Mandiant

CAPTIVE IOC ACTION OVERVIEW

One of the features included with the TAAM license is the ability to Run Captive IOC (Indicators of Compromise) Actions. These Actions allow for the safe evaluation of defensive performance related to blocking communication with publicly routable destination addresses for a Threat Actor.

You can create URL-based and PCAP-based Actions, as well as run any PCAP Action that includes HTTP traffic as a Captive IOC Action. Before running these Actions, you must first configure the Captive IOC Action Settings and enable Actors to run them.

Challenge

Customers need a way to test/validate their security controls and analytics against network traffic using known-bad IP addresses and FQDNs.

- URL classification validation
  - Can my users get to a bad website or will my controls classify it and stop it appropriately?
- Testing analytical/correlation/machine learning/AI models
  - Example: If our systems begin contacting known bad C2 domains, will my systems alert me appropriately?
- The problem is that in a production network, sending traffic to a known-bad IP or FQDN goes to the bad actor target and introduces risk
  - The nature of IP is that if traffic is sent to 5.5.5.5, it routes it to 5.5.5.5

Solution

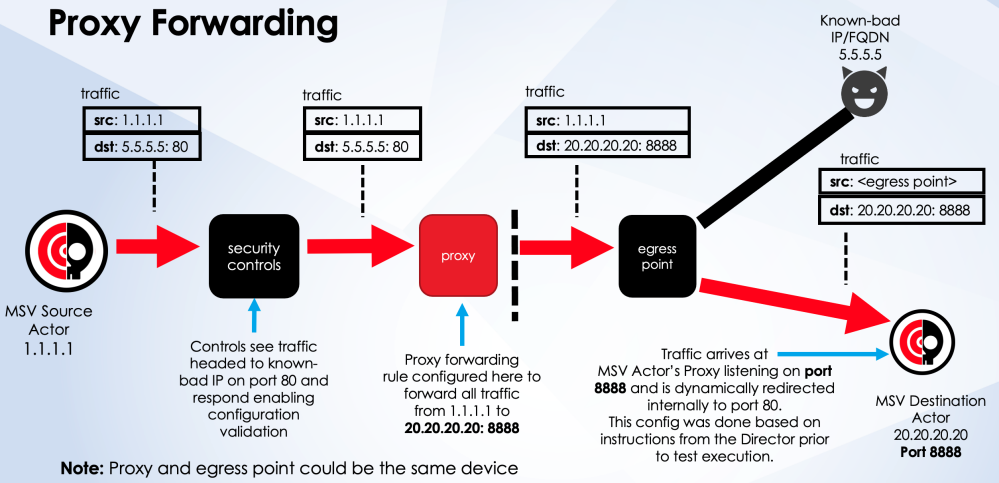
- Combination of changes in MSV and a network config change in the customers environment enable the controls being tested to see the real known-bad IP in a production network safely.
- Allow the user an option to preserve the original IP/FQDN addresses from the PCAP (or other test source) with the MSV test's metadata.
  - Additionally, the user could override the destination IP/FQDN at runtime.
- At execution time, while the source IP will be the source MSV Actor, the destination IP will be set to the known-bad IP address and sent to it.
- In combination with the above, a customer would need to make one of two network changes.

Requirements

- Network Actor running CentOS
- Your license must include the Threat Actor Assurance Module.

Proxy Forwarding

- For this option, the customer would need a proxy that supports source-based proxy chaining located at or near the edge of their data transfer point (or at least "past" the other controls being tested, if there are others).
- The customer would write a rule for their proxy to forward all traffic from the MSV Source Actor's IP to the MSV Destination Actor's proxy IP/port (new).
- This would cause the traffic to go through the customer's network with the real known-bad IP address up until it hits the proxy with this rule.
- At that point, the traffic would be dynamically redirected to the MSV Destination Actor's IP/proxy port and never arrive at the actual bad site.
- The MSV Destination Actor acts as an upstream proxy listening on port 8888 for the Action then forwards it to port 80 on the Destination Actor web server.



