Connectors

1. ANY.RUN
2. APIVoid APIs
3. AWS EKS
4. AWS Organizations
5. Abnormal Security
6. Absolute
7. Abuse URLhaus
8. AbuseIPDB

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

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.

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

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".

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.

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

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

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

81. Cisco Umbrella Managed Service Providers

The Cisco Umbrella Managed Service Providers connector integrates with Turbine to manage MSPs

Prerequisites

The MSPs (MSP and Multi-Org consoles) endpoints require a MSP ID (mspId). Use your Umbrella Management API key and secret to authorize an API request. For more information about creating a legacy Umbrella API key, see **Authentication**

Capabilities

The Cisco Umbrella Management connector has the following capabilities:

- Find the customers for the MSP

Configurations

HTTP Basic Authentication

Authenticates using username and password.

Configuration Parameters

Parameter	Description	Type	Required
url	A URL to the target host.	string	Required
username	Username	string	Required
password	Password	string	Required
verify_ssl	Verify SSL certificate	boolean	Optional
http_proxy	A proxy to route requests through.	string	Optional

Actions

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

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

111. Cyera

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.

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

141. Elastic Kibana 8 - Security

151. Expel Workbench

Expel Workbench is a security operations platform that centralizes alert management, investigations, and remediation actions.

Expel Workbench is a security operations platform that provides comprehensive visibility and actionable insights into security incidents. This connector allows Swimlane Turbine users to seamlessly integrate with Expel Workbench, enabling automated retrieval and management of alerts, investigations, and remediation actions. By leveraging this integration, users can enhance their incident response capabilities, streamline security operations, and ensure timely remediation of threats.

Prerequisites

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

- an API token authentication using the following parameters:
  - URL: The endpoint URL for accessing Expel Workbench API.
  - API Key: A valid API key to authenticate requests to Expel Workbench.

Obtaining an API Key

API keys are obtained through your Expel Engagement Manager. Please contact Expel.

Capabilities

This Expel Workbench integration provides the following capabilities:

- Get Expel Alerts
- Get Investigations
- Get Investigation Actions
- Get Investigation Alerts
- Get Investigation Findings
- Get Investigation Remediations
- Get Security Devices

161. Fortinet FortiManager

171. Google Bigquery

Google BigQuery is a serverless, highly scalable, and cost-effective multi-cloud data warehouse designed for business agility.

Google BigQuery is a fully-managed, serverless data warehouse that enables scalable analysis over petabytes of data. The Google BigQuery connector for Swimlane Turbine allows users to execute SQL queries and manage data analytics seamlessly within the platform. By integrating with Google BigQuery, Swimlane Turbine end-users can automate data retrieval and analysis processes, enhancing their ability to make data-driven decisions quickly and efficiently. This integration empowers security teams to leverage BigQuery's powerful data processing capabilities directly within their automated workflows, reducing manual effort and improving response times.

Prerequisites

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

- Google OAuth2 authentication using the following parameters:
  - URL: The endpoint for accessing Google APIs.
  - Credentials: Your Google account credentials for authentication.
  - Scopes: Permissions required for accessing specific Google services.
  - API Key: A key to authenticate requests to the Google API.

Limitations

None to date.

Capabilities

This Connector provides the following capabilities:

- Jobs Query

Jobs Query

181. Google Translate

The Swimlane Google Translate Connector integrates with Swimlane Turbine to do the translate text from spam emails & strings found in malware analysis.

Prerequisites

This Connector requires a OAuth Client IDs.

For setting up OAuth 2.0 client ID & token - **https://support.google.com/cloud/answer/6158849**

Capabilities

The Swimlane Google Translate connector has the following capabilities:

- Language
- Translate

Credentials Information

When this document uses the term user account, it refers to a Google Account, or a user account managed by your identity provider and federated with workforce identity federation.

