



Connectors

CONTENTS

1. ANY.RUN	2
2. APIVoid APIs	1
3. AWS EKS	1
4. AWS Organizations	1
5. Abnormal Security	1
6. Absolute	1
7. Abuse URLhaus	1
8. AbuseIPDB	1
9. Accelo	1
10. Accenture MxDR	1
11. Adlumin	3
12. After Actions Report	1
13. Airlock Digital	1
14. Akamai	1
15. Alert Logic	1
16. AlienVault Open Threat Exchange	1
17. AlienVault USM Anywhere	1
18. AlienVault USM Central	1

1. ANY.RUN

The ANY.RUN connector facilitates the integration of ANY.RUN's interactive malware analysis service with other platforms, enabling automated threat detection and response workflows.

ANY.RUN is an interactive malware hunting service that enables the in-depth analysis of cyber threats in a safe and controlled environment. The ANY.RUN connector for Swimlane Turbine allows users to automate the retrieval of execution histories, comprehensive task reports, available analysis environments, and user account limits. It also facilitates the initiation of new analyses for dynamic examination of files or URLs. This integration empowers security teams to streamline their malware investigation and analysis processes, enhancing their ability to respond to threats quickly and efficiently within the Swimlane Turbine platform.

Prerequisites

To effectively utilize the ANY.RUN connector within the Swimlane Turbine platform, ensure you have the following prerequisites:

- HTTP Basic Authentication with these parameters:
 - URL: Endpoint for the ANY.RUN API.
 - Username: Your ANY.RUN account username.
 - Password: Your ANY.RUN account password.
- API Key Authentication with these parameters:
 - URL: Endpoint for the ANY.RUN API.
 - API Key: A unique identifier to authenticate requests to the ANY.RUN API.

Capabilities

This connector provides the following capabilities:

- Get History
- Get Report
- Request Available Environment
- Request User Limits
- Run New Analysis

Notes

- [ANY.RUN API Documentation Link](#)

Additional Documentation

- [ANY.RUN Connector Documentation](#)
- [ANY.RUN API Documentation](#)
- [ANY.RUN Authentication Guide](#)

11. Adlumin

The Adlumin connector enables streamlined integration with Adlumin's security platform, facilitating automated data retrieval and analysis for enhanced threat detection and response.

Adlumin delivers a cutting-edge security and compliance automation platform, designed to provide comprehensive visibility into an organization's cybersecurity posture. The Adlumin Turbine Connector enables users to seamlessly integrate Adlumin's rich security data into Swimlane's low-code automation workflows. By leveraging this connector, users can automate the retrieval and analysis of detections, device data, endpoint information, and network insights, enhancing their ability to rapidly respond to threats and maintain compliance. The integration empowers security teams to efficiently manage and analyze large volumes of security data, streamline incident response, and bolster their overall security operations.

Limitations

None to date.

Supported Versions

This connector supports the latest version of the Adlumin API.

Additional Docs

None to date.

Configuration

Prerequisites

To effectively utilize the Adlumin connector within the Swimlane Turbine platform, ensure you have the following prerequisites:

- API Key Authentication:
 - URL: The base endpoint for Adlumin's API services.
 - API Key: A unique identifier to authenticate requests to Adlumin's API.
 - Tenant ID: The specific tenant domain within Adlumin to scope API access.

Authentication Methods

- API Key Authentication for the Adlumin API with the following parameters:
 - URL: The base endpoint for Adlumin API access
 - API Key: Your unique identifier to authenticate with the Adlumin API
 - Tenant ID: The specific identifier for your organization within Adlumin

Capabilities

This Adlumin Connector provides the following capabilities:

21. Amazon AWS CloudWatch

This connector allows Turbine to connect with AWS CloudWatch.

Prerequisites

This connector authenticates with AWS CloudWatch using the following input values:

Requirements

- AWS Access Key ID: A long-term AWS access key ID with access to IAM.
- AWS Secret Key ID: A long-term secret access key associated with the above AccessKey ID.

Capabilities

This Connector provides the following capabilities:

- Get Log Events
- Get Query Results
- List Log Groups
- List Log Streams
- List Queries
- Start Query
- Stop Query

Notes

For more information on AWS Identity and Access Management(IAM):

- [AWS CloudWatch](#)
- [AWS CloudWatch Actions](#)

Configurations

AWS CloudWatch Asset

Authenticates using AWS credentials.

Configuration Parameters

Parameter	Description	Type	Required
access_key	A specific long-term AWS access key ID.	string	Required
secret_key	A specific long-term AWS secret access key.	string	Required

31. Amazon AWS Secrets Manager

The Amazon AWS Secrets Manager connector enables secure storage, retrieval, and management of sensitive information like passwords and API keys.

AWS Secrets Manager is a secure vault service that centralizes the storage and management of sensitive information such as passwords, tokens, and API keys. This connector enables Swimlane Turbine users to automate the lifecycle of secrets, including creation, retrieval, and rotation, directly within their security workflows. By integrating with AWS Secrets Manager, Swimlane Turbine enhances security posture by ensuring that secrets are encrypted, access-controlled, and auditable, while reducing the risk of secret sprawl and hard-coded credentials in code.

Asset Setup

This integration authenticates with AWS Secrets Manager using the following input values:

Prerequisites

To utilize the Amazon AWS Secrets Manager connector within Swimlane Turbine, ensure you have the following:

- AWS Secrets Manager authentication credentials:
 - Access Key: Your AWS IAM user's access key ID.
 - Secret Key: Your AWS IAM user's secret access key.
 - Region Name: The AWS region where your secrets are stored.

Obtaining AWS Credentials

To use this integration, you will need to have an AWS account and obtain the necessary AWS credentials. You can obtain these credentials by following the steps below:

- Log in to your AWS account and navigate to the IAM console.
- In the left navigation pane, click on the "Users" tab and select the user for which you want to create credentials.
- Click on the "Security credentials" tab, and then click on "Create access key".
- Make sure to save the access key ID and secret access key in a secure location, as you will not be able to see the secret access key again after this step.
- If you want to use an AWS IAM Role to access the Secrets Manager, you will need to have the ARN of the role and an optional External ID, if one was specified by the AWS account administrator.

Permissions

- Open the IAM Management Console.
- Navigate to the user or role that requires the permission.
- Click on the **permissions** tab and then click on the **add permissions** button at the right side

41. Armis Centrix

Armis Centrix provides asset visibility and security for connected devices, enhancing threat detection and response.

Armis Centrix is a leading platform for device visibility and security, offering comprehensive insights into connected devices. This connector enables Swimlane Turbine users to automate device information retrieval and alert management, enhancing security operations. By integrating Armis Centrix with Swimlane Turbine, users can efficiently manage device tags, search alerts, and update alert statuses, streamlining security workflows and improving response times.

Prerequisites

Before you can use the Armis Centrix connector for Turbine, you'll need access to the Armis Centrix API. This requires the following:

- Custom authentication using Secret Key with the following parameters:
 - URL: The endpoint URL for accessing the Armis Centrix API.
 - Secret API Key: A unique key provided by Armis Centrix for secure API access.

Capabilities

This Connector provides the following capabilities:

- Get Device Info
- Search Alerts
- Tag Device
- Untag Device
- Update Alert Status

Notes

Search Alerts Action can search below entities with the help of **AQL** search string as below given example.

```
JS JS

{
  "aql": "in:devices name:(system)"
}

{
  "aql": "in:alerts alertId:(57)"
}
```

- alerts

51. Axis Atmos

This Connector integrates Axis Atmos's REST API with Swimlane Turbine.

Prerequisites

The asset requires an **URL** and a **token** to interact with the Axis Atmos REST API.

Capabilities

This Connector provides the following capabilities:

- Create New Application
- Delete Application
- Get Web Categories
- Get Existing Application Details
- List Web Categories
- List Existing Applications
- Update Web Categories
- Update Existing Application

Notes

To access API Documentation for the Connector – [Check Here](#)

Configurations

Axis Atmos HTTP Bearer Authentication

Authenticates using bearer token such as a JWT, etc.

Configuration Parameters

Parameter	Description	Type	Required
url	A URL to the target host.	string	Required
token	The API key, token, etc.	string	Required
verify_ssl	Verify SSL certificate	boolean	Optional
http_proxy	A proxy to route requests through.	string	Optional

Actions

Create New Application

The management API allows administrators to create a new application.

