Spur Context API Playbooks App Documentation v1.0

Overview

This document aims to provide an understanding of the Spur Context API playbooks app for ThreatConnect.

Topics Covered

About Spur Context API

Spur Context API is a REST API service providing detailed IP Context data. It offers rapid IP search with actionable data, including client behaviors, geographical concentration, and associated risks.

App Functionality Overview

The Spur Context API app allows users to pull content from Spur's API and work with it in ThreatConnect's playbooks.

Input Data Types

- **IP Address**: The primary input for the Spur Context API is an IP address (IPv4 or IPv6).

Output Data Types

- **Autonomous System Details**: Information about the autonomous system to which the IP address belongs.
- **Client Behaviors**: Behaviors associated with clients using the IP address.
- **Geographical Concentration**: Geographical data related to the IP address, including location concentration of clients.
- **Risks and Threats**: Potential risks and threats associated with the IP address.
- **Infrastructure Classification**: Classification of the infrastructure where the IP is located.
- **Organization Details**: Information about the organization operating the IP address.
- **Services Running**: Details about protocols and services running on the IP address.
- **VPN/Proxy Details**: Information about VPN/Proxy usage and operator details for the IP address.

For a comprehensive understanding of the data provided by the IP Context Object, refer to the full IP Context Object documentation.

Spur Endpoints Utilized

- **/v2/context/:IP**: This endpoint retrieves an IP Context Object by IPv4 or IPv6 Address. It provides comprehensive details about the IP address, including all the output data types listed above.

Output Variable Details

The following output variables are provided by the Spur Context API app, each with its respective data type:

- **spur.as.number** (String): Autonomous System Number (e.g., `147049`)
- **spur.as.organization** (String): Autonomous System Organization (e.g., `PacketHub S.A.`)
- **spur.client.behaviors** (StringArray): Array of client behaviors (e.g., `['FILE_SHARING']`)
- **spur.client.behaviors.joined** (String): Concatenated client behaviors (e.g., `FILE_SHARING`)
- **spur.client.concentration.city** (String): City of client concentration (e.g., `Richmond`)
- **spur.client.concentration.country** (String): Country of client concentration (e.g., `CA`)
- **spur.client.concentration.density** (String): Density of client concentration (e.g., `1`)
- **spur.client.concentration.geohash** (String): Geohash of client concentration (e.g., `c28ry2`)
- **spur.client.concentration.skew** (String): Skew of client concentration (e.g., `8`)
- **spur.client.count** (String): Number of clients (e.g., `3`)
- **spur.client.countries** (String): Number of countries clients have come from (e.g., `1`)
- **spur.client.proxies** (StringArray): Array of client proxies (e.g., `['IPIDEA_PROXY', 'LUMINATI_PROXY']`)
- **spur.client.proxies.joined** (String): Concatenated client proxies (e.g., `IPIDEA_PROXY|LUMINATI_PROXY`)
- **spur.client.types** (StringArray): Array of client device types (e.g., `['MOBILE']`)
- **spur.client.types.joined** (String): Concatenated client device types (e.g., `MOBILE`)
- **spur.infrastructure** (String): Infrastructure classification
- **spur.json.data.raw** (String): Raw JSON data of the IP context
- **spur.location.city** (String): City of the IP location (e.g., `Vancouver`)
- **spur.location.country** (String): Country of the IP location (e.g., `CA`)
- **spur.location.state** (String): State of the IP location (e.g., `British Columbia`)
- **spur.organization** (String): Organization operating the IP address (e.g., `Packethub S.A.`)
- **spur.risks** (StringArray): Array of risks associated with the IP address (e.g., `['CALLBACK_PROXY', 'TUNNEL']`)
- **spur.risks.joined** (String): Concatenated risks (e.g., `CALLBACK_PROXY|TUNNEL`)
- **spur.services** (StringArray): Array of services running on the IP address
- **spur.services.joined** (String): Concatenated services
- **spur.tunnels.anonymous** (StringArray): Array indicating if the tunnel is anonymous (e.g., `['True']`)
- **spur.tunnels.anonymous.joined** (String): Concatenated tunnel anonymity status (e.g., `True`)
- **spur.tunnels.operator** (StringArray): Array of tunnel operators (e.g., `['NORD_VPN']`)
- **spur.tunnels.operator.joined** (String): Concatenated tunnel operators (e.g., `NORD_VPN`)
- **spur.tunnels.type** (StringArray): Array of tunnel types (e.g., `['VPN']`)
- **spur.tunnels.type.joined** (String): Concatenated tunnel types (e.g., `VPN`)

