



ANY.RUN's Interactive Sandbox & TI Lookup

Integration with SentinelOne

Configuration guide

Table of Contents

Interactive Sandbox	3
How to Integrate Interactive Sandbox with SentinelOne	3-9
Installation and configuration	3-4
Using ANY.RUN Templates	5-8
Using the Actions Tab	8-9
Threat Intelligence Lookup (TI Lookup)	10
How to Integrate TI Lookup with SentinelOne	10-15
Installation and configuration	10-11
Using ANY.RUN Templates	12-15
Using the Actions Tab	15

Interactive Sandbox

Interactive Sandbox helps SOC teams and MSSPs investigate suspicious files, URLs, phishing pages, and malware while observing attack behavior in real time.

Analysts get in-depth visibility into processes, network activity, browser behavior, persistence, credential access, and other malicious activity, helping them understand the full attack scope and reach faster, more confident verdicts.

The sandbox supports Windows, Linux, macOS, and Android environments and combines automated analysis with interactive investigation, allowing analysts to examine threats without maintaining dedicated analysis infrastructure.

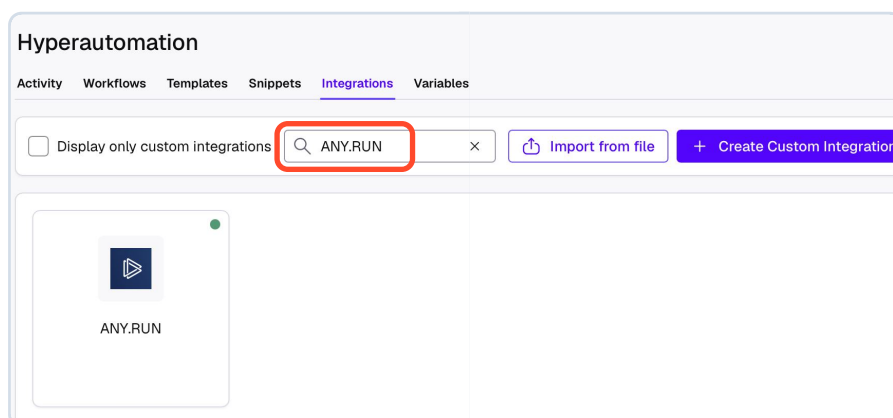
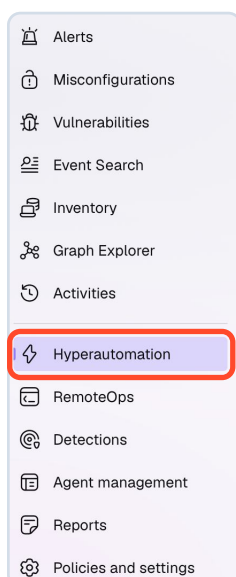
- **Full attack visibility:** See how threats behave in real time, including process execution, network connections, dropped files, registry changes, browser activity, and other attack behavior.
- **Faster investigations:** Automated detection and behavioral analysis surface malicious activity and IOCs, reducing manual work during triage and investigation.
- **Interactive analysis:** Interact with the environment during analysis to trigger hidden behavior, follow attack chains, and investigate threats beyond automated execution.

Interactive Sandbox can be integrated into existing security workflows using API and SDK. For more details, feel free to [contact us](#).

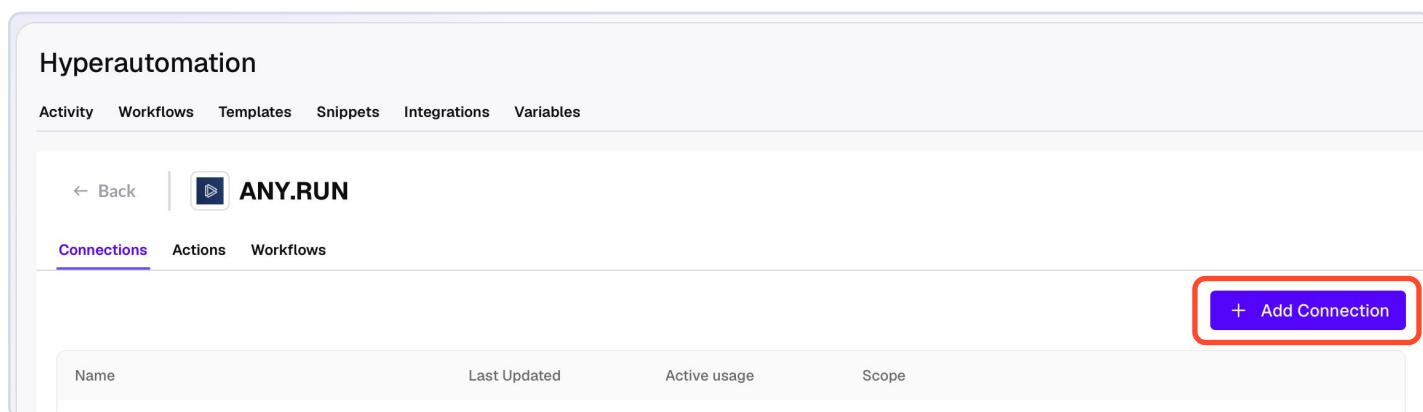
How to Integrate Interactive Sandbox with SentinelOne