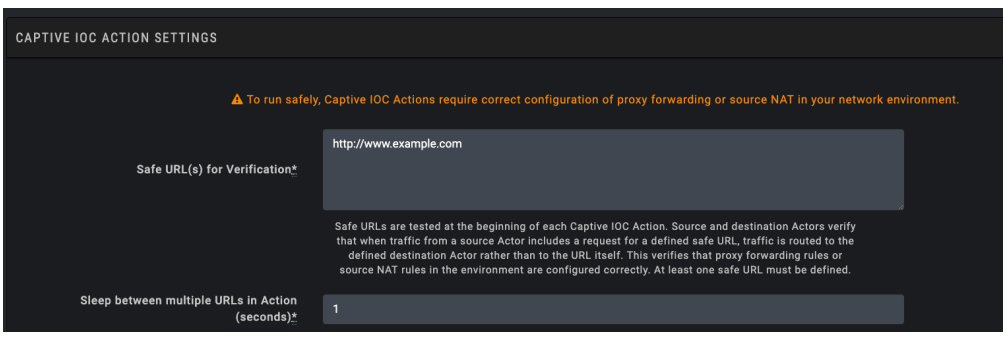
Configuration Requirements

Before running Captive IOC actions, the following settings must be configured (see section 7.1 within the TAAM Guide for more information):

- **Safe URLs**
  - Verifies traffic gets to the Actor when Actions are run.
  - Verifies that Proxy Forwarding Rules or Source NAT rules are configured correctly.
- **Captive IOC Communication Rules**
  - Defines how communications run between two Captive IOC actors will occur when running a Captive IOC actions.
- **Enable IOC Actors**
  - To run Captive IOC Actions, Actors must have Captive IOC enabled.
- **OPTIONAL: Configure Proxy Rules**
  - If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. To set up the rule and assignment, go to **Proxy Rules Settings**.

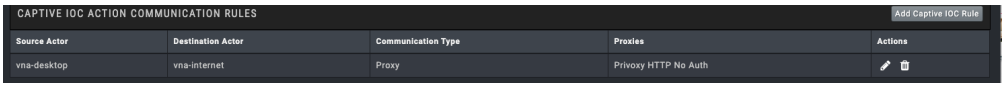
Setup: Safe URL

- Required to have at least 1 safe URL entered.
- Choose a URL that is not commonly used to ensure caching is not an issue.
- Verifies traffic gets to the Actor when Actions are run.
- Also verifies that Proxy Forwarding Rules or Source NAT rules are configured correctly.

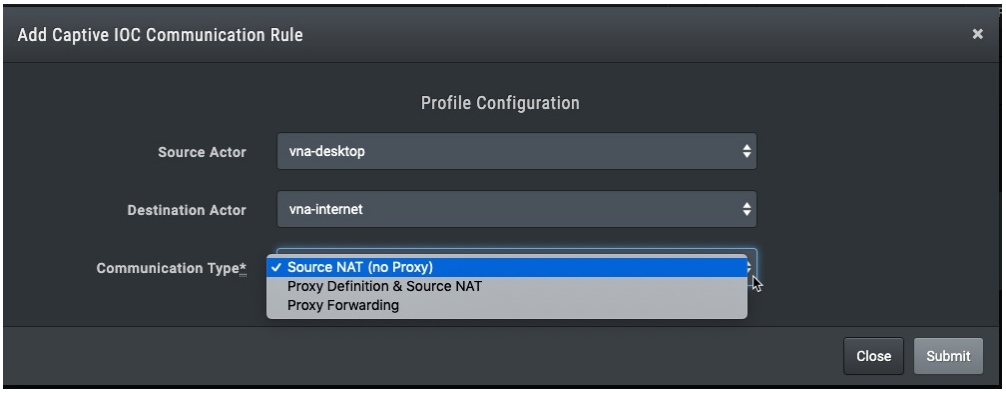


Setup: Captive IOC Communication Rules

- These rules define how communication between 2 actors will occur when running an IOC Action.
- Click **Add Captive IOC Rule** to add a new rule



- Add IOC Comm Rule
- Select the Source and Destination Actor
- Choose Comm Type
- Click Submit



Note: If you select one of the proxy types, you will be prompted to select a proxy to use.

Setup: IOC Actors

- Enable Actors for IOC by editing the Actor
- Environment > Actors >
- Edit Actor > Set Captive IOC Enabled to **Yes**
- Click Update Actor