Cisco
Customer Experience

Ask the Experts

機能概要（応用編）：Cisco Secure Network Analytics と SIEM の統合および対応管理の構成
（Advanced Feature Overview: Configuring Response Management and Integrating Cisco Secure Network Analytics with SIEM）

Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

本日の学習内容：

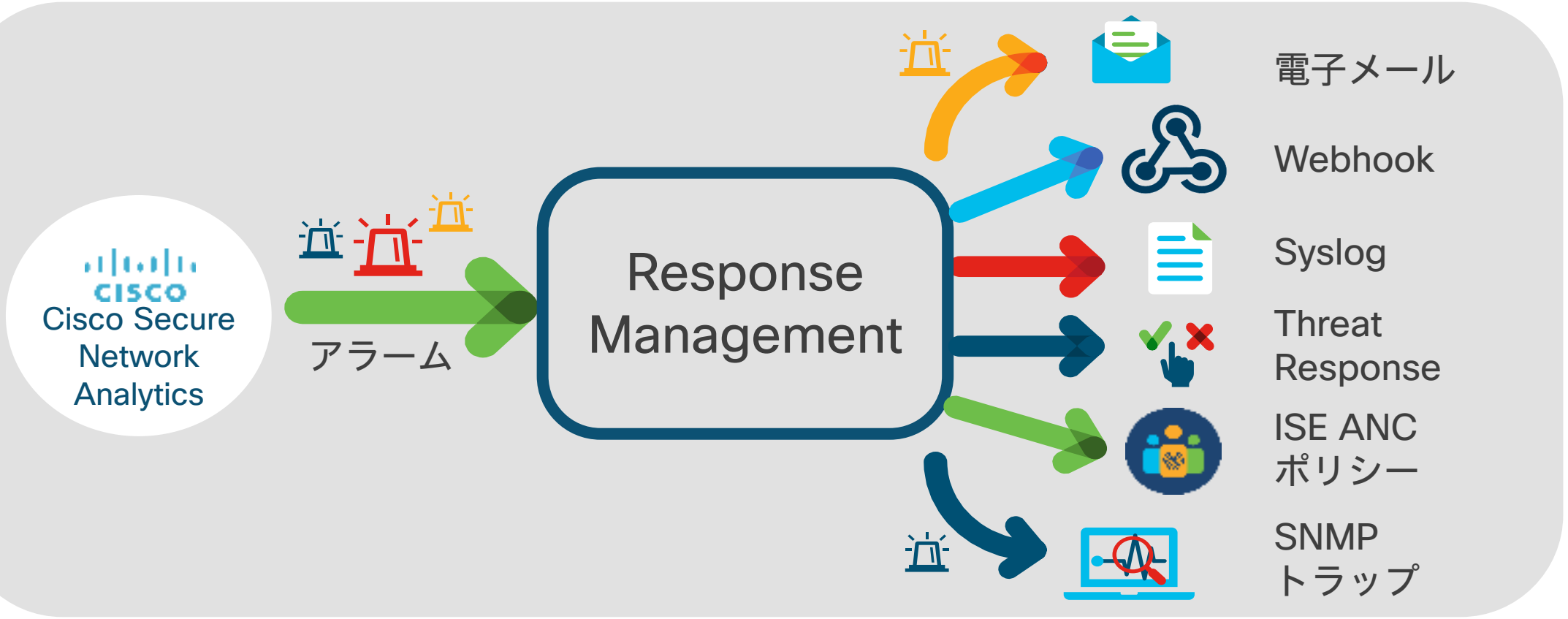
- Response Management の概要と使用方法
- Response Management を使用する利点
- Response Management のルールとアクションを作成する手順
- Response Management のデモ

本日のトピック

1. Response Management の概要
2. Response Management の利点
3. Response Management の仕組み
4. デモ

Response Managementの概要

Response Management の概要



Response Management の利点

Response Management の利点

- 手動で行う反復作業を削減
- アラームへのCisco Secure Network Analytics の対応方法を制御
- 焦点を当てるべきポイントの優先順位付けを支援
- インシデント対応の迅速化と効率化

Response Managementの仕組み

Response Management モジュールの刷新

自動対応

定義された条件に一致した場合、　　割り当てられたアクションを自動で実行

設定可能
- ルール
- アクション
- 対応タイプ

(If) この**条件**が満たされたら、 (Then) この**アクション**をトリガーする

ルール
アラームの内容

アクション
アラームへの対処方法

- ルール：1 つまたは複数定義された条件のリスト。アクションをトリガーするタイミングを定義する 。
- アクション：ルールにに関連付けられ、特定のタイプの処理を実行する。

