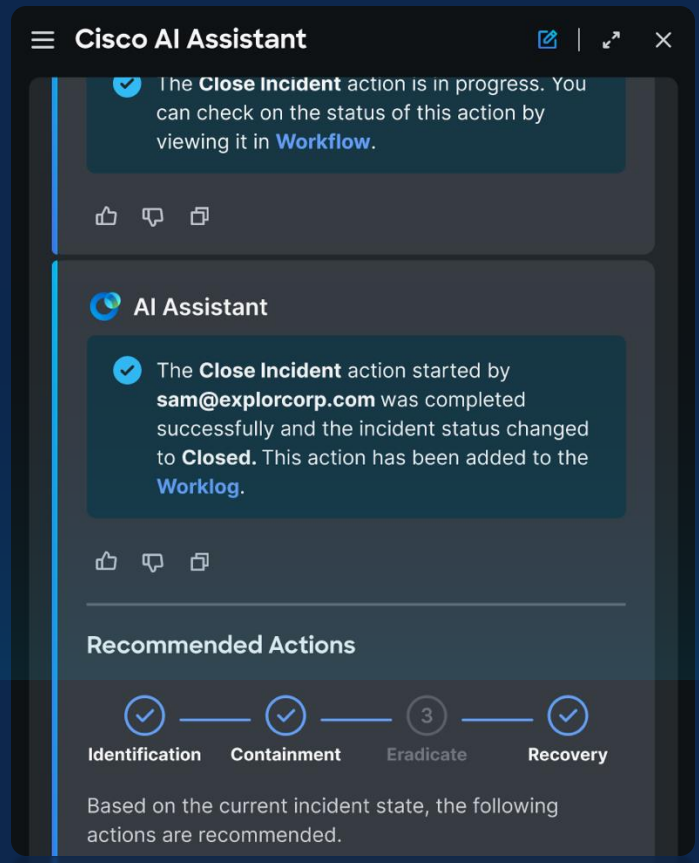
Secure Access



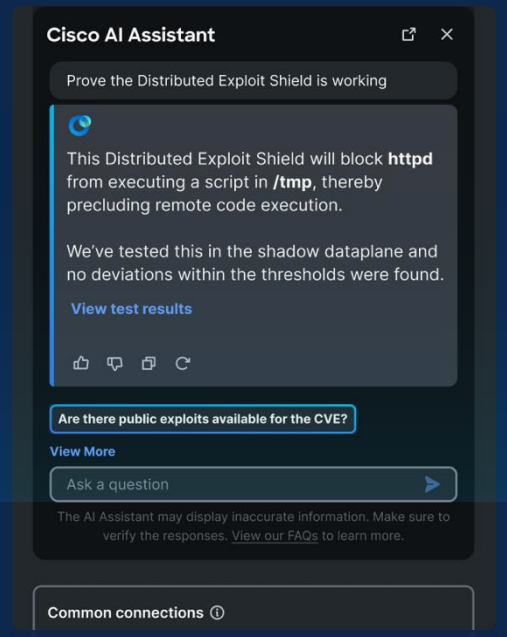
Firewall



NEW: XDR



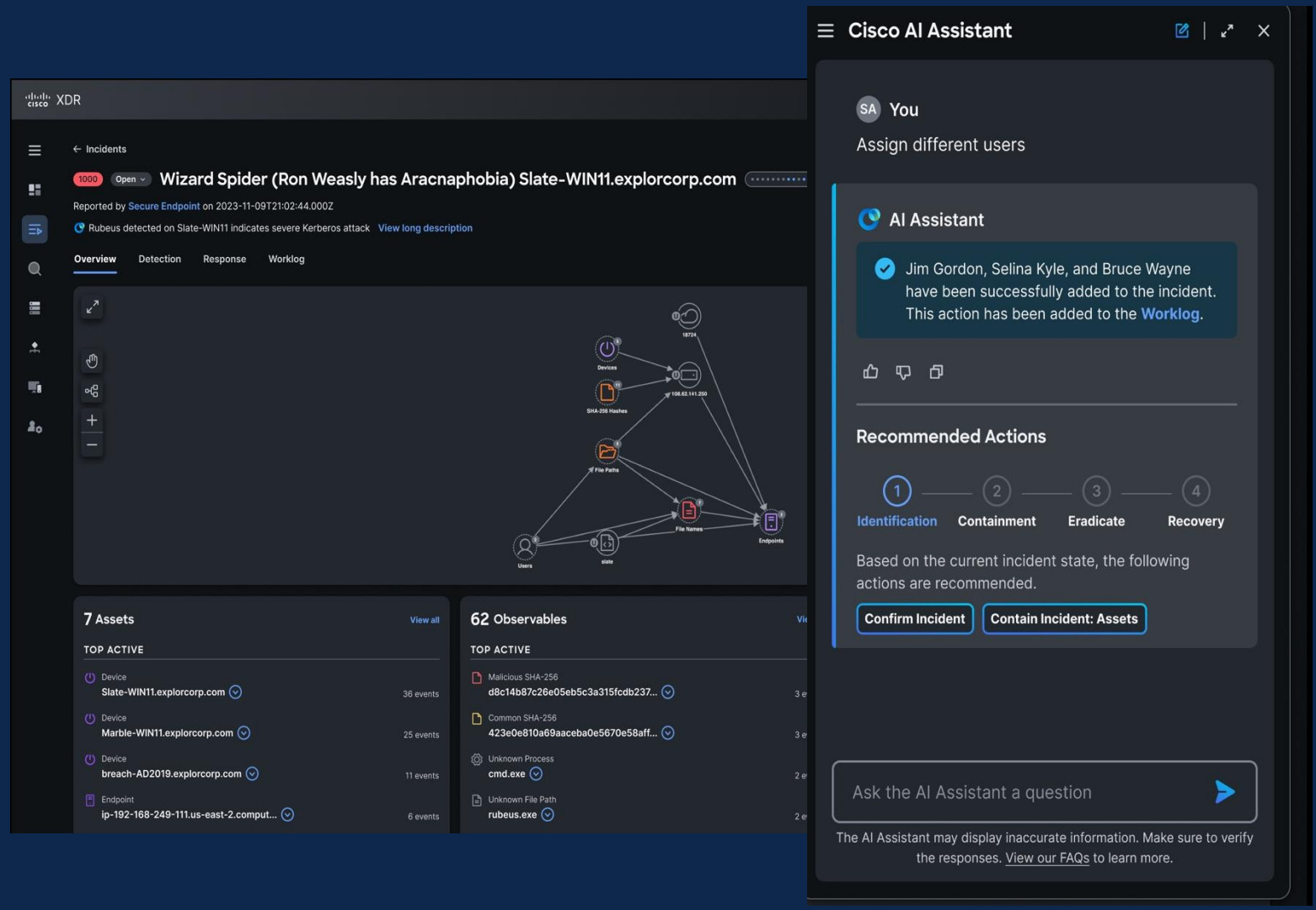
