



# 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 Managed Service Providers

Cisco Umbrella Managed Service Providers connector allows MSPs to manage customer environments and security policies efficiently.

Cisco Umbrella is a cloud-delivered security service that provides comprehensive threat protection and internet security. This connector enables seamless integration with Cisco Umbrella Managed Service Providers, allowing Swimlane Turbine users to automate customer management tasks such as creating, updating, and deleting customer records. By leveraging this integration, users can streamline operations, enhance threat response capabilities, and improve overall security posture through automated workflows.

### Prerequisites

---

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

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

### Capabilities

---

The Cisco Umbrella Management connector has the following capabilities:

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

#### Create Customer for Provider

Create a customer for a provider.

Cisco Umbrella's documentation for this action can be found [here](#).

#### Get Customer for Provider

# 91. Cofense Triage

Cofense Triage is an email security platform that helps organizations detect and respond to phishing threats.

Cofense Triage is a leading phishing threat analysis and response platform that helps organizations manage and respond to phishing threats effectively. By integrating with Swimlane Turbine, users can automate the categorization of phishing reports, create and manage threat indicators, and streamline incident response processes. This integration enhances security operations by providing real-time insights and automating repetitive tasks, allowing security teams to focus on more strategic initiatives.

## Prerequisites

---

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

- OAuth 2.0 Client Credentials authentication using the following parameters:
  - URL: The endpoint URL for accessing the Cofense Triage API.
  - Client ID: The 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.

## Capabilities

---

This connector provides the following capabilities:

- Categorize a Report
- Create a Threat Indicator
- Create Category
- Create Response
- Delete To-Many Relationship
- Delete To-One Relationship
- Get a Category
- Get a Cluster
- Get a Header
- Get a Hostname
- Get a Report
- Get a Reporter
- Get a Response
- Get a Rule
- Get a Threat Indicator

... and so on

# 101. CrowdStrike Falcon V2

CrowdStrike Falcon is a cloud-native endpoint security platform that provides advanced threat prevention, detection, and response capabilities through real-time telemetry and integrated threat intelligence.

CrowdStrike Falcon is a leading cloud-native endpoint protection platform that delivers advanced threat detection, response, and intelligence across endpoints, workloads, and identities. The CrowdStrike Falcon V2 connector for Swimlane Turbine enables seamless integration with Falcon's robust APIs, allowing users to automate incident response, threat intelligence enrichment, case management, and real-time endpoint actions—all without writing code. By leveraging this integration, security teams can orchestrate complex workflows, accelerate investigations, and respond to threats faster, while maintaining full visibility and control across their security operations.

## Limitations

- None to date.

## Supported Versions

- This CrowdStrike Falcon V2 connector is implemented based on the CrowdStrike Falcon SDK (pip package crowdstrike-falconpy 1.4.3).

## Additional Documents

- [CrowdStrike Falcon Documentation](#)
- [CrowdStrike Falcon V2 Connector Documentation](#)

## Configuration

---

### Prerequisites

To use the CrowdStrike Falcon V2 connector, ensure you have the following prerequisites in place:

- OAuth 2.0 Client Credentials authentication configured, which requires:
  - URL: The base URL for your CrowdStrike Falcon API instance.
  - Client ID: The unique identifier for your CrowdStrike Falcon API client application.
  - Client Secret: The secret key associated with your API client, used for secure authentication.

### Authentication Methods

---

- URL: The base URL for accessing the CrowdStrike Falcon API.
- Client ID: The client identifier for authenticating API requests.
- Client Secret: The secret key associated with the client ID for secure authentication.

### Capabilities

---

# 11. Cyborg Security

Cyborg Security is a cybersecurity platform that enhances threat detection and response through advanced threat hunting and intelligence capabilities.

Cyborg Security offers advanced threat hunting capabilities, enabling organizations to proactively identify and mitigate potential threats. By integrating with Swimlane Turbine, users can automate the creation and management of hunt packages and templates, streamline threat intelligence retrieval, and enhance security analysis with real-time data. This integration empowers security teams to efficiently manage threat data, automate responses, and improve overall security posture without the need for extensive coding.