61. Bitsight

The Bitsight connector allows users to access detailed security performance insights and ratings for various organizations directly through the Swimlane platform.

Bitsight provides comprehensive security ratings and detailed insights into organizational security performance. With the Swimlane Turbine Bitsight connector, users can effortlessly retrieve detailed security issue insights for specified organizations, leveraging entity GUIDs to enhance threat analysis and risk management. This integration empowers end-users to prioritize risks effectively, streamline remediation efforts, and bolster their overall security posture without the need for complex coding.

Limitations

None to date.

Supported Versions

This Bitsight connector uses the Version 1 API.

Additional Docs

- [Bitsight Authentication Link](#)
- [Bitsight API Documentation Link](#)

Configuration

Prerequisites

To effectively utilize the Bitsight connector for Swimlane Turbine, ensure you have the following:

- API Key Authentication with the necessary parameters:
 - URL: Endpoint for the Bitsight API.
 - API Token: Your unique identifier to authenticate with the Bitsight platform.

Authentication Methods

API Key Authentication:

- URL: The endpoint URL for the Bitsight API.
- API Token: Your unique identifier to authenticate with the Bitsight API.

Setup Instructions:

- Generating a Token: To generate a token, determine the token type and navigate to the User Preferences page: Settings → Account → User Preferences.
 1. Generating a User API Token
 - In the User API Token section, select Generate New Token. Generate a new user token as needed, especially if you suspect your token has been compromised.

71. Checkpoint XDR

Checkpoint XDR is a security platform that provides extended detection and response capabilities across various environments.

Checkpoint XDR is a comprehensive extended detection and response platform that provides advanced threat prevention and incident response capabilities. The Checkpoint XDR connector for Swimlane Turbine allows users to seamlessly integrate Checkpoint's incident management capabilities into their security automation workflows. By leveraging this integration, Swimlane Turbine users can efficiently retrieve and manage incidents, apply advanced filtering, and normalize data into the Turbine Schema for enhanced analysis and response. This integration empowers security teams to streamline their incident response processes, reduce manual effort, and improve overall security posture.

Prerequisites

Before you can use the Checkpoint XDR connector for Turbine, you'll need access to the Checkpoint XDR API. This requires the following:

- Custom authentication using Check Point XDR external client credentials:
 - URL: The endpoint for accessing Checkpoint XDR services.
 - Client ID: Unique identifier for your application.
 - Access Key: Key used to authenticate API requests.
 - Client Key: Secret key associated with your client ID.

Capabilities

This Connector provides the following capabilities:

- Capabilities
- Go
- Here
- e.g. Manage Firewall Policies instead of listing each individual tasks

Limitations

Include information about known limitations here, including supported or minimum versions, especially known unsupported versions.

Asset Setup

The content here should discuss asset setup in a conversational manner. Be sure to include any known login and test connection errors.

Tasks Setup

81. Cisco Umbrella Providers

Cisco Umbrella Providers connector facilitates management of customer data and operations within the Cisco Umbrella platform.

Cisco Umbrella is a cloud-delivered security service that provides protection against internet threats. The Cisco Umbrella Providers connector enables seamless integration with Swimlane Turbine, allowing users to automate customer management tasks such as creating, updating, and deleting customer records. This integration enhances operational efficiency by streamlining customer management processes, reducing manual effort, and ensuring accurate data handling within the Cisco Umbrella ecosystem.

Prerequisites

Before you can use the Cisco Umbrella Providers connector for Turbine, you'll need access to the Cisco Umbrella API. This requires the following:

- Custom authentication using Umbrella API Key ID and Key Secret (OAuth 2.0 client credentials):
 - URL: The endpoint URL for accessing Cisco Umbrella services.
 - API Key: A unique key provided by Cisco Umbrella for API access.
 - Key Secret: A secret key associated with the API Key for secure authentication.

Authentication Methods

Cisco Umbrella OAuth 2.0 Client Authentication

You need both an API Key and a Key Secret. HTTP Basic against `management.api.umbrella.com` is no longer supported.

- **URL:** Base URL for the Umbrella Admin API (default: `https://api.umbrella.com/admin/v2`).
- **API Key:** Umbrella API Key ID.
- **Key Secret:** Umbrella API Key Secret.
- **Verify SSL Certificates:** (Optional) Enable or disable SSL certificate verification.
- **HTTP(s) Proxy:** (Optional) A proxy URL to route requests through.

Token endpoint used by the connector: `https://api.umbrella.com/auth/v2/token`.

See [Umbrella API Authentication](#).

Capabilities

- Create Customer for Provider
- Get Customer for Provider
- Update Customer for Provider
- Delete Customer for Provider
- List Customers for Provider

91. Cofense Vision

Cofense Vision is an email security solution that helps organizations detect and respond to phishing threats.

Cofense Vision is a powerful platform designed to automate phishing threat detection and response. It enables users to quarantine suspicious emails, conduct detailed searches, and retrieve search results efficiently. By integrating Cofense Vision with Swimlane Turbine, users can enhance their security operations with automated workflows, allowing for rapid identification and mitigation of phishing threats. This integration empowers security teams to streamline their processes, reduce manual effort, and improve response times to potential threats.

Prerequisites

Before you can use the Cofense Vision connector for Turbine, you'll need access to the Cofense Vision API. This requires the following:

- OAuth2 client credentials authentication using the following parameters:
 - URL: The endpoint for accessing the Cofense Vision API.
 - Client Name: The name of the client used for authentication.
 - Client Password: The password associated with the client for secure access.

Capabilities

This connector provides the following capabilities:

- Create a New Quarantine Job
- Create New Search
- Get All Searches
- Get Search Results

Asset Setup

The following permissions are required to run each of the tasks:

- Create a New Quarantine Job: **QUARANTINE ADMIN**, **QUARANTINE_USER**, or **SYSTEM_ADMIN**.
- Create New Search: **SEARCH_ADMIN**, **SEARCH USER**, or **SYSTEM_ADMIN**.
- Get All Searches: **SEARCH_ADMIN**, **SEARCH USER**, or **SYSTEM_ADMIN**.
- Get Search Results: **SEARCH_ADMIN**, **SEARCH USER**, or **SYSTEM_ADMIN**.

Notes

This connector supports Cofense Vision API Version 5.

Additional Documentation

- [Cofense Vision Connector Documentation](#)

101. CrowdStrike Falcon

CrowdStrike Falcon is a cloud-native endpoint protection platform designed to detect, prevent, and respond to cyber threats.

CrowdStrike Falcon is a leading endpoint protection platform that provides comprehensive threat intelligence and real-time response capabilities. This connector enables seamless integration with Swimlane Turbine, allowing users to automate threat detection, response, and management tasks. By leveraging the capabilities of CrowdStrike Falcon, Swimlane Turbine users can enhance their security operations with automated incident response, real-time threat intelligence, and efficient management of security incidents and vulnerabilities.

Prerequisites

Before you can use the CrowdStrike Falcon connector for Turbine, you'll need access to the CrowdStrike Falcon API. This requires the following:

- OAuth 2.0 Client Credentials authentication using the following parameters:
 - URL: The base URL for accessing the CrowdStrike Falcon API.
 - Client ID: A unique identifier for your application to authenticate with the API.
 - Client Secret: A secret key used in conjunction with the Client ID to authenticate your application.

Asset Configuration

Each CrowdStrike cloud has a different base URL. When making requests to the CrowdStrike API, use the base URL that corresponds to the cloud where your integration is hosted.

- US-1: <https://api.crowdstrike.com>
- US-2: <https://api.us-2.crowdstrike.com>
- EU-1: <https://api.eu-1.crowdstrike.com>
- US-GOV-1: <https://api.laggar.gcw.crowdstrike.com>
- US-GOV-2: <https://api.us-gov-2.crowdstrike.mil>

Capabilities

This connector has the following capabilities:

Detections

- Get Detections
- Get Detections Summary
- Update Detections

Host

- Get Host Info

11. Cyera

Cyera is a data security platform that automates discovery, classification, and protection of sensitive data across hybrid and multi-cloud environments.

Cyera is a leading data security platform that provides comprehensive visibility and control over sensitive data across cloud and on-premises environments. This connector enables Swimlane Turbine users to automate the discovery, classification, and management of datastores, identities, incidents, and issues within Cyera. With robust actions for incident response, datastore scanning, ownership management, and compliance reporting, the integration empowers security teams to streamline data protection workflows, accelerate incident remediation, and maintain regulatory compliance. By leveraging Cyera's deep data intelligence within Turbine's low-code automation, organizations can proactively reduce risk, enforce data governance, and respond to threats faster—all without writing code.

