IBM

Lab guide

# Using IBM QRadar SIEM

Course code LSL0232X

## August 2020 edition

# Contents

# Exercises

With IBM® Security QRadar® SIEM you can minimize the time gap between when a suspicious activity occurs and when you detect it. Attacks and policy violations leave their footprints in log events and the network flows of your IT systems. QRadar SIEM connects the dots and provides you insight by performing the following tasks:

- Alerts to suspected attacks and policy violations in the IT environment
- Provides deep visibility into network, user, and application activity
- Puts security-relevant data from various sources in context with each other
- Provides reporting templates to meet operational and compliance requirements
- Provides reliable, tamper-proof log storage for forensic investigations and evidential use

The exercises in this lab provide a broad introduction to the features of QRadar SIEM. The exercises cover the following topics:

- Navigating the web interface
- Investigating a suspicious activity
- Creating a report
- Managing the network hierarchy

**Important:** These exercises are presented in a virtual lab format. A virtual lab is an interactive simulation of the original virtual machines. A virtual lab is not an actual virtual machine. Therefore, your interaction opportunities are restricted to the exercise steps with some minor variance. You use this lab guide, which walks you through usage and responses for the components that are taught.

You can run the virtual lab multiple times without restriction.

## Virtual machines

This virtual lab simulates the following environment:

- QRadar 7.4.0 fp4 - a virtual machine running IBM QRadar on Red Hat Enterprise Linux.
- CentOS Client - a virtual machine providing a graphical user interface. Your interaction with QRadar is done by using this virtual machine.

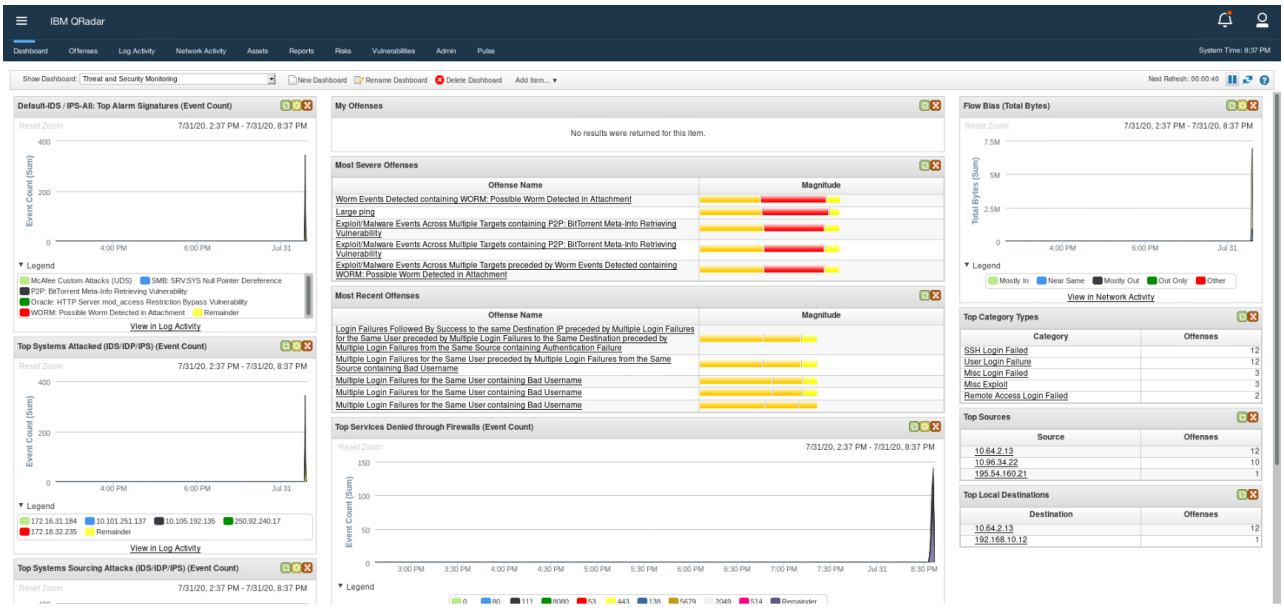
# Exercise 1 Logging in to the QRadar SIEM Console

Before attempting to create a report, you must first have available data for it to display. This lab environment automatically feeds prepared sample data to QRadar a few minutes before you start following the steps in this guide.

1. To start the web browser, double-click the **Firefox** icon on the desktop.


2. On the QRadar login page, the **Username** and **Password** fields are already populated. To access to QRadar Console in the Firefox browser, click **Login**.

