CHAPTER 20

Configuring and Generating Reports

This chapter describes IME reports and how to configure and generate them. It contains the following topics:

- Understanding IME Reporting, page 20-1
- Configuring and Generating Reports, page 20-2

Understanding IME Reporting

IME lets you create different reports that you can customize using different filters. A report consists of a window with a bar or pie chart along with the tabular data used for the graphs. There are four types:

- Top Attacker—Shows top attacker IP addresses for a specified time. You specify the top number of attacker IP addresses.
- Top Victim—Shows top victim IP addresses for a specified time. You specify the top number of victim IP addresses.
- Top Signature—Shows top signatures fired for a specified time. You specify the top number of signatures.
- Attacks Over Time—Shows the attacks over a specified time.

These reports show the number of top attackers, victims, signatures matched, and total attacks during a specific time period. There are also user-defined reports and demo reports that are predefined examples of reports.

The Reports window is divided in to two parts: the left-hand pane, the Report tree, shows the reports list in the form of a tree, and the right-hand pane, the Report Settings pane, contains the report. The Report tree contains a set of predefined reports, such as Basic Top Attacker, and a user-defined report under the My Reports node. When you select a report in the list and click **Generate Report**, the corresponding report containing a graph and a table is displayed in the lower half of the Report Settings pane. The Reports Setting pane contains two tabs, General and Filter, which let you customize the report.

Note The filtering fields now support IPv6 and IPv4 addresses.

Configuring and Generating Reports

You can customize your report by configuring the number of items you want in your report and what the time interval should be. You can also use DNS to resolve the IP addresses. You can also use filters to further refine the type of information you want your report to contain.

Note The filtering fields now support IPv6 and IPv4 addresses.

To configure and generate reports, follow these steps:

Step 1 In the Report tree, click **New**, and then in the New Report dialog box, enter the name of the new report, choose the type of report from the drop-down list, and then click **OK**.

Your new report shows up under My Reports in the Report tree.

Step 2 Select your report, and on the **General** tab, configure the settings for your report:

a. In the Report Description field, enter a description for this report.

b. In the Top field, enter how many top events you want to see in this report.

c. Check the **Resolve Addresses Using DNS** check box, if you want to use DNS address resolution.

d. Configure the time interval for this report, either the duration or enter a custom time.

Step 3 On the **Filter** tab, from the Filter Name drop-down menu, choose the filter name, or to add a filter, click the **Note** icon.

Step 4 Click **Generate Report**.

Your report shows up in the bottom half of the Report Settings pane, displaying the statistics in graph and table form.

Step 5 To customize the display, choose Bar or Pie Chart in the **Display Type** drop-down menu.

Step 6 Click **Print** to print the report, or click **Save** to save the report in PDF or RFT format to your hard-disk drive.

Step 7 To see events for a single IP address, choose the IP address from the Events for drop-down list.

For More Information

- For the procedure for creating a filter, see Configuring Filters, page 3-14.
- For the procedure for configuring events for single IP addresses, see Working With a Single Event for Individual Top Attacker and Victim IP Addresses, page 3-12.
- For the procedure for configuring events for single signatures, see Working With a Single Event for a Top Signature, page 3-13.