For authentication, credentials are a digital object that provide proof of identity. Passwords, PINs, and biometric data can all be used as credentials, depending on the application requirements. For example, when you log into your user account, you provide your password and satisfy any two-factor authentication requirement as proof that the account in fact belongs to you, and you are not being spoofed by a bad actor.

Tokens are sometimes referred to as credentials, but for this documentation, they are instead referred to as a digital object that proves that the caller provided proper credentials, but they are not credentials themselves.

The type of credential you need to provide depends on what you are authenticating to. The following types of credentials can be created in the Google Cloud console:

191. Hackerone

201. HubSpot CRM

The HubSpot CRM connector facilitates the integration of HubSpot's CRM capabilities into automated workflows, enabling efficient management and analysis of customer data.

HubSpot CRM is a comprehensive customer relationship management platform that helps businesses manage their sales, marketing, and customer service efforts in one place. The HubSpot CRM Connector for Swimlane Turbine enables users to automate the creation, retrieval, and updating of company records within HubSpot CRM directly from the Swimlane platform. By integrating with HubSpot CRM, users can streamline their sales and marketing workflows, maintain up-to-date customer information, and enhance their overall customer engagement strategies without the need for manual data entry or complex API interactions.

Prerequisites

To effectively utilize the HubSpot CRM connector with Swimlane Turbine, you must have the following:

- OAuth2 refresh token authentication with these parameters:
  - URL: The endpoint URL for HubSpot API access.
  - Client ID: Your HubSpot application's client identifier.
  - Client Secret: The secret key associated with your HubSpot application.
  - Refresh Token: A token used to obtain a new access token when the current one expires.

Asset Setup

Client Credential Flow Authentication

Authentication uses HubSpot application OAuth2. You will need an admin account in HubSpot to create the application.

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

- **A Developer Account**
- **An App** associated with your developer account

211. Infoblox BloxOne Threat Defense

Infoblox BloxOne Threat Defense is a DNS-based security solution that protects networks from cyber threats by analyzing and blocking malicious traffic.

Infoblox BloxOne Threat Defense is a comprehensive security solution that provides advanced threat intelligence and protection. This connector enables Swimlane Turbine users to automate the creation of dossier lookup jobs and retrieve active threat data, enhancing their threat detection and response capabilities. By integrating with Infoblox, users can streamline threat intelligence processes, reduce manual effort, and improve the accuracy and speed of threat investigations.

The Infoblox BloxOne Threat Defense integrates with Swimlane Turbine to lookup IPs, Hosts, and URLs and Query Threats.

Prerequisites

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

- an API key authentication using the following parameters:
  - URL: The endpoint URL for accessing Infoblox services.
  - API Key: A unique key provided by Infoblox for authenticating API requests.

Capabilities

This connector provides the following capabilities:

- Create Dossier Lookup Jobs
  - Lookup Host
  - Lookup IP
  - Lookup URL
  - Lookup hash
  - Lookup email
- Get Threat Intelligence Data Exchange
  - Query Threats

221. Jinja

The Jinja connector enables the rendering of dynamic content using templating, allowing for the creation of customized outputs based on user-provided JSON data and templates.

Jinja is a powerful templating engine used to generate dynamic content with ease. The Jinja connector for Swimlane Turbine allows users to automate the creation of customized documents by rendering templates with JSON data. This integration streamlines the process of generating reports, alerts, and notifications, tailored to the specific needs of security operations. By leveraging Jinja's templating capabilities within Swimlane Turbine, users can enhance their security workflows with personalized, data-driven document generation, saving time and reducing manual effort.

Limitations

None to date.

Supported Versions

This Jinja connector uses the latest Version.

Additional Docs

- **Jinja Reference Docs Link**

Authentication Methods

None to date.

Capabilities

This Jinja Connector provides the following capabilities:

- Render Object
- Render Template

Render Object

231. Lastline Analyst

The Lastline Analyst connector enables automated malware analysis and threat intelligence gathering directly within security workflows.

