Cisco **Security**

Cisco Security Summit Tokyo 2025

AI 時代の SOC を加速する
– Cisco XDR × Splunk –

シスコシステムズ合同会社
APJC XDR Sales Lead
平岡 龍弘

Splunk Services Japan
Partner & Solutions Architect Senior Manager
横田 聡

Aug 5, 2025

今日お話したいこと

- CiscoXDRのアップデート
- Cisco XDR with Splunkのメッセージ

今日お話したいこと

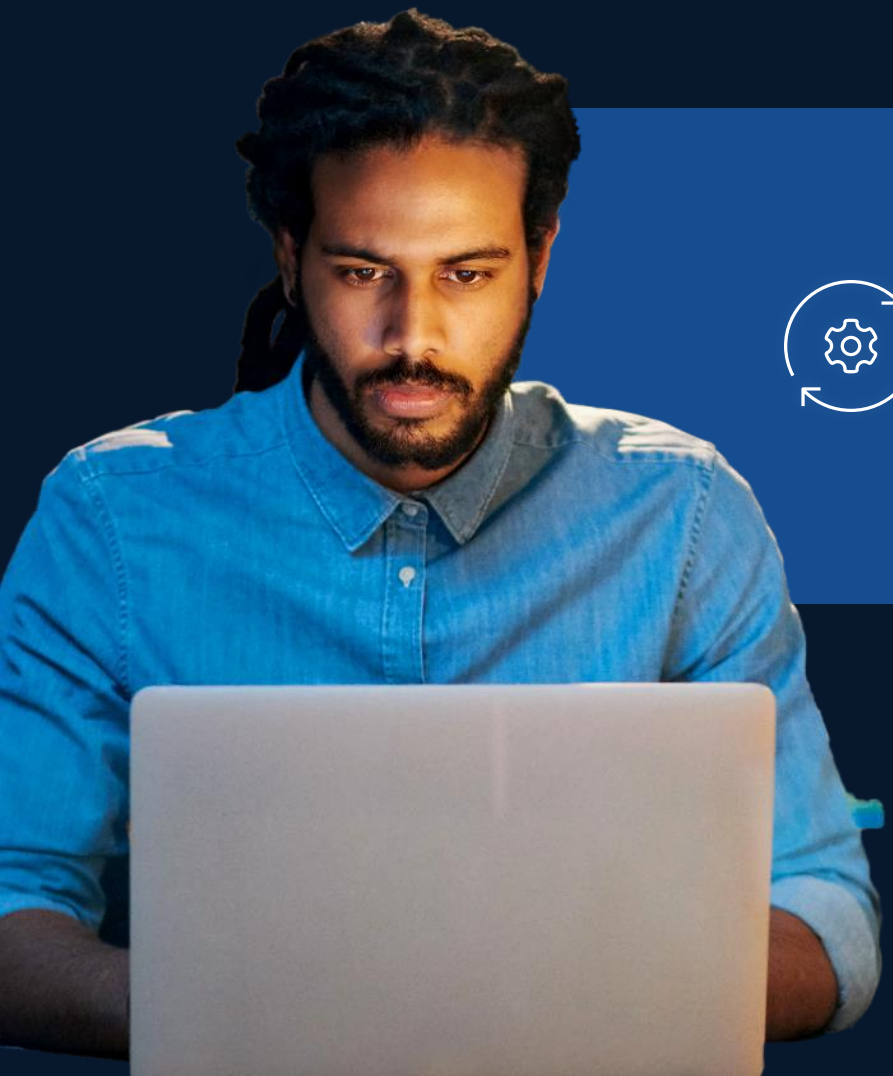
- CiscoXDRのアップデート
- Cisco XDR with Splunkのメッセージ