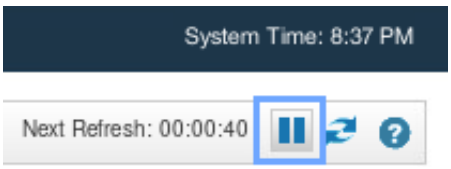
After logging in, you see a web interface similar to the one in the following image.



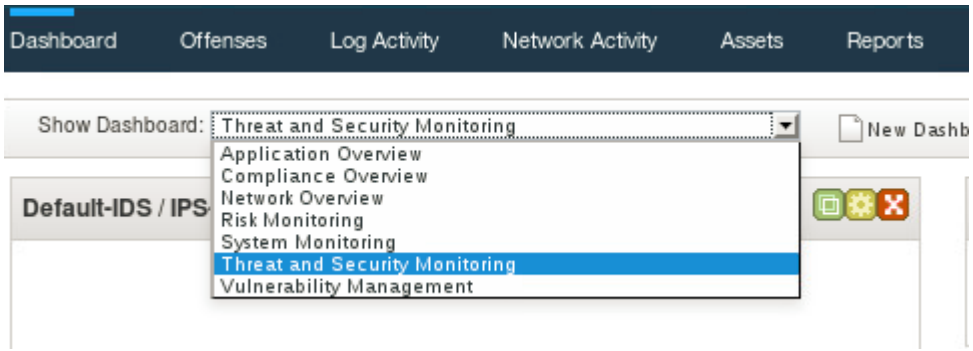

# Exercise 2 Using dashboards and dashboard items

QRadar SIEM displays the Dashboard tab when you log in to QRadar SIEM. Multiple items on a dashboard display information about activities in your environment. With these items,you can focus on specific areas of interest such as security or network operations. You can customize each dashboard to meet the needs and responsibilities of the analyst. In this exercise, you use the Dashboard tab to watch network activities in your lab environment.

1. Each dashboard displays items that provide information that is derived from the data that is fed into QRadar SIEM. QRadar SIEM refreshes the information on the Dashboard tab every minute. Data is fed into the Dashboard automatically. To pause the refreshing of the Dashboard, click the Pause button located in the upper right of the toolbar. The button changes to a Play button.

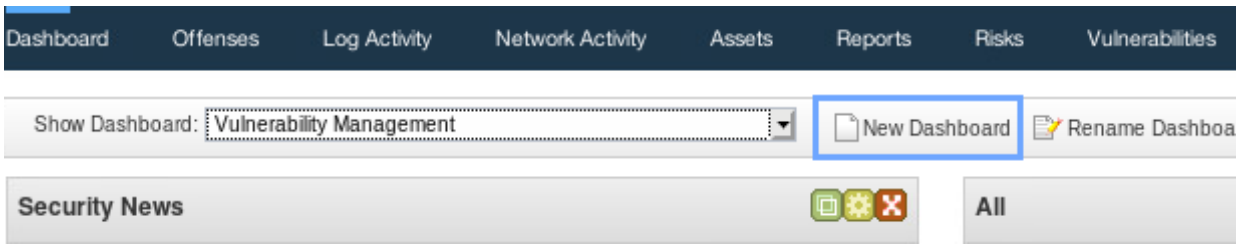


2. QRadar SIEM provides seven preconfigured dashboards. Open the **Show Dashboard** menu and select every dashboard, one at a time.




The dashboards do not yet display much information because the system was just started and began receiving data. The longer the sample data is fed to QRadar SIEM, the more information the dashboard that is displayed.

3. After you review the different dashboards, to move to the next step, select the **Vulnerability Management** dashboard and review the toolbar buttons, which perform the following tasks:
   - Create a new dashboard
   - Rename an existing dashboard
   - Delete a dashboard
   - Add an item to an existing dashboard