Limitations

None to date.

Supported Versions

This Cyera connector uses the Version 1 and 3 API.

Prerequisites

To use the Cyera connector, ensure you have the following prerequisites in place:

- Authentication using Client ID and Secret:
 - URL: The base endpoint for your Cyera API instance.
 - Client ID: The unique identifier for your Cyera application client.
 - Secret: The secret key associated with your Cyera client ID for secure authentication.

Authentication Methods

- URL: The endpoint URL for the Cyera API.
- Client ID: The API Key. Your unique identifier to authenticate with the Cyera API.
- Secret: The API Secret associated with your Client ID for secure access.

Capabilities

This Cyera Connector provides the following capabilities:

- Add Datastore Owner
- Datastore Classifications
- Datastore Objects
- Get All Objects for a Specific Issue
- Get Classifications for a Specific Issue

121. Databricks

Databricks is a cloud-based data platform that provides a collaborative environment for big data analytics and machine learning.

Databricks is a unified data analytics platform, known for its ability to process large volumes of data and perform complex analytics. The Databricks Turbine Connector allows users to execute SQL queries directly on Databricks clusters or SQL warehouses, seamlessly integrating with Swimlane Turbine's security automation workflows. This integration empowers security teams to automate data-driven decision-making processes, enhancing their ability to respond to security incidents with data-backed insights and reducing manual intervention.

Limitations

None to date.

Supported Versions

This Databricks connector uses the latest Version.

Prerequisites

Before you can use the Databricks connector for Turbine, you'll need access to the Databricks API. This requires the following:

- Custom authentication using the following parameters:
 - Server Hostname: The hostname of your Databricks server.
 - Client ID: The client identifier for authentication.
 - Client Secret: The secret key associated with the client ID.
 - HTTP Path: The HTTP path to connect to your Databricks instance.

Authentication Methods

- This authentication with the following parameters:
 - Server Hostname: The address of your Databricks server.
 - Client ID: Your Databricks client identifier.
 - Client Secret: A secret key associated with your client ID for authentication.
 - HTTP Path: The HTTP path to the target server.
- To check Server Hostname and HTTP Path [Click Here.](#)
- To create Client ID and Client Secret [Click Here.](#)

Capabilities

This Databricks Connector provides the following capabilities:

- Run Query

131. Domaintools

DomainTools provides domain and DNS-based threat intelligence to help organizations investigate and monitor domain names.

DomainTools is a leading provider of domain and DNS-based cyber threat intelligence. This connector enables Swimlane Turbine users to automate the enrichment and investigation of domain-related data, enhancing threat detection and response capabilities. By integrating DomainTools, users can efficiently monitor domain activities, assess domain reputations, and retrieve historical domain data, all within the Swimlane platform. This integration empowers security teams to streamline their workflows, reduce manual efforts, and make informed decisions based on comprehensive domain intelligence.

Prerequisites

Before you can use the DomainTools connector for Turbine, you'll need access to the DomainTools API. This requires the following:

- API key authentication using the following parameters:
 - URL: The endpoint URL for accessing DomainTools API services.
 - API Key: A unique key provided by DomainTools to authenticate API requests.

Capabilities

The DomainTools Connector has the following capabilities:

- Add and Remove Domain Watchlist
- Get Brand Monitor
- Get Domain Profile
- Get Hosting History
- Get Reputation
- Get Reverse IP
- Get Reverse WhoIS
- Get WhoIS
- Get WhoIS History

Additional Documentation

- [Domaintools Connector Documentation](#)
- [Domaintools API Documentation](#)

Configurations

DomainTools Intelligence API Key Authentication

Authenticated using an API Key:

141. Elastic Kibana 8 – Security

Elastic Kibana 8 – Security is a powerful tool for visualizing and analyzing security data, providing advanced threat detection and response capabilities.

Elastic Kibana 8 is a powerful data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases. This connector enables seamless integration with Swimlane Turbine, allowing users to automate security operations by creating and managing cases, detection rules, and exceptions directly from the Swimlane platform. The integration enhances the ability to respond to security incidents efficiently by leveraging Kibana's robust capabilities in data analysis and visualization, thus providing a comprehensive security management solution.

Prerequisites

Before you can use the Elastic Kibana 8 – Security connector for Turbine, you'll need access to the Elastic Kibana API. This requires the following:

- an API key authentication using the following parameters:
 - URL: The endpoint URL for accessing the Elastic Kibana API.
 - API Key: A valid API key for authenticating requests.
- HTTP Basic authentication using the following parameters:
 - URL: The endpoint URL for accessing the Elastic Kibana API.
 - Username: The username for basic authentication.
 - Password: The password associated with the username.

Capabilities

This connector provides the following capabilities:

Case Tasks

- Add Case Comment
- Create Case
- Find Cases
- Get Case
- Update Case
- Get All Case Activity

Connector Tasks

- Create Connector
- Get All Connectors
- Get Current Connector
- Push Case to External Service

151. Exabeam Security Management Platform

Exabeam Security Management Platform is a comprehensive security solution that enhances threat detection and response through advanced analytics and automation.

Exabeam Security Management Platform is a comprehensive solution for security information and event management (SIEM) that enhances threat detection, investigation, and response. This connector allows Swimlane Turbine users to automate queries to the Exabeam Data Lake, enabling efficient data retrieval and analysis. By integrating with Exabeam, users can streamline their security operations, quickly access relevant data, and enhance their incident response capabilities through automated workflows.

Prerequisites

Before you can use the Exabeam Security Management Platform connector for Turbine, you'll need access to the Exabeam API. This requires the following:

- an API key authentication using the following parameters:
 - URL: The endpoint URL for accessing the Exabeam API.
 - API Token: A valid API token for authenticating requests to the Exabeam platform.

Capabilities

The Exabeam Security Management Platform integration provides the following capabilities:

- Query Data Lake

Query Exabeam's Data Lake

- The Exabeam Data Lake attempts to normalize the data from various sources but some unique variables may be missing.

These variables can be found in the JSON payload which will have the entirety of the API response.

- There are default queries to make automation more simple. They are as follows:
- IP: `src_ip:"1.2.3.4" OR dest_ip:"1.2.3.4"`
- Domain or URL: `"swimlane.com" AND data_type:"web-activity"`
- other such as hash or username: `"username"` (just a raw search of the IOC input)
- The `start_time` and `end_time` keys adds the time filter to the above queries and default to a 1-month look back.

Ex. The IP query would be: `src_ip:"1.2.3.4" OR dest_ip:"1.2.3.4" AND indexTime=[2020-07-22T13:35:35+00:00 TO 2020-08-26T13:35:35+00:00]`

unless the "time_key" (indexTime) or the time look back is changed.

Additional Documentation

161. Forcepoint Management

Forcepoint Management is a security platform that provides centralized control over web content filtering and network security.

Forcepoint Management is a comprehensive web security platform that enables organizations to manage and enforce security policies across URLs and IP addresses. This connector allows Swimlane Turbine users to seamlessly integrate with Forcepoint Management, providing capabilities to add, commit, and manage categories for enhanced policy enforcement. By leveraging this integration, users can automate the organization and categorization of web resources, ensuring efficient policy application and reporting, while also enabling rollback and transaction management for streamlined operations.

Limitations

None to date.

Supported Versions

This Forcepoint Management connector uses the Version 1 API.

Additional Docs

- [API Documentation](#)
- [Authentication](#)

Configuration

Prerequisites

Before you can use the Forcepoint Management connector for Turbine, you'll need access to the Forcepoint Management API. This requires the following:

- HTTP Basic authentication using the following parameters:
 - URL: The endpoint for accessing Forcepoint Management services.
 - Username: Your Forcepoint Management account username.
 - Password: The password associated with your Forcepoint Management account.

HTTP Basic Authentication with the following parameters:

- URL: The endpoint URL for the Forcepoint Management API.
- Username: Your Forcepoint Management account username.
- Password: Your Forcepoint Management account password.

Capabilities

This Connector provides the following capabilities:

171. Github

GitHub is a platform for version control and collaboration, enabling developers to manage and share code.

GitHub is a leading platform for version control and collaboration, enabling developers to manage and review code. The GitHub connector for Swimlane Turbine allows users to automate various GitHub operations such as managing repositories, issues, and pull requests. By integrating GitHub with Swimlane Turbine, users can streamline their security workflows, enhance collaboration, and automate repetitive tasks, thereby improving efficiency and reducing manual errors.

