ADDING CAPTIVE IOC - PCAP ACTIONS

Captive IOC - PCAP Actions test the effectiveness of network controls against known malicious targets in a PCAP.

NOTE: All PCAP files that contain http traffic should be supported. If you have issues with a PCAP file, submit a support ticket.

TO CREATE A CAPTIVE IOC - PCAP ACTION

IMPORTANT: Since all PCAP-based Action that include http traffic can be run as an IOC Action, verify there isn't a standard PCAP-based Action that meets your needs before creating a new IOC Action. There is a new Run Captive IOC Action on an Action's preview if this is supported. When you run PCAP-based Actions this way, the Job results will include a Captive IOC - PCAP icon.

1. Go to **Library > Actions**.
2. Click **Add Action** and select **Captive IOC - PCAP**.
3. Before uploading your PCAP file, determine if the IP and MAC addresses should be anonymized. You may choose to do this if you don't want to use your network information in an Action.
    a. If you want to anonymize IP addresses in the PCAP file, select **Yes**.
    b. If you want to anonymize MACs in the PCAP file, select **Yes**.
4. Add a PCAP (.pcap) file. The platform automatically advance to the next page after the upload completes.

    NOTE: A progress bar that includes an estimated time remaining is displayed to show how the PCAP import is progressing.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec47e07dc756be50aaf3/n/pcap-upload.png)

Uploading a PCAP file

5. The **Add PCAP Action Step 2** page displays.
   The platform analyzes the PCAP and identifies conversations. It automatically provides you feedback regarding issues with the PCAP that must be resolved.

    NOTE: Actions can only contain TCP or UDP traffic, not both. Actions can only have 2 unique IP Addresses.

    NOTE: If you use **Back to Upload PCAP** or exit this screen without using one of the buttons, your PCAP will stay in the system.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec45e07dc756be50aae0/n/pcap-convo-select.png)

PCAP upload feedback

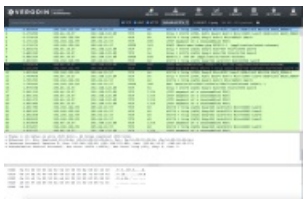
6. Remove Conversations as necessary.
   a. (Optional) Select one or more conversations and click **Remove Conversations**.

> **NOTE:** This button only appears when conversations are selected.

> **TIP:** You can select conversations across pages. This includes selecting a conversation on one page, using the page arrows to advanced to another page, and then Shift +clicking on a conversation to select all conversations in between.

   b. (Optional) Select **Remove TCP** or **Remove UDP** to remove all conversations of that type.

7. (Optional) Click **Packet View** to view remaining packets.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec34e07dc756be50aa12/n/pcap-packetview.png)

Adding Actions from packet

8. Return to the Conversations page, and then click **Next**.
9. Complete the applicable Dimensions presented and 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.

> **NOTE:** If you click **Cancel** during the creation process, the Action will not be created.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec45e07dc756be50aadd/n/pcap-filled-in-ioc.png)

Complete Dimension selections

HTTP Headers for Hex Actions

The Validation Platform includes a global setting, **Hex Actions - Update Host in HTTP Header** . This allows you to

configure the platform so the host is always or never replaced when running Actions. However, to demonstrate specific behavior, such as demonstrating Header Spoofing techniques or leveraging web services as C2s, you may need the Action to run the opposite of the global setting. To support this, there is a **Update Host in HTTP Header** runtime parameter. This defaults to the global setting but can be modified. We recommend you add a note in the Action's description if the Action requires a specific setting for that parameter.