Flowmon Application for QRadar is an extension connecting IBM QRadar with events from Flowmon ADS Solution. Flowmon Application was built with our best practices in mind: it’s easy to use, offers intuitive drill-down from dashboard down to the individual flows to quickly resolve issues and to uncover malicious and suspicious behavior. It enables to view flows and events right in the QRadar without having to switch between two different interfaces while simultaneously taking advantage of the power of Flowmon Solution. This seamless integration is achieved by leveraging Flowmon REST API and syslog message standard. QRadar connector and correlation rules are pre-configured in an installation package.

This guide explains all the steps necessary to install, configure and start using the Flowmon Application for QRadar.
Installation

After downloading zip package from IBM X-Force Exchange to your computer open QRadar Console GUI, sign in to account with admin rights, open tab **Admin** (in some versions navigation menu, **Admin tab**), then click on **Extension Management** in the section **System Configuration**.

In newly opened window click on button “**Add**” and choose package that was previously downloaded.
Configuration

Before starting using application it must be configured. Configuration page is located in the tab Admin under the section Plug-ins (in some versions section Apps).

Main settings

Following screenshot illustrates connecting Flowmon Application to Flowmon public demo:

- Input address to Flowmon API. In case Flowmon Console GUI has the same IP address you can just check “Same as API address” - second address is used for generating links to open concrete event in the Flowmon Console GUI.
- Username and Password values are used for obtaining token, which is necessary for API calls. During the first configuration input that values into the fields. If you open configuration page once again after saving, field Password will remain empty - that is done for security reasons. If you want to leave the same password, just leave this field empty. In case you want to change password, input new value to this field.
- Due to possible long time of collecting data from Flowmon user can change Timeout value by himself. If you get notification that timeout was reached during usage of application too often, try to increase this value.
Flows output format

Corresponding columns in Flow view:

<table>
<thead>
<tr>
<th>Source IP address</th>
<th>Destination IP address</th>
<th>Start Time (UTC)</th>
<th>Duration</th>
<th>Protocol</th>
<th>Source port</th>
<th>Destination port</th>
<th>Bytes</th>
<th>Packets</th>
<th>TCP Flags</th>
<th>Input MAC address</th>
<th>Output MAC address</th>
<th>URG</th>
<th>ACK</th>
<th>PSH</th>
<th>RST</th>
<th>SYN</th>
<th>FIN</th>
<th>HEAD</th>
<th>App Tag</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>10.0.0.1</td>
<td>2016-07-20T23:23:25</td>
<td>2.027</td>
<td>0</td>
<td>0</td>
<td>84</td>
<td>3</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>192.168.0.1</td>
<td>2016-07-20T23:23:25</td>
<td>0.030</td>
<td>LDP</td>
<td>23097</td>
<td>138</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>192.168.0.1</td>
<td>2016-07-20T23:23:25</td>
<td>0.030</td>
<td>LDP</td>
<td>23097</td>
<td>138</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To save new configuration click button “Save” at the bottom part of the page.
Configuration in Flowmon Solution

Permissions

Create or edit role in Flowmon Configuration Center/System/User Settings with following permissions. It is recommended to create also a new user for Qradar concern.

Application requires access to Flowmon Monitoring Center (FMC) and Flowmon ADS:

Select at least one source. *All Sources* profile is always available as well as profiles for selected sources. Optionally, select additional profiles to make them available in application.
User permissions in Flowmon ADS Settings control which perspectives and filters are available in the application. All perspectives and filters are allowed by default. Optionally, select individual perspectives and filters in Flowmon ADS/Settings/User permissions.
Syslog

In Flowmon ADS, Processing page, Event reporting tab - Syslog configure syslog as illustrated in the screenshot below.

DNS Resolving

Please note that the domain name resolving user settings in Flowmon Solution has an immediate effect on values appearing in Flowmon ADS for QRadar (Event evidence and Flows).
Comparison of domain name resolving turned off / on (left / right):

- Autonomous system resolving
- Port name resolving
- Router resolving
- Type of service (ToS) resolving
Usage

Connector

Connector is delivered as separate extension and can be installed and used without installation of main application. It has no GUI or configuration page, because it consists only of custom rules, custom DSMs, QID records and other internal things in order to help QRadar in recognizing events from Flowmon ADS. Its installation process is the same as installation of main app. Furthermore, Flowmon must be configured to send events info to QRadar.

Connector installation

After downloading zip package with connector to your computer open QRadar Console GUI, sign in to account with admin rights, open tab Admin, then click on Extension Management in the section System Configuration.