Prerequisites

Before you can use the GitHub connector for Turbine, you'll need access to the GitHub API. This requires the following:

- HTTP Bearer authentication using the following parameters:
 - URL: The base URL for accessing the GitHub API.
 - Token: A GitHub Personal Access Token (PAT) or JWT-Token for authenticating API requests.

Asset Setup

- To generate a Personal Access Token, please follow the instructions [here](#).
- To generate a JWT-Token, please follow the instructions [here](#).

Capabilities

The GitHub bundle has the following capabilities:

- Block a user
- Create a Repository Dispatch Event
- Create an Issue
- Create or Update File Contents
- Get a Pull Request
- Get a User
- Get an Issue
- Get an Organization by ID
- Get File
- List Organizations
- Revoke PAT (Fine-Grained Token)

Task Setup

Create a Repository Dispatch Event

181. Google Gemini

Google Gemini is an AI platform that provides intelligent, context-aware responses to user queries.

Google Gemini is a powerful AI-driven platform designed for advanced text generation and natural language processing. The Google Gemini Connector allows Swimlane Turbine users to seamlessly integrate AI-generated responses into their security workflows. By leveraging this integration, users can enhance their playbooks with dynamic, AI-driven insights, improving decision-making and response times in security operations. This connector empowers users to automate complex text generation tasks, providing a significant boost to the efficiency and effectiveness of security processes.

Prerequisites

Before you can use the Google Gemini connector for Turbine, you'll need access to the Google Gemini API. This requires the following:

- an API key authentication using the following parameters:
 - API Key: A unique key provided by Google to authenticate requests.
 - Model: The specific AI model to be used for generating responses.

Getting an API Key

1. Go to [Google AI Studio](#)
2. Navigate to the **API Keys** page from the Dashboard
3. Click **Create API Key** and select your project
4. Copy the generated API key for use in the connector

Capabilities

This Connector provides the following capabilities:

- **Text Generation:** Generate human-like text responses to prompts
- **Question Answering:** Ask questions and receive comprehensive answers
- **Content Analysis:** Analyze and summarize text content
- **Creative Writing:** Generate creative content, stories, and explanations
- **Code Generation:** Generate and explain code snippets
- **Multi-model Support:** Access to multiple Gemini model variants with different capabilities

Limitations

- **Rate Limits:** Subject to Google's API rate limits and quotas
- **Model Availability:** Some models may have regional availability restrictions
- **Parameter Support:** Not all models support all generation parameters (e.g., top_k)
- **Token Limits:** Responses are limited by the max_tokens parameter (default: 1024, max: 8192)

191. HTTP

The HTTP connector facilitates interaction with web services and APIs by enabling the construction and dispatch of custom HTTP requests.

The HTTP connector enables seamless integration with web services and APIs, allowing users to automate HTTP requests within their security workflows. By leveraging this connector, Swimlane Turbine users can build and send custom HTTP requests to specified endpoints, facilitating flexible web interactions. This integration empowers security teams to automate web service interactions, enhancing the efficiency and effectiveness of their security operations.

Prerequisites

Before you can use the HTTP connector for Turbine, you'll need to configure authentication mechanisms based on your requirements. This includes:

- Bearer token authentication using the following parameters:
 - URL: The endpoint URL for the HTTP request.
 - Token: The bearer token used for authentication.
 - Basic authentication using the following parameters:
 - URL: The endpoint URL for the HTTP request.
 - Username: The username for basic authentication.
 - Password: The password associated with the username.
 - API key authentication using the following parameters:
 - URL: The endpoint URL for the HTTP request.
 - API Key: The key used to authenticate the request.
 - API Key Name: The name of the API key parameter.
 - API Key Location: The location where the API key should be included (e.g., header, query).
 - OAuth 2.0 client credentials using the following parameters:
 - URL: The endpoint URL for the HTTP request.
 - Client ID: The client identifier issued by the authorization server.
- ... and so on

Capabilities

This connector provides the following capabilities:

- Send an HTTP Request

Limitations

This connector works for any API that conforms to a standard authentication scheme. Any API that has implemented its own custom method is not supported by this connector.

Asset Setup

201. Hero AI

The Hero AI connector enables the execution of advanced language models within Swimlane playbooks, enhancing automation with AI-driven natural language processing.

Hero AI is an advanced AI platform that integrates with Swimlane Turbine to provide intelligent automation capabilities within security workflows. By leveraging the 'call_llm' action, users can execute large language models (LLMs) to generate insights, automate responses, and enhance decision-making processes. The integration allows for dynamic interaction with AI models using custom prompts, enabling tailored outputs that can inform security strategies and operations. This connector empowers end-users to harness the power of AI directly within their security playbooks, streamlining complex tasks and providing a competitive edge in threat detection and response.

Prerequisites

To effectively utilize the Hero AI connector within Swimlane, ensure you have the following prerequisites:

- Personal Access Token authentication with the following parameters:
 - URL: Endpoint for Hero AI API services.
 - PAT: Your unique Personal Access Token for secure access.
 - Account ID: Identifier for your specific Hero AI account.
 - Tenant ID: Identifier for your tenant within Hero AI.

PAT Authentication

Personal access token along with **Account ID** and **Tenant ID** is required to authenticate **Swimlane Hero AI** connector.

Capabilities

This Connector provides the following capabilities:

- Call LLM

Notes

- To Get **PAT(Personal Access Token)** Follow below steps:
 - Login in **Turbine** using username and password.
 - Go to **Profile & user settings**(top right corner).
 - Click on **Personal access token** tab.
 - Generate the token and use to authenticate.
- Swimlane LLM API will be an external API. In order to have better control over the load on this API, this action has been added to used in playbooks.

Additional Notes

211. Ibm Xforce

The IBM Xforce connector integrates with Swimlane to query malware, IPs, and URLs.

Capabilities

This connector provides the following capabilities:

- Get IP Report
- Get IP Reputation
- Get Malware for Family
- Get Malware for File Hash
- Get Malware for IP
- Get Malware for URL
- Get URL Category List
- Get URL History
- Get URL Report
- Get URL Updates of Deltas
- Get Urls by Category
- Wildcard Search Malware Family

Asset Setup

The IBM Xforce asset requires an `url` , `API Key` and `API Password`

Documentation

[API Doc](#)

Additional Documentation

- [Ibm Xforce Connector Documentation](#)
- [Ibm Xforce API Documentation](#)

Configurations

HTTP Basic Authentication

Authenticates using username and password.

Configuration Parameters

Parameter	Description	Type	Required
url	A URL to the target host.	string	Required

221. Ipqualityscore

The IPQualityScore connector offers a variety of different risk analysis APIs designed to Proactively Prevent Fraud™ for your company, website, or app.

Prerequisites

This section shows you how to create your account and obtain the private key needed for the Swimlane connector.

Account Setup

Get started with IPQualityScore by following this link:

- [IPQualityScore Sign Up](#)

How to obtain an API Token

1. Create an account using the link above. If you have an existing account, log in and skip to step 4.
2. Select **Get Free API Key** on the landing page. This will prompt the registration.
3. Follow the registration steps to create your account.
4. Once you arrive at the Dashboard page, select **API Docs** located in the middle of the screen.
5. Select **Proxy and VPN Detection API** and scroll down until you see the private key.
6. Copy and paste the private key into the Swimlane Asset.

Capabilities

This connector integrates with email validation, proxy/VPN, request, and fraudulent posting APIs.

The following are just some of the example use cases:

- Bot Detection
- Low Quality Users
- IP Reputation
- Account Takeover
- Geo Filtering
- High Risk Behavior
- Lead Generation & User Data Verification
- Report fraudulent IPS, Email Addresses and previous lookups
- Spam Traps
- List Cleaning

Asset Setup

This section provides instructions for obtaining information for the Swimlane asset.

231. Knowbe4 Api

The KnowBe4 API connector allows for automated interactions with KnowBe4's security awareness training platform, enabling streamlined management of training campaigns and policy enforcement.

KnowBe4 is a platform specializing in security awareness training and simulated phishing. The KnowBe4 API connector for Swimlane Turbine allows users to automate the retrieval and management of security policies, training campaigns, and enrollment data. By integrating with KnowBe4, Swimlane Turbine users can enhance their security posture through streamlined access to risk scores, policy details, and training effectiveness, directly within their security workflows. This connector empowers organizations to proactively manage employee security awareness and reduce the risk of social engineering attacks.

