Table 34. By Destination IP page search options (continued)

Options	Description
Specific Interval	To specify a particular interval to search for, you can select the **Specific Interval** option, and then select one of the following options: • To specify a particular interval to search for, you can select the **Specific Interval** option, and then select one of the following options: • **Last Event/Flow between** - Select this check box to search destination IP addresses associated with offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search
Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Destination IP	You can type the destination IPv4 or IPv6 address or CIDR range you want to search for.
Magnitude	From this list box, you can specify a magnitude, and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value.
VA Risk	From this list box, you can specify a VA risk, and then select display only offenses with a VA risk that is equal to, less than, or greater than the configured value. The range is 0 - 10.
Events/Flows	From this list box, you can specify an event or flow count magnitude, and then select display only offenses with an event or flow count that is equal to, less than, or greater than the configured value.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **By Destination IP**.
3. From the **Search** list box, select **New Search**.
4. On the Time Range pane, select an option for the time range you want to capture for this search. See Table 1.
5. On the Search Parameters pane, define your specific search criteria. See Table 1.
6. On the Column Definition pane, define the order in which you want to sort the results:
   a) From the first list box, select the column by which you want to sort the search results.
   b) From the second list box, select the order in which you want to display the search results. Options include **Descending** and **Ascending**.
7. Click **Search**.

What to do next

Saving search criteria on the Offense tab

Searching offenses on the By Networks page

On the **By Network page** of the **Offense** tab, you can search offenses that are grouped by the associated networks.

About this task

The following table describes the search options that you can use to search offense data on the **By Networks** page:

Table 35. Search options for search offense data on the By Networks page

Option	Description
Network	From this list box, you can select the network that you want to search for.
Magnitude	From this list box, you can specify a magnitude, and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value.
VA Risk	From this list box, you can specify a VA risk, and then select display only offenses with a VA risk that is equal to, less than, or greater than the configured value.
Event/Flows	From this list box, you can specify an event or flow count, and then select display only offenses with an event or flow count that is equal to, less than, or greater than the configured value.

Procedure

1. Click the **Offenses** tab.
2. Click **By Networks**.
3. From the **Search** list box, select **New Search**.
4. On the Search Parameters pane, define your specific search criteria. See Table 1.
5. On the Column Definition pane, define the order in which you want to sort the results:
   a) From the first list box, select the column by which you want to sort the search results.
   b) From the second list box, select the order in which you want to display the search results. Options include **Descending** and **Ascending**.
6. Click **Search**.

What to do next

Saving search criteria on the Offense tab

Saving search criteria on the Offenses tab

On the **Offenses** tab, you can save configured search criteria so that you can reuse the criteria for future searches. Saved search criteria does not expire.

Procedure

1. Procedure
2. Perform a search. See Offense searches.
3. Click **Save Criteria**.

4. Enter values for the following parameters:

Option	Description
Parameter	Description
Search Name	Type a name you want to assign to this search criteria.
Manage Groups	Click **Manage Groups** to manage search groups. See Managing search groups.
Timespan options:	Choose one of the following options: • **All Offenses** - Select this option to search all offenses regardless of time range. • **Recent** - Select the option and, from this list box, select the time range that you want to search for. • **Specific Interval** - To specify a particular interval to search for, select the **Specific Interval** option, and then select one of the following options: `Start Date between - Select this check box to search offenses that started during a certain time period. After you select this check box, use the list boxes to select the dates you want to search for.` `Last Event/Flow between - Select this check box to search offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search.Last Event between - Select this check box to search offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search.`
Set as Default	Select this check box to set this search as your default search.

5. Click **OK**.

Searching for offenses that are indexed on a custom property

Define search criteria to filter the offense list and make it easier to see which offenses you need to investigate. You can use the offense type in your search criteria to find all offenses that are based on a custom property. You can filter the query results to show offenses that have a specific custom property capture result.

Before you begin

The custom property must be used as a rule index. For more information, see "Offense indexing" on page 28.

Procedure

1. Click the **Offenses** tab.
2. From the **Search** list, select **New Search**.
3. On the **Offense Source** pane, select the custom property in the **Offense Type** list.

   The **Offense Type** list shows only normalized fields and custom properties that are used as rule indexes. You cannot use **Offense Source** to search `DateTime` properties.
4. Optional: To search for offenses that have a specific value in the custom property capture result, type the value that you want to search for in the filter box.
5. Configure other search parameters to satisfy your search requirements.
6. Click **Search**.

Results

All offenses that meet the search criteria are shown in the offense list. When you view the offense summary, the custom property that you searched on is shown in the **Offense Type** field. The custom property capture result is shown in the **Custom Property Value** field in the **Offense Source Summary** pane.

Finding IOCs quickly with lazy search

You use the IBM QRadar *lazy search* to search for an indicator of compromise (IOC), such as unusual outbound network traffic or anomalies in privileged user account activity.

Before you begin

Lazy search returns the first 1000 events that are related to the search criterion. For example, if you need to search for a particular MD5 as part of a malware outbreak investigation, you do not need to review every related event. Do a *lazy search* to quickly return a limited result set.

To take advantage of the *lazy search*, you must have the Admin security profile, or a non-administrator security profile that is configured in the following way:

- Permission precedence set to **No Restrictions**.
- Access to all networks and log sources.

Lazy search cannot be used by users with non-administrator security profiles on networks where domains are configured.

Procedure

1. To do a lazy search for quick filters, do these steps:
   a) On the **Log Activity** tab, in the **Quick Filter** field, enter a value.
   b) From the **View** list, select a time range.
2. To do a lazy search for basic searches, do these steps:
   a) On the Log Activity tab, click **Search** > **New Search**.
   b) Select a **Recent** time range or set a **Specific Interval**.
   c) Ensure that **Order by** field value is set to `Start Time` and the **Results Limit** field value is `1000` or less. Aggregated columns must not be included in the search.
   d) Enter a value for the **Quick Filter** parameter and click **Add Filter**.
3. To disable lazy search completely, do these steps:
   a) Click the **System Settings** on the **Admin** tab.
   b) In the **System Settings** window, remove any values from the **Default Search Limit** field.

Deleting search criteria

You can delete search criteria.

About this task

When you delete a saved search, then objects that are associated with the saved search might not function. Reports and anomaly detection rules are QRadar objects that use saved search criteria. After you delete a saved search, edit the associated objects to ensure that they continue to function.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.

- Click the **Network Activity** tab.

2. From the **Search** list box, select **New Search** or **Edit Search**.
3. In the Saved Searches pane, select a saved search from the **Available Saved Searches** list box.
4. Click **Delete**.
   - If the saved search criteria is not associated with other QRadar objects, a confirmation window is displayed.
   - If the saved search criteria is associated with other objects, the **Delete Saved Search** window is displayed. The window lists objects that are associated with the saved search that you want to delete. Note the associated objects.
5. Click **OK**.
6. Choose one of the following options:
   - Click **OK** to proceed.
   - Click **Cancel** to close the **Delete Saved Search** window.

What to do next

If the saved search criteria was associated with other QRadar objects, access the associated objects that you noted and edit the objects to remove or replace the association with the deleted saved search.

Using a subsearch to refine search results

You can use a subsearch to search within a set of completed search results. The subsearch is used to refine search results, without searching the database again.

Before you begin

When you define a search that you want to use as a base for subsearching, make sure that Real Time (streaming) option is disabled and the search is not grouped.

About this task

This feature is not available for grouped searches, searches in progress, or in streaming mode.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Perform a search.
3. When your search is complete, add another filter:
   a) Click **Add Filter**.
   b) From the first list box, select a parameter that you want to search for.
   c) From the second list box, select the modifier that you want to use for the search. The list of modifiers that are available depends on the attribute that is selected in the first list.
   d) In the entry field, type specific information that is related to your search.
   e) Click **Add Filter**.

Results

The Original Filter pane specifies the original filters that are applied to the base search. The Current Filter pane specifies the filters that are applied to the subsearch. You can clear subsearch filters without restarting the base search. Click the **Clear Filter** link next to the filter you want to clear. If you clear a filter from the Original Filter pane, the base search is relaunched.

If you delete the base search criteria for saved subsearch criteria, you still have access to saved subsearch criteria. If you add a filter, the subsearch searches the entire database since the search function no longer bases the search on a previously searched data set.

What to do next

Save search criteria

Managing search results

You can initiate multiple searches, and then navigate to other tabs to perform other tasks while your searches complete in the background.

You can configure a search to send you an email notification when the search is complete.

At any time while a search is in progress, you can return to the **Log Activity** or **Network Activity** tabs to view partial or complete search results.

Canceling a search

While a search is queued or in progress, you can cancel the search on the **Manage Search Results** page.

About this task

If the search is in progress when you cancel it, the results that were accumulated until the cancellation are maintained.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. From the **Search** menu, select **Manage Search Results**.
3. Select the queued or in progress search result you want to cancel.
4. Click **Cancel**.
5. Click **Yes**.

Deleting a search

If a search result is no longer required, you can delete the search result from the **Manage Search Results** page.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. From the **Search** menu, select **Manage Search Results**.
3. Select the search result that you want to delete.
4. Click **Delete**.
5. Click **Yes**.

Managing search groups

Using the **Search Groups** window, you can create and manage event, flow, and offense search groups.

These groups allow you to easily locate saved search criteria on the **Log Activity**, **Network Activity**, and **Offenses** tabs, and in the Report wizard.

Viewing search groups

A default set of groups and subgroups are available.

About this task

You can view search groups on the **Event Search Group**, **Flow Search Group**, or **Offense Search Group** windows.

All saved searches that are not assigned to a group are in the **Other** group.

The **Event Search Group, Flow Search Group**, and **Offense Search Group** windows display the following parameters for each group.

Table 36. Search Group window parameters

Parameter	Description
Name	Specifies the name of the search group.
User	Specifies the name of the user that created the search group.
Description	Specifies the description of the search group.
Date Modified	Specifies the date the search group was modified.

The **Event Search Group**, **Flow Search Group**, and **Offense Search Group** window toolbars provide the following functions.

Table 37. Search Group window toolbar functions

Function	Description
New Group	To create a new search group, you can click **New Group**. See Creating a new search group.
Edit	To edit an existing search group, you can click **Edit**. See Editing a search group.
Copy	To copy a saved search to another search group, you can click **Copy**. See Copying a saved search to another group.
Remove	To remove a search group or a saved search from a search group, select the item that you want to remove, and then click **Remove**. See Removing a group or a saved search from a group.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. **Select Search** >**Edit Search**.

3. Click **Manage Groups**.
4. View the search groups.

Creating a new search group

You can create a new search group.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. **Select Search Edit Search**.
3. Click **Manage Groups**.
4. Select the folder for the group under which you want to create the new group.
5. Click **New Group**.
6. In the **Name** field, type a unique name for the new group.
7. Optional. In the **Description** field, type a description.
8. Click **OK**.

Editing a search group

You can edit the **Name** and **Description** fields of a search group.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Select **Search** > **Edit Search**.
3. Click **Manage Groups**.
4. Select the group that you want edit.
5. Click **Edit**.
6. Edit the parameters:
   - Type a new name in the **Name** field.
   - Type a new description in the **Description** field.
7. Click **OK**.

Copying a saved search to another group

You can copy a saved search to one or more groups.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Select **Search** > **Edit Search**.
3. Click **Manage Groups**.
4. Select the saved search that you want to copy.

5. Click **Copy**.
6. On the **Item Groups** window, select the check box for the group you want to copy the saved search to.
7. Click **Assign Groups**.

Removing a group or a saved search from a group

You can use the **Remove** icon to remove a search from a group or remove a search group.

About this task

When you remove a saved search from a group, the saved search is not deleted from your system. The saved search is removed from the group and automatically moved to the **Other** group.

You cannot remove the following groups from your system:

- Event Search Groups
- Flow Search Groups
- Offense Search Groups
- Other

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Select **Search** > **Edit Search**.
3. Click **Manage Groups**.
4. Choose one of the following options:
   - Select the saved search that you want to remove from the group.
   - Select the group that you want to remove.
5. Click **Remove**.
6. Click **OK**.

Search example: Daily employee reports

The following example describes how to use a complex advanced search query to see specific employee information.

For identity management purposes, you decide to generate a daily report of the user activity in QRadar. The report must include information about the employee, such as their user names, their serial number, their manager, and their activities.

An employee might have multiple user names in QRadar. You use the RESTful API to build a reference map that returns all associated user names to the employee's name, `Global_User`. For the serial number and the manager's name, you create another reference data set and add it to the reference map.

Employee activities can range from login failures to QRadar tasks, such as deleting objects. These events are recorded by QRadar. By specifying the frequency of the events in the map, you can gauge when suspicious activity occurs. You group the data by the employee's name and the event name, and then sort the data by the highest event frequency within a 24-hour time frame.

To see this daily report, you log in to QRadar Console. In the Advanced Search text box on the **Log Activity** tab, you type the following search query:

```
select REFERENCEMAP('GlobalID_Mapping', username) as Global_User, QIDNAME(qid)
as 'Event Name', count(*) as 'Event Count', FIRST(username) as UserId,
REFERENCETABLE('employee_data','SerialNum', Global_user) as 'Serial Number',
REFERENCETABLE('employee_data','Manager',Global_User) as Manager from events
where (Global_User IS NOT NULL) GROUP BY Global_user,'Event Name' ORDER BY
'Event Count' DESC last 1 DAYS
```

Chapter 11. Custom event and flow properties

IBM QRadar normalizes standard information that is parsed by the DSM, such as user names, IP addresses, and ports.

Some event sources send unique information that is not normalized. You can use custom properties to extract that data from the event or flow payload, and then use the non-normalized data in custom rules, searches, and reports.

The type of custom property that you create depends on the method that you want to use to define the non-normalized data in the payload.

Extraction-based properties

Create an extraction-based property when you want to use a regex or JSON expression to parse the property values from the event or flow payloads.

For example, you have a report that shows all the users who changed other user's permissions on an Oracle server. The report uses normalized data to show the list of users who made the permission changes and the number of changes they made. The user account that was changed is not normalized and cannot be shown in the report. You can create a regex-based custom property to extract this information from the logs, and then use the property in searches and reports.

When the event or flow is parsed, the expression pattern is tested against each payload until the pattern matches. The first pattern to match the event or flow payload determines the data to be extracted.

When you define custom regex patterns, follow the regex rules as defined by the Java programming language. To learn more about regex rules, you can view regex tutorials on the web.

Calculation-based properties

Create a calculation-based property when you want to do calculations on existing numeric event and flow properties. For example, you can create a calculation-based property that divides one numeric property by another numeric property to display a percentage value.

