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. Cherwell Service Management Rest

The Cherwell Service Management Rest connector allows for streamlined automation of IT service management tasks by interfacing with Cherwell's ITSM platform.

Cherwell Service Management is a comprehensive IT service management (ITSM) solution that streamlines service delivery and enhances IT workflow efficiency. This connector enables Swimlane Turbine users to automate ITSM processes by creating, updating, and retrieving Cherwell Business Objects directly within the Swimlane platform. By integrating with Cherwell Service Management Rest, users can leverage real-time data synchronization, incident management, and service request fulfillment, enhancing their security automation and response capabilities.

Limitations

None to date.

Supported Versions

This Cherwell Service Management Rest connector uses the Version 1 API.

Additional Docs

- **API Documentation**
- **Authentication**

Configuration

Prerequisites

To utilize the Cherwell Service Management Rest connector, you must have the following:

- Cherwell Service Management authentication credentials, which include:
  - URL: The endpoint URL for the Cherwell Service Management API.
  - Cherwell Client ID: The unique identifier for your Cherwell application.
  - Grant Type: The OAuth grant type used for obtaining the necessary tokens.

81. Cisco Webex

The Cisco Webex connector allows for streamlined communication within Webex by automating message handling and collaboration directly through the Swimlane platform.

Cisco Webex is a leading enterprise solution for video conferencing, online meetings, screen share, and webinars. The Cisco Webex connector for Swimlane Turbine enables users to automate communication and collaboration workflows within their security operations. By integrating with Webex, security teams can streamline incident response by sending messages, managing content, and coordinating team efforts directly through the Swimlane platform. This connector enhances real-time communication and collaboration, ensuring rapid dissemination of critical information and cohesive team action during security incidents.

Prerequisites

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

- Custom authentication with Cisco Webex using the following parameter:
  - URL: The base endpoint URL for the Cisco Webex API.

Asset Setup

To use the Cisco Webex connector with Swimlane Turbine, you need to set up custom authentication with one of the following configurations:

- OAuth2 access token authentication with these parameter:
  - URL: Endpoint for the Cisco Webex API service.
  - Access Token: Token used to authenticate API requests.
- OAuth2 refresh token authentication with these parameters:
  - URL: Endpoint for the Cisco Webex API service.
  - Client ID: Your Cisco Webex application's client identifier.
  - Client Secret: The secret key associated with your Cisco Webex application.
  - Refresh Token: A token used to obtain a new access token when the current one

91. Cohesity Helios

101. CrowdStrike Logscale

CrowdStrike Logscale is a log management platform that enables efficient ingestion, searching, and analysis of log data.

CrowdStrike Logscale is a powerful platform for log management and analysis, designed to handle large volumes of data with speed and efficiency. By integrating with Swimlane Turbine, users can automate security operations and data analysis, leveraging Logscale's capabilities to enhance threat detection and response. This integration allows for seamless ingestion, querying, and management of log data, enabling security teams to streamline workflows and improve incident response times.

Prerequisites

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

- HTTP Bearer authentication using the following parameters:
  - URL: The endpoint URL for accessing CrowdStrike Logscale services.
  - Token: A bearer token such as a JWT for authenticating API requests.

Asset Setup

The asset for this Connector requires the following input:

- Token

Capabilities

This Connector provides the following capabilities:

- Create Alert
- Create Query Jobs
- Delete Alert by ID
- Delete File for Cloud Users
- Delete File for on Premises Users

111. Cylance Protect

Cylance Protect is an AI-driven endpoint protection platform designed to prevent, detect, and respond to cyber threats.

Cylance Protect is a leading endpoint security platform that leverages AI and machine learning to prevent cyber threats. This connector enables seamless integration with Swimlane Turbine, allowing users to automate endpoint security tasks such as managing devices, zones, and threat lists. By integrating Cylance Protect with Swimlane Turbine, users can enhance their security operations with automated threat management, device control, and policy enforcement, ensuring a robust defense against cyber threats.