INSTALLATION AND CONFIGURATION

1. Go to the **Hyperautomation** section in SentinelOne.
2. Open the **Integration** tab, enter **ANY.RUN** in the search bar, and select the integration.



3. Click **Add Connection**.



4. Enter your **API key**. The other fields are prefilled.

The 'Create Connection' form is shown with the following fields and values:

- Global /** ANY.RUN - NFR **/** Select site
- Connection Name:** ANY.RUN connection
- Integration:** ANY.RUN
- Network:**
 - Protocol:** https
 - Host / Base URL:** api.any.run
 - Port:** 443
- Authentication:**
 - Type:** API key
 - API Key:** Enter API key... (highlighted with a red box)
 - Way to pass:** Header
 - Header Key Name:** Authorization
 - Header Value Prefix (optional):** API-Key

Buttons: Cancel, Create Connection

5. Click **Create Connection** to complete the setup.

USING ANY.RUN TEMPLATES

1. To use ready-made ANY.RUN workflows, go to the **Templates** tab and enter **ANY.RUN** in the search bar.

The screenshot shows the 'Hyperautomation' interface with the 'Templates' tab selected. A search bar at the top contains the text 'Name contains ANY.RUN'. Below the search bar, there are three workflow templates displayed in a grid. Each template has a title, a description, a set of icons representing the workflow steps, and a 'View' button.

- Enrich Alert with ANY.RUN TI Lookup**: Singularity Response Trigger. This workflow allows enriching entities from a SentinelOne alert using the ANY.RUN TI Lookup database, which helps understand the context and threat level of the indicator.
- Submit a file from Alert to ANY.RUN Sa...**: Singularity Response Trigger. This workflow is used for automatically submitting malicious files from your alert to ANY.RUN Sandbox to obtain analysis results and make more efficient and faster decisions.
- Submit a URL from Alert to ANY.RUN S...**: Singularity Response Trigger. This workflow is used for automatically submitting a URL from your alert to ANY.RUN Sandbox to obtain analysis results and make more efficient and faster decisions.

2. Choose one of the available ANY.RUN templates:

Submit a file from Alert to ANY.RUN Sandbox
automatically submits files from alerts to the sandbox.

Submit a URL from Alert to ANY.RUN Sandbox
automatically submits URLs from alerts to the sandbox.

Note: By default, these templates are designed for automated workflows. You can also configure a workflow to run on demand and launch it manually for individual alerts.

3. Click **View** on the template you'd like to use.

This block shows three workflow templates in detail, each with a 'View' button highlighted. The templates are:

- Enrich Alert with ANY.RUN TI Lookup**: Singularity Response Trigger. This workflow allows enriching entities from a SentinelOne alert using the ANY.RUN TI Lookup database, which helps understand the context and threat level of the indicator.
- Submit a file from Alert to ANY.RUN Sa...**: Singularity Response Trigger. This workflow is used for automatically submitting malicious files from your alert to ANY.RUN Sandbox to obtain analysis results and make more efficient and faster decisions.
- Submit a URL from Alert to ANY.RUN S...**: Singularity Response Trigger. This workflow is used for automatically submitting a URL from your alert to ANY.RUN Sandbox to obtain analysis results and make more efficient and faster decisions.

4. Click [Use this template](#)

Submit a URL from Alert to ANY.RUN Sandbox

Use this template

This workflow is used for automatically submitting a URL from your alert to ANY.RUN Sandbox to obtain analysis results and make more efficient and faster decisions.

Steps in this template

5. Name the workflow and click [Create](#)

Create Workflow

Creates a new workflow using "Submit a URL from Alert to ANY.RUN Sandbox" as a template.