AQL-based properties

Create an AQL-based property when you want to combine multiple extraction and calculation-based properties into a single property. For example, you can use AQL-based custom properties to combine extraction-based URLs, virus names, or secondary user names into a single property.

```
CONCAT( 'Src=', sourceip, ' | ', 'User=', username, ' | ', 'Domain=',
DOMAINNAME(domainid) )
```

Note: The AQL expression can include AQL functions.

It does not support expressions that use SELECT, FROM, or database names.

You cannot use aggregate functions, such as SUM or GROUP, or other AQL-based custom properties.

Creating a custom property

Create a custom property to extract data that IBM QRadar does not typically show from the event or flow payloads. Custom properties must be enabled, and extraction-based custom properties must be parsed, before you can use them in rules, searches, reports, or for offense indexing.

Before you begin

QRadar includes a number of existing custom event properties that are not enabled or parsed by default. Ask your administrator to review the custom event property that you want to create to ensure that it does not exist.

To create custom event properties, you must have the **User Defined Event Properties** permission.

To create custom flow properties, you must have the **User Defined Flow Properties** permission. You must also set the **IPFIX Additional Field Encoding** field to **Payload** or **TLV and Payload**.

Users with administrative capabilities can create custom event and flow properties by selecting **Custom Event Properties** or **Custom Flow Properties** on the **Admin** tab.

You must configure a flow collector to export data to a flow processor. For more information, see Configuring the Flow Collector format.

About this task

Although multiple default custom properties might have the same name and the same log source, they can have different regex expressions, event names, or categories. For example, there are multiple custom properties for Microsoft Windows Security Event Log called **AccountName**, but each one is defined by a unique regex expression.

Procedure

1. Click the **Log Activity** tab or the **Network Activity** tab.
2. If you are viewing the events or flows in streaming mode, click the **Pause** icon to pause streaming.
3. Double-click the event or flow that contains the data that you want to extract, and then click **Extract Property**.
4. In the **Property Type Selection** pane, select the type of custom property that you want to create.
5. Configure the custom property parameters.

   Click the help icon (?) to see information about the custom property parameters.
6. If you are creating an extraction-based custom property that is to be used in rules, search indexes, or forwarding profiles, ensure that the **Enable for use in Rules, Forwarding Profiles and Search Indexing** check box is selected.
7. Click **Test** to test the expression against the payload.
8. Click **Save**.

What to do next

"Modifying or deleting a custom property" on page 175

Related concepts

AQL search string examples

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Modifying or deleting a custom property

Edit a property when you want to change the property parameters, such as the regex expression or the log source type.

About this task

You can search for a specific property by using the **Search properties** field. The search is not case-sensitive.

Make a copy of a custom property when you want to change it, and then save it using a different name.

To delete a property, you must first remove all dependencies to it. Deleting a custom property does not delete the indexed property fields from the Ariel database.

Procedure

1. Choose one of the following options:
   - To edit or delete a custom event property, click the **Log Activity** tab.
   - To edit or delete a custom flow property, click the **Network Activity** tab.
2. From the **Search** list box, select **Edit Search**.
3. Click **Manage Custom Properties**.
4. Select the property from the list, and click **Edit**, **Copy**, or **Delete**.
5. Make the required changes to the property, and then click **Save**.

Defining custom properties by using custom property expressions

Define a custom property for an event payload by using a custom property expression. Because JSON parsing begins when a valid JSON object is detected, the entire event does not need to be in JSON format. Similarly, LEEF and CEF parsing begins only when a valid LEEF/CEF message is detected within the event. Regex parsing runs through the entire payload.

About this task

IBM QRadar supports the following custom property expression types:

- Regex
- JSON
- LEEF
- CEF
- Name Value Pair
- Generic List
- XML

You can use different expressions to capture various custom properties for the same event. You can also use a combination of expression types to capture the same custom property if that property can be captured from multiple event formats.

Procedure

1. Log in to QRadar and click the **Admin** tab.
2. From the **Data Sources** section, click **Custom Event Properties**, and then click **Add**.

3. In the **Property Type Selection** section, select **Extraction Based**.
4. In the **Test Field**, enter the event payload that you want to use to test your custom property.
5. In the **Property Definition** section, complete the following steps:
    a) If you're adding an expression to an existing property, select **Existing Property** and select a property from the list.
    b) If you're defining a new property, select **New Property** and enter the name of the property.
    c) To use the property for rules, reports and searches, select the **Enable for use in Rules, Forwarding Profiles and Search Indexing** check box.

    You must select this check box to use the property for rules and indexes. Selecting the check box increases the efficiency of reports and searches, but you don't need to select it to use the property for reports and searches. When you select the check box, properties are parsed when the event is initially received and before it is stored. As a result, the loads are put on the event collection service.

    d) Select a **Field Type** for the property.

    If you choose IP as the type for your custom property, QRadar supports only IPv4.

    e) Optional: Enter a description for the property.
6. In the **Property Expression Definition** section, complete the following steps:
    a) Keep the **Enabled** check box selected; otherwise, clear the check box to disable the property.
    b) From the **Log Source Type** list, select a log source type for the property.
    c) If the expression is only evaluated against events for a specific log source, select the log source from the **Log Source** list. If you want it to be evaluated against all log sources, don't select.
    d) If the expression is only evaluated against events with a specific event name or QID, click the **Event Name** and browse for a QID to associate the expression with.
    e) If the expression is evaluated against any event with a specific low-level category, select **Category**, and select the **High Level Category** and then **Low Level Category** for the event.

    Tip: If the expression is evaluated for all events of the selected log source type and log source, ensure that you set the **Low Level Category** and **High Level Category** to **Any**.

    f) From the **Extraction using** field, select the extraction method to use for the property.

Table 38. Property extraction methods

Extraction method	Valid expression form	Example
Regex	Enter the regex and the capture group number.	

Table 38. Property extraction methods (continued)

Extraction method	Valid expression form	Example

JSON Keypath	A valid JSON expression is in the form:
	`/"<name of top-level field>"`
	For an event in a nested JSON format, a valid JSON expression is in the form:
	`/"<name of top-level field>"/"<name of sub-level field_1>".../"<name of sub-level field_n>"`
	To extract the 'user' field, type `/"user"` in the **JsonKeypath** field.
	To extract just the 'last_name' value from the 'user' subobject, type this expression:
	`/"user"/"last_name"`
		The following example is a simple case of an event for a flat JSON record:
		`{"action": "login", "user": "Firstname Lastname"}`
		The following example is a complex case of an event for a JSON record with nested objects:
		`{ "action": "login", "user": { "first_name": "Firstname", "last_name": "Lastname" } }`

Table 38. Property extraction methods (continued)

Extraction method	Valid expression form	Example

LEEF Key	Valid LEEF expressions are in the form of either a single key reference, or a special LEEF header field reference.
	To extract the 'usrName' property, type `usrName` in the **LEEF Key** field.
	The possible keys that can be extracted in these examples are:
	• devTimeFormat
	• devTime
	• usrName
	• name
	• authType
	• src
	To extract a header key property, type the key in the following format in the **LEEF Key** field:
	`$eventid$`
	The LEEF header values can be extracted by using the following expressions:
	• $leefversion$
	• $vendor$
	• $product$
	• $version$
	• $eventid$
		The following example is a simple case of an event that is formatted in LEEF V1.0:
		`LEEF:1.0|ABC Company|`
		`SystemDefender|1.13|`
		`console_login|`
		`devTimeFormat=yyyy-MM-`
		`dd'T'HH:mm:ss.SSSZ`
		`devTime=2017-10-18T11:26:03.060+0`
		`200`
		`usrName=flastname`
		`name=Firstname Lastname`
		`authType=interactivePassword`
		`src=192.168.0.1`
		The following example is a simple case of an event that is formatted in LEEF V2.0 with the caret (^) separator character, and contains the same keys as the LEEF V1.0 example:
		`LEEF:2.0|ABC Company|`
		`SystemDefender|1.13|`
		`console_login|^|`
		`devTimeFormat=yyyy-`
		`MMdd'T'HH:mm:ss.SSSZ^`
		`devTime=2017-10-18T11:26:03.060+0`
		`200^usrName=`
		`flastname^name=Firstname Lastname`
		`^authType=interactivePassword^src`
		`=192.168.0.1`

Table 38. Property extraction methods (continued)

Extraction method	**Valid expression form**	**Example**

CEF Key	Valid CEF expressions are in the form of either a single key reference, or a special CEF header field reference.
	To extract the 'cs1' property, type `cs1` in the **CEF Key** field.
	The possible keys that can be extracted in the example are:
	• start
	• duser
	• cs1
	• cs1Label
	• cs2
	• cs2Label
	• src
	To extract a header key property, type the key in the following format in the **CEF Key** field:
	`$id$`
	The CEF header values can be extracted by using the following expressions:
	• $cefversion$
	• $vendor$
	• $product$
	• $version$
	• $id$
	• $name$
	• $severity$
		The following example shows an event that is in CEF format:
		`CEF:0|ABC Company|SystemDefender|`
		`1.13|console_login|`
		`Console Login|1|start=Oct 18`
		`2017 11:26:03`
		`duser=flastname cs1=Firstname`
		`Lastname cs1Label=Person`
		`Name cs2=interactivePassword`
		`cs2Label=authType src=192.168.0.1`

Name Value Pair Key	Valid Name Value Pair expressions are in the form of a single key reference.	The following example shows an event that is in Name Value Pair format:
		`Company=ABC`
		`Company;Product=SystemDefender;`
		`Version=1.13;EventID=console_logi`
		`n;`
		`Username=jsmith;Name=John`
		`Smith;authType=interactivePasswor`
		`d;`

Table 38. Property extraction methods (continued)

Extraction method	**Valid expression form**	**Example**

Generic List Keypath	Valid Generic List expressions are in the form of a *$<number>* notation. For example, $0 represents the first property in the list, $1 is the second property, and so on.	The following example shows an event that is in Generic List format:
		`ABC`
		`Company;1.13;console_login;jsmith`
		`;`
		`John Smith;interactivePassword;`

XML Key	Valid XML expressions are in the form of a single key reference.
	Enter the path to the XML field that you want to use to populate the property's value. An XML key path must begin with a forward slash (/) to indicate the root of the XML object, and be followed by one or more XML field names within double quotation marks.
		The following example shows an event that is in XML format:
		`<EPOEvent><MachineInfo>`
		`<MachineName>NEPTUNE</`
		`MachineName>`
		`<MachineName>VALUE23</`
		`MachineName><AgentGUID>`
		`9B-B5-A6-A8-37-B3</`
		`AgentGUID><IPAddress`
		`someattrib="someattribvalue">`
		`192.0.2.0</IPAddress>`
		`<OSName>Windows 7</`
		`OSName><UserName>I`
		`am a test user</UserName></`
		`MachineInfo></EPOEvent>`

g) If you chose the Numeric **Field Type** in the **Property Definition** section, select a number format in the **Extracted Number Format** field in the **Format** section to define any digit group separators for the locale of the custom property.

h) If you chose the Date/Time **Field Type** in the **Property Definition** section, enter a format in the **Extracted Date/Time Format** and **Locale** fields in the **Format** section to define the date and time for the locale of the custom property.

i) Click **Test** to test the property expression definition.

7. Click **Save**.

Use case: Create a report that uses event data that is not normalized

You can use a custom property to extract data that is not normalized from a payload, and use that data to build a report. For example, you can build a report that is based on the interface information that is in Cisco ASA firewall deny messages.

In this example, we'll use the following sample Cisco ASA firewall events to demonstrate how to extract the interface value from the event payload, and then build a report that uses that data.

```
<162>Sep 02 2014 11:49:41: %ASA-2-106001: Inbound TCP connection denied
from 10.10.10.128/58826 to 10.11.11.11/9100 flags SYN on interface External
<162>Sep 02 2014 11:49:40: %ASA-2-106001: Inbound TCP connection denied
from 10.10.10.128/58826 to 10.11.11.11/9100 flags SYN on interface Loopback
<162>Sep 02 2014 11:49:17: %ASA-2-106001: Inbound TCP connection
denied from 10.10.10.128/58821 to 10.11.11.11/9100 flags SYN on interface Internal
```

1. Create the custom property.

   In the sample events above, you can see that the event payload includes the word `interface` followed by the value that you want to extract. To capture the interface information from the events above, create an extraction-based custom property and configure it to use the regex expression `interface\s(.*)\b`.

   To ensure that the new custom property is available to use in a search, select the **Enable for use in Rules, Forwarding Profiles and Search Indexing** check box, and enable the custom property.

2. Create a search, and in the **Group By** field, select the new custom event property.

   To ensure that the search results include only Cisco ASA events, add the log source as a quick filter option in the search parameters. Save the search criteria so that you can use it in a report. Assign the saved search to a group to make it easier to find later.

3. Create a report, and configure the graph content to use the new saved search.

   If the report was not configured to run after saving, you can run the report immediately by selecting **ActionsRun Report**.

Chapter 12. Custom rules in IBM QRadar

Rules, sometimes called correlation rules are applied to events, flows, or offenses to search for or detect anomalies. If all the conditions of a test are met, the rule generates response.

What are rules?

Custom rules test events, flow, and offenses to detect unusual activity in your network. You create new rules by using AND and OR combinations of existing rule tests. Anomaly detection rules test the results of saved flow or events searches to detect when unusual traffic patterns occur in your network. Anomaly detection rules require a saved search that is grouped around a common parameter.

What are building blocks?

A building block is a collection of tests that don't result in a response or an action.

A building block groups commonly used tests to build complex logic so that it can be reused in rules. A building block often tests for IP addresses, privileged user names, or collections of event names. For example, a building block can include the IP addresses of all DNS servers. Rules can then use this building block.

QRadar has default rules and you can also download more rules from the IBM Security App Exchange to create new rules.

How do rules work?

QRadar Event Collectors gather events from local and remote sources, normalize these events, and classify them into low-level and high-level categories. For flows, QRadar Flow Collectors read packets from the wire or receive flows from other devices and then converts the network data to flow records. Each Event Processor processes events or flow data from the QRadar Event Collectors. Flow Processors examine and correlate the information to indicate behavioral changes or policy violations. The custom rules engine (CRE) processes events and compares them against defined rules to search for anomalies. When a rule condition is met, the Event Processor generates an action that is defined in the rule response. The CRE tracks the systems that are involved in incidents, contributes events to offenses, and generates notifications.

How is an offense created from a rule?

QRadar creates an offense when events, flows, or both meet the test criteria that is specified in the rules.

QRadar analyzes the following information:

- Incoming events and flows
- Asset information
- Known vulnerabilities

The rule that created the offense determines the offense type.

The magistrate prioritizes the offenses and assigns the magnitude value based on several factors, including number of events, severity, relevance, and credibility.

Note: Building blocks are tested before rules are tested.

For example, you have a building block that is defined to trigger an offense on high magnitude events. The log activity can show that there were high magnitude events, but no offense was triggered. This can happen because when the building block was tested, the events was not at high magnitude. The magnitude of the event did not increase until the rules were tested.