Prerequisites

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

- OAuth 2.0 Client Credentials authentication using the following parameters:
  - URL: The endpoint URL for accessing the Cylance Protect API.
  - Client ID: The unique identifier for your application in Cylance Protect.
  - Client Secret: The secret key associated with your client ID for secure authentication.

Capabilities

The Cylance Protect connector has the following capabilities:

- Manage Devices
  - ***Note***: To update a device zone, the zone ID, which is the ID in the URL of a zone, must be used.
    The zone ID is at the end of the URL. Multiple zones should be entered as a comma-separated list.
  - EX: **https://protect.cylance.com/Zone/ZoneDetails/**_59008bce-42e9-4e6e-a7a6-36eefdccc0eb_**
- Manage Device Threats

121. Dataminr Pulse

Dataminr Pulse is a real-time information discovery platform that provides critical alerts from publicly available data sources.

Dataminr Pulse is a leading real-time information discovery platform that provides critical alerts on global events. By integrating Dataminr Pulse with Swimlane Turbine, users can seamlessly retrieve and manage real-time alerts and preconfigured alert lists. This integration empowers security teams to enhance situational awareness and respond swiftly to emerging threats, leveraging Dataminr's comprehensive alerting capabilities within the Swimlane Turbine environment.

Prerequisites

Before you can use the Dataminr Pulse connector for Swimlane, you'll need access to the Dataminr API. This requires the following:

- OAuth2 authorization using the following parameters:
  - URL: The endpoint for accessing Dataminr's API services.
  - Client ID: A unique identifier for your application to authenticate with Dataminr.
  - Client Secret: A secret key used in conjunction with the Client ID to authenticate your application securely.

Asset Setup

You will need a `client ID` and `client secret` along with the `url` to access the API.

Capabilities

This Connector provides the following capabilities:

- Get Alerts
- Get Alert Lists

Get Alerts

Input param `query` is required if `lists` is not provided.

131. Duo Security

Duo Security provides multi-factor authentication and secure access solutions to protect organizations' sensitive data.

Duo Security is a trusted platform for advanced identity verification and access management, ensuring secure user authentication and device management. This connector enables seamless integration with Swimlane Turbine, allowing users to automate identity and access management tasks such as associating phones with users, modifying administrators, and retrieving user and device information. By leveraging this integration, security teams can enhance their operational efficiency, streamline user management processes, and ensure robust security measures without manual intervention.

Prerequisites

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

- HMAC authentication using the following parameters:
  - URL: The endpoint URL for accessing Duo Security services.
  - Username: The username required for authenticating API requests.
  - Secret Key: A secret key used to sign requests and verify authenticity.

Capabilities

This Connector provides the following capabilities:

- Associate Phone Device with User
- Modify Administrator
- Retrieve Administrators
- Retrieve Bypass Codes
- Retrieve Phones by User ID
- Retrieve Phones
- Retrieve User by User ID
- Retrieve Users

141. Exabeam Aa V2

The Exabeam AA v2 connector facilitates seamless integration with Swimlane Turbine, enabling automated security incident response and rule management.

Exabeam AA v2 is an advanced analytics platform that enhances security operations by identifying complex threats and improving incident response. This connector allows Swimlane Turbine users to automate the creation, deletion, and management of correlation rules, as well as to search for events within Exabeam. By integrating with Exabeam AA v2, users can streamline their security workflows, enforce consistent security policies, and rapidly respond to potential threats with precision and efficiency.

Prerequisites

To effectively utilize the Exabeam AA v2 connector with Swimlane Turbine, ensure you have the following:

- OAuth 2.0 client credentials for secure authentication, which include:
  - URL: The endpoint URL for the Exabeam AA v2 API.
  - API Key: Your unique identifier to authenticate with the Exabeam AA v2 API.
  - API Key Secret: A secret key paired with your API Key for enhanced security.

Capabilities

This connector provides the following capabilities:

- Create A New Correlation Rule
- Delete A Correlation Rule
- Get A List Of All Correlation Rules
- Get Correlation Rule Details
- Search For Events
- Update A Correlation Rule

Notes

For more information on Exabeam:

151. Fireeye

The FireEye connector allows seamless integration with FireEye's security services, enabling automated threat detection and response workflows.