Scope Account Site

Global / ANY.RUN - NFR / Select site

Workflow Name

Submit a URL to ANY.RUN Sandbox

Cancel [Create](#)

6. Configure the template trigger. It's the event that will start the automated workflow.

ANY.RUN - NFR Submit a URL to ANY.RUN Sandbox Private Draft

Share with team [Activate](#)

Singularity Response Trigger

Singularity Response Trigger

Test Action Test Downstream Manual Output

Test Results Not Tested

Add Event Filter

Alert Run Automatically Enabled

Severity High

+ Add Condition

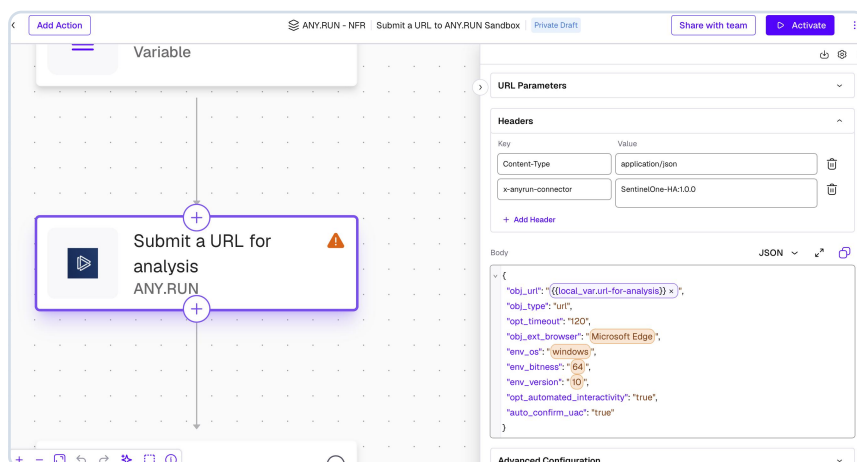
For the **Submit a URL from Alert to ANY.RUN Sandbox** template:
Specify the alert field containing the URL in the **Value** field.

The screenshot shows a workflow editor interface. On the left, a 'Singularity Response Trigger' block is connected to a 'URL for analysis Variable' block. The variable block has a warning icon. On the right, a configuration panel for the 'URL for analysis' variable is open. It includes a 'Name' field with the value 'url-for-analysis' and a 'Value' field with the value '[1,2,3]'. A red error message 'Required' is displayed below the value field. The panel also has buttons for 'Save As Custom Action', 'Test Action', 'Test Downstream', and 'Add Variable'.

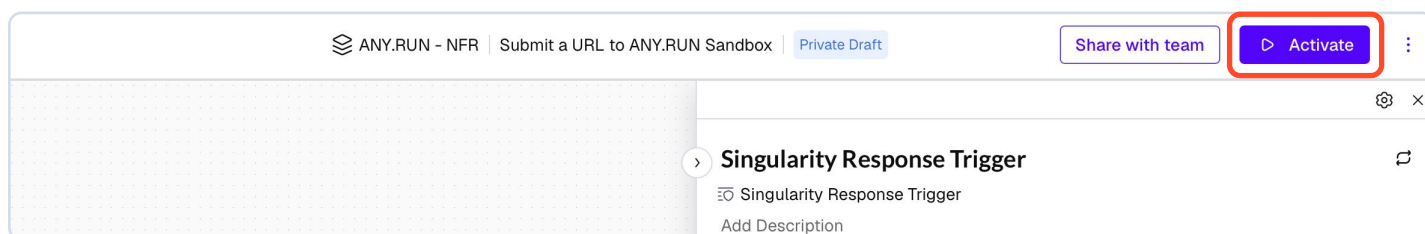
For the **Submit a file from Alert to ANY.RUN Sandbox** template:
Create a password and enter it in the Value field.

The screenshot shows a workflow editor interface. On the left, a 'Singularity Response Trigger' block is connected to a 'Set a password for the fetched file Variable' block. On the right, a configuration panel for the 'Set a password for the fetched file' variable is open. It includes a 'Name' field with the value 'file-password' and a 'Value' field with the value 'password'. The panel also has buttons for 'Save As Custom Action', 'Test Action', 'Test Downstream', and 'Add Variable'.