This Connector integrates Cyborg Security's Rest API with Swimlane Turbine.

## Asset Setup or Prerequisites

---

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

- an API key authentication using the following parameters:
  - URL: The endpoint URL for accessing Cyborg Security's API.
  - API Key: A unique key provided by Cyborg Security for API access.
- HTTP Basic authentication using the following parameters:
  - URL: The endpoint URL for accessing Cyborg Security's API.
  - Username: Your Cyborg Security account username.
  - Password: Your Cyborg Security account password.

## Capabilities

---

This Connector provides the following capabilities:

- Add Hunt Package by Template ID
- Create Hunt Template
- Get ES Query Search
- Get Search Recent Updates
- Get Threat Actors
- Get Threat Reports

## Notes

---

- For more information on Cyborg Security is found at:  
[Cyborg Security API Documentation](#)

## Additional Documentation

---

- [Cyborg Security Connector Documentation](#)

# 121. Data Converter

Data Converter provides fast and reliable transformation between EML, JSON, and XML formats for seamless data integration.

The Data Converter connector enables seamless data format transformation within Swimlane Turbine, supporting JSON, XML, and EML email files. This connector provides low-code actions to convert between JSON and XML, as well as extract structured data from EML files into JSON. By automating data conversion processes, users can easily integrate disparate systems, normalize data for downstream analysis, and streamline playbook development without manual intervention. Integration with Data Converter enhances interoperability and accelerates automation workflows across diverse security and IT environments.

## Capabilities

- Convert from JSON to XML
- Convert from XML to JSON
- Convert from EML to JSON

## Actions

### Convert JSON to XML

Convert JSON input into XML format for seamless data interchange and integration with other systems.

#### Input

| Argument Name     | Type   | Required | Description                       |
|-------------------|--------|----------|-----------------------------------|
| <code>json</code> | string | Required | Parameter for Convert JSON to XML |

#### Input Example

```
{"json":{"name":"John","age":30,"city":"New York"}}
```

#### Output

| Parameter                | Type   | Description                      |
|--------------------------|--------|----------------------------------|
| <code>xml</code>         | string | Output field: xml                |
| <code>headers</code>     | object | HTTP headers for the request     |
| <code>reason</code>      | string | Response reason phrase           |
| <code>status_code</code> | number | HTTP status code of the response |

#### Output Example

# 131. Domain Squatting

Domain Squatting helps organizations monitor and manage potential domain squatting threats by identifying and responding to suspicious domain registrations.

Domain Squatting is a critical security service that identifies and mitigates the risks associated with domain squatting. This connector enables Swimlane Turbine users to automate the detection, analysis, and response to potential squatting domains. By integrating with Domain Squatting, users can efficiently monitor domain activities, compare current and historical data, and take swift action to deactivate or refresh domain records. This integration enhances security operations by providing real-time insights and automated responses to potential threats, reducing the risk of brand impersonation and phishing attacks.

## Prerequisites

---

Before you can use the Domain Squatting connector for Turbine, you'll need access to the necessary authentication mechanisms. This requires the following:

- HTTP Basic Authentication using the following parameters:
  - Swimlane URL: The URL endpoint for accessing Swimlane services.
  - Swimlane Username: Your username for authenticating with Swimlane.
  - Swimlane Password: Your password for authenticating with Swimlane.
- API Key Authentication using the following parameters:
  - Swimlane URL: The URL endpoint for accessing Swimlane services.
  - Swimlane API/Admin PAT: Personal Access Token for API authentication.

## Capabilities

---

This connector provides the following capabilities:

- Check associated threat intelligence records reputation results
- Compare current and previous DOM hashes
- Create & erase snapshot records
- Deactivate all potential squatting domain records
- Find potential squatting domains
- Refresh potential squatting domains
- Retrieve associated monitored domain and threat intelligence records

## Initial Setup

---

This connector is intended to work with the Swimlane Domain Squatting use case only.

You will need:

- A Swimlane Administrator/API User Personal Access Token (PAT)

# 141. Elastic Kibana 7 – Security

## Elastic Kibana V7

This connector is for Elastic Security, both on-premises and Elastic Cloud versions starting with 7.9.0. The primary focus is on the Elastic Security feature of Kibana, but this uses additional APIs for Kibana.

