ANY.RUN's Interactive Sandbox & TI Lookup

Integration with SentinelOne

Configuration guide

Table of Contents

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.

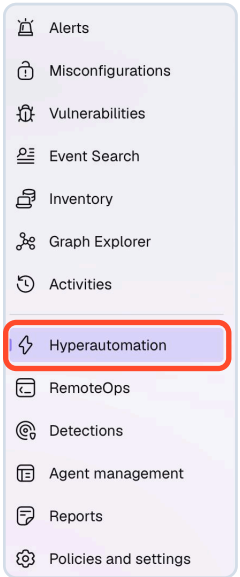
- **Full attack visibility:** See how threats behave in real time, including process execution, network connections, dropped files, registry changes, browser activity, and other attack behavior.
- **Faster investigations:** Automated detection and behavioral analysis surface malicious activity and IOCs, 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**.

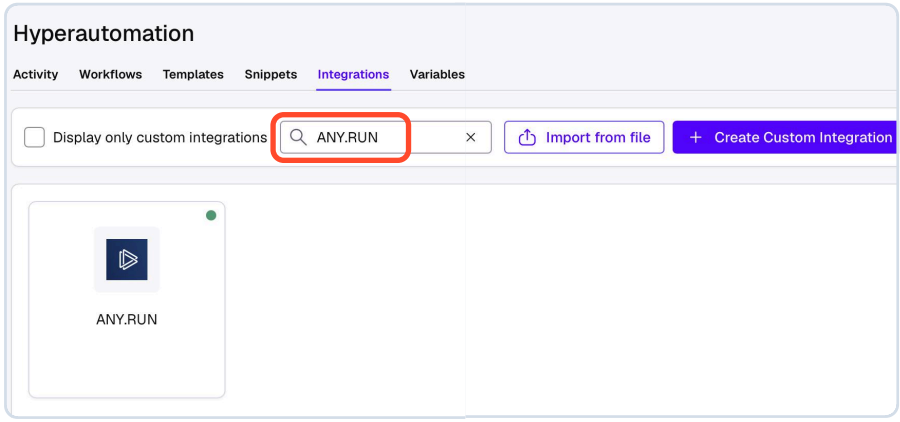
How to Integrate Interactive Sandbox with SentinelOne

INSTALLATION AND CONFIGURATION

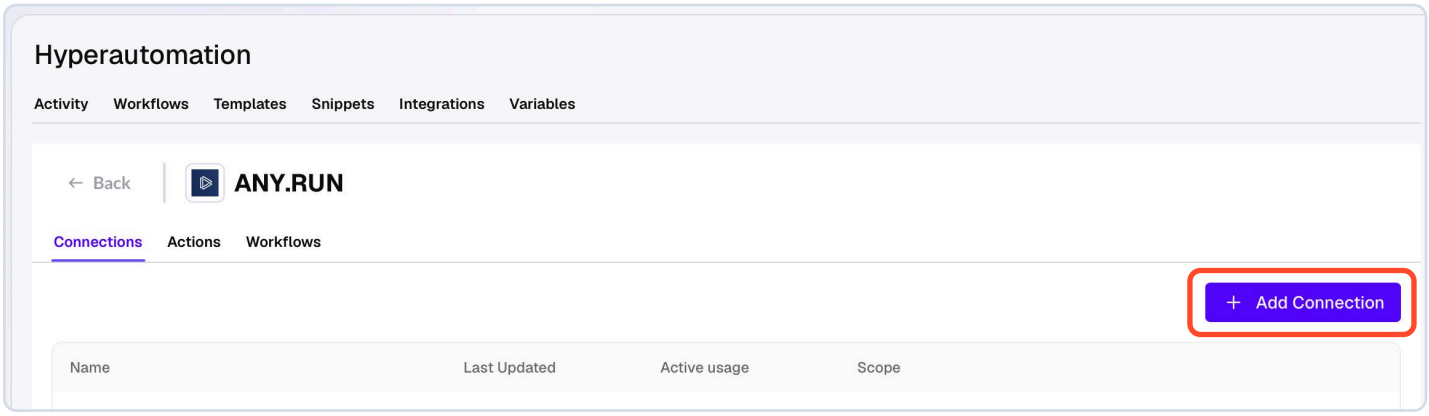
1. Go to the **Hyperautomation** section in SentinelOne.



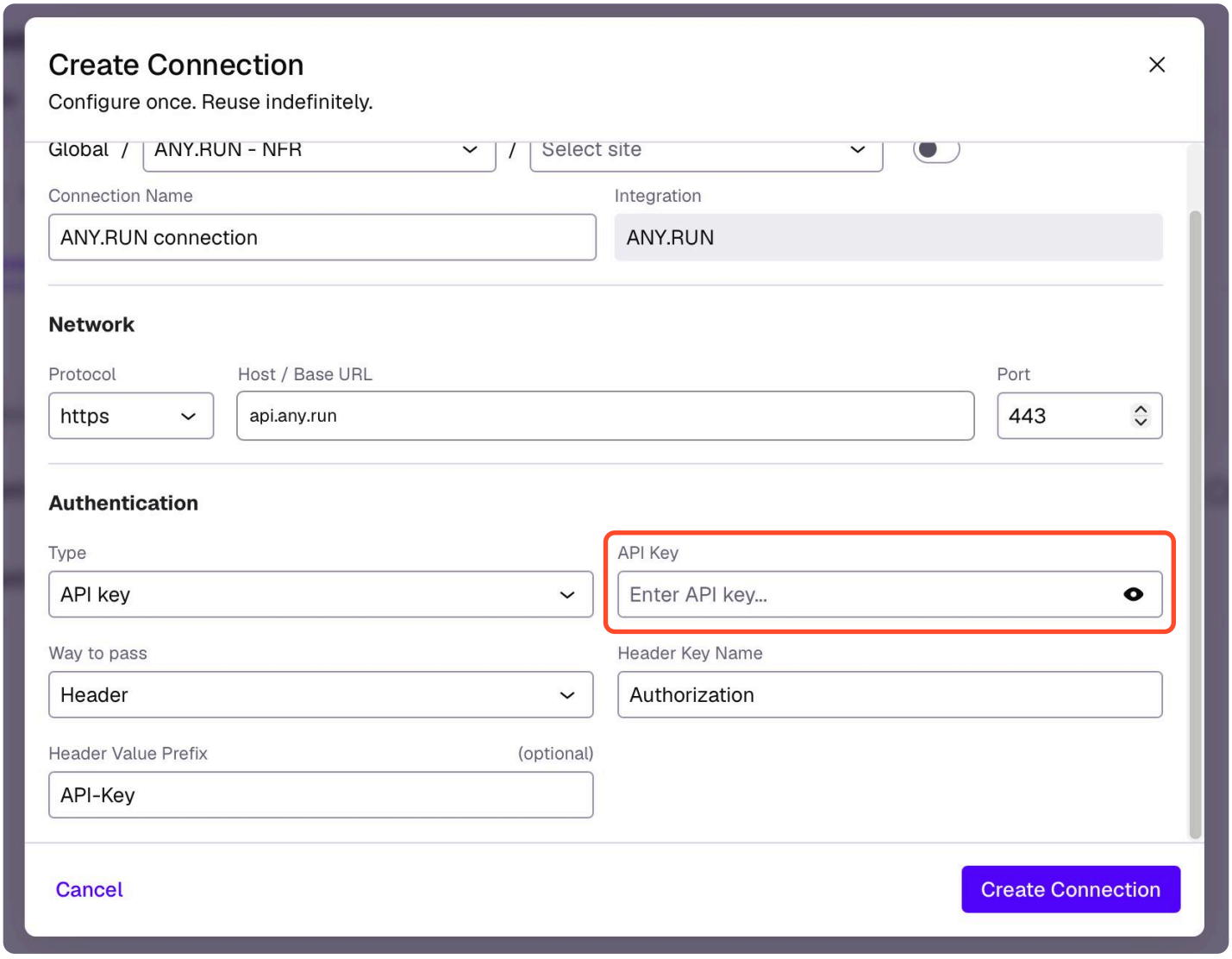
2. Open the **Integration** tab, enter **ANY.RUN** in the search bar, and select the integration.



