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

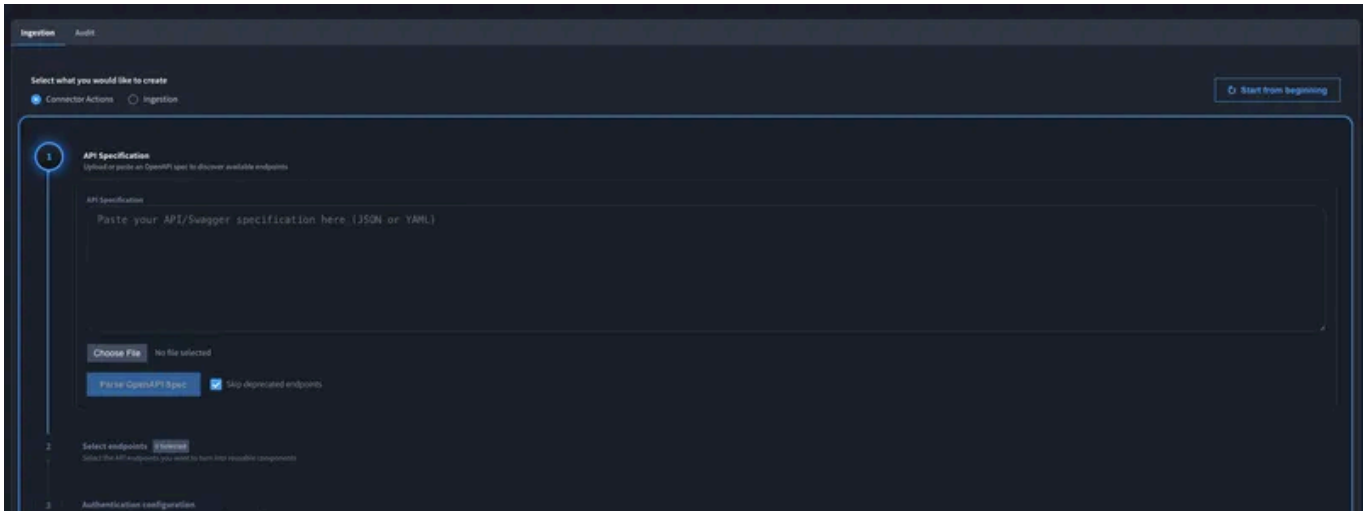
The **AI Ingestion** application helps you build vendor connectors and alert ingestion pipelines quickly — without writing code or learning JSONata. A guided custom widget builds Turbine components from an uploaded OpenAPI specification, one per endpoint. Hero AI then assists in mapping incoming raw 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

1.1.7.7. Understanding Verdict Generation

The **Generate Verdict** step in the Determination phase uses Hero AI to analyze the signal and produce a verdict.

Verdict Inputs

The verdict generation uses:

- Signal tracking ID
- Signal data (observables, severity, source, etc.)
- Threat intelligence enrichment results
- Knowledge Base Articles linked to the signal
- Similar signals and their verdicts
- Investigation comments and summaries

Verdict Outputs

After running the verdict step, you'll see:

Final AI Verdict:

- **Malicious:** Confirmed threat requiring response
- **Suspicious:** Needs further investigation
- **Benign:** False positive, no threat
- **Unknown:** Insufficient data to determine

Verdict Analysis:

- Narrative explanation of the verdict
- Confidence score (0-10 scale)
- Summary of key factors
- Improvement guidance (what data would increase confidence)

Threat Intelligence Analysis:

- TI verdict and confidence

1.2.1. Installing SOC Solutions Bundle

The SOC Solutions Bundle is a solution bundle that is made of four smaller, interconnected solutions: Phishing Triage, Alert Triage, Threat Intelligence (TI), and Case and Incident Management (CIM). For more information, see the corresponding sections.

> This installation and configuration documentation is for the Canvas version of the SOC Solutions Bundle only.

Important Definitions

- Ingestion Component - A component or set of components that:
  - Interact with a vendor endpoint, such as run a SIEM search, look up observable reputation, or initiate a remediation action
  - Normalize inputs and outputs using interfaces to enable swappable component usage
  - Convert various 3rd-party alerts, reputations, emails, and so on to a common schema for use in Turbine solutions such as SOC Solutions
- **Turbine Extendable Data Schema (TEDS)** - Turbine's native common schema for interacting with alerts, emails, reputations, and so on.

