Technical note
Version 7.2.1

Enhancing the right-click menu for event and flow viewers

Note
Before using this information and the product that it supports, read the information in “Notices” on page 3.

Contents

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 comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM(r) 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.

Enhancing the right-click menu for event and flow viewers

On the IBM Security QRadar® SIEM Console appliance, you can add more actions, such as an option to view more information about the source IP or destination IP.

About this task

You can pass any data that is in the event or flow to the URL or command-line script.

Restriction: You can add options to the right-click menu only on the QRadar SIEM Console appliance and only to some Ariel database fields.

Procedure

1. Using SSH, log in to the QRadar Console appliance as the root user.
2. Go to the `/opt/qradar/conf` directory and create a file named `arielRightClick.properties`.
3. Edit the `/opt/qradar/conf/arielRightClick.properties` file. Use the following table to specify the parameters that determine the options for the right-click menu.

Table 1. Description and example of the arielRightClick.properties file parameters

Parameter	Requirement	Description	Example
`pluginActions`	Required	Define the Ariel properties.	
`arielProperty`	Required	Defines where the right-click menu will be enabled.	Some examples are **sourceIP**, **sourcePort**, **destinationIP**, and **qid**. For more information about field names, see the *AQL Flow and Event Query Guide*.
`text`	Required	the text that is displayed on the **right click** menu.	Google search
`useFormattedValue`	Optional	Specifies whether formatted values are passed to the script. Default is **true**. If set to **true**, the formatted value is passed. If set to **false**, the unformatted value is passed.	For the event name (QID) property, if the parameter is set to true, the event name of the QID is passed to the script. If the parameter is set to false, the raw, unformatted QID value is passed to the script.

Table 1. Description and example of the arielRightClick.properties file parameters (continued)

Parameter	Requirement	Description	Example
url	Required to access a URL	The URL that opens in a new window. Specifies the parameters to pass to the URL. Use the format: $<Ariel_Field Name>$	The following example shows a source IP passed to a web URL: `sourceIPwebUrlAction.url= http://www.mywebsite.com? q=$sourceIP$`
command	Required if the action is a command	Specifies the absolute path of the command or script file. No arguments are required.	`destinationPortScript Action.command=/bin/echo`
arguments	Required if the action is a command	Specifies data to pass to the script. Use the following format: $<Ariel_Field Name>$	`destinationPortScript Action.arguments=$qid$`

For each of the key names that are specified in the *pluginActions* list, define the action by using a key with the format *key name*, *property*.

4. Save and exit the file.
5. Log in to the QRadar user interface.
6. Click the **Admin** tab.
7. Select **Advanced** > **Restart Web Server**.

Example

The following example shows how to add *Test URL* as a right-click option for source IPs.

```
pluginActions=sourceIPwebUrlAction,destinationPortScriptAction

sourceIPwebUrlAction.arielProperty=sourceIP
sourceIPwebUrlAction.text=Test URL
sourceIPwebUrlAction.url=http://www.mywebsite.com?q=$sourceIP$

destinationPortScriptAction.arielProperty=destinationPort
destinationPortScriptAction.text=Test Unformatted Command
destinationPortScriptAction.useFormattedValue=false
destinationPortScriptAction.command=/bin/echo
destinationPortScriptAction.arguments=$qid$
```

The following example shows handing of more than one parameter to a url or a scripting action.

```
qidwebUrlAction.arielProperty=qid,device,eventCount
qidwebUrlAction.text=Search on Google
qidwebUrlAction.url=http://www.google.com?q=$qid$-$device$-$qid$-$eventCount$

sourcePortScriptAction.arielProperty=sourcePort
sourcePortScriptAction.text=Port Unformatted Command
sourcePortScriptAction.useFormattedValue=true
sourcePortScriptAction.command=/bin/echo
sourcePortScriptAction.arguments=$qid$-$sourcePort$-$device$
```

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

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 states 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All 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 the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols

indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

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.

Index