3. Click **Add Connection**.



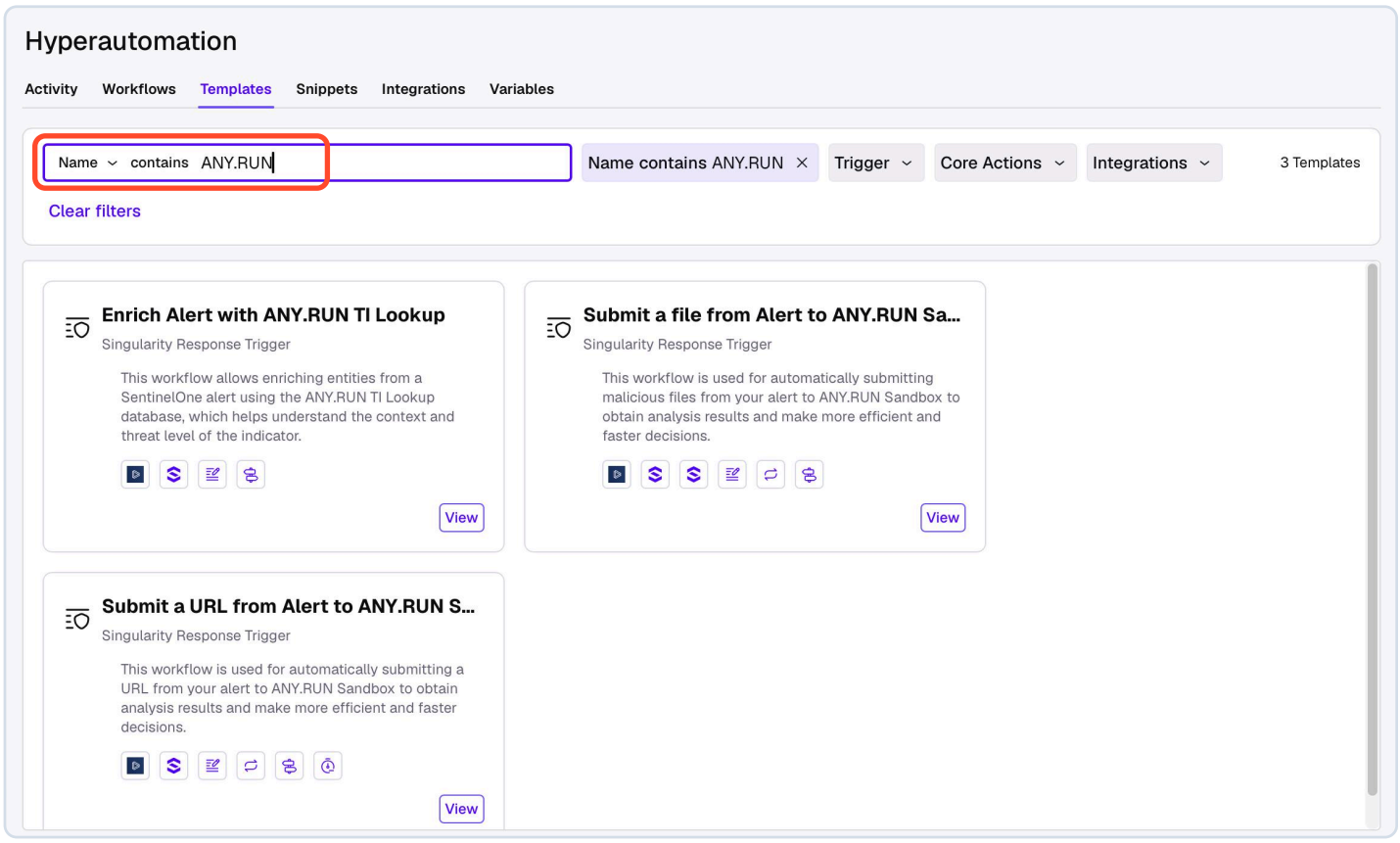
4. Enter your **API key**. The other fields are prefilled.



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.



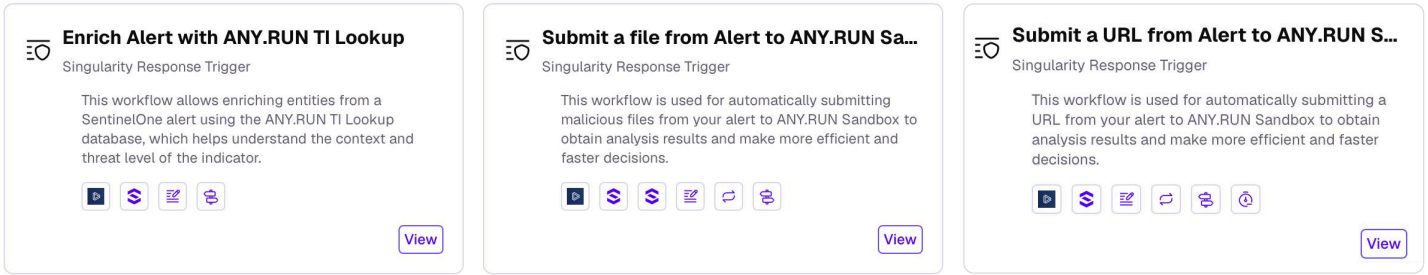
2. Choose one of the available ANY.RUN templates:

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

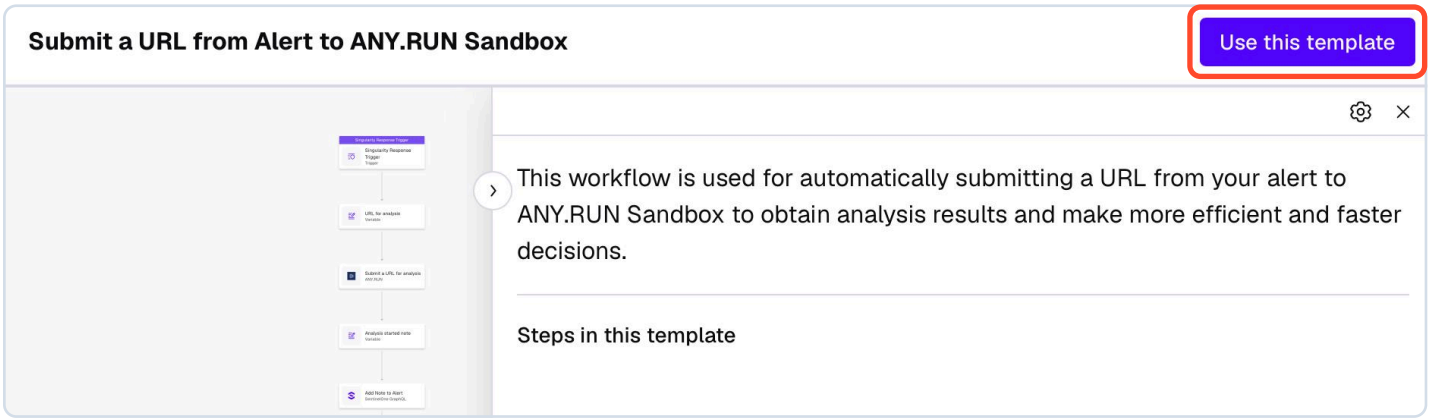
Submit a URL from Alert to ANY.RUN Sandbox automatically submits URLs from alerts to the sandbox.

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.