Install from Library

Follow these steps:

1. Navigate to the **Swimlane Content Library**
   1. From your desired tenant, click Library
   2. Click Swimlane Content
2. Install SOC Solutions Bundle
   1. Select SOC Solutions Bundle from the list of Solutions
   2. Click **Install** on the solution

1.3.3. Using Business Continuity Management

Workspaces

Utilities – BCM

- Used for importing data records (Resources, BIAs, Solutions, Tasks, Threat Scenarios).

Business Continuity Management

- Daily BCM workspace.
- Applications include: Approvals, BIAs, Resources, Threat Scenarios, Incident Repository, Inventory - Solutions, Solutions, Inventory - Tasks, Tasks, Unavailability Scenarios, and Documents.
- Provides dashboards for both program-level and owner-level views.

Application Records

Application Records are the data structures that power BCM. They establish relationships between business processes, resources, continuity plans, incidents, and approvals.

Resources

Represents assets (applications, buildings, suppliers, equipment, infrastructure, etc.).

Business Impact Assessments (BIAs)

Determines criticality of processes and defines recovery objectives. Includes **Initial Pre-Screening** and the **full BIA workflow** for Critical processes.

Inventory – Solutions

Continuity and contingency plans linked to BIAs and Threat Scenarios.

Inventory – Tasks

Step-level actions tied to continuity plans.

Threat Scenarios

Risks that may disrupt business operations (for example, cyber, human, natural, technical).

Incident Repositor

1.4.7. SCF Evidence Application Overview

The solution builds the **SCF Evidence** application during installation. An SCF Evidence record stores information about audit evidence artifacts, collection methods, and review status. The application automatically populates up to 230 pre-defined evidence records from the SCF data based on what compliance frameworks are chosen during installation. The pre-defined evidence records are provided as a courtesy of Swimlane but certainly do not represent the whole body of evidence in the user's compliance program. The pre-defined evidence records will come with the following fields populated as read-only values:

Application Field Name	Desciption
ERL #	Evidence ID is the primary key of an evidence record.
Area of Focus	Single-select: Groupings of security related areas that the evidence relates to.
Documentation Artifact	The name of the evidence artifact.
SCF Control Mappings	Pre-mapped SCF control ID.
Artifact Description	Description of the evidence artifact.

SCF Evidence records also have editable fields to input information about the evidence such as collection type, evidence owner, and implementation notes.

Evidence Collection Types:

- A user can import files as evidence such as pdf, excel, or word documents.
- Users can provide an external URL link as evidence.
- A user can also link Turbine playbooks as evidence. This would be the case if the audit evidence is contained in a Turbine automation use case. This is a URL field where you can link a Turbine playbook URL. If a user does not have the "Orchestrator" role for the linked playbook, the URL will not work.

> Users can select multiple collection types and store as much evidence as they want

1.6.1. Installing and Configuring Crafted AI Prompts

The Crafted AI Prompts extension integrates and works well with the Turbine SOC Solutions Bundle and the Case and Incident Management (CIM) application. This user guide uses the SOC Solutions Bundle and CIM application in examples to instruct how to utilize the Crafted AI Prompts extension.

> To best understand the documentation and examples, you can install and configure the SOC Solutions Bundle and the CIM application. For assistance in SOC Solutions Bundle Installation and Setup, contact your Swimlane professional services point of contact.

The Crafted AI Prompts extension is a collection of bundled components to create custom prompts to be sent to large language models such as OpenAI or the Swimlane LLM. For additional information, navigate to **Crafted AI Prompts**.

Start by installing the extension

Go to Marketplace

Navigate to the Turbine Marketplace. Follow these steps:

1. Log in to Turbine.
2. In the navigation pane, click **TENANTS**.
3. Select the desired tenant.
4. In the navigation pane, click **LIBRARY**.
5. In the LIBRARY navigation pane, click **Swimlane Content**.

Install

Now, you can install the Crafted AI Prompts extension:

1. From the Swimlane Content Library, under **Solutions**, click **Crafted AI Prompts Extension**.
2. Click **Install** on the right-bottom of the solution.
   The Crafted AL Prompts Extension details open.

1.8.2.3. Creating Ingestion Pages

When vulnerability data is imported into VRM—either via CSV or through a connector—the system automatically splits the data into multiple ingestion pages. These pages are designed to manage processing in batches, ensuring scalability and reliability even for large datasets.

Each ingestion page corresponds to a portion of the original dataset and is stored as a record in **VRM - Ingestion Page**.