One solution is to set a rule to check for the different in Severity, Credibility, and Relevance rather than to use a building block.

Custom rules

IBM QRadar includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. You can also create your own rules to detect unusual activity.

What are custom rules?

Customize default rules to detect unusual activity in your network.

Rule types

Each of the event, flow, common, and offense rule types test against incoming data from different sources in real time. There are multiple types of rule tests. Some check for simple properties from the data set. Other rule tests are more complicated. They track multiple, event, flow, and offense sequences over a period of time and use "counter" that is on one or more parameters before a rule response is triggered.

Event rules

Test against incoming log source data that is processed in real time by the QRadar Event Processor. You create an event rule to detect a single event or event sequences. For example, to monitor your network for unsuccessful login attempts, access multiple hosts, or a reconnaissance event followed by an exploit, you create an event rule. It is common for event rules to create offenses as a response.

Flow rules

Test against incoming flow data that is processed by the QRadar Flow Processor. You can create a flow rule to detect a single flow or flow sequences. It is common for flow rules to create offenses as a response.

Common rules

Test against event and flow data. For example, you can create a common rule to detect events and flows that have a specific source IP address. It is common for common rules to create offenses as a response.

Offense rules

Test the parameters of an offense to trigger more responses. For example, a response generates when an offense occurs during a specific date and time. An offense rule processes offenses only when changes are made to the offense. For example, when new events are added, or the system scheduled the offense for reassessment. It is common for offense rules to email a notification as a response.

Managing rules

You can create, edit, assign rules to groups, and delete groups of rules. By categorizing your rules or building blocks into groups, you can efficiently view and track your rules. For example, you can view all rules that are related to compliance.

Domain-specific rules

If a rule has a domain test, you can restrict that rule so that it is applied only to events that are happening within a specified domain. An event that has a domain tag that is different from the domain that is set on, the rule does not trigger a response.

To create a rule that tests conditions across the entire system, set the domain condition to **Any Domain**.

Rule conditions

Most rule tests evaluate a single condition, like the existence of an element in a reference data collection or testing a value against a property of an event. For complex comparisons, you can test event rules by building an Ariel Query Language (AQL) query with WHERE clause conditions. You can use all of the WHERE clause functions to write complex criteria that can eliminate the need to run numerous individual tests. For example, use an AQL WHERE clause to check whether inbound SSL or web traffic is being tracked on a reference set.

You can run tests on the property of an event, flow, or offense, such as source IP address, severity of event, or rate analysis.

With functions, you can use building blocks and other rules to create a multi-event, multi-flow, or multi-offense function. You can connect rules by using functions that support Boolean operators, such as OR and AND. For example, if you want to connect event rules, you can use **when an event matches any|all of the following rules** function.

Related information

How do rules perform tests on events, flows, and offenses? (Security Learning Academy course)

Creating a custom rule

IBM QRadar includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. You can also create your own rules to detect unusual activity.

Before you begin

Before you create a new rule, you must have the **Offenses** > **Maintain Custom Rules** permission.

About this task

When you define rule tests, test against the smallest data possible. Testing in this way helps rule test performance and ensures that you don't create expensive rules. To optimize performance, start with broad categories that narrow the data that is evaluated by the rule test. For example, start with a rule test for a specific log source type, network location, flow source, or context (R2L, L2R, L2L). Any mid-level tests might include IP addresses, port traffic, or any other associated test. The rule must test payload and regex expressions last.

Similar rules are grouped by category. For example, Audit, Exploit, DDoS, Recon, and more. When you delete an item from a group, the rule or building block is only deleted from the group; it remains available on the **Rules** page. When you delete a group, the rules or building blocks of that group remain available on the **Rules** page.

Procedure

1. From the **Offenses**, **Log Activity**, or **Network Activity** tabs, click **Rules**.
2. From the **Display** list, select **Rules** to create a new rule.
3. Optional: From the **Display** list, select **Building Blocks** to create a new rule by using building blocks.
4. From the **Actions** list, select a rule type.

   Each rule type tests against incoming data from different sources in real time. For example, event rules test incoming log source data and offense rules test the parameters of an offense to trigger more responses.
5. In the **Rule Wizard** window, select the **Skip this page when running this rules wizard** checkbox and click **Next**.

   If you select the **Skip this page when running this rules wizard** checkbox, the **Welcome** page does not appear each time that you start.
6. On the **Rule Test Stack Editor** page, in the **Rule** pane, type a unique name that you want to assign to this rule in the **Apply** text box.
7. From the list box, select **Local** or **Global**.

- If you select **Local**, all rules are processed on the Event Processor on which they were received and offenses are created only for the events that are processed locally.
- If you select **Global**, all matching events are sent to the QRadar Console for processing and therefore, the QRadar Console uses more bandwidth and processing resources.

Learn more about Local and Global rules:

Global rule tests
Use global rules to detect things like "multiple user login failures" where the events from that user might appear on multiple Event processors. For example, if you configured a **Local** rule for five login failures in 10 minutes from the same username, all 5 of those login failures must appear on the same Event Processor. Therefore, if three login failures were on one Event Processor and 2 were on another, no offense is generated. However, if you set this rule to **Global**, it generates an offense.

8. From the **Test Group** list, select one or more tests that you want to add to this rule. The CRE evaluates rule tests line-by-line in order. The first test is evaluated and when true, the next line is evaluated until the final test is reached.
If you want to select the **when the event matches this AQL filter query** test for a new event rule, click the add **(+)** icon. In the **Rule** pane, click **This** and enter an AQL WHERE clause query in the **Enter an AQL filter query** text box.

Learn more about using rules for events that are not detected:

The following rule tests can be triggered individually, but rule tests in the same rule test stack are not acted upon.

- **when the event(s) have not been detected by one or more of these log source types for this many seconds**
- **when the event(s) have not been detected by one or more of these log sources for this many seconds**
- **when the event(s) have not been detected by one or more of these log source groups for this many seconds**

These rule tests are not activated by an incoming event, but instead are activated when a specific event is not seen for a specific time interval that you configured. QRadar uses a *watcher task* that periodically queries the last time that an event was seen (last seen time), and stores this time for the event, for each log source. The rule is triggered when the difference between this last seen time and the current time exceeds the number of seconds that is configured in the rule.

9. To export the configured rule as a building block to use with other rules, click **Export as Building Block**.
10. On the **Rule Responses** page, configure the responses that you want this rule to generate.

Learn more about rule response page parameters:

Table 39. Event , Flow and Common Rule, and Offense Rule Response page parameters

Parameter	Description
Severity	Select this checkbox to assign a severity level to the event, where 0 is the lowest and 10 is the highest. The severity is displayed in the **Annotation** pane of the event details.
Credibility	Select this checkbox to assign credibility to the log source. For example, is the log source noisy or expensive? The range is 0 (lowest) to 10 (highest) and the default is 10. Credibility is displayed in the **Annotation** pane of the event details.

Table 39. Event , Flow and Common Rule, and Offense Rule Response page parameters (continued)

Parameter	Description
Relevance	Select this checkbox to assign relevance to the weight of the asset. For example, how much do you care about the asset? The range is 0 (lowest) to 10 (highest) and the default is 10. Relevance is displayed in the **Annotation** pane of the event details.
Bypass further rule correlation event	Select this checkbox to match an event or flow to bypass all other rules in the rule engine and prevent it from creating an offense. The event is written to storage for searching and reporting.
Dispatch New Event	Select this checkbox to dispatch a new event in addition to the original event or flow, which is processed like all other events in the system. Dispatches a new event with the original event, and is processed like all other events in the system. The **Dispatch New Event** parameters are displayed when you select this checkbox . By default, the checkbox is clear.
Email	Select this checkbox to change the **Email Locale** setting from the **System Settings** on the **Admin** tab.
Send to Local Syslog	Select this checkbox to log the event or flow locally. By default, this checkbox is clear. **Note:** Only normalized events can be logged locally on an appliance. If you want to send raw event data, you must use the Send to Forwarding Destinations option to send the data to a remote syslog host.
Send to Forwarding Destinations	Select this checkbox to log the event or flow on a forwarding destination. A forwarding destination is a vendor system, such as SIEM, ticketing, or alerting systems. When you select this checkbox, a list of forwarding destinations is displayed. To add, edit, or delete a forwarding destination, click the **Manage Destinations** link.
Notify	Select this checkbox to display events that are generated as a result of this rule in the System Notifications item on the Dashboard tab. If you enable notifications, configure the **Response Limiter** parameter.

Table 39. Event , Flow and Common Rule, and Offense Rule Response page parameters (continued)

Parameter	**Description**
Add to Reference Set	Select this checkbox to add events that are generated as a result of this rule to a reference set. You must be an administrator to add data to a reference set. To add data to a reference set, follow these steps: a. From the first list, select the property of the event or flow that you want to add. b. From the second list, select the reference set to which you want to add the specified data.
Add to Reference Data	To use this rule response, you must create the reference data collection.
Remove from Reference Set	Select this checkbox to remove data from a reference set. To remove data from a reference set: a. From the first list box, select the property of the event or flow that you want to remove. Options include all normalized or custom data. b. From the second list box, select the reference set from which you want to remove the specified data. The **Remove from Reference Set** rule response provides the following function: **Refresh** Click **Refresh** to refresh the first list box to ensure that the list is current.
Remove from Reference Data	To use this rule response, you must have a reference data collection.
Execute Custom Action	Select this checkbox to write scripts that do specific actions in response to network events. For example, you might write a script to create a firewall rule that blocks a particular source IP address from your network in response to repeated login failures. You add and configure custom actions by using the **Define Actions** icon on the **Admin** tab.
Response Limiter	Select this checkbox to configure the frequency in which you want this rule to respond.

An SNMP notification might resemble the following example:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

A syslog output might resemble the following example:

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

What to do next

To test your rules, run Chapter 13, “Historical correlation,” on page 203.

To verify that the event triggers the rule test based on your building block, you can create an email response, see “Sending email notifications” on page 42.

Related information

Managing Custom Rules in QRadar SIEM

How is Custom Rule Engine capacity calculated? (Security Learning Academy course)

Example: Configuring a Modified Offense Rule Test

You can apply a modified offense rule test when any offense property is changed based on the events that are associated with that offense. Modified rule tests allow for better configuration of how and when rules are implemented.

Procedure

1. From the **Network Activity** tab or the **Log Activity** tab, click **Rules** to display the **Rules** page. Double-click an offense rule to open the **Rule Wizard**.
2. From the **Rule Test Stack Editor** page, add a test to the offense rule.
   a) To filter the options in the **Test Group** list, type "modified" in the **Type to filter** field.
   b) From the **Test Group** list, select **when an offense is modified.**
   c) To identify a test as an excluded test, click **and** at the beginning of the test in the Rule pane to toggle the display to **and not**.
   d) Click the underlined configurable parameters to customize the variables of the test.
   e) From the dialog box, select values for the variable, and then click **Submit**.
3. To test the total selected accumulated properties for each event or flow group, disable **Test the [Selected Accumulated Property] value of each [group] separately**.
4. In the groups pane, enable the groups that you want to assign this rule to.
5. In the **Notes** field, type any notes that you want to include for this rule, and then click **Next**.
6. On the **Rule Responses** page, configure the responses that you want this rule to generate.
7. Ensure the **Response Limiter** checkbox is selected and use the list boxes to configure how frequently you want this rule to respond.

   Important: If many events are contributing to the offense, use a response limiter. Any new event that contributes to an offense triggers the rule.
8. Click **Next**, and then click **Finish**.

Configuring an event or flow as false positive

You might have legitimate network traffic that triggers false positive flows and events that makes it difficult to identify true security incidents. You can prevent events and flows from correlating into offenses by configuring them as false positives.

Procedure

1. From the, **Log Activity**, or **Network Activity** tabs, click the pause on the upper right to stop real-time streaming of events or flows.
2. Select the event that you want to tune.
3. Click **False Positive**.
4. Select an event or flow property option.
5. Select a traffic direction option.

6. Click **Tune**.

Results

The event or flow that matches the specified criteria will no longer correlates into offenses. To edit false positive tuning, use the **User-BB_FalsePositive: User Defined Positive Tunings building** block in the **Rules** section on the **Offenses** tab.

Anomaly detection rules

Anomaly detection rules test the results of saved flow or events searches to detect when unusual traffic patterns occur in your network.

Anomaly detection rules require a saved search that is grouped around a common parameter, and a time series graph that is enabled. Typically the search needs to accumulate data before the anomaly rule returns any result that identifies patterns for anomalies, thresholds, or behavior changes.

Anomaly rules

Test event and flow traffic for changes in short-term events when you are comparing against a longer timeframe. For example, new services or applications that appear in a network, a web server crashes, firewalls that all start to deny traffic.

Example: You want to be notified when one of your firewall devices is reporting more often than it usually does because your network might be under attack. You want to be notified when you receive twice as many events in 1 hour. You follow these steps:

1. Create and save a search that groups by log source, and displays only the count column.
2. Apply the saved search to an anomaly rule, and add the rule test, **and when the average value (per interval) of count over the last** 1 hour **is at least** 100% **different from the average value (per interval) of the same property over the last** 24 hours.

Threshold rules

Test events or flows for activity that is greater than or less than a specified range. Use these rules to detect bandwidth usage changes in applications, failed services, the number of users connected to a VPN, and detecting large outbound transfers.

Example: A user who was involved in a previous incident has large outbound transfer.

When a user is involved in a previous offense, automatically set the Rule response to add to the Reference set. If you have a watch list of users, add them to the Reference set. Tune acceptable limits within the Threshold rule.

A reference set, WatchUsers, and Key:username are required for your search.

Complete the following search, and then apply it to a Threshold rule.

```
select assetuser(sourceip, now()) as 'srcAssetUser',
Applicationname(applicationid)as 'AppName', long(sum(sourcebytes
+destinationbytes)) as 'flowsum' from flows where flowdirection = 'L2R' and
REFERENCESETCONTAINS('Watchusers', username)group by 'srcAssetUser',
applicationid order by 'flowsum' desc last 24 hours
```

Behavioral rules

Test events or flows for volume changes that occur in regular patterns to detect outliers. For example, a mail server that has an open relay and suddenly communicates with many hosts, or an IPS (intrusion protection system) that starts to generate numerous alert activities.

A behavioral rule learns the rate or volume of a property over a pre-defined season. The season defines the baseline comparison timeline for what you're evaluating. When you set a season of 1 week, the behavior of the property over that 1 week is learned and then you use rule tests to alert you to any significant changes.

After a behavioral rule is set, the season adjusts automatically. When the data in the season is learned, it is continually evaluated so that business growth is profiled within the season; you do not have to change your rules. The longer a behavioral rule runs, the more accurate it becomes. You can then adjust the rule responses to capture more subtle changes.