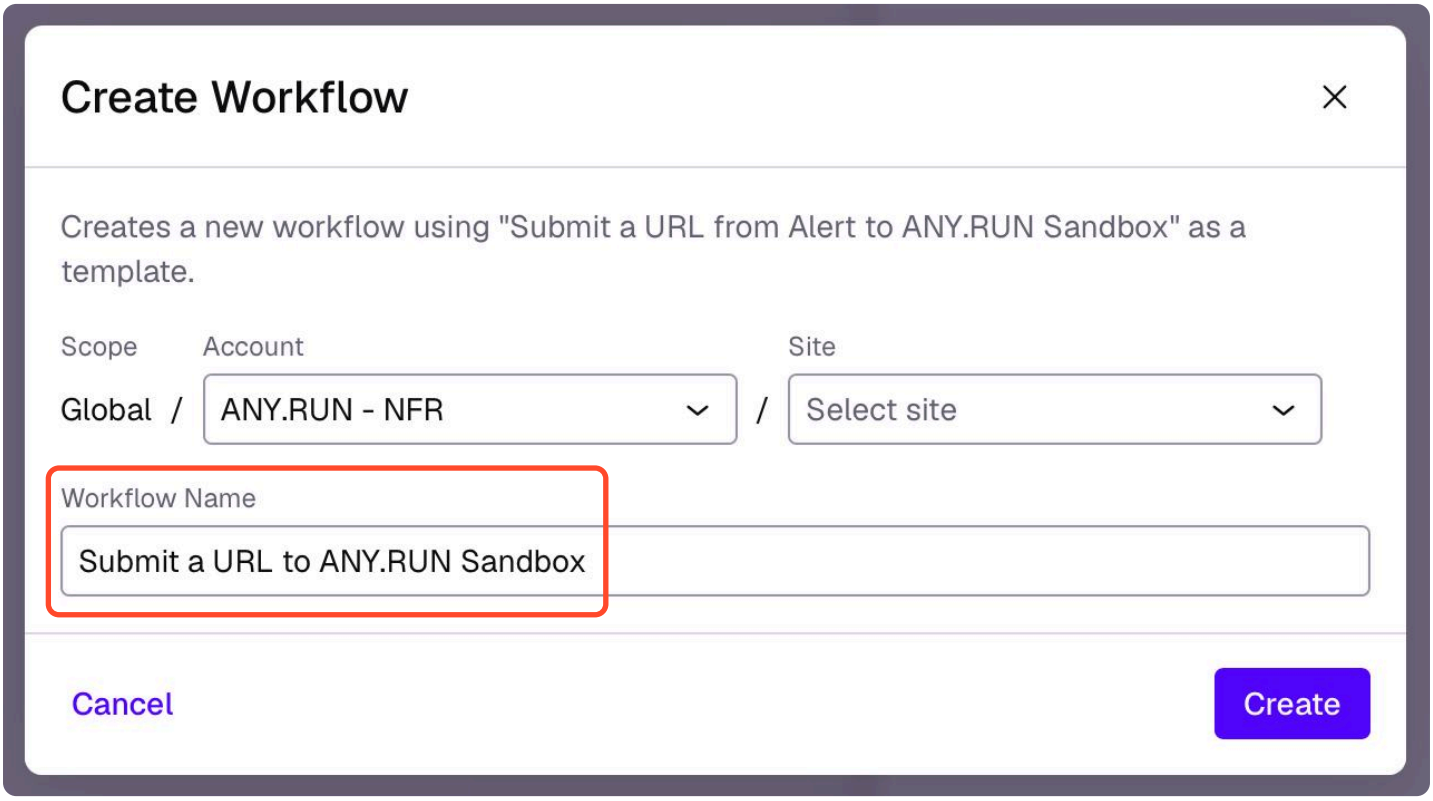
3. Click View on the template you'd like to use.



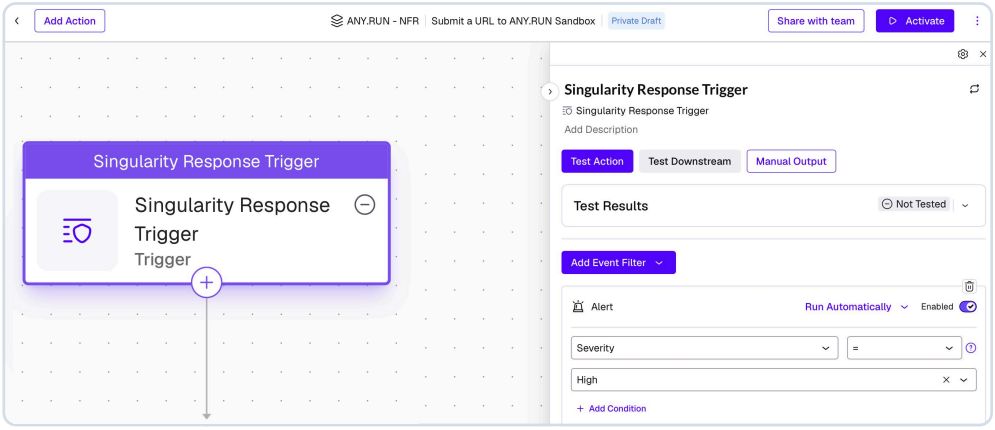
4. Click **Use this template**



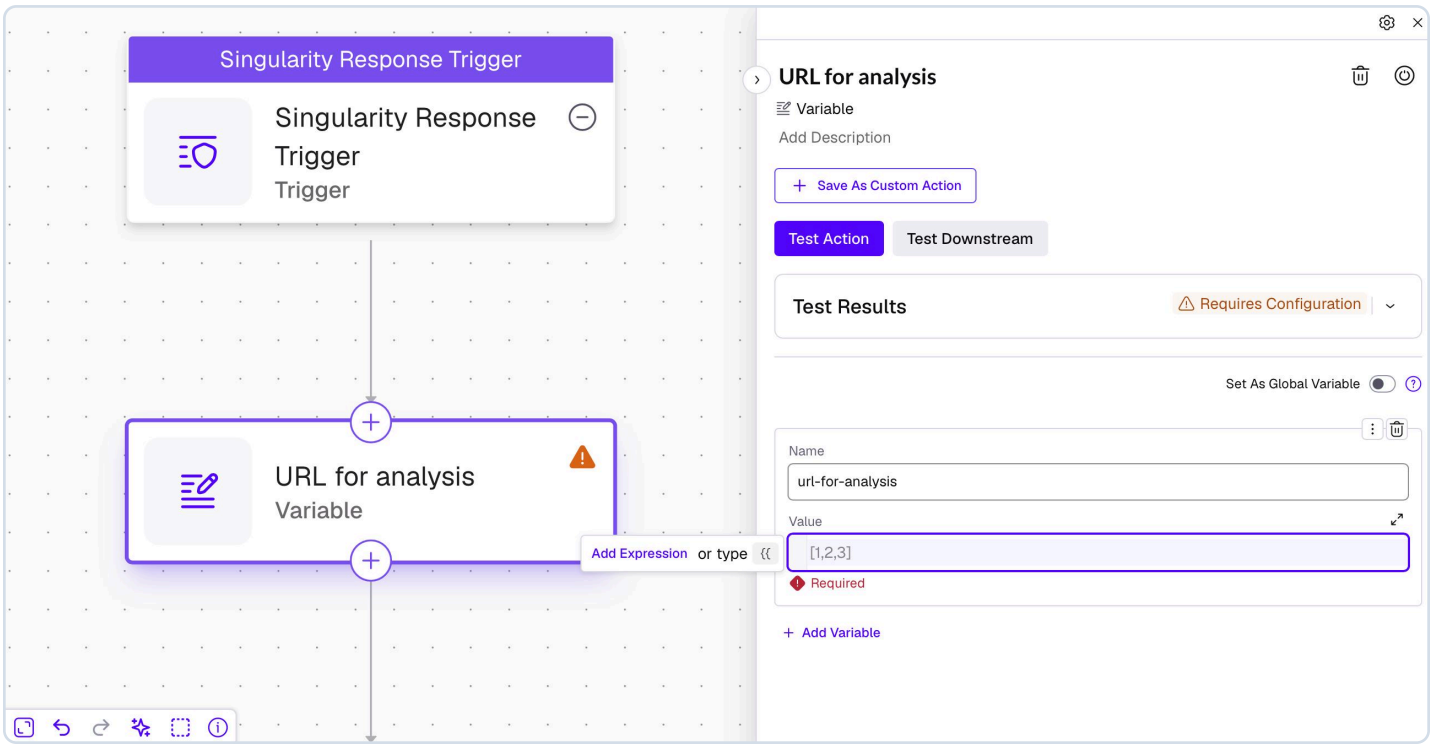
5. Name the workflow and click **Create**