Lastline Analyst is a renowned platform for advanced malware analysis, providing detailed insights into emerging threats. The Lastline Analyst Connector for Swimlane Turbine enables users to automate the creation of Indicators of Compromise (IOCs), retrieve IOC metadata, analyze files and URLs, and track detailed analysis results. This integration empowers security teams to enhance their threat detection and response capabilities, streamline analysis workflows, and rapidly identify and mitigate potential security risks within their digital environment.

Prerequisites

To effectively utilize the Lastline Analyst connector with Turbine, ensure you have the following prerequisites:

- HTTP Basic Authentication with these parameters:
  - URL: The endpoint URL for the Lastline Analyst API.
  - API Key: Your unique API key provided by Lastline Analyst for authentication.
  - API Token: A token paired with your API key to establish a secure connection.

Capabilities

The VMWare Lastline Analyst connector has the following capabilities:

- Submit URL
- Submit File
- Get URL Results
- Get File Results
- Get IOC
- Create IOC

Configurations

241. Manageengine Servicedesk Plus

The ManageEngine ServiceDesk Plus connector streamlines IT service management by automating interactions with the ServiceDesk Plus platform.

ManageEngine ServiceDesk Plus is a comprehensive IT service management (ITSM) solution that enables organizations to manage and resolve service requests efficiently. The Swimlane Turbine connector for ServiceDesk Plus allows users to automate a wide range of ITSM tasks, including the creation, update, and deletion of service requests, tasks, approvals, notes, and worklogs. By integrating with ServiceDesk Plus, Swimlane Turbine users can streamline their ITSM workflows, enhance incident response with detailed documentation, and improve overall efficiency by reducing manual processes.

The ManageEngine ServiceDesk Plus Connector allows the Cloud API allows you to perform all the operations that you do with our web client.

Prerequisites

To effectively utilize the ManageEngine ServiceDesk Plus connector for Turbine, ensure you have the following prerequisites:

- API Key Authentication with the following parameters:
  - URL: Endpoint URL for the ServiceDesk Plus API.
  - API Key: Unique identifier to authenticate API requests.
- Custom Authentication with the following parameters:
  - url: Endpoint URL for the ServiceDesk Plus API.
  - Client ID: Identifier for the OAuth client.
  - Client Secret: Secret key for the OAuth client.
  - Code: Authorization code obtained during OAuth flow.

Custom Authentication

The ServiceDesk Plus Connector requires a client ID, a client secret and a temporary code.

The following steps are required to set up the asset. The procedure is somewhat different than with other Connectors.

251. Microsoft Azure Sentinel

Microsoft Azure Sentinel is a scalable, cloud-native SIEM solution that provides intelligent security analytics and threat intelligence.

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. This connector enables seamless integration with Swimlane Turbine, allowing users to automate incident management, threat detection, and response actions. By leveraging Azure Sentinel's capabilities, Swimlane Turbine users can enhance their security operations with real-time insights, streamline workflows, and improve threat response times.

Prerequisites

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

- OAuth 2.0 Client Credentials authentication using the following parameters:
  - URL: The endpoint for accessing Azure Sentinel services.
  - Client ID: The application ID registered in Azure Active Directory.
  - Client Secret: The secret key associated with the client ID.
  - Token URL: The URL used to obtain the OAuth token.
  - Scopes: The permissions required for accessing Azure Sentinel resources.

Token URL

Use the following as the token URL,

- To run the Log Analytics Query action, use `https://login.microsoftonline.com/{tenant_id}/oauth2/token`.
- For all other actions, use `https://login.microsoftonline.com/{tenant_id}/oauth2/v2.0/token`.

Host URL

- To run the Log Analytics Query action, use `https://api.loganalytics.azure.com/`.

261. Microsoft Graph API Device Management

Microsoft Graph API Device Management provides tools for managing and securing devices via the Microsoft Graph API.

