ADDING CAPTIVE DNS QUERY ACTIONS

Captive DNS Query Actions are processed to test internal DNS capabilities. With Captive DNS Query Actions, you define the expected response and when you run the Action, the traffic goes from Actor to Actor instead of Actor to DNS. You use this type of Action to determine if there are controls in place to detect if someone attempts a DNS record change.

TO CREATE A CAPTIVE DNS QUERY ACTION

1. Select **Library > Actions**.
2. Click **Add Action** and select **Captive DNS Query**.
3. Enter the **Query**.
4. Select the **Query type**. Options include: A, AAA, CNAME, MX, NULL, NS, PTR, SOA, SRV, TXT.
5. Enter the **(expected) Response**.
6. Enter the **Name**.
7. Enter the **Description**.
8. Select the **Attacker Vector**. This will be Protocols / DNS.
9. Select the **Attacker Location**. This will vary.
10. Select the **Behavior Type**. Unless you determine otherwise, Malicious DNS Query is generally the closet option.
11. Select the **Covert behavior**. This is generally set to No.
12. Select the **OS/Platform**. This will vary.
13. Select the **Stage of Attack**. This is generally set to Command and Control.
14. (Optional) Assign **User Tags**.
15. Click **Save Captive DNS Query**.
    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.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec3ee07dc756be50aa8f/n/captive-dns1.png)

Captive DNS Query Action form

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.