Each variable provides specific details about the IP address, contributing to a comprehensive understanding of its context.

Requirements

- A ThreatConnect account.
- Access to Spur Context API with a valid API token.

Installation

For installation instructions, refer to the ThreatConnect System Administration Guide (Install an App).

Practical Examples

Example: Using Spur Context API for IP Address Enrichment

This example demonstrates how to use the "Spur Context API Enrichment" app within a ThreatConnect playbook to enrich IP address indicators and display the results via a tooltip.

Scenario

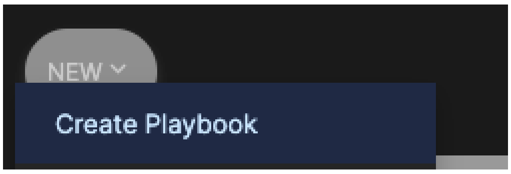
The playbook is designed to be executed from the IP address indicator page in ThreatConnect. When a user navigates to an IP address indicator and triggers the playbook, it fetches detailed information about the IP address from the Spur Context API and displays it in a tooltip.

Playbook Components

1. **TRIGGER**: User Action Trigger
    - The playbook is initiated by a user action. When viewing an IP address indicator in ThreatConnect, the user can execute the playbook directly from the playbooks section.
2. **APP**: Spur Context API Enrichment
    - The playbook uses the "Spur Context API Enrichment" app to query the Spur Context API with the IP address as input.
    - The app retrieves detailed information about the IP address, such as geographical concentration, client behaviors, risks, and other relevant data.
3. **TOOLTIP DISPLAY**: Showing API Results
    - Upon successful retrieval of data, the playbook displays the results in a tooltip format.
    - This tooltip provides a quick and informative summary of the IP address details, allowing the user to understand the context and potential risks associated with the IP address.

