CHAPTER 19

Configuring Event Monitoring

This chapter describes IME event monitoring and how to configure it. It contains the following sections:

Understanding Event Monitoring

The Event Viewer contains views—a window of events either in real time or historical time (events stored in the database). IME contains predefined views and you can also create your own views. You cannot delete or save changes to the predefined views. The left-hand side of the Event Monitoring window is a view tree, and the right-hand side contains the view.

The Event Viewer pane consists of three parts:

- Settings tab—You can specify what events and how you want to see events. You can specify filters, grouping, or coloring.

  You can use color so that certain specific data stand out. For example, if you are looking for events from a certain attacker IP address, you can highlight the events with the severity level as high and then apply a certain color to those event
- Events table—Displays the events. You can interface with events by selecting a row and then performing various actions using the toolbar or the right-click menu.
- Event Details—Select a single row in the Events table and the details for that event are displayed in the Event Details section of the pane.

You can create filters based on a variety of criteria so that only the information you want to see is shown in your view. You can group events in single levels or columns, or according to the following criteria:

- None
- Severity
- Attacker IP address

- Victim IP address
- Signature ID
- Signature Name
- Threat rating
- Risk rating
- Device

Understanding Grouping and Color Rules

Grouping lets you group events based on the attributes of an event. Up to four levels of nested grouping are allowed. For example, you can group on severity, then on Attacker IP address, and so forth.

Color rules let you select events based on specific criteria and then apply different background and foreground colors to those events. The selection criteria is the same as that for creating filters. You must apply the colors from top to bottom. At the first match, the color rule is applied.

Understanding Filters

You can configure filtering properties for specific views in IME, thus allowing you to view only the events you want to see. If you do not apply filters to events, you see all events; otherwise, with a filter applied, you see only the events that match the criteria specified in the filter.

For example, if you are interested in all events that have high severity, you can create a filter with the **High** check box checked in the Severity section of the filter. This filter will then show only events that have a high severity.

You can use predefined filters or add new ones. You cannot edit or delete the predefined filters. You can enter comma-separated values in each field. Each field supports single entries, ranges, and NOT operations. For example, the attacker IP address supports the following formats:

- 10.1.1.1,10.1.1.5
- 10.1.1.1-10.1.1.15
- ! 10.1.1.1

Using filters, you can run queries, such as the following:

- Show events with attacker IP 10.1.1.1 or 10.1.1.5 and Sig ID 5042
- Show events with a risk rating 75-100 and attacker IP address 192.2.3.3

Risk rating, threat rating, and destination port fields support the following formats:

- =
- !=
- >
- >=
- <
- <=

- in the range
- not in the range

The Manage Filters dialog box displays these filter definitions.

Filter Pane Field Definitions

The following fields are found in the Filter pane:

- Filter Name—Lets you name this filter.
- Attacker IP—Attacker IP address you want to include in this filter.

  The valid values are *ip_address*, *ip_address_range*, for example, 10.0.0.1, !10.0.0.1, !10.1.1.1.
- Victim IP—Victim IP address you want to include in this filter.

  The valid values are *ip_address*, *ip_address_range*, for example, 10.0.0.1, !10.0.0.1, !10.1.1.1.
- Signature Name/ID—Signature Name/ID you want to include in this filter.

  The valid values are *signature_name* or *signature_id* or *signature_id/subsig_id* or *signature_id_range*, for example:
  - no_checkpoint
  - no_checkpoint, 3320
  - no_checkpoint, 3320/1
  - 3300-400
- Victim Port—Victim port you want to include in this filter.

  The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Severity—Severity levels you want to include in this filter.
- Risk Rating—Risk rating you want to include in this filter.

  The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Threat Rating—Threat rating you want to include in this filter.

  The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Action(s) Taken—Lets you choose which actions the filter looks for in the alerts.

  The actions are a string that you can chose or you can enter free format strings.
- Sensor Name(s)—Lets you assign which sensors are included in this filter.
- Virtual Sensor—Lets you assign which virtual sensors are included in this filter.
- Status—Lets you assign a status to this filter (All, New Assigned, Closed, Detected, Acknowledged).