Hypershield



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

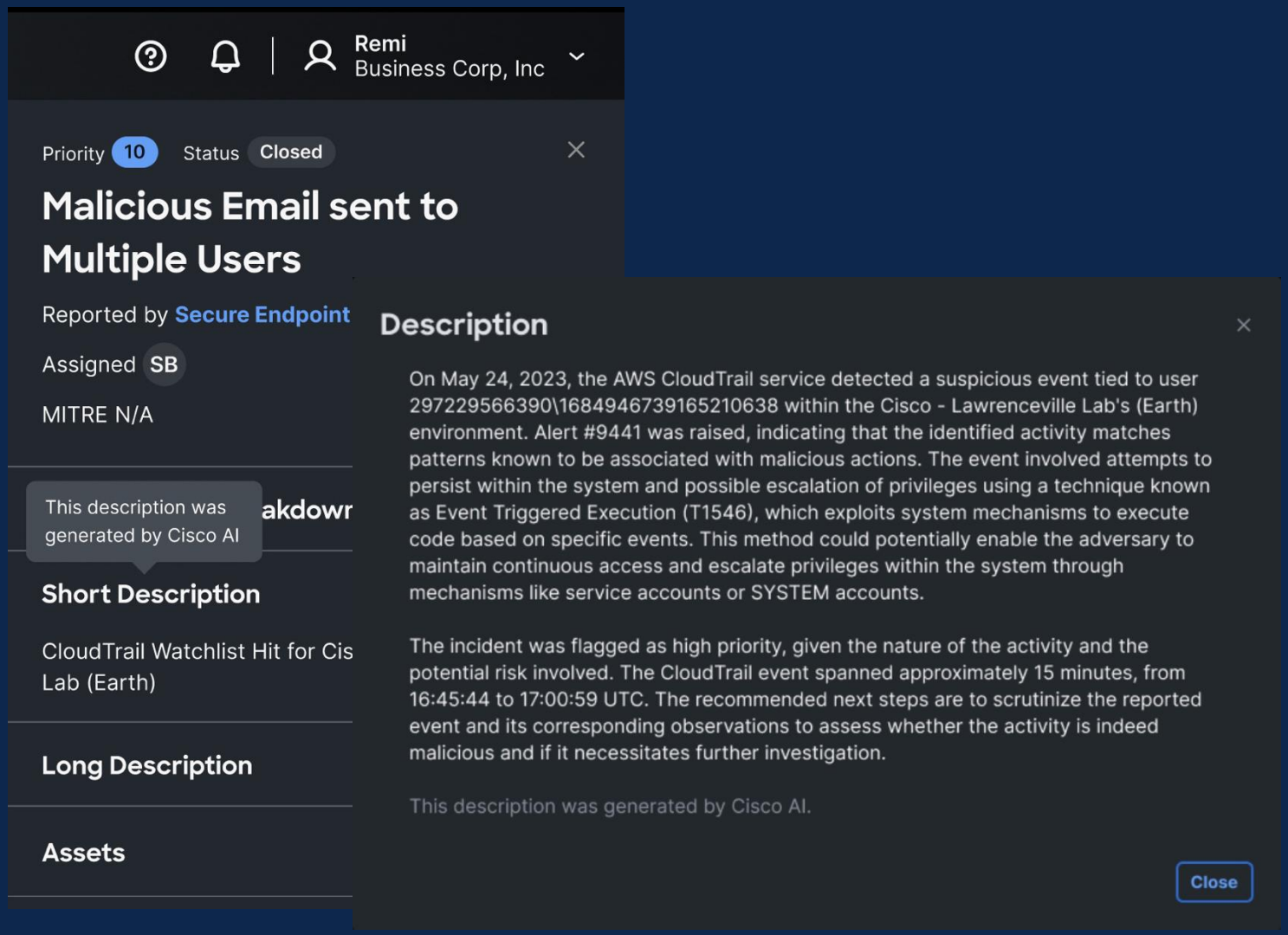


RELEASED

AI help for the SOC analytst