7. If needed, configure the analysis parameters. See the [ANY.RUN API documentation](#) for all available options.



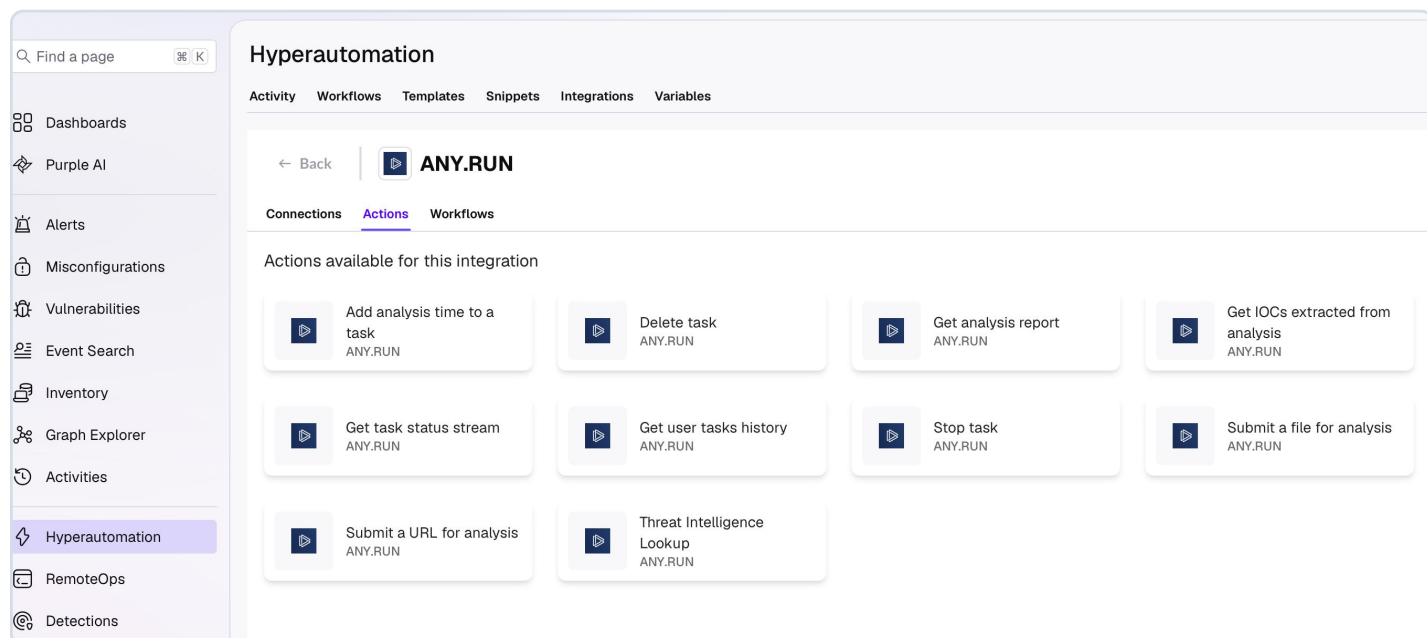
8. Click **Activate** to complete the setup.



✓ Your automated workflow is ready for use.

USING THE ACTIONS TAB

Templates are the primary way to automate workflows with the ANY.RUN integration. You can also use individual actions available in the **Actions** tab of the integration.



Available options:

Add analysis time to a task

Adds 60 seconds to the task runtime by the task ID if the task has not been completed yet.

Delete task

Deletes a task in ANY.RUN if the user making the request has permission to do so.

Get analysis report

Returns analysis report for a submission by its task ID.

Get IOCs extracted from analysis

Returns IOCs extracted from analysis by its task ID.

Get task status stream

Returns task status information by the task UUID.

Get user tasks history

Returns up to 100 last tasks from the user's history and their basic information.

Stop task

Stops task by task ID if the task has not been completed yet.

Submit a file for analysis

Submits a file with the specified analysis environment configuration and returns the task ID of the newly created analysis. [Learn more about analysis capabilities.](#)

Submit a URL for analysis

Submits a URL with the specified analysis environment configuration and returns the task ID of the newly created analysis. [Learn more about analysis capabilities.](#)

If you have any questions,
contact us via [this form](#) or write to techsupport@any.run

Threat Intelligence Lookup (TI Lookup)

Threat Intelligence Lookup turns data from real-world sandbox investigations across 16K+ SOC teams into actionable threat context for enrichment, detection, threat hunting, and incident response.

Analysts can go from a single IP, domain, URL, or hash to related infrastructure, malware activity, sandbox analyses, and other threat context in seconds. Flexible search, including natural-language queries, also lets teams investigate threats by geography, industry, behavior, and other characteristics.

This helps analysts move beyond isolated IOC verdicts to understand relationships between indicators, uncover related activity, and investigate threats using fresh intelligence from real-world attacks.