In newly opened window click on button “Add” and choose package that was previously downloaded
After successful installation you will see new custom rules on the Offenses page.
Correlation rules

The main part of the Connector is custom rules with definitions of Flowmon ADS detection methods.

**Flowmon: ACCESSATTACK**
The method is aggregating the simple events informing about the attacks against authentication.

**Flowmon: Anomaly destination IP to list – Reference Set**
**Flowmon: Anomaly source IP to list – Reference Set**
These methods are adding suspicious IP addresses to designated reference sets.

**Flowmon: DATALEAKS**
The method is aggregating the simple events informing about possible data leaks.

**Flowmon: DNSTRAFFIC**
The method is aggregating simple events informing about the nonstandard DNS traffic.

**Flowmon: DOSATTACK**
The method is aggregating simple events informing about different kinds of denial of service attacks.

**Flowmon: LARGETRANSFER**
The method is aggregating simple events informing about the large data transfers.

**Flowmon: Load Basic Building Blocks**
Rule ensures all Flowmon building blocks are being applied.

**Flowmon: MALWARE**
The method is aggregating simple events that could be the sign of malware infection.

**Flowmon: MISCONFIGURED**
The method is aggregating simple events that could mean wrong configuration of the device.

**Flowmon: NETANOMALY**
The method is aggregating simple events related to the standard behavior of the network.

**Flowmon: NETDISCOVERY**
The method is aggregating simple events informing about the devices trying to discover the monitored network.

**Flowmon: PROXYBYPASS**
The method is aggregating simple events informing about the devices that are bypassing (or trying to bypass) the specified proxy server.

**Flowmon: SNIFTER**
The method is aggregating simple events unveiling the devices that are possibly eavesdropping the traffic on the network.

**Flowmon: SPAMMER**
The method is aggregating simple events informing about potential spammers.
Flowmon: SRVOUTAGE
The method is aggregating simple events informing about unavailable services.

Flowmon: UNDESIRED
The method is aggregating simple events informing about the use of applications, that could be undesired in the given environment.

Flowmon: VPNTRANSFER
The method is detecting VPN tunneled traffic.

Building blocks
Flowmon content pack also includes several building blocks – these building blocks are used to label Flowmon single events or their combination, building blocks are used in the correlation rules but can be used also in user custom searches and reports.

- Flowmon: BB: ANOMALY
- Flowmon: BB: Anomaly DHCP
- Flowmon: BB: Anomaly L3
- Flowmon: BB: Anomaly or Attack
- Flowmon: BB: Anomaly SMTP
- Flowmon: BB: Attack dst IP followed Anomaly src IP
- Flowmon: BB: Attack or anomaly chain (malware)
- Flowmon: BB: BITTORRENT
- Flowmon: BB: BLACKLIST
- Flowmon: BB: BPATTERNS
- Flowmon: BB: COUNTRY
- Flowmon: BB: DIVCOM
- Flowmon: BB: DNSANOMALY
- Flowmon: BB: DNSQUERY
- Flowmon: BB: HONEYPOT
- Flowmon: BB: ICGUARD
- Flowmon: BB: INSTMSG
- Flowmon: BB: IPV6TUNNEL
- Flowmon: BB: Misconfigured device
- Flowmon: BB: MULTICAST
- Flowmon: BB: Network access attack
- Flowmon: BB: Network anomaly
- Flowmon: BB: Network discovery
- Flowmon: BB: REFLECTDOS
- Flowmon: BB: SMTPANOMALY
- Flowmon: BB: SRVNA
- Flowmon: BB: TEAMVIEWER
- Flowmon: BB: TELNET
- Flowmon: BB: TOR
- Flowmon: BB: Undesired apps
- Flowmon: BB: Upload or Country
- Flowmon: BB: Upload or Webshare
- Flowmon: BB: Utilization
- Flowmon: BB: WEBSHARE
Flowmon App - Dashboard

Flowmon App Dashboard provides overview of events and detection methods. Dashboard consists of a main stacked column graph, expandable filter above the main graph and interactive legend on the right side.

Main graph

Each column in the main graph represents timeframe which begins at time specified under the column and ends when the new column begins. There are always 30 columns and timeframe of each column scales with the time interval specified in the filter (For example, each column represents 1 minute when filter is set between 10:00 and 10:30).

Hovering over column segment in the main graph shows the name of detection method to which does the event relate to.
Legend

Hovering over the detection method abbreviation in legend reveals tooltip with explanation.