Cisco XDR Overview

Cisco **Security**

Cisco Security Summit Tokyo 2025

セキュリティオペレーションの問題



人材不足
24/365対応

アラート
疲れ

ツールの
複雑さ

手動調査による
遅延

オペレーションの複雑な問題

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

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

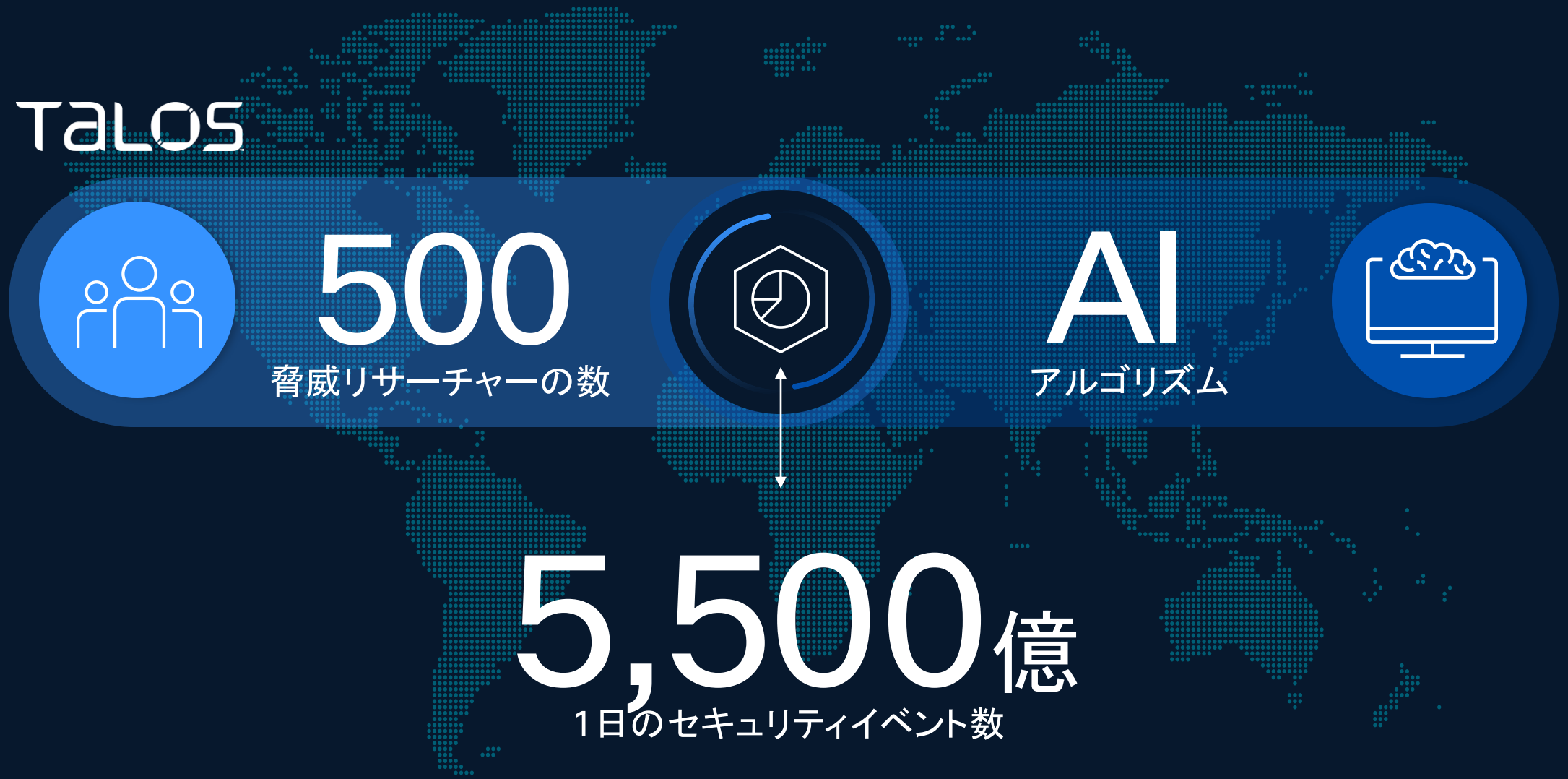
自動隔離

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



Cisco XDR Update

Cisco **Security**

Cisco Security Summit Tokyo 2025

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

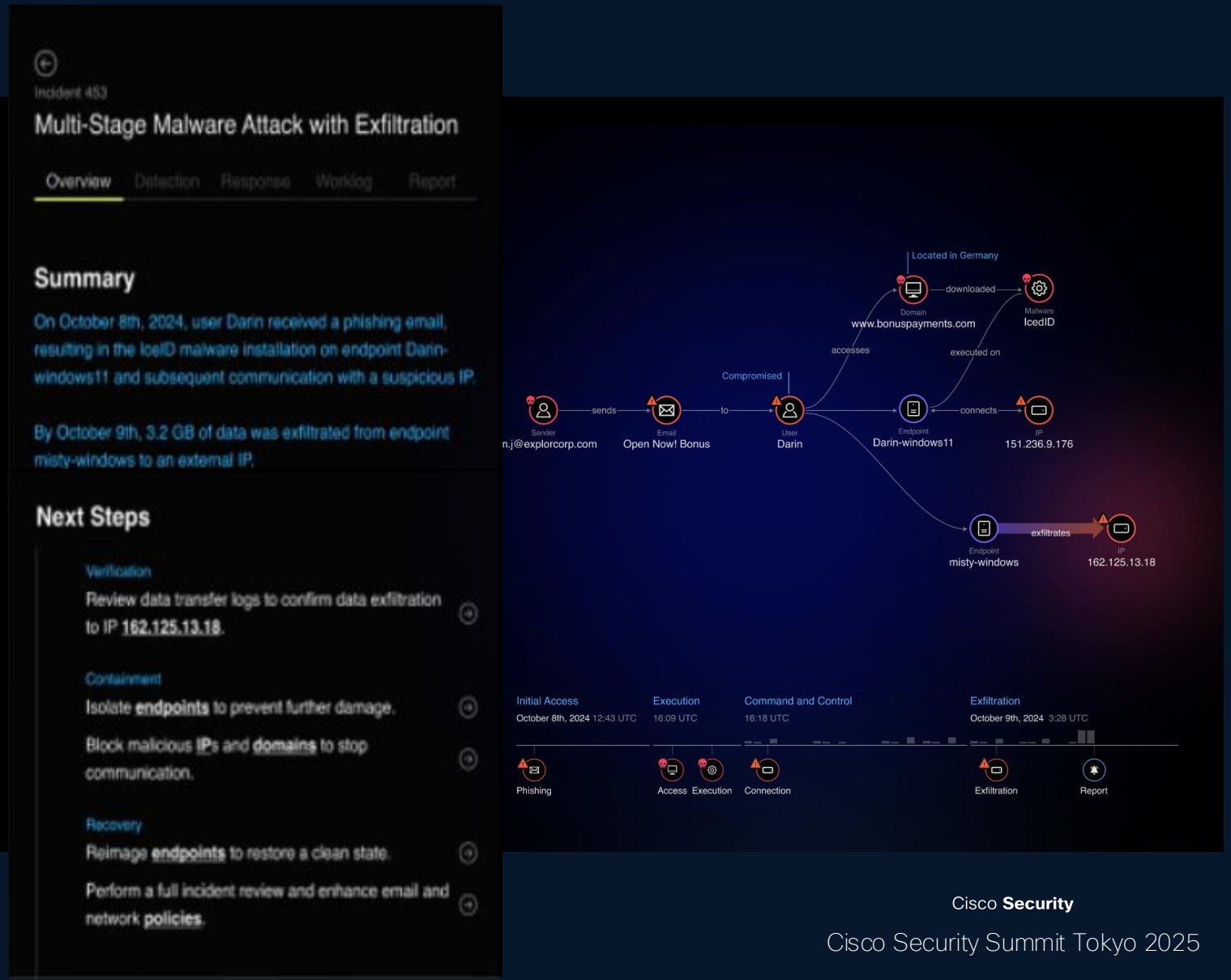
Attack Storyboard

Automated Forensics

OCSF Format

