Atomic Fishbowl

Context Menu Actions for NetWitness

Summary

Atomic Fishbowl provides the means to drill directly from the Investigate area of NetWitness back into Atomic Fishbowl. This allows an analyst to visualize IP addresses and hostnames using Atomic Fishbowl. To do this, it is necessary to create Context Menu Actions in the NetWitness configuration.

Note: the screenshots for this procedure are taken from NetWitness 11.3.x. While screenshots from other NetWitness versions may be slightly different, the procedure is substantially the same.

There are five JSON files for which the procedure will need to be performed. The procedure is identical for each of the files. They are:

- **nw-investigation-ad-username-dst-action.json** – Allows an analyst to visualize usernames by putting the username on the **destination** side of Atomic Fishbowl's NetWitness query. E.g. *ad.username.dst* = *'someuser'.*
  - It works with the following meta keys:
    - **user.src**
    - **user.dst**
    - **username**
    - **ad.username.src**
    - **ad.username.dst**

- **nw-investigation-ad-username-src-action.json** - Allows an analyst to visualize usernames by putting the username on the **source** side of Atomic Fishbowl's NetWitness query. E.g. *ad.username.src* = *'someuser'*
  - It works with the following meta keys:
    - **user.src**
    - **user.dst**
    - **username**
    - **ad.username.src**
    - **ad.username.dst**

- **nw-investigation-host-action.json** - Allows an analyst to visualize hostnames. E.g. *alias.host* = *'somehost'*.
  - It works with the following meta keys:
    - **alias.host**
    - **host.src**
    - **host.dst**

- **nw-investigation-ip-dst-action.json** - Allows an analyst to visualize IP addresses by putting the address on the **destination** side of Atomic Fishbowl's NetWitness query.
    - It works with the following meta keys:
        - ip.src
        - ip.dst
        - orig.ip
        - device.ip
        - ip.addr
        - alias.ip

- **nw-investigation-ip-src-action.json** - Allows an analyst to visualize IP addresses by putting the address on the **source** side of Atomic Fishbowl's NetWitness query.
    - It works with the following meta keys:
        - ip.src
        - ip.dst
        - orig.ip
        - device.ip
        - ip.addr
        - alias.ip

Installation Procedure

1. In the NetWitness user interface, navigate to **Admin > System > Context Menu Actions**.

2. Click the '**+**' sign near the top to add a new context menu definition.

3. Click the "**Switch to Advance View**" button at the bottom of the the "Context Menu Action Configuration" dialog.

4. From the same directory from which you opened this document, using your favourite text editor (but not Windows Notepad – it doesn't handle UNIX line breaks properly), open the file **nw-investigation-ad-username-dst-action.json**.

5. Highlight and copy the contents of the JSON file to the clipboard.

6. Back in NetWitness, highlight the default JSON text that's populated in the configuration, and paste what you have copied into the configuration, and press your **delete** key.

7. Paste the JSON text you copied into the configuration.

8. Click the "**Switch to Basic View**" button

9. In the Definition box, change the hostname from **localhost** to the hostname of your Atomic Fishbowl host.

10. Click **Save**.

11. Repeat the procedure for the other **.json** files contained in the archive.

Using the Integration