## Prerequisites

This connector has only been tested using Elasticsearch & Kibana on-premises & Elastic Cloud 7.16.

Depending on how your organization has setup Elasticsearch/Kibana/etc., you need to make sure that the following requirements have been met:

1. Create or know which Kibana space they will primarily use.
2. Create a signal index. This index needs to be in the following format `.siem-signals-<Kibana Space Name>`. Using the `Default` Kibana space this would be `.siem-signals-default`.
3. Create detection rule(s) or load Elastic's Pre-Packaged Detection Rules

## Asset Setup

### Connecting to Elastic Cloud

In order to use this connector with Elastic Cloud you must provide the following inputs in the configured asset:

- host
- port
- api\_key

If you generated a ApiKey from within the Elastic Cloud portal you **may** have need run the following commands to generate the correct ApiKey:

```
JS JS
echo "<your-base64-encoded-api-key>" | base64 -d
```

Which will result in a value similar to the following:

```
JS JS
<api-id>:<api-secret>
```

# 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. Illumio Core Protection

Illumio Core Protection provides segmentation to secure on-premises and cloud data center workloads. Illumio Core secure reduces the impact of breaches. This connector integrates Illumio Core with Turbine.

### Prerequisites

---

This connector can be authenticated in one of two ways:

- Using `Email` and `Password` for PCE account.
- Using `API Authentication Username` and `API Key Secret`.

### Capabilities

---

This connector provides the following capabilities:

- Get a Workload by ID
- Get Firewall Policies
- Get Ransomware details for a Workload
- Get Security Policy Versions
- Get VEN Instance Details
- Get Workloads Settings
- Get Workloads

### Asset Setup

---

To create API Keys in the PCE web console, follow the following instructions:

- In the drop-down **User** menu, select **My API Keys**. A list of configured API keys is displayed. If no API keys are configured, the message "No API Keys" is displayed.
- To add a new API key, click **Add**.
- In the **Create API Key** pop-up window, enter a name for the API key in the Name field. Optionally, enter a description in the Description field.
- Click **Save** to save your API key or click **Cancel** to close the pop-up window without saving your changes.
- When the **API Key Created** window appears, click the > button next to "Show credentials" to display the credentials for your API key. The following information is displayed:
  - **Key ID**: The unique ID of the API key.
  - **Authentication Username**: The username that authenticates the API calls.
  - **Secret**: The password for the API key
- Click **Download Credentials** to download the credentials as a text file. Make sure that you have saved the credential information before clicking **Done**. After you click **Done**, the API Keys page displays a summary of your new API key, including the following information:

## 221. Ivanti Neurons For Itsm

This Connector integrates Ivanti Neurons for ITSM's REST API with Swimlane Turbine.

### Prerequisites

This Connector requires the following input parameters to authenticate:

1. URL
2. API Key

### Capabilities

This Connector provides the following capabilities:

- Create a Business Object
- Get a Business Object by Rec ID or Unique Key
- Get all Business Objects
- Update a Business Object

### Notes

- Ensure the business object name is suffixed with an "s".
- For information see the [Ivanti Documentation](#).

## Configurations

### Ivanti Neurons for ITSM API Key Authentication

Authenticates using an API Key

#### Configuration Parameters

| Parameter     | Description                        | Type    | Required |
|---------------|------------------------------------|---------|----------|
| url           | A URL to the target host.          | string  | Required |
| Authorization | API key.                           | string  | Required |
| verify_ssl    | Verify SSL certificate             | boolean | Optional |
| http_proxy    | A proxy to route requests through. | string  | Optional |

## Actions

### Create a Business Object

You can create business objects available out-of-the-box, such as a Change, Problem, Incident, or any custom defined business object of your choice.

## 231. Knowbe4 Phisher

The KnowBe4 Phisher connector allows for seamless integration with the Phisher platform, enabling automated phishing threat management and analysis.

