Swimlane Solutions and Applications

1. Solutions and Applications

Turbine solutions are end-to-end use cases that contain components, playbooks, and assets that are mostly preconfigured to reduce a practitioner's time and level of effort when creating common security solutions.

Current Turbine Solutions

Solutions are available in Turbine under **Library** → **Swimlane Content**. Current solutions and extensions include:

Solution	Description
AI SOC Solution	AI-powered SOC solution for alert ingestion, signal triage, threat intelligence enrichment, and case management. Includes Hero AI–driven investigation plans, signal routing rules, dashboards, reports, and the AI Ingestion application for building connectors and ingestion pipelines.
SOC Solutions Bundle	Security operations center solution for SOC workflows, triage, and response.
Swimlane AI Agents Case Management Extension	Part of the SOC Solutions Bundle. Provides Hero AI agents and a unified UI to speed up SOC analyst workflows for triage, investigation, and incident response. Integrates with the Case and Incident Management (CIM) application; includes on-demand and automated Hero AI analysis, verdict and threat intelligence analysis, and MITRE ATT&CK & D3FEND mapping. Install from **Library** → **Swimlane Content** after the SOC Solutions Bundle is installed.
Business Continuity Management (BCM) Solution	End-to-end use case for business continuity and resilience planning, testing, and response.
Complian	Solution for managing compliance controls, evidence, and audit readiness

1.1.4. AI SOC Ingestion

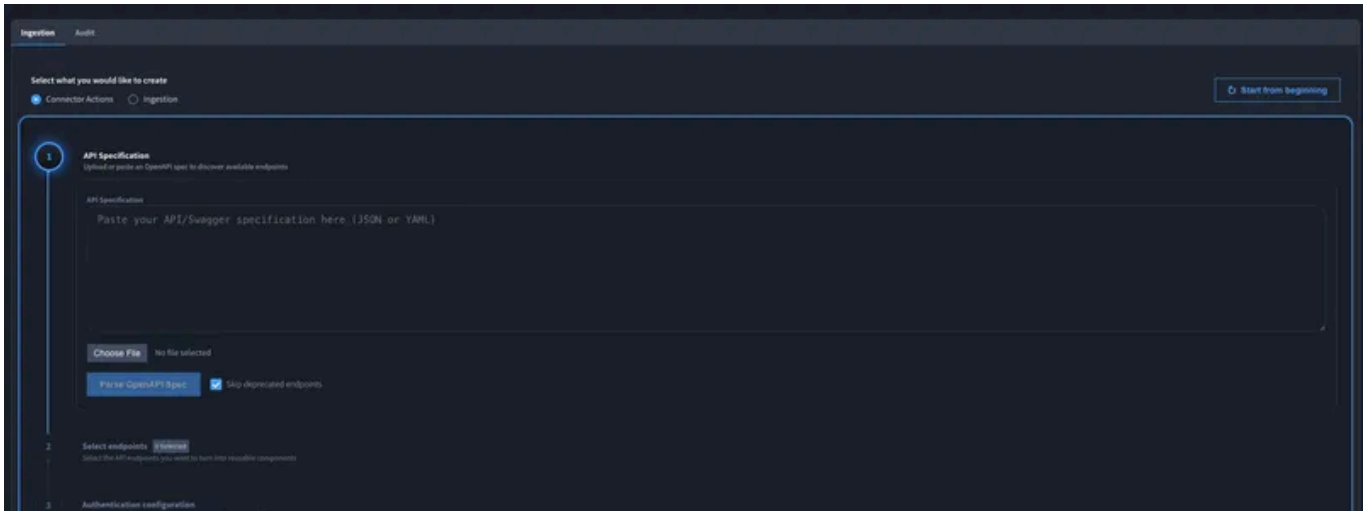
The **AI Ingestion** application helps you build vendor connectors and alert ingestion pipelines quickly — without writing code or learning JSONata. A guided custom widget builds Turbine components from an uploaded OpenAPI specification, one per endpoint. Hero AI then assists in mapping incoming raw alert data — from any source — to a standardized Turbine Schema object, producing an ingestion component ready to use in downstream AI SOC playbooks.