Instant Attack Verification

2025.10 リリース



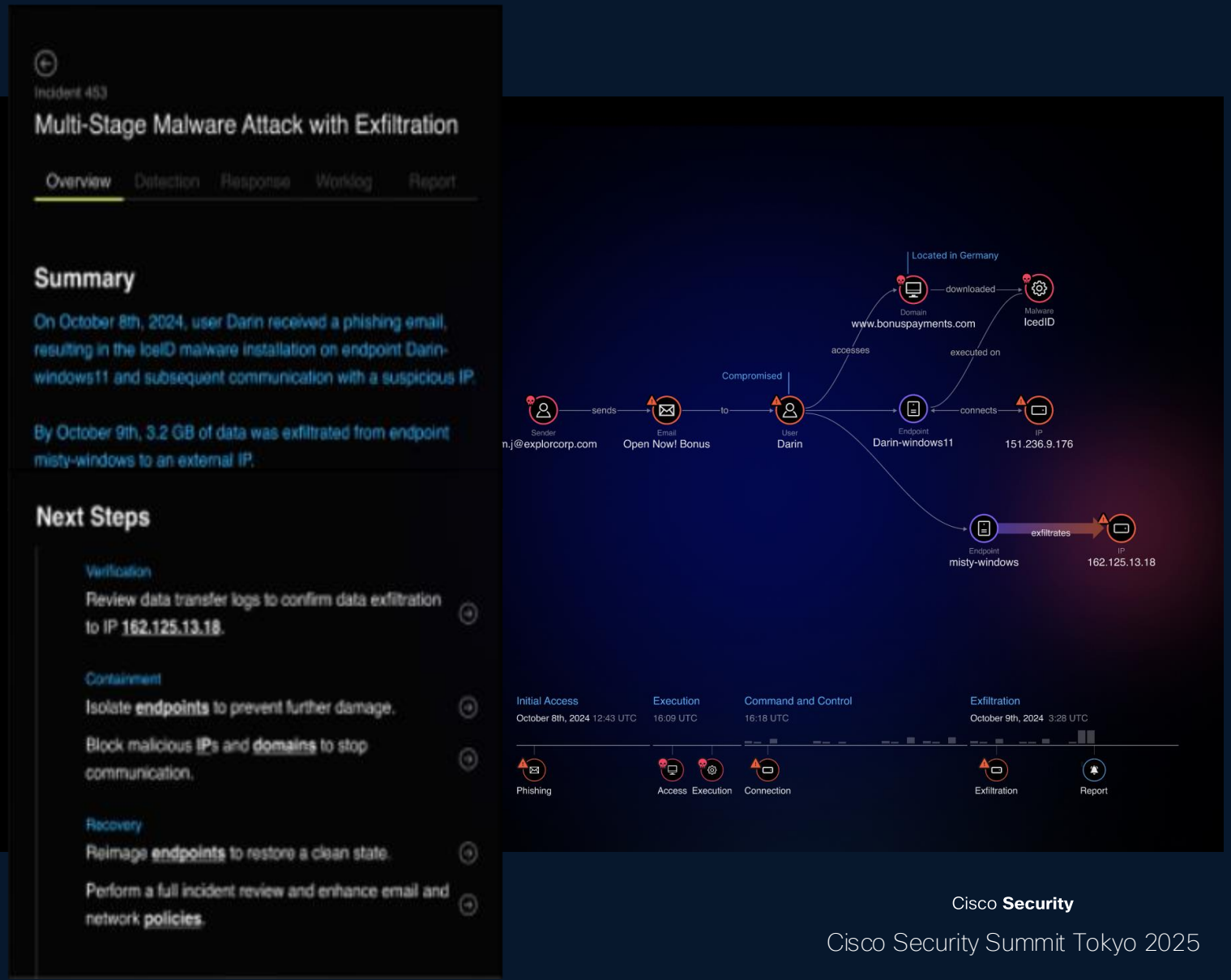
Agentic AIによるインシデントの自律的評価機能。

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。

Attack Storyboard

2025年秋リリース



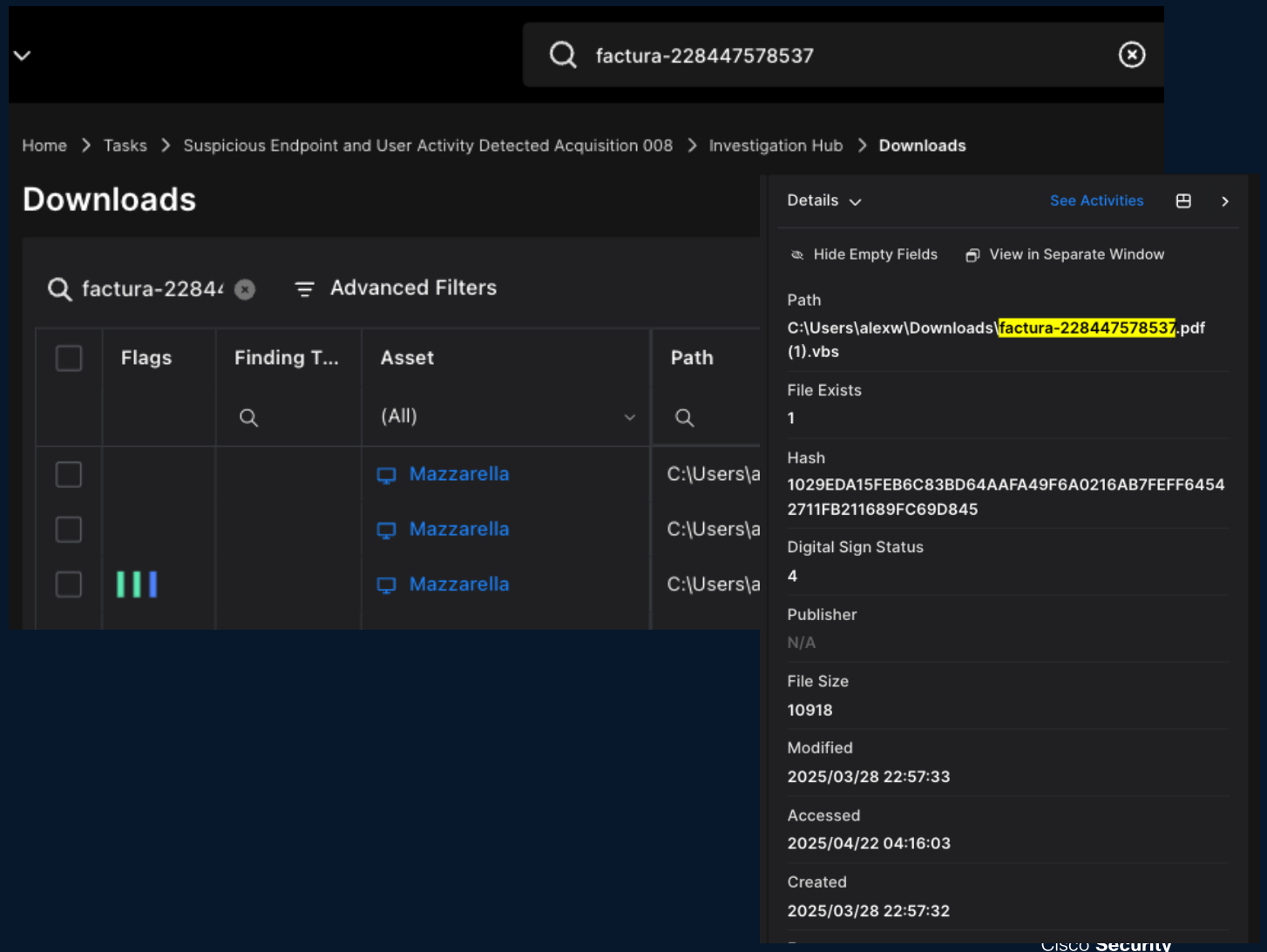
攻撃の全体像を30秒以内に把握できる可視化機能。

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年秋リリース



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

2025年秋リリース

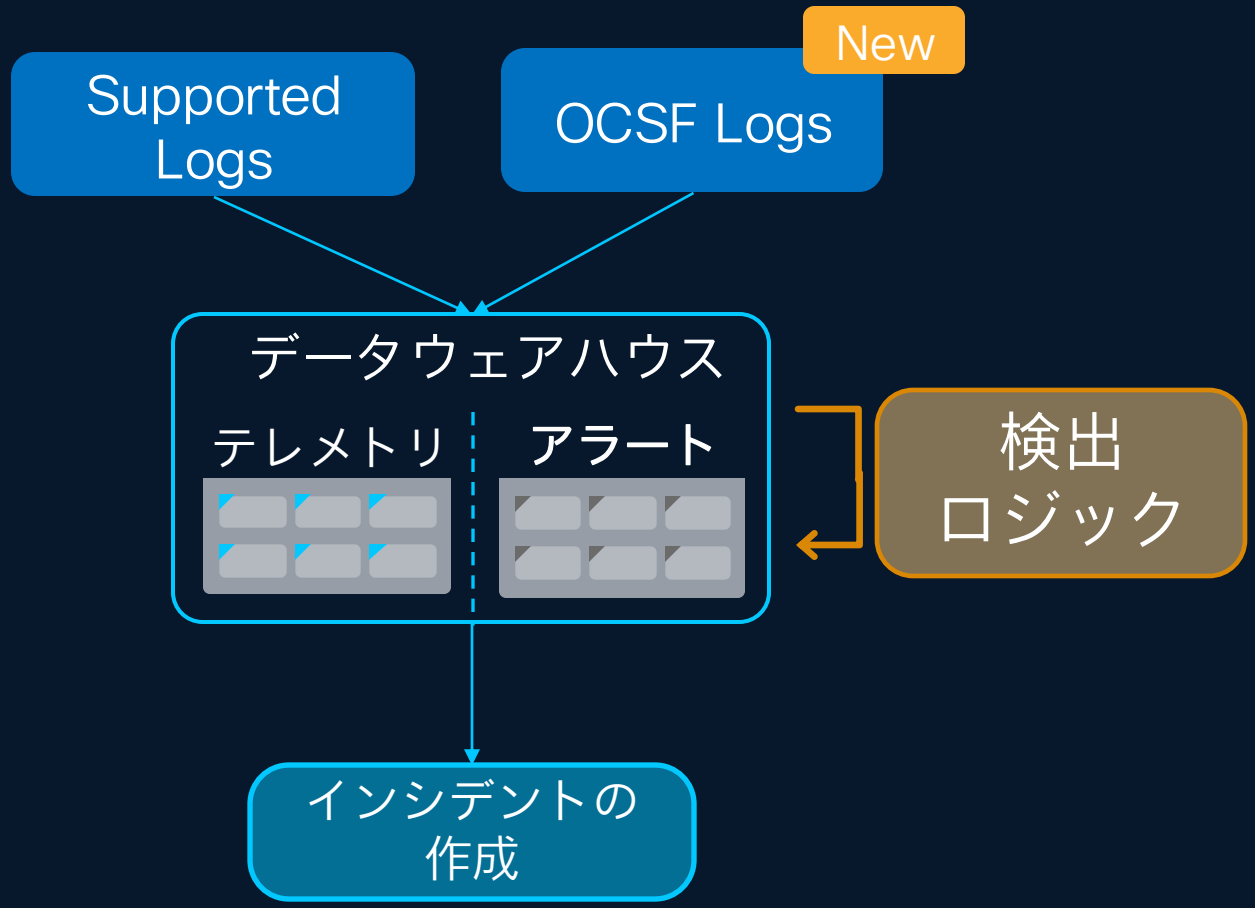
OCSFとは

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



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

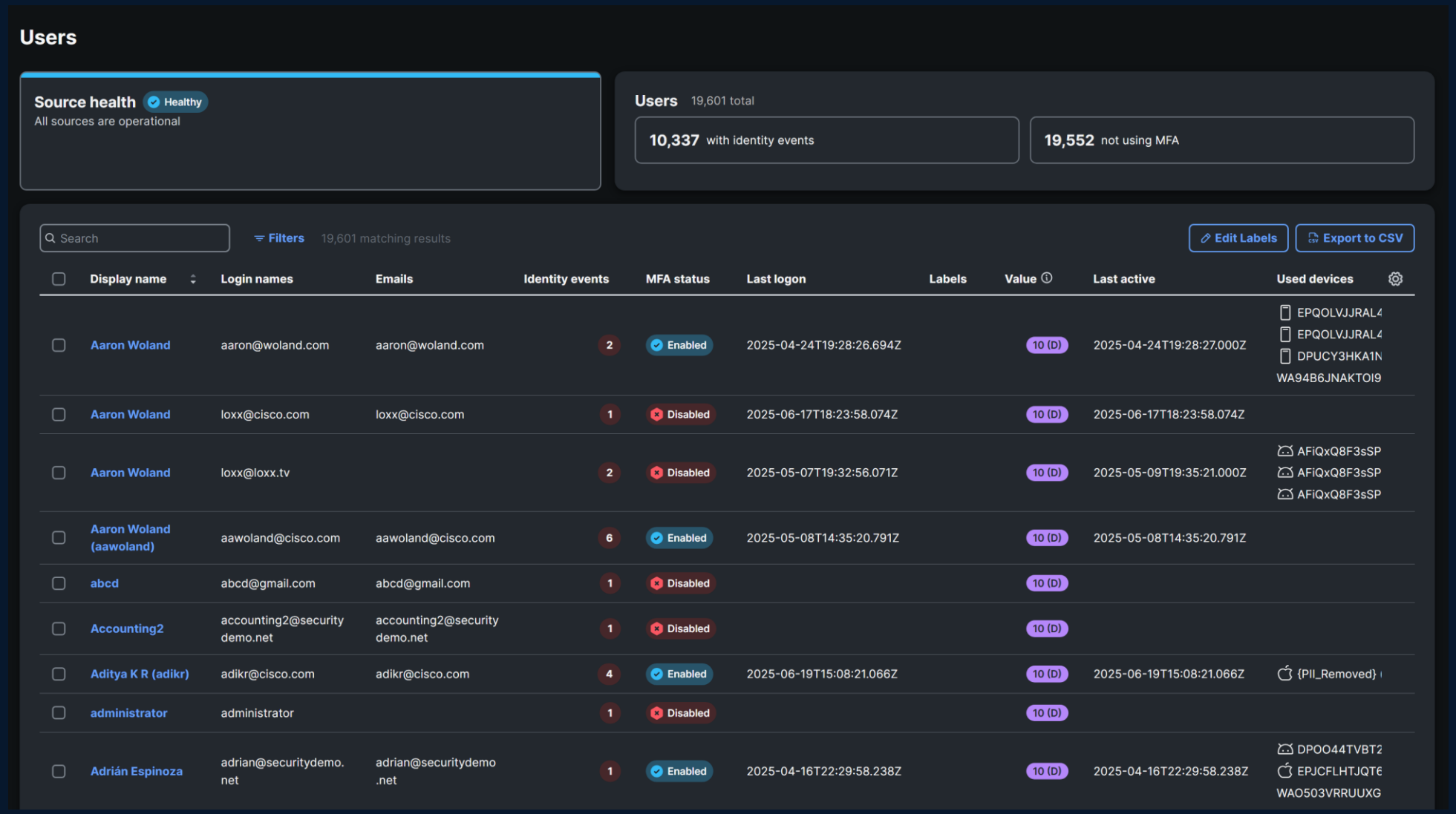
ISPM
(ポスチャ管理)