The following table describes the behavioral rule test parameter options.

Table 40. Behavioral rule test definitions

Rule test parameter	Description
Season	The most important value. The season defines the baseline behavior of the property that you are testing and which the other rule tests use. To define a season, consider the type of traffic that you are monitoring. For example, for network traffic or processes that include human interaction, 1 week is a good season timeframe. For tracking automated services where patterns are consistent, you might want to create a season as short as 1 day to define that pattern of behavior.
Current traffic level	Weight of the original data with seasonal changes and random error accounted for. This rule test asks the question, "Is the data the same as yesterday at the same time?" The weight must be in the range of 1 to 100. A higher value places more weight on the previously recorded value.
Current traffic trend	Weight of changes in the data for each time interval. This rule test asks the question, "How much does the data change when it compares this minute to the minute before?" The weight must be in the range of 1 to 100. A higher value places more weight on traffic trends than the calculated behavior.
Current traffic behavior	Weight of the seasonal effect for each period. This rule test asks the question, "Did the data increase the same amount from week 2 to week 3, as it did from week 1 to week 2?" The weight must be in the range of 1 to 100. A higher value places more weight on the learned behavior.
Predicted value	Use predicted values to scale baselines to make alerting more or less sensitive. The sensitivity must be in the range of 1 to 100. A value of 1 indicates that the measured value cannot be outside the predicted value. A value of 100 indicates that the traffic can be more than four times larger than the predicted value.

The forecast for value from $(n+1)^{th}$ interval is calculated by using the following formula:

$$F_{n+1} = B_n + T_n + T_{n+1-s}$$

Where F is the predicted value, B is the base value for interval n, T is the trend value for interval n, and T is the trend value for season intervals ago and s is the number of intervals within the season.

The base value is calculated by using the following formula:

$$B_{n+1} = (0.2 + 0.3*(\langle \textit{Current traffic level} \rangle / 100.0))*(\mathrm{value}_{n+1} - T_{n+1-s}) + (1 - (0.2 + 0.3*(\langle \textit{Current traffic level} \rangle / 100.0)))*T_n$$

The trend value is calculated by using the following formula:

$$T_{n+1} = (0.2 + 0.3*(\langle \textit{Current traffic trend} \rangle / 100.0))*(B_{n+1} - B_n) + (1 - (0.2 + 0.3*(\langle \textit{Current traffic trend} \rangle / 100.0)))*T_n$$

Smoothed deviation D is calculated by using the following formula:

$$D_{n+1} = (0.2 + 0.3*(\langle \textit{Current traffic behavior} \rangle / 100.0))*|\mathrm{value}_{n+1} - F_{n+1}| + (1 - (0.2 + 0.3*(\langle \textit{Current traffic behavior} \rangle / 100.0)))*D_{n+1-s}$$

The behavioral rule produces an alert for the interval if the following expression is false:

$$F - (1 + (\textit{sensitivity} / 100.0)*3)*D <= \mathrm{value} <= F + (1 + (\textit{sensitivity} / 100.0)*3)*D$$

During the first season, the behavioral rule learns for future calculations and doesn't produce any alerts.

Creating an anomaly detection rule

Anomaly detection rules test the result of saved flow or event searches to search for unusual traffic patterns that occur in your network. Behavioral rules test event and flow traffic according to "seasonal" traffic levels and trends. Threshold rules test event and flow traffic for activity less than, equal to, or greater than a configured threshold or within a specified range.

Before you begin

To create anomaly detection rules on the **Log Activity** tab, you must have the **Log Activity Maintain Custom Rules** role permission.

To create anomaly detection rules on the **Network Activity** tab, you must have the **Network Activity Maintain Custom Rules** role permission.

To manage default and previously created anomaly detection rules, use the **Rules** page on the **Offenses** tab.

About this task

When you create an anomaly detection rule, the rule is populated with a default test stack, based on your saved search criteria. You can edit the default tests or add tests to the test stack. At least one **Accumulated Property** test must be included in the test stack.

By default, the **Test the [Selected Accumulated Property] value of each [group] separately** option is selected on the **Rule Test Stack Editor** page.

An anomaly detection rule tests the selected accumulated property for each event or flow group separately. For example, if the selected accumulated value is **UniqueCount(sourceIP)**, the rule tests each unique source IP address for each event or flow group.

The **Test the [Selected Accumulated Property] value of each [group] separately** option is dynamic. The **[Selected Accumulated Property]** value depends on the option that you select for the **this accumulated property test** field of the default test stack. The **[group]** value depends on the grouping options that are specified in the saved search criteria. If multiple grouping options are included, the text might be truncated. Move your mouse pointer over the text to view all groups.

Procedure

1. Click the **Log Activity** or **Network Activity** tab.
2. Perform an aggregated search.

   You can add a property to the **group by** in a new historical search or select a property from the **Display** list on the current search page.
3. On the search result page, click **Configure**, and then configure the following options:
   a) Select a property from the **Value to Graph** list.
   b) Select **time series** as the chart type from the **Value to Graph** list
   c) Enable the **Capture Time Series Data** check box.
   d) Click **Save**, and then enter a name for your search.
   e) Click **OK**.
   f) Select last 5 minutes from the **Time Range** list, while you wait for the time series graph to load.

   You must have time series data for the property that you selected in the **Value to Graph** list to run a rule test on that accumulated property.
4. From the **Rules** menu, select the rule type that you want to create.
   - Add Anomaly Rule
   - Add Threshold Rule
   - Add Behavioral Rule
5. On the **Rule Test Stack Editor** page, in the **enter rule name here** field, type a unique name that you want to assign to this rule.
6. To apply your rule by using the default test, select the first rule in the anomaly **Test Group** list.

   You might need to set the accumulated property parameter to the property that you selected from the **Value to Graph** list that you saved in the search criteria. If you want to see the result sooner, set the percentage to a lower value, such as 10%. Change **last 24 hours** to a lesser time period, such as 1 hour. Because an anomaly detection tests on aggregated fields in real time to alert you of anomalous network activity, you might want to increase or decrease events or flows in your network traffic.
7. Add a test to a rule.
   a) To filter the options in the **Test Group** list, type the text that you want to filter for in the **Type to filter** field.
   b) From the **Test Group** list, select the type of test that you want to add to this rule.
   c) To identify a test as an excluded test, click **and** at the beginning of the test in the Rule pane. The **and** is displayed as **and not**.
   d) Click the underlined configurable parameters to customize the variables of the test.
   e) From the dialog box, select values for the variable, and then click **Submit**.
8. To test the total selected accumulated properties for each event or flow group, disable **Test the [Selected Accumulated Property] value of each [group] separately**.
9. In the groups pane, enable the groups you want to assign this rule to.
10. In the **Notes** field, type any notes that you want to include for this rule, and then Click **Next**.
11. On the **Rule Responses** page, configure the responses that you want this rule to generate.

    Learn more about rule response page parameters for anomaly detection rules:

    The following table provides the **Rule Response** page parameters if the rule type is Anomaly.

Table 41. Anomaly Detection Rule Response page parameters

Parameter	Description
Dispatch New Event	Specifies that this rule dispatches a new event with the original event or flow, which is processed like all other events in the system. By default, this check box is selected and cannot be cleared.
Offense Naming	If you want the Event Name information to contribute to the name of the offense, select the **This information should contribute to the name of the associated offense(s)** option. If you want the configured Event Name to contribute to the offense, select the **This information should set or replace the name of the associated offense(s)**. **Note:** After you replace the name of the offense, the name won't change until the offense is closed. For example, if an offense is associated with more than one rule, and the last event doesn't trigger the rule that is configured to override the name of the offense, the offense's name won't be updated by the last event. Instead, the offense name remains the name that is set by the override rule.
Severity	The severity level that you want to assign to the event. The range is 0 (lowest) to 10 (highest) and the default is 5. The Severity is displayed in the Annotations pane of the event details.
Credibility	The credibility that you want to assign to the log source. For example, is the log source noisy or expensive? Using the list boxes, select the credibility of the event. The range is 0 (lowest) to 10 (highest) and the default is 5. Credibility is displayed in the Annotations pane of the event details.
Relevance	The relevance that you want to assign to the weight of the asset. For example, how much do you care about the asset? Using the list boxes, select the relevance of the event. The range is 0 (lowest) to 10 (highest) and the default is 5. Relevance is displayed in the Annotations pane of the event details.
Ensure that the dispatched event is part of an offense	As a result of this rule, the event is forwarded to the magistrate. If an offense exists, this event is added. If no offense was created on the Offenses tab, a new offense is created.
Notify	Events that generate as a result of this rule are displayed in the System Notifications item in the **Dashboard** tab. If you enable notifications, configure the **Response Limiter** parameter.
Send to Local SysLog	Select this check box if you want to log the event or flow locally. By default, the check box is clear. **Note:** Only normalized events can be logged locally on a QRadar appliance. If you want to send raw event data, you must use the **Send to Forwarding Destinations** option to send the data to a remote syslog host.

Table 41. Anomaly Detection Rule Response page parameters (continued)

Parameter	**Description**
Add to Reference Set	Adds events that are generated as a result of this rule to a reference set. You must be an administrator to add data to a reference set. To add data to a reference set, follow these steps: a. From the first list, select the property of the event or flow that you want to add. b. From the second list, select the reference set to which you want to add the specified data.
Add to Reference Data	To use this rule response, you must create the reference data collection.
Remove from Reference Set	If you want this rule to remove data from a reference set, select this check box. To remove data from a reference set, follow these steps: a. From the first list, select the property of the event or flow that you want to remove. b. From the second list, select the reference set from which you want to remove the specified data.
Remove from Reference Data	To use this rule response, you must have a reference data collection.
Execute Custom Action	You can write scripts that do specific actions in response to network events. For example, you might write a script to create a firewall rule that blocks a particular source IP address from your network in response to repeated login failures. Select this check box and select a custom action from the **Custom action to execute** list. You add and configure custom actions by using the **Define Actions** icon on the **Admin** tab.
Publish on the IF-MAP Server	If the IF-MAP parameters are configured and deployed in the system settings, select this option to publish the offense information about the IF-MAP server.
Response Limiter	Select this check box and use the list boxes to configure the frequency with which you want this rule to respond
Enable Rule	Select this check box to enable this rule. By default, the check box is selected.

An SNMP notification might resemble:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

A syslog output might resemble:

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

12. Click **Next**.
13. Click **Finish**.

Configuring a rule response to add data to a reference data collection

Set up rules that use reference data to alert you to suspicious activity. For example, include a list of privileged users into reference data and then set up a rule that is triggered to alert you when privileged user anomalies occur.

Before you begin

Before you send data to a reference set, your QRadar administrator must create the reference set.

About this task

QRadar supports the following data collection types:

Reference set
A set of elements, such as a list of IP addresses or user names, that are derived from events and flows that are occurring on your network.

Reference map
Data is stored in records that map a key to a value. For example, to correlate user activity on your network, you create a reference map that uses the **`Username`** parameter as a key and the user’s **`Global ID`** as a value.

Reference map of sets
Data is stored in records that map a key to multiple values. For example, to test for authorized access to a patent, use a custom event property for **`Patent ID`** as the key and the **`Username`** parameter as the value. Use a map of sets to populate a list of authorized users.

Reference map of maps
Data is stored in records that map one key to another key, which is then mapped to single value. For example, to test for network bandwidth violations, you create a map of maps. Use the **`Source IP`** parameter as the first key, the **`Application`** parameter as the second key, and the **`Total Bytes`** parameter as the value.

Reference table
In a reference table, data is stored in a table that maps one key to another key, which is then mapped to single value. The second key has an assigned type. This mapping is similar to a database table where each column in the table is associated with a type. For example, you create a reference table that stores the **`Username`** parameter as the first key, and has multiple secondary keys that have a user-defined assigned type such as **IP Type** with the **`Source IP`** or **`Source Port`** parameter as a value. You can configure a rule response to add one or more keys that are defined in the table. You can also add custom values to the rule response. The custom value must be valid for the secondary key's type.

Procedure

1. Create the reference data collection by using the **Reference Set Management** widget on the **Admin** tab.

   You can also create a reference data collection by using the `ReferenceDataUtil.sh` script.
2. Create a rule by using the **Rules** wizard.

3. Create a rule response that sends data to a reference data collection. You can add the data as either shared data or domain-specific data.

   Learn more about Add to Reference Data parameters:

   Add to a Reference Map
   Sends data to a collection of single key/multiple value pairs. You must select the key and value for the data record, and then select the reference map that you want to add the data record to.

   Add to a Reference Map Of Sets
   Sends data to a collection of key/single value pairs. You must select the key and the value for the data record, and then select the reference map of sets you want to add the data record to.

   Add to a Reference Map Of Maps
   Send data to a collection of multiple key/single value pairs. You must select a key for the first map, a key for the second map, and then the value for the data record. You must also select the reference map of maps you want to add the data record to.

   Add to a Reference Table
   Sends data to a collection of multiple key/single value pairs, where a type was assigned to the secondary keys. Select the reference table that you want to add data to, and then select a primary key. Select your inner keys (secondary keys) and their values for the data records.

Editing building blocks

You can edit any of the default building blocks to use it in multiple rules or to build complex rules or logic. You can save a group of tests as building blocks for use with rules.

For example, you can edit the **BB:HostDefinition: Mail Servers** building block to identify all mail servers in your deployment. Then, you can configure any rule to exclude your mail servers from the rule tests.

Procedure

1. Click the **Offenses** or **Network Activity tab**.
2. Click **Rules**.
3. From the **Display** list, select **Building Blocks**.
4. Double-click the building block that you want to edit.
5. Update the building block, as necessary.
6. Click **Next**.
7. Continue through the wizard.
8. Click **Finish**.

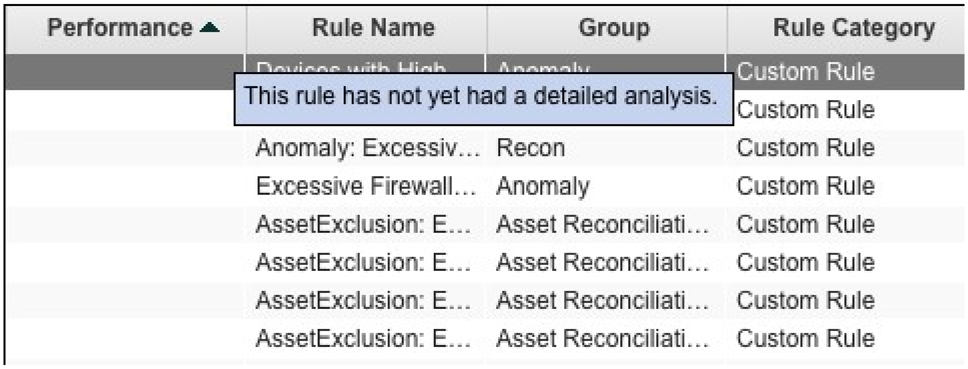
Related information
Overview of Building Blocks in QRadar SIEM

Rule performance visualization

Rule performance visualization extends the current logging around performance degradation and the expensive custom rules in the QRadar pipeline. With rule performance visualization, you can easily determine the efficiency of rules in the QRadar pipeline, directly from the **Rules** page.