FireEye is a renowned cybersecurity company that provides advanced solutions for threat detection and response. The FireEye connector for Swimlane Turbine enables users to automate critical security operations tasks such as acknowledging alerts, managing quarantined emails, and retrieving detailed threat intelligence. By integrating with FireEye, Swimlane Turbine users can streamline incident response, enhance email security, and access rich threat insights directly within their automated workflows, significantly improving their security posture and response times.

Prerequisites

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

- HTTP Basic Authentication with the following parameters:
  - URL: Endpoint URL for the FireEye API.
  - Username: Your FireEye account username.
  - Password: Your FireEye account password.

Asset Configuration

This connector requires a `Username` and a `Password` for secure communication with the FireEye appliances. It uses basic HTTP authentication, a widely-adopted method that ensures secure interactions with your FireEye systems.

Functionalities

The FireEye connector provides a comprehensive set of functionalities:

- **Acknowledge Alert**: Allows for acknowledgment and recording of alerts for potential security threats.
- **Delete Quarantined Email**: Enables safe removal of emails in quarantine, maintaining the integrity of your communication systems.

161. Freshworks Freshdesk

The Freshdesk connector enables streamlined customer support operations by automating ticket management tasks within the Freshdesk platform.

Freshworks Freshdesk is a dynamic customer support platform that offers a suite of tools for ticketing, collaboration, and resolution of customer issues. This connector enables Swimlane Turbine users to automate ticket management, change requests, and communication workflows directly within the platform. By integrating with Freshdesk, users can create, update, delete, and view tickets, add notes, and manage change requests without leaving the Swimlane environment. This streamlines incident response, enhances customer service efficiency, and ensures seamless collaboration among support agents.

The Freshworks Freshdesk connector integrates with Swimlane to allow for automated tasks to be conducted using the Fresdesk REST API.

Prerequisites

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

- HTTP Basic Authentication with the following parameters:
  - URL: The endpoint URL for your Freshdesk instance.
  - API Key: Your Freshdesk API key for authentication.
  - Password: The password associated with the Freshdesk account.

Capabilities

This Freshworks Freshdesk Connector provides the following capabilities:

- Create a Note
- Create a Change
- Create a Ticket
- Delete a Ticket
- List all Tickets
- Create a Reply

171. Google Drive

The Google Drive connector enables automated interactions with Google Drive, allowing for efficient file and folder management, including creation, duplication, and deletion, as well as data sharing and collaboration.

The Google Drive connector for Swimlane Turbine provides a comprehensive suite of actions to manage files and folders directly within your security workflows. With this integration, users can create, copy, and delete files and folders, manage spreadsheets, and list files based on specific queries, all without leaving the Swimlane platform. This seamless connection enhances productivity by automating routine Google Drive tasks, ensuring that document management is both efficient and secure. By leveraging the Google Drive connector, Swimlane Turbine users can focus on critical security tasks while the connector handles the intricacies of file management.

Google Cloud Platform and Google Admin Provisioning

Prerequisites

To utilize the Google Drive connector for Swimlane Turbine, ensure you have the following prerequisites:

- OAuth2 Client Credentials with the following parameters:
  - Client ID: The unique identifier for your application.
  - Client Secret: A secret known only to the application and the authorization server.
  - Refresh Token: A token used to obtain a new access token when the current one expires.
- Service Account Authentication with the following parameter:
  - Credentials: A file containing credentials such as client_email and private_key for a Google Service Account.

GCP Project Creation:

1. Log in to GCP Console here: **https://console.cloud.google.com/**
2. Navigate to this link to create a new project:

181. Group-IB Intelligence

Group-IB Intelligence provides detailed threat intelligence data, enabling organizations to detect, analyze, and respond to cyber threats effectively.

Group-IB Intelligence provides comprehensive threat intelligence data, including insights from dark web marketplaces, compromised accounts, bank cards, and more. This connector enables Swimlane Turbine users to seamlessly integrate Group-IB's actionable intelligence into their security workflows. By leveraging this integration, users can enhance threat detection, automate intelligence gathering, and streamline incident response processes, ensuring a proactive security posture.