ITDR
(脅威検知対処)

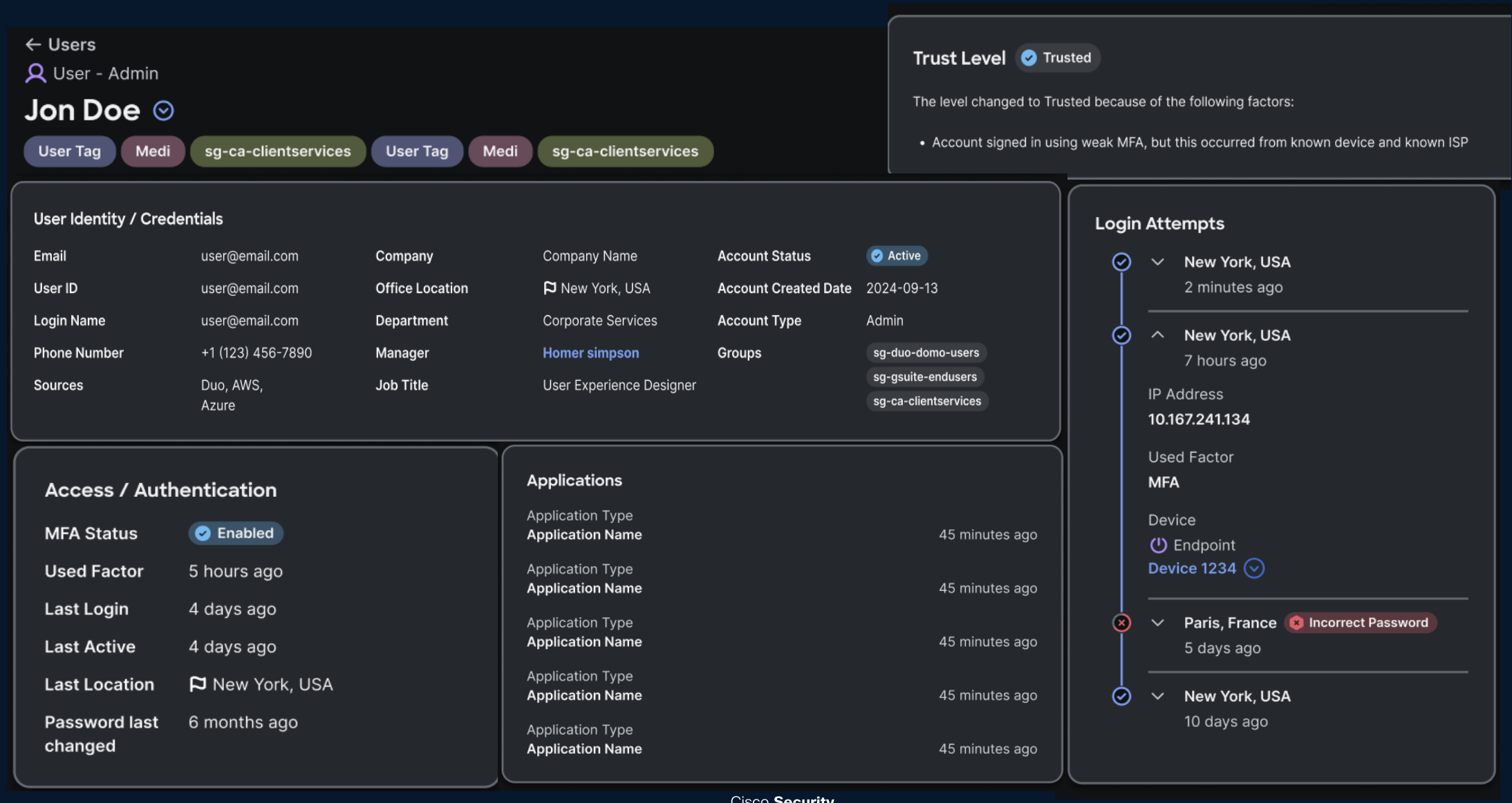
Asset Insight
(ユーザー情報の可視化)

Cisco XDRに直接
アイデンティティ情報を取り込み

Duo連携の成果



Duo連携の成果　(将来像)



ゼロトラストの脅威を包括管理

Released

今日お話したいこと

- CiscoXDRのアップデート
- Cisco XDR with Splunkのメッセージ

Cisco XDR with Splunk

Cisco **Security**

Cisco Security Summit Tokyo 2025

XDR ≠ SIEM

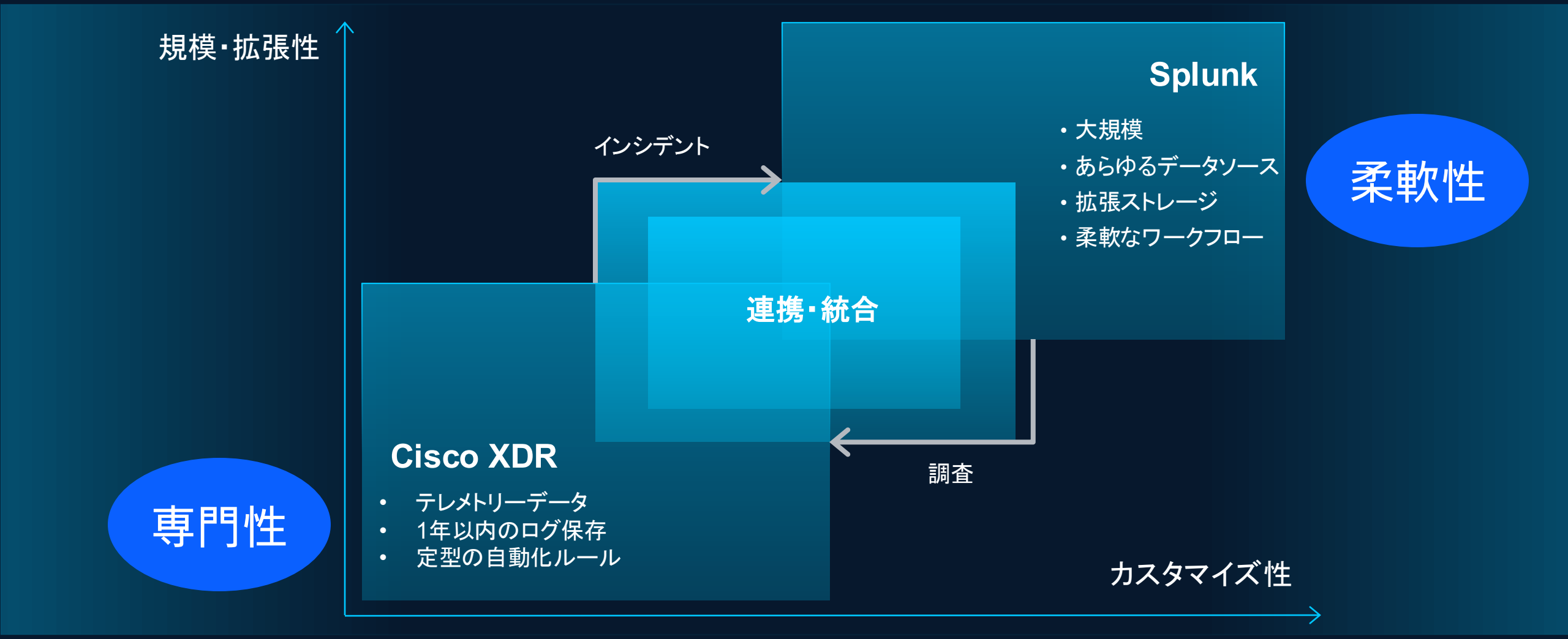
XDR	SIEM
ニアリアルタイム	数時間、日～週（後日評価）
相関	集約
より高度な検出・対処	イベント監視・ログ監視
人の介在（低）	人の介在（高）

XDR ≠ SIEM

XDR	SIEM
生ログ なし	生ログ あり

従来の Cisco XDR with Splunk

これからの Cisco XDR with Splunk



ツールから何を得たいか

Cisco XDR

NIST
サイバーセキュリティ
フレームワーク

識別	防御 (予防含む)	検知 (可視化含む)	対応 (分析調査含む)	復旧
リスクを特定し認識	脅威を防御	脅威および異常を監視・検知	脅威・異常を分析(調査)し、当座の対策を実施	安全な状態に復旧恒久対策の実施
• 脆弱性スキャン等	• FW / IDS,IPS / WAF / Sandbox / AV Proxy / CASB等	• EDR / NDR • 脅威インテリジェンス • **XDR/SIEM/UEBA**	• **XDR/SIEM/SOAR** • フォレンジックツール 等	