KnowBe4 Phisher is a comprehensive phishing response platform that enables security teams to prioritize, analyze, and respond to threats. This connector allows Swimlane Turbine users to automate the management of phishing incidents by integrating with Phisher's capabilities. Users can add comments, tags, download email files, and update message statuses directly within Swimlane Turbine, streamlining the incident response process. The integration enhances operational efficiency, reduces response times, and improves threat categorization within the security operations workflow.

### Prerequisites

---

To utilize the KnowBe4 Phisher connector within Swimlane Turbine, ensure you have the following prerequisites:

- HTTP Bearer Authentication with the following parameters:
  - URL: The endpoint URL for the Phisher API.
  - Product API Token: Your unique token to authenticate with the Phisher API.

### Capabilities

---

This connector provides the following capabilities:

- Add Comment to Multiple Messages
- Add Comment
- Add Tags
- Get All Messages
- Get Message by ID
- Download EML using RawUrl
- Update Message
- Update Multiple Messages

### Notes

---

[Phisher API Documentation](#)

## Configurations

### HTTP Bearer Authentication

---

Authenticates using bearer token such as a JWT, etc.

### Configuration Parameters

---

# 241. Malware Detection

The Swimlane Malware Detection Connector provides basic tools to aid in malware detection.

## Capabilities

This Connector provides the following capabilities:

- Swimlane Malware Detection YARA Check

## Tasks Setup

To run the YARA Scan task, you must write a yara rule which can either be sent to the integration as a file or a string.

Example:

Markdown

```
rule silent_banker : banker
{
  meta:
    description = "This is just an example"
    threat_level = 3
    in_the_wild = true
  strings:
    $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
    $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
    $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
  condition:
    $a or $b or $c
}
```

## Actions

### Swimlane Malware Detection YARA Check

Swimlane connector with general malware detection tools. Scan strings or files using a YARA Rule.

#### Input

| Argument Name   | Type   | Required | Description                                       |
|-----------------|--------|----------|---------------------------------------------------|
| yara_rule       | string | Required | Either a file or a string containing a YARA Rule. |
| suspicious_data | string | Required | File or string of suspicious data.                |

#### Input Example

```
{"yara_rule": "rule foo: bar {strings: $a = \"lmn\" condition:
```

# 251. Microsoft Azure DevOps

Microsoft Azure DevOps is a cloud-based service providing development collaboration tools, including source control, build pipelines, and release management.

Microsoft Azure DevOps is a comprehensive suite of development tools for planning, building, and deploying applications. This connector enables seamless integration with Swimlane Turbine, allowing users to automate work item management, streamline project tracking, and enhance collaboration. By leveraging Azure DevOps within Swimlane Turbine, users can efficiently manage work items, automate project workflows, and improve team productivity, all without writing a single line of code.

## Prerequisites

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

- HTTP Basic authentication using the following parameters:
  - Username: Your Azure DevOps username.
  - Personal Access Token (PAT): A token generated in Azure DevOps for authentication.
  - URL: The base URL for your Azure DevOps organization.

## Capabilities

This connector provides the following capabilities:

- Delete User
- Get Organizations List
- Get User Entitlements
- Get User
- Get Users List
- List PATs
- Revoke PATs

## Notes

[Azure DevOps API Documentation](#)

## Configurations

### HTTP Basic Authentication

Authenticates using username and PAT.

### Configuration Parameters

| Parameter | Description | Type | Required |
|-----------|-------------|------|----------|
|-----------|-------------|------|----------|

## 261. Microsoft Exchange

The Microsoft Exchange connector enables streamlined email management and automation directly within the Swimlane Turbine platform, facilitating enhanced security and operational efficiency.

Microsoft Exchange is a widely-used email and calendaring service that enables efficient communication and collaboration within organizations. The Microsoft Exchange Connector for Swimlane Turbine provides a suite of actions to manage email operations, automate incident response, and streamline workflow processes directly within the Swimlane platform. By integrating with Microsoft Exchange, users can perform actions such as deleting emails, exporting email content, retrieving email metadata, and sending emails programmatically, enhancing the capabilities of security automation and improving response times to potential threats.

