IBM QRadar Network Insights
Version 7.3.0

IBM QRadar Network Insights Users Guide

Note
Before you use this information and the product that it supports, read the information in "Notices" on page 11.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.3.0 and subsequent releases unless superseded by an updated version of this document.

© Copyright IBM Corporation 2017.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2017

Introduction to installing QRadar Network Insights

This guide contains information about analyzing network data in real-time by using IBM® QRadar® Network Insights.

Intended audience

Investigators extract information from the network traffic and focus on security incidents, and threat indicators.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

© Copyright IBM Corp. 2017

Chapter 1. Real-time threat investigations with QRadar Network Insights

IBM QRadar Network Insights provides real-time analysis of network data and an advanced level of threat detection and analysis.

QRadar Network Insights is a network threat analytics solution that quickly and easily detects insider threats, data exfiltration, and malware activity. Essential threat indicators are gathered and traced with full visibility from network traffic.

Advanced cybersecurity threats are increasingly difficult to detect and prevent. Malicious activity is often disguised as normal usage, which allows threats to move and communicate across networks to accomplish their objectives. For example, malware morphs to avoid signature-based detection, and social engineering techniques, such as phishing, are effective at opening the door to these attacks.

Search capability

The search capability of QRadar Network Insights finds and extracts important indicators from the packet data, for example, flow information, metadata, extracted content, and suspect content. You can use the extracted content for long-term retrospective analysis.

Integration with IBM Security QRadar Incident Forensics

QRadar Network Insights records application activities, captures artifacts, and identifies assets, applications, and users that participate in network communications. QRadar Network Insights is tightly integrated with IBM Security QRadar Incident Forensics for post incident investigations and threat hunting activities. QRadar Incident Forensics and IBM QRadar Network Packet Capture captures, reconstructs, and replays the entire conversation, but QRadar Network Insights provides the incident detection, and informs you whether suspect items or topics of interest were discussed at any time during the conversation.

Suspect content can originate from a wide variety of sources, such as malware, non-standard ports, regex, or Yara rules.

Value of flows

Flows provide QRadar with visibility across network activity because they enable asset detection when devices connect to a network. With QRadar Network Insights, you can correlate the flow data with event data to detect threats that cannot be identified by logs alone. IBM Security QRadar QFlow Collector provides network flows and also recognizes layer 7 applications, and you can capture the beginning of the sessions. QRadar Network Insightsreveals previously hidden threats, and malicious behaviors.

Related concepts:

Chapter 3, “QRadar Network Insights Flow Inspection Levels,” on page 7
To improve performance, you must choose the appropriate flow rate that is required by configuring the **Flow Inspection Level** setting.

© Copyright IBM Corp. 2017

QRadar Network Insights deployments

IBM QRadar Network Insights is a managed host that you attach to the QRadar console.

For a QRadar Network Insights deployment, you must select the `6200` appliance option during the installation. For more information about installing the QRadar Network Insights appliance, see the *IBM Security QRadar Incident Forensics Installation Guide*.

For a QRadar Network Insights deployment, you need to allocate one license to the `6200` appliance option. QRadar Network Insights requires a separate license for the `6200` appliance, but you do not need a QRadar Network Insights license on the QRadar console.

QRadar Network Insights appliance relationship with IBM Security QRadar Incident Forensics

You can deploy QRadar Network Insights separately from the IBM Security QRadar Incident Forensics Processor deployment. QRadar Network Insights requires only a connection to the QRadar console, and does not require a connection to the QRadar Incident Forensics appliance.

QRadar Network Insights appliance

The QRadar Network Insights 1920 appliance comes with two third-generation network cards. The network cards are tapped directly to the network to help with real-time packet inspection.

The configurable flow forwarding capability enables load-balancing across multiple appliances. The hardware configuration helps with in-memory processing to enable real-time analysis of network data.

Table 1. Network card specifications

1920 appliance	**Description**
System	X3650 M5
CPU	2 x E5-2680 v4 14C 2.4 GHz 35 MB 2400 MHz 120 W
RAM	8 x 16 GB
HDD	2 x 200 GB SSD
ServeRAID	M1215
I/O cards	Intel X520 2P 10 GbE + 2 x 10G SR 2 x NT40E3 4P 40G + 2 x 10G SR + 2 x 10G LR
P/S	2 x 900 W

Chapter 2. QRadar Network Insights configuration requirements

After you install IBM QRadar Network Insights and attach it to the QRadar Console as a managed host, you must configure your appliance before you can begin to use it for investigating threats on your network. The QRadar Network Insights appliance reads the raw packets from a network tap or span port and then generates IPFIX packets. The IPFIX packets are sent to the QFlow process on the QRadar Console.

