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

11. Adlumin

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

41. Armis Centrix

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

71. Cherwell Service Management Rest

101. CrowdStrike Logscale

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

131. Duo Security

141. Exabeam Aa V2

151. Fireeye

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

191. Hero AI

201. Illumio Core Protection

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

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

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

241. Microsoft Azure DevOps

251. Microsoft Exchange

261. Microsoft Intune

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

301. Palo Alto Networks Pan-OS

311. Pixis

321. Rapid7 Insight VM

331. Reversinglabs A1000

341. SSP Deployer

351. Securonix Snypr

361. Slack

371. Stellar SIEM

Stellar SIEM is a security information and event management solution that provides real-time threat detection and response capabilities.

Stellar SIEM is a comprehensive security information and event management platform designed to enhance threat detection and incident response. By integrating with Swimlane Turbine, users can automate case management, streamline alert handling, and perform advanced data queries without writing code. This integration empowers security teams to efficiently manage incidents, enrich threat intelligence, and improve overall security posture through seamless automation and actionable insights.

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

391. Teamt5 Threatsonar Edr

401. ThreatQuotient ThreatQ

411. TruffleHog

421. Velociraptor Dfir

431. Wait Timer

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.

Additional Docs

- **xMatters Authentication Link**
- **xMatters Roles and Permissions Link**
- **xMatters API Documentation Link**

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