Integrate TippingPoint
EventTracker Enterprise
Abstract

This guide provides instructions to configure TippingPoint to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.x and later, and TippingPoint for the S-Series (330) IPS device, TOS version 3.6.4 and 3.6.5.

Audience

Administrators, who are responsible for monitoring TippingPoint using EventTracker Enterprise.
# Table of Contents

Abstract .................................................................................................................................................. 1  
Scope .................................................................................................................................................. 1  
Audience ............................................................................................................................................. 1  
Introduction ........................................................................................................................................... 3  
Pre-requisites ........................................................................................................................................ 3  
Integration Method for TippingPoint .................................................................................................... 3  
EventTracker Knowledge Pack (KP) ....................................................................................................... 5  
  Categories .......................................................................................................................................... 5  
  Alerts .................................................................................................................................................. 5  
  Flex Reports ....................................................................................................................................... 5  
Import TippingPoint knowledge pack into EventTracker ...................................................................... 6  
  Category ............................................................................................................................................. 7  
  Alerts ................................................................................................................................................ 9  
  Templates ........................................................................................................................................ 10  
  Knowledge Object ............................................................................................................................ 11  
  Flex Reports ..................................................................................................................................... 13  
Verify TippingPoint knowledge pack in EventTracker ......................................................................... 14  
  Category ........................................................................................................................................... 14  
  Alerts .............................................................................................................................................. 14  
  Templates ....................................................................................................................................... 15  
  Knowledge Object ............................................................................................................................ 16  
  Flex Reports ..................................................................................................................................... 16  
Create Flex Dashboards in EventTracker ............................................................................................... 17  
  Schedule Reports ............................................................................................................................ 17  
  Create Dashlets ............................................................................................................................... 19  
Sample Flex Dashboards .................................................................................................................... 22
Introduction

The TippingPoint Next-Generation Intrusion Prevention System (IPS) offers comprehensive threat protection against advanced and evasive targeted attacks with high accuracy. Using a combination of technologies such as deep packet inspection, threat reputation and advanced malware analysis, it provides enterprises with a proactive approach to security.

EventTracker collects the logs, helps administrator to analyze the events and generate the reports for the TippingPoint IPS traffic being allowed or blocked.

Pre-requisites

- EventTracker v7.x or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.
- TippingPoint 330 IPS module must be configured.

Integration Method for TippingPoint

1. Log into IPS Local Security Manager (LMS) with valid credentials.

   ![Local Security Manager](image1)

   **Figure 1**

2. On IPS LMS Expand System then select Syslog Servers.
3. Enable System Log, Audit Log and Quarantine log.
4. Enter the IP address of EventTracker Manager Machine.
5. Click on APPLY to save.
NOTE: Once Syslog Server destination is configured, events must be sent via the Action Sets Contact(s) to forward to Remote system (Syslog) and Management Console. Both steps must be configured before logs are sent.
EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and reports can be configured into EventTracker.

The following Knowledge Packs are applicable in EventTracker v7.x and later to support TippingPoint.

Categories

- **TippingPoint: IPS traffic allowed**
  This category provides information related to IP traffic allowed on the network.

- **TippingPoint: IPS traffic blocked**
  This category provides information related to IP traffic blocked on the network.

Alerts

- **TippingPoint: IPS traffic blocked**
  This alert is generated if the IP traffic is blocked when an attack is detected by the TippingPoint IPS.

Flex Reports

- **TippingPoint-IPS traffic allowed**
  This report provides the information related to IP traffic being allowed based on the rules configured on TippingPoint IPS.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device Name</th>
<th>Alert Severity</th>
<th>Alert Message</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Action</th>
<th>Security Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 10 08:11:54</td>
<td>IPS01</td>
<td>Minor</td>
<td>ICMP: Redirect</td>
<td>90.138.157.173</td>
<td>0</td>
<td>90.138.157.175</td>
<td>0</td>
<td>icmp</td>
<td>Permit - Notify</td>
<td>ANY-ANY</td>
</tr>
</tbody>
</table>

Figure 4
Logs Considered:

- **TippingPoint-IPS traffic blocked**

  This report provides the information related to IP traffic being blocked when an attack is detected based on the rules configured on TippingPoint IPS.

Logs Considered

Import TippingPoint knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence

- Categories
- Alerts
- Templates
EventTracker: TippingPoint

- Flex Reports
- Knowledge Objects

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility.