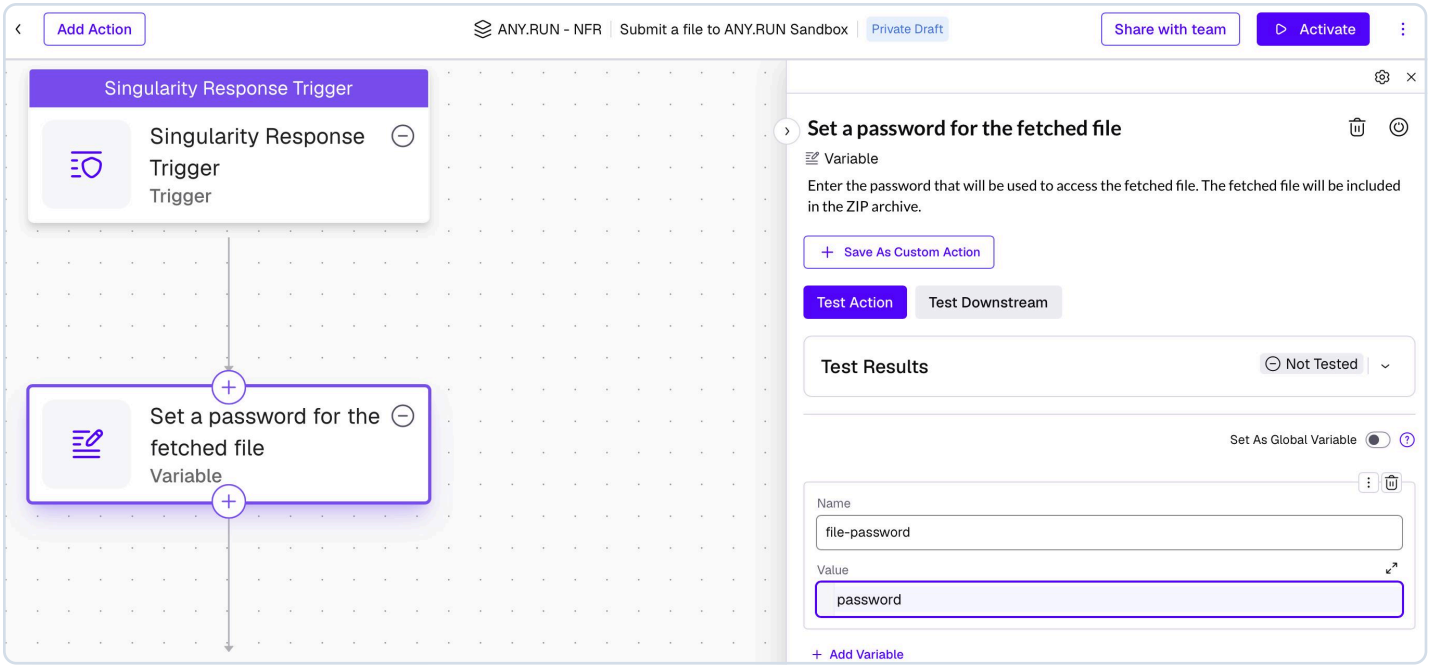
6. Configure the template trigger. It's the event that will start the automated workflow.



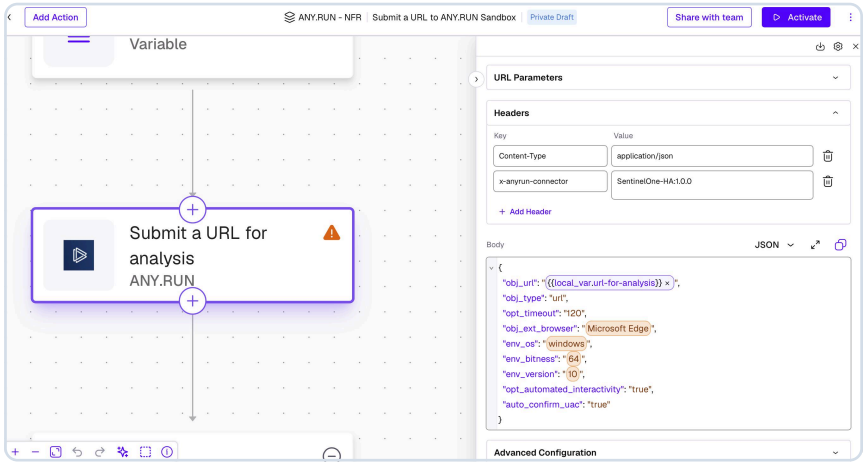
For the **Submit a URL from Alert to ANY.RUN Sandbox** template:
Specify the alert field containing the URL in the **Value** field.



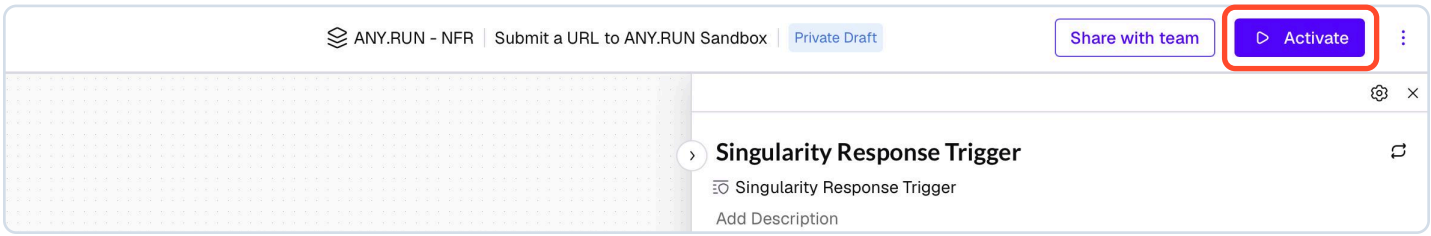
For the **Submit a file from Alert to ANY.RUN Sandbox** template:
Create a password and enter it in the Value field.



7. If needed, configure the analysis parameters. See the ANY.RUN **API documentation** for all available options.



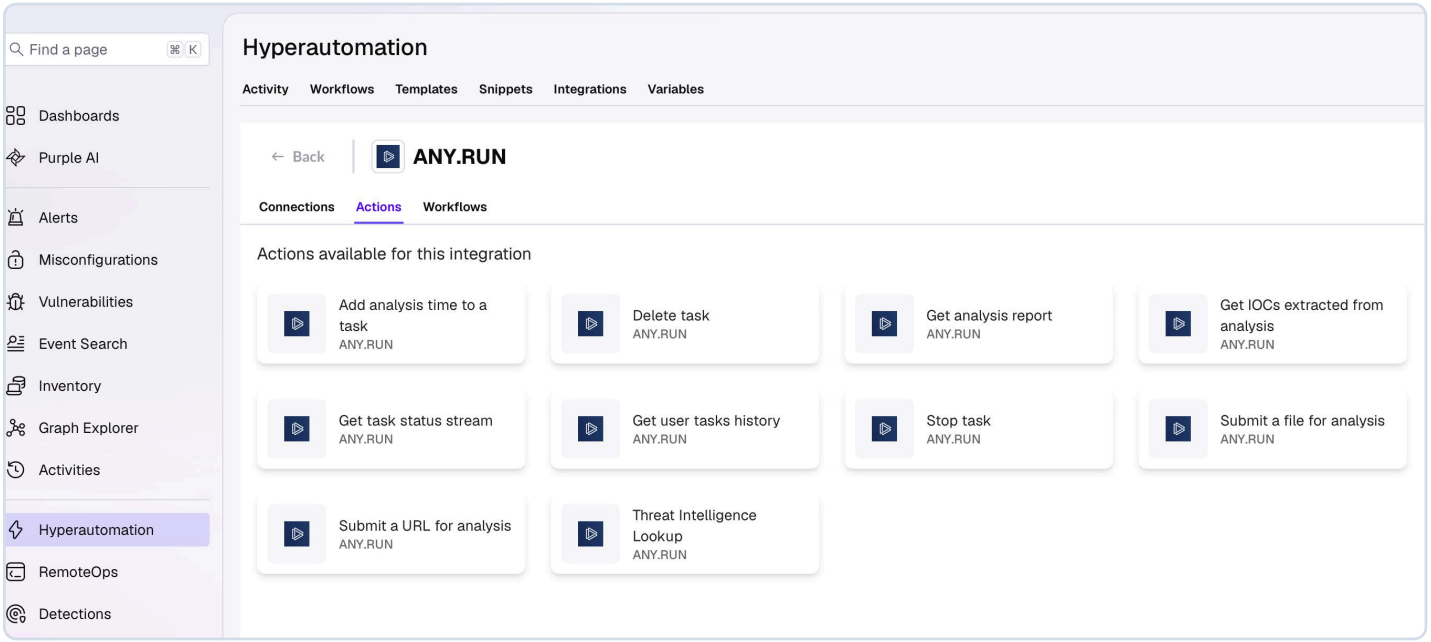
8. Click **Activate** to complete the setup.