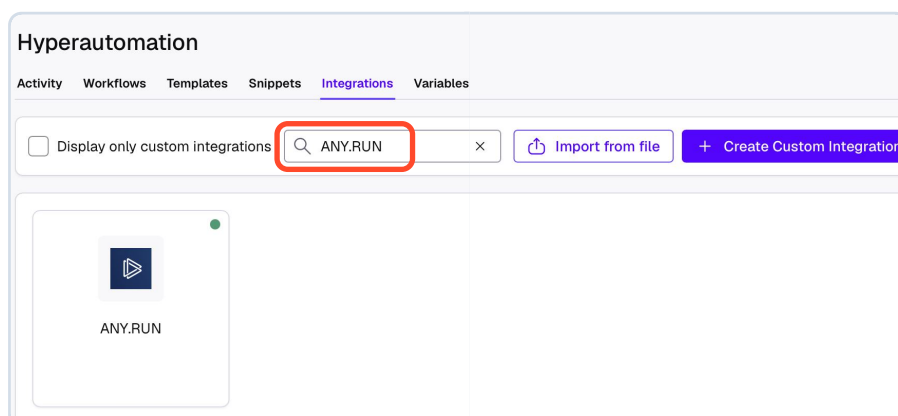
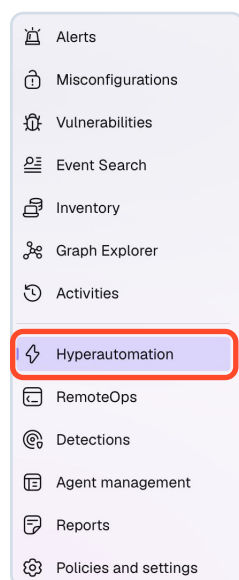
- **Deep threat context:** Pivot from individual indicators to related infrastructure, malware, IOCs, sandbox analyses, TTPs, and other evidence.
- **Flexible threat search:** Search by IP, URL, domain, or hash, or use natural-language and advanced queries to investigate specific behaviors, geographies, industries, and threat patterns.
- **Faster investigations and hunting:** Enrich alerts, validate suspicious indicators, uncover related threats, and identify relevant activity without manually checking multiple intelligence sources.

Threat Intelligence Lookup is available through the web interface and API for integration into existing security workflows. For more details, feel free to [contact us](#).

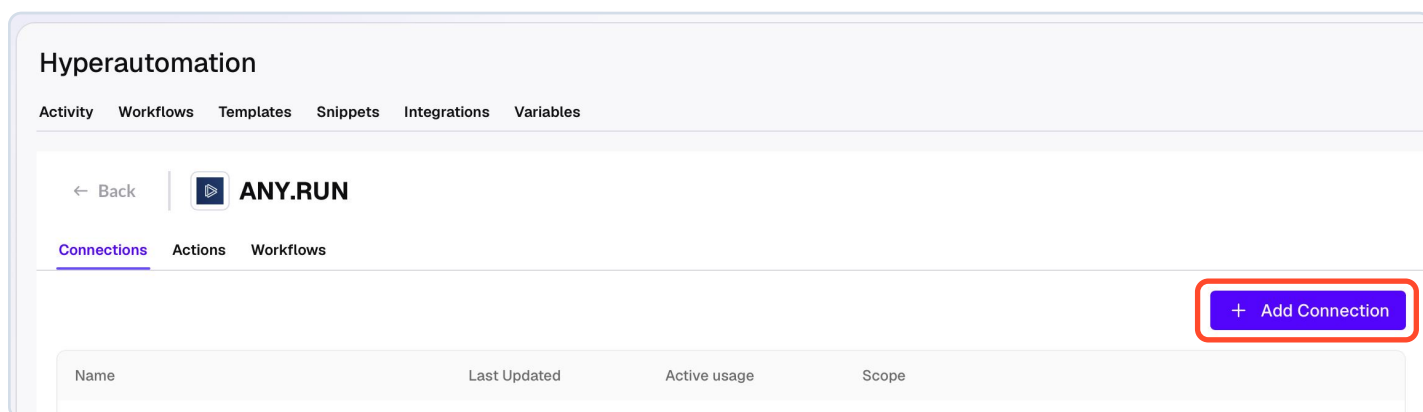
How to Integrate TI Lookup with SentinelOne

