Endpoint Beaconing C2 Communication

Brief / Purpose

This workflow detects and responds to endpoint beaconing c2 communication. It receives alerts via a webhook, enriches the event, decides whether it's suspicious, and notifies the SOC team if necessary.

Why use it?

- ✅ Ensure only trusted clients can call your workflow (via Bearer token).

- ✅ Validate that all expected fields are present in the request body.

- ✅ Return helpful and consistent JSON responses (`200`, `400`, `401`).

How it works:

1. `Webhook` – Entry point for external `POST` requests.

2. `Configuration` – Defines `config.bearerToken` and `config.requiredFields`.

3. `Check Authorization Header` – Compares incoming Bearer token with config.

4. `401 Unauthorized` – Returned if the token is missing or incorrect.

5. `Has required fields?` – JS code checks for required fields in the request body.

6. `400 Bad Request` – Returned if any required field is missing.

7. `Create Response` & `200 OK` – Returns a custom success message.

Setup Instructions:

- Set your desired Bearer token in `config.bearerToken`.

- For each required field, set a key in `config.requiredFields`

(e.g., `config.requiredFields.message)*.

The value doesn't matter, only the keys are checked.

- Replace the `Add workflow nodes here` node with your own workflow logic.

- Edit the `Create Response` node to build your response.