

## ATTACK\_TYPE Attributes Used by the Threat Mitigation Application

---

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

### ***category***

- Category of the attack; displayed in the Attack Details page.
- Value—Text string
- Examples
  - DEFAULT
  - predefined

### ***subcategory***

- Subcategory of the attack; displayed in the Attack Type column.
- Value—Text string
- Examples
  - DEFAULT
  - FTP:USER:ROOT
  - ICMP:EXPLOIT:FLOOD

### ***definingAttributes***

- Attributes used to identify an attack. Defining attributes determine whether an attack is a new record or an update to an existing attack record. The srcAddr attribute is always considered a defining attribute for the attack, even if it is not specified as a defining attribute.
- Value—List of defining attributes separated by semicolons
  - srcAddr—Source address; displayed in the Source column
  - srcPort—Source port; displayed in the Attack Details page
  - dstAddr—Destination address; displayed in the Destination column
  - dstPort—Destination port; displayed in the Attack Details page
  - protocol—Protocol; displayed in the Attack Details page
  - user—User; displayed in the Attack Details page
  - app—Application; displayed in the Attack Details page
  - uri—Uniform resource identifier; displayed in the Attack Details page
- Examples
  - srcAddr

- srcAddr;dstAddr;dstPort
- srcAddr;dstAddr

***description***

- Description of the attack; displayed in the Attack Details page.
- Value—Text string
- Examples
  - There is no specific information for this type of attack.
  - This attack indicates an ICMP session that contains more than 250 ICMP packets per second. This may indicate that an attacker is trying to degrade network performance, causing poor service for legitimate users.