✔ 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**.

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.

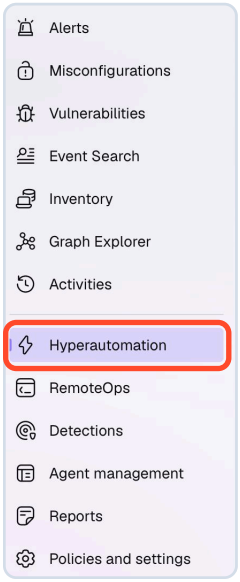
- **Deep threat context:** Pivot from individual indicators to related infrastructure, malware, IOCs, sandbox analyses, TTPs, and other evidence.
- **Flexible threat search:** Search by IP, URL, domain, or hash, or use natural-language and advanced queries to investigate specific behaviors, geographies, 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.

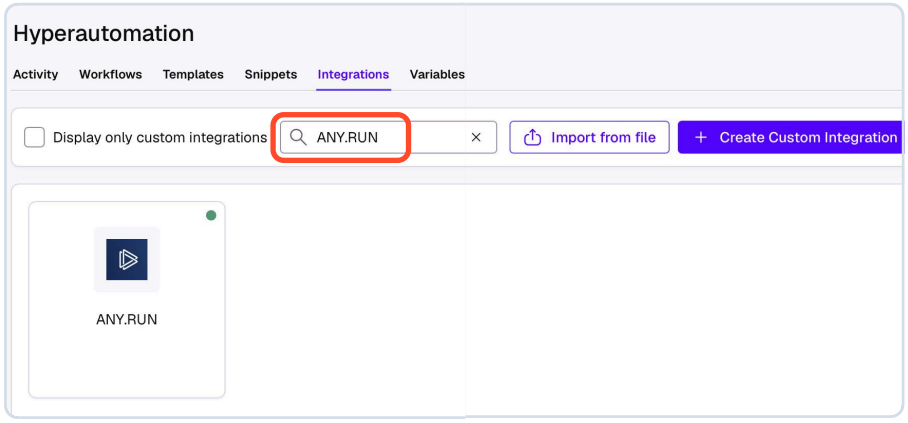
How to Integrate TI Lookup with SentinelOne

INSTALLATION AND CONFIGURATION

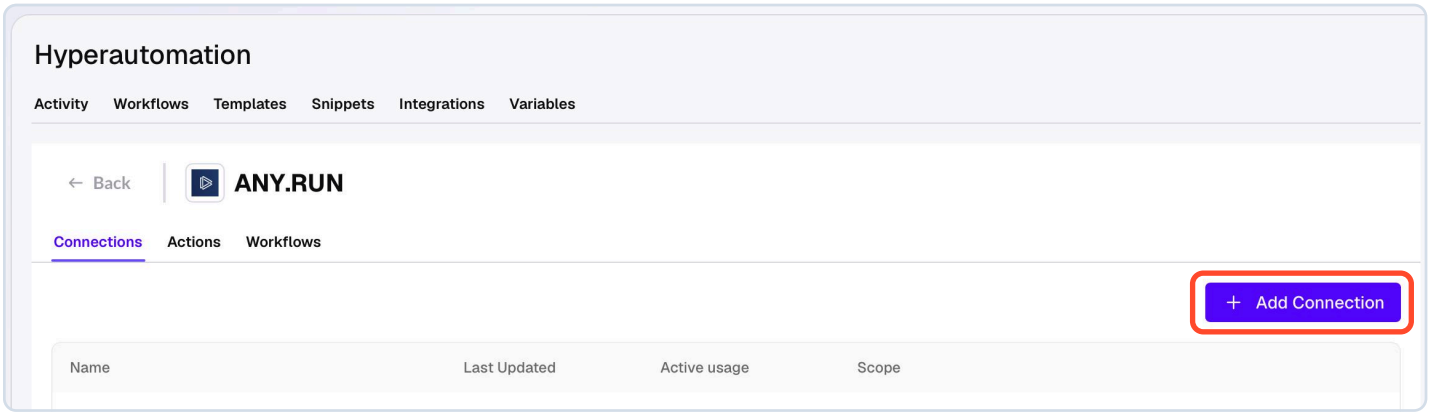
1. Go to the **Hyperautomation** section in SentinelOne.



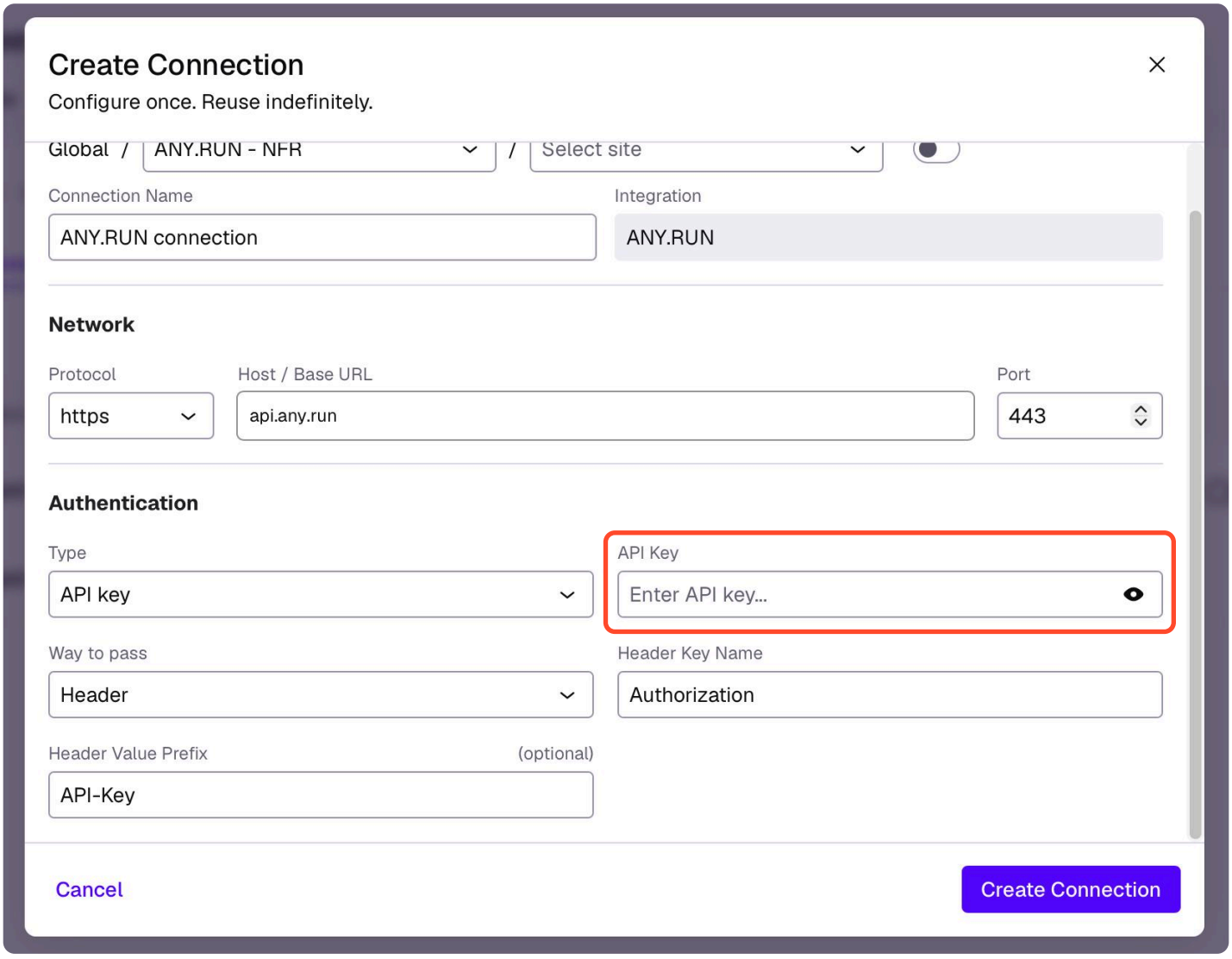
2. Open the **Integration** tab, enter **ANY.RUN** in the search bar, and select the integration.