Limitations

None to date.

Prerequisites

To effectively utilize the KnowBe4 API connector with Swimlane Turbine, ensure you have the following prerequisites:

- HTTP Bearer Authentication with the following parameters:
 - URL: Endpoint for the KnowBe4 API.
 - Token: A valid bearer token to authenticate API requests.

Capabilities

This connector provides the following capabilities:

- Get a Specific Policy
- Get a Specific Training Campaign
- Get a Specific Training Enrollment
- Get Account Risk Score History
- Get all Policies
- Get all Training Campaigns
- Get all Training Enrollments

Notes

[KnowBe4 API Documentation](#)

Configurations

HTTP Bearer Authentication

Authenticates using bearer token such as a JWT, etc.

241. MITRE ATT&CK (PyAttck)

Swimlane Pyattck Connector

The MITRE ATT&CK (PyAttck) connector enables automated interaction with the MITRE ATT&CK framework using the PyAttck library.

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The PyAttck connector allows Swimlane Turbine users to seamlessly integrate this intelligence into their security automation workflows. By leveraging this integration, users can enhance their threat detection and response capabilities, automate the retrieval of threat actor, malware, and technique data, and generate formatted intelligence for use in security operations. This empowers security teams to make informed decisions and respond swiftly to threats, improving overall security posture.

Swimlane Pyattck Connector

pyattck is a light-weight python package to retrieve actors, malware, mitigations, tactics, techniques and tools from MITRE ATT&CK Frameworks. With pyattck you can access data from the Enterprise, Mobile, and PRE-ATT&CK MITRE ATT&CK Frameworks. Additionally, you have access to external data which provides more rich context like the ability to retrieve potential commands, queries, and detections for techniques. Actors and Tools also have additional contextual data available.

This connector pulls information from Swimlane's open-source project, pyattck.

Prerequisites

Before you can use the MITRE ATT&CK (PyAttck) connector for Turbine, ensure the following prerequisites are met:

- Access to the MITRE ATT&CK framework via the PyAttck library.
 - No additional parameters are required for this integration.

Capabilities

Each task in this Connector allows you to retrieve all named objects (e.g. Actors, Malwares, etc.) as well as filter based on property values of related object types. Additionally, you can select which MITRE ATT&CK Framework to pull data from (default is enterprise). This connector provides the following tasks:

- Get Actors
- Get Controls
- Get Malwares
- Get Mitigations
- Get Tactics
- Get Techniques
- Get Tools

251. Micro Focus ArcSight ESM

This Connector integrates Micro Focus ArcSight ESM's REST API with Swimlane Turbine.

Prerequisites

The ArcSight ESM Asset requires an `URL`, `login` and `password` for authentication.
More Information on Authentication can be found [here](#).

Capabilities

The Micro Focus ArcSight ESM Connector has the following capabilities:

- Get Event Data by QueryViewerID
- Get Security Events by IDs

Notes

- More information on ArcSight ESM can be found [here](#)

Configurations

Asset

Micro Focus ArcSight ESM Asset

Configuration Parameters

Parameter	Description	Type	Required
url	A URL to the target host.	string	Required
login	The login or username for authentication	string	Required
password	The password for authentication	string	Required
verify_ssl	Verify SSL certificate	boolean	Optional
http_proxy	A proxy to route requests through.	string	Optional

Actions

Get Event Data by Query Viewer ID

Retrieve the matrix data identified by the specified resource ID.

Endpoint

- **URL:** `/v1/queryviewers/matrixData/{{id}}`
- **Method:** `GET`

261. Microsoft Defender IoT

The Microsoft Defender IoT connector integrates with Swimlane Turbine. Microsoft Defender for IoT provides comprehensive threat detection for IoT/OT environments, with multiple deployment options that include cloud-connected, fully on-premises, or hybrid.

Prerequisites

The Microsoft Defender IoT asset requires an **URL** and an **API Key** to interact with the API.

Capabilities

This connector provides the following capabilities:

Inventory Management

Endpoints to access device information, connection details, and CVEs.

- Get Connections
- Get Connections per Device
- Get CVEs
- Get CVEs per IP Address
- Get Devices

Alert management

Endpoints designed to retrieve alert information and related timeline events.

- Get Alerts
- Get Events

Vulnerability Management

Endpoints to gather information about operational vulnerabilities, device-specific vulnerabilities, mitigation steps, and security vulnerabilities.

- Retrieve Device Vulnerability Information
- Retrieve Mitigation Steps
- Retrieve Operational Vulnerabilities
- Retrieve Security Vulnerabilities

Integration APIs

These endpoints are for continuous data streaming, including retrieving device connections, device details, device CVEs, creating/updating devices, etc.

- Create and Update Devices
- Get Deleted Devices
- Get Details for a Device
- Get Device Connections

271. Microsoft Graph API Threat Intelligence

The Microsoft Graph API Threat Intelligence connector facilitates the automation of threat detection and response by integrating with Microsoft's security intelligence ecosystem.

Microsoft Graph API Threat Intelligence is a comprehensive platform for security analysis and threat detection. It enables users to retrieve detailed insights, analyze threat assessments, and manage Threat Intelligence indicators within Microsoft Graph Security API. By integrating with Swimlane Turbine, security teams can automate the ingestion and analysis of threat data, enhance security posture, and respond to incidents more efficiently, leveraging the vast intelligence capabilities of Microsoft Graph API without the need for manual coding.

Configuration

Prerequisites

To effectively utilize the Microsoft Graph API Threat Intelligence connector, ensure you have the following prerequisites:

- Client Credentials and Tenant ID authentication with these parameters:
 - URL: Endpoint for Microsoft Graph API
 - Client ID: Application ID registered in Azure AD
 - Client Secret: Key generated for the application in Azure AD
 - Tenant ID: Directory ID of the Azure AD tenant
 - Scope: Permissions required for the API access
- OAuth 2.0 Client Credentials with these parameters:
 - URL: Endpoint for Microsoft Graph API
 - Client ID: Application ID registered in Azure AD
 - Client Secret: Key generated for the application in Azure AD
 - Token URL: URL to retrieve the OAuth token
 - Scope: Permissions required for the API access
- Delegated Flow Authentication with these parameters:
 - URL: Endpoint for Microsoft Graph API
 - Tenant ID: Directory ID of the Azure AD tenant

... and so on

Authentication Methods

OAuth 2.0 client credentials authentication with these parameters:

- url: Endpoint for Microsoft Graph API.
- client_id: Application (client) ID registered in Azure AD.

281. Microsoft defender threat intelligence

The Microsoft Defender Threat Intelligence connector enables automated access to threat intelligence data, facilitating proactive cybersecurity measures.

Microsoft Defender Threat Intelligence offers a comprehensive suite of threat detection and analysis tools. This connector enables Swimlane Turbine users to integrate with Microsoft's threat intelligence capabilities, allowing for the retrieval and analysis of SSL certificates, passive DNS records, and WHOIS information. By leveraging this integration, security teams can enhance their threat detection and response workflows, gaining access to Microsoft's rich threat intelligence data directly within Swimlane Turbine playbooks.

Limitations

When using **\$filter** and **\$orderby** in the same query to get messages, make sure to specify properties in the following ways:

- Properties that appear in **\$orderby** must also appear in **\$filter**.
- Properties that appear in **\$orderby** are in the same order as in **\$filter**.
- Properties that are present in **\$orderby** appear in **\$filter** before any properties that aren't.

Failing to do this results in the following error:

- Error code: InefficientFilter
- Error message: The restriction or sort order is too complex for this operation.

Supported Versions

This Microsoft Defender Threat Intelligence connector uses the Version 1.0 API.

Additional Docs

- [Microsoft Defender Threat Intelligence Authentication Link](#)
- [Microsoft Defender Threat Intelligence API Documentation](#)
- [Microsoft Defender Threat Intelligence Permissions Link](#)
- [Azure AD OAuth2 flow](#)

Configuration

Prerequisites

To effectively utilize the Microsoft Defender Threat Intelligence connector within Swimlane Turbine, ensure you have the following prerequisites:

- OAuth 2.0 client credentials for secure authentication, which include:
 - URL: Endpoint URL for API access

291. Netskope Security V1

The Netskope connector uses the Netskope API to manage events, alerts, reports, and policies.