INSTALLATION AND CONFIGURATION

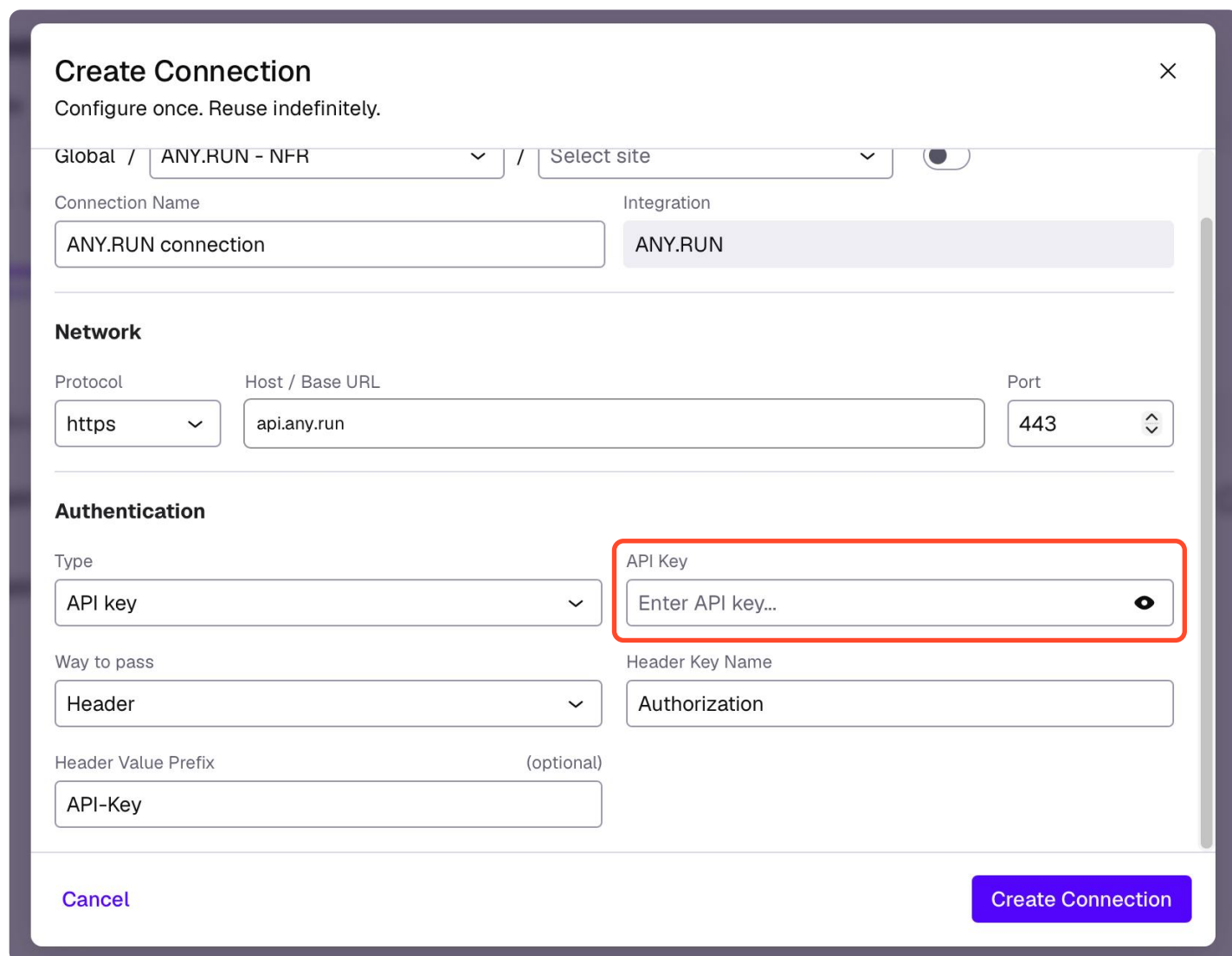
1. Go to the **Hyperautomation** section in SentinelOne.
2. Open the **Integration** tab, enter **ANY.RUN** in the search bar, and select the integration.



3. Click **Add Connection**.



4. Enter your **API key**. The other fields are prefilled.



The 'Create Connection' form is shown with the following fields and values:

- Global /** ANY.RUN - NFR **/** Select site
- Connection Name:** ANY.RUN connection
- Integration:** ANY.RUN
- Network:**
 - Protocol:** https
 - Host / Base URL:** api.any.run
 - Port:** 443
- Authentication:**
 - Type:** API key
 - API Key:** Enter API key... (highlighted with a red box)
 - Way to pass:** Header
 - Header Key Name:** Authorization
 - Header Value Prefix (optional):** API-Key

