

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

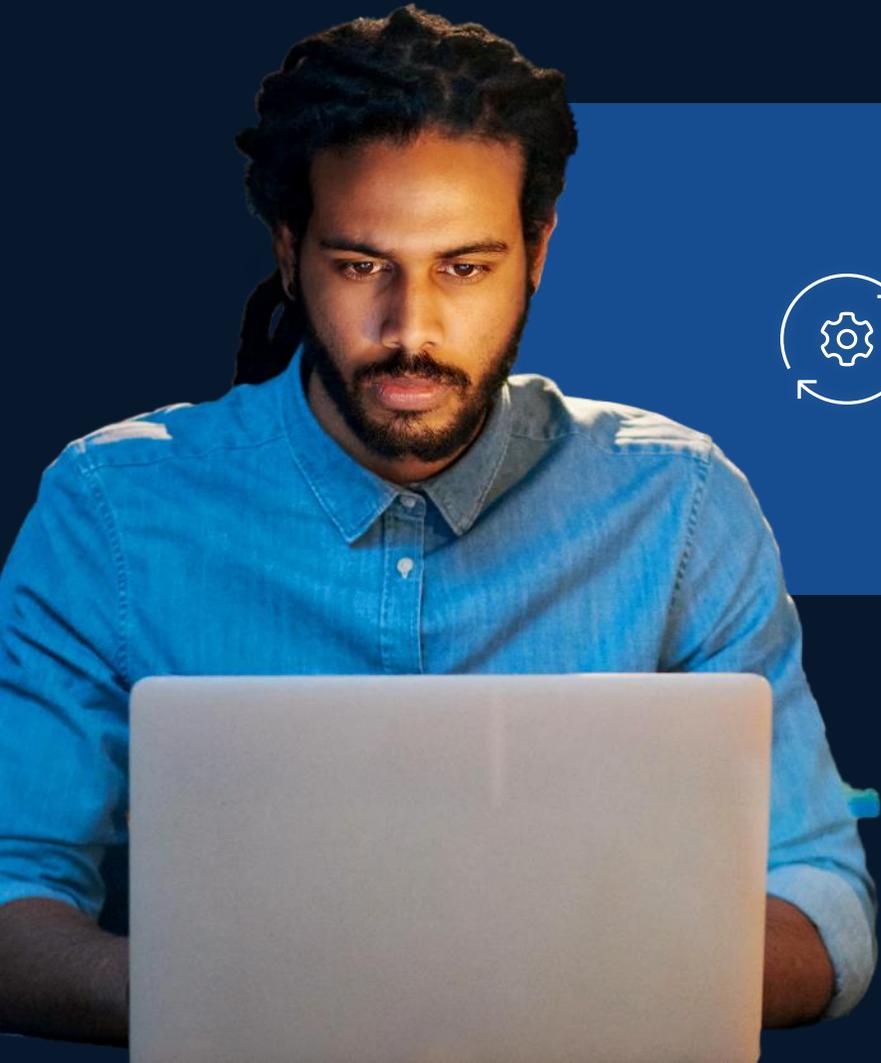
- CiscoXDRのアップデート
- Cisco XDR with Splunkのメッセージ

# 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

# 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

Security Center

Overview 123 Events 123 XDR incidents 44

44 Incidents 5 New incidents 22 Open incidents

Priority	Name	Source	Created	Assigned
1000	Ransomware Detection	SCA	3 days	Unassigned
978	A malicious SHA-256 targeted an endpoint	SCA	4 days	Unassigned
875	Suspicious Web Access	Meraki API	9 hours	Unassigned
832	Authentication Bypass Attempt	Meraki API	11 hours	Unassigned

A malicious SHA-256 targeted an endpoint

Priority 978 Status New

Reported by Cisco Secure Cloud (Cisco Secure Cloud) 1 month ago

Assigned Unassigned

Priority score breakdown 978 97 Detection Risk 10

Short description  
A process running has a hash matching a known malicious process hash