Prerequisites

The Netskope connector requires a tenant instance and an API token.

Capabilities

The Netskope connector provides the following capabilities:

- Acknowledge Anomalies
- Get Reports Data
- Ingest Alerts
- Ingest Events
- Update URL list
- Update File Hash List

Configurations

Netskope V1 Authentication

Netskope V1 Authentication

Configuration Parameters

Parameter	Description	Type	Required
url	A URL to the target host.	string	Required
token	API Token	string	Required

Actions

Get Alerts

Returns alerts generated by Netskope, including policy, DLP, and watch list alerts

Endpoint

- **URL:** `api/v1/alerts`
- **Method:** `POST`

Input

Argument Name	Type	Required	Description
---------------	------	----------	-------------

301. OneTrust

The OneTrust connector enables automated interactions with OneTrust's assessment and management features, facilitating streamlined compliance and risk management processes.

OneTrust is a comprehensive platform for privacy, security, and third-party risk management. This connector enables seamless integration with OneTrust, allowing users to automate the retrieval, modification, and management of assessments directly within Swimlane Turbine. By leveraging this connector, organizations can enhance their compliance workflows, streamline risk assessments, and ensure timely responses to privacy and security issues.

Prerequisites

To effectively utilize the OneTrust connector within Swimlane Turbine, ensure you have the following prerequisites:

- OAuth2 client credentials for secure authentication, which include:
 - URL: Endpoint for OneTrust API access
 - Client ID: Unique identifier for OAuth2 authentication
 - Client Secret: Confidential key for OAuth2 authentication
- Alternatively, an API key authentication method is available, requiring:
 - URL: Endpoint for OneTrust API access
 - API Key: Secret token to authenticate API requests

Capabilities

This connector provides the following capabilities:

- Get Assessment
- Get List of Assessments
- Get List of Assessments by Criteria
- Launch Assessment
- Modify Assessment
- Reassign Assessment
- Set Primary Record

OAuth 2.0 Scopes

Scope to API Assignments

The following table details the APIs an external system will access when the corresponding scope is defined for the respective client credential.

OAuth Scope	Action
ASSESSMENT_READ	Get Assessment

311. PCAP

PCAP is a standard file format for capturing and analyzing network traffic at the packet level, commonly used for network forensics and troubleshooting.

PCAP (Packet Capture) files are widely used in network security to record and analyze network traffic for threat detection, forensic investigations, and troubleshooting. The PCAP connector enables Swimlane Turbine users to automatically extract packet metadata, identify source and destination IP addresses, and parse IPs from text or PCAP files—all within low-code playbooks. By integrating PCAP analysis directly into Turbine, security teams can accelerate incident response, enrich investigations with network telemetry, and automate the extraction of critical network indicators without manual intervention.

Prerequisites

The Swimlane PCAP Connector does not require an asset.

Capabilities

The Swimlane PCAP connector has the following capabilities:

- Analyze PCAP
- Carve IPs from string
- Extract IP's from PCAP

Actions

Analyze PCAP

Extract packet metadata from an uploaded PCAP file to provide detailed network traffic insights.

Input

Argument Name	Type	Required	Description
<code>attachments</code>	array	Required	PCAP file.
<code>attachments.file_name</code>	string	Required	Name of the resource
<code>attachments.file</code>	string	Required	Parameter for Analyze PCAP
<code>limit</code>	number	Optional	Maximum number of packets to return.

Input Example

```
{"limit":10}
```

Output

Parameter	Type	Description
-----------	------	-------------

321. Palo Alto Networks URL Filtering

The Palo Alto Networks URL Filtering connector enables automated querying of URL categories, aiding in the enforcement of web security policies.

Palo Alto Networks URL Filtering is a robust web security solution that classifies URLs to prevent access to malicious websites. This connector enables Swimlane Turbine users to automate the retrieval of URL categories, enhancing security workflows by quickly identifying potential threats. By integrating with Palo Alto Networks URL Filtering, users can leverage real-time data to enforce security policies and reduce manual categorization efforts. This streamlined process aids in the prevention of web-based threats, ensuring a secure and compliant network environment.

Prerequisites

To effectively utilize the Palo Alto Networks URL Filtering connector in Swimlane Turbine, ensure you have the following:

- Custom authentication with the necessary parameters:
 - URL: The endpoint for the Palo Alto Networks URL Filtering API.
 - API Key: A valid API key provided by Palo Alto Networks to authenticate requests.

Asset Setup

You need the following inputs:

- URL
- API Key

Capabilities

The Palo Alto URL Filtering integration provides the following capabilities:

- Get URL Category

Additional Information

The following table outlines the IDs for potential URL categories:

ID	Category	Description
1	Real Estate	Information on property rentals, sales and related tips or information. Includes sites for real estate agents, firms, rental services, listings (and aggregates), and property improvement.
2	Dynamic DNS	Sites that provide and/or utilize dynamic DNS services to associate domain names to dynamic IP addresses. Dynamic DNS is often used by attackers for command-and-control communication and other malicious purposes.
3	Financial	Websites pertaining to personal financial information or advice, such as online banking loans mortgages debt management credit card companies and insurance

331. ProofPoint

The ProofPoint connector enables automated interactions with ProofPoint's security services, facilitating threat detection and response activities.

ProofPoint is a leading cybersecurity and compliance company that protects organizations' people, data, and brand against advanced threats and compliance risks. The ProofPoint connector for Swimlane Turbine enables users to automate the decoding of URLs, retrieval of forensic data, and extraction of SIEM events. By integrating with ProofPoint, Swimlane Turbine users can enhance their security operations with streamlined threat intelligence and incident response capabilities, leveraging ProofPoint's advanced email protection and targeted attack analysis.

Prerequisites

To effectively utilize the ProofPoint connector with Swimlane Turbine, ensure you have the following prerequisites:

- HTTP Basic Authentication with the following parameters:
 - URL: The endpoint URL for the ProofPoint API.
 - Principal: Your ProofPoint account username.
 - Secret: Your ProofPoint account password.

Capabilities

The Proofpoint integration provides the following capabilities:

- Decode URLs
- Decode URLs – Offline (This uses a local script to decode the URLs.)
- Forensics Campaign Lookup
- Forensics Threat Lookup
- SIEM All
- SIEM Messages Blocked
- SIEM Messages Delivered
- SIEM Clicks Blocked
- SIEM Clicks Delivered

Limitations

The URLs passed to the decode tasks are case sensitive.

Proofpoint encodes the URLs with base64, if you are passing extracted IOCs from the Swimlane Utilities plugin with the IOC Parser task, please make sure that you have the input `To Lower` marked as False.

Notes

341. Rapid7 InsightIDR V2

Rapid7 InsightIDR is a SIEM solution that helps organizations detect, investigate, and respond to security threats.

Rapid7 InsightIDR is a comprehensive security information and event management (SIEM) solution that provides advanced threat detection and response capabilities. This connector enables seamless integration with Swimlane Turbine, allowing users to automate incident response and streamline security operations. By leveraging this integration, users can efficiently manage investigations, execute saved queries, and retrieve alerts and evidence, enhancing their security posture and operational efficiency.

Prerequisites

Before you can use the Rapid7 InsightIDR V2 connector for Turbine, you'll need access to the Rapid7 InsightIDR API. This requires the following:

- an API key authentication using the following parameters:
 - URL: The endpoint URL for accessing the Rapid7 InsightIDR API.
 - API Key: A valid API key for authenticating requests to the Rapid7 InsightIDR API.

Capabilities

This connector provides the following capabilities:

- Assign User to Investigation
- Bulk Close Investigations
- Create a Saved Query
- Create investigation
- Delete a Saved Query
- Get Investigation
- Get Product List Alerts by Investigation
- List Alerts Investigation
- List All Saved Queries
- List Investigations
- Retrieve Evidence for Alert
- Run Saved Query
- Search investigations
- Set Disposition Investigation
- Set Priority Investigation

... and so on

Asset Setup

351. Rovo MCP

Rovo MCP is an integration platform that facilitates seamless interaction with Atlassian tools like Jira, Confluence, and Bitbucket.

Rovo MCP is a versatile platform that facilitates seamless integration with Atlassian tools such as Jira, Confluence, and Bitbucket. This connector allows users to perform JSON-RPC calls, retrieve accessible resources, and conduct natural-language searches across Atlassian sites. By integrating Rovo MCP with Swimlane Turbine, users can automate the retrieval and management of Atlassian resources, enhancing their security operations with streamlined workflows and expanded actionability.