Buttons: Cancel, Create Connection

5. Click **Create Connection** to complete the setup.

USING ANY.RUN TEMPLATES

1. To use ready-made ANY.RUN workflows, go to the **Templates** tab and enter **ANY.RUN** in the search bar.

The screenshot shows the 'Hyperautomation' dashboard with the 'Templates' tab selected. A search bar at the top contains the text 'Name contains ANY.RUN'. Below the search bar, three workflow templates are displayed:

- Enrich Alert with ANY.RUN TI Lookup**: Singularity Response Trigger. Description: This workflow allows enriching entities from a SentinelOne alert using the ANY.RUN TI Lookup database, which helps understand the context and threat level of the indicator.
- Submit a file from Alert to ANY.RUN Sa...**: Singularity Response Trigger. Description: This workflow is used for automatically submitting malicious files from your alert to ANY.RUN Sandbox to obtain analysis results and make more efficient and faster decisions.
- Submit a URL from Alert to ANY.RUN S...**: Singularity Response Trigger. Description: This workflow is used for automatically submitting a URL from your alert to ANY.RUN Sandbox to obtain analysis results and make more efficient and faster decisions.

2. Click **View** in the ANY.RUN TI Lookup template:

The screenshot shows the same three workflow templates as before. The first template, 'Enrich Alert with ANY.RUN TI Lookup', is highlighted with a red rectangular box. The 'View' button for this template is visible at the bottom right of its card.

Note: By default, these templates are designed for automated workflows. You can also configure a workflow to run on demand and launch it manually for individual alerts.

3. Click [Use this template](#)

Enrich Alert with ANY.RUN TI Lookup

```

graph TD
    A[Singularity Response Trigger] --> B[Set hash Variable]
    B --> C[Hash is unknown Condition]
    C -- False --> A
    C -- True --> D[ ]
            
```

This workflow allows enriching entities from a SentinelOne alert using the ANY.RUN TI Lookup database, which helps understand the context and threat level of the indicator.

Steps in this template

4. Name the workflow and click [Create](#)

Create Workflow

Creates a new workflow using "Enrich Alert with ANY.RUN TI Lookup" as a template.

Scope Account Site

Global / ANY.RUN - NFR / Select site

Workflow Name

Enrich with ANY.RUN TI Lookup

Cancel [Create](#)

5. Configure the template trigger. It's the event that will start the automated workflow.

ANY.RUN - NFR | Enrich with ANY.RUN TI Lookup | Private Draft

[Share with team](#) [Activate](#)

Singularity Response Trigger

Singularity Response Trigger

Add Description

Test Action Test Downstream Manual Output

Test Results Not Tested

Add Event Filter

Alert Run Automatically Enabled

Severity =

High x

+ Add Condition

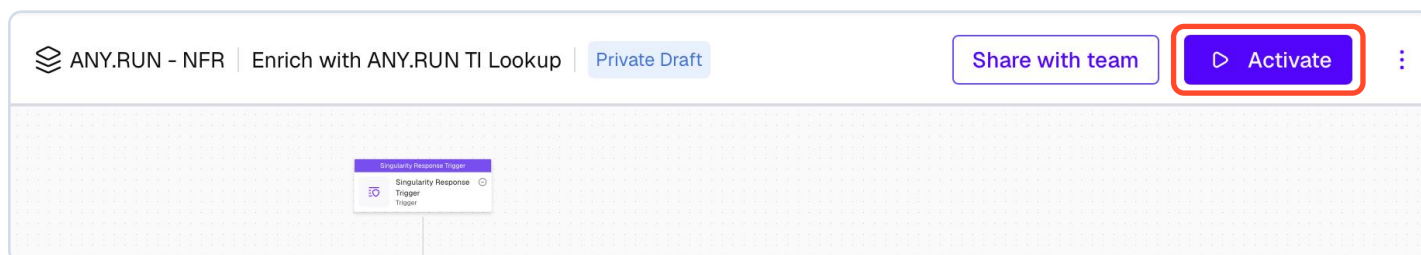
6. By default, the workflow is designed to process hashes. If needed, you can configure it to process IPs, URLs, or domains instead.

The screenshot displays a workflow editor interface. The main workspace shows a sequence of actions: 'Singularity Response Trigger' followed by 'Set hash Variable'. The 'Set hash Variable' action is highlighted with a purple border. To the right, a configuration panel for the 'Set hash' action is open. It includes a 'Variable' field set to 'hash' and a 'Value' field containing the expression: `{{Function.DEFAULT(Function.DEFAULT(singularity-response-trigger.data.process.file`. Below the configuration panel, there are buttons for 'Test Action' and 'Test Downstream', and a 'Test Results' section showing 'Not Tested'.