Note: You must be an Administrator to turn on rule performance visualization. After rule performance visualization is turned on, users can view performance metrics for rules. For more information about turning on rule performance visualization, see the *IBM QRadar Administration Guide*.

When rule performance visualization is turned on, the **Performance** column is added to the **Rules** page. The **Performance** column is blank until a performance issue occurs in the custom rule engine.



Performance ▲	Rule Name	Group	Rule Category
	Devices with High…	Anomaly	Custom Rule
			Custom Rule
	Anomaly: Excessiv…	Recon	Custom Rule
	Excessive Firewall…	Anomaly	Custom Rule
	AssetExclusion: E…	Asset Reconciliati…	Custom Rule
	AssetExclusion: E…	Asset Reconciliati…	Custom Rule
	AssetExclusion: E…	Asset Reconciliati…	Custom Rule
	AssetExclusion: E…	Asset Reconciliati…	Custom Rule

This rule has not yet had a detailed analysis.

*Figure 10. Performance column on the **Rules** page*

When events or flows are routed to storage, QRadar begins collecting metrics on enabled rules for efficiency measures. Metrics are collected on all event, common, and flow rules. When you save rule updates, the metrics are cleared for the rules that you updated to avoid any confusion around performance and updated rules. This option is configurable by an Administrator.

You can sort rules by their performance metrics and identify the more expensive rules. When you review the rules, you can adjust the tests to optimize each rule, and reduce the load on the system.

With rule performance visualization, you see how expensive the rules are. QRadar operations teams can monitor any expensive rules and ensure that they do not cause future performance issues.

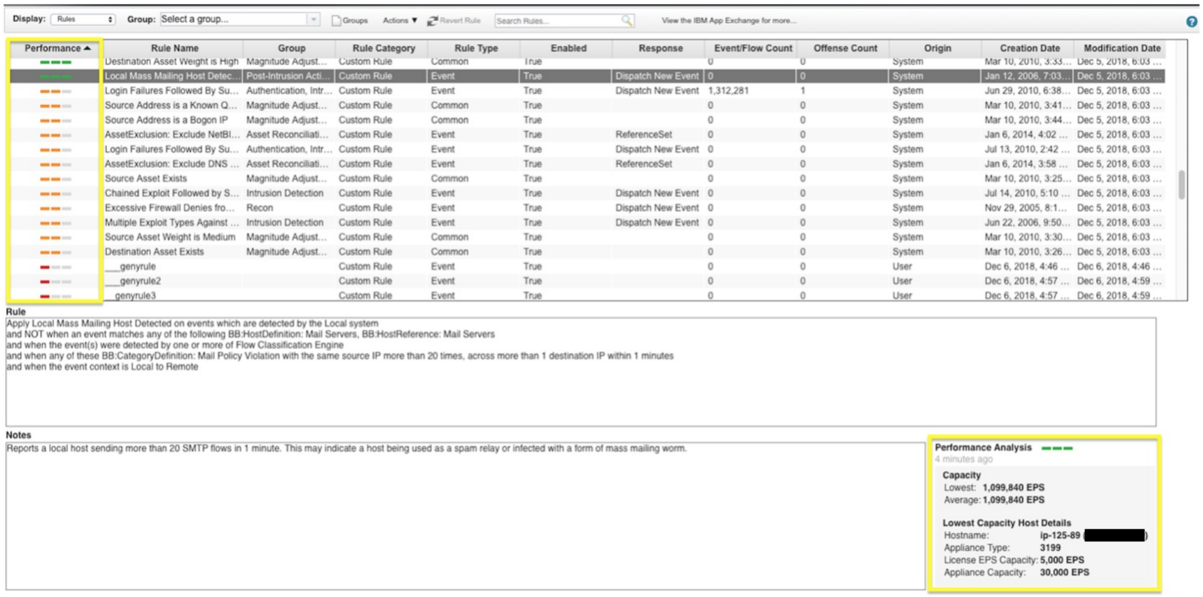
By having rules run efficiently, the workload on the system can decrease. Over time, this efficiency can help QRadar avoid any performance degradations around rules, which cause rules to bypass rule correlation. As a result, potential suspect activity might not trigger a notification, potentially missing future security-related issues.

For more information about tuning rules, see the *IBM QRadar Tuning Guide*.

View the metrics for a rule

You can view the metrics for a rule from the **Rules** page when you move the mouse pointer over the colored bars in the **Performance** column, and in the **Performance Analysis** textbox, which is in the lower-right corner of the **Rules** page. You can also view the metrics for a rule in the **Rule Wizard** when you edit a rule. The timestamp in the **Performance Analysis** textbox shows when the metrics for the rule were updated. For more information about creating rules, see the Rules topic.

From the **Network Activity** tab or the **Log Activity** tab, click **Rules** to display the **Rules** page. Double-click a rule to open the **Rule Wizard**.



Performance ▲	Rule Name	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin	Creation Date	Modification Date
🟩🟩🟩	Destination Asset Weight is High	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:33...	Dec 5, 2018, 6:03 ...
🟩🟩🟩	Local Mass Mailing Host Detec...	Post-Intrusion Acti...	Custom Rule	Event	True	Dispatch New Event	0	0	System	Jan 12, 2006, 7:03...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Login Failures Followed By Su...	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	1,312,281	1	System	Jun 29, 2010, 6:38...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Source Address is a Known Q...	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:41...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Source Address is a Bogon IP	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:44...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	AssetExclusion: Exclude NetBI...	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 6, 2014, 4:02 ...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Login Failures Followed By Su...	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	0	0	System	Jul 13, 2010, 2:42 ...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	AssetExclusion: Exclude DNS ...	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 6, 2014, 3:58 ...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Source Asset Exists	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:25...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Chained Exploit Followed by S...	Intrusion Detection	Custom Rule	Event	True	Dispatch New Event	0	0	System	Jul 14, 2010, 5:10 ...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Excessive Firewall Denies fro...	Recon	Custom Rule	Event	True	Dispatch New Event	0	0	System	Nov 29, 2005, 8:1...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Multiple Exploit Types Against ...	Intrusion Detection	Custom Rule	Event	True	Dispatch New Event	0	0	System	Jun 22, 2006, 9:50...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Source Asset Weight is Medium	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:30...	Dec 5, 2018, 6:03 ...
🟧🟧⬜	Destination Asset Exists	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:26...	Dec 5, 2018, 6:03 ...
🟥⬜⬜	___genyrule		Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:46 ...	Dec 6, 2018, 4:46 ...
🟥⬜⬜	___genyrule2		Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:57 ...	Dec 6, 2018, 4:59 ...
🟥⬜⬜	___genyrule3		Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:57 ...	Dec 6, 2018, 4:59 ...

Rule

Apply Local Mass Mailing Host Detected on events which are detected by the Local system
and NOT when an event matches any of the following BB:HostDefinition: Mail Servers, BB:HostReference: Mail Servers
and when the event(s) were detected by one or more of Flow Classification Engine
and when any of these BB:CategoryDefinition: Mail Policy Violation with the same source IP more than 20 times, across more than 1 destination IP within 1 minutes
and when the event context is Local to Remote

Notes

Reports a local host sending more than 20 SMTP flows in 1 minute. This may indicate a host being used as a spam relay or infected with a form of mass mailing worm.

Performance Analysis 🟩🟩🟩

4 minutes ago

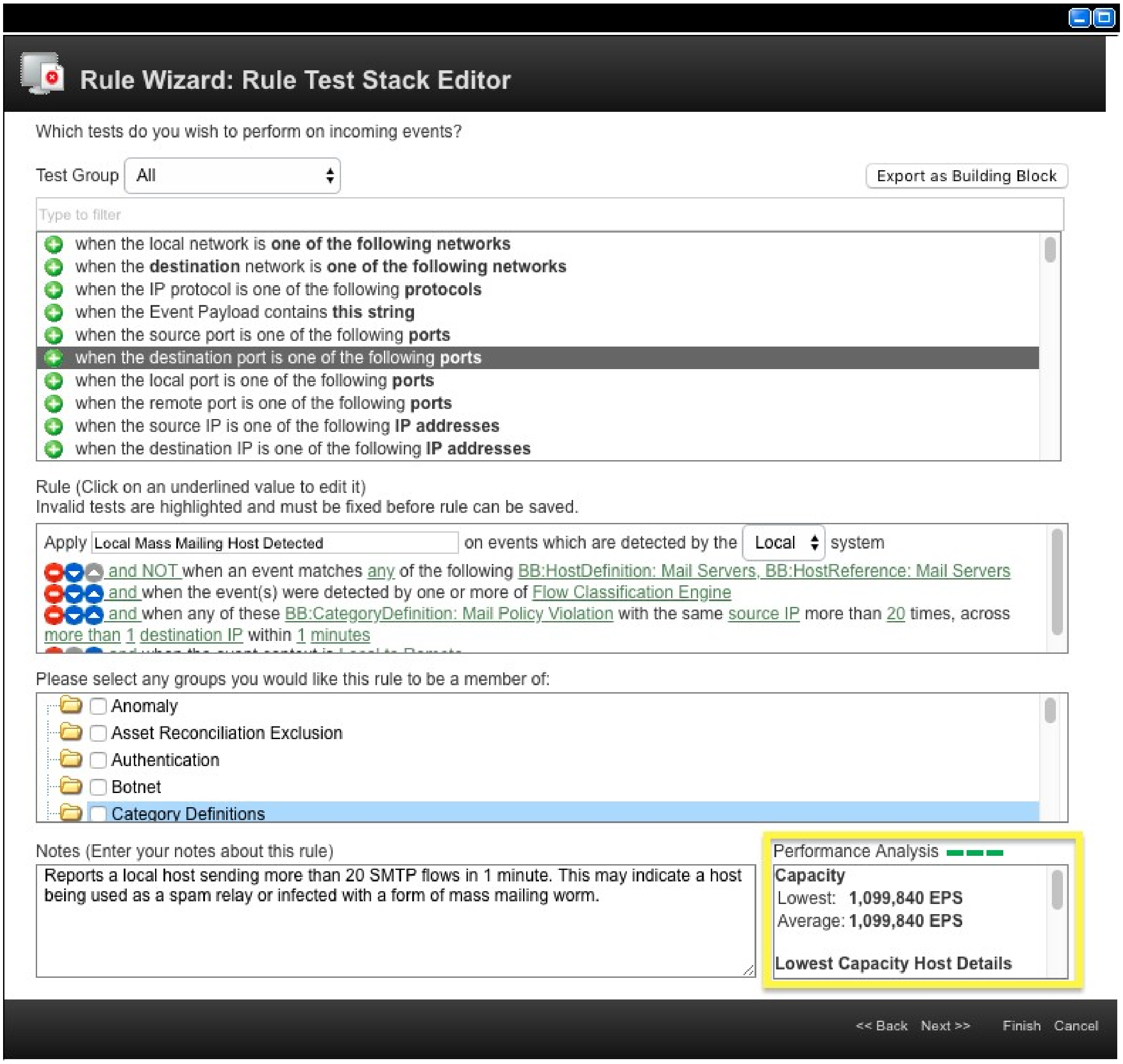
Capacity

Lowest: **1,099,840 EPS**
Average: **1,099,840 EPS**

Lowest Capacity Host Details

Hostname: **ip-125-89 ([redacted])**
Appliance Type: **3199**
License EPS Capacity: **5,000 EPS**
Appliance Capacity: **30,000 EPS**

Figure 11. Performance Analysis on the ***Rules*** *page*



Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group All

Export as Building Block

Type to filter

- when the local network is **one of the following networks**
- when the **destination** network is **one of the following networks**
- when the IP protocol is one of the following **protocols**
- when the Event Payload contains **this string**
- when the source port is one of the following **ports**
- when the destination port is one of the following **ports**
- when the local port is one of the following **ports**
- when the remote port is one of the following **ports**
- when the source IP is one of the following **IP addresses**
- when the destination IP is one of the following **IP addresses**

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Local Mass Mailing Host Detected on events which are detected by the Local system

and NOT when an event matches any of the following BB:HostDefinition: Mail Servers, BB:HostReference: Mail Servers

and when the event(s) were detected by one or more of Flow Classification Engine

and when any of these BB:CategoryDefinition: Mail Policy Violation with the same source IP more than 20 times, across more than 1 destination IP within 1 minutes

Please select any groups you would like this rule to be a member of:

- □ Anomaly
- □ Asset Reconciliation Exclusion
- □ Authentication
- □ Botnet
- □ Category Definitions

Notes (Enter your notes about this rule)

Reports a local host sending more than 20 SMTP flows in 1 minute. This may indicate a host being used as a spam relay or infected with a form of mass mailing worm.

Performance Analysis 🟩🟩🟩

Capacity
Lowest: **1,099,840 EPS**
Average: **1,099,840 EPS**

Lowest Capacity Host Details

Figure 12. Performance Analysis in the ***Rule Wizard***

Colors and bars in the Performance column on the Rules page

The number of bars that display is a visual aid for color blindness.

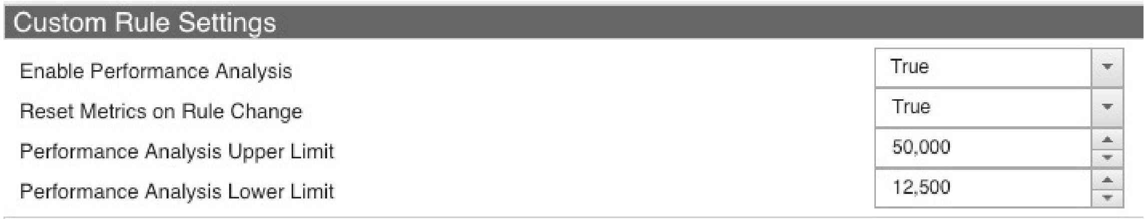
One red bar
: The rule is under-performing and needs to be tuned. The EPS/FPS throughput for this rule is below the lower limit. Open the rule and tune the tests.

Two orange bars
: The rule might need some tuning.

Three green bars
: The rule has a high throughput above the upper limit of the EPS/FPS threshold.

Note: The colors and number of bars can't be changed. The definition of a rule that is under-performing is configurable by an Administrator.

The following image shows the default **Custom Rule Settings** in QRadar.



Custom Rule Settings

Enable Performance Analysis	True
Reset Metrics on Rule Change	True
Performance Analysis Upper Limit	50,000
Performance Analysis Lower Limit	12,500

Figure 13. ***Custom Rule Settings***

For more information about tuning rules, see the Custom" rule testing order" topic in the *IBM QRadar Tuning Guide*.