Page Record Contents

Each ingestion page includes:

- **Status:** Tracks progress (e.g., Pending, Submitted, Completed)
- **Page Type:** Source of data (CSV or API)
- **Source:** Logical source name, used in mapping logic
- **Timestamp:** When the page was created/updated
- **JSON File:** Encoded subset of findings
- **Finding Count:** Number of findings in this batch
- **Sample Data:** Preview of the findings payload

Common Statuses:

- Pending Submission to Enrichment: Page is queued but not yet picked up
- Submitting to Enrichment: Page is actively being processed
- Successfully Submitted: All findings in the page have been sent for enrichment

Notes:

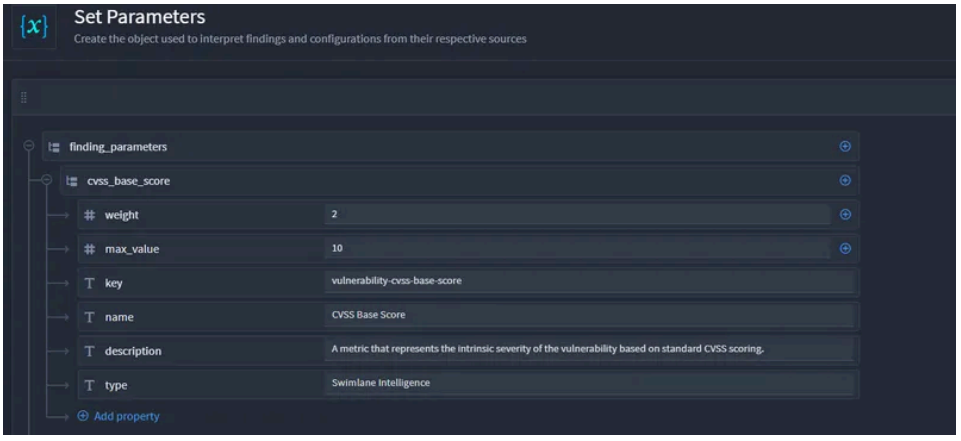
- **Page size** is defined in the import step (default: 1000). This controls how many findings go into each page.
- All ingestion pages are viewable in the **VRM - Ingestion Page** application.
- Errors or issues encountered during enrichment are reflected in page-level status and logs.

1.8.2.4. Pre-processing and Enrichment

1.8.3.2. Configuring and Calculating Risk Score

To configure and calculate the risk score:

1. Open the **VRM – Calculate Turbine Risk Score** component
2. Edit the **Set Parameters** Create Variable action.
3. To change weight:
    1. Modify the weight value for any existing scoring object to an integer between 0 and 10.
4. To remove scoring objects from the calculation
    1. Delete any of the objects within the finding_parameters parent object
5. To add a new scoring object
    1. Create a new scoring object under the finding_parameters base object
    2. Give it a unique name
    3. Create a new integer value called “weight” and give it any value 0 or greater
    4. Create a new integer value called “max_value” and assign the maximum value that the first can possibly have.
        1. For booleans, use 1 as a max_value.
6. Create a string value with the name of "key" and assign to it the field name from the vulnerability_finding object that is being added
7. Create a string value called "name" and assign the display name of the new scoring object.
8. If the new scoring object is a boolean, do the following:



1.8.4. Using VRM for MSSPs

Overview of MSSP Mode

Swimlane's Vulnerability Response Management (VRM) solution supports Managed Security Service Provider (MSSP) scenarios, enabling a central tenant to aggregate, monitor, and report on vulnerabilities from multiple client tenants.

Each client tenant operates independently and retains full control of its ingestion, enrichment, remediation, and reporting flows. The central tenant receives selective records—such as work items based on Vulnerability Findings, Remediation Items, Cases, or Assets, as well as reporting, —via webhook synchronization for unified oversight.

This setup allows MSSPs to:

- Maintain multi-tenant isolation
- Perform centralized reporting
- Track performance across clients via shared dashboards
- Avoid operational conflicts between environments

Architecture of MSSP Mode

The MSSP architecture is built on secure, event-driven data sharing between tenants.

Key Roles

- **Client Tenant**: Executes vulnerability ingestion and enrichment flows. Shares relevant outcomes (for example,work items) with the central tenant. Automates response, syncing with ITSM systems, and case management. Manages assets and findings per client.
- **Central Tenant**: Collects data across clients and aggregates insights into dashboards and reports. Collects work items from client tenants for review and action to unblock automation on the client tenant side.

Flow Overview

1. The client tenant runs ingestion and enrichment workflows, case creation, and