![EventTracker Control Panel](image)

3. Click the Import tab.

**Category**

1. Click Category option, and then click the browse button.
2. Locate the All TippingPoint group of categories.iscat file, and then click Open button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

4. Click the **OK**, and then click the Close button.
Alerts

1. Click Alerts option, and then click the browse button.

2. Locate the All TippingPoint group of alerts.isalt file, and then click the Open button.

![Figure 11]

2. To import alerts, click the Import button.
   EventTracker displays success message.

![Figure 12]

3. Click OK, and then click the Close button.
Templates

1. Click the Admin menu, and then click Parsing rule.

2. Select Template tab, and then click on Import option.

3. Click on Browse button.

4. Locate All TippingPoint group of templates.ettd file, and then click the Open button.
5. Now select the check box and then click on 'Import' option. EventTracker displays success message.

Figure 16

6. Click OK, and then click the Close button.

Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects.
2. Click on 'Import' option.
3. In IMPORT pane click on Browse button.

4. Locate All TippingPoint group of knowledge object.etko file, and then click the UPLOAD button then OVERWRITE.
Flex Reports

1. Click **Reports** option, and then click the browse button.

2. Locate the **All TippingPoint group of flex reports.issch** file, and then click the **Open** button.

![Figure 20](image)

3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

![Figure 21](image)
Verify TippingPoint knowledge pack in EventTracker Category

1. In the EventTracker Enterprise web interface.
2. Click the Admin dropdown, and then click Categories.
3. In the Category Tree, search TippingPoint to see the imported categories.

Alerts

1. In the EventTracker Enterprise, web interface, click the Admin dropdown, and then click Alerts.
2. In the Search field, type 'TippingPoint', and then click Go button.

Alert Management page will display all the imported TippingPoint alert
3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Successfully saved configuration.](image)

**Figure 24**

4. Click the **OK** button, and then click the **Activate now** button.

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

**Templates**

1. Click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on ‣ `'Import'` option.

**Figure 25**
Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects.
2. Scroll down and select TippingPoint in Objects pane. Imported TippingPoint object details are shown.

![Figure 26](image)

Flex Reports

1. In the EventTracker Enterprise, web interface.
2. Click the Reports menu, and then select Configuration.
3. In Reports Configuration pane, select Defined option.
4. In search box enter 'TippingPoint', and then click the Search button.
   EventTracker displays Flex reports of TippingPoint

![Figure 27](image)
## Create Flex Dashboards in EventTracker

**NOTE:** To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

### Schedule Reports

1. Open *EventTracker* in browser and logon.

   ![Figure 28](image)

2. Navigate to *Reports>Configuration*.

3. Select *TippingPoint* in report groups. Check *Defined* dialog box.

   ![Figure 29](image)

5. Click on ‘*schedule*’ to plan a report for later execution.
EventTracker: TippingPoint

Figure 30

Figure 31
6. Check column names to persist using PERSIST checkboxes beside them. Choose suitable Retention period.
7. Proceed to next step and click Schedule button.
8. Wait till the reports get generated.

Create Dashlets

1. Open EventTracker Enterprise in browser and logon.

![Dashboard pane](image)

Figure 32

2. Navigate to Dashboard>Flex.
   Flex Dashboard pane is shown.

![Flex Dashboard](image)

Figure 33
3. Fill suitable title and description and click **Save** button.
4. Click to configure a new flex dashlet. Widget configuration pane is shown.

**WIDGET CONFIGURATION**

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.
14. If satisfied, click **Configure** button.

15. Click ‘customize’ to locate and choose created dashlet.
16. Click to add dashlet to earlier created dashboard.
Sample Flex Dashboards

For below dashboard **DATA SOURCE: TippingPoint: IPS traffic allowed**

1. **TippingPoint: IPS traffic allowed**
   - **WIDGET TITLE:** IPS traffic allowed by Source IP
   - **CHART TYPE:** Donut
   - **AXIS LABELS [X-AXIS]:** Source IP
   - **Label Text:** Source IP

![IPS Traffic Allowed by Source IP](image)

*Figure 37*
For below dashboard **DATA SOURCE: TippingPoint: IPS traffic blocked**

2. **TippingPoint: IPS traffic blocked by source IP**
   - **WIDGET TITLE:** IPS traffic blocked by source IP
   - **CHART TYPE:** Stacked column
   - **AXIS LABELS [X-AXIS]:** Source IP
   - **Label Text:** Source IP

![IPS Traffic Blocked by Source IP](image)

*Figure 38*