Swimlane Solutions and Applications

1. Solutions and Applications
    1.1. AI SOC Solution
        1.1.1. Architecture and Data Flow
        1.1.2. Installing and Configuring AI SOC Solution
            1.1.2.1. Swimlane Content, User Content, and Integrated Marketplace
            1.1.2.2. Configure Custom Assets

1. Solutions and Applications

1.1.4. AI SOC Ingestion

1.1.6.4. Signal Routing Rules (RULE)

Signal Routing Rules control how signals are routed to playbooks. Each rule is a **record** (for example, RULE-29) that you can open, edit, and enable.

Routing Rule Management dashboard

The primary place to manage routing rules is the **Routing Rule Management** dashboard. The dashboard shows all rules in a table ordered by **Rule Order** (ascending). Rule order is **unique** and evaluated like firewall rules: the **first matching rule** runs, so order matters.

From the dashboard you can:

- **Reorder rules:** Use the **drag handles** (stack of dots) in the **Order** column to drag and drop rules into the desired order. Reordering changes which rule runs first when multiple rules could match.
- **Open the rule record:** Click the **ID** column icon (open-in-new view) or the **Edit** (pencil) icon to open the rule record and change conditions, playbook, or description.
- **Open the associated playbook:** Click the **Associated Playbook** link to open the playbook that runs when the rule matches.
- **Enable or disable a rule:** Use the **Enabled** toggle for each row. Rules are inactive when disabled; only enabled rules evaluate and trigger playbooks.
- **Edit a rule:** Click the **Edit** (pencil) icon to open the rule record in a slider or view so you can modify conditions, **Rule Application**, **Selected Playbook**, or other fields.
- **Delete a rule:** Use the **Delete** (trash) icon to remove a rule. Use with care; deletion cannot be undone from the UI.

Use **Add New Rule** on the dashboard to create a rule, or **Apply** to save order changes after reordering.

1) Open **Signal Routing Rules**

- Navigate to **Application Records** -> **Signal Routing Rules** or open the **Routing Rule Management** dashboard to view and manage all rules.
- Open an existing rule via the dashboard **Edit** icon or by opening it from the application list.

2) Open fields

1.1.8. Dashboards and Reports

1.1.8.1. Dashboards

1.2.2. SOC - Alert Ingestion (Webhook) - Template Playbook Overview

This document provides detailed information about the **SOC - Alert Ingestion (Webhook) - Template** playbook, which ingests alerts via webhook events, processes them, and handles actions such as enrichment, correlation, and case creation. Users need to configure only the following components:

- **Placeholder - Create TEDS Alert (Webhook)**
- **Custom Alert Data Extension (Webhook)**
- **Correlate (Webhook)**

Note: These playbooks can and should be **duplicated** and the **Placeholder - Create TEDS Alert (Webhook)** component swapped out to match the technology stack in your organization. This ensures the playbook works seamlessly with your chosen vendor's tools.

Overview

- **Objective:** Automate webhook-based alert ingestion using Turbine logic to process alerts and transform them into actionable items.
- **Key Workflow Steps:**
  1. Alerts are ingested through webhook events.
  2. Fetched alerts are standardized into TEDS objects.
  3. Each alert undergoes deduplication, enrichment, and correlation.
  4. Enriched and correlated alerts are used to create cases for investigation.

Accessing the Playbook

To access the playbook:

1. Navigate to **Orchestration** in the Swimlane platform.
2. Click on **Playbooks**.
3. Select **SOC - Alert Ingestion (Webhook) - Template**.

Loop-Based Alert Processing in the Playbook

1.3.4. Dashboards in BCM

1.3.5. References

1.4.7.1. Creating Custom Evidence Records

1.7. Detection Engineering Extension

1.8.2.4. Processing and Enrichment

1.8.2.5. Filtering and Deduplication

1.8.3.3. Vulnerability Case Management

1.8.5. References

1.8.5.1. Vulnerability Finding Data Model