Mean time to Respond

Mean time to Detection

Supported by AI

ツールから何を得たいか

Splunk

NIST
サイバーセキュリティ
フレームワーク

識別	防御 (予防含む)	検知 (可視化含む)	対応 (分析調査含む)	復旧
リスクを特定し認識	脅威を防御	脅威および異常を監視・検知	脅威・異常を分析(調査)し、当座の対策を実施	安全な状態に復旧恒久対策の実施
• 脆弱性スキャン等	• FW / IDS,IPS / WAF / Sandbox / AV Proxy / CASB等	• EDR / NDR • 脅威インテリジェンス • **XDR/SIEM/UEBA**	• **XDR/SIEM/SOAR** • フォレンジックツール 等	

Mean time to Respond

Mean time to Detection

Supported by AI

ツールから何を得たいか

CiscoXDR with Splunk

NIST
サイバーセキュリティ
フレームワーク

識別	防御 (予防含む)	検知 (可視化含む)	対応 (分析調査含む)	復旧
リスクを特定し認識	脅威を防御	脅威および異常を監視・検知	脅威・異常を分析(調査)し、当座の対策を実施	安全な状態に復旧恒久対策の実施
• 脆弱性スキャン等	• FW / IDS,IPS / WAF / Sandbox / AV Proxy / CASB等	• EDR / NDR • 脅威インテリジェンス • **XDR/SIEM/UEBA**	• **XDR/SIEM/SOAR** • フォレンジックツール 等	

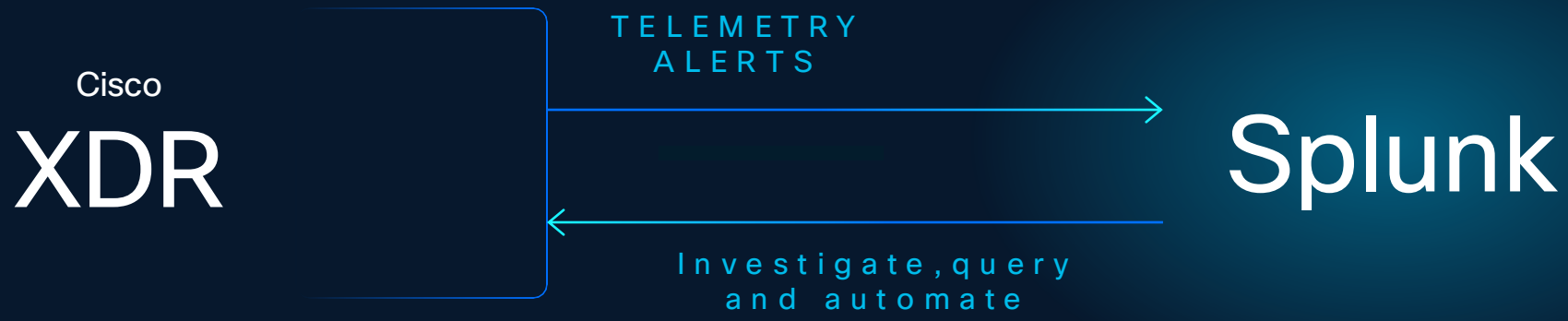
Mean time to Respond

Mean time to Detection

Supported by AI

Cisco XDRとSplunkの相互連携

Technical add-ons



Splunk with Cisco XDR

Cisco **Security**

Cisco Security Summit Tokyo 2025

CiscoXDRの相関分析とSplunk調査連携

Cisco XDR/Splunk ESで実現する統合TDIR

Networking
Clouds
Endpoint
Email

Cisco XDR

Tier1:
セキュリティオペレーションの簡素化

- 一元的な可視化
- 迅速な脅威検出
- Talos（脅威インテル）
- 自動化プレイブック
- 相関分析と優先度付
- Agentic AIと生成AI

リアルタイム検知・対応

- XDRの情報をダッシュボード表示
- 情報のエンリッチメント
- インシデント情報の相関分析

- **対象のSplunkのログを検索、表示**
- **情報のエンリッチメント**
- Splunkの情報を相関分析

Splunk Enterprise Security

SIEM

Tier 2-3:
セキュリティオペレーションの統合

- UEBAによる内部脅威検知
- SOARによる自動化
- 脅威インテル活用
- AIによるサポート
- 資産情報の高度な活用
- 脅威ハンティング

高度な検知・分析、調査全体の可視化

Data centers
Identity
Applications
IT/OT
Networking
Talos
Third-party tools
Any machine data

統合されたプラットフォームで、MTTD/MTTRの削減とセキュリティオペレーションの高度化と効率化を実現します

Cisco×Splunkによる統合TDIRプラットフォームのコンセプト

CiscoとSplunkがOne Communiyとなってお届けする解決策

運用負荷の増大による**対応の遅延・形骸化**

統合された
アナリストエクスペリエンス

- Cisco XDR & Splunk

インシデント対応の
簡素化

セキュリティ対策にかかる**コストの増加**

分散分析型
セキュリティデータレイク

- DMX & Federation
- Free Cisco Data

セキュリティ対策にかかる
コストの最適化

高度な専門スキルを持つ**人材の慢性的な不足**

セキュリティ運用のためのAI

- AI Assistant
- Agentic AI

少ない人材でも回せるSOC体制の実現

Splunkデータマネジメント戦略

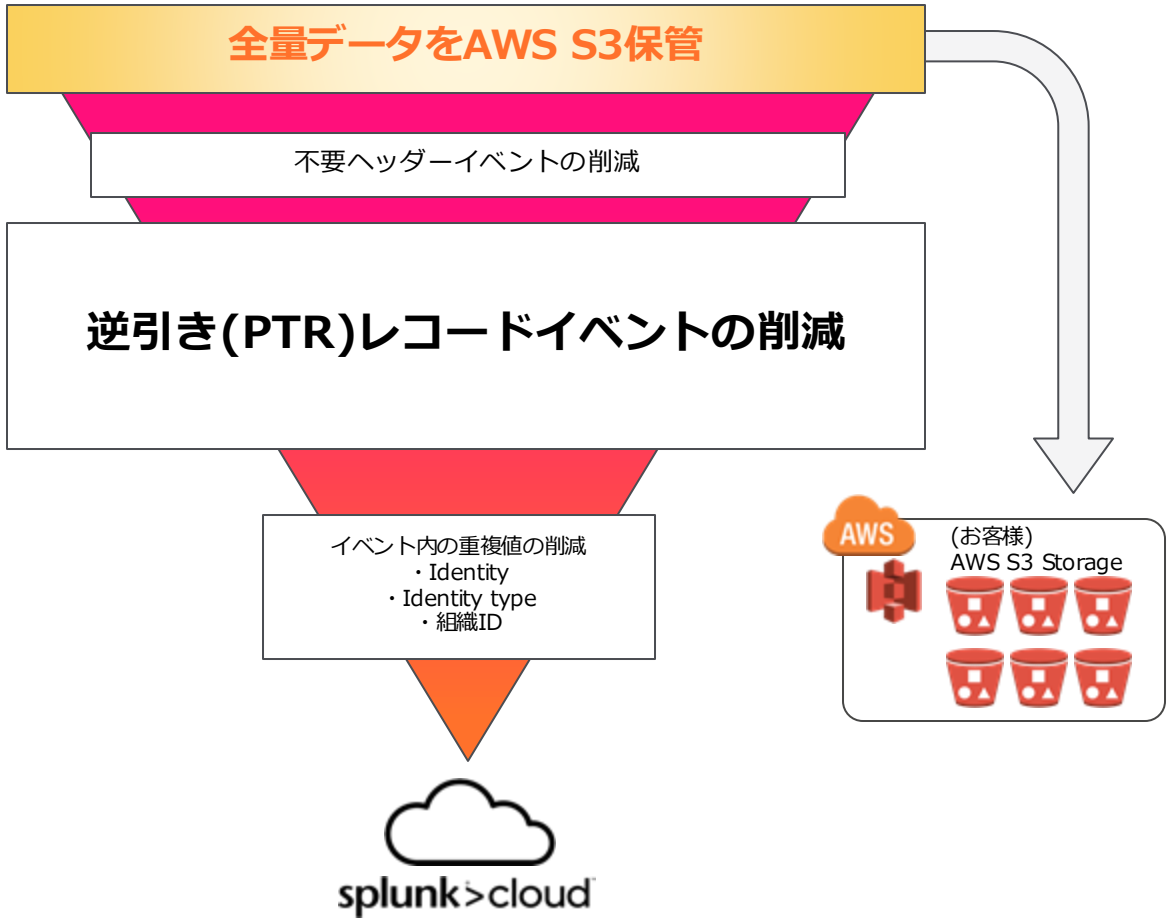
Unify data configuration, processing, and management

代表的ユースケース：
SASE/Firewallなどの大量データからLow-Value(不要なイベント)を除外し60%容量削減に成功

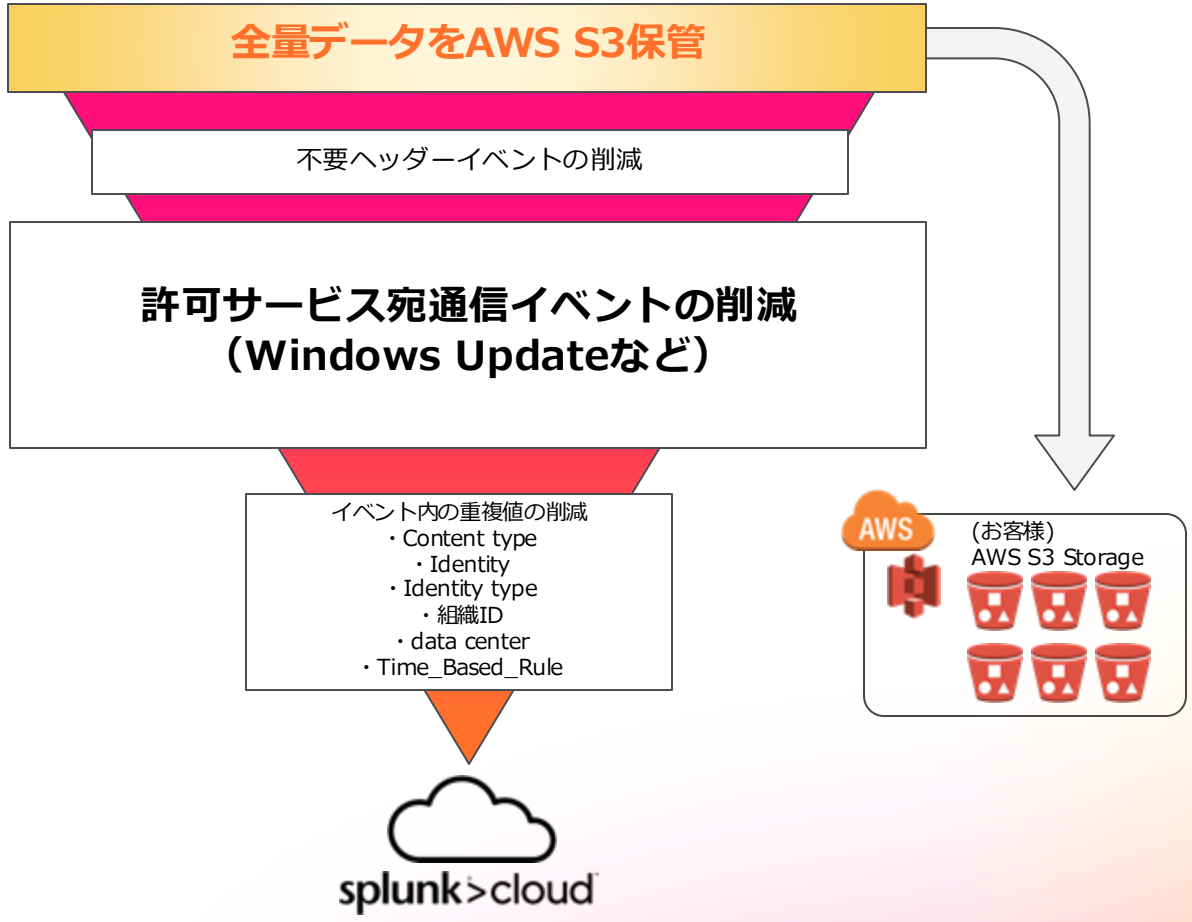
例: Cisco Cloud Securityデータのフィルタリングプラクティス

セキュリティ分析に不要なLow-Valueデータはイベントごと削減/イベント内の不要フィールドを削減

DNSクエリログの削減テンプレート



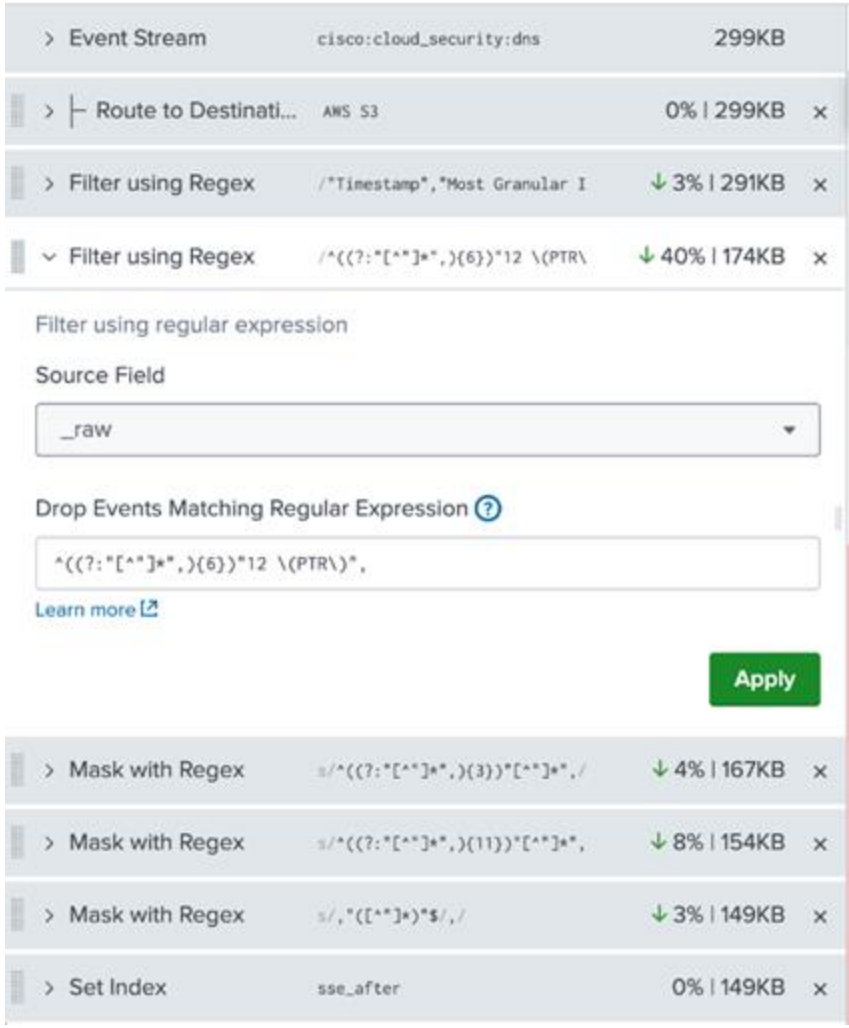
Proxyログの削減テンプレート

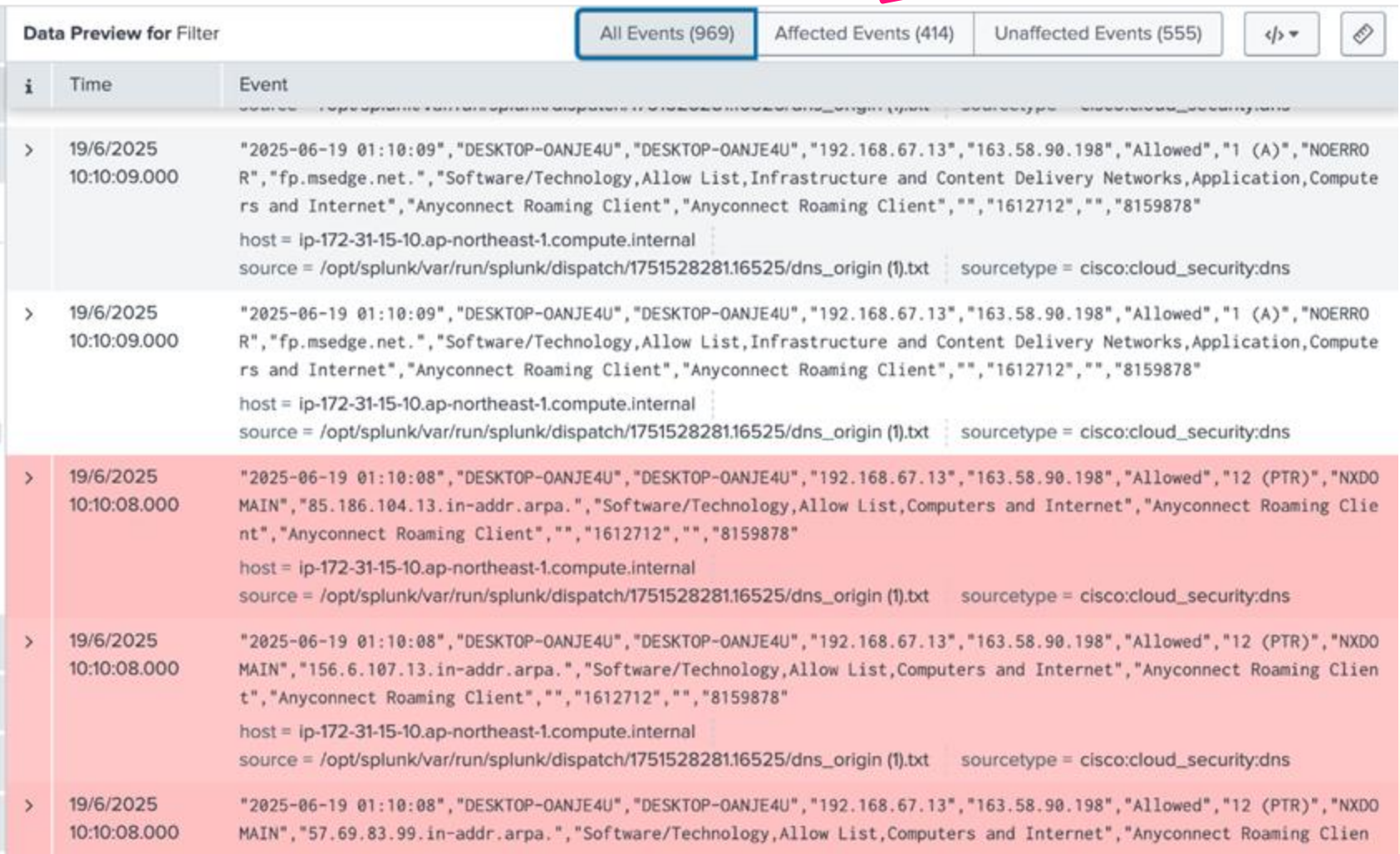


Ingest Actionsの削減効果

DNSログの中で不要なイベントをフィルタ

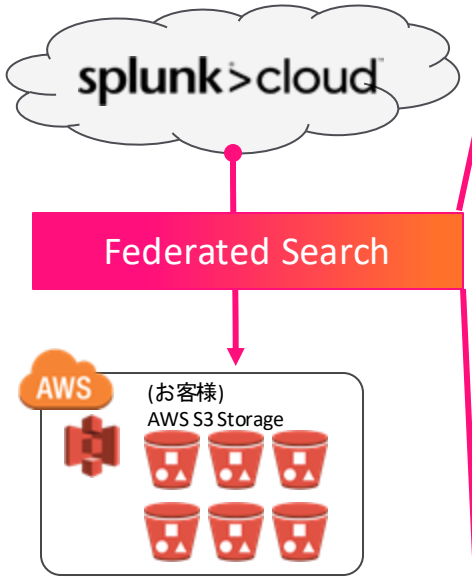
約50-60%の
DNSログ削減に成功





Federated Search for S3を使った過去ログ調査

過去ログの調査であればシンプルなSPLで簡単に調査可能




```
|sdselect * from federated:sase-dns
|eval time=strftime(time, "%Y-%m-%d %H:%M:%S")
|fields time event
|sort - time
|search event=*192.168.67.13*
```

時間範囲: 日付と時間の範囲

✓ 8,371件の結果 (2025/07/03 10:00:00.000～2025/07/03 17:00:00.000)　ジョブ　ポリシーベースのプール　スマート

イベントサンプリングを行わない

イベント　パターン　統計情報 (8,371)　視覚エフェクト

表示: 20/ページ　フォーマット　プレビュー：オン　前へ　1　2　3　4　5　6　7　8

time	event
2025-07-03 16:59:50	"2025-07-03 16:59:50","DESKTOP-OANJE4U","DESKTOP-OANJE4U","192.168.67.13","163.58.90.198","Allowed","1 (A)","NOERROR","swg-url-proxy-https-sse.sigproxy.qq.opendns.com.","Software/Technology,Allow List,Computer Security,Application,Computers and Internet,Cloud and Data Centers","Anyconnect Roaming Client","Anyconnect Roaming Client","","1612712","","8159878"
2025-07-03 16:59:50	"2025-07-03 16:59:50","DESKTOP-OANJE4U","DESKTOP-OANJE4U","192.168.67.13","163.58.90.198","Allowed","1 (A)","NOERROR","swg-url-proxy-https-sse.sigproxy.qq.opendns.com.","Software/Technology,Allow List,Computer Security,Application,Computers and Internet,Cloud and Data Centers","Anyconnect Roaming Client","Anyconnect Roaming Client","","1612712","","8159878"
2025-07-03 16:59:31	"2025-07-03 16:59:31","DESKTOP-OANJE4U","192.168.67.13","163.58.90.198","52.123.128.14","","ALLOWED","https://ecs.office.com/config/v1/ODSP_Sync_Client/25.105.0601.0002?UpdateRing=Prod&OS=Win&OSVer=10.0.26100&OSSku=48&accountType=Consumer&clientid=6335419a-c9ad-5b58-bb1d-1a87f6773abe&userid=acbb9eaf4e7abbcc","","OneDrive-25.105.0601.0002","304","","","","","Software/Technology,Computers and Internet","","","","","","Anyconnect Roaming Client","","DESKTOP-OANJE4U","Anyconnec

様々なセキュリティリスクに対応できるTDIRの重要性

様々なセキュリティリスクに対応できるCisco+SplunkのTDIRプラットフォーム

統合セキュリティリスクマネジメント

SOC　CSIRT　CISO　各施策担当　リスク管理

外部脅威

Cisco XDR

Splunk Enterprise Security

標的型攻撃　情報漏えい　クラウドリスク　アカウント悪用

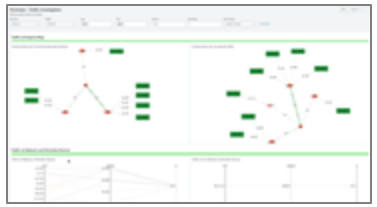
内部不正

Splunk Enterprise Security

Splunk UBA

内部不正　情報漏えい

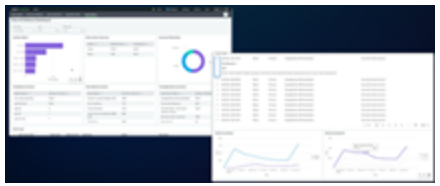
OTセキュリティ



OT Security Add-on for Splunk

標的型攻撃

AIセキュリティ



Cisco AI Defenseとの連携

情報漏えい

Fraud
なりすまし不正ログイン

Splunk App for Fraud Analytics

アカウント悪用

衛生管理
（サイバーハイジーン）

設定・構成管理

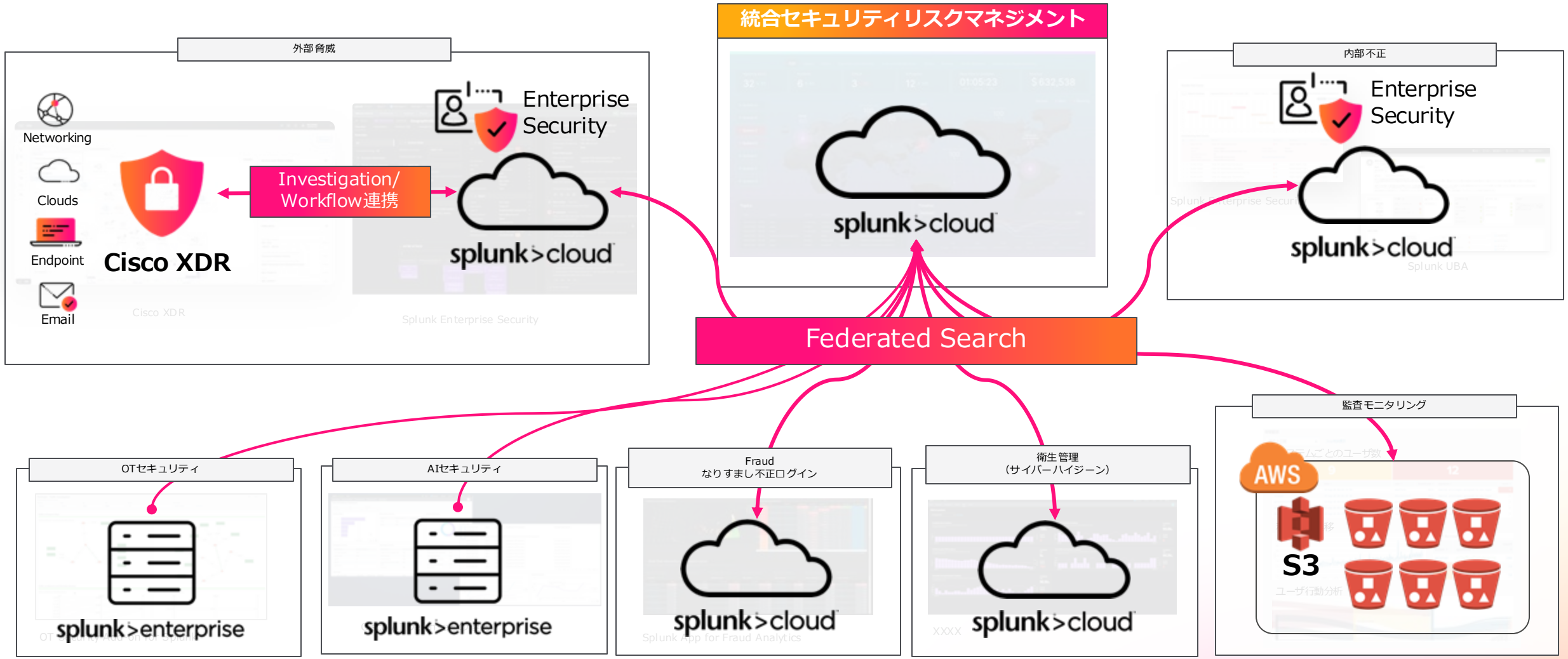
情報漏えい

監査モニタリング

監査
コンプライアンス

分散セキュリティデータレイクに対応できるTDIRの重要性

データ保管先が分散していても柔軟に統合分析できるTDIR



※Splunk Enterprise (BYOL)はSplunk Cloud/BYOL宛のみサーチ可。SplunkCloudからBYOL宛は不可。

2025年8月以降予定

Cisco FirewallログのSplunk取り込みが無料に

2025.06 のCisco Liveにて発表

AIベースの検知ルール提供と自然言語によるルール作成

Mean time to Detection を短縮化するためのFoundational AI / Gen AI及びルール評価機能

既知の脅威 ⟵ ⟶ 未知の脅威

EDR　SASE
Sandbox　FW　IDS/IPS

既存のセキュリティ機器
アラート（**Critical**/High）
例： UTM Alert - critical

既存のセキュリティ機器
アラート（Mid/Low/Info）
例： UTM Alert - Information

Talos

Splunk Enterpirse Securityをご利用の場合、Cisco Talosの脅威インテリジェンスを無償提供

Foundational AI
膨大なデータからシグナルを読み取る

機械学習ベースの検知 in Splunk Enterprise Security

ふるまい分析 with Splunk UBA/UEBA

1700個を超えるルールベース、ML/AIベース検知ルールを提供

Gen AI
自然言語を元に検知ルールを生成

AI Assistant for SPL

Rule / AI Rule Validation
ルールの検知テスト/評価

Attack Range
(Githubにて公開)

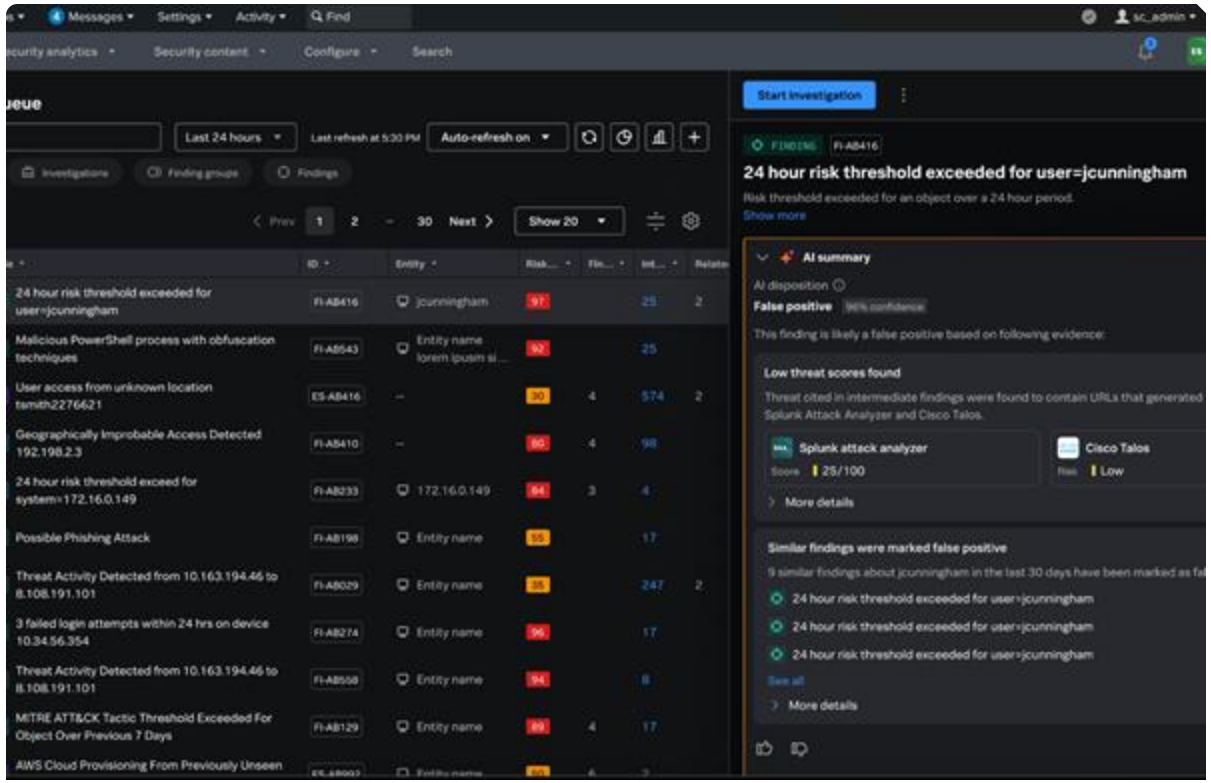
SnapAttack
（2025年1月買収）

2025年後半予定

Agentic AI

自立的にAIがSOC業務をトリアージしていく世界に向けて

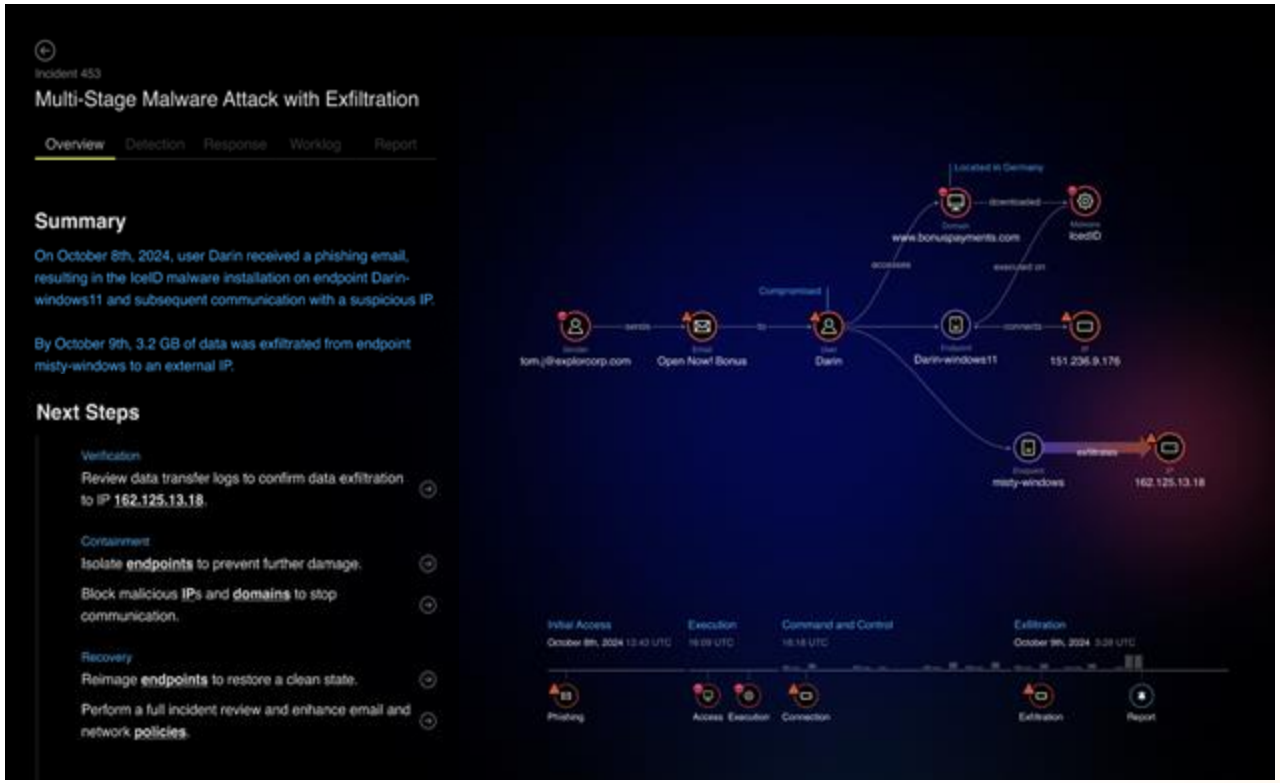
Enterprise Security - Triage Agent



Agentic AI よるアラートの過検知フィルタリング

アラートの信頼度を定量的に判断し、判断に至ったエビデンスを元に過検知を自動判定。

Cisco XDR - Instant Attack Verification



Agentic AI よるインシデントの自己検証機能

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。

さらに、具体的な影響、調査プランの立案、推奨アクションを提示

Cisco XDR Demo

Instant Attack Verification

Cisco **Security**

Cisco Security Summit Tokyo 2025

CiscoならOne PlatformでSOCの未来を実現

Cisco XDR with Splunk

- データの相互連携
- 高度な脅威検知
- AIを活用した調査
- 自動応答

組み込みAI

Cisco Talosによるインテリジェンス


User/Cloud/
Breach/


Networking


Third-party
tools


Talos


Clouds


Devices


Data
centers


Applications

Cisco **Security**

Cisco Security Summit Tokyo 2025

Thank you