### Prerequisites

---

To utilize the Microsoft Exchange connector for Swimlane Turbine, ensure you have the following prerequisites:

- OAuth 2.0 client credentials authentication with these parameters:
  - URL: Endpoint for the Microsoft Exchange server
  - Client ID: Unique identifier for the application registration
  - Client Secret: Secret key generated during application registration
  - Tenant ID: Directory ID of the Azure AD tenant
  - SMTP Mailbox Address: Email address associated with the mailbox
- HTTP Basic (NTLM) Authentication with these parameters:
  - Server URL: Endpoint for the Microsoft Exchange server
  - Username Identifier: User account name for server access
  - Password: Corresponding password for the user account
  - SMTP Mailbox Address: Email address associated with the mailbox

### NTLM Authentication

---

NTLM authentication is only available for Exchange on-premises servers.

### Graph Confidential Client

This authentication method allows you to authenticate using an Azure application.

Recommended Application Permissions:

- **EWS\_AccessAsUser.All** (Delegated)
- **full\_access\_as\_app** (Application, Grand admin consent for organization)

In order to set up the asset, you need the following:

- Azure Application Client ID
- Azure Application Client Secret

## 271. Microsoft Graph API

Microsoft Graph API provides a unified programmatic interface to access data and intelligence across Microsoft 365 services, enabling automation, management, and security operations at scale.

Microsoft Graph API is a unified gateway to Microsoft 365 services, including security, identity, email, collaboration, and directory management. This connector enables Swimlane Turbine users to automate a wide range of Microsoft 365 tasks—such as managing users, groups, emails, incidents, alerts, authentication methods, and Teams communications—without writing code. By integrating Microsoft Graph API with Turbine, security and IT teams can orchestrate identity lifecycle management, automate incident response, streamline email and collaboration workflows, and enhance threat detection and remediation. This integration empowers organizations to break down silos between security, IT, and collaboration teams, accelerating response times and improving operational efficiency across the Microsoft ecosystem.

### Configuration

---

#### Prerequisites

Before using the Microsoft Graph API connector, ensure you have the following prerequisites in place:

- OAuth 2.0 Client Credentials authentication:
    - URL: The base endpoint for your Microsoft Graph API instance.
    - Client ID: The application/client identifier registered in Azure AD.
    - Client Secret: The secret key associated with your Azure AD application.
    - Token URL: The OAuth 2.0 token endpoint for acquiring access tokens.
    - Scope: The permissions required for the intended Graph API operations.
  - OAuth 2.0 Refresh Token authentication:
    - URL: The base endpoint for your Microsoft Graph API instance.
    - Client ID: The application/client identifier registered in Azure AD.
    - Client Secret: The secret key associated with your Azure AD application.
  - Delegated Flow Authentication (on behalf of a user):
    - URL: The base endpoint for your Microsoft Graph API instance.
    - Tenant ID: The unique identifier of your Azure AD tenant.
    - Username: The username of the account to authenticate as.
    - Password: The password for the specified user account.
- ... and so on

### Authentication Methods

---

**OAuth 2.0 client credentials authentication with these parameters:**

- url: Endpoint for Microsoft Graph API.

## 281. Mimecast Security

Mimecast Security is an email security platform that protects against threats like phishing and malware while offering archiving solutions.

Mimecast Security is a comprehensive email security platform that provides advanced threat protection, data leak prevention, and secure email archiving. The integration with Swimlane Turbine enables seamless automation of email threat detection and response, allowing security teams to efficiently manage incidents, retrieve detailed message information, and enforce security policies. This integration enhances the ability to automate routine security tasks, streamline workflows, and improve overall security posture by leveraging Mimecast's robust capabilities within the Swimlane Turbine environment.

### Prerequisites

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

- HMAC authentication using the following parameters:
  - URL: The endpoint URL for accessing Mimecast's API.
  - Access Key: A unique key provided by Mimecast for API access.
  - App ID: The application identifier for your Mimecast integration.
  - App Key: A key associated with your application ID for secure access.
  - Secret Key: A secret key used for generating HMAC signatures.
- OAuth2 authorization using the following parameters:
  - URL: The endpoint URL for accessing Mimecast's OAuth2 service.
  - Client ID: The client identifier for your OAuth2 application.
  - Client Secret: A secret associated with your client ID for secure access.

