Mandiant

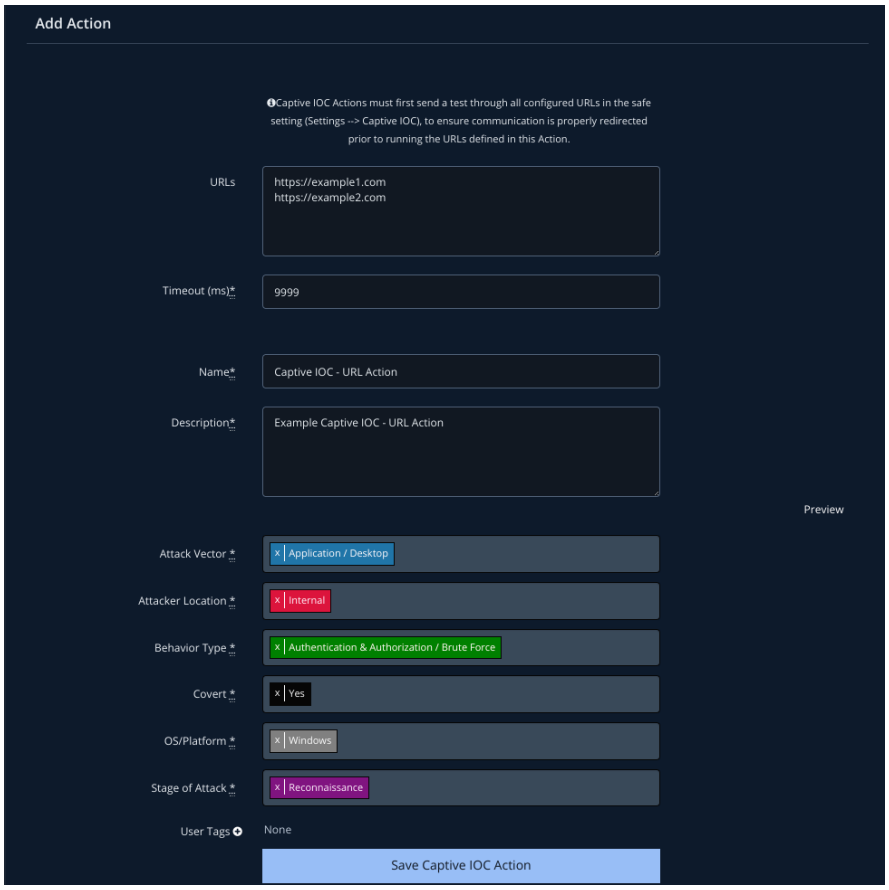
ADD CAPTIVE IOC - URL ACTIONS

Captive IOC - URL Actions test the effectiveness of network controls against known malicious URLs. When these Actions are run, one or multiple URLs are requested, and a small custom response is sent from the Destination Actor. The response is not representative of actual malicious content and, as such, this Action methodology only validates whether the request is allowed through network controls.

1. Select **Library > Actions**.
2. Click **Add Action** and select **Captive IOC - URL**.
3. Enter one or more URLs (one per line).

   You must enter the entire URL (http / https, the domain, and any desired path / arguments).
4. Enter **Timeout** (in milliseconds). This time is used for each URL attempt.
5. Enter a **Name**.
6. Enter a **Description**.
7. Select the **Attack Vector**.
8. Select the **Attacker Location**.
9. Select the **Behavior Type**.
10. Select the **Covert** option (Yes or No).
11. Select the **OS/Platform**.
12. Select the **Stage of Attack**.
13. (Optional) Enter or select **User Tags**.
14. Click **Save Captive IOC Action**.
    The Action Library is displayed. A confirmation message that your Action was created successfully is shown and the Action is selected and displayed in the Action preview.



Add Action - Captive IOC URL