3. Click **Add Connection**.



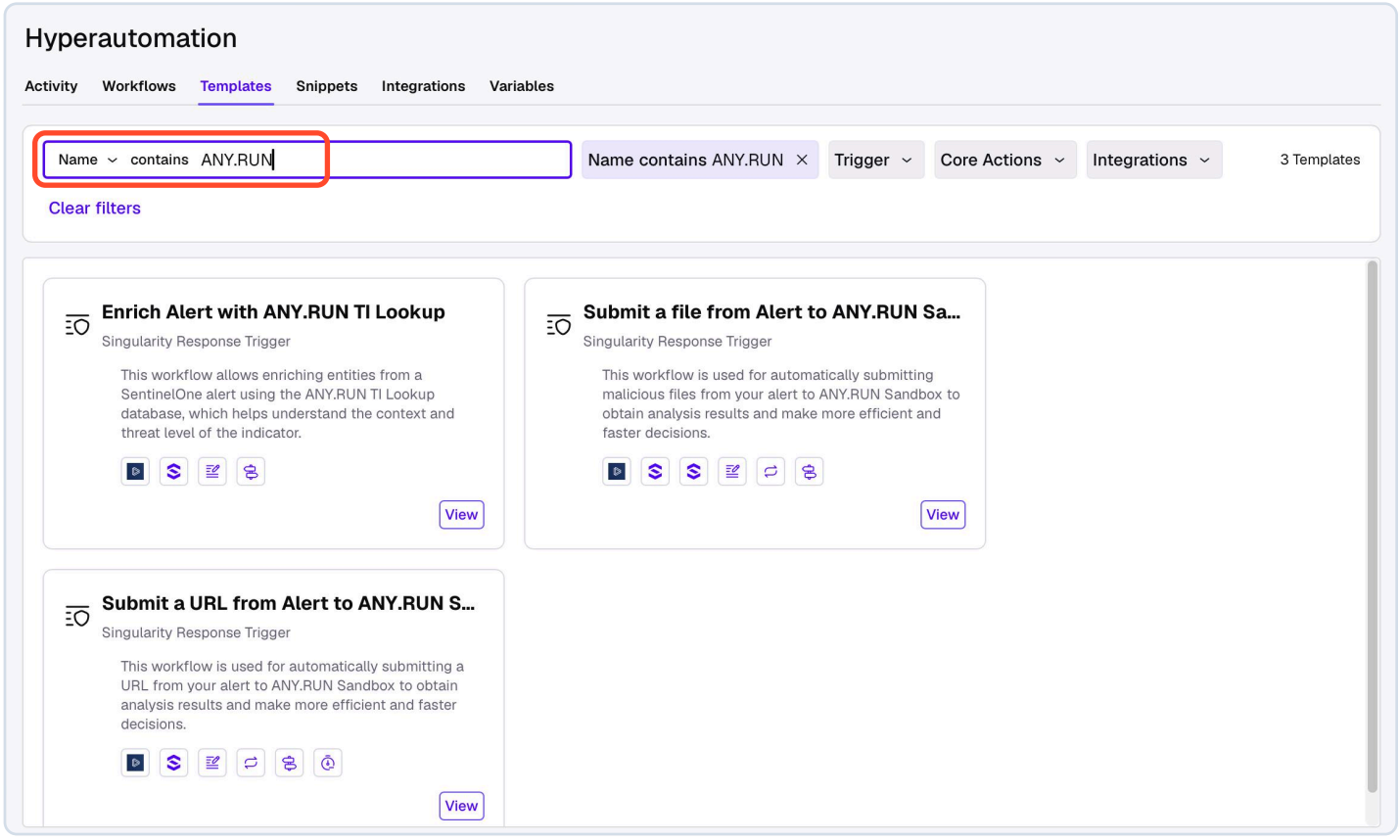
4. Enter your **API key**. The other fields are prefilled.



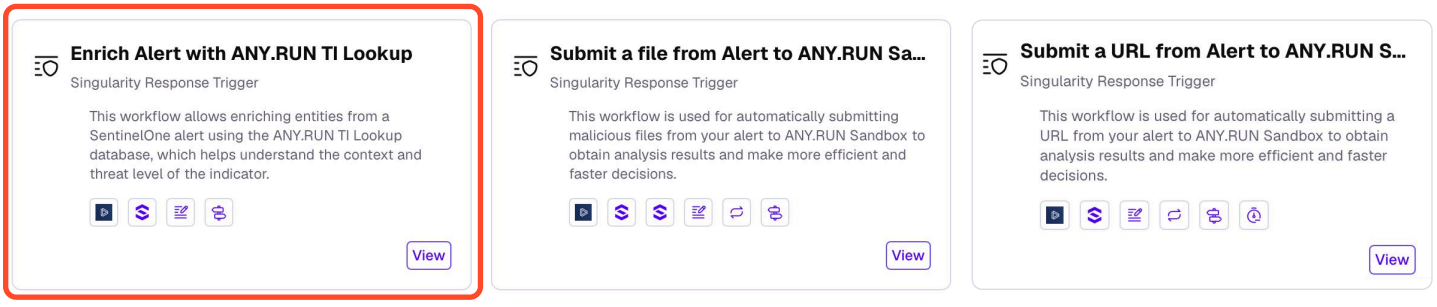
5. Click Create Connection to complete the setup.

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.