Configuring QFlow Collector format

As a manager of a QRadar deployment, you can choose the format that your QFlow Collectors use to export data to the QFlow Processor: TLV (type-length-value) or Payload. TLV format stores the content metadata properties in the flow record, and can be searched without extra configuration in QRadar. The payload format stores the content metadata properties in the **payload** field of the flow record, and need to be extracted by using custom properties for searching.

Before you begin

Important:

QRadar Network Insights V7.3 introduces a content pack based on TLV; which supersedes the content pack based on custom properties that was released in V7.2.8. After you install the V7.3 content pack, you must set the QFlow format setting to TLV; otherwise the rules in the content pack don't work.

Ensure that the following requirements are met:

__ • Install a QRadar Console with a QRadar Network Insights attached as a managed host.

__ • Perform a full deployment after you attach IBM QRadar Network Insights as a managed host.

Procedure

1. Log in to QRadar: `https://IP_Address_QRadar.`

   The default user name is `admin`. The password is the password of the root user account.
2. Click the **Admin** tab.
3. In the navigation pane, click **System Settings**.
4. Click the **QFlow Settings** menu, and choose the QFlow format.

Table 2. QFlow format options

QFlow format	Description
`TLV`	Default QFlow format setting. Choose **TLV** (type-length-value) for new installations, or for upgrades that don't have a QRadar Network Insights appliance as part of their deployment. QRadar Network Insights V7.3 supports only TLV for content flows.

© Copyright IBM Corp. 2017

Table 2. QFlow format options (continued)

QFlow format	Description
Payload	Choose **Payload** for upgrades that have a QRadar Network Insights appliance as part of their deployment.

5. Click **Save**.
6. From the **Admin** tab menu bar, click **Deploy Full Configuration**, and confirm your changes.
7. Refresh your web browser to view the **Forensics** tab.

Setting up DTLS on a QRadar Network Insights managed host

The QRadar Network Insights appliance is a managed host. To prevent eavesdropping and tampering, you must set up Datagram Transport Layer Security (DTLS) on a QRadar Network Insights managed host. You must configure a flow source first.

Procedure

1. Add the QRadar Network Insights appliance as a managed host:
   a. Click the **Admin** tab.
   b. In the navigation pane, click **System and License Management** under the **System Configuration** section.
   c. Select the QRadar Network Insights managed host. The appliance type is 6200.
   d. Click the **Deployment Actions** icon, and select **Add Host**.
   e. When prompted enter the IP address and root password of the QRadar Network Insights managed host, and click **Add**.
2.
3. To configure a flowsource, use the following steps:
   a. Log in to QRadar as an administrator.
   b. Click the **Admin** tab.
   c. In the navigation pane, click **Flow Sources** under the **Flows** section.
   d. Click the **Add** icon.
   e. Specify a descriptive **Flow Source Name**.
   f. Select a **Target Flow Collector** or accept the value provided.
   g. Select **Netflow v.1/v.5/v.7/v.9/IPFIX** as the **Flow Source Type**.
   h. Enter a value for the **Monitoring Port** or accept the value provided.
   i. Select DTLS from the **Linking Protocol** list.
   j. Click **Save**.
   k. From the **Admin** tab menu bar, click **Deploy Full Configuration**, and confirm changes.
   l. Refresh your web browser.
4. To configure DTLS communication, use the following steps:

   Important: If you change the QRadar Flow Collector or flow source of any QRadar Network Insights managed host in your deployment, you must run the DTLS setup script again.
   a. Click the **Deployment Actions** icon, and select **Edit Host Connection**.

b. On the Modify Flow Collector Connection page, select the QRadar Flow Collector and flow source.
c. Click the **Save**.
d. Close the System and License Management page.
e. On the **Admin** tab, click the **Deploy Changes** icon.
f. Use **SSH** to log in as the root user on the QRadar Console.
g. Run this command to set up the DTLS certificate:
```
python /opt/qradar/bin/qflow_dtls_cert_setup.py
```
h. Log in to QRadar as an administrator.
i. On the **Admin** tab, select **Advanced** > **Deploy Full Configuration**.