4. To create an additional dashboard, click **New Dashboard**.
   The New Dashboard window opens.

5. For **Name**, enter `Watch`.

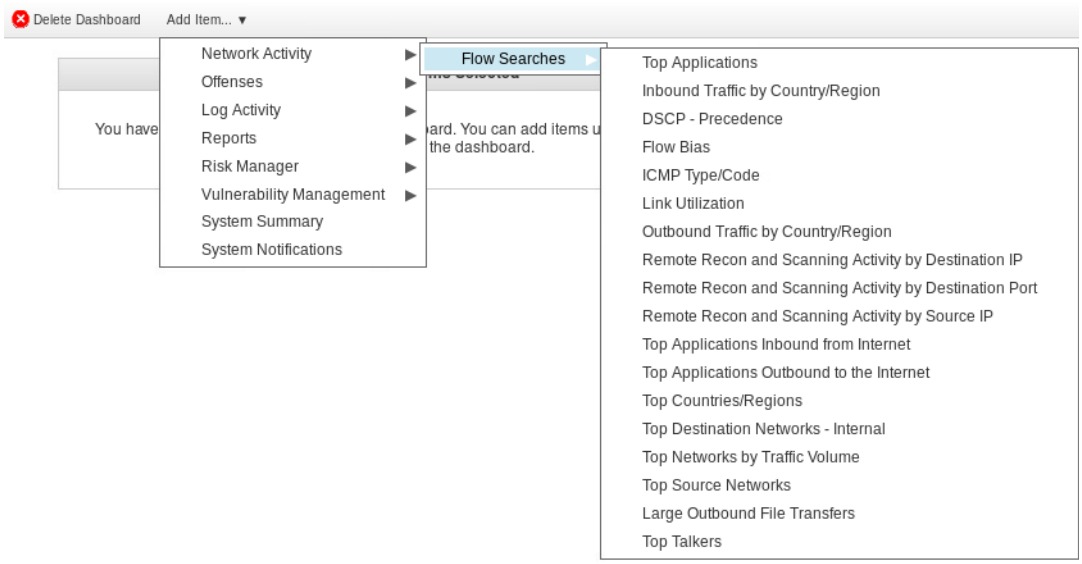
**Hint:** If you want to provide this dashboard to other users, select **Share**.

6. To create the Watch dashboard, click **OK**.
   The New Dashboard window closes.

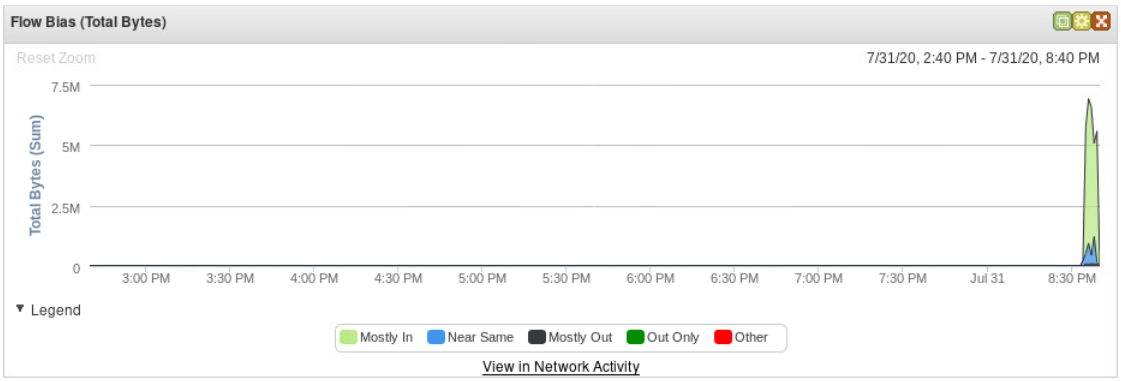
7. The **Dashboard** tab displays the new Watch dashboard but does not display any dashboard items yet. To add a Flow Bias preconfigured item, in the toolbar, click **Add Item**.

**Note:** Flow bias is explained in detail in the next exercise.

8. Select **Network Activity** > **Flow Searches** > **Flow Bias**.




The Flow Bias item is displayed in the Watch dashboard.




**Note:** When you use the actual product, you can move dashboard items and rearrange their order. In this virtual environment, the items are already positioned in the center of the dashboard.

**Hint:** If the **Flow Bias** dashboard item does not display data, click Refresh in the upper right of the toolbar.

# Exercise 3 Using a dashboard item

The QRadar SIEM installation in the lab environment has QFlow enabled. QFlow taps into the network traffic, including the traffic between the virtual machines in your lab environment. In addition, at the beginning of this lab, when the data is generated, many sample network connections to QFlow in QRadar SIEM are sent automatically.

In the lab environment, QFlow monitors the network interface of the QRadar virtual machines. For higher capacity, dedicated Flow collector and processor appliances are available.

In addition to QFlow, QRadar SIEM can receive information about IP connections from other network devices in IPFIX/NetFlow, sFlow, J-Flow, and Packeteer accounting technologies.

QRadar SIEM creates flows from the network activity information that it receives. A **flow** is a record of network activity between network sockets. IP address, port, and transport protocol identify a network socket uniquely.

In this exercise, you learn how to add a flow bias chart to your newly created Watch dashboard. The main reason to add this chart is to aid you in recent possible security breaches based on the network flow behavior. However, these steps were designed to teach you how to navigate graphs in any QRadar dashboard.