Related concepts

“Custom rules in IBM QRadar” on page 183
Rules, sometimes called correlation rules are applied to events, flows, or offenses to search for or detect anomalies. If all the conditions of a test are met, the rule generates response.

Chapter 13. Historical correlation

Use historical correlation to run past events and flows through the custom rules engine (CRE) to identify threats or security incidents that already occurred.

Restriction: You cannot use historical correlation in IBM QRadar Log Manager. For more information about the differences between IBM QRadar SIEM and IBM QRadar Log Manager, see Chapter 2, “Capabilities in your IBM QRadar product,” on page 5.

By default, an IBM QRadar SIEM deployment analyzes information that is collected from log sources and flow sources in near real-time. With historical correlation, you can correlate by either the start time or the device time. *Start time* is the time that the event was received by QRadar. *Device time* is the time that the event occurred on the device.

Historical correlation can be useful in the following situations:

Analyzing bulk data

If you bulk load data into your QRadar deployment, you can use historical correlation to correlate the data against data that was collected in real-time. For example, to avoid performance degradation during normal business hours, you load events from multiple log sources every night at midnight. You can use historical correlation to correlate the data by device time to see the sequence of network events as they occurred in the last 24 hours.

Testing new rules

You can run historical correlation to test new rules. For example, one of your servers was recently attacked by new malware for which you do not have rules in place. You can create a rule to test for that malware. Then, you can use historical correlation to check the rule against historical data to see whether the rule would trigger a response if it were in place at the time of the attack. Similarly, you can use historical correlation to determine when the attack first occurred or the frequency of the attack. You can continue to tune the rule and then move it into a production environment.

Re-creating offenses that were lost or purged

If your system lost offenses because of an outage or other reason, you can re-create the offenses by running historical correlation on the events and flows that came in during that time.

Identifying previously hidden threats

As information becomes known about the latest security threats, you can use historical correlation to identify network events that already occurred but did not trigger an event. You can quickly test for threats that have already compromised your organization's system or data.

Historical correlation overview

You configure a historical correlation profile to specify the historical data that you want to analyze and the rule set that you want to test against. When a rule is triggered, an offense is created. You can assign the offense for investigation and remediation.

Data selection

The profile uses a saved search to collect the historical event and flow data to use in the run. Ensure that your security profile grants permission to view the events and flows that you want to include in the historical correlation run.

Rule selection and handling

The QRadar console processes data against only the rules that are specified in the historical correlation profile.

Common rules test data in both events and flows. You must have permission to view both events and flows before you can add common rules to the profile. When a profile is edited by a user who doesn't have permission to view both events and flows, the common rules are automatically removed from the profile.

You can include disabled rules in a historical correlation profile. When the profile runs, the disabled rule is evaluated against the incoming events and flows. If the rule is triggered, and the rule action is to generate an offense, the offense is created even when the rule is disabled. To avoid generating unnecessary distractions, rule responses, such as report generation and mail notifications, are ignored during historical correlation.

Because historical correlation processing occurs in a single location, the rules that are included in the profile are treated as global rules. The processing does not change the rule from local to global, but handles the rule as if it were global during the historical correlation run. Some rules, such as stateful rules, might not trigger the same response as they would in a normal correlation that is run on a local event processor. For example, a local stateful rule that tracks five failed logins in 5 minutes from the same user name behaves differently under normal and historical correlation runs. Under normal correlation, this local rule maintains a counter for the number of failed logins that are received by each local event processor. In historical correlation, this rule maintains a single counter for the entire QRadar system. In this situation, offenses might be created differently compared to a normal correlation run.

Offense creation

Historical correlation runs create offenses only when a rule is triggered and the rule action specifies that an offense must be created. A historical correlation run does not contribute to a real-time offense, nor does it contribute to an offense that was created from an earlier historical correlation run, even when the same profile is used.

The maximum number of offenses that can be created by a historical correlation run is 100. The historical correlation run stops when the limit is reached.

You can view historical offenses on the **Threat and Security Monitoring** dashboard and on the **Offenses** tab at the same time that you review real-time offenses.

Creating a historical correlation profile

You create a historical correlation profile to rerun past events and flows through the custom rules engine (CRE). The profile includes information about the data set and the rules to use during the run.

Restriction: You can create historical profiles only in IBM QRadar SIEM. You cannot create historical profiles in IBM QRadar Log Manager.

Before you begin

Common rules test data in both events and flows. You must have permission to view both events and flows before you can add common rules to the profile. When a profile is edited by a user who doesn't have permission to view both events and flows, the common rules are automatically removed from the profile.

About this task

You can configure a profile to correlate by either start time or device time. *Start time* is the time when the events arrive at the event collector. *Device time* is the time that the event occurred on the device. Events can be correlated by start time or device time. Flows can be correlated by start time only.

You can include disabled rules in the profile. Rules that are disabled are indicated in the rules list with **(Disabled)** after the rule name.

A historical correlation run does not contribute to a real-time offense, nor does it contribute to an offense that was created from an earlier historical correlation run, even when the same profile is used.

⚠ **Attention:** If you create too many historical correlation profiles that have many rules that are assigned to them, your offenses can be slow to load. If your offenses are slow to load, you can either delete unneeded profiles or edit them to have fewer rules.

Procedure

1. Open the Historical Correlation dialog box.
    - On the **Log Activity** tab, click **Actions** > **Historical Correlation**.
    - On the **Network Activity** tab, click **Actions** > **Historical Correlation**.
    - On the **Offenses** tab, click **Rules** > **Actions** > **Historical Correlation**.
2. Click **Add** and select **Event Profile** or **Flow Profile**.
3. Type a name for the profile and select a saved search.

    You can use only non-aggregated saved searches.
4. On the **Rules** tab, select the rules to be run against the historical data, and choose the correlation time.

    If you select the **Use all enabled rules** check box, you cannot include disabled rules in the profile. If you want to include both enabled and disabled rules in the profile, you must select them individually from the rules list and click **Add Selected**.
5. On the **Schedule** tab, enter the time range for the saved search and set the profile schedule settings.
6. On the **Summary** tab, review the configuration and choose whether to run the profile immediately.
7. Click **Save**.

    The profile is put into a queue to be processed. Queued profiles that are based on a schedule take priority over manual runs.

Viewing information about historical correlation runs

View the history of a historical correlation profile to see information about past runs for the profile.

You can see the list of offenses that were created during the run and the catalog of events or flows that match the triggered rules in the profile. You can view the history for historical correlation runs that are queued, running, complete, complete with errors, and canceled.

About this task

For each rule in the profile that contributes to an offense, a catalog is created for each unique value of the property that the offense is indexed on. For each rule that does not contribute to an offense, a single catalog is created.

The following table shows how a historical correlation profile handles catalog creation under different scenarios. In each scenario, the catalog contains all the events or flows that either fully or partially match the triggered rule.

Table 42. Historical correlation catalog examples

Scenario	**Result**
A rule generates offenses that are indexed on source IP address. The events that triggered the rule have three different source IP addresses.	The historical correlation profile creates three catalogs.
A rule generates offenses that are indexed on username. The events that triggered the rule have five different usernames.	The historical correlation profile creates five catalogs.
A rule is triggered, but the rule action does not create an offense.	The historical correlation profile creates a single catalog that includes all events that triggered the rule.

You cannot build reports on historical correlation data directly from QRadar. If you want to use third-party programs to build reports, you can export the data from QRadar.

Procedure

1. Open the **Historical Correlation** dialog box.
   - On the **Log Activity** or **Network Activity** tab, click **Actions** > **Historical Correlation**.
   - On the **Offenses** tab, click **Rules** > **Actions** > **Historical Correlation**.
2. Select a profile and click **View History**.
   a) If the historical correlation run status is **Completed** and the **Offense Count** is 0, the profile rules did not trigger any offenses.
   b) If the historical correlation run created offenses, in the **Offense Count** column, click the link to see a list of the offenses that were created.

      If only one offense was created, the offense summary is shown.
3. In the **Catalogs** column, click the links to see the list of events that either fully or partially match the profile rules.

   The **StartTime** column in the event list represents the time that QRadar received the event.
4. Click **Close**.

Chapter 14. IBM X-Force integration in IBM QRadar

IBM X-Force security experts use a series of international data centers to collect tens of thousands of malware samples, to analyze web pages and URLs, and to run analysis to categorize potentially malicious IP addresses and URLs. You can use this data to identify and remediate undesirable activity in your environment before it threatens the stability of your network.

For example, you can identify and prioritize these types of incidents:

- A series of attempted logins for a dynamic range of IP addresses
- An anonymous proxy connection to a Business Partner portal
- A connection between an internal endpoint and a known botnet command and control
- Communication between an endpoint and a known malware distribution site

IBM Security Threat Content application

The **IBM Security Threat Content** application on the IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub) contains rules, building blocks, and custom properties that are intended for use with the X-Force.

The X-Force data includes a list of potentially malicious IP addresses and URLs with a corresponding threat score. You use the X-Force rules to automatically flag any security event or network activity data that involves the addresses, and to prioritize the incidents before you begin to investigate them.

The following list shows examples of the types of incidents that you can identify using the X-Force rules:

- **when the *[source IP|destinationIP|anyIP]* is part of any of the following *[remote network locations]***
- **when *[this host property]* is categorized by X-Force as *[Anonymization Servers|Botnet C&C|DynamicIPs|Malware|ScanningIPs|Spam]* with confidence value *[equal to] [this amount]***
- **when *[this URL property]* is categorized by X-Force as *[Gambling|Auctions|Job Search|Alcohol|Social Networking|Dating]***

Your QRadar administrator must install the **IBM Security Threat Content** application in order for the rules to appear in the **Threats** group in the **Rules List** window. The rules must be enabled before you can use them.

Enabling X-Force rules in IBM QRadar

By adding the IBM Security Threat Content application to your QRadar system, X-Force rules are added to the **Rules List**. The rules must be enabled before you can use them.

Procedure

1. Click the **Log Activity** tab.
2. On the toolbar, click **Rules** > **Rules**.
3. From the **Group** menu, click **Threats**.

   The **Group** column might show both legacy and enhanced rules. By default, X-Force legacy rules are disabled. However, you might see legacy rules that are enabled. Use the newer enhanced rules in the **Threat** group, and not the legacy rules that use the remote nets.
4. Select the **X-Force** rules in the **Threat** group and click **Actions** > **Enable/Disable**.

IP address and URL categories

X-Force Threat Intelligence categorizes IP address and URL information.

The IP addresses are grouped into the following categories:

- Malware hosts
- Spam sources
- Dynamic IP addresses
- Anonymous proxies
- Botnet Command and Control
- Scanning IP addresses

The X-Force Threat Intelligence feed also categorizes URL addresses. For example, URL addresses might be categorized as dating, gambling, or pornography sites. To see the complete list of categories for URL classification, see the IBM X-Force Exchange website (https://exchange.xforce.ibmcloud.com/faq).

Finding IP address and URL information in X-Force Exchange

Use right-click menu options in IBM QRadar to find information about IP addresses and URLs that is found on IBM Security X-Force Exchange. You can use the information from your QRadar searches, offenses, and rules to research further or to add information about IP addresses or URLs to an X-Force Exchange collection.

About this task

You can contribute either public or private information to track data in collections when you research security issues.

A *collection* is a repository where you store the information that is found during an investigation. You can use a collection to save X-Force Exchange reports, comments, or any other content. An X-Force Exchange report contains both a version of the report from the time when it was saved, and a link to the current version of the report. The collection contains a section that has a wiki-style notepad where you can add comments that are relevant to the collection.

For more information about X-Force Exchange, see X-Force Exchange (https://exchange.xforce.ibmcloud.com/).

Procedure

1. To look up an IP address in X-Force Exchange from QRadar, follow these steps:
   a) Select the **Log Activity** or the **Network Activity** tab.
   b) Right-click the IP address that you want to view in X-Force Exchange and select **More Options** > **Plugin Options** > **X-Force Exchange Lookup** to open the X-Force Exchange interface.
2. To look up a URL in X-Force Exchange from QRadar, follow these steps:
   a) Select either the **Offenses** tab, or the event details windows available on the **Offenses**.
   b) Right-click the URL you want to look up in X-Force Exchange and select **Plugin Options > X-Force Exchange Lookup** to open the X-Force Exchange interface.

Creating a URL categorization rule to monitor access to certain types of websites

You can create a rule that sends an email notification if users of the internal network access URL addresses that are categorized as gambling websites.

Before you begin

To use X-Force data in rules, your administrator must configure QRadar to load data from the X-Force servers.

To create a new rule, you must have the **Offenses** > **Maintain Custom Rules** permission.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Actions** list, select **New Event Rule**.
4. Read the introductory text on the Rule wizard and click **Next**.
5. Click **Events** and click **Next**.
6. From the **Test Group** list box, select **X-Force Tests**.
7. Click the plus (+) sign beside the **when URL (custom) is categorized by X-Force as one of the following categories** test.
8. In the **enter rule name here** field in the Rule pane, type a unique name that you want to assign to this rule.
9. From the list box, select **Local** or **Global**.
10. Click the underlined configurable parameters to customize the variables of the test.
    a) Click **URL (custom)**.
    b) Select the URL property that contains the URL that was extracted from the payload and click **Submit**.
    c) Click **one of the following categories**.
    d) Select **Gambling / Lottery** from the X-Force URL categories, click **Add +** and click **Submit**.
11. To export the configured rule as a building block to use with other rules:
    a) Click **Export as Building Block**.
    b) Type a unique name for this building block.
    c) Click **Save**.
12. On the Groups pane, select the check boxes of the groups to which you want to assign this rule.
13. In the **Notes** field, type a note that you want to include for this rule, and click **Next**.
14. On the **Rule Responses** page, click **Email** and type the email addresses that receive the notification.
15. Click **Next**.
16. If the rule is accurate, click **Finish**.

Confidence factor and IP address reputation

IP address reputation data is evaluated on the time that it is seen and the volume of messages or data. X-Force categorizes IP address reputation data and assigns a confidence factor value 0 - 100, where 0 represents no confidence and 100 represents certainty. For example, X-Force might categorize a source IP address as a scanning IP with a confidence factor of 75, which is a moderately high level of confidence.

Determining a threshold

As an example, spam messages with an IP address reputation entry of 0 indicates that the source IP traffic is not spam, whereas an entry of 100 indicates definite spam traffic. Thus, values less than 50 indicate less probability that the message is spam, and values greater than 50 indicate more probability that the message is spam. A value of 50 or higher is the threshold where you might consider action on a triggered rule.