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

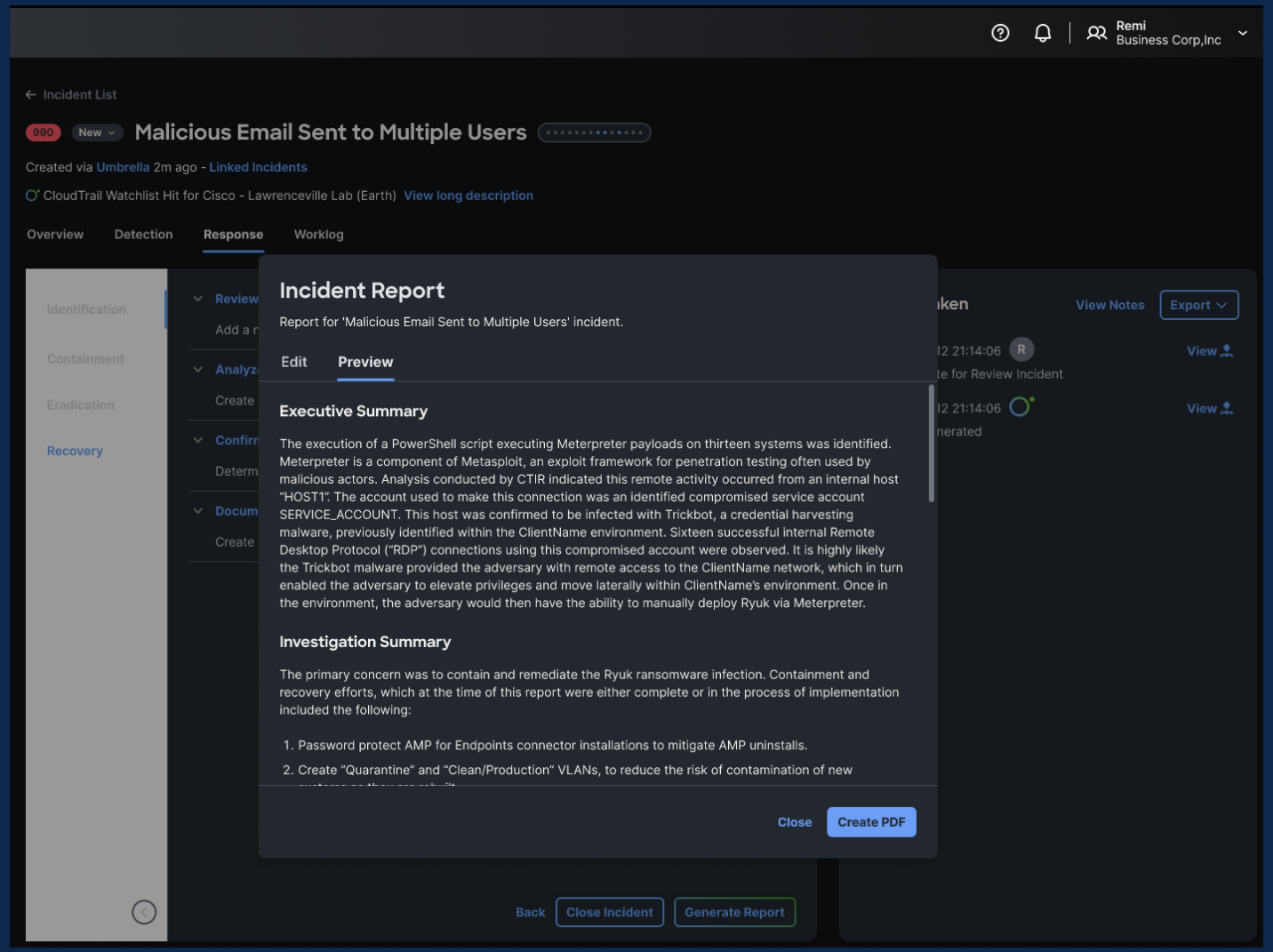


RELEASED

AI help for the SOC analytst

