ADDING MALICIOUS DNS QUERY ACTIONS

Malicious DNS Query Actions test internal DNS capabilities, specifically the addition of known bad domains to your blocked list. Network and Endpoint Actors query DNS servers and compare the response (NXDomain, redirect, etc.) to pre-established rules to validate defenses. These rules are configured in the DNS Settings. See the Admin Guide for additional information.

When you run these Actions, you choose one Actor and the traffic tests the DNS Controls. Examples of when you would create this type of Action include when you receive the TTP associated with an IOC or you have an unverified IOC, such as a clickjacking domain or malicious advertising, from threat intel.

IMPORTANT: Before running Malicious DNS Actions, the DNS server you want to test must be added to the Director and assigned to the Actor or Actors.

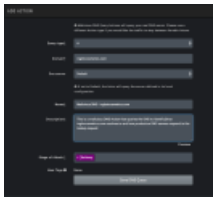
NOTE: When running DNS Query Actions, you can expand Runtime parameters and set a temporary DNS Server.

TO CREATE A MALICIOUS DNS QUERY ACTION

1. Select **Library** > **Actions**.
2. Click **Add Action** and select **Malicious DNS Query**.
3. Select the **Query type**.
4. Enter the **Domain**.
5. Select the **DNS Server**.

   NOTE: Default will query the server defined in the Actor's local configuration.
6. Enter the **Name**.
7. Enter the **Description**.
8. Select the **Stage of Attack**. This is generally set to Command and Control.
9. (Optional) Assign **User Tags**.
10. Click **Save 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/629cec3de07dc756be50aa86/n/create-malicious-dns.png)

Create Malicious DNS Query Action form