These probabilities are based on ongoing web-based data that IBM Security X-Force Threat Intelligence continuously collects and analyzes from around the world in X-Force data centers. As data is collected, the system evaluates how much spam is received from a particular IP address, or how frequently the flagged IP address is in the IP address reputation category. The more times, the higher the system scores the confidence factor.

Tuning false positives with the confidence factor setting

Use the confidence factor to limit the number of offenses that are created by triggered rules. Depending on the level of protection that you want, you adjust the confidence values to a level that best matches your network environment.

About this task

When you tune rules, consider a scale where 50 is the tipping point. On assets of lower importance, you might weigh an X-Force rule to trigger at a higher confidence factor for specific categories, like spam. For example, tuning a rule to a confidence factor of 75 means the rule triggers only when X-Force sees an IP address at or above a confidence factor of 75. This tuning reduces the number of offenses that are generated on lower priority systems and non-critical assets. However, an important system or critical business asset with a confidence factor of 50 triggers an offense at a lower level and brings attention to an issue more quickly.

For your DMZ, choose a higher confidence value such as 95% or higher. You do not need to investigate many offenses in this area. With a high confidence level, the IP addresses are more likely to match the category that is listed. If it is 95% certain that a host is serving malware, then you need to know about it.

For more secure areas of the network, like a server pool, lower the confidence value. More potential threats are identified and you spend less effort investigating because the threat pertains to a specific network segment.

For optimum false positive tuning, manage your rule triggers by segment. Look at your network infrastructure and decide which assets need a high level of protection, and which assets do not. You can apply different confidence values for the different network segments. Use building blocks for grouping commonly used tests so that they can be used in rules.

Procedure

1. Click the **Log Activity** tab.
2. On the toolbar, click **Rules** > **Rules**.
3. Double-click a rule to start the Rule wizard.
4. In the filter box, type the following text:

   ```
   when this host property is categorized by X-Force as this category with
   confidence value equal to this amount
   ```
5. Click the **Add test to rule (+)** icon.
6. In the Rule section, click the `this amount` link.
7. Enter a confidence value.
8. Click **Submit**.
9. Click **Finish** to exit the Rules wizard.

Searching data from IBM X-Force Exchange with advanced search criteria

For complex queries, you can search and filter data from X-Force Exchange by using Advanced Search expressions.

About this task

Advanced searches return data from the **Log Activity** or the **Network Activity** tab in QRadar.

URL searches cannot be returned from the **Network Activity** tab because the URL information is provided by the event data.

For a list of parameters and functions available when you search for data from IBM X-Force Exchange, see https://exchange.xforce.ibmcloud.com/faq#ipr_categories_list

Procedure

1. Click the **Log Activity** tab.
2. On the **Search** toolbar, select the **Advanced Search**.
3. Type an AQL query expression.

   The following table describes some common search expressions.

Table 43. X-Force advanced search expressions

Description	Example

Searches for HTTP hosts from flows that match a bad category.	`select * from flows where`
	`XFORCE_URL_CATEGORY("HTTP Host") in`
	`('Anonymization Services','Malware',`
	`'Botnet Command and Control Server', 'Spam URLs',`
	`'Cryptocurrency Mining', 'Bots', 'Phishing URLs')`

Searches for URLs found in events that match a bad category.	`select * from events where`
	`XFORCE_URL_CATEGORY("UrlHost") in ('Anonymization`
	`Services','Malware', 'Botnet Command and Control`
	`Server',`
	`'Spam URLs', 'Cryptocurrency Mining', 'Bots',`
	`'Phishing URLs')`

Searches for IP addresses that match a bad category with a confidence factor above 75.	`select * from events where`
	`XFORCE_IP_CONFIDENCE('Anonymization`
	`Services',destinationaddress) > 75 OR`
	`XFORCE_IP_CONFIDENCE('Malware',destinationaddress)`
	` > 75 OR`
	`XFORCE_IP_CONFIDENCE('Botnet Command and Control`
	`Server',destinationaddress) > 75 OR`
	`XFORCE_IP_CONFIDENCE('Spam',destinationaddress) >`
	`75 OR`
	`XFORCE_IP_CONFIDENCE('Cryptocurrency`
	`Mining',destinationaddress) > 75 OR`
	`XFORCE_IP_CONFIDENCE('Scanning`
	`IPs',destinationaddress) > 75 OR`
	`XFORCE_IP_CONFIDENCE('Bots',destinationaddress) >`
	`75 OR`
	`XFORCE_IP_CONFIDENCE('Anonymization`
	`Services',sourceaddress) > 75 OR`
	`XFORCE_IP_CONFIDENCE('Malware',sourceaddress) >`
	`75 OR`
	`XFORCE_IP_CONFIDENCE('Botnet Command and Control`
	`Server',sourceaddress) > 75 OR`
	`XFORCE_IP_CONFIDENCE('Spam',sourceaddress) > 75`
	`OR`
	`XFORCE_IP_CONFIDENCE('Cryptocurrency`
	`Mining',sourceaddress) > 75 OR`
	`XFORCE_IP_CONFIDENCE('Scanning`
	`IPs',sourceaddress) > 75 OR`
	`XFORCE_IP_CONFIDENCE('Bots',sourceaddress) > 75`

Searches associated with a URL.	`select url,`
	`XFORCE_URL_CATEGORY(url)`
	`as myCategories from events where`
	`XFORCE_URL_CATEGORY(url) IS NOT NULL`

Table 43. X-Force advanced search expressions (continued)

Description	Example

Searches associated with a source IP address.	`select sourceip,`
	`XFORCE_IP_CATEGORY(sourceip)`
	`as IPcategories from events where`
	`XFORCE_IP_CATEGORY(destinationip) in ('Malware',`
	`'Botnet Command and Control Server',`
	`'Spam', 'Cryptocurrency Mining', 'Scanning IPs',`
	`'Bots', 'Phishing')`

4. Click **Search**.

Related information

Chapter 15. Report management

You can use the **Reports** tab to create, edit, distribute, and manage reports.

Detailed, flexible reporting options satisfy your various regulatory standards, such as PCI compliance.

You can create your own custom reports or use a default reports. You can customize and rebrand default reports and distribute these to other users.

The **Reports** tab might require an extended period of time to refresh if your system includes many reports.

Note: If you are running Microsoft Exchange Server 5.5, unavailable font characters might be displayed in the subject line of emailed reports. To resolve this, download and install Service Pack 4 of Microsoft Exchange Server 5.5. For more information, contact Microsoft support.

Timezone considerations

To ensure that the Reports feature uses the correct date and time for reporting data, your session must be synchronized with your timezone.

During the installation and setup of QRadar products, the time zone is configured. Check with your administrator to ensure your QRadar session is synchronized with your timezone.

Report tab permissions

Administrative users can view all reports that are created by other users.

Non-administrative users can view reports that they created only or reports that are shared by other users.

Report tab parameters

The **Reports** tab displays a list of default and custom reports.

From the **Reports** tab, you can view statistical information about the reports template, perform actions on the report templates, view the generated reports, delete generated content.

If a report does not specify an interval schedule, you must manually generate the report.

You can point your mouse over any report to preview a report summary in a tooltip. The summary specifies the report configuration and the type of content the report generates.

Report layout

A report can consist of several data elements and can represent network and security data in various styles, such as tables, line charts, pie charts, and bar charts.

When you select the layout of a report, consider the type of report you want to create. For example, do not choose a small chart container for graph content that displays many objects. Each graph includes a legend and a list of networks from which the content is derived; choose a large enough container to hold the data. To preview how each chart displays a data, see Graph types.

Chart types

When you create a report, you must choose a chart type for each chart you include in your report.

The chart type determines how the data and network objects appear in your report.

You can use any of the following types of charts:

Table 44. Chart Types

Chart Type	**Description**
None	Use this option if you need white space in your report. If you select the None option for any container, no further configuration is required for that container.
Asset Vulnerabilities	Use this chart to view vulnerability data for each defined asset in your deployment. You can generate Asset Vulnerability charts when vulnerabilities have been detected by a VA scan. This chart is available after you install IBM QRadar Vulnerability Manager.
Connections	This chart option is only displayed if you purchased and licensed IBM QRadar Risk Manager. For more information, see the *IBM QRadar Risk Manager User Guide*.
Device Rules	This chart option is only displayed if you purchased and licensed IBM QRadar Risk Manager. For more information, see the *IBM QRadar Risk Manager User Guide*.
Device Unused Objects	This chart option is only displayed if you purchased and licensed IBM QRadar Risk Manager. For more information, see the *IBM QRadar Risk Manager User Guide*.
Events/Logs	Use this chart to view event information. You can base a chart on data from saved searches on the **Log Activity** tab. You can configure the chart to plot data over a configurable period of time to detect event trends. For more information about saved searches, see Chapter 10, “Event and flow searches,” on page 139.
Log Sources	Use this chart to export or report on log sources. Select the log sources and log source groups that you want to appear in the report. Sort log sources by report columns. Include log sources that are not reported for a defined time period. Include log sources that were created in a specified time period.
Flows	Use this chart to view flow information. You can base a chart on data from saved searches on the **Network Activity** tab. You can configure the chart to plot flow data over a configurable period of time to detect flow trends. For more information about saved searches, see Chapter 10, “Event and flow searches,” on page 139.
Top Destination IPs	Use this chart to display the top destination IPs in the network locations you select.
Top Offenses	Use this chart to display the top offenses that occur at present time for the network locations you select.

Table 44. Chart Types (continued)

Chart Type	Description
Offenses Over Time	Use this chart to display all offenses that have a start time within a defined time span for the network locations you select.
Top Source IPs	Use this chart to display and sort the top offense sources (IP addresses) that attack your network or business assets.
Vulnerabilities	The Vulnerabilities option is only displayed when the IBM QRadar Vulnerability Manager was purchased and licensed. For more information, see the *IBM QRadar Vulnerability Manager User Guide*.

Table 45. Chart Types

Chart Type	Description
None	Use this option if you need white space in your report. If you select the None option for any container, no further configuration is required for that container.
Asset Vulnerabilities	Use this chart to view vulnerability data for each defined asset in your deployment. You can generate Asset Vulnerability charts when vulnerabilities have been detected by a VA scan. This chart is available after you install IBM QRadar Vulnerability Manager.
Vulnerabilities	The Vulnerabilities option is only displayed when the IBM QRadar Vulnerability Manager was purchased and licensed. For more information, see the *IBM QRadar Vulnerability Manager User Guide*.

Report tab toolbar

You can use the toolbar to perform a number of actions on reports.

The following table identifies and describes the Reports toolbar options.

Table 46. Report toolbar options

Option	Description
Group	
Manage Groups	Click **Manage Groups** to manage report groups. Using the Manage Groups feature, you can organize your reports into functional groups. You can share report groups with other users.

Table 46. Report toolbar options (continued)

Option	Description
Actions	Click **Actions** to perform the following actions: • **Create** - Select this option to create a new report. • **Edit** - Select this option to edit the selected report. You can also double-click a report to edit the content. • **Duplicate** - Select this option to duplicate or rename the selected report. • **Assign Groups** - Select this option to assign the selected report to a report group. • **Share** - Select this option to share the selected report with other users. You must have administrative privileges to share reports. • **Toggle Scheduling** - Select this option to toggle the selected report to the Active or Inactive state. • **Run Report** - Select this option to generate the selected report. To generate multiple reports, hold the Control key and click on the reports you want to generate. • **Run Report on Raw Data** - Select this option to generate the selected report using raw data. This option is useful when you want to generate a report before the required accumulated data is available. For example, if you want to run a weekly report before a full week has elapsed since you created the report, you can generate the report using this option. • **Delete Report** - Select this option to delete the selected report. To delete multiple reports, hold the Control key and click on the reports you want to delete. • **Delete Generated Content** - Select this option to delete all generated content for the selected rows. To delete multiple generated reports, hold the Control key and click on the generate reports you want to delete.
Hide Interactive Reports	Select this check box to hide inactive report templates. The **Reports** tab automatically refreshes and displays only active reports. Clear the check box to show the hidden inactive reports.

Table 46. Report toolbar options (continued)

Option	Description
Search Reports	Type your search criteria in the **Search Reports** field and click the **Search Reports** icon. A search is run on the following parameters to determine which match your specified criteria: • Report Title • Report Description • Report Group • Report Groups • Report Author User Name

Graph types

Each chart type supports various graph types that you can use to display data.

The network configuration files determine the colors that the charts use to depict network traffic. Each IP address is depicted by using a unique color. The following table provides examples of how network and security data is used in charts. The table describes the chart types that are available for each type of graph.

Table 47. Graph types

Graph type	Available chart types
Line	• Events/Logs • Flows • Connections • Vulnerabilities
Stacked Line	• Events/Logs • Flows • Connections • Vulnerabilities
Bar	• Events/Logs • Flows • Asset Vulnerabilities Connections • Connections • Vulnerabilities
Horizontal Bar	• Top Source IPs • Top Offenses • Offenses Over Time • Top Destination IPs
Stacked Bar	• Events/Logs • Flows • Connections

Table 47. Graph types (continued)

Graph type	Available chart types
Pie	• Events/Logs • Flows • Asset Vulnerabilities • Connections • Vulnerabilities
Table	• Events/Logs • Flows • Top Source IPs • Top Offenses • Offenses Over Time • Top Destination IPs • Connections • Vulnerabilities To display content in a table, you must design the report with a full page width container.
Aggregate Table	Available with the Asset Vulnerabilities chart. To display content in a table, you must design the report with a full page width container.

The following graph types are available for QRadar Log Manager reports:

- Line
- Stacked Line
- Bar
- Stacked Bar
- Pie
- Table

Note: When you create bar and stacked bar graph reports, the legend is presented in a fixed format and the bars or bar sections are represented by color coded labels in most cases. If you select time as the value for the x axis, you can create time intervals on the x axis.

Creating custom reports

Use the Report wizard to create and customize a new report.

Before you begin

You must have appropriate network permissions to share a generated report with other users.

For more information about permissions, see the *IBM QRadar Administration Guide*.

About this task

The Report wizard provides a step-by-step guide on how to design, schedule, and generate reports.

The wizard uses the following key elements to help you create a report:

- **Layout** - Position and size of each container
- **Container** - Placeholder for the featured content
- **Content** - Definition of the chart that is placed in the container

After you create a report that generates weekly or monthly, the scheduled time must elapse before the generated report returns results. For a scheduled report, you must wait the scheduled time period for the results to build. For example, a weekly search requires seven days to build the data. This search will return results after 7 days.

When you specify the output format for the report, consider that the file size of generated reports can be one to 2 megabytes, depending on the selected output format. PDF format is smaller in size and does not use a large quantity of disk storage space.