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

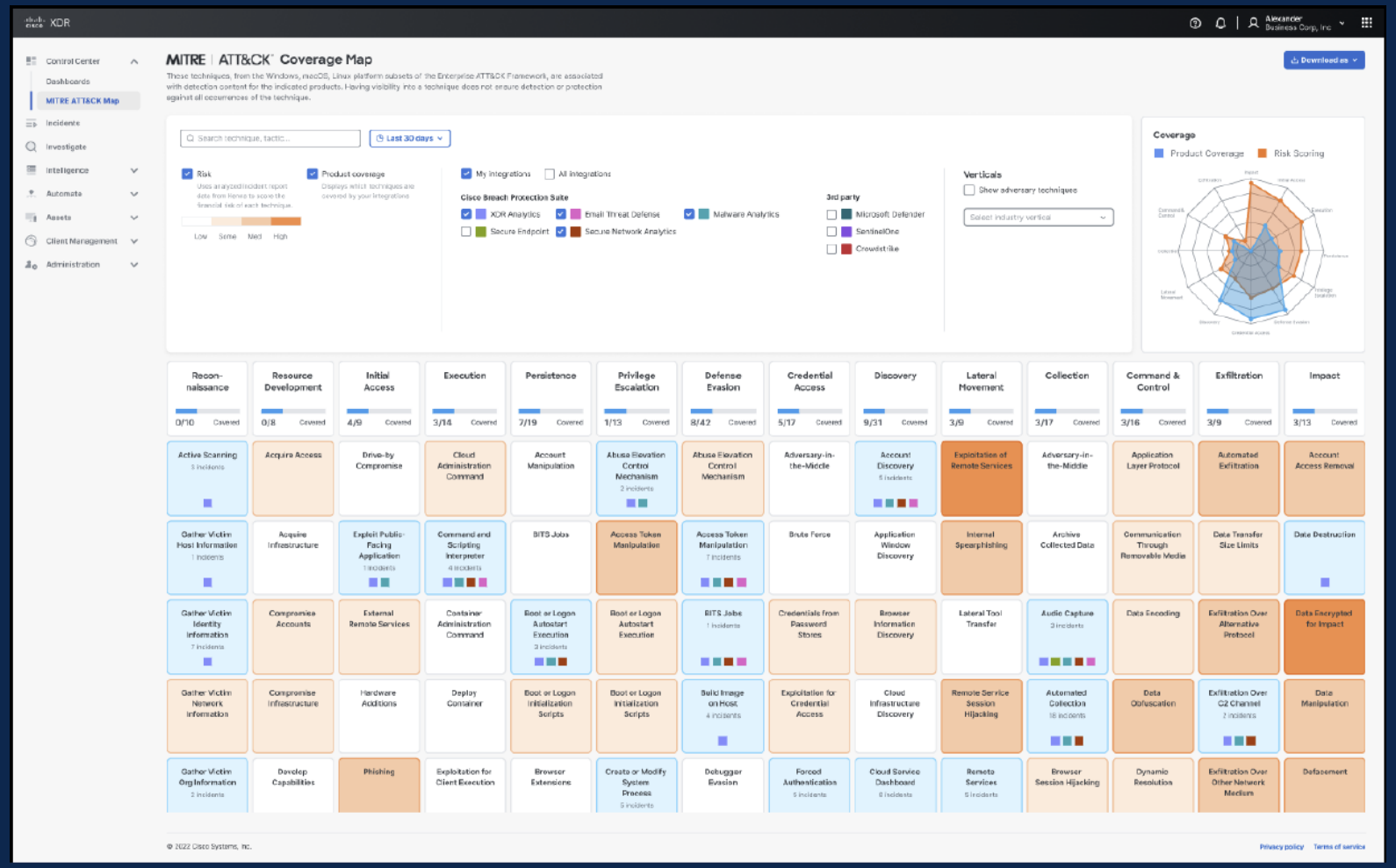


RELEASED

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