Use the legend to show/hide specific detection methods from the main graph (before and after hiding DIRINET):
This is one of the ways to tidy up the main graph. Alternatively, click "Toggle all" above the legend to hide all detection methods and only select the ones you need.

Filter

Expand filter by clicking on the expand arrow on the right side:

Filter in Dashboard provides the following options:
- Filter by Time interval.
Specify the graph type (Events, Sources or Targets count).
Filter by Source and Target.
Filter by Perspective.
Filter by Priority (above, below and specific priority).
Filter by both atomic and relations filters from Flowmon ADS Processing.
Filter by Data feed (flow data source).
Show Events button

Applied filter parameters can be quickly removed by clicking on the red x mark:

Workflow of switching between Dashboard, Events and Flows

On Dashboard, clicking on the button "Show events" in the filter changes view to Events and automatically pre-filters the event list. Similarly, applying specific IP address as a filter to the Events table changes view to Events. In Events view there are similar buttons to switch back to Dashboard and drill-down to individual Flows. In Flows view you can switch back to Events. This makes investigation and switching between Dashboard, Events and Flows intuitive and easy.

Detail

Clicking on a column in the main graph shows details for this timeframe and detection method. Donut chart shows event count for each of the top 5 source IP addresses for the specified detection method. Click "Show all" to expand the list of all IPs.
Click on the IP address to examine it further. There are two options:

**Detail - Apply Source IP to the graph**

After applying IP to the main graph, filter above the graph shows selected IP as a Source. Main graph now shows what events and when does the IP caused.
Detail - Apply Source IP to the Events table

This action switches from Dashboard to Events view. Time interval in Events filter corresponds to column timeframe previously selected in the Dashboard.
In Events view you can inspect individual events. Events can be classified to perspectives (event can belong to zero or multiple perspectives). Similarly, event priority can be specified. Each event is identified with a unique ID and have a timestamp (Time). Type column specifies the detection method type. More detailed information can be found in the Detail column. Involved IP addresses are specified in columns Source and Targets. Data feeds specify flow data source.

Perspectives and Data feeds are configured in Flowmon Solution. See Flowmon ADS User Guide for details.

Events unassigned to any perspective can be listed selecting the "-" in the Perspective drop-down menu in the filter. You can use this to verify that all events which should have been classified were assigned perspective. You can also check whether events are being classified to the right perspective when sending with syslog to QRadar.

Filter

Filter in Events view provides following options:

- Filter by Time interval.
- Filter by Type of detection method.
- Filter by Source and Target.
- Filter by Perspective.
- Filter by Priority (above, below and specific priority).
- Filter by both atomic and relations filters from Flowmon ADS Processing.
- Filter by Data feed (flow data source).
- Show Dashboard button and keep the filter
- Show flows - switch to Filters and keep the selected time interval
Instant search

This feature allows to instantly find events by a particular piece of information. Just start typing and table of events will be filtered on-the-fly. Partial matches are supported.

Event info (Event Details and Evidence)
Double-click on a event row in the table or click on an event ID to open window with event info window with event details and evidence.

Here you can see all the information about the event and associated flows.
You can inspect event directly in Flowmon Solution. Use the buttons in the top right corner. *Open in Flowmon* button opens a new browser tab with a deep link right to the event details in Flowmon Solution. Similarly, *Visualisation* button opens an interactive event visualization in Flowmon Solution.

Right-click on Source and Target IP addresses provides an option to add address to a filter. Right-click anywhere on event row provides an option to open event info window.
Flowmon App - Flows

In Flows view you can inspect individual flows, sort flows by columns, use instant search and apply filters.

Column configuration
See chapter Flows output format to configure which columns are shown and their order.

Instant search
This feature enables you to type in any column value and immediately get a list of flows where is this value used. Partial matches are supported.

Filters
In Flows view you can use filters to narrow down list of flows before turning to instant search.

Filter in Flows provides option to:

- Filter by Time interval
- Filter by Profile
- Filter by Channels
- Use advanced filter (click on the question mark icon to show how-to)
- Specify number of flows in the result (Count)
- Switch to Events and keep the selected time interval (Show events)
Flowmon QRadar Dashboard Widget

Widgets provide a quick overview of events by priority right in IBM QRadar Dashboard. Up to 5 Flowmon widgets can be added. Perspective and Time interval can be specified for each widget.