### Flow bias

A flow records characteristics of the network activity that it represents, including its **flow bias**. The bias of a flow marks the ratio between bytes leaving from and arriving at your organization's perimeter. QRadar SIEM distinguishes between the following flow biases:

- Out only: Unidirectional outbound

  This bias indicates outbound connection attempts that are blocked by a firewall, such as beaconing attempts by a malware to its command-and-control (C&C) servers.

- In only: Unidirectional inbound

  This bias indicates inbound connection attempts that are blocked by a firewall or a port scan attempt of a publicly reachable IP address in your organization.

- Mostly out: 70% to 99% of bytes outbound

  This bias indicates data that leaves your organization. Only your publicly reachable servers should have many flows with this bias.

- Mostly in: 70% to 99% of bytes inbound

  This bias is typical for user computers.

- Near same: inbound-outbound byte ratio between 31% and 69%

  This bias is typical for VOIP, chat, and SSH.

- Other

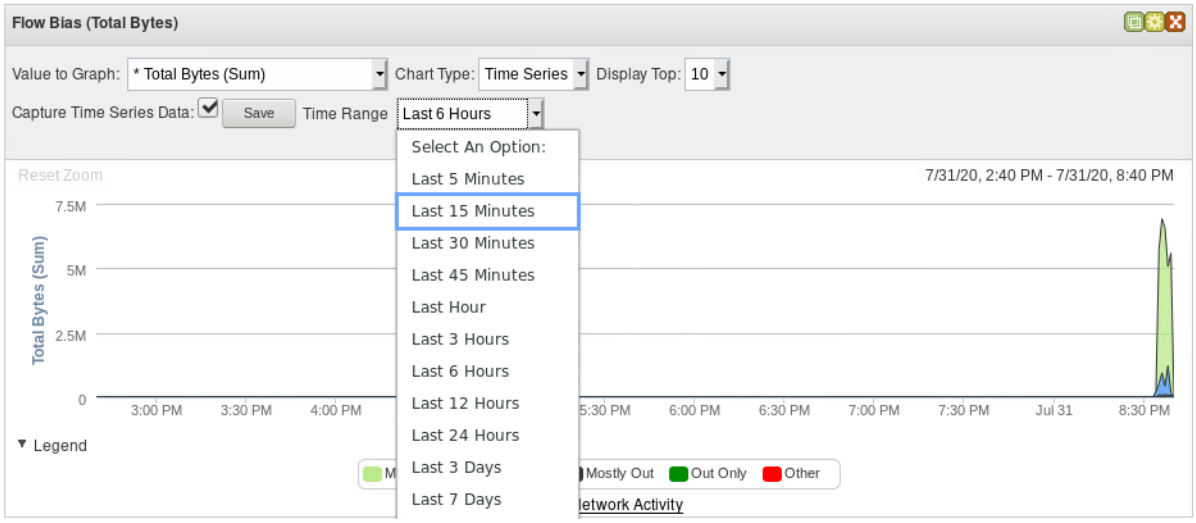
This bias usually indicates traffic between local computers. It can also indicate traffic between two remote computers that either points to a misconfiguration of an organization's network or notifies you that a local network is missing in the QRadar SIEM network hierarchy.

QRadar SIEM considers every network that is configured in its **network hierarchy** as part of your organization's local network. Therefore, the QRadar SIEM administrator needs to add any network that belongs to your organization to the network hierarchy. You perform this task in Exercise 7, Configuring the network hierarchy.

Unusual flow biases hint of a misconfiguration or a security breach.