Microsoft Graph API Device Management provides a comprehensive interface for managing Intune devices and retrieving BitLocker recovery keys. This integration allows Swimlane Turbine users to seamlessly automate device management tasks, such as listing managed devices and retrieving critical recovery keys, enhancing operational efficiency and security posture. By leveraging this connector, users can streamline device management processes and ensure quick access to essential device information, all within the Swimlane Turbine platform.

Prerequisites

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

- Delegated flow authentication using the following parameters:
  - URL: The endpoint for Microsoft Graph API.
  - Tenant ID: The directory tenant identifier.
  - Username: The username for authentication.
  - Password: The password for authentication.
  - Client ID: The application client identifier.
  - Client Secret: The application client secret.
- OAuth2 refresh token authentication using the following parameters:
  - URL: The endpoint for Microsoft Graph API.
  - Client ID: The application client identifier.
  - Client Secret: The application client secret.
- OAuth2 client credentials authentication using the following parameters:
  - URL: The endpoint for Microsoft Graph API.
  - Client ID: The application client identifier.
  - Client Secret: The application client secret.

271. Microsoft OneDrive

The OneDrive connector allows Swimlane to integrate with Microsoft Graph OneDrive enpoints.

Prerequisites

Ensure that you have administrator rights so that you can add permissions that will fully utilize all capabilities within this connector.

Capabilities

The Microsoft Graph API connector gives the ability to get and update security alerts, and modify user licenses and sessions.

- Create Drive Folder
- Create Group Folder
- Create Site Folder
- Create User Folder
- Dowload Drive File
- Upload Drive File

Asset Setup

Authentication uses Azure application OAuth2. You will need an admin account in Azure to create the application.

Recommended Application Permissions (feel free use custom permissions if you only use certain actions):

- User.ReadWrite.All
- Directory.ReadWrite.All
- Directory.AccessAsUser.All
- SecurityEvents.Read.All
- SecurityEvents.ReadWrite.All

281. Mongodb Atlas

The MongoDB Atlas connector enables seamless integration with Swimlane Turbine, allowing for the automation of database management tasks and trigger creation.

MongoDB Atlas is a fully-managed cloud database developed by the same people that build MongoDB. The MongoDB Atlas connector for Swimlane Turbine allows users to automate complex database operations, such as creating triggers for authentication, database, and scheduled events, as well as running queries and retrieving configurations. This integration empowers security teams to streamline their database-related workflows, enhance real-time data processing, and enforce security measures directly within their security automation playbooks.

MongoDB Atlas is a fully managed cloud database service that allows you to deploy, manage, and scale MongoDB databases easily.
It offers various features and tools to ensure your database operates efficiently, securely, and reliably.

Prerequisites

To effectively utilize the MongoDB Atlas connector with Swimlane Turbine, ensure you have the following:

- Username and API Key authentication with the following parameters:
  - URL: The base endpoint for MongoDB Atlas API access.
  - Public API Key: Your MongoDB Atlas account's public API key.
  - Private API Key: Your MongoDB Atlas account's private API key.

Capabilities

This connector provides the following capabilities:

- Create a Authentication Trigger
- Create a Database Trigger
- Create a Scheduled Trigger
- Get All Triggers

291. Noname

The Noname API Connector is a powerful tool designed to bridge the gap between your applications and the Noname API. By leveraging this connector, you can conveniently streamline your access to various functionalities provided by the Noname API.

Getting Started

Before you begin, ensure you meet the following prerequisites:

- You must have a valid email address and password associated with your Noname API account.

Key Features

The Noname API Connector offers a robust set of capabilities aimed at improving the efficiency of your operations:

1. **Fetch Specific Issue:** Allows you to retrieve the details of a specific issue by providing the corresponding ID.
2. **Access Issue Evidence:** Empowers you to gather supportive evidence associated with a specific issue. The required input is the respective Issue ID.