To add a new Flowmon widget, press Add item, select Flowmon and add desired Widget. There can be up to 5 widgets (numbered 1 to 5), as QRadar allows to place the widget 5 times each time with a different configuration. Drag and drop widget to move it to a specific place on the dashboard.
To change widget perspective, click on currently selected perspective and choose a new one.

Note that perspectives are defined in Flowmon ADS. In this example we are using perspectives from our demo:

- Man-in-the-Middle Attack, DNS amplification, DHCP (APT)
- Critical services
- Alerts
- Operational issues
- Security issues


To change Time interval, click on the currently selected Time interval and choose a new one.
Clicking on any row in a Widget (Critical, High, Medium, Low or Information) takes you directly to automatically pre-filtered list of events in Flowmon App.

For example, clicking on Critical row in this widget:

Will open list of related events in Flowmon App:

Note automatically applied filter above the list:
Opening Flowmon Application directly from Offenses & Log Activity

Quickly find related events for a particular IP addresses directly from Offenses and Log Activity pages. Options to pre-filter IP address has been added to the context menu (you can choose whether to filter the IP as Source or Target).

Context menu is available in both offenses list and in offense summary.
Context menu in Log Activity.

### Event Information

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Task Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Level Category</td>
<td>SIM User Action</td>
</tr>
<tr>
<td>Event Description</td>
<td>A task has successfully completed</td>
</tr>
<tr>
<td>Magnitude</td>
<td><img src="image" alt="Magnitude Bar" /></td>
</tr>
<tr>
<td>Username</td>
<td>N/A</td>
</tr>
<tr>
<td>Start Time</td>
<td>Aug 28, 2018, 12:42:21 PM</td>
</tr>
<tr>
<td>Domain</td>
<td>Default Domain</td>
</tr>
</tbody>
</table>

### Source and Destination Information

<table>
<thead>
<tr>
<th>Source IP</th>
<th>127.0.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Asset Name</td>
<td>N/A</td>
</tr>
<tr>
<td>Source Port</td>
<td>0</td>
</tr>
<tr>
<td>Pre NAT Source IP</td>
<td>0</td>
</tr>
<tr>
<td>Pre NAT Source Port</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter options:
- **Filter by Source IP in Flowmon app**
- **Filter by Target IP in Flowmon app**
Investigation examples (use-cases)

Activities of a specific IP address

In Dashboard, we've selected several detection methods. One of the peaks corresponds to DIRINET (Direct internet communication). By clicking on the bar in the chart we open details below with a donut chart and list of IPs.

We apply first IP with highest count as Source IP to the graph. This gives us an overview about detected activities throughout the day.
We can see that there were a couple of ANOMALY events, the rest is DIRINET.

Suspicious activity of an IP

This is a basic example showing how to investigate suspicious host.

Let's investigate communication with blacklisted hosts in the Dashboard. Untoggle all and check BLACKLIST.

IP 192.168.3.225 is a source of this communication. This is an IoC (Indicator of Compromise). Let's what has been this IP up to by applying it as a filter to the graph.

And we can see that the IP has been involved in scanning, dictionary attacks and anomalies as a source and it means that the host was probably compromised.
From dictionary attacks to compromised host

In this example, we'll see how an attack can spread. We're going to observe host (victim) becoming the source of subsequent attacks and investigate the chain of events.

First, let's select the SSHDICT (SSH dictionary attacks) detection method.
Similarly, as in the first example we apply source IP as a filter to the graph. It's clear that the IP has done a substantial amount of scanning.

Which hosts have been affected? Let's find out by expanding the filter (arrow in the corner) and clicking the Show events button.

We can see a list of events with applied filter (SSHDICT, and our source IP). By clicking on an IP in the Targets column we can see whether the targets themselves tried anything suspicious. If so, this could mean that the dictionary attacks were successful and target host is compromised.
There are no events. This is because we're still applying the SSHDICT filter. Remove it by clicking on the red cross.

There are 34 pages of events. This is too much to sift through and will be better to use high level graph view for fast analysis.
We can switch back to Dashboard by expanding the filter and clicking the Show dashboard button.
Now, we can see all events at once in an interactive visual form. There are few suspicious events and a lot of direct internet communication (DIRINET).

Let's uncheck DIRINET. The first and most maliciously looking event is the green DICTATTACK in the morning. We can uncheck the rest of detection methods.

Apply the source IP as a filter to the Events table.
After applying DICTATTACK filter and the source IP we can see one event of an attack with all the details. It's clear that the previous target of an attack has itself become source of malicious activities.