Prerequisites

Before you can use the Rovo MCP connector for Turbine, ensure you meet the following prerequisites:

- Custom authentication setup:
 - Ensure proper configuration of your Rovo MCP instance to allow API access.

Capabilities

This Connector provides the following capabilities:

- Capabilities
- Go
- Here
- e.g. Manage Firewall Policies instead of listing each individual tasks

Limitations

Include information about known limitations here, including supported or minimum versions, especially known unsupported versions.

Asset Setup

The content here should discuss asset setup in a conversational manner. Be sure to include any known login and test connection errors.

Tasks Setup

Special task setup as needed depending on plugin, exclude if empty.

Known available allowed input options from enum type selection

Notes

361. Safebreach

This Connector integrates SafeBreach API with Swimlane Turbine. The SafeBreach breach and attack simulation (BAS) platform allows you to continuously validate all layers of your security by simulating real-world attacks to identify gaps in controls, prioritize and reveal actual risk.

Prerequisites

The SafeBreach Connector asset requires an **URL** and an **API Token** to interact with the API.

Capabilities

This connector provides the following capabilities:

- Add Simulation Label
- Delete Simulation Label
- Delete Test Summary
- Get Detailed Test Summaries
- Get Execution History Suggestions
- Get Executions History Results
- Get Service Status
- Get Simulation Stats Regarding Path between Nodes
- Get Simulations Labels
- List Vulnerability Detections for all Simulators
- Post Simulation Stats Regarding Path between Nodes
- Return Insight List
- Return Insight through Post Includes Filters
- Return Remediation Data for a Specified Insight
- Return Remediation Data through Post
- ... and so on

Notes

- [SafeBreach API Documentation Link](#)
- [Query Link](#)

Configurations

SafeBreach API Key Authentication

Authenticates using an API Key

Configuration Parameters

371. Security Scorecard

The Security Scorecard connector allows for automated interactions with Security Scorecard's platform, enabling users to manage portfolios, analyze company scorecards, and generate security reports.

Security Scorecard offers a comprehensive platform for monitoring and managing enterprise security posture and third-party risk. By integrating with Swimlane Turbine, users can automate the process of adding companies to portfolios, generating detailed security reports, and retrieving company scores and issue counts. This connector streamlines the risk assessment process, enabling users to make informed security decisions quickly and efficiently. The integration enhances Swimlane's low-code automation capabilities, allowing users to leverage Security Scorecard's powerful analytics without manual intervention.

Limitations

None to date.

Supported Versions

This Security Scorecard connector uses the Version 1 API.

Additional Docs

- [API Documentation](#)
- [Authentication](#)

Configuration

Prerequisites

To effectively utilize the Security Scorecard connector with Swimlane Turbine, ensure you have the following:

- API Key Authentication:
 - URL: The endpoint URL for Security Scorecard's API.
 - API Key: Your unique identifier to authenticate with Security Scorecard's API.

Authentication Methods

API Key Authentication with the following parameters:

- URL: The base endpoint for Security Scorecard's API.
- API Key: Your unique identifier to authenticate with Security Scorecard's API.

Capabilities

This Connector provides the following capabilities:

381. SkyHigh Security Secure Web Gateway

The SkyHigh Security Secure Web Gateway connector enables automated interactions with the SkyHigh security platform, facilitating advanced threat protection and policy enforcement.

SkyHigh Security Secure Web Gateway is a comprehensive web security solution that provides advanced threat protection, data security, and compliance capabilities. This connector enables Swimlane Turbine users to automate web security management tasks such as adding or removing entries from lists, committing changes, and retrieving list information. By integrating with SkyHigh Security Secure Web Gateway, users can streamline their security operations, enforce policies, and respond to threats more efficiently within the Swimlane ecosystem.

Prerequisites

To effectively utilize the SkyHigh Security Secure Web Gateway connector within Swimlane Turbine, ensure you have the following prerequisites:

- HTTP Basic Authentication with the following parameters:
 - URL: The endpoint URL for the SkyHigh Security Secure Web Gateway API.
 - Username: Your SkyHigh Security Secure Web Gateway username.
 - Password: Your SkyHigh Security Secure Web Gateway password.

Capabilities

The SkyHigh Security Secure Web Gateway Connector has the following capabilities:

- Add Entry List
- Commit
- Delete Entry List
- Get List by ID
- Get Lists
- Logging Off
- Retrieving a List Entry
- Retrieving a List of List Entries

Notes

- You cannot modify system lists. The task will fail with an 'unparsable xml' exception.
- If an account is logged in, you can't use it for anything until it logs out, or the timeout period expires. That means multiple tasks can't be run parallel without multiple users.
- The task will fail if you add entries that already exists on a list.
- The task will fail if you delete an entry that doesn't exists on a list.
- To delete an entry from the list, the position field should be specified as i-1. For example, to

391. Spok

The Spok connector facilitates critical communications by integrating Spok's messaging services with Swimlane's automation capabilities.

Spok delivers critical communications solutions for healthcare, government, and other industries requiring on-call management and secure messaging. The Spok Turbine Connector enables seamless integration with Spok services, allowing users to automate the retrieval of on-call group assignments, current roles, messaging IDs, and the sending of pages directly from the Swimlane platform. By leveraging this connector, Swimlane Turbine users can enhance their incident response capabilities, streamline communication workflows, and ensure timely notifications and escalations within their security operations.

Limitations

None to date.

Supported Versions

This connector supports the latest version of the Spok API.

Additional Docs

Configuration

Prerequisites

To utilize the Spok connector within the Swimlane platform, ensure you have the following prerequisites:

- Custom authentication credentials with the following parameters:
 - Username: The Spok account username.
 - Password: The corresponding password for the Spok account.
 - Primary IP: The primary IP address of the Spok server.
 - Port: The port number used to connect to the Spok server.

Authentication Methods

- Spok credentials authentication with the following parameters:
 - Username: The Spok account username.
 - Password: The corresponding password for the Spok account.
 - Primary IP: The primary IP address of the Spok server.
 - Port: The port number used to connect to the Spok server.

Capabilities

This Connector provides the following capabilities:

401. Swimlane Ssl

Swimlane SSL provides automated retrieval and analysis of SSL certificate information for specified domains, supporting proactive certificate management.

SSL certificates are essential for securing communications and verifying the authenticity of websites and services. The Swimlane SSL connector enables automated retrieval and monitoring of SSL certificate details—including validity periods, issuers, and encryption parameters—for any specified domain. By integrating with Swimlane Turbine, security teams can proactively identify expiring or misconfigured certificates, streamline compliance checks, and reduce the risk of service disruptions or security breaches due to certificate issues. This automation ensures continuous visibility and strengthens the organization's security posture without manual intervention.

Limitations

None to date.

Supported Versions

This connector supports the latest version of the API.

Configuration

Prerequisites

To use the Swimlane SSL connector, ensure you have the following prerequisites:

- SSL Certificate Checker asset configured to check SSL certificate information for your domains:
 - Domain List: A list of domain names for which SSL certificate details will be retrieved and monitored.

Authentication Methods

List of domains for SSL cert check

Setup Instructions:

The asset should contain the list of the domain certificates to be tracked.

Capabilities

Swimlane SSL Connector provides the following capabilities:

- Get SSL Information

Get SSL Information

Retrieve SSL Certificate information for the nominated domains including expiration dates, issuer, and encryption methods.

Configurations

411. Tanium Threat Response

Prerequisites

To authenticate this connector, you need an **API Token**.

Capabilities

This connector provides the following capabilities:

- Create Connection
- Create liveResponse Action
- Download File Evidence
- Get Alert by ID
- Get Collection Configs
- Get Intel Doc by ID
- Get Response Actions
- List Alerts
- List Connections
- List File Evidence
- Update Alert State by ID

Asset Setup

To generate an API Token, please follow the instructions below:

- From the homepage after logging into your Tanium instance, Navigate to **Administration** -> **API Tokens**
- Click on **New API Token** at the right side of the page.
- Set the Expiration, Persona and Trusted IP Addresses details and click on **Create**.

Note: Only IP addresses mentioned in **Trusted IP Addresses**, will be able to make successful connections to the API. If you want to allow any IP, use **0.0.0.0/0** as the Trusted IP address.