Please note that your ability to use these features effectively may depend on the permissions and access rights tied to your Noname API account. Always ensure that your account has sufficient privileges for the operations you wish to carry out.

Configurations

Noname Authentication

Authenticates using email and password.

Configuration Parameters

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

301. Opswat Metadefender

The OPSWAT MetaDefender Connector integrates with Swimlane to retrieve information from OPSWAT.

Prerequisites

The OPSWAT MetaDefender asset requires an API Key.

Capabilities

The OPSWAT MetaDefender Connector has the following capabilities:

- Get EXIF Lookup
- Get PE Info Lookup
- Get APK Manifest Lookup
- Download Sanitize File
- Get IP Lookup
- Analyze File
- Retrieving Webhook Status
- Retrieving Scan Reports using Data Hash
- Fetch Analysis Result

Additional information about the API's endpoints can be found **here**.

This Connector was last tested against product version: API V4.

Configurations

API Key Authentication

Authenticates using an API Key

Configuration Parameters

Parameter	Description	Type	Required

311. Palo Alto Networks Pan-OS

The Palo Alto Networks Pan-OS connector enables streamlined integration and automation of network security tasks within the Swimlane Turbine platform.

Palo Alto Networks Pan-OS is a comprehensive suite for network security, offering advanced threat prevention, firewall functionalities, and unified policy management. This connector enables Swimlane Turbine users to automate configuration changes, policy management, and security enforcement across their network infrastructure. By integrating with Pan-OS, security teams can streamline their workflows, enforce consistent security policies, and respond to threats with agility and precision, all within the Swimlane Turbine platform.

Prerequisites

To effectively utilize the Palo Alto Networks Pan-OS connector for Swimlane Turbine, ensure you have the following prerequisites:

- API Key Authentication with the following parameters:
  - URL: The base URL of the Palo Alto Networks Pan-OS instance.
  - API Key: A valid API key to authenticate requests to the Pan-OS instance.

Actions Setup

Commit Changes

The following are examples of commit commands. Note that the 'cmd' input is a valid XML.

Commit:

```
type=commit
cmd=<commit></commit>
```

Force Commit:

321. Pixis

The Pixis connector allows seamless integration with the Pixis platform, enabling automated network management and security operations.

Pixis is a comprehensive network security management platform that allows for the monitoring and control of network access based on device MAC addresses. The Pixis Turbine Connector enables users to automate critical network security operations such as authorizing, blocking, and querying MAC addresses, as well as managing custom security policies and retrieving customer-specific data. By integrating with Swimlane Turbine, security teams can enhance their network security posture, streamline access control processes, and gain valuable insights into network activity without manual intervention.

Limitations

None to date.

Supported Versions

This Pixis Connector uses the lastest version.

Additional Docs

Configuration

Prerequisites

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

- API key authentication with the following parameters:
  - URL: Endpoint for the Pixis API.
  - Account: Your Pixis account identifier.
  - Watchword: A secure passphrase used for API authentication.

Capabilities

331. Rapid7 Insight VM

341. Reversinglabs A1000

351. SSH

The SSH connector is capable of running SSH commands.

Prerequisites

The SSH asset requires a host IP, username, and password.

Capabilities

The SSH connector has the following capabilities:

- Run Command(s)
- Get Files
- Put Files

Configurations

SSH Authentication

SSH Authentication

Configuration Parameters

Parameter	Description	Type	Required
host	Address of the SSH server	string	Required
port	Port	integer	Optional
username	Username	string	Required
password	Password	string	Required

Actions

Run Command

361. Security Scorecard

371. 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

381. Spycloud

The SpyCloud connector provides access to a comprehensive database of breached credentials and personal information, enabling proactive threat mitigation and account protection.

SpyCloud is a leader in cybercrime analytics and identity protection, offering a comprehensive database of compromised assets. The SpyCloud Turbine Connector enables users to automate the retrieval of compromised application and device data, breach details, and specific application or device breach information. By integrating with SpyCloud, Swimlane Turbine users can proactively protect against account takeovers, streamline breach analysis, and enhance their security posture with actionable intelligence on exposed credentials and potential threats.