### Action API Permissions

Below is the table of required API scopes for the set of credentials used in the asset and broken down by action.

| Action                       | Required API Permissions      |
|------------------------------|-------------------------------|
| Add or Remove Group Members  | <u><b>API Permissions</b></u> |
| Archive Message Search       | <u><b>API Permissions</b></u> |
| Create Managed URL           | <u><b>API Permissions</b></u> |
| Create Remediation Incident  | <u><b>API Permissions</b></u> |
| Decode URL                   | <u><b>API Permissions</b></u> |
| Get Archived File Attachment | <u><b>API Permissions</b></u> |
| Get Archived Message Details | <u><b>API Permissions</b></u> |
| Get Archived Message Part    | <u><b>API Permissions</b></u> |

## 291. Ninjaone

The NinjaOne connector allows for automated IT operations and endpoint management through Swimlane Turbine, providing efficient patch management and device monitoring.

NinjaOne is a unified IT operations platform that simplifies the way IT teams work, offering a suite of tools for device management, monitoring, and security. The NinjaOne connector for Swimlane Turbine enables users to automate the retrieval of critical device and network information, manage alerts, and oversee software and OS patching directly within the Swimlane ecosystem. By integrating with NinjaOne, Swimlane Turbine users gain the ability to streamline their security operations, enhance endpoint visibility, and maintain system health with minimal manual intervention.

### Prerequisites or Asset Setup

---

This connector supports the following authentication types:

- API Key Authentication
- OAuth2.0 Client Credentials Authentication

#### API Key Authentication

- **Session Key** and **URL** are required.

#### OAuth2.0 Client Credentials Authentication

Below fields are required to get access token for authorizing API's.

- **Client ID(required)**
- **Client Secret(required)**
- **URL(required)**
- **Scopes(required)**= Array of scopes.
- **Token URL**

### Capabilities

---

This connector provides the following capabilities:

- Get Alerts
- Get Device by ID
- Get Device Disk Drives
- Get Last Logged on User
- Get OS Patch Installs
- Get OS Patches by Device ID
- Get Software Patch History
- List Logged on Users
- List Network Interfaces

## 301. OpenCTI Threat Intel Enrichment

The OpenCTI connector provides actionable threat intelligence enrichment capabilities, enabling automated incident creation and indicator management within the Swimlane platform.

OpenCTI is an open-source platform that specializes in the analysis and sharing of cyber threat intelligence. The OpenCTI Threat Intel Enrichment connector for Swimlane Turbine allows users to create and manage threat intelligence incidents and indicators directly within the Swimlane ecosystem. By integrating with OpenCTI, users can enrich their security automation workflows with detailed threat intelligence, enabling more informed decision-making and proactive defense strategies. This connector facilitates the retrieval and filtering of threat indicators, incident management, and the searching of observables for precise threat intelligence matching, enhancing the overall security posture of organizations.

### Prerequisites

To utilize the OpenCTI Threat Intel Enrichment connector, ensure you have the following:

- Custom API Key Authentication with the necessary parameters:
  - URL: The endpoint URL for the OpenCTI API.
  - API Key: A valid API key to authenticate requests to the OpenCTI platform.

### Capabilities

The OpenCTI Threat Intel Enrichment Connector has the following capabilities:

- Create Incidents
- Create Indicators
- Filter Indicators
- Get Incidents
- Search Observables

### Notes

- More information on OpenCTI Threat Intel Enrichment can be found [here](#)

## Configurations

### OpenCTI Threat Intel Enrichment Authentication

Authenticates using an API Key

#### Configuration Parameters

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

## 311. Palo Alto Networks Cortex XDR

Palo Alto Networks Cortex XDR is a comprehensive detection and response platform that unifies endpoint, network, and cloud data to prevent and respond to threats.