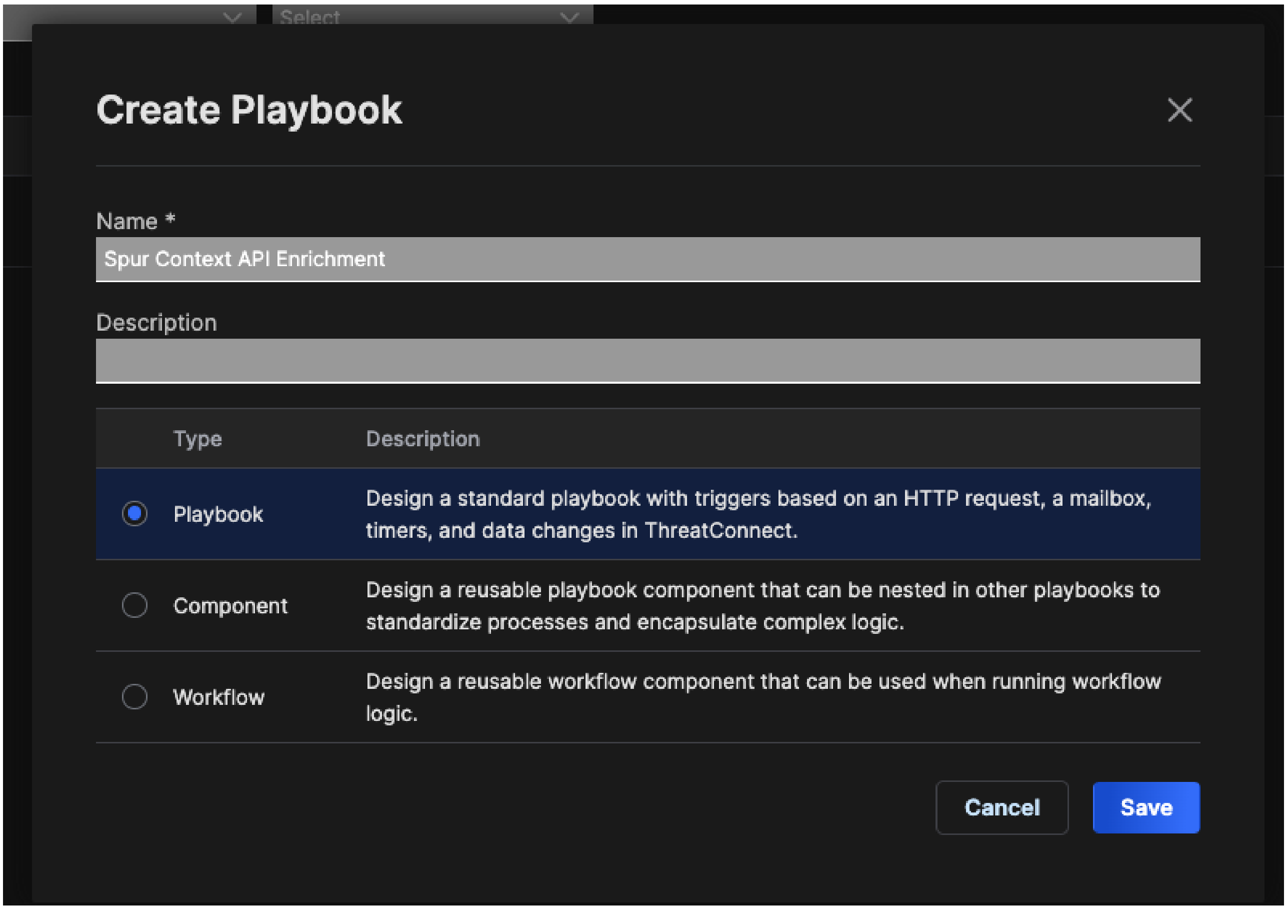
Step by Step Guide

1. Navigate to the playbooks page in ThreatConnect.
2. Click on the "NEW" button and select "Create Playbook".



3. For the name enter "Spur Context API Enrichment".

4. Select 'Playbook' for the type.



Create Playbook

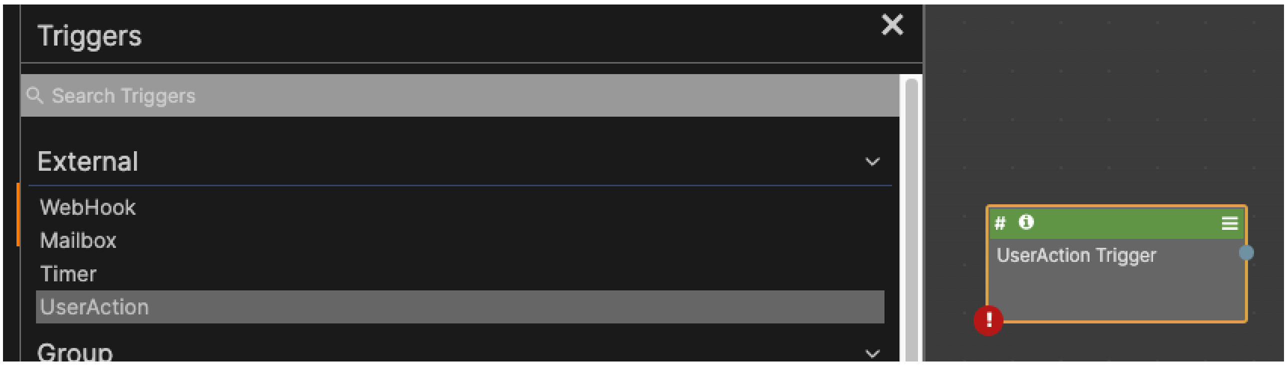
Name *

Spur Context API Enrichment

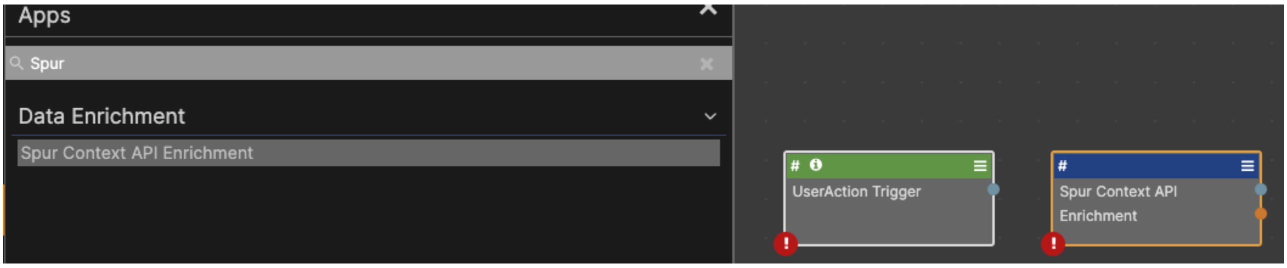
Description

	Type	Description
●	Playbook	Design a standard playbook with triggers based on an HTTP request, a mailbox, timers, and data changes in ThreatConnect.