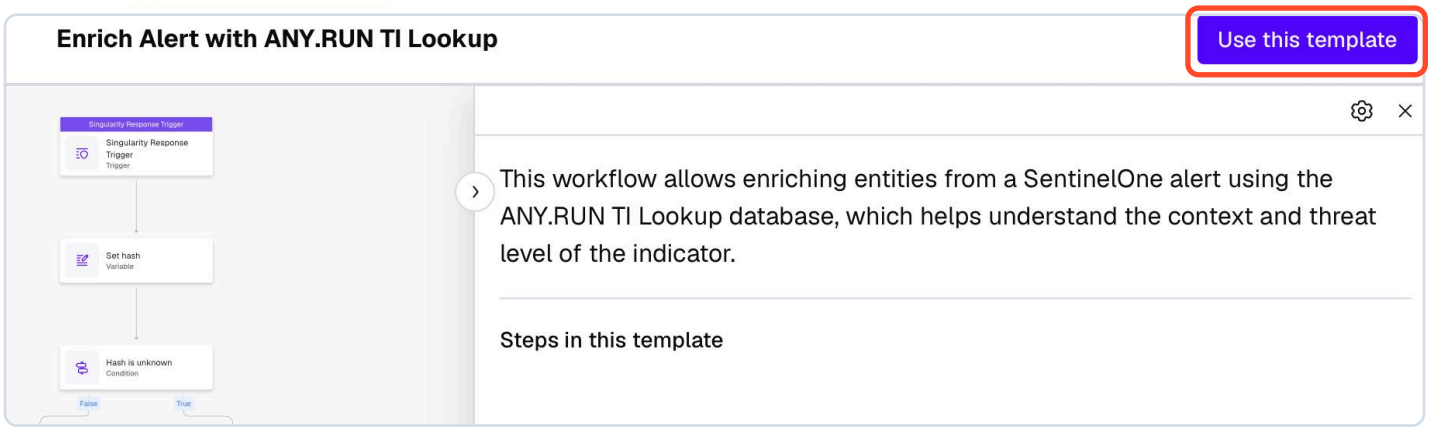


2. Click View in the ANY.RUN TI Lookup template:

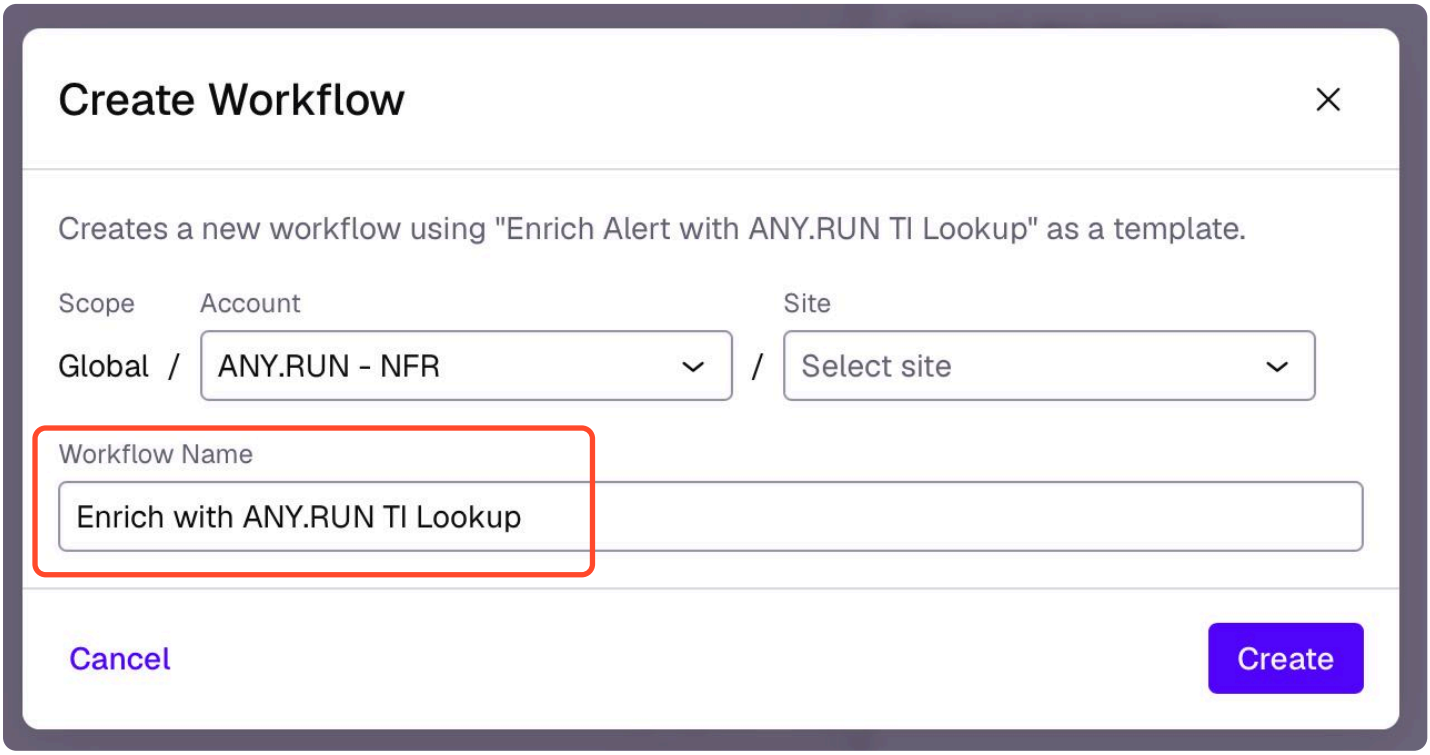


Note: By default, these templates are designed for automated workflows. You can also configure a workflow to run on demand and launch it manually for individual alerts.

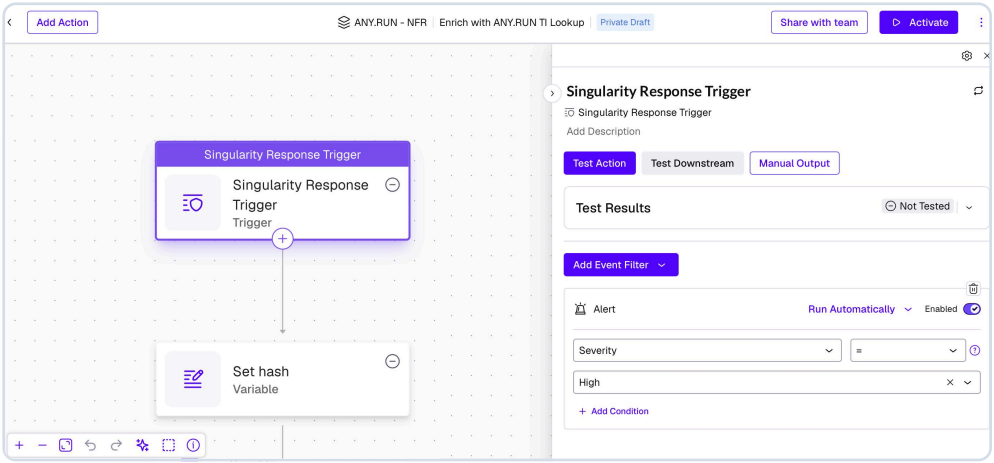
3. Click **Use this template**



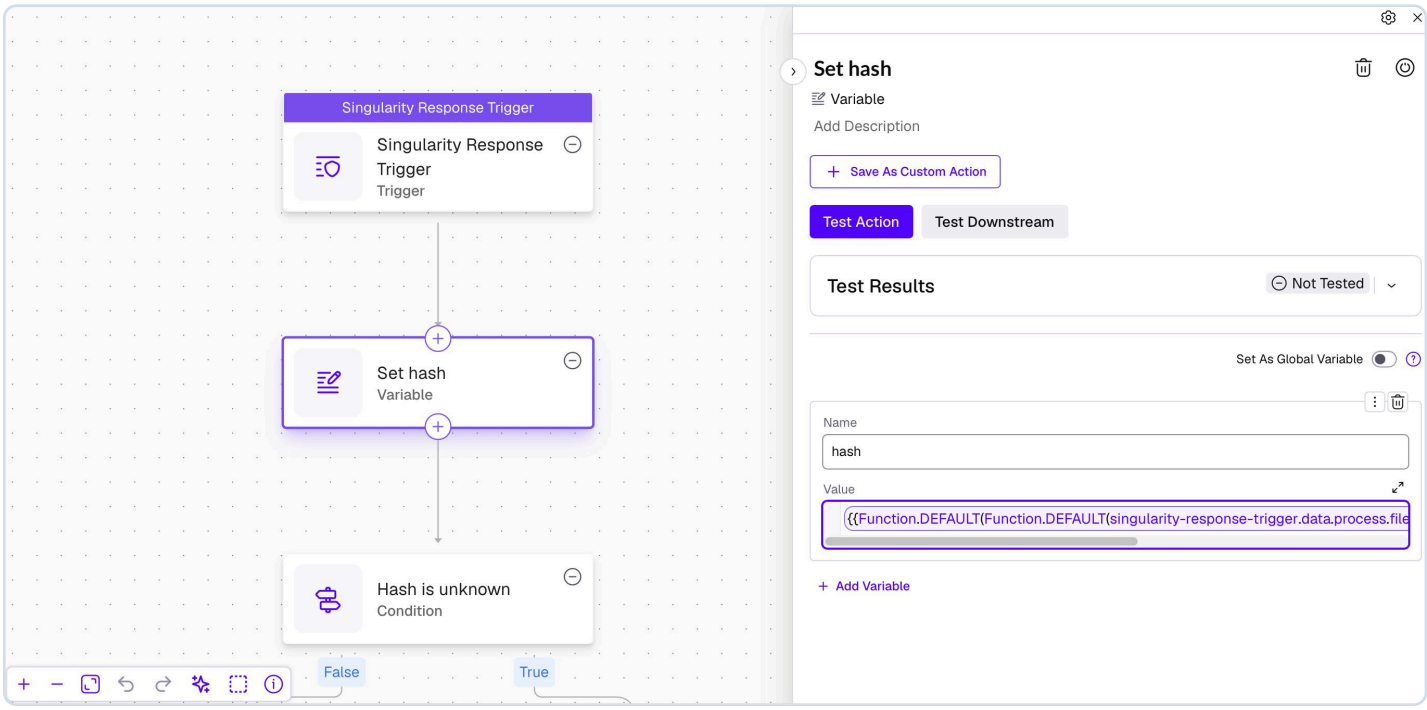
4. Name the workflow and click **Create**