Palo Alto Networks Cortex XDR is a comprehensive security platform that integrates endpoint, network, and cloud data to detect and respond to threats. This connector allows Swimlane Turbine users to automate advanced threat response and policy management tasks, such as retrieving alerts, managing incidents, and isolating endpoints. By integrating with Cortex XDR, users can enhance their security operations with streamlined workflows and real-time threat intelligence, improving incident response times and reducing manual effort.

### Prerequisites

---

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

- Cortex custom authentication using the following parameters:
  - URL: The endpoint URL for accessing the Cortex XDR API.
  - Token: A valid token for authenticating API requests.
  - Cortex XDR API Key ID: The unique identifier for your Cortex XDR API key.

### Asset Setup

---

#### Generating an API Token

- Instructions for generating an API token can be found [here](#)

### Capabilities

---

This connector provides the following capabilities:

- Blacklist Files
- Get Action Status
- Get Alerts
- Get All Endpoints
- Get Endpoint
- Get Incident Additional Data
- Get Incidents
- Get PCAP Packet
- Get Policy
- Get Script Code
- Get Script Metadata
- Get Scripts
- Get Violations

# 321. Pdf Parser

## PDF Utilities

PDF Parser enables automated extraction and security analysis of PDF documents to identify content and potential threats.

PDF Parser enables automated extraction and analysis of PDF files, allowing security teams to detect threats such as embedded scripts or malicious actions within documents. This connector provides capabilities to parse text content, decrypt password-protected PDFs, and identify suspicious elements, all without manual intervention. By integrating PDF Parser with Swimlane Turbine, users can seamlessly incorporate PDF analysis into their security workflows, accelerating threat detection and response. This empowers organizations to efficiently process and investigate PDF-based threats as part of their broader security automation strategy.

## Capabilities

The PDF Utilities connector has the following capabilities

- Analyze a PDF for strings using PDFiD
- Parse a PDF to extract text

## Actions

### Analyze PDF

Extract and analyze content from a PDF attachment to identify potential threats, such as embedded JavaScript or actions triggered upon opening.

#### Endpoint

- **Method:** GET

#### Input

| Argument Name           | Type   | Required | Description               |
|-------------------------|--------|----------|---------------------------|
| eval                    | string | Optional | Python to eval            |
| attachments             | array  | Required | File to be uploaded       |
| attachments.file        | string | Optional | Parameter for Analyze PDF |
| attachments.file_name   | string | Optional | Name of the resource      |
| attachments.description | string | Optional | Parameter for Analyze PDF |

#### Input Example

```
{"eval":"string","attachments":[{"file":"string","file_name":"Example Name","description":"string"}]}
```

## 331. Qualys Container Support

The Qualys Container Support connector allows for seamless integration with Qualys' container security services, enabling automated vulnerability management and container security insights.

Qualys Container Security provides comprehensive visibility into container-related security issues, enabling organizations to enforce compliance and protect their container environments. The Qualys Container Security Connector for Swimlane Turbine allows users to automate the retrieval of container image information, vulnerability reports, and inventory management directly within their security workflows. By integrating with Qualys, security teams can enhance their container security posture, streamline vulnerability management, and maintain an up-to-date inventory of container images, all through the Swimlane Turbine platform.

### Prerequisites

---

To effectively utilize the Qualys Container Support connector with Swimlane, ensure you have the following prerequisites:

- API Key Authentication with the following parameters:
  - URL: The endpoint URL for Qualys API services.
  - Username: Your Qualys account username.
  - Password: Your Qualys account password.

### 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.

## 341. Recorded Future

Recorded Future is a threat intelligence platform that aggregates and analyzes data from diverse sources to provide actionable insights for identifying and mitigating cyber threats.

Recorded Future is a leading threat intelligence platform that aggregates and analyzes data from open, dark web, and technical sources to deliver actionable security insights. This connector enables Swimlane Turbine users to automate enrichment of indicators of compromise (IOCs), retrieve real-time threat intelligence on domains, IPs, hashes, URLs, vulnerabilities, and identities, and manage alert workflows directly within their security automation playbooks. By integrating Recorded Future with Swimlane Turbine, security teams can accelerate threat detection, prioritize and respond to incidents, and proactively mitigate risks using up-to-date intelligence. This integration empowers analysts to streamline investigations, automate alert triage, and enhance their organization's security posture with minimal manual effort.