  The Status field is useful, for example, in a situation where you want to save analysis of certain events for later. You can add a note and change the status to ‘Acknowledged,’ and then later you can filter by status to see all cases that are acknowledged and then do further analysis.
- Victim Locality—An alert attribute in the participants/address alert on which you can filter. It is defined in the event action rules variables.

Working With Event Views

To work with event views, follow these steps:

Step 1 Choose **Event Monitoring > Event Monitoring > Event Views**.

There are three predefined views: Basic View, Grouped By Severity View, and Real-Time Colored View.

The events appear in the lower half of the View pane.

Step 2 To create a view, click **New**.

Step 3 In the New View dialog box, enter a name for the view in the Name field, and then click **OK**.

The new view now appears in the left part of the pane under My Views.

You can work with a single event and apply and create filters for your view.

For More Information

- For the procedure for working with a single event, see Working With a Single Event, page 19-4.
- For the procedure for applying and creating filters for your view, see Configuring Filters for Event Views, page 19-5.

Working With a Single Event

To work with a single event, follow these steps:

Step 1 Chose **Event Monitoring > Event Monitoring > Event Views > Basic View**.

Step 2 Configure the time period from which you want to gather events.

Step 3 To work with a single event, select the event in the list, and then click **Event** on the toolbar.

From the Event drop-down list, you can view the following information (it also appears in the lower half of the window under Event Details displayed in tab form):

- Summary—Summarizes all of the information about that event.
- Explanation—Provides the description and related signature information about the signature associated with this event.
- Related Threats—Provides the related threats with a link to more detailed information in MySDN.
- Trigger Packet—Displays information about the packet that triggered the event.
- Context Data—Displays the packet context information.
- Actions Taken—Lists which event actions were deployed.
- Notes—Lets you take action on this event by assigning a designation for it (New, Assigned, Acknowledged, Closed, or Deleted). Add any notes in the Notes field and click **Save Note** to save it.

Step 4 To print the details of this event, click **Show All Details** to display the event details in a printer-friendly window.

Step 5 To add an attribute from a selected event, from the Filter drop-down menu, click **Add to Filter > Attacker IP/Victim IP/Signature ID**.

The Filter tabs appear in the upper half of the window.

Step 6 To create a filter from this event, from the Filter drop-down menu, click **Create a Filter**.

Step 7 To edit the signature associated with this event, click **Edit Signature**.

This takes you to **Configuration >** ***sensor_name*** **> Policies > Signature Definitions > sig0 > Active Signatures** where you can edit the signature.

Step 8 To create an event action rules filter from this event, click **Create Rule**.

This takes you to **Configuration >** ***sensor_name*** **> Policies > IPS Policies > Add Event Action Filter** where you can add the event action rules filter.

Step 9 To stop the attacker, from the Stop Attacker drop-down menu, choose one of the following options:

- Using Inline Deny

  This takes you to **Configuration >** ***sensor_name*** **> Sensor Monitoring > Time-Based Actions > Denied Attackers > Add Denied Attacker**.

- Using Block on another device

  This takes you to **Configuration >** ***sensor_name*** **> Sensor Monitoring > Time-Based Actions > Host Blocks > Add Host Block**.

Step 10 To use ping, traceroute, DNS, and whois on the IP addresses involved in this event, choose them from the Tools drop-down menu.

Step 11 To save, delete, or copy the event, from the Other drop-down list, choose the action you want to perform.

Step 12 To save any changes that you have made to the view, click **Apply**. To discard any changes, click **Reset**.

For More Information

- For the procedure for adding filters, see Configuring Filters for Event Views, page 19-5.
- For the procedure for adding an event action rules filter, see Configuring Event Action Filters, page 11-14.
- For the procedure for adding a denied attacker, see Configuring and Monitoring Denied Attackers, page 18-4.
- For the procedure for adding a host block, see Configuring and Managing Host Blocks, page 18-7.
- For more information on these tools, see Using Tools for Devices, page 2-5.