○	Component	Design a reusable playbook component that can be nested in other playbooks to standardize processes and encapsulate complex logic.
○	Workflow	Design a reusable workflow component that can be used when running workflow logic.

5. Add a UserAction trigger.

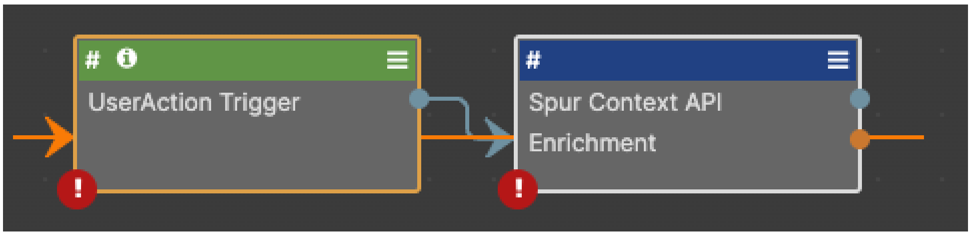


6. Add the "Spur Context API Enrichment" app.



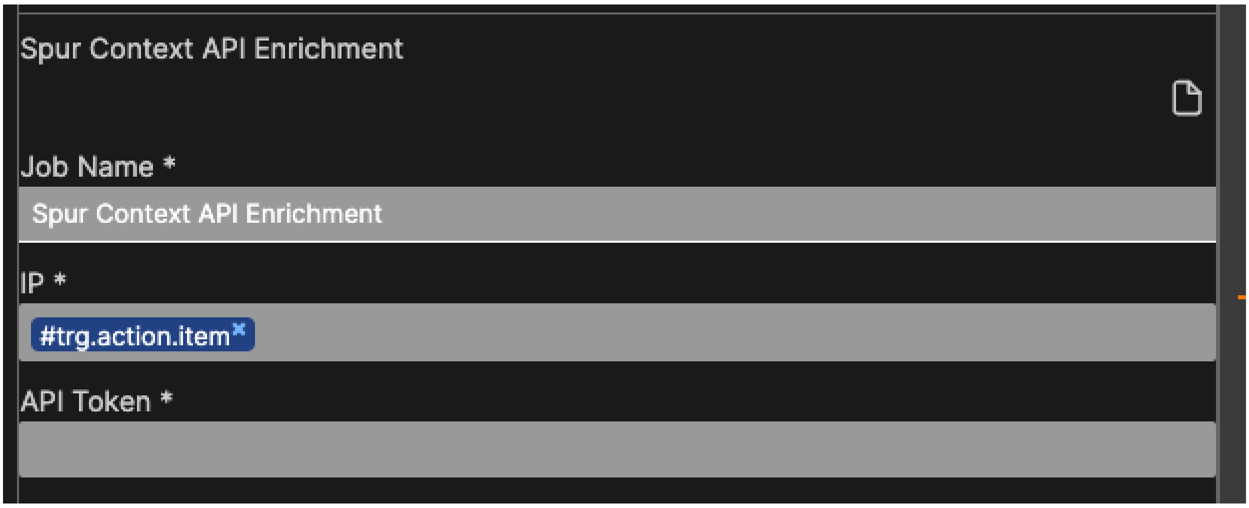
7. Connect the trigger to the app. (Blue line)