7. If needed, configure the analysis parameters. See the [ANY.RUN API documentation](#) for all available options.

The screenshot shows a workflow editor with a 'Threat Intelligence Lookup ANY.RUN' action highlighted. The workflow includes a 'Hash is unknown Condition' that branches into 'False' and 'True' paths. The 'False' path leads to the 'Threat Intelligence Lookup ANY.RUN' action, which then leads to a 'Hash found in ANYRUN TI Data Condition'. The 'True' path leads to a 'No hash Variable' action. To the right, a configuration panel for the 'Threat Intelligence Lookup ANY.RUN' action is open. It shows the 'URL' field set to `https://api.anyrun.com/v1/intelligence/api/search`, the 'Method' set to 'POST', and the 'Headers' section with 'Content-Type' set to 'application/json' and 'x-anyrun-connector' set to 'SentinelOne-HA:1.0.0'. The 'Body' section is set to 'JSON' and contains the query: `"query": "{{local_var.hash}} x"`.

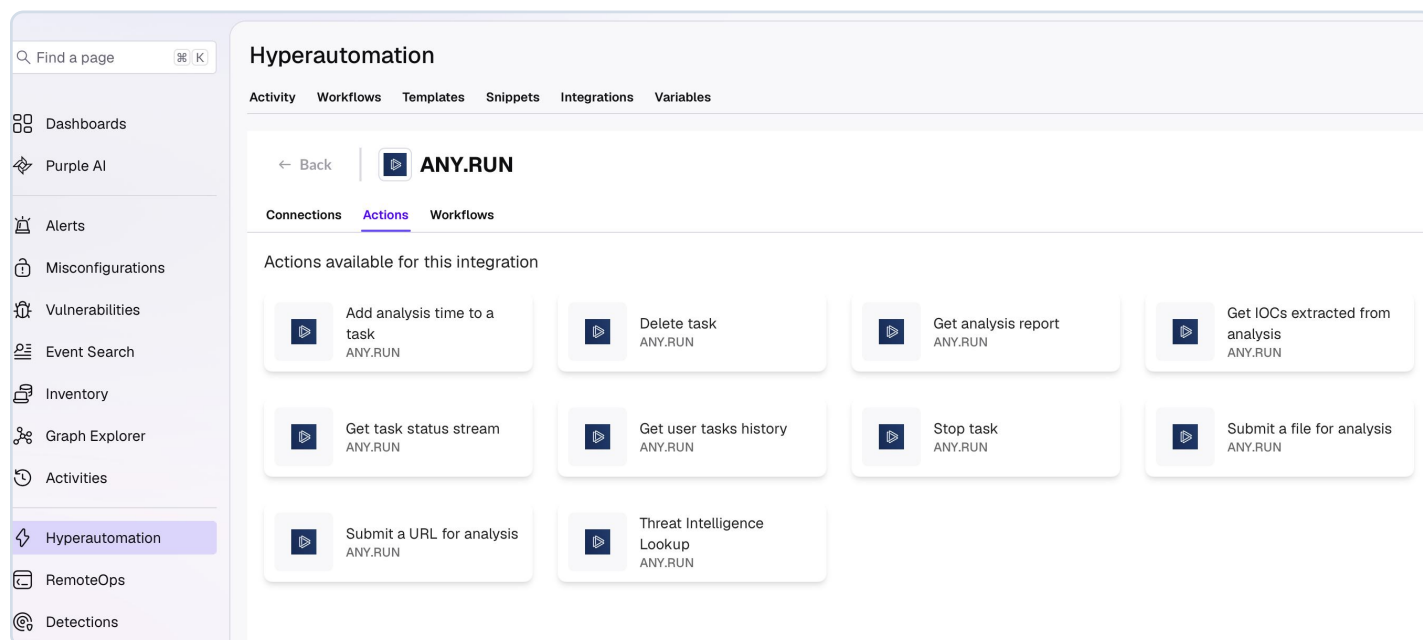
8. Click **Activate** to complete the setup.



✓ Your automated workflow is ready for use.

USING THE ACTIONS TAB

Templates are the primary way to automate workflows with the ANY.RUN integration. You can also use individual actions available in the **Actions** tab of the integration.



For TI Lookup, the available option is:

Threat Intelligence Lookup

Retrieves threat intelligence data from ANY.RUN. Search by IP address, URL, domain, or hash, or create a custom query such as MITRE:"T1001".

[Learn more about the ANY.RUN TI API.](#)

If you have any questions,
contact us via [this form](#) or write to techsupport@any.run