Configuring Filters for Event Views

To configure filters, follow these steps:

Step 1 Chose **Event Monitoring** and then click **New**.

Tip To select more than one item in the list, hold down the **Ctrl** key.

Step 2 In the New View dialog box, enter the name of the new view.

The new view appears under My Views in the View tree.

Step 3 Click **View Settings > Filter**.

Step 4 From the Filter Name drop-down menu, choose the filter name for this filter, or click the **Note** icon and then click **Add** to add a new filter:

Note The filtering fields now support IPv6 and IPv4 addresses.

a. In the Filter Name field, enter a name for this filter.

b. In the Attacker IP field, enter an attacker IP address, or click the **Note** icon and add a unique IP address or a range of IP addresses, and then click **OK**.

c. In the Victim IP field, enter a victim IP address, or click the **Note** icon and add a unique IP address or a range of IP addresses, and then click **OK**.

d. In the Signature Name/ID field, enter a signature name or ID, or click the **Note** icon, and then choose a signature type, and click **OK**.

e. In the Victim Port field, enter a victim port, or click the **Note** icon and enter a victim port that meets the conditions you require, and then click **OK**.

f. Choose the severity levels you want for this filter.

g. In the Risk Rating field, enter the risk rating for this filter, or click the **Note** icon, and then enter the risk rating that meets the conditions you require, and click **OK**.

h. In the Threat Rating field, enter the threat rating for this filter, or click the **Note** icon, and then enter the threat rating that meets the conditions you require, and click **OK**.

i. In the Actions Taken field, enter the actions you want to trigger this filter, or click the **Note** icon, and then check the check boxes of the actions that you want to trigger this filter, and click **OK**.

j. In the Sensor Name(s) field, enter the names of the sensors that are affected by this filter, or click the **Note** icon, and check the check boxes of the sensor to which this filter applies and click **OK**.

k. In the Virtual Sensor field, enter the virtual sensor to which this filter applies.

l. From the Status drop-down menu, choose on which status you want to filter.

m. In the Victim Locality field, enter the name of any event action rules variable that you created on which you want to filter.

Step 5 To configure grouping, click the **Group By** tab:

n. Check the **Group events based on the following criteria** check box, and then set up the hierarchy of how you want to group the events by selecting the category from the drop-down menus.

o. Under Grouping Preferences, you can check the check boxes of the **Single Level**, **Show Group Columns**, or **Show Count Columns** check boxes.

You can only show count columns if you enable Show Group Columns.

Step 6 To add color rules, click the **Color Rules** tab, and then click **Add**.

a. In the Filter Name field, enter a name for this color rules filter.

b. Check the **Enable** check box.

Note If you do not check the **Enable** check box, your color rules filter will not go in to effect.

c. Under Packet Parameters, enter the IP addresses, signature names and/or victim ports for which you want this color rules filter to apply.

d. Under Rating and Action Parameters, enter the severity, risk rating, threat rating, and actions for which you want this color rules filter to apply.

e. Under Other Parameters, enter the sensor name, virtual sensor name, status, and/or victim locality for which you want this color rules filter to apply.

f. Under Color Parameters, choose the foreground and background colors, and the font type for this color rules filter, and then click **OK**.

Tip For aid in entering the correctly formatted values for these fields, click the **Note** icon.

Step 7 To event fields and their order, click the **Fields** tab, and then click **Add >>**, **<< Remove**, **Move Up**, and **Move Down** to chose which fields you want to display and to arrange the fields in the order in which you want to see them.

Step 8 Click the **General** tab, and then in the View Description field enter a description for your view.

Step 9 Click **Save As** to create the new view, and then in the Name field, enter a name for your view.

The settings are copied to the new view.

Step 10 Click **Save** to save any changes to the view.

Your filter now appears in the Filter Name drop-down menu.

Step 11 To save any changes that you have made to the view, click **Apply**. To discard any changes, click **Reset**.