Prerequisites

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

- API Key Authentication with the necessary parameters:
  - URL: Endpoint for SpyCloud API services.
  - SpyCloud API Key: Unique identifier to authenticate requests.

Capabilities

This plugin provides the following capabilities:

- Get Compass Applications List
- Get Compass Breach Data by Application Search
- Get Compass Breach Data
- Get Compass Devices Data
- Get Compass Devices List

API Documentation Link

- For more information on SpyCloud is found at: **SpyCloud API Documentation**

391. Swimlane Turbine API

The Swimlane Turbine API connector enables users to perform generic API requests to the Swimlane platform, facilitating custom automation and integration scenarios.

The Swimlane Turbine API Connector enables seamless integration with the Swimlane Turbine platform, a leading low-code security automation solution. By leveraging this connector, users can execute generic API requests to interact with the Turbine platform, allowing for the automation of security workflows and the expansion of actionability across their security ecosystem. The connector simplifies the process of sending and receiving data through the Turbine API, providing a streamlined experience for managing security operations without the need for coding expertise.

Prerequisites

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

- Turbine API authentication credentials, which can be either:
  - Username and Password: Credentials associated with a user account on the Swimlane platform.
  - Personal Access Token (PAT): A secure token generated within the Swimlane platform for API access without using a password.

Username/Password Authentication:

- URL: The base URL of your Swimlane Turbine instance.
- Username: A valid username with the necessary permissions.
- Password: The password associated with the username.

PAT Authentication:

- URL: The base URL of your Swimlane Turbine instance.
- PAT: A valid Personal Access Token generated from your Swimlane Turbine instance.

Capabilities

401. Tanium

411. Thinkst Canary

Thinkst Canary is a deception technology platform that helps organizations detect intrusions by deploying honeypots and Canarytokens.

Thinkst Canary is a leading deception technology platform designed to detect intrusions and unauthorized access by deploying decoy systems and tokens. The Thinkst Canary connector for Swimlane Turbine enables seamless integration for automated incident management, allowing users to acknowledge, delete, and fetch incidents and Canarytokens efficiently. This integration enhances threat detection and response capabilities, providing Swimlane Turbine users with real-time insights and automated workflows to manage security incidents effectively.

Limitations

- None to date.

Supported Versions

- This Thinkst Canary connector uses the v1 API.

Additional Documents

- Documentation **Thinkst Canary**

Configuration

Prerequisites

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

- Authentication using an Authentication Token:
  - URL: The endpoint URL for accessing the Thinkst Canary API.
  - Auth Token: A valid authentication token to authorize API requests.

Authentication Methods

421. Trend Micro Vision One V3

Trend Micro Vision One is a comprehensive threat detection and response platform that provides enhanced visibility and protection across multiple environments.

Trend Micro Vision One is a comprehensive security platform designed to enhance threat detection and response capabilities. This connector allows seamless integration with Swimlane Turbine, enabling users to automate security operations such as alert management, threat intelligence, and endpoint protection. By leveraging this integration, Swimlane Turbine users can efficiently manage alerts, block or remove suspicious objects, and perform detailed threat analysis, thereby enhancing their security posture and operational efficiency.

This Connector integrates Trend Micro Vision One API version 3 with Swimlane Turbine.

Prerequisites

Before you can use the Trend Micro Vision One v3 connector for Turbine, you'll need access to the Trend Micro Vision One API. This requires the following:

- HTTP Bearer authentication using the following parameters:
  - URL: The endpoint URL for accessing Trend Micro Vision One API.
  - Token: A valid bearer token for authenticating API requests.