1. To configure what is displayed in the chart, in the header of the Flow Bias item, click the **Settings** icon.

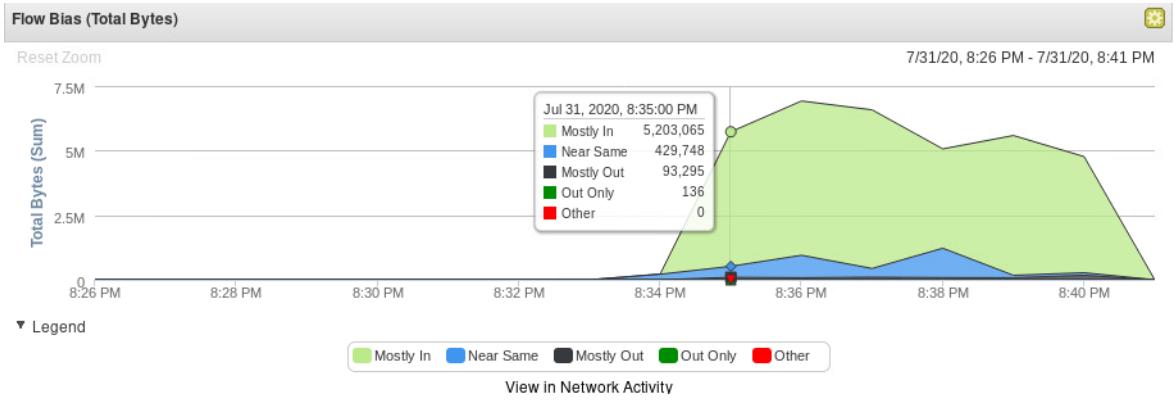

2. To focus on the most recent flow biases, for **Time Range**, select **Last 15 Minutes**.




3. To detach the Flow Bias item, click the **Detach this item** icon (next to the Settings icon) in the header of the Flow Bias item.

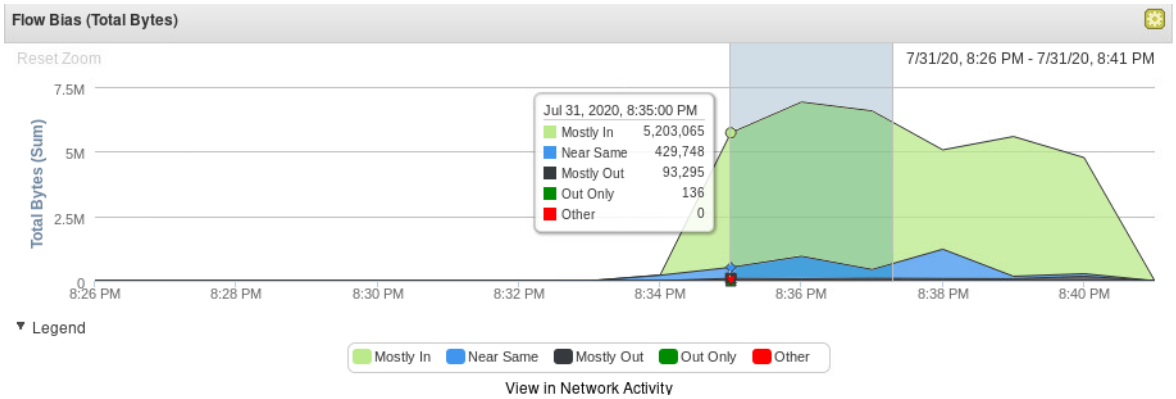

The item opens in a separate browser window. QRadar SIEM continues to update the item in the window, even if you close the main window without logging out of QRadar SIEM. However, do not close the main browser window during this lab.

4. To learn about the flow biases during a particular 1-minute time interval, hover your mouse pointer over the chart.

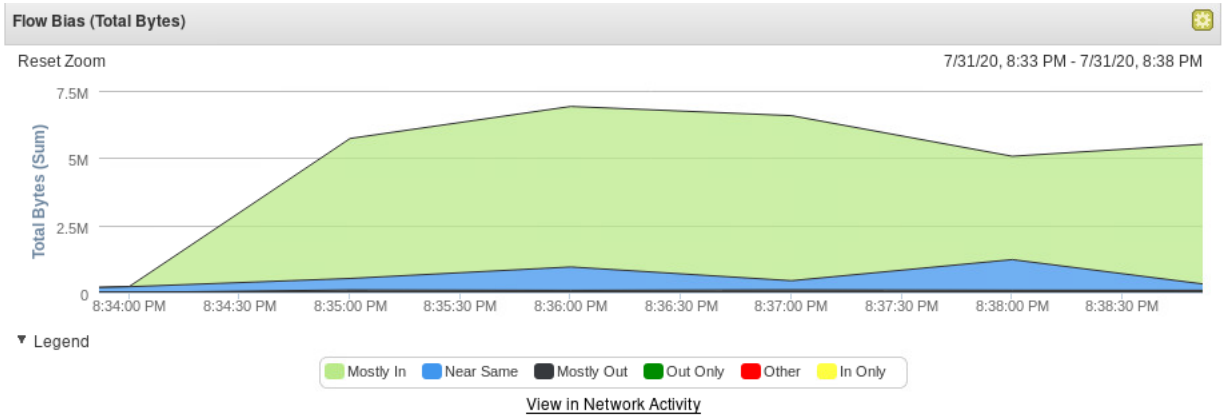



5. To zoom in to a shorter chart interval, click the graph.

**Important:** In this virtual environment, this step is simplified. To zoom in to the real Console interface, press and hold the left mouse button while you move the mouse pointer to the left or right. Release the mouse button when you have highlighted the interval that you want to zoom in to.