Prerequisites

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

- HTTP Basic authentication using the following parameters:
  - URL: The endpoint URL for accessing Group-IB Intelligence services.
  - Username: Your Group-IB account username for authentication.
  - API Key: A unique key provided by Group-IB for secure access to their API.

Asset

- The Group-IB Connector requires Username and API Key.
- Group-IB accepts connections only from whitelisted IP addresses. If a customer is using Swimlane on-cloud solution, they should contact the Swimlane Infrastructure team to get the public IPs of the instance and whitelist them in Group-IB Portal.
- Group-IB has strict rate limiting and raises `429 Client Error: Too Many Requests for url`. The customer should wait for at least 15sec before making another request.

Capabilities

The Group-IB Intelligence Connector provides the following capabilities:

- Get Access

191. 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

201. 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

211. 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
[illegible]	[illegible]	[illegible]	[illegible]

221. 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

231. 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:

```
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

241. 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

251. 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

261. Microsoft Intune

The Microsoft Intune Connector is a software component that allows for seamless integration between Intune and Turbine,
leveraging the OAuth2 protocol for secure authentication and authorization.
This readme provides instructions for configuring and using the connector with Graph's OAuth2 configuration.

Prerequisites

Before you can use the Microsoft Intune Connector, you must meet the following prerequisites:

- A Microsoft Intune subscription
- An Azure AD tenant with at least one registered application
- An OAuth2 client ID and secret for your registered application

Note that if there is a Microsoft Graph API asset configured in Turbine, there is no need to create a new as long as the
asset has the correct permissions.

Configurations

Oauth 2.0 Client Credentials

Authenticates using oauth 2.0 client credentials

Configuration Parameters

Parameter	Description	Type	Required
url	A URL to the target host.	string	Required
token_	Must start with **https://login.microsoftonline.com/** and then	stri	Require

271. Misp

MISP is an open-source threat intelligence platform that facilitates the sharing of structured threat information among organizations.

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source threat intelligence platform designed to improve the sharing of structured threat information. The MISP Turbine Connector enables seamless integration with Swimlane Turbine, allowing users to automate the management of threat intelligence data. This integration enhances security operations by enabling automated actions such as adding, editing, and deleting threat attributes and events, enriching threat data, and executing custom scripts for advanced threat analysis.

Prerequisites

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

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

Capabilities

The Connector for MISP needs to support the following capabilities:

- Add Attribute
- Add Event
- Add Event Tag
- Add Tag to Attribute
- Delete Attribute
- Delete Event
- Edit Attribute
- Get a Filtered and Paginated List of Attributes
- Get a Filtered and Paginated List of Objects

281. 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

291. 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

301. 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:

311. 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

321. Rapid7 Insight VM

The Rapid7 Insight VM connector facilitates seamless integration with Swimlane Turbine, enabling automated vulnerability management and security processes.

Rapid7 InsightVM is a powerful vulnerability management tool that provides comprehensive visibility into the security posture of your assets. This connector enables Swimlane Turbine users to automate asset discovery, vulnerability assessment, and reporting tasks within their security workflows. By integrating with Rapid7 InsightVM, users can streamline vulnerability management processes, enhance asset visibility, and expedite remediation efforts, all from within the Swimlane platform. The connector's actions facilitate real-time security analytics and proactive risk management, empowering users to maintain a robust security posture.

Prerequisites

To effectively utilize the Rapid7 Insight VM connector with Swimlane Turbine, ensure you have the following prerequisites:

- HTTP Basic Authentication with the following parameters:
  - URL: The base endpoint for the Rapid7 Insight VM API.
  - Username: Your Insight VM account username.
  - Password: Your Insight VM account password.

Capabilities

The Rapid7 InsightVM connector has the following capabilities:

- Get Scan Details
- Create Tag
- Get Tag
- Get Tags
- Create Report for Report Generation
- Report Download
- Report Generation
- Get Affected Assets

331. Reversinglabs A1000

341. SSP Deployer

The SSP Deployer connector facilitates the automated import, validation, and deployment of SSP configurations, enhancing the efficiency of security service management.

The SSP Deployer Connector bridges Swimlane Turbine with the SSP (Swimlane Solution Package) deployment process, enabling seamless import, status tracking, and deployment of SSP configurations. Users can validate SSPs through dry runs, track import statuses using unique tracking IDs, and upload SSPs to specified tenants with options for background processing and entity overwrites. This integration streamlines the management of solution packages, significantly reducing manual effort and enhancing operational efficiency within the Swimlane ecosystem.

This connector integrates with Swimlane Turbine to deploy SSP packages to tenants.

Asset Setup or Prerequisites

To effectively utilize the SSP Deployer connector, ensure you have the following prerequisites in place:

- Username and password authentication with the following parameters:
  - Hostname: The address of the server where SSP configurations are managed.
  - Username: The user account with permissions to access and manage SSP configurations.
  - Password: The corresponding password for the provided username.

Capabilities

This Connector provides the following capabilities:

- Import SSP
- Retrieve Status by Tracking ID
- Upload SSP

Notes

- To access Swimlane SSP Deploy API Documentation Link, **click here to check**

351. Securonix Snypr

SNYPR is a big data security analytics platform built on Hadoop that utilizes Securonix machine-learning-based anomaly detection techniques and threat models to detect sophisticated cyber and insider attacks.

Capabilities

This connector provides the following capabilities:

- Run Activity Query
- Get Top Threats
- Get Top Violations
- Get Top Violators
- List All Policies
- List All Users
- Retrieve List of Incidents

Note: To get "All Violations by Policy Name", use "Run Activity Query" action with the query:

```
index=violation AND policyname = <policyname> AND <additional conditions>
```

Asset Setup

This connector asset requires an URL, Username and a Password to authenticate.

Notes

- **API Documentation**

Additional Notes

- **BASE_URL** or **HOST_URL** must be in the format: **HOSTNAME_or_IPADDRESS/Snypr**
- While using the **Retrieve List of Incidents** action, please note that the parameter **tenantname** is optional for non-MSSP and is required to pass for MSSP and if needed, check here for documentation **Retrieve List of Incidents API Documentation**

361. Slack

Slack is a collaboration platform that facilitates team communication and integrates with various tools to streamline workflows.

Slack is a leading collaboration platform that facilitates team communication and collaboration through channels, direct messaging, and integrations. The Slack connector for Swimlane Turbine enables seamless integration with Slack's messaging and channel management capabilities, allowing security teams to automate communication workflows. By integrating Slack with Swimlane Turbine, users can enhance their security response by automating alerts, managing channels, and retrieving message histories, thereby improving collaboration and efficiency in incident response.

Prerequisites

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

- HTTP Bearer authentication using the following parameters:
  - URL: The endpoint URL for accessing Slack's API.
  - Token: A bearer token for authenticating API requests.
- API Key authentication using the following parameters:
  - URL: The endpoint URL for accessing Slack's API.
  - API Key: A key provided by Slack to authenticate API requests.

Capabilities

The Slack Connector has the following capabilities:

- Create, archive, and retrieve history of conversations
- Get Message Permalink
- Invite and remove users from a conversation
- Retrieve current users in a conversation
- Send broadcast messages
- Lookup by Email

371. Stellar SIEM

Stellar SIEM is a robust platform that provides advanced threat detection and security analytics to protect enterprise networks.

Stellar SIEM is a comprehensive security information and event management platform designed to enhance threat detection and response capabilities. By integrating with Swimlane Turbine, users can automate security incident management tasks such as case creation, alert retrieval, and Elasticsearch queries. This integration empowers security teams to streamline operations, improve incident response times, and gain deeper insights into security events, all without the need for extensive coding.

Limitations

The alerts endpoint returns at most **50 results** per request; use `skip` and `limit` for pagination (e.g. second page: `skip=10&limit=10`). The Execute Elasticsearch Job action may require custom code depending on query structure.

Supported Versions

This Stellar SIEM connector uses the Stellar Cyber public API (v1). Refer to **Stellar Cyber API documentation** for version-specific details.

Additional Docs

- **Stellar Cyber Swagger UI (API Reference)**
- **Configuring API Authentication**
- **Using the API to Retrieve Case Details**
- **Elasticsearch Query API**

Configuration

Prerequisites

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

381. Swimlane Utilities

Swimlane Utilities enhances the Swimlane platform with additional data processing and security analysis capabilities.

The Swimlane Utilities Connector is an essential toolkit designed to enhance the Swimlane Turbine platform's capabilities by providing a suite of utilities for security automation. It enables users to decrypt files, extract data from QR codes and barcodes, identify MIME types, generate hashes, parse Indicators of Compromise (IOCs), and perform DNS lookups. By integrating these utilities, end-users can streamline their security workflows, automate content analysis, and enhance threat intelligence operations without the need for coding expertise.

Capabilities

The Swimlane Util connector has the following capabilities:

- Decrypt Files
