The Trend Micro TippingPoint app contains pre-configured dashboards that highlight blocked and permitted attacks in your environment. You can also track security policy and Digital Vaccine updates and retrieve PCAPS when available.

A Security Management System (SMS) is required to send data to Splunk.

**SMS configuration**

SMS configuration includes creating a Splunk syslog format and configuring a syslog exporter to send events and messages to Splunk.

- **Create a Splunk syslog format**
- **Configure syslog exporter to send events to Splunk**
- **Configure syslog exporter to send messages to Splunk**

**Create a Splunk syslog format**

To integrate Splunk with the SMS, first create a Splunk syslog format. Splunk requires data in a specific format from the SMS.

**Procedure**

1. On the SMS, select Admin > Server Properties > Syslog.
2. Under Syslog Formats, click New.
3. Select Events from the Log Type drop-down list.
4. Enter a name and description.
5. Enter the syslog pattern, as shown below:

```plaintext
CEF:0|TippingPoint|UnityOne|1.0.0.17|${signatureNumber}|${filterName}|${severity}|
appl=${protocol} cnt=${hitCount} dst=${destAddressv4} dpt=${destPort}|
act=${flowControl} cn1=${vlanTag} cn1Label=${VLAN ID} cn2=${taxonomyID}|

A Security Management System (SMS) is required to send data to Splunk.

7. Click OK.

Configure syslog exporter to send events to Splunk

After you create a Splunk syslog format, you can configure the syslog exporter to send device events, including packet trace files, from the SMS to Splunk.

Procedure

1. On the SMS, select Admin > Server Properties > Syslog.


3. Select the Enabled check box.

4. Enter the IP address of the Splunk server in the Syslog Server field.

5. Select a Protocol.

6. Enter 514 for the Port number.

7. Select the Splunk syslog format from the Log Type drop-down list.

8. Select pipe from the Delimiter drop-down list.

9. Select Include SMS Hostname in Header to send packet trace files.
10. Select **Send New Events/Log Only**.

11. Click **OK**.

![Create Remote Syslog Notification Settings](image)

**Configure syslog exporter to send messages to Splunk**

After you create a Splunk syslog format, you can configure the syslog exporter to send SMS audit messages to Splunk. SMS audit messages also include Digital Vaccine and profile distribution history information.

**Procedure**

1. On the SMS, select **Admin > Server Properties > Syslog**.
3. Select the Enable check box.
4. Enter the IP address of the Splunk server in the Syslog Server field.
5. Select a Protocol.
6. Enter 8514 for the Port number.
7. Select SMS Audit from the Log Type drop-down list.
8. Select a query from the Event Query drop-down list.
9. Select Log Audit from the Facility drop-down list.
10. Select a severity from the Severity drop-down list.
11. Select Pipe from the Delimiter drop-down list.
12. Click OK.

Install the TippingPoint Splunk app

To install the TippingPoint app on the Splunk Enterprise platform, select Apps > Browse more app and then search for TippingPoint.

Alternatively, you can directly download the app from the splunkbase https://splunkbase.splunk.com/app/3532/, and then select Install app from file.

Search and specify time ranges

Click Search on the TippingPoint Intrusion Prevention System app to perform a Splunk Enterprise search and to review your search history.

To filter Splunk data by time period or to adjust the time period, select a preset from the Period/Range. Data is sent to Splunk as it is generated. By default, data displays in real-time (All time). You can filter your results from the last minute, hour, day, week, or month. To narrow larger sets of data to a specific time period, you can configure your own custom date and time range.

To synchronize Splunk data, reload the page on your web browser.

Summary

Click Summary on the TippingPoint Intrusion Prevention System app to view the following event data:

• Top permitted attacks by filter name and hit count
• Top permitted sources by source IP address, hit count, and country
• Top permitted destinations by destination IP address, hit count, and country
• Top blocked or quarantined attacks by filter name and hit count
• Top blocked or quarantined sources by source IP address, hit count, and country
• Top blocked or quarantined destinations by destination IP address, hit count, and country
Action Based

Click **Action Based** on the TippingPoint Intrusion Prevention System app to view the following action sets:

- All
- Permitted - Top attacks by filter name, top sources, and top destinations
- Blocked - Top attacks by filter name, top sources, and top destinations
- Quarantined - Top attacks by filter ID, top attacks by filter name, top sources, and top destinations

Distribution History

Click **DV Distribution History** on the TippingPoint Intrusion Prevention System app to track Digital Vaccine and profile distributions. Digital Vaccine distributions include the version and distribution time for each device. Profile distributions include the profile name, device or segment, and the distribution time.

Packet Trace

Click **Packet Trace** on the TippingPoint Intrusion Prevention System app to view packet trace information for events on the SMS. You can search for packet trace information by Event ID.

To download a packet trace, copy and paste the **API Key** from the SMS, and then click **Download**. To access the API Key on the SMS, select **Admin > Authentication and Authorization > Users > Authentication**.

The following information displays.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Server Name</td>
<td>Domain name of the SMS server.</td>
</tr>
<tr>
<td>SMS Server IP</td>
<td>IP address of the SMS server.</td>
</tr>
<tr>
<td>Event ID</td>
<td>SMS event identifier (Event No).</td>
</tr>
<tr>
<td>Source IP</td>
<td>Source IP address for the event.</td>
</tr>
<tr>
<td>Source Port</td>
<td>Port of the source IP address.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Destination IP address for the event.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Port of the destination IP address.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Name of the IPS/TPS device that generate the event.</td>
</tr>
<tr>
<td>Segment Number</td>
<td>Segment for the event.</td>
</tr>
<tr>
<td>Event Time</td>
<td>The time that the event was created.</td>
</tr>
</tbody>
</table>