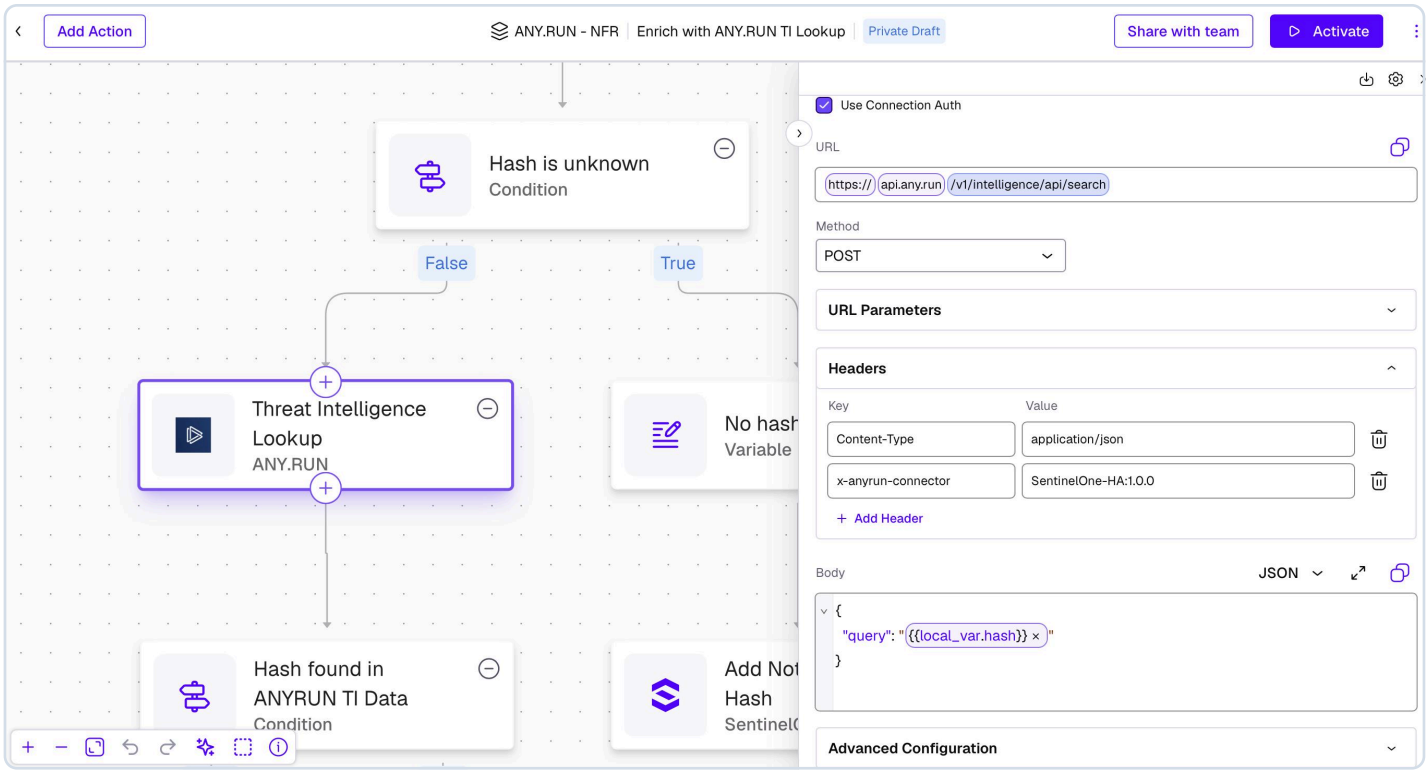
5. Configure the template trigger. It's the event that will start the automated workflow.



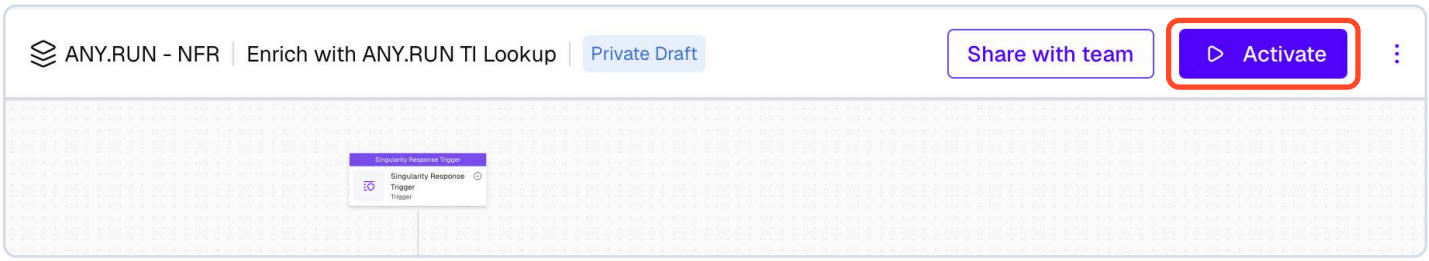
6. By default, the workflow is designed to process hashes. If needed, you can configure it to process IPs, URLs, or domains instead.



7. If needed, configure the analysis parameters. See the **ANY.RUN API documentation** for all available options.



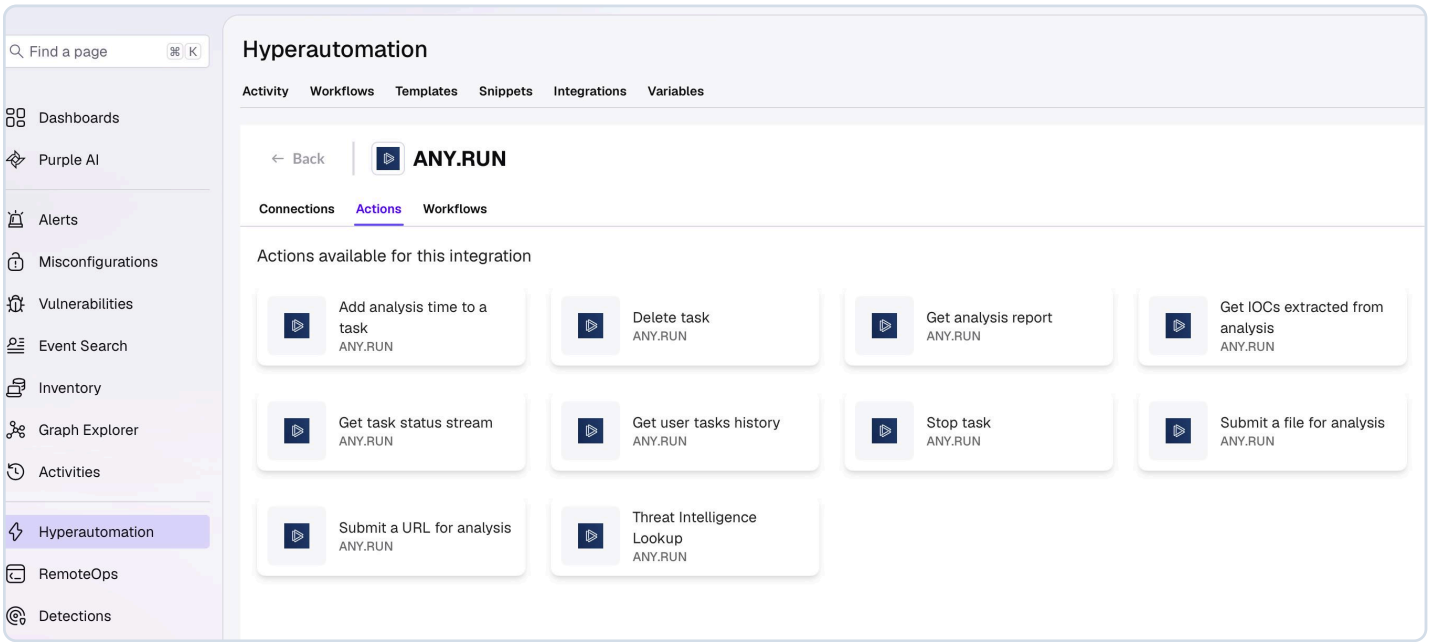
8. Click Activate to complete the setup.



✔ 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.



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