### Prerequisites

---

Before using the Recorded Future connector, ensure you have the following prerequisites:

- API Key Authentication is required to access Recorded Future services:
  - URL: The base endpoint for accessing the Recorded Future API.
  - API Token: A valid API token issued by Recorded Future for authenticating requests.

### Limitations

---

None to date.

### Supported Versions

This connector uses the "Connect API" from Recorded Future. Actions use V2 unless otherwise noted.

### Additional Docs

- [Recorded Future Connect API](#)
- [rfapi-python](#)

### Configuration

---

#### Authentication Methods

##### API Key Authentication:

- URL: The endpoint for the Recorded Future API.
- API Token: Your unique authentication token to access the Recorded Future API.

### Capabilities

---

## 351. SOAP

This connector provides a generic SOAP client for interacting with web services. SOAP, or Simple Object Access Protocol, is a messaging protocol that allows programs running on disparate operating systems to communicate using Hypertext Transfer Protocol (HTTP) and XML. This connector is versatile and can be used to interact with various SOAP services by simply configuring the WSDL URL and other options as required by the service. Use cases include automating interactions with legacy systems, integrating with third-party services that expose SOAP APIs, and consolidating various SOAP service calls through a single interface.

### Prerequisites

---

- The WSDL URL of the SOAP service you wish to interact with.
- If the service requires HTTP Basic Authentication, you will need the username and password.
- If the service requires a client-side certificate for TLS connections, you will need the certificate in base64 format.
- Optionally, you may need to configure the transport timeout and TLS verification settings depending on your network and security requirements.

### Capabilities

---

This connector provides the following capabilities:

- Dynamically interact with various SOAP services.
- Send custom requests to a SOAP service.
- Customize transport settings including HTTP Basic Authentication, client-side certificates, TLS verification, and transport timeout.
- Parse and handle responses from SOAP services.

### Limitations

- This is a generic client; specific configurations or customizations for particular SOAP services are not provided out of the box.

### Asset Setup

---

To set up the asset, enter the WSDL URL which is mandatory. Additionally, if your SOAP service requires authentication, provide the transport username and password.

If the service requires a client-side certificate, upload it in base64 format in the `transport_certificate` field.

If you need to bypass TLS verification (not recommended for production environments), set `transport_bypassssl` to `True`.

You can also set a custom timeout for the transport connection by setting the `transport_timeout` field. This is an integer value representing seconds.

## 361. Scf Common Controls And Evidence Management

This connector facilitates the management of security controls and evidence by providing access to the Secure Controls Framework data.

The SCF Common Controls and Evidence Management connector streamlines compliance processes by integrating with the Secure Controls Framework (SCF), a comprehensive catalog of controls and evidence management practices. It enables users to obtain the latest SCF data, manage controls, and handle evidence within their security environment, either by using a user-uploaded SCF Excel file or fetching the official SCF file based on the specified version. This integration facilitates the alignment of security measures with various frameworks and standards, ensuring a robust compliance posture and simplifying evidence collection for audits within the Swimlane Turbine platform.

### Limitations

This connector has been verified on Turbine 25.0.2 & SCF version 2024.3 & 2024.4.

### Supported Versions

- Version 2024.4 represents a minor update, based on new and changed controls. The SCF had a minor formatting change that changed bullet listings to numbered listings.

## Configuration

---

### Prerequisites

To effectively use the SCF Common Controls and Evidence Management connector, ensure you have the following:

- Configuration for SCF Version with these parameters:
  - Version: Specify the version of the SCF you wish to use.
  - Selected Frameworks: Choose the frameworks from SCF relevant to your organization.
  - Verify SSL Certificates: Determine whether to enforce SSL certificate verification.

## Authentication Methods

---

### SCF Configuration Management Authentication:

- Configure & Set SCF Version with these parameters:
  - Version: Specify the version of the SCF you wish to use.
  - Selected Frameworks: Choose the frameworks from the SCF that are relevant to your organization.
  - Verify SSL Certificates: Determine whether to enforce SSL certificate verification for secure communication.

# 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](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 |