Response Management の使用手順

01

ルールがトリガーされたときに SNA に実行させたいアクションを設定

02

要件に適したルールを選択

03

ルールをトリガーするための条件を作成

04

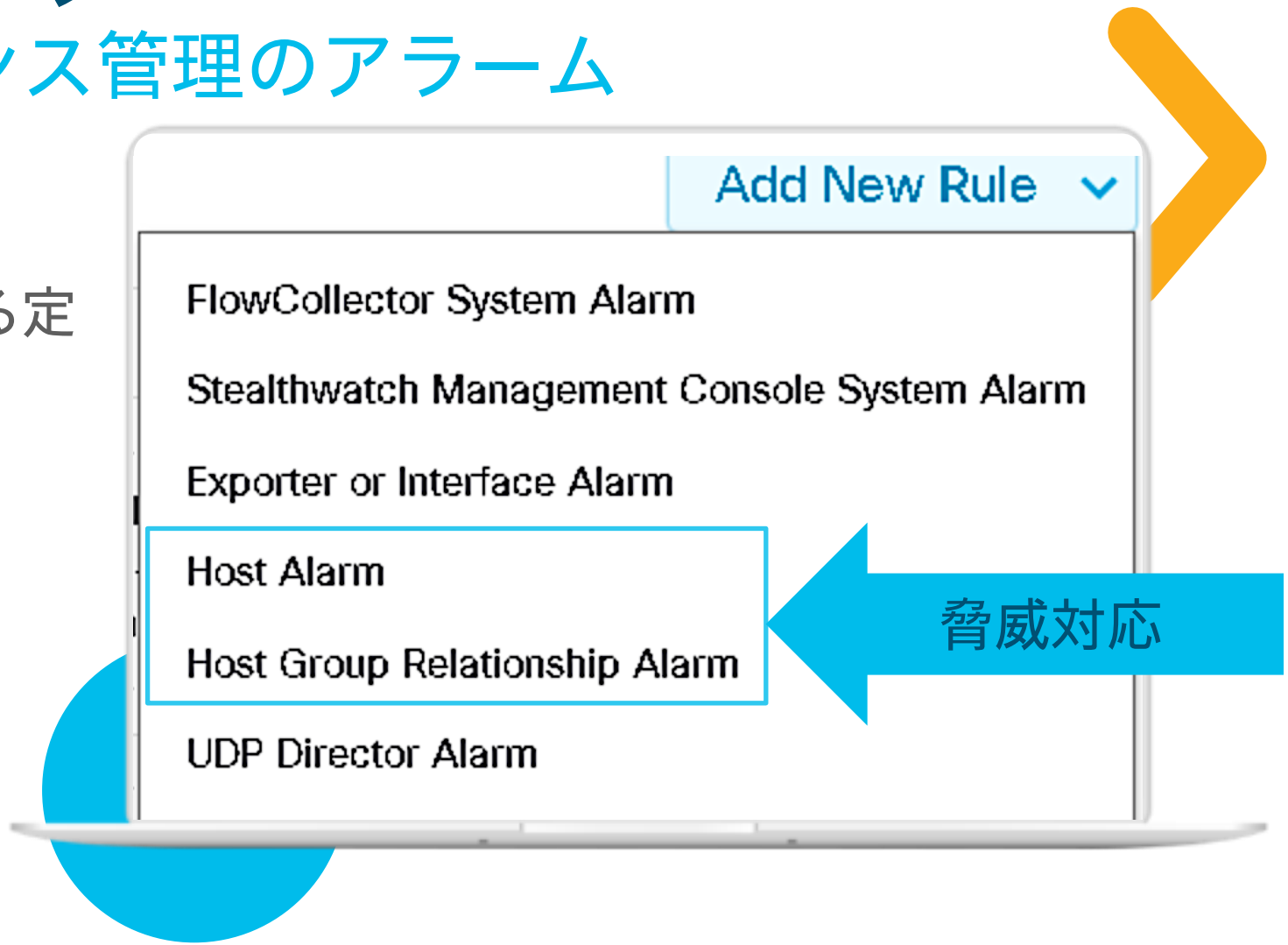
アラームに対応するために SNA が実行するアクションを割り当て

ルールとルールタイプ

脅威対応とアプライアンス管理のアラーム

SNA イベントの特性に関連する定義された一連の条件。