8. Connect the app to the tooltip display. (Orange line)



9. Double click on the Spur Context API Enrichment app to edit it.

10. For the IP field enter `#trg.action.item`



Spur Context API Enrichment

Job Name *

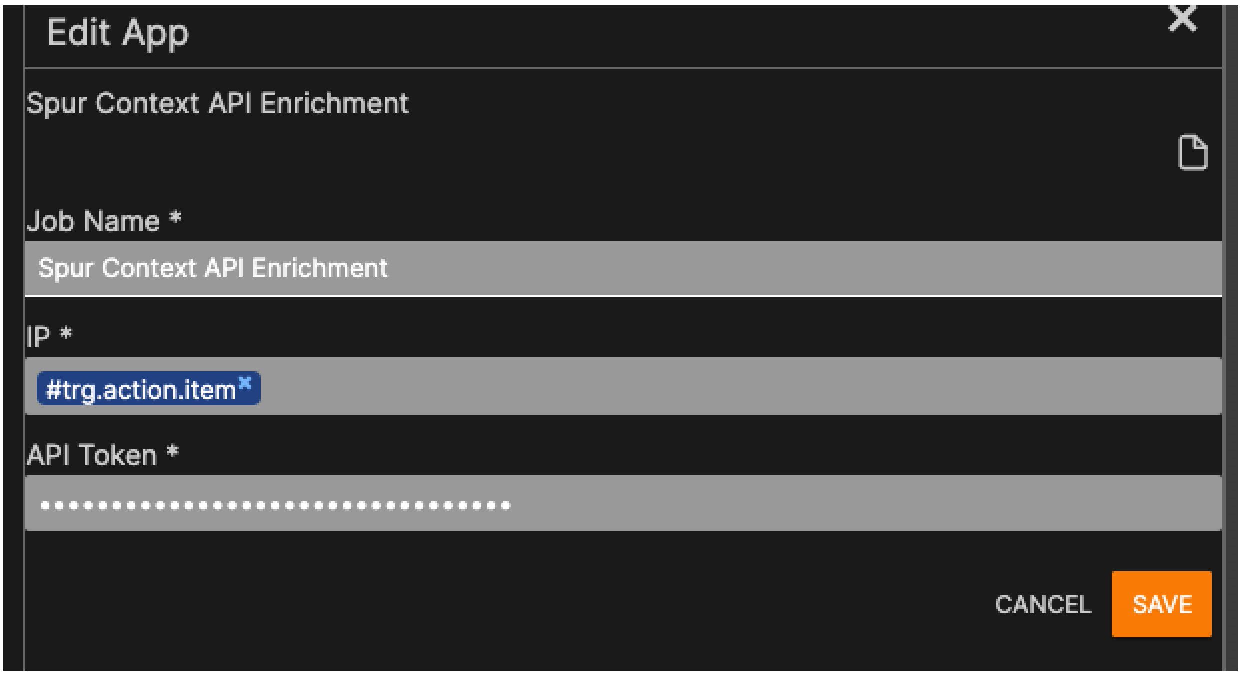
Spur Context API Enrichment

IP *

#trg.action.item

API Token *

11. For the API Token field enter your Spur Context API token.



Edit App

Spur Context API Enrichment

