

ACTION Attributes Used by the Threat Mitigation Application

The SRC-TMP displays the configured attributes for the actions that are used by the Threat Mitigation Application.

serviceName

- Service activated in response to an attack.
- Value—Text string

The following values are passed to the service as parameter substitutions:

- category—Name of the category
 - subcategory—Name of the subcategory
 - severity—Severity level as a number in the range 0–5
 - 0—not set
 - 1—info
 - 2—warning
 - 3—minor
 - 4—major
 - 5—critical
- srcAddr—IP address; enclose in single quotes if not in IPv4 format
- srcPort—Port number
- dstAddr—IP address; enclose in single quotes if not in IPv4 format
- dstPort—Port number
- protocol—Protocol number
- user—Username
- app—Name of the application
- uri—Uniform resource identifier

The category, subcategory, user, app, and uri parameters are encoded as valid parameter names (not text strings) so that these parameter values can be provided to the policies.

For example, you could define a policy that takes the app parameter as the value for a policer rate with a default value of 64000. Then, you could define global parameters named after different applications, such as http = 32000. When the attack includes an HTTP application, the Threat Mitigation Application would pass app = http, and 32000 would be the value in the policer definition.

- Example—BlockAttacker

name

- Name of action; displayed in the Action drop-down list.
- Value—Text string
- Example—Block Attacker

description

- Description of the action; displayed in the Action Help page.
- Value—Text string
- Example—This action blocks all traffic to and from the attacker.