Procedure

1. Click the **Reports** tab.
2. From the **Actions** list box, select **Create**.
3. On the **Welcome to the Report wizard!** window, click **Next**.
4. Select one of the following options:

Option	Description
Manually	By default, the report generates 1 time. You can generate the report as often as you want.
Hourly	Schedules the report to generate at the end of each hour. The data from the previous hour is used. From the list boxes, select a time frame to begin and end the reporting cycle. A report is generated for each hour within this time frame. Time is available in half-hour increments. The default is 1:00 a.m for both the **From** and **To** fields.
Daily	Schedules the report to generate at the end of each day. The data from the previous day is used. From the list boxes, select the time and the days of the week that you want the report to run.
Weekly	Schedules the report to generate weekly using the data from the previous calendar week, from Monday to Sunday. Select the day that you want to generate the report. The default is Monday. From the list box, select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.
Monthly	Schedules the report to generate monthly using the data from the previous calendar month. From the list box, select the date that you want to generate the report. The default is the first day of the month. Select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.

5. In the **Allow this report to generate manually** pane, **Yes** or **No**.
6. Configure the layout of your report:
   a) From the **Orientation** list box, select **Portrait** or **Landscape** for the page orientation.
   b) Select one of the six layout options that are displayed on the Report wizard.
   c) Click **Next** .
7. Specify values for the following parameters:

Parameter	Values
Report Title	The title can be up to 60 characters in length. Do not use special characters.
Logo	From the list box, select a logo.
Pagination Options	From the list box, select a location for page numbers to display on the report. You can choose not to have page numbers display.
Report Classification	Type a classification for this report. You can type up to 75 characters in length. You can use leading spaces, special characters, and double byte characters. The report classification displays in the header and footer of the report. You might want to classify your report as `confidential`, `highly confidential`, `sensitive`, or `internal`.

8. Configure each container in the report:
   a) From the **Chart Type** list box, select a chart type.
   b) On the **Container Details** window, configure the chart parameters.

      Note: You can also create asset saved searches. From the **Search to use** list box, select your saved search.
   c) Click **Save Container Details**.
   d) If you selected more than one container, repeat steps a to c.
   e) Click **Next** .
9. Preview the **Layout Preview** page, and then click **Next**.
10. Select the check boxes for the report formats you want to generate, and then click **Next**.

    Important: Extensible Markup Language is only available for tables.
11. Select the distribution channels for your report, and then click **Next**. Options include the following distribution channels:

Option	Description
Report Console	Select this check box to send the generated report to the **Reports** tab. **Report Console** is the default distribution channel.
Select the users that should be able to view the generated report.	This option displays after you select the **Report Console** check box. From the list of users, select the users that you want to grant permission to view the generated reports.
Select all users	This option is only displayed after you select the **Report Console** check box. Select this check box if you want to grant permission to all users to view the generated reports. You must have appropriate network permissions to share the generated report with other users.
Email	Select this check box if you want to distribute the generated report by email.
Enter the report distribution email address(es)	This option is only displayed after you select the **Email** check box. Type the email address for each generated report recipient; separate a list of email addresses with commas. The maximum characters for this parameter are 255. Email recipients receive this email from no_reply_reports@qradar.
Include Report as attachment (non-HTML only)	This option is only displayed after you select the **Email** check box. Select this check box to send the generated report as an attachment.

Option	Description
Include link to Report Console	This option is only displayed after you select the **Email** check box. Select this check box to include a link to the Report Console in the email.

12. On the **Finishing Up** page, enter values for the following parameters.

Option	Description
Report Description	Type a description for this report. The description is displayed on the **Report Summary** page and in the generated report distribution email.
Please select any groups you would like this report to be a member of	Select the groups to which you want to assign this report. For more information about groups, see Report groups.
Would you like to run the report now?	Select this check box if you want to generate the report when the wizard is complete. By default, the check box is selected.

13. Click **Next** to view the report summary.
14. On the **Report Summary** page, select the tabs available on the summary report to preview your report configuration.

Results

The report immediately generates. If you cleared the **Would you like to run the report now** check box on the final page of the wizard, the report is saved and generates at the scheduled time. The report title is the default title for the generated report. If you reconfigure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Related information

Creating reports in QRadar SIEM

Editing a report

Using the Report wizard, you can edit any default or custom report to change.

About this task

You can use or customize a significant number of default reports. The default **Reports** tab displays the list of reports. Each report captures and displays the existing data.

Note: When you customize a scheduled report to generate manually, select the time span **End Date** before you select the **Start Date**.

Procedure

1. Click the **Reports** tab.
2. Double-click the report that you want to customize.
3. On the Report wizard, change the parameters to customize the report to generate the content you require.

Results

If you reconfigure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Viewing generated reports

On the **Reports** tab, an icon is displayed in the **Formats** column if a report has generated content. You can click the icon to view the report.

About this task

When a report has generated content, the **Generated Reports** column displays a list box. The list box displays all generated content, which is organized by the time-stamp of the report. The most recent reports are displayed at the top of the list. If a report has no generated content, the **None** value is displayed in the **Generated Reports** column.

Icons representing the report format of the generated report are displayed in the **Formats** column.

Reports can be generated in PDF, HTML, XML, and XLS formats.

Note: The XML and XLS formats are available only for reports that use a single chart table format (portrait or landscape).

You can view only the reports to which you have been given access from the administrator. Administrative users can access all reports.

Procedure

1. Click the **Reports** tab.
2. From the list box in the **Generated Reports** column, select the time-stamp of report you want to view.
3. Click the icon for the format you want to view.

Deleting generated content

When you delete generated content, all reports that have generated from the report template are deleted, but the report template is retained.

Procedure

1. Click the **Report**s tab.
2. Select the reports for which you want to delete the generated content.
3. From the **Actions** list box, click **Delete Generated Content**.

Manually generating a report

A report can be configured to generate automatically, however, you can manually generate a report at any time.

About this task

While a report generates, the Next Run Time column displays one of the three following messages:

- **Generating** - The report is generating.
- **Queued (position in the queue)** - The report is queued for generation. The message indicates the position that the report is in the queue. For example, 1 of 3.
- **(x hour(s) x min(s) y sec(s))** - The report is scheduled to run. The message is a count-down timer that specifies when the report will run next.

You can select the **Refresh** icon to refresh the view, including the information in the **Next Run Time** column.

Procedure

1. Click the **Reports** tab.
2. Select the report that you want to generate.
3. Click **Run Report**.

What to do next

After the report generates, you can view the generated report from the Generated Reports column.

Duplicating a report

To create a report that closely resembles an existing report, you can duplicate the report that you want to model, and then customize it.

Procedure

1. Click the **Reports** tab.
2. Select the report that you want to duplicate.
3. From the **Actions** list box, click **Duplicate**.
4. Type a new name, without spaces, for the report.

What to do next

You can customize the duplicated report.

Sharing a report

You can share reports with other users. When you share a report, you provide a copy of the selected report to another user to edit or schedule.

About this task

Any updates that the user makes to a shared report does not affect the original version of the report.

You must have administrative privileges to share reports. Also, for a new user to view and access reports, an administrative user must share all the necessary reports with the new user.

You can only share the report with users that have the appropriate access.

Procedure

1. Click the **Reports** tab.
2. Select the reports that you want to share.
3. From the **Actions** list box, click **Share**.
4. From the list of users, select the users with whom you want to share this report.

Branding reports

To brand reports, you can import logos and specific images. To brand reports with custom logos, you must upload and configure the logos before you begin using the Report wizard.

Before you begin

Ensure that the graphic you want to use is 144 x 50 pixels with a white background.

To make sure that your browser displays the new logo, clear your browser cache.

About this task

Report branding is beneficial for your enterprise if you support more than one logo. When you upload an image, the image is automatically saved as a Portable Network Graphic (PNG).

When you upload a new image and set the image as your default, the new default image is not applied to reports that have been previously generated. Updating the logo on previously generated reports requires you to manually generate new content from the report.

If you upload an image that is larger in length than the report header can support, the image automatically resizes to fit the header; this is approximately 50 pixels in height.

Procedure

1. Click the **Reports** tab.
2. On the navigation menu, click **Branding**.
3. Click **Browse** to browse the files that are located on your system.
4. Select the file that contains the logo you want to upload. Click **Open**.
5. Click **Upload Image**.
6. Select the logo that you want to use as the default and click **Set Default Image**.

Report groups

You can sort reports into functional groups. If you categorize reports into groups, you can efficiently organize and find reports.

For example, you can view all reports that are related to Payment Card Industry Data Security Standard (PCIDSS) compliance.

By default, the **Reports** tab displays the list of all reports, however, you can categorize reports into groups such as:

- Compliance
- Executive
- Log Sources
- Network Management
- Security
- VoIP
- Other

When you create a new report, you can assign the report to an existing group or create a new group. You must have administrative access to create, edit, or delete groups.

For more information about user roles, see the *IBM QRadar Administration Guide*.

Creating a report group

You can create new groups.

Procedure

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. Using the navigation tree, select the group under which you want to create a new group.
4. Click **New Group**.
5. Enter values for the following parameters:
   - **Name** - Type the name for the new group. The name can be up to 255 characters in length.

- **Description** - Optional. Type a description for this group. The description can be up to 255 characters in length.

6. Click **OK**.
7. To change the location of the new group, click the new group and drag the folder to the new location on the navigation tree.
8. Close the **Report Groups** window.

Editing a group

You can edit a report group to change the name or description.

Procedure

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. From the navigation tree, select the group that you want to edit.
4. Click **Edit**.
5. Update values for the parameters, as necessary:
    - **Name** - Type the name for the new group. The name can be up to 255 characters in length.
    - **Description** - Optional. Type a description for this group. The description can be up to 255 characters in length. This field is optional.
6. Click **OK**.
7. Close the **Report Groups** window.

Sharing report groups

You can share report groups with other users.

Before you begin

You must have administrative permissions to share a report group with other users.

For more information about permissions, see the *IBM QRadar Administration Guide*.

You cannot use the Content Management Tool (CMT) to share report groups.

For more information about the CMT, see the *IBM QRadar Administration Guide*

About this task

On the **Report Groups** window, shared users can see the report group in the report list.

To view a generated report, the user must have permission to view the report.

Procedure

1. Click the **Reports** tab.
2. On the **Reports** window, click **Manage Groups**.
3. On the **Report Groups** window, select the report group that you want to share and click **Share**.
4. On the **Sharing Options** window, select one of the following options.

Option	Description
Default (inherit from parent)	The report group is not shared. Any copied report group or generated report remains in the users report list.

Option	Description
	Each report in the group is assigned any parent report sharing option that was configured.
Share with Everyone	The report group is shared with all users. **Restriction:** You must have the Admin security profile to share search requirements.
Share with users matching the following criteria...	The report group is shared with specific users. **User Roles** Select from the list of user roles and press the add icon (+). **Security Profiles** Select from the list of security profiles and press the add icon (+).

5. Click **Save**.

Results

On the **Report Groups** window, shared users see the report group in the report list. Generated reports display content based on security profile setting.

Related tasks

"Creating custom reports" on page 218
Use the Report wizard to create and customize a new report.

Assign a report to a group

You can use the **Assign Groups** option to assign a report to another group.

Procedure

1. Click the **Reports** tab.
2. Select the report that you want to assign to a group.
3. From the **Actions** list box, select **Assign Groups**.
4. From the **Item Groups** list, select the check box of the group you want to assign to this report.
5. Click **Assign Groups**.

Copying a report to another group

Use the **Copy** icon to copy a report to one or more report groups.

Procedure

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. From the navigation tree, select the report that you want to copy.
4. Click **Copy**.
5. Select the group or groups to which you want to copy the report.
6. Click **Assign Groups**.
7. Close the **Report Groups** window.

Removing a report

Use the **Remove** icon to remove a report from a group.

About this task

When you remove a report from a group, the report still exists on the **Reports** tab. The report is not removed from your system.

Procedure

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. From the navigation tree, navigate to the folder that contains the report you want to remove.
4. From the list of groups, select the report that you want to remove.
5. Click **Remove**.
6. Click **OK**.
7. Close the **Report Groups** window.

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.

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.

The registered trademark Linux®® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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".

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr

Glossary

This glossary provides terms and definitions for the IBM QRadar software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

accumulator
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

active system
In a high-availability (HA) cluster, the system that has all of its services running.

Address Resolution Protocol (ARP)
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

administrative share
A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

anomaly
A deviation from the expected behavior of the network.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

ARP
See Address Resolution Protocol.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN
See autonomous system number.

asset
A manageable object that is either deployed or intended to be deployed in an operational environment.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior
The observable effects of an operation or event, including its results.

bonded interface
See link aggregation.

burst
A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR
See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client
A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A display station from which an operator can control and observe the system operation.

content capture
A process that captures a configurable amount of payload and then stores the data in a flow log.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS
See Common Vulnerability Scoring System.

D

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.

DHCP
See Dynamic Host Configuration Protocol.

DNS
See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

DSM
See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

endpoint
The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

external scanning appliance
A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive
An event or flow that the user can decide should not create an offense, or an offense that the user decides is not a security incident.

flow
A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway
A device or program used to connect networks or systems with different network architectures.

H

HA
See high availability.

HA cluster
A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

I

ICMP
See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

IDS
See intrusion detection system.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

Internet service provider (ISP)
An organization that provides access to the Internet.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP
See Internet Protocol.

IP multicast
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPS
See intrusion prevention system.

ISP
See Internet service provider.

K

key file
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L
See Local To Local.

L2R
See Local To Remote.

LAN
See local area network.

LDAP
See Lightweight Directory Access Protocol.

leaf
In a tree, an entry or node that has no children.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

link aggregation
The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

live scan
A vulnerability scan that generates report data from the scan results based on the session name.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.

Local To Remote (L2R)
Pertaining to the internal traffic from one local network to another remote network.

log source
Either the security equipment or the network equipment from which an event log originates.

log source extension
An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT
See network address translation.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
A type of container that is a hierarchical collection of network objects.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
A component of a network hierarchy.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI
See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID
See “QRadar Identifier (QID)” on page 238.

QID Map
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

QRadar Identifier (QID)
A numeric representation of a specific event. Each QID includes a name, description, severity, and low-level category.

R

R2L
See Remote To Local.

R2R
See Remote To Remote.

recon
See reconnaissance.

reconnaissance (recon)
A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance
A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L)
The external traffic from a remote network to a local network.

Remote To Remote (R2R)
The external traffic from a remote network to another remote network.

report
In query management, the formatted data that results from running a query and applying a form to it.

report interval
A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule
A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule
A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner
An automated security program that searches for software vulnerabilities within web applications.

secondary HA host
The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity
A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

SOAP
A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork.

subnet mask
For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search
A function that allows a search query to be performed within a set of completed search results.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view
A visual representation of both primary and managed hosts that compose a system.

T

TCP
See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

truststore file
A key database file that contains the public keys for a trusted entity.

V

violation
An act that bypasses or contravenes corporate policy.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

whois server

A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

Index

IBM®