Job Name *

Spur Context API Enrichment

IP *

#trg.action.item

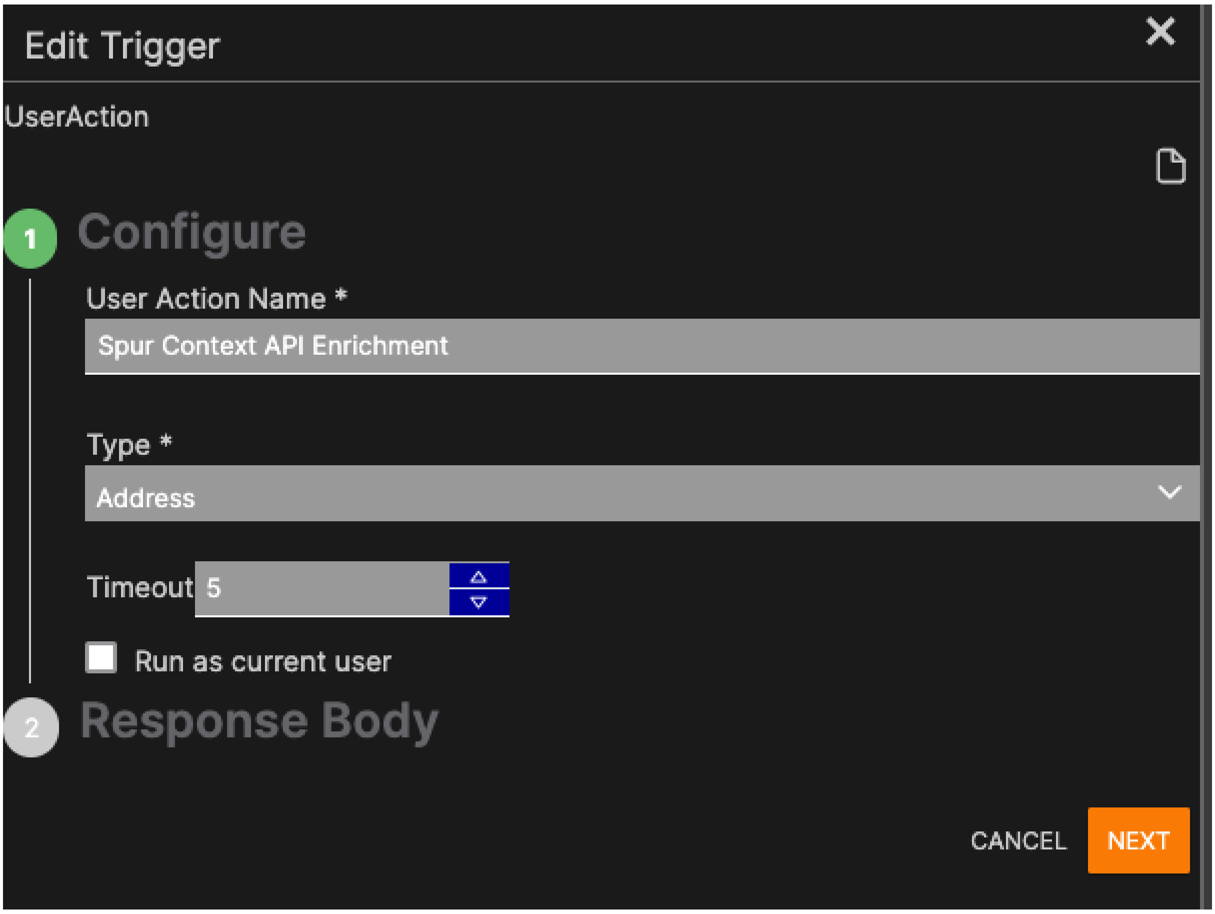
API Token *

••••••••••••••••••••••••••••••••

12. Click "SAVE".

13. Double click on the UserAction trigger to edit it.

14. For the name enter "Spur Context API Enrichment".



Edit Trigger

UserAction

1 Configure

User Action Name *

Spur Context API Enrichment

Type *

Address

Timeout 5

□ Run as current user