イベントがルールに定義された一連の条件に一致する場合、割り当てられたアクションがトリガーされる。



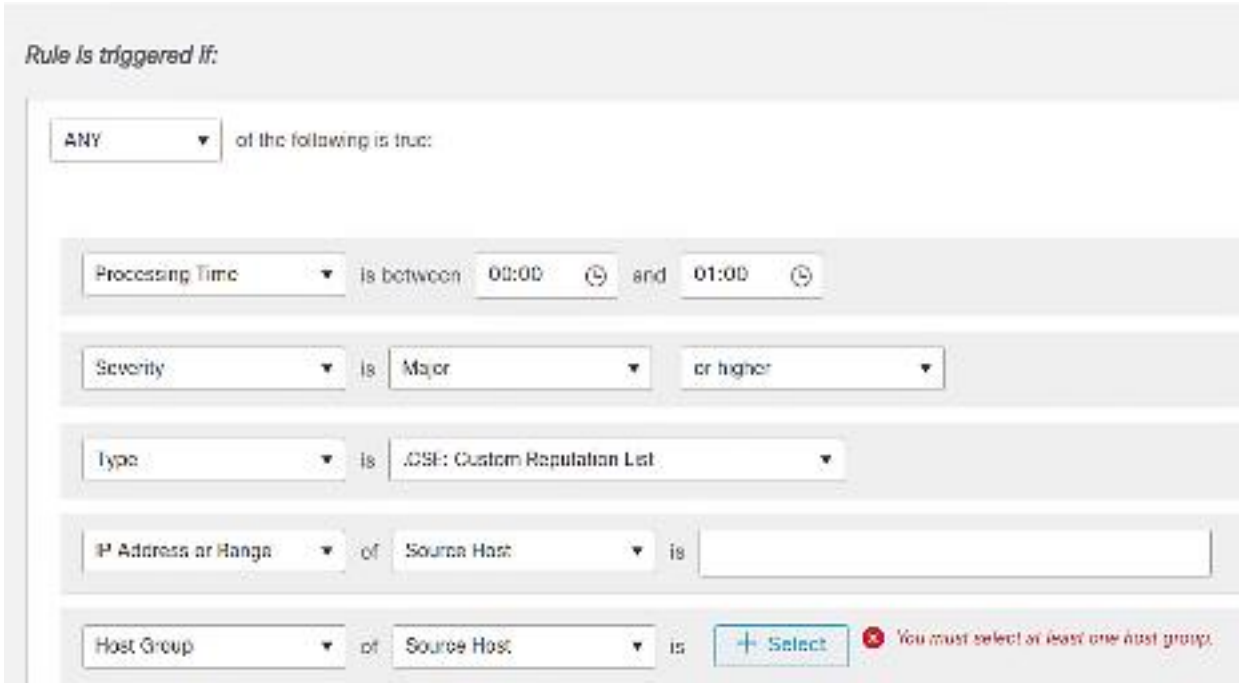
条件の指定

「If/Then」ステートメントの「If」部分

まず、ルールがトリガーされるために満たす必要がある条件を決定

- [すべて（All）]：すべての条件を満たした場合にルールをトリガー
- [いずれか（Any）]：いずれかの条件を満たした場合にルールをトリガー
- [なし（None）]：いずれの条件も満たさなかった場合にルールをトリガー

