Check Point Application for QRadar Integration

Guide
Check Point SmartView Monitor and IBM QRadar Integration

The integration of Check Point SmartView Monitor and IBM QRadar delivers network data and security events from Check Point appliances to QRadar, for real-time threat information in the QRadar console. This integration significantly speeds up the analytical process, with all analysis functions, from both QRadar and Check Point SmartEvent, on the one QRadar console.

Security analysts also benefit from SmartEvent’s internal aggregation functions, which summarize Check Point logs to easy-to-read event data. A security analyst with full access to QRadar and SmartEvent can fine-tune Check Point protections directly from the SmartEvent-QRadar integration toolset.

System Requirements and Prerequisites

- IBM Security QRadar Log Manager, version 7.2.6 and higher
- Check Point R80 SmartEvent Server, with the supplement http://supportcontent.checkpoint.com/solutions?id=sk112315
- Check Point Security Management Server or Multi-Domain Management Server, version R77 or higher

Before you install this application:

- Make sure the IBM QRadar server is connected to a Check Point Log Server to read logs.
- Make sure the Check Point R80 SmartEvent server is connected to a Check Point Log Server to read logs.
- Make sure you have Admin permission for IBM QRadar.

Troubleshooting

IBM Security QRadar products:


Check Point:

- To configure an R80 SmartEvent server with an R77.xx Security Management, see sk110894 http://supportcontent.checkpoint.com/solutions?id=sk110894.
- To connect a dedicated R80 SmartEvent server to a dedicated R77.xx Security Management Server, see sk110874 http://supportcontent.checkpoint.com/solutions?id=sk110894.
- To troubleshoot the Gaia Portal (WebUI), see sk91380 http://supportcontent.checkpoint.com/solutions?id=sk91380.
Installation and Usage

From the QRadar tab, open the Check Point features:

- **Check Point** tab - Graphical security overview of important attacks, allowed high risk applications, infected machines, and quick access to the Check Point SmartView portal.

- **Search in Check Point SmartView** – Click a Log Activity or Offense to drill down for advanced investigation with Check Point SmartEvent features.

**Recommended: Replace Certificates**

Replace the SSL certificate with a self-signed or a trusted certificate.

**IBM Security QRadar:**


**Check Point:**

- To configure the Gaia Portal to use a 3rd party CA-issued certificate (and not a self-signed certificate), see sk106839 [http://supportcontent.checkpoint.com/solutions?id=sk106839](http://supportcontent.checkpoint.com/solutions?id=sk106839).


Enabling this Application

**To enable the integration application:**


2. Connect to IBM QRadar.


   Use the IBM® Security QRadar® Extension Management tool to upload your app ZIP archive directly to your QRadar Console:

   a) Click Admin tab > Extension Management.

   b) In the Extension Management window, click Add.

   c) Select the Check Point app ZIP archive.

   d) Select Install immediately.

   e) See the list of installation items before installation, to make sure you selected the correct app.

      **Note:** It can take several minutes for the app to become active.

   f) When installation is complete, clear your browser cache and refresh the browser window, before you use the app.
4. Configure the SmartView Monitor IP address.
   a) Click Admin tab > Plug-ins.
   b) Select Check Point SmartView.
   c) In the Check Point SmartView window > SmartLog Server > Log Server, enter the IP address or DNS name of the R80 SmartEvent Server.
   d) To validate the certificate, select Check Certificate. If you are using a self-sign certificate, you must deselect this option.
   e) Click Submit.

5. Browse to: https://<SmartEventServer_IP>/smartview/

6. Confirm that you trust the certificate.

**Known Limitations**

- This application supports only one R80 SmartEvent server.
- The QRadar supplement is only supported for Gaia 64-bit.
- The IBM QRadar Offenses tab > Search in Check Point SmartView, is only supported by:
  - Top 5 Source IPs: by Source IP
  - Top 5 Destination IPs: by Destination IP

**Supported Clients:**

- Firefox version: 50 and above
- Safari version : 9.1 and above
- Opera version : 9.2 and above
- Android Browser version: 4.4 and above
- Chrome for Android version : 51 and above
- Microsoft Edge version : 13 and above