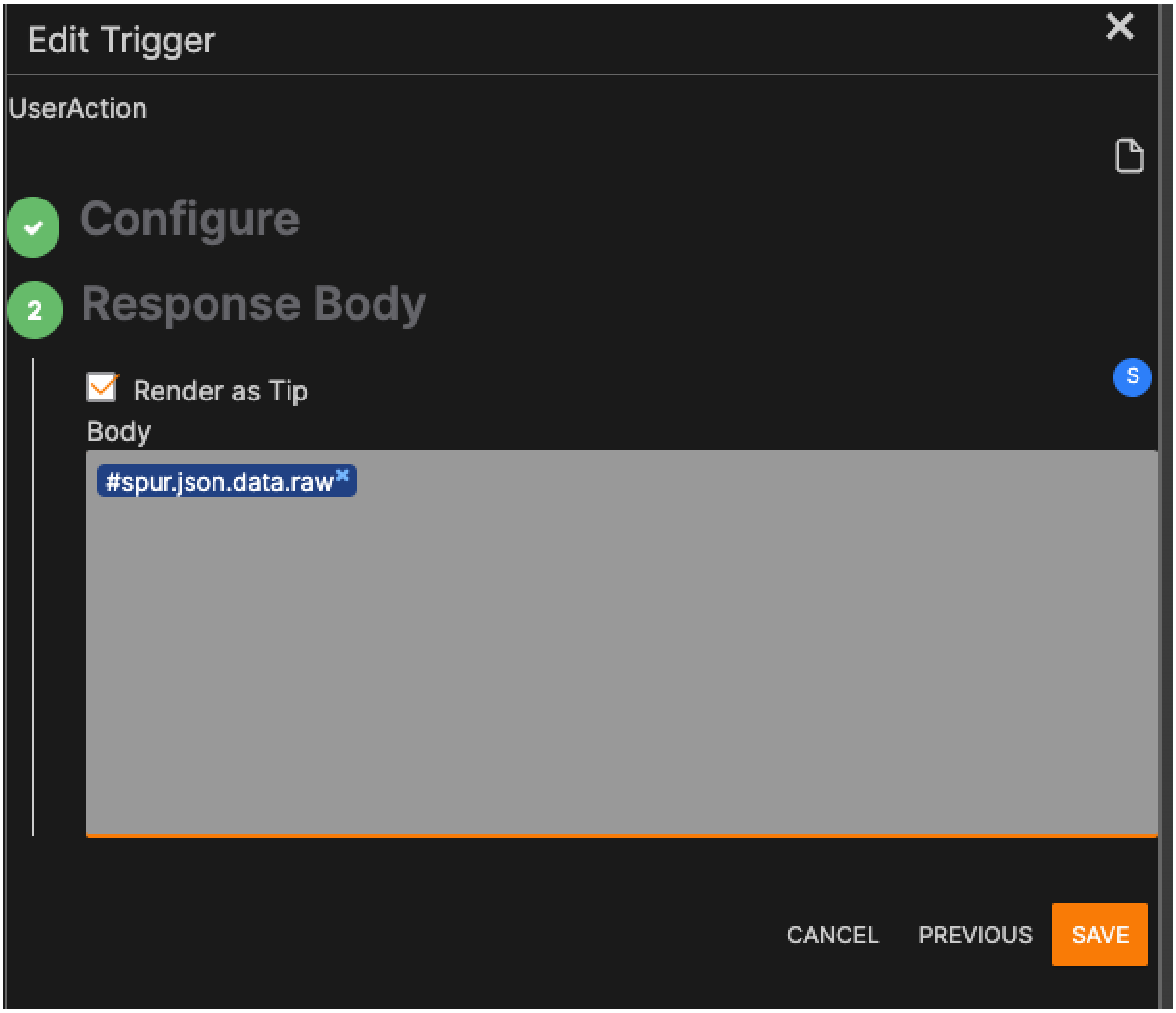
2 Response Body

15. For the type select "Address".

16. Click "NEXT".

17. Click the checkbox 'Render as Tip'.

18. For the body enter `#spur.json.data.raw`. This will display the raw JSON data from the Spur Context API. You can also use any of the output variables listed in the "Output Variable Details" section. A full example using html with the output variables is available here.