Why Use the AI Ingestion

Use the AI Ingestion when you want to **integrate new alert sources faster**, **prototype ingestion paths** against real vendor APIs, and **hand standardized Turbine Schema output** to your existing AI SOC playbooks without hand-building every connector and mapping from scratch.

What it helps you do:

- **Quick integration:** Upload an OpenAPI specification and generate Turbine components per endpoint so you can connect to vendor APIs in a repeatable way.
- **Prototyping and iteration:** Test API calls, inspect sample payloads, and adjust mappings before you commit to production routing and automation.
- **Consistent normalization:** Hero AI suggests how raw vendor fields map to Turbine Schema fields (the Turbine Schema is the mapping target you work against) so alerts land in a predictable shape for downstream Flows.
- **Reuse across playbooks:** Components you generate can be referenced from multiple playbooks and templates, so you invest once and reuse.



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) Core fields

1.1.8. Dashboards and Reports

1.1.8.1. Dashboards

Dashboards provide real-time visibility into SOC operations through interactive widgets. Use dashboards to monitor current state, identify trends, and quickly access records requiring attention.

The **AI SOC** workspace in current packages (for example, AI SOC beta v1.2.4) includes these dashboards: **Routing Rule Management**, **Analyst Triage Queue**, **Security Operations Overview**, **MITRE ATT&CK Techniques**, and **Threat Intelligence Overview**. If your workspace lists different dashboard titles, open **Dashboards** under the **AI SOC** workspace and use the view that matches your need (queue, overview, MITRE, or threat intelligence).

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

Program Overview

For BCM Managers:

- **BCM Sankey View** – lifecycle of Critical vs. Not Critical BIAs.
- **Resource Type Distribution** – donut charts across Applications, Buildings, Employees, and so on.
- **Pre-Screening Results** – breakdown of Critical vs. Not Critical.
- **Tasks by Status** – Completed, Not Started, WIP, Cannot Complete.
- **BIAs by Status** – bar chart view.
- **Threat Scenarios by Type** – count of risks by type.

BIA Owner

For business process owners:

- **My BIAs Sankey** – statuses of owned BIAs.
- **My BIAs List** – detailed table (Criticality, Status, RTO, Last Review).
- **Approval Records Over Time** – historical approval trends.
- **Approval Status Chart** – pending, approved, denied.

Pending Approvals – records awaiting action.

1.3.5. References

Application Record Schemas

Resources

Field	Type	Required	Description
Resource Name	String	Yes	Name of the resource.

1.4.7.1. Creating Custom Evidence Records

You can create custom evidence records for requirements not covered in the pre-populated records. Custom evidence will be highly leveraged for controls in the catalog that do not have pre-defined evidence records mapped to them out of the box.

Steps to create a custom evidence record:

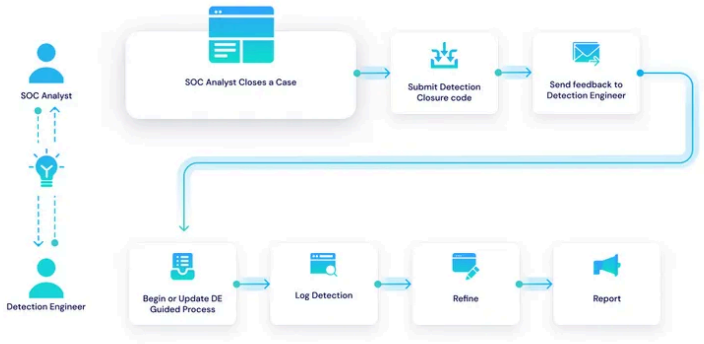
1. Navigate to SCF Evidence Application, click + New Record to start a custom evidence entry.
2. Set **Evidence Status**
3. Use the Evidence Status dropdown to indicate the current state of the evidence (for example, Not Started, In Progress, Ready, or Expired).
4. Select **Evidence Collection Type**
    - Manual Upload (PDF, Word, Excel, etc.)
    - External URL (for example, links to internal wikis or cloud storage)
    - Monitored in Turbine (for automation-based artifacts)
5. Attach Supporting Materials
    - Drag and drop files into the Evidence Artifacts upload area.
    - Populate the External URL field if evidence is stored remotely.
    - If applicable, link relevant Turbine playbooks in the Referenced Playbooks section.
6. Describe the Evidence
    - Context for the evidence
    - How the control is met
    - Hyperlinks to additional resources
7. Fill Metadata Fields
    - ERL #: Optional custom identifier.
    - Area of Focus: Security domain the evidence addresses.
    - Documentation Artifact: Defaults to Custom.
    - Custom Documentation Artifact Name: Provide a descriptive title.
    - Evidence Owner and Title: Identify the responsible party.

1.7. Detection Engineering Extension

Overview

The Detection Engineering Extension is a comprehensive suite of content components, including Playbooks, Applets, Applications, Reports, Dashboards, and more, designed to enhance the efficiency and effectiveness of detection engineering within a security program.

This extension equips Detection Engineers with the necessary tools to effectively identify, develop, and iterate on detections, ensuring the continuous improvement and optimal performance of a SOC's detection capabilities. Additionally, it provides a centralized system of record for the organization's current detection posture. The extension also bridges the feedback loop between analysts and Detection Engineering by facilitating the collection of detailed feedback from analysts directly into the Detection Library application.



Capabilities

- **Centralized System of Record for Detection Use Cases within a SOC**: A unified platform to maintain and manage all detection use cases, ensuring consistent documentation and easy access within the Security Operations Center (SOC).
- **Guided Best Practice Detection Engineering Process**: A prescribed workflow that provides a structured and efficient approach to detection engineering, ensuring adherence to best practices.
- **Case & Incident Management Extension**: An integrated extension that links analyst feedback from the Detection Library with relevant closure codes, streamlining the incident management process and ensuring a comprehensive feedback loop.

1.8.2.4. Processing and Enrichment

1. Scheduled Flow Picks Up Pages
    - A system flow runs every 10 minutes.
    - For each page:
        - JSON content is read
        - Findings are mapped via TEDS and sent to enrichment individually
        - Errors or duplicates are logged
2. Enrichment Pipeline Handles Each Finding
    - Enrichment applies logic like asset association, severity evaluation, and deduplication.
    - Deduplication uses **VRM - Export Results** to skip known findings
3. Monitoring and Reporting
    - Dashboards and page records display real-time ingestion health.
    - **VRM - Filtering Activity** shows what was skipped, added, or reused.

1.8.2.5. Filtering and Deduplication

Metrics and Logic

During ingestion, VRM compares each batch of findings against the most recently processed export to detect and exclude previously seen data. This ensures only new or modified findings are enriched.

Metrics tracked include:

