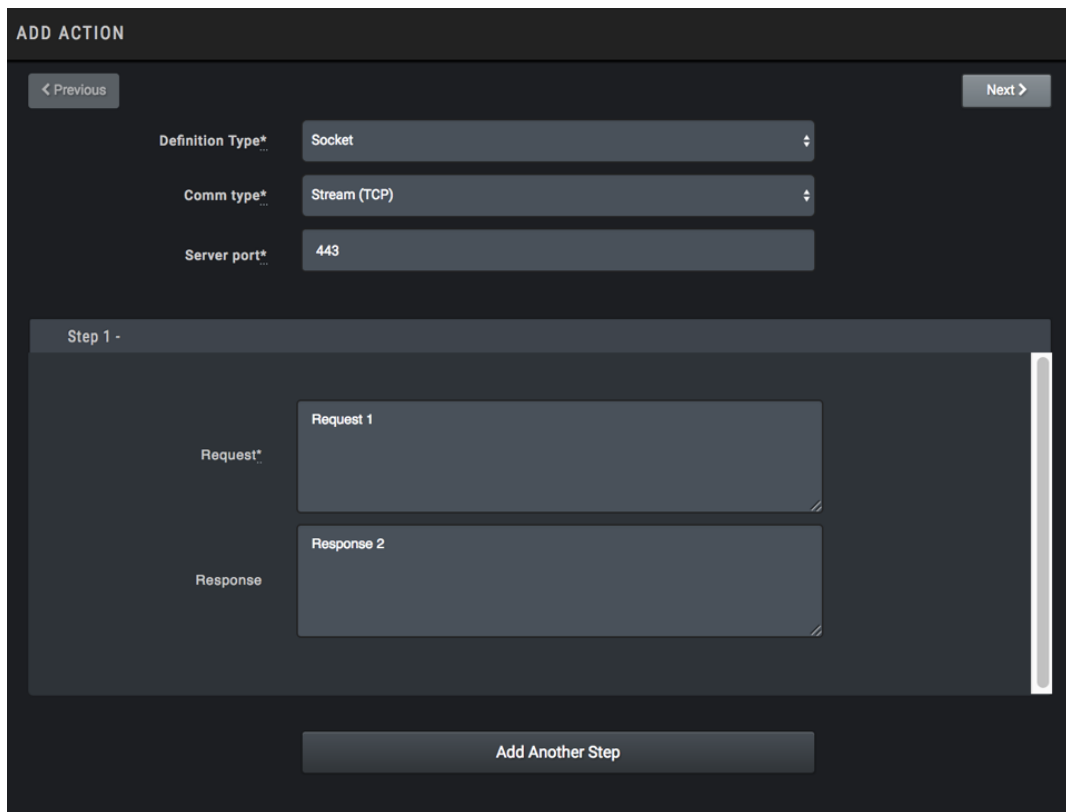


## ADD SOCKET-BASED ACTIONS

For advanced users, Actions can be created at the socket level to ingest specific TTPs . This Action type uses a basic TCP or UDP connection that data is sent over. This is helpful when a PCAP is not available.

1. From the Director, go to **Library > Actions**.
2. Click **Add Action** and then select **Socket**. The Add Socket Action form displays.
3. Select **Comm Type** (TCP or UDP) and enter the **Server port**.
4. Add Step information:
  - a. Click on the Step 1 label to expand the step.
  - b. Enter the **Request**.
  - c. Optional: Enter the **Response**.
  - d. If you want to add additional steps, click **Add Another Step** and then repeat steps b & c.



Adding steps to socket-based Actions

5. After all steps are entered, click **Next**.
6. Populate the Action Name, Description, and Dimensions.
  - a. Name
  - b. Description
  - c. Attack Vector
  - d. Attacker Location
  - e. Behavior Type
  - f. Covert
  - g. OS/Platform

- h. Stage of Attacks
  - i. Optional: User Tags
7. Click **Save Action**. The Action Library displays. A confirmation message that your Action was created successfully is shown and the Action is selected and displayed in the Action preview.