Configurations

Tanium Threat Response API Key Authentication

Authenticates using an API Key

Configuration Parameters

Parameter	Description	Type	Required
url	A URL to the target host.	string	Required
session	API key	string	Required

421. TheHive

TheHive connector enables seamless integration with TheHive's incident response platform, facilitating the creation and management of security cases directly from Swimlane.

TheHive is a scalable, open-source and free Security Incident Response Platform designed to make life easier for SOCs, CSIRTs, CERTs, and any information security practitioner dealing with security incidents. The connector allows Swimlane Turbine users to automate incident response by integrating with TheHive's capabilities to create, update, and manage security cases and observables. By leveraging this integration, users can streamline their incident management process, reduce response times, and enhance collaboration among security teams. TheHive connector provides a direct link to manage incident data, add observables to cases, and synchronize case information, ensuring a comprehensive and efficient security operation workflow within Swimlane Turbine.

This connector integrates with Swimlane Turbine to manage cases in TheHive.

Prerequisites

To integrate TheHive with Swimlane Turbine, ensure you have the following:

- API Key Authentication with these parameters:
 - URL: The base URL of your TheHive instance.
 - API Key: Your personal API key for authentication.
- HTTP Basic Authentication with these parameters:
 - URL: The base URL of your TheHive instance.
 - Username: Your TheHive username.
 - Password: Your TheHive password.

Capabilities

This connector provides the following capabilities:

- Add Observables to Case
- Create Case
- Get Case
- Get Case Observable
- List Cases
- Update Case

Asset Setup

- For `apikey` authentication, `url` and `apikey` are required.
- For `http_basic` authentication, `username` and `password` along with `url` are required.

Notes

431. Trend Micro Apex Central

The Trend Micro Apex Central connector enables automated interactions with the Apex Central security management platform, facilitating tasks such as YARA file management and UDSO list manipulation.

Trend Micro Apex Central serves as a central security management hub, facilitating the automation of threat detection and response across an organization's network. This connector enables Swimlane Turbine users to integrate with Apex Central to manage security agents, suspicious objects, and YARA rules. By leveraging this integration, security teams can automate the addition of suspicious files to blocklists, manage security agent configurations, and retrieve detailed agent and threat information, enhancing their security posture and response capabilities.

Limitations

None to date.

Prerequisites

To utilize the Trend Micro Apex Central connector with Swimlane, ensure you have the following:

- API Key Authentication with the necessary parameters:
 - Host Address: The endpoint URL for the Trend Micro Apex Central instance.
 - App ID: The application identifier used for API access.
 - API Key: A unique key provided by Trend Micro for authenticating API requests.

Capabilities

This Connector provides the following capabilities:

- Add file object to UDSO list
- Add UDSO to list
- Isolate Restore Relocate or Uninstall Sec Agent
- List Security Agents
- List UDSO entries
- List uploaded YARA files

Add file object to UDSO list

Adds the uploaded file information to the User-Defined Suspicious Objects list.

Trend Micro Apex Central API Documentation for this action can be found [here]
(https://automation.trendmicro.com/apex-central/api/#tag/UDSO/operation/SuspiciousObjectResource_GetProductServers)

Add UDSO to list

Adds the specified object information to the User-Defined Suspicious Objects list.

441. TypeSafe AI

Typesafe AI provides a platform for structured, explainable AI-powered decision-making using typed questions and contextual state.

Typesafe AI is an advanced AI decision engine designed to evaluate, score, and classify unstructured data using customizable models. This connector enables Swimlane Turbine users to automate complex decision-making processes—such as single-choice selection, yes/no probability assessments, and multi-level scoring—directly within their security workflows. By integrating Typesafe AI, security teams can leverage AI-driven evaluations to triage incidents, prioritize alerts, and enrich case data without manual intervention. The connector also allows users to retrieve available AI models and flexibly tailor automation to their unique operational needs, enhancing both accuracy and efficiency in security operations.

Limitations

- Text only. No image, audio, or video. Serialize a JSON object or array to a string before binding it as `state`.
- Rate limits (`429`) and overload (`529`) are returned to the action. The definition runner does not retry. A `529` is transient, so add an on-failure retry path when the flow cannot miss a call.
- The `ask_*` actions always publish the answer under the question id `result`. Use Evaluate when you need more than one question id.
- `model` is required. A blank Model field is omitted from the body and the API returns `422`. The actions default it to `jev-latest`.
- Choice `criteria` is one object with 2 to 255 options. Score `criteria` is an array of 2 to 10 strings. Bind Noul and Choice criteria as object expressions.

Supported Versions

- This TypeSafe AI connector uses the v1 API (`/v1/systemone` and `/v1/models`).

Additional Documents

- Documentation [TypeSafe API](#)
- Models and aliases [TypeSafe models](#)

Configuration

Prerequisites

To use the Typesafe AI connector, ensure you have the following prerequisites:

- HTTP Bearer authentication to `api.typesafe.ai` using these parameters:
 - URL: The endpoint for the Typesafe AI API (e.g., <https://api.typesafe.ai>)
 - API Key: A valid API key generated from your Typesafe AI dashboard, used for authenticating requests

451. Vmware Carbon Black Cloud

The VMWare Carbon Black Cloud connector enables seamless integration with Swimlane Turbine, providing automated actions such as device searches, alert management, and sensor device updates within the security infrastructure.

VMWare Carbon Black Cloud is a comprehensive endpoint security platform that provides organizations with advanced threat detection and response capabilities. This connector enables Swimlane Turbine users to automate critical security operations such as device quarantine, alert management, and vulnerability searches. By integrating with VMWare Carbon Black Cloud, users can streamline their security workflows, rapidly respond to threats, and enhance their overall security posture without the need for manual intervention.

Prerequisites

To effectively utilize the VMWare Carbon Black Cloud connector for Turbine, ensure you have the following prerequisites:

- HTTP Basic Authentication with the following parameters:
 - URL: Endpoint URL for the VMWare Carbon Black Cloud API.
 - API ID: Unique identifier for API access.
 - API Secret: Secret key associated with the API ID for authentication.

Capabilities

The Swimlane VMWare Carbon Black Cloud connector has the following capabilities:

- Bypass Device
- Delete Sensor Device
- Dismiss Alerts
- Get Alert by ID
- Get Alerts
- Get Device by ID
- Quarantine or Unquarantine Device
- Search Devices
- Search Specific Device Vulnerabilities
- Set Background Scan for device
- Uninstall Sensor Device
- Update Alert
- Update Device Policy

Using the Schema

Following are the definitions for each field, default values, whether it is required, searchable and/or tokenized. You can also see accepted values and routes supported per each field.

461. Workday V2

Workday API Connector

This Connector allows you to interact with the Workday API. This connector is based on the Workday Rest API and uses version v2.

Prerequisites

The Workday asset requires an `Host` , `Private Key` , `Client ID` , and an `org` to interact with the API.

Capabilities

This connector provides the following capabilities:

- Get Job by ID
- Get Jobs
- Get People by Universal ID
- Get People by ID
- Get Request by ID
- Get Requests

Notes

For more information on Workday API : [Click here!](#)

Configurations

Oauth 2.0 Client Credentials

Authenticates using oauth 2.0 client credentials

Configuration Parameters

Parameter	Description	Type	Required
host	Server Host Address	string	Required
private_key	Also created when you create a new Application in Cred Admin. You must save this key immediately upon creation of an Application. Workday does not hold this key for you.	string	Required
client_id	This is created when you create a new Application in Cred Admin	string	Required

471. Zoho Crm

This Connector integrates Zoho CRM's REST API with Swimlane Turbine.

Asset Setup

The Connector can be authenticated in one of the following two ways:

- Bearer token authentication, which requires an `URL` and an `API token`.
- OAuth 2.0 client credentials flow, which requires the following inputs :
 1. URL
 2. API Token URL
 3. Client ID
 4. Client Secret
 5. Redirect URI
 6. Code (Authorization Code)

Capabilities

This Connector provides the following capabilities:

- Get Records

Notes

For more information on Zoho CRM is found at:

[Zoho CRM Main Site](#)

API Documentation Link

- For generating the Authorization Code, please refer [Authorization Code Generation](#)
- [Zoho CRM API Documentation Link](#)

Configurations

HTTP Bearer Authentication

Authenticates using bearer token such as a JWT, etc.

Configuration Parameters

Parameter	Description	Type	Required
url	A URL to the target host.	string	Required
token	The API key, token, etc.	string	Required
verify_ssl	Verify SSL certificate	boolean	Optional