- IOC Parser: Parse IOCs from a Text Field or a List of IOC(s)
- Perform NSLookup
- Get Mime Type
- Hash Files and Strings
- Extract QR/Barcodes from HTML content

IOC Parse/Typer:

If you find edge case IOCs that you don't want the IOC Parser to return, add a `Whitelist Regex` input to exclude them.

Domains will only be found if they are in a URL or use a public suffix found **in this list**.

Actions

Decrypt File

391. Teamt5 Threatsonar Edr

The TeamT5 Threatsonar EDR connector facilitates seamless integration with TeamT5's endpoint detection and response system, enabling automated threat analysis and incident response.

TeamT5 Threatsonar EDR is a cutting-edge endpoint detection and response platform that provides comprehensive visibility into endpoint activities and potential threats. By integrating with Swimlane Turbine, users can automate the retrieval of endpoint data, manage isolation states, and access detailed incident and malware information. This connector empowers security teams to streamline their incident response workflows, enhance threat hunting capabilities, and maintain robust endpoint security posture without manual intervention. The actionable intelligence and automated response capabilities provided by this integration are crucial for maintaining a proactive defense against evolving cyber threats.

Prerequisites

To effectively utilize the TeamT5 Threatsonar EDR connector with Swimlane Turbine, ensure you have the following prerequisites:

- API Key Authentication with the following parameters:
  - URL: The base endpoint URL for the TeamT5 Threatsonar EDR API.
  - API Key: A valid API key provided by TeamT5 to authenticate requests.

Capabilities

This Connector provides the following capabilities:

- Data Retrieval Count
- Data Retrieval Deisolate
- Data Retrieval Endpoints List
- Data Retrieval Isolate
- Data Retrieval Show
- Endpoint Events Connections

401. ThreatQuotient ThreatQ

The ThreatQuotient ThreatQ connector facilitates the automation of threat intelligence operations by enabling seamless integration with the ThreatQ platform.

ThreatQuotient ThreatQ is a threat intelligence platform that aggregates, correlates, and analyzes threat data to provide actionable insights. This connector enables Swimlane Turbine users to automate the ingestion and management of threat intelligence, streamline event and indicator handling, and enhance security operations with enriched data. By integrating with ThreatQuotient ThreatQ, users can create and manage events, indicators, and import sessions, as well as perform detailed searches and updates, all within the Swimlane Turbine environment.

Prerequisites

Before integrating ThreatQuotient ThreatQ with Swimlane Turbine, ensure you have the following:

- OAuth 2.0 authentication credentials with the following parameters:
  - URL: The endpoint URL for ThreatQ API access
  - API User Email: The email associated with your ThreatQ account
  - Client Password: Your password for OAuth client authentication
  - OAuth Client ID: The client ID provided by ThreatQ for OAuth setup
  - API Type: The specific API type or version supported by ThreatQ

Capabilities

The ThreatQuotient Connector has the following capabilities:

- Create Event
- Create Indicators List
- Delete Import Indicator
- Get Event List
- Get Indicators List
- Get Indicator by ID

411. TruffleHog

TruffleHog searches through git repositories for secrets, digging deep into commit history and branches. This is effective at finding secrets accidentally committed.

TruffleHog is a cutting-edge secret detection tool that scans code repositories and other sources to identify exposed secrets like passwords, API keys, and tokens. The TruffleHog connector for Swimlane Turbine enables users to automate the process of detecting, listing, and managing secrets across multiple platforms. By integrating with TruffleHog, Swimlane Turbine users can enhance their security posture by proactively identifying and addressing potential secret leaks, streamlining the triage process, and ensuring sensitive information is securely managed within their environment.