Capabilities

This Connector provides the following capabilities:

- Add Alert Note
- Add to Block List
- Delete Alert Notes
- Edit Alert Note
- Get Alert Note
- Get Alert Notes
- Get Alerts Details
- Get Alerts List

431. Vali Cyber ZeroLock

The ZeroLock platform addresses the entire Linux threat landscape from ransomware to cryptojacking. ZeroLock goes beyond traditional mandatory access control capabilities. In contrast to SELinux and AppArmor, ZeroLock offers easily configured and universally applied rules and policies that can be deployed across all your Linux and cloud environments from a single console.

Prerequisites

You need an `username` and `password` to authenticate the connector.

Capabilities

This connector provides the following capabilities:

- Archive Endpoints
- Change Agent Version
- Create User
- Get Alert Details by ID
- Get Alert List
- Get Alerts by Time
- Get Alerts per Endpoint
- Get Endpoint Count
- Get Endpoint Data by ID
- Get Endpoint Uptime
- Get Frontend Table Alert List
- Get Number of Alerts
- Get Summary Information about Protected Endpoints
- Kill Alert by ID
- Kill Alerts

  ... and so on

441. Vmware Vcenter

The VMWare vCenter connector allows for seamless integration with VMWare's virtualization management platform, enabling automated interactions with virtual machines and their operating systems.

VMware vCenter is a centralized management platform for VMware vSphere environments, designed to simplify virtual infrastructure management. This connector enables Swimlane Turbine users to automate key virtual machine operations such as retrieving guest identities, managing power states, and querying guest OS processes. By integrating with VMware vCenter, users can enhance their security automation workflows, ensuring efficient VM management and rapid response to security incidents within their virtualized environments.

Prerequisites

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

- Custom authentication with the following parameters:
  - URL: The endpoint URL for the VMWare vCenter API.
  - Grant Type: The OAuth grant type used for authorization.
  - Subject Token: The subject token required for obtaining an access token.
  - Subject Token Type: The type of the subject token provided for authentication.

Capabilities

This connector provides the following capabilities:

- Get Guest Identity
- Get Guest Power
- Get VM PID Processes
- List Guest Process
- Reboot Guest Power
- Shutdown Guest Power
- Standby Guest Power

451. Workday

This Connector allows you to interact with the Workday API. This connector is based on the Workday Rest API and uses version v1.

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 Activities for a Specific Customer
- Get Activity for Customer
- Get Customer
- Get Direct Reports for Worker
- Get History Items for Worker
- Get Leave Status
- Get Organization by ID
- Get Organizations
- Get Organizations for Worker
- Get Pay Slips for Worker
- Get Time Off Entires for Worker
- Get Values Time off Status
- Get Worker by ID
- Get Workers
- Get Workers Eligible Absence Types

  ... and so on

Notes

461. Zscaler Security

The Zscaler Security connector enables seamless integration of Zscaler's cloud-based security services with Swimlane's automation capabilities, facilitating real-time policy management and threat intelligence.

Zscaler Security is a cloud-based information security platform that offers comprehensive protection against cyber threats. This connector enables Swimlane Turbine users to automate Zscaler policy management and threat response, streamlining security operations. By integrating with Zscaler Security, users can instantly apply configuration changes, manage firewall rules, and update URL categories, enhancing their security posture with minimal manual intervention.

Prerequisites

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

- Client Credentials and Tenant ID authentication with these parameters:
  - URL: The endpoint URL for Zscaler API services.
  - Client ID: Your unique identifier for Zscaler API access.
  - Client Secret: A secret key associated with your Client ID for authentication.
  - Tenant ID: The identifier for your specific Zscaler tenant instance.
  - Scope: The scope of access requested for the API token.
- API Key authentication with these parameters:
  - URL: The endpoint URL for Zscaler API services.
  - Username: Your Zscaler account username.
  - Password: Your Zscaler account password.
  - API Token: A unique token generated for API access.

Client Credential Flow Authentication

Authentication uses Zscaler's OAuth 2.0 client credentials flow via the ZIdentity platform.

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