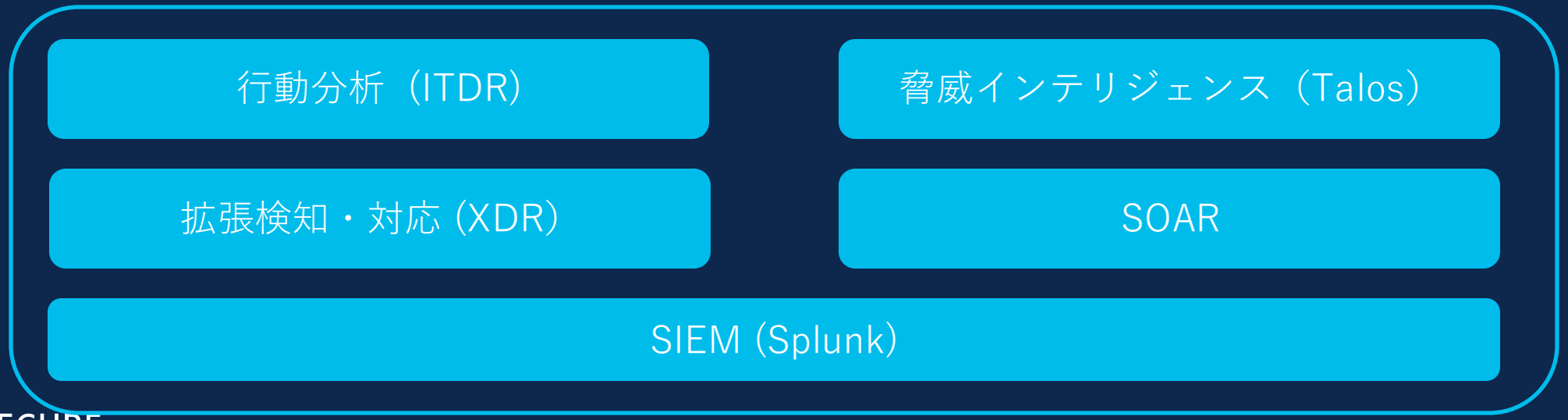
セキュリティとオブザーバビリティ機能の拡張

Cisco XDR with Splunk

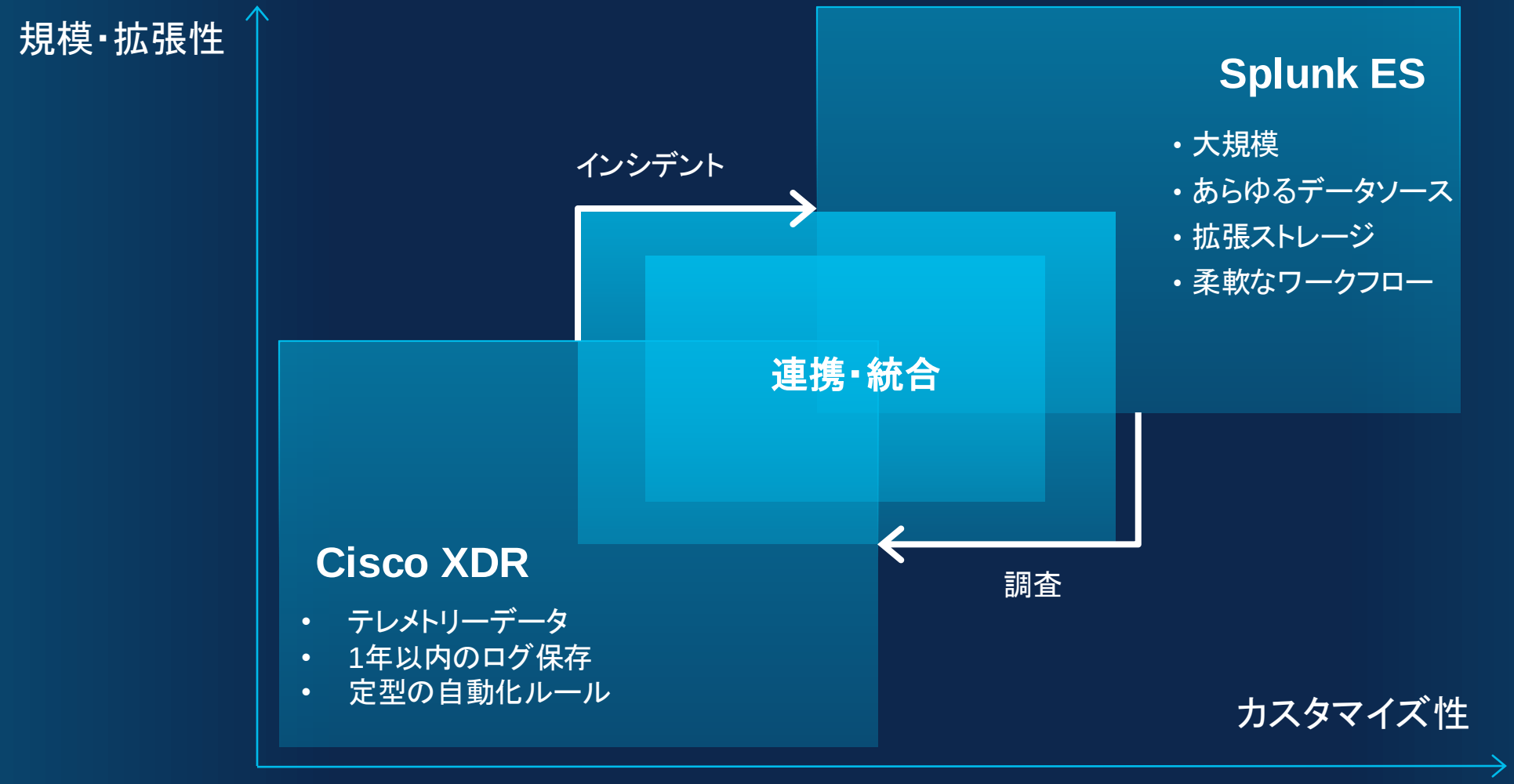
行動分析、脅威インテリジェンス、拡張検知・対応（XDR）、SOARなどの機能を統合することで、
従来のSIEMの機能を超えて、包括的なSOCプラットフォームを提供

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



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)


cisco SECURE