次に、アラームをトリガーするために満たす必要のある条件セットを選択。
複数の条件セットを利用可能



事前定義されたルール

Response Managementには、事前定義された一連のルールが用意されている

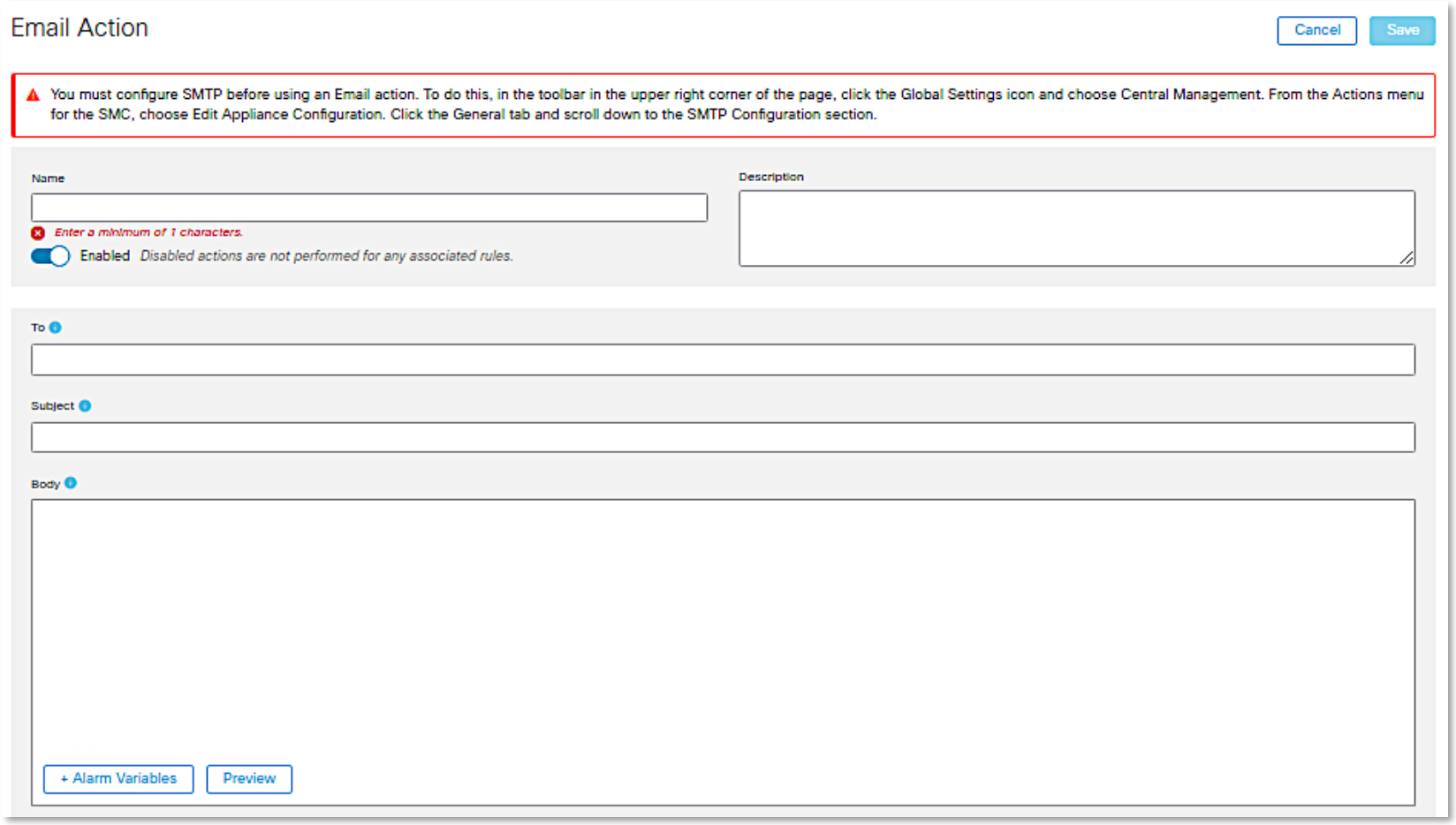
- All Exporters or Interface Alarms
- All FlowCollector System Alarms
- All SMC System Alarms
- All UDP Director Alarms
- Trapped Host Alarm

- Inside Hosts as the source of alarm
- Outside Hosts as the source of alarm
- Priority A: Severity Critical
- Priority B: Severity Major
- Priority C: Severity Minor

アクション

Syslog メッセージ	指定されたデバイスに Syslog メッセージを送信
電子メール	指定された電子メールアドレスに電子メールメッセージを送信
SNMP トラップ	指定されたデバイスに SNMP トラップを送信
ISE ANC ポリシー	ホストアラームがトリガーされたソースまたはターゲットのホストに適応型ネットワーク制御（ANC）ポリシーを適用
Webhook	Web サービスまたは REST API を介して SNA を外部システムと統合
Threat Response Incident	Cisco SecureX Threat Response にアクティブなイベント検出結果を送信

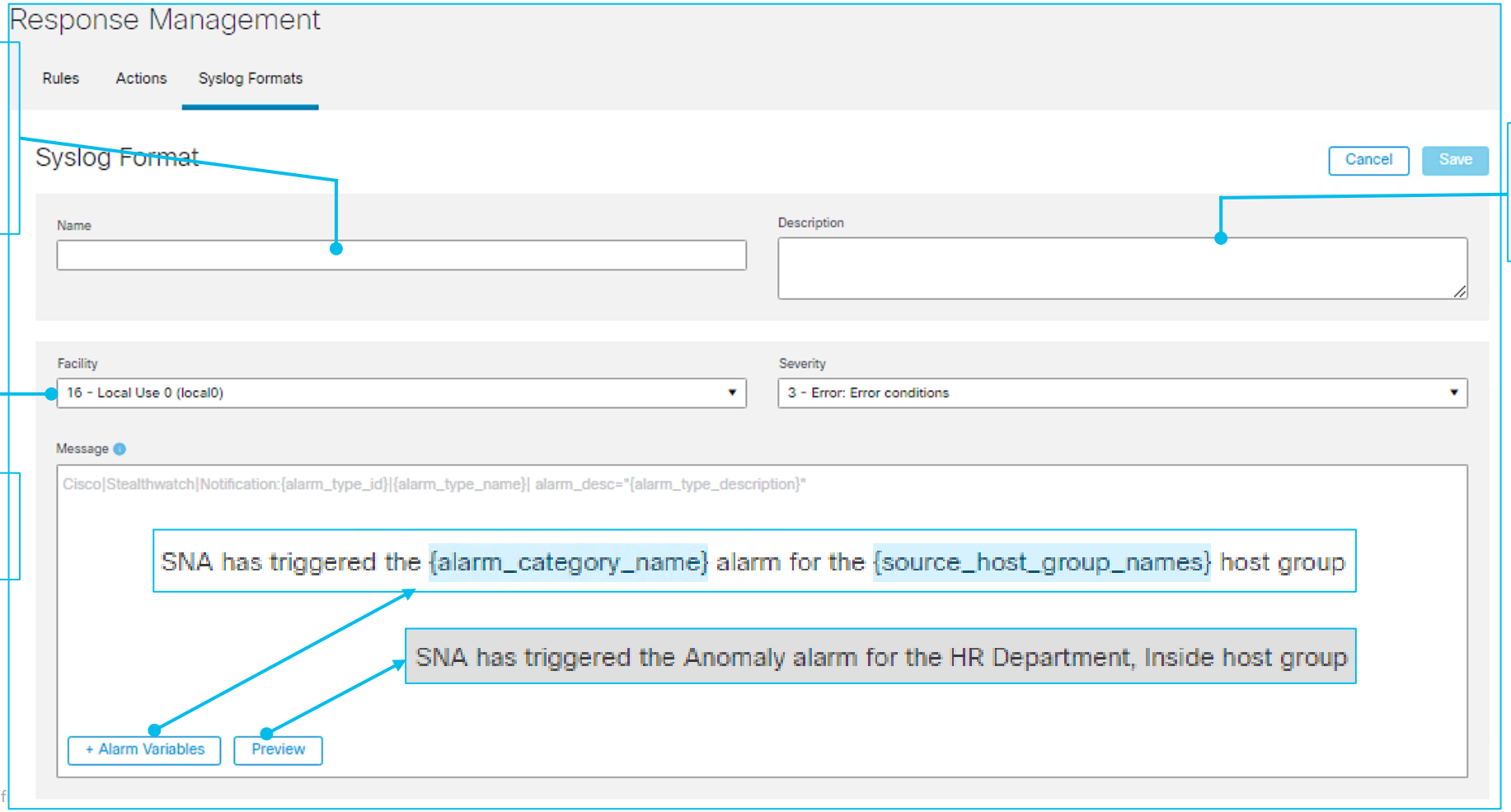
電子メールアクションタイプ



Syslog メッセージアクションタイプ
SIEM との統合

意味のある名前を付けると、ルールとの関連付けがしやすくなる

Syslog Facilityの設定



このメッセージの目的を明確に記述

最小要件

Response Management の基本要件（WebUI）

- Cisco Secure Network Analytics バージョン 7.3.0 以降
- SNA Manager および Flow Collector

ISE ANC ポリシーアクションの要件

- SNA と ISE の統合（pxGrid を使用）

Threat Response Incident アクションの要件

- SecureX Threat Response 関連の設定を含め、SNA と SecureX の統合

本日の振り返り

Response Management により、特定の条件に対する SNA の応答方法をより詳細に制御

この機能によってを使用することで、アラーム監視と対応の優先順位付けを効率化

一部のアクションタイプは、ISE や SecureX との統合が必要

SNA のコンポーネントで行き詰った場合は、デモで紹介したようにオンラインヘルプを活用

Q&A

右側のQ&Aウィンドウよりご質問ください

Resources

- Secure Network Analytics ATXsリソースリンク集
- https://community.cisco.com/t5/-/-/ta-p/4633653
- ※本日のATXs以外のリソースリンクも確認できます。

Cisco
Customer Experience