Edit Trigger

UserAction

Configure

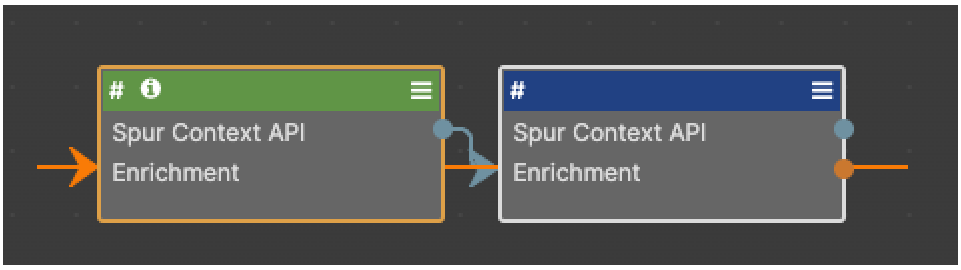
Response Body

☑ Render as Tip

Body

#spur.json.data.raw

19. Click "SAVE". Your final playbook should look like this:

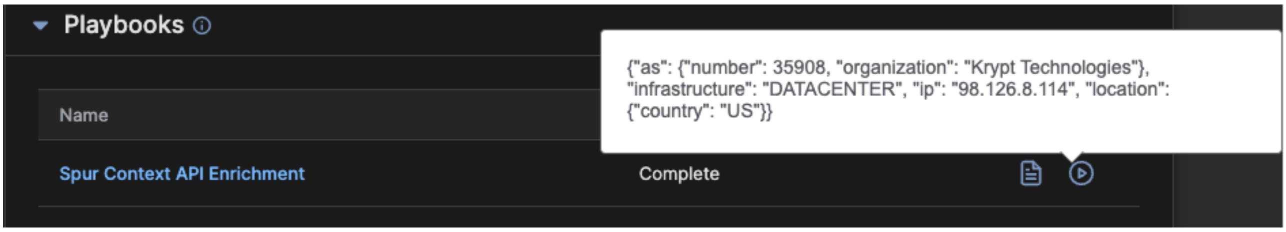


20. Move the playbook from Design Mode to Active.

21. Navigate to the IP address indicator page in ThreatConnect.

22. Locate the playbooks section on the page.

23. Execute the "Spur Context API Enrichment" playbook.



```
{"as": {"number": 35908, "organization": "Krypt Technologies"},
"infrastructure": "DATACENTER", "ip": "98.126.8.114", "location":
{"country": "US"}}
```

Usage Instructions

1. Navigate to the IP address indicator page in ThreatConnect.
2. Locate the playbooks section on the page.
3. Execute the "Spur Context API Enrichment" playbook.
4. View the enriched data displayed in a tooltip on the same page.

This practical example illustrates how ThreatConnect users can leverage the Spur Context API to gain deeper insights into IP addresses directly within the platform, enhancing their cybersecurity analysis and decision-making process.

Support

For support, contact the Spur Context API team at support@spur.us.

Appendix

This section provides additional resources and links for further information and exploration.

Additional Documentation

- **Spur Context API Detailed Documentation**: For in-depth information about the Spur Context API, visit Spur Context API Documentation.
- **Data Types and Structures**: Detailed descriptions of the data types and structures used by the Spur Context API can be found here.

Developer Resources

- **API Reference**: Access the complete API reference for developers at Spur API Reference.
- **Code Examples**: Find code examples and usage scenarios here.

Support and Community

- **FAQs**: Frequently Asked Questions about the Spur Context API are available here.

Company and Product Information

- **About Us**: Learn more about our team and mission at Our Company Website.
- **Product Updates**: Stay updated with the latest product news and updates at Spur Blog.

Contact Information

- **Support Contact**: For direct support, reach out to us at support@spur.us.
- **Sales Inquiries**: Contact our sales team for inquiries at sales@spur.us.