

Overview of the SRC-TMP

The SRC-TMP provided with the SRC software is designed to be used with the sample data for the Threat Mitigation Application. The SRC-TMP is a Web application that lets you use a Web browser to manage threats.

Once you have configured and deployed the Threat Mitigation Application, you can use the SRC-TMP to manage attack events.

When the NetScreen-Security Manager reports incidents to the SRC-TMP, the SRC-TMP:

- Provides a description of the incident, including source IP address, destination IP address, attack type, severity, time of first received record, time of last received record, count of repeated attacks, and possible actions.
- Allows the administrator to choose how to handle the threat in the appropriate manner by taking action, activating or deactivating a service, or managing an action already taken.
- Displays general information if the SRC software cannot collect information about an attack type because it is not defined in the ATTACK_TYPE table.

About the Record Servlet

The record servlet receives messages from the SRC **thm.py** script that runs in NetScreen-Security Manager. The **thm.py** script posts messages to a specified URL. The default pathname in the URL is /thmp/record. For information about changing the default pathname, see Configuring the Threat Mitigation Application.

NetScreen-Security Manager sends the following information from its XML schema to the record servlet for display in the SRC-TMP.

- **dayId**—Date of the record as displayed in the Attack ID column to the left of the colon.
- **recordId**—Identifier for the record as displayed in the Attack ID column to the right of the colon.
- **timeReceived**—Time the attack event is received as displayed in the First Received Time and Last Received Time columns.
- **subCategory**—Subcategory of the attack as displayed in the Attack Type column.
- **srcAddr**—Source address of the attack as displayed in the Source column.
- **dstAddr**—Destination address of the attack as displayed in the Destination column.
- **severity**—Severity of the attack as displayed in the Severity column.
- **repeatCount**—Number of occurrences of the attack as displayed in the Repeat Count field.

The record servlet maps an attack ID with an attack type and its defining attributes (including protocol, source address, source port, destination address, destination port, user, application, uri). If the servlet receives more than one record for the same attack type with the same defining attribute values, the servlet stores the record with

that attack ID once and increases the value of Repeat Count for that attack ID by one for each subsequent occurrence. The record servlet also records the highest severity of all attacks with the same defining attribute values and updates the last received timestamp.

If applicable, the SRC-TMP displays the following information in the Attack Details page.

- category—Category of the attack; displayed in the Attack Type field.
- subCategory—Subcategory of the attack; displayed in the Attack Type field.
- srcAddr—Source address of the attack; displayed in the Source field.
- srcDns—The result of a reverse DNS lookup on the source address of the attack; displayed in the Source DNS field as a comma-separated list.
- srcPort—Source port of the attack; displayed in the Source Port field.
- dstAddr—Destination address of the attack; displayed in the Destination field.
- dstDns—The result of a reverse DNS lookup on the destination address of the attack; displayed in the Destination DNS field as a comma-separated list.
- dstPort—Destination port of the attack; displayed in the Destination Port field.
- protocol—Protocol of the attack; displayed in the Protocol field.

Related Topics

- Overview of Configuring and Deploying the SRC-TMP
- Accessing the SRC-TMP
- Installing and Initially Configuring the Threat Mitigation Application
- For information about the SRC **thm.py** script that runs in NetScreen-Security Manager, see Enabling Actions from NetScreen-Security Manager