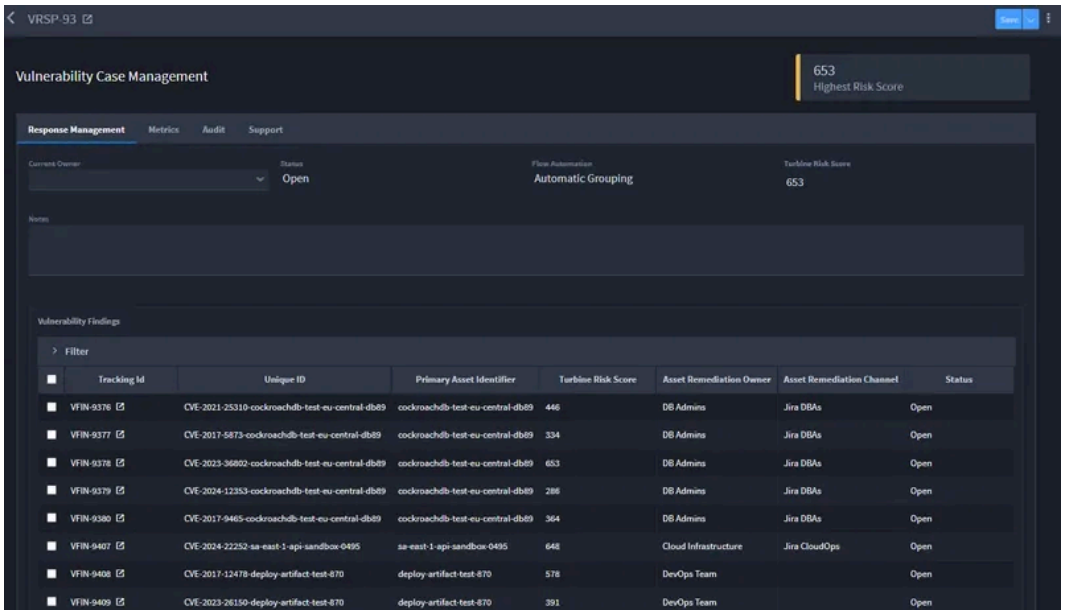
- **number_unseen_findings:** Number of findings not present in the previous export
- **deduplication_count:** Number of duplicates excluded based on export comparison
- **excluded_findings_count:** Entries excluded through custom filtering logic
- **message:** Description of export status (for example, *New Export* or *Existing Export*

1.8.3.3. Vulnerability Case Management

The **Vulnerability Case Management** process centralizes the tracking, management, and resolution efforts for vulnerabilities. It offers a streamlined approach to address grouped findings, create actionable remediation items, and monitor the resolution lifecycle effectively. Below is a detailed breakdown of the process, its components, and actions.

Key Features of Vulnerability Case Management

- **Vulnerability Findings Table:**
  - Displays detailed information about findings, including:
    - **Tracking ID:** Unique identifier for each finding
    - **Unique ID:** Unique ID for the finding, comprised of Vulnerability ID and asset identifier.
    - **Primary Asset Identifier:** Specifies the affected asset
    - **Turbine Risk Score:** Numerical risk score for prioritizing remediation
    - **Asset Remediation Owner:** The owner in question for the indicated finding
    - **Status:** Tracks whether the finding is open, resolved, or in exception.
- **Create Vulnerability Remediation Items:**



- **Grouping and Flow Automation:**
  - Offers insights into how findings were grouped and addressed:

1.8.5. References

- **Vulnerability Finding Data Model**
- **ITSM Response Data Model (Ticket Creation and Updating)**

1.8.5.1. Vulnerability Finding Data Model

Title	Key	Type
Vulnerability Finding	finding	object
Merged Risk Scores	finding.merged-risk-scores	string
Vulnerability Commercial Exploit Found	finding.vulnerability-commercial-exploit-found	string
Vulnerability CVSS Base Score	finding.vulnerability-cvss-base-score	integer
Vulnerability CVSS Temporal/Threat Score	finding.vulnerability-cvss-temporal-threat-score	integer
Vulnerability CVSS Vector String	finding.vulnerability-cvss-vector-string	string
Vulnerability CVSS Version	finding.vulnerability-cvss-version	string
Vulnerability Description	finding.vulnerability-description	string
Vulnerability EPSS Percentile	finding.vulnerability-epss-percentile	integer
Vulnerability EPSS Score	finding.vulnerability-epss-score	integer
Vulnerability Exploits Trending on Github	finding.vulnerability-exploits-trending-on-github	string
Vulnerability Exploits	finding.vulnerability-exploits	string
Vulnerability Finding Asset Criticality	finding.vulnerability-finding-asset-criticality	integer