Supported Version

- The TruffleHog connector supports the latest API version.

Limitations

None to date.

Asset Setup

TruffleHog API allows clients to manage sources and secrets. API requests require X-Thog-Key and X-Thog-Secret headers which can be generated at the your-instance.trufflehog.org/api-keys

Prerequisites

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

- TruffleHog API authentication:
    - URL: The endpoint URL for the TruffleHog API.
    - API Key: Your personal API key to authenticate requests.
    - App ID: The application identifier for your TruffleHog instance.

421. Velociraptor Dfir

The Velociraptor DFIR connector enables automated forensic data collection and incident response actions within the Swimlane Turbine platform.

Velociraptor DFIR is a powerful digital forensics and incident response (DFIR) tool that provides detailed endpoint visibility and facilitates in-depth investigations. This connector allows Swimlane Turbine users to integrate Velociraptor's capabilities directly into their security workflows, enabling automated labeling, quarantining, and retrieval of client data. By leveraging this integration, security teams can execute custom queries, manage client statuses, and analyze forensic artifacts, thereby enhancing their incident response efficiency and reducing time to resolution.

Prerequisites

Before integrating Velociraptor DFIR with Swimlane Turbine, ensure you have the following:

- API Config File authentication with these parameters:
  - URL: The endpoint URL for the Velociraptor DFIR server.
  - API Config Base64: A base64-encoded string containing the API configuration details for secure communication with the Velociraptor server.

Capabilities

This Connector provides the following capabilities:

- Add Client Label
- Add Client Quarantine
- Get Client Flow Results
- Get Client Flows
- Get Client ID
- Get Client Label
- Get Hunt Flows
- Get Hunt Results
- Remove Client Label

431. Wait Timer

A connector that waits for N seconds before exiting. Returns all the inputs as outputs.
Be aware that the connector will wait for the specified number of seconds once the action is executed. There might be a
delay between the time the action is called and the time the action is executed while the container gets spun up.

Actions

Wait N seconds

This script will wait N seconds then pass the inputs straight to the outputs

Endpoint

- **Method:** `GET`

Input

Argument Name	Type	Required	Description
`seconds`	number	Optional	Parameter for Wait N seconds
`input_var_1`	string	Optional	Input data for the action
`input_var_2`	string	Optional	Input data for the action

Input Example

```
{"seconds":3,"input_var_1":"hello","input_var_2":"howdy"}
```

Output

Parameter	Type	Description
`input_var_1`	string	Input data for the action
`input_var_2`	string	Input data for the action

441. Xmatters

The xMatters connector enables automated interactions with the xMatters platform, facilitating incident management and communication processes.

xMatters is a digital service reliability platform that enables IT, DevOps, and MIM (Major Incident Management) teams to automate and orchestrate tasks across their operations. The xMatters Turbine Connector allows Swimlane Turbine users to integrate with xMatters, enabling automated incident response, device management, and event handling. By leveraging this connector, users can streamline their security operations, reduce response times, and ensure consistent execution of incident management procedures.

Limitations

None to date.

Supported Versions

This xMatters connector uses the Version 1 API.

Configuration

Prerequisites

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

- HTTP Basic Authentication with these parameters:
  - URL: The endpoint URL for the xMatters API.
  - Username: Your xMatters account username.
  - Password: Your xMatters account password.
- OAuth2 Password Credentials with these parameters:
  - URL: The endpoint URL for the xMatters API.
  - Username: Your xMatters account username.
  - Password: Your xMatters account password.