Chapter 3. QRadar Network Insights Flow Inspection Levels

To improve performance, you must choose the appropriate flow rate that is required by configuring the **Flow Inspection Level** setting.

The flow rate is related to the levels of visibility through the available content, such as source, destination, protocol, and specific file types.

The flow inspection levels are cumulative, so each level takes the properties of the preceding level.

Flows

Flows is the lowest level of inspection. Flows are detected by 5-tuple, and the number of bytes and packets that are flowing in each direction are counted. This kind of information is similar to what you get out of a router or network switch that does not perform deep packet inspection. This level supports the highest bandwidth, but generates the least amount of flow information.

The attributes that QRadar Network Insights generates using the flows inspection level are: 5-tuple values, a flow ID, packet and octet counts in each direction, and flow start and end times.

Enriched Flows

Each flow is identified and inspected by one of the protocol or domain inspectors, and many kinds of attributes can be generated from that inspection.

The following list describes the attributes that QRadar Network Insights generates by using the enriched flows inspection level are:

- HTTP metadata values - including categorization of URLs
- Application ID and action
- File information (name, size, hash)
- Originating and recipient user names
- Limited suspect content values

Content enriched flows

Content enriched flows is the default setting and the highest level of inspection. It contains all the attributes that the enriched flows level does and it also scans and inspects the content of the files that it finds. This results in a more accurate content-type determination, and can yield more suspect content values that result from the inspection of the file contents.

The following list describes the attributes that QRadar Network Insights generates by using the content enriched flows inspection level:

- Personal information
- Confidential data
- Embedded scripts
- Redirects

© Copyright IBM Corp. 2017

- Configurable content-based suspect content

Table 3. Performance considerations

Flow Inspection Level Setting	Performance
Flows	10 Gbps
Enriched Flows	Approximately 10 Gbps. Performance varies depending on the inspection level setting, search, extraction criteria and network data.
Content Enriched Flows (Advanced)	Approximately 3.5 Gbps. 10 Gbps performance is achievable with multiple appliances.

Related concepts:

Chapter 1, “Real-time threat investigations with QRadar Network Insights,” on page 1
IBM QRadar Network Insights provides real-time analysis of network data and an advanced level of threat detection and analysis.

Configuring QRadar Network Insights settings

To improve performance, configure the levels of flows that the QRadar Network Insights appliances in your deployments produce. Each inspection level provides deeper visibility and extracts more content.

Procedure

1. Log in to QRadar as an administrator.
2. Click the **Admin** tab.
3. In the navigation pane, click **System Settings**.
4. Click the **Network Insights Settings** menu.
5. From the **Flow Inspection Level**, select the flow rate that is required. Use the following table to understand the flow inspection levels:

Table 4. Flow inspection levels

Flow Inspection Level	Description
Flows	Lowest level of inspection. Flows are detected by 5-tuple, and the number of bytes and packets that are flowing in each direction are counted.
Enriched Flows	Each flow is identified and inspected by one of the protocol or domain inspectors, and many kinds of attributes can be generated from that inspection.
Content Enriched Flows	The default setting. The highest level of inspection. It does everything that the Enriched Flows levels does, but it also scans and inspects the content of the files that it finds.

6. Click **Save**.
7. From the **Admin** tab menu bar, click **Deploy Full Configuration**.
8. Refresh your web browser.

What to do next

Deploy QRadar Incident Forensics Processor managed host.

Chapter 4. Threat detection with QRadar Network Insights

For real-time visibility to threat activity across your network, use QRadar Network Insights to detect indicators of cyber attacks and their malicious activity.

Downloading the QRadar Network Insights content

You download the QRadar Network Insights content (extension) from IBM Security App Exchange (http://exchange.xforce.ibmcloud.com/hub/extension/522bf1095f047b0b37225d8efc5d4877). You use the **Extensions Management** tool to install them.

For information about using the **Extensions Management** tool, see the *IBM Security QRadar Administration Guide*.

© Copyright IBM Corp. 2017

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corp. 2017

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Printed in USA