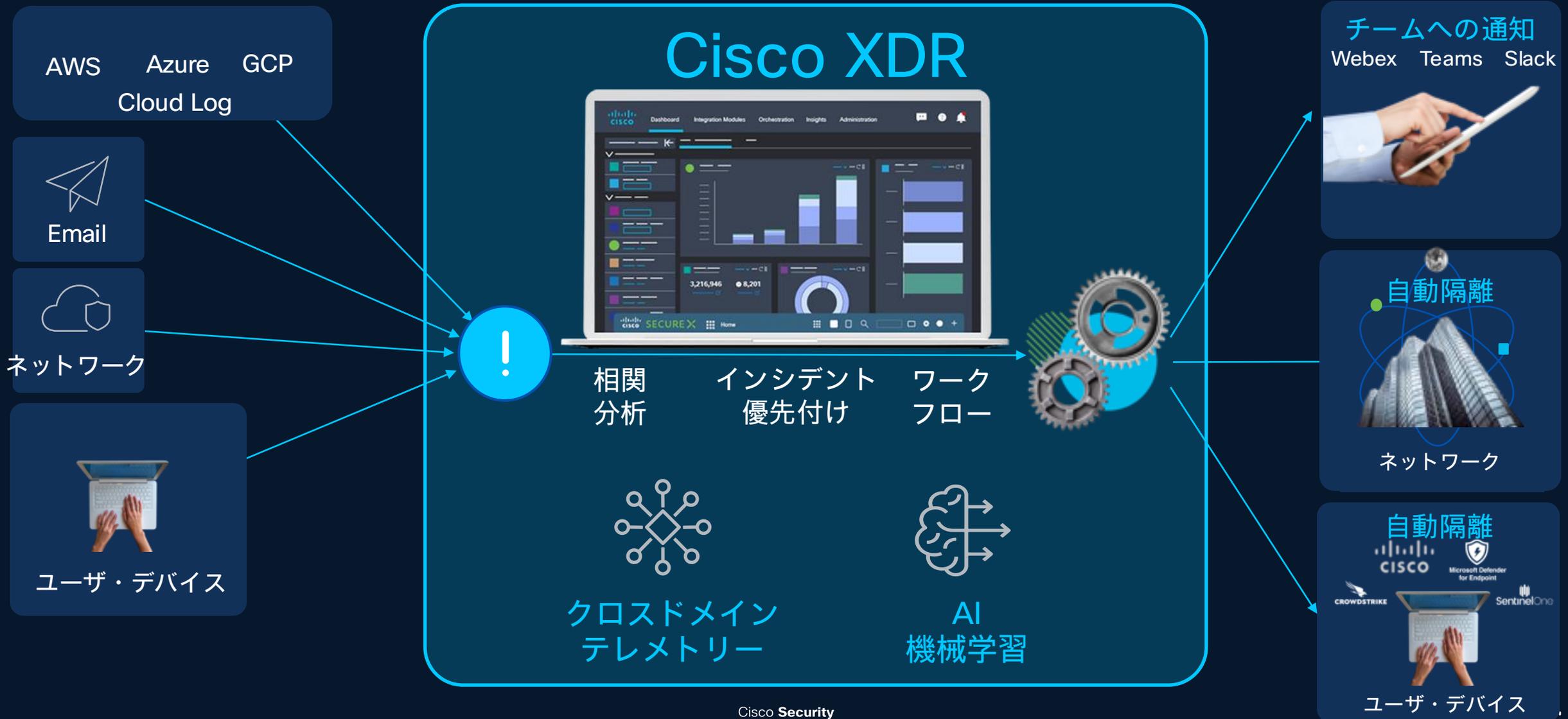
Long description

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



# 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

# 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

## 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。

## 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

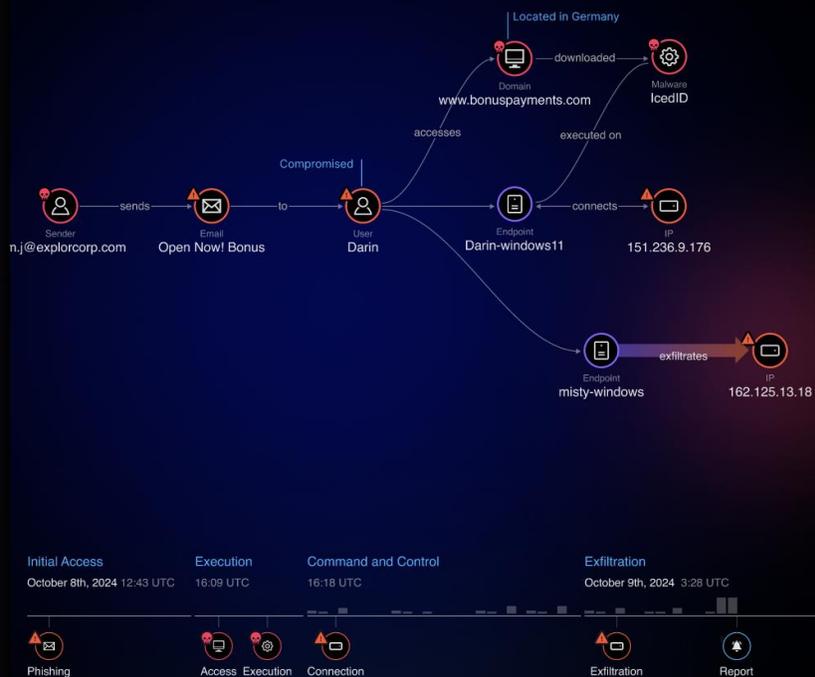
Isolate endpoints to prevent further damage.

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。

The screenshot displays the Automated Forensics interface. At the top, a search bar contains the query 'factura-228447578537'. Below the search bar, a breadcrumb trail shows the navigation path: Home > Tasks > Suspicious Endpoint and User Activity Detected Acquisition 008 > Investigation Hub > Downloads. The main content area is titled 'Downloads' and features a table of search results. The table has columns for 'Flags', 'Finding T...', 'Asset', and 'Path'. Three rows are visible, all with 'Mazzarella' as the asset name and 'C:\Users\alexw\Downloads\factura-228447578537.pdf' as the path. To the right of the table, a 'Details' panel provides information about the selected file, including its path, file existence status, hash, digital signature status, publisher, file size, and modification/access/creation dates.

Flags	Finding T...	Asset	Path
		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**

Path: C:\Users\alexw\Downloads\factura-228447578537.pdf (1).vbs

File Exists: 1

Hash: 1029EDA15FEB6C83BD64AAFA49F6A0216AB7FEFF64542711FB211689FC69D845

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。

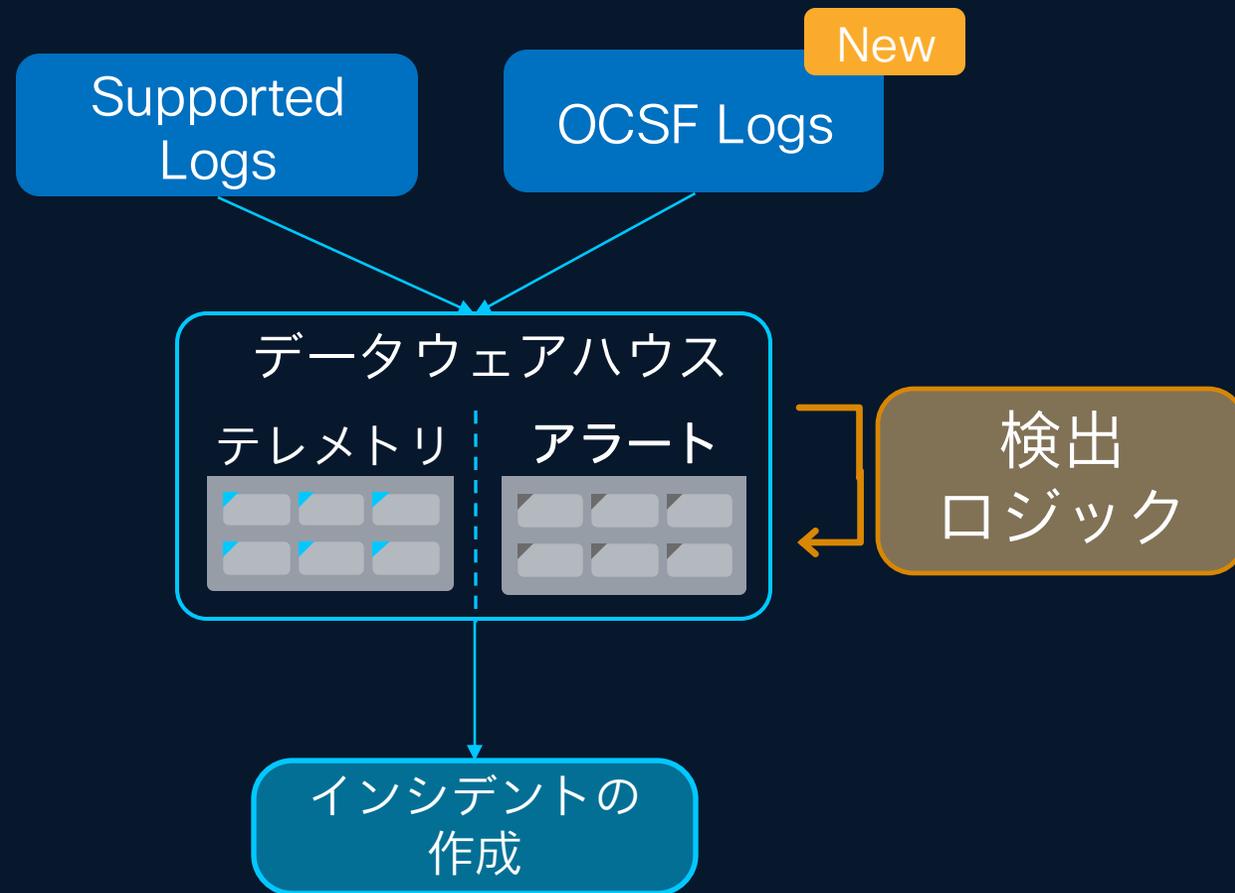
## OCSFとは

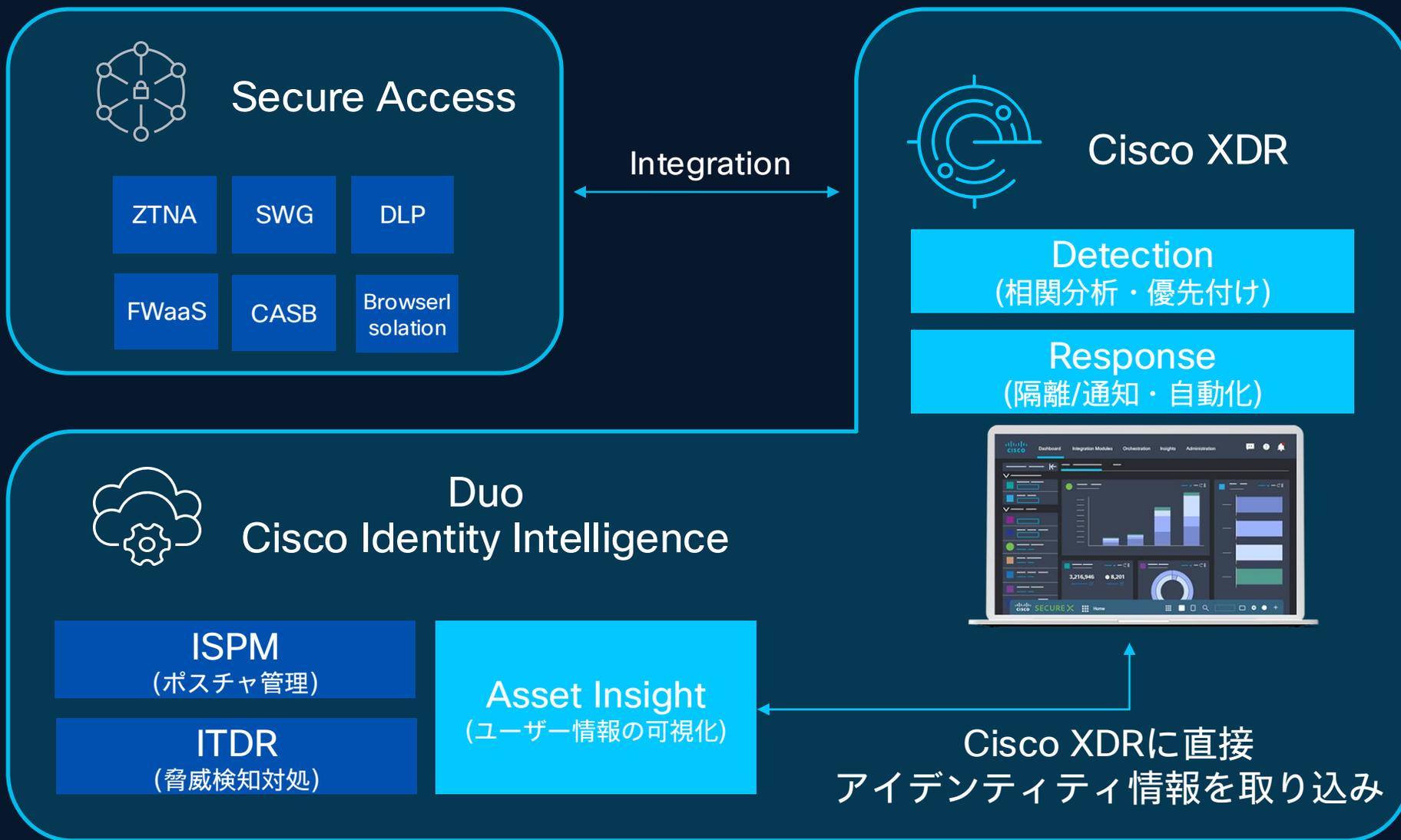
複数のIT企業によって創設されログの統合プロジェクト。

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





# 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

Search

Filters 19,601 matching results

Edit Labels

Export to CSV

<input type="checkbox"/>	Display name	Login names	Emails	Identity events	MFA status	Last logon	Labels	Value	Last active	Used devices
<input type="checkbox"/>	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
<input type="checkbox"/>	Aaron Woland	loxx@cisco.com	loxx@cisco.com	1	Disabled	2025-06-17T18:23:58.074Z		10 (D)	2025-06-17T18:23:58.074Z	
<input type="checkbox"/>	Aaron Woland	loxx@loxx.tv		2	Disabled	2025-05-07T19:32:56.071Z		10 (D)	2025-05-09T19:35:21.000Z	AFIQxQ8F3sSP AFIQxQ8F3sSP AFIQxQ8F3sSP
<input type="checkbox"/>	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	
<input type="checkbox"/>	abcd	abcd@gmail.com	abcd@gmail.com	1	Disabled			10 (D)		
<input type="checkbox"/>	Accounting2	accounting2@securitydemo.net	accounting2@securitydemo.net	1	Disabled			10 (D)		
<input type="checkbox"/>	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}
<input type="checkbox"/>	administrator	administrator		1	Disabled			10 (D)		
<input type="checkbox"/>	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 EPJCFLHTJQTE WAO503VRRUUXG

# Duo連携の成果 (将来像)

← Users  
User - Admin

## Jon Doe

User Tag Medi sg-ca-clientservices User Tag Medi sg-ca-clientservices

**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

### User Identity / Credentials

Email	user@email.com	Company	Company Name	Account Status	<span>Active</span>
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-users sg-gsuite-endusers sg-ca-clientservices
Sources	Duo, AWS, Azure	Job Title	User Experience Designer		

### Access / Authentication

MFA Status	<span>Enabled</span>
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

### 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

# ゼロトラストの脅威を包括管理

Released



# 今日お話ししたいこと

- Cisco XDR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

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）

# XDR ≠ SIEM

---

XDR

生ログ  
なし

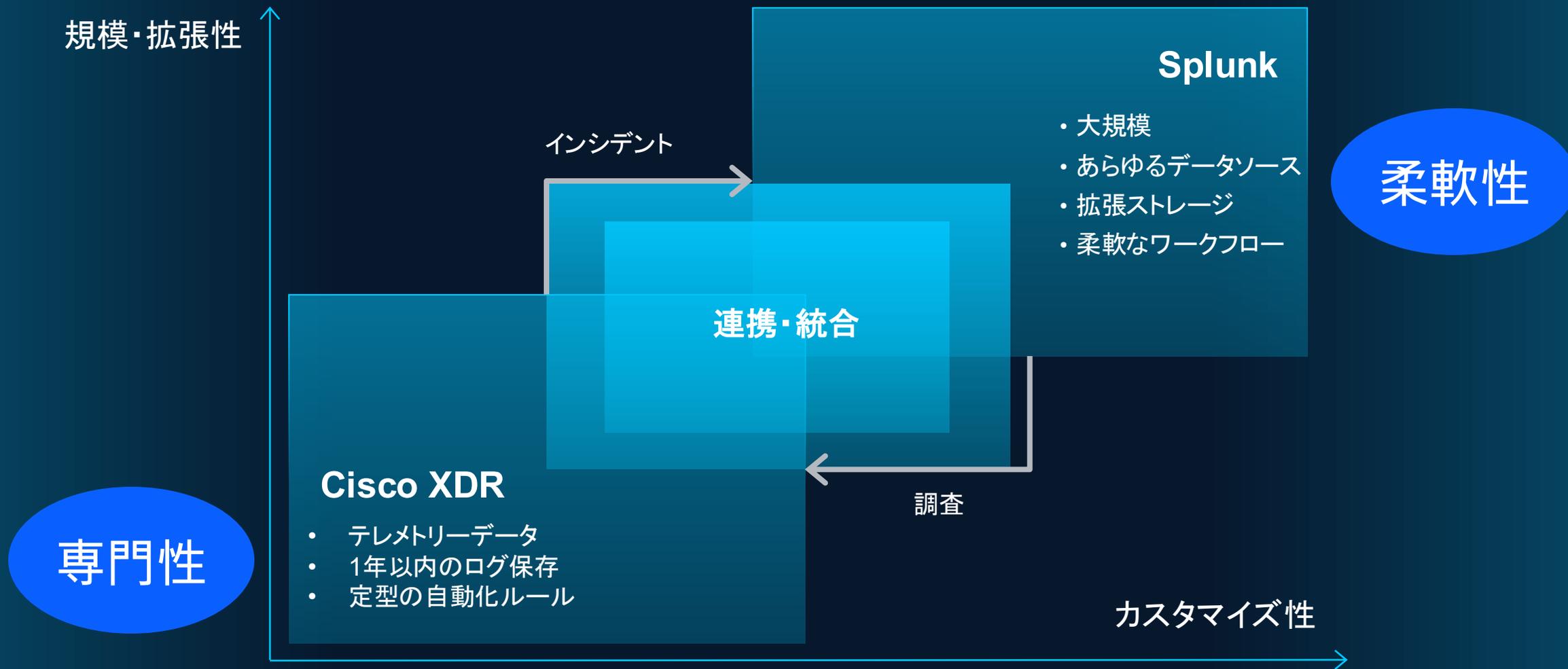
SIEM

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

リスクを特定し認識

- 脆弱性スキャン等

防御

(予防含む)

脅威を防御

- FW / IDS,IPS / WAF / Sandbox / AV Proxy / CASB等

検知

(可視化含む)

脅威および異常を  
監視・検知

- EDR / NDR
- 脅威インテリジェンス
- XDR/SIEM/UEBA**

対応

(分析調査含む)

脅威・異常を分析(調査)  
し、当座の対策を実施

- XDR/SIEM/SOAR**
- フォレンジックツール等

復旧

安全な状態に復旧  
恒久対策の実施

Mean time to Respond

Mean time to Detection

サイバーキルチェーン

偵察

武器化

配送

攻撃

インストール

コマンド  
&  
コントロール

目的の実行

PRE-ATT&CK

ATT&CK



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

リスクを特定し認識

- 脆弱性スキャン等

防御

(予防含む)

脅威を防御

- FW / IDS,IPS / WAF / Sandbox / AV Proxy / CASB等

検知

(可視化含む)

脅威および異常を  
監視・検知

- EDR / NDR
- 脅威インテリジェンス
- XDR/SIEM/UEBA

対応

(分析調査含む)

脅威・異常を分析(調査)  
し、当座の対策を実施

- XDR/SIEM/SOAR
- フォレンジックツール等

復旧

安全な状態に復旧  
恒久対策の実施

Mean time to Detection

Mean time to Respond

サイバーキルチェーン

偵察

武器化

配送

攻撃

インストール

コマンド  
&  
コントロール

目的の実行

PRE-ATT&CK

ATT&CK

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

リスクを特定し認識

- 脆弱性スキャン等

防御

(予防含む)

脅威を防御

- FW / IDS,IPS / WAF / Sandbox / AV Proxy / CASB等

検知

(可視化含む)

脅威および異常を  
監視・検知

- EDR / NDR
- 脅威インテリジェンス
- XDR/SIEM/UEBA**

対応

(分析調査含む)

脅威・異常を分析(調査)  
し、当座の対策を実施

- XDR/SIEM/SOAR**
- フォレンジックツール等

復旧

安全な状態に復旧  
恒久対策の実施

Mean time to Respond

Mean time to Detection

サイバーキルチェーン

偵察

武器化

配送

攻撃

インストール

コマンド  
&  
コントロール

目的の実行

PRE-ATT&CK

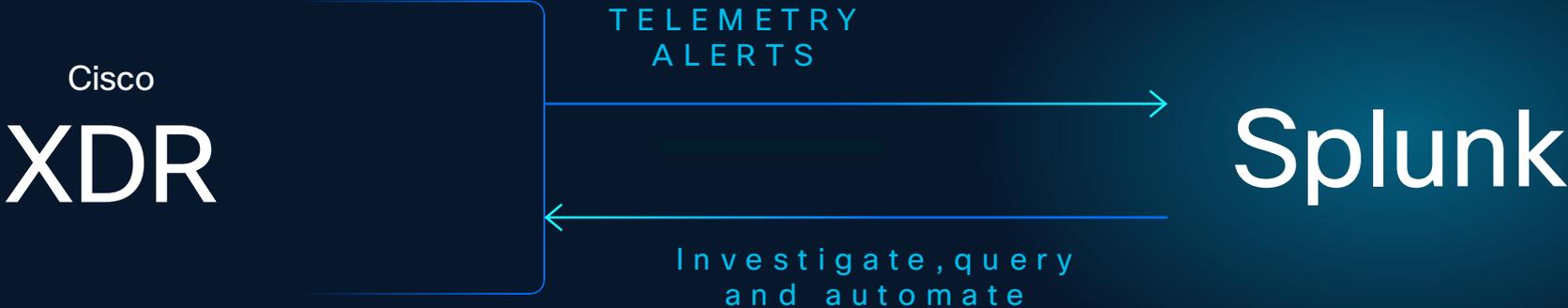
ATT&CK



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

# Cisco XDR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



#### Tier 1:

#### セキュリティオペレーションの簡素化

一元的な可視化

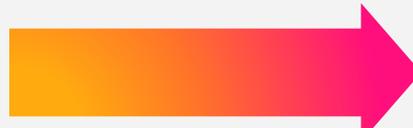
迅速な脅威検出

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



#### 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  
tools0010  
01010  
0101  
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 Community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

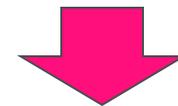


セキュリティ対策にかかる  
コストの最適化

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

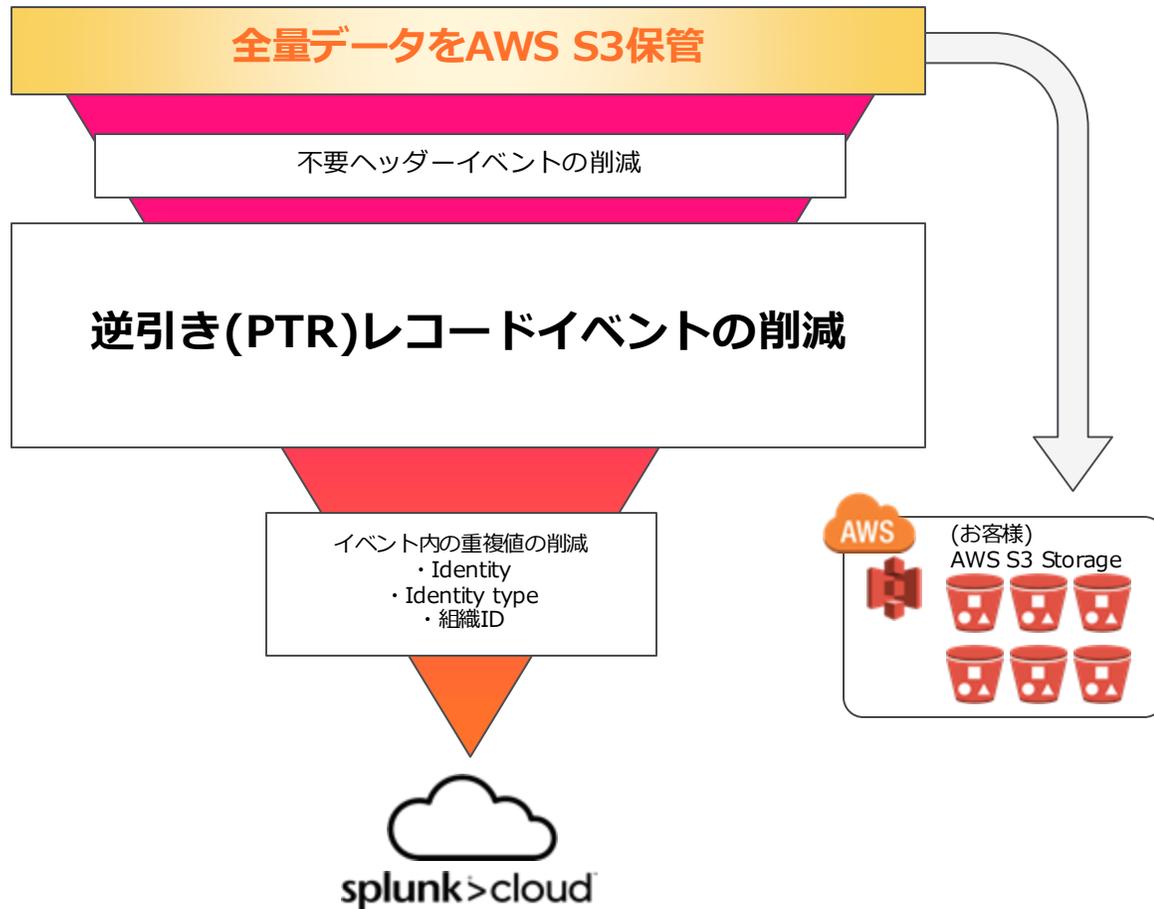


代表的ユースケース：  
SASE/Firewallなどの大量データからLow-Value(不要なイベント)を除外し60%容量削減に成功

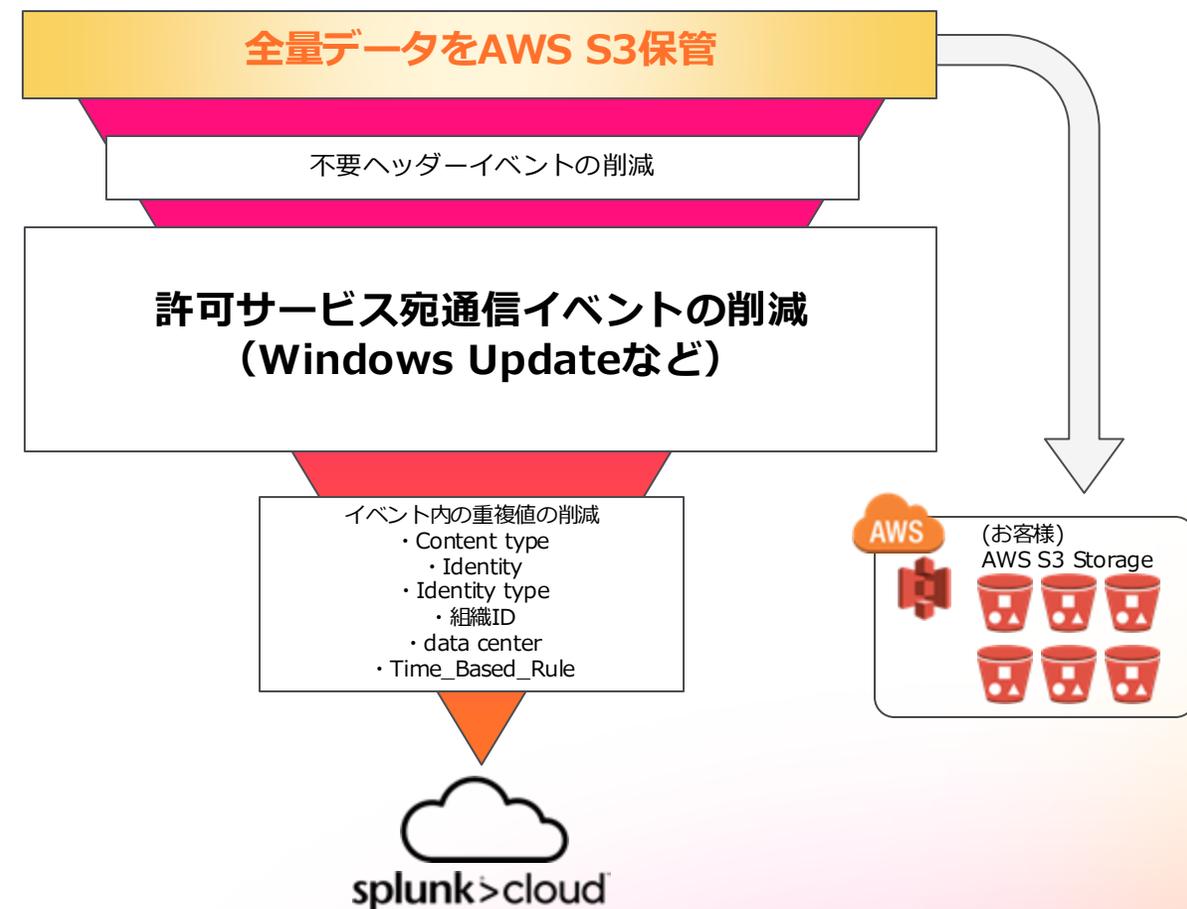
# 例: Cisco Cloud Securityデータのフィルタリングプラクティス

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

The screenshot shows the Splunk interface for filtering DNS logs. On the left, a list of filter actions is shown:

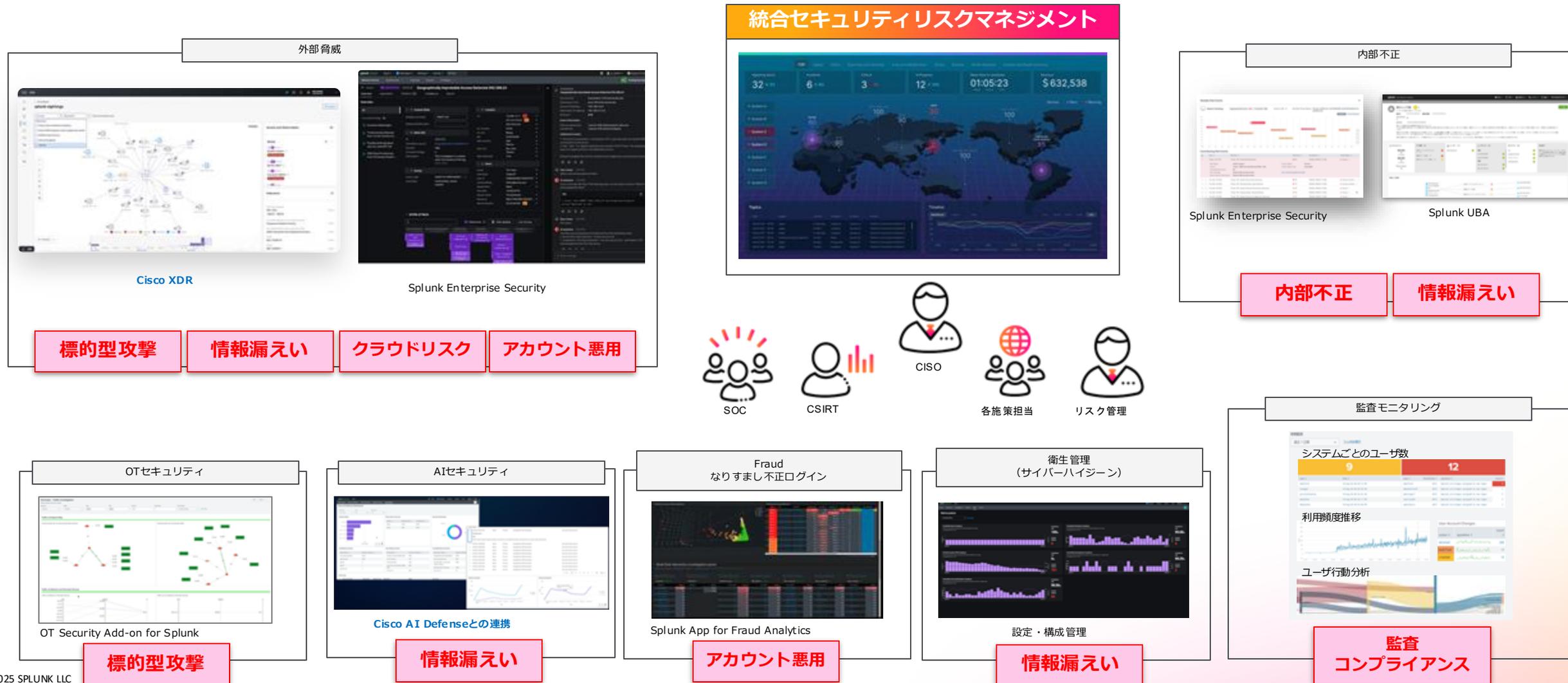
- Event Stream: cisco:cloud\_security:dns, 299KB
- Route to Destination: AWS S3, 0% | 299KB
- Filter using Regex: /\*Timestamp\*/, \*Most Granular I, ↓ 3% | 291KB
- Filter using Regex: /^(?:[\*]\*,){6}\*12 \(\PTR\), ↓ 40% | 174KB
- Mask with Regex: /^(?:[\*]\*,){3}[\*]\*,/, ↓ 4% | 167KB
- Mask with Regex: /^(?:[\*]\*,){11}[\*]\*,/, ↓ 8% | 154KB
- Mask with Regex: /,.\*[\*]\*\$,/, ↓ 3% | 149KB
- Set Index: sse\_after, 0% | 149KB

The right side shows the 'Data Preview for Filter' with the following columns: Time and Event. The preview displays several event entries for 19/6/2025 at 10:10:09.000 and 10:10:08.000. The events include details such as source IP (192.168.67.13), destination IP (163.58.90.198), and event type (Allowed). The filter action is applied to the 'Drop Events Matching Regular Expression' field, which contains the regex: /^(?:[\*]\*,){6}\*12 \(\PTR\),.



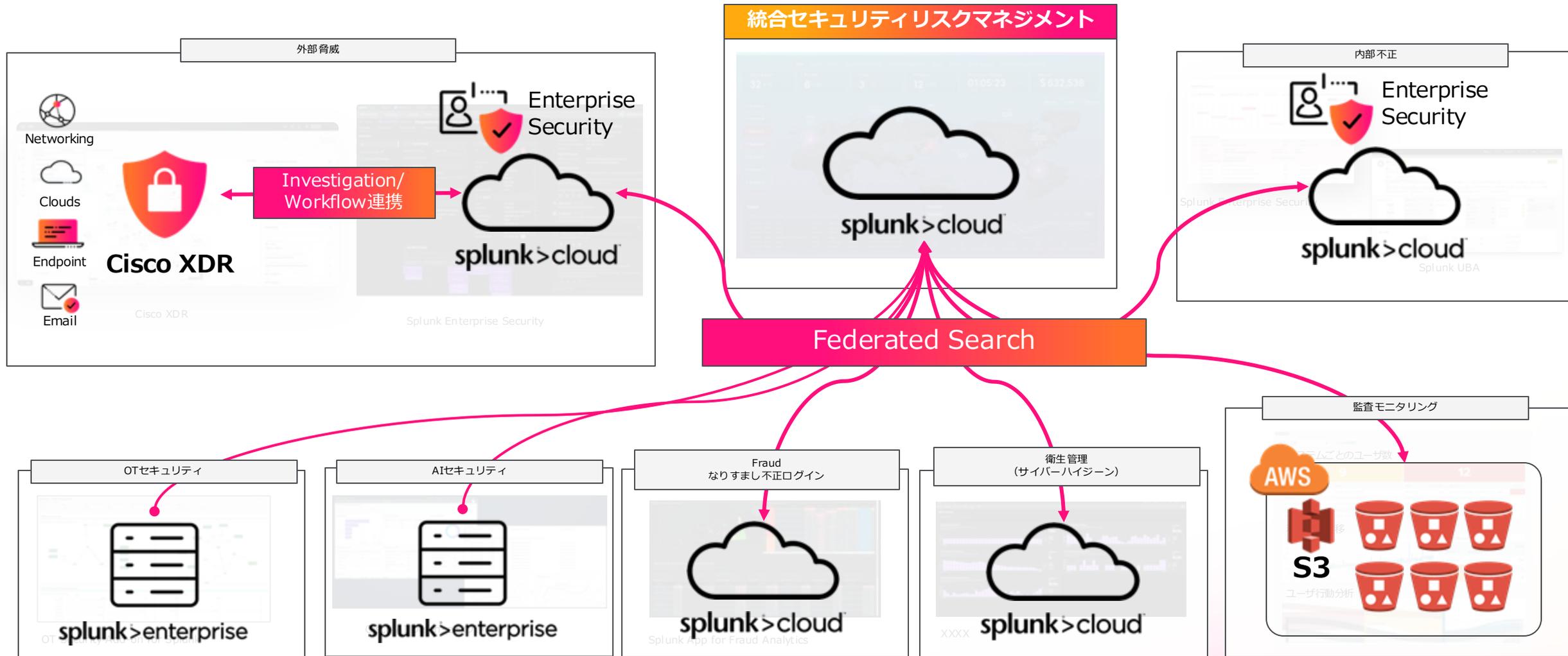
# 様々なセキュリティリスクに対応できるTDIRの重要性

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



# 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



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

## Security Insight, on Us Firewall logs free in Splunk

Free log management\*

AVAILABLE AUG 2025



New detections | Automated response

\* With active Firewall Threat Defense subscription, some limits and constraints apply

# 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

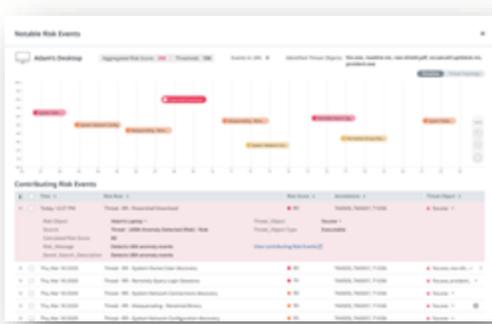
Mean time to Detection を短縮化するための Foundational AI / Gen AI 及びルール評価機能



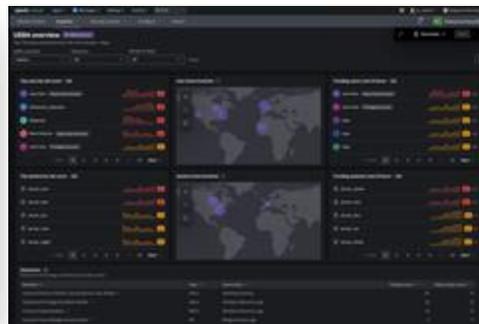
## Foundational AI

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

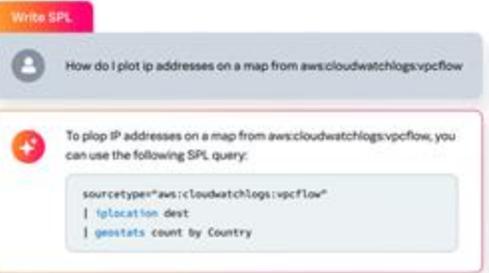


1700個を超えるルールベース、ML/AIベース検知ルールを提供

## Gen AI

自然言語を元に検知ルールを生成

AI Assistant for SPL

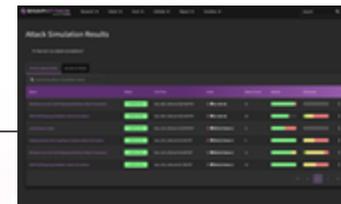


## Rule / AI Rule Validation

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)



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

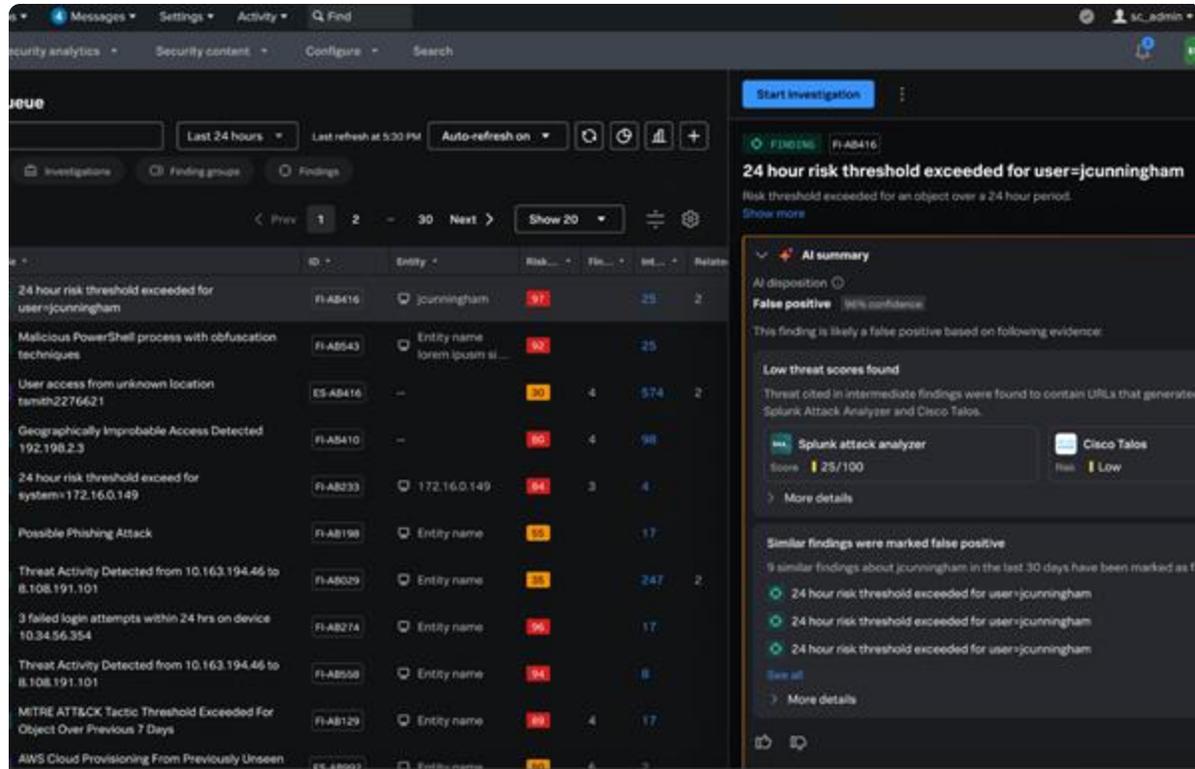
Splunk Enterprise Securityをご利用の場合、Cisco Talosの脅威インテリジェンスを無償提供

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

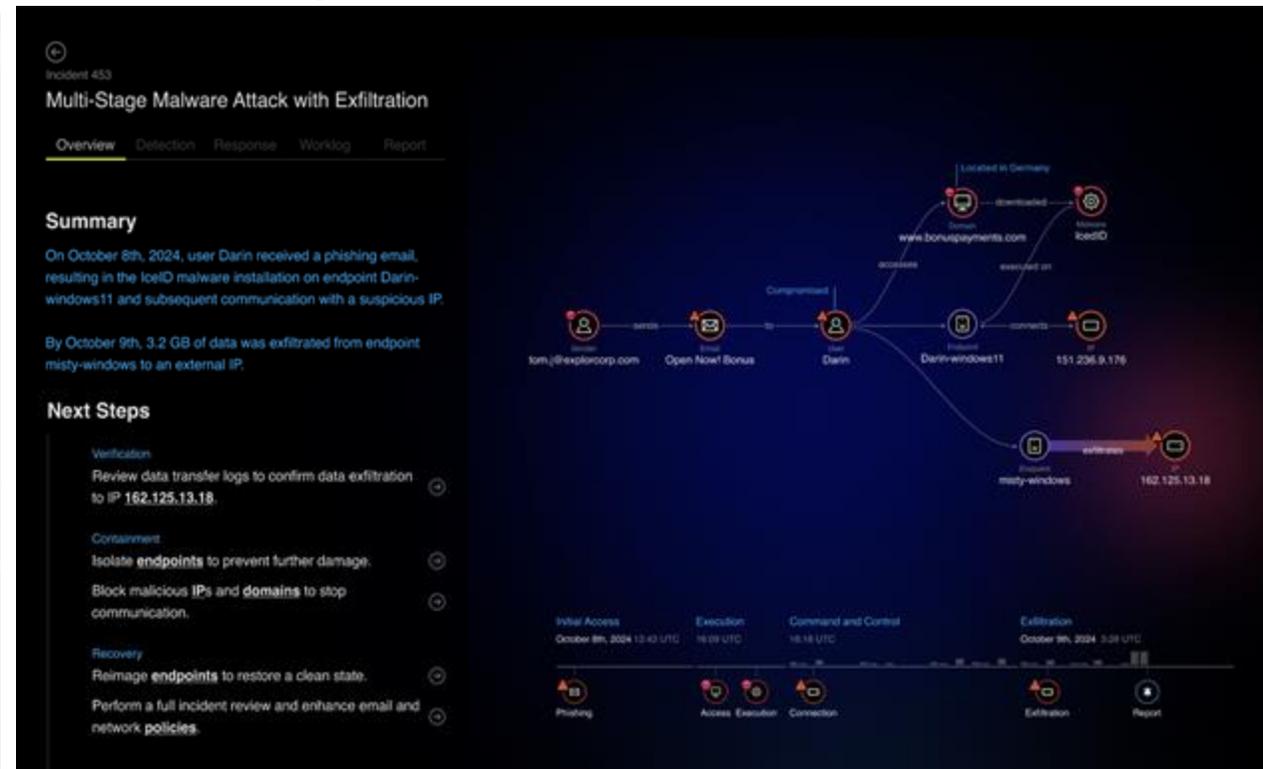
 Enterprise Security - Triage Agent



The screenshot displays the Enterprise Security - Triage Agent interface. On the left, a list of findings is shown with columns for ID, Entity, Risk score, and other metrics. The right pane shows an AI summary for finding FI-AB416, titled "24 hour risk threshold exceeded for user=jcunningham". The AI summary includes a "False positive" classification with a confidence level of 92%, a "Low threat scores found" section, and a "Similar findings were marked false positive" section. The interface also shows a "Splunk attack analyzer" and "Cisco Talos" risk scores.

**Agentic AI** に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



The screenshot displays the Cisco XDR - Instant Attack Verification interface for Incident 453, titled "Multi-Stage Malware Attack with Exfiltration". The interface shows a summary of the attack, including a timeline of events from October 8th to 9th, 2024. The summary describes a phishing email received by user Darin, leading to the installation of IoelD malware on endpoint Darin-windows11 and subsequent communication with a suspicious IP. A timeline at the bottom shows the attack stages: Initial Access (October 8th, 13:43 UTC), Execution (16:03 UTC), Command and Control (16:16 UTC), and Exfiltration (October 9th, 3:28 UTC). The next steps section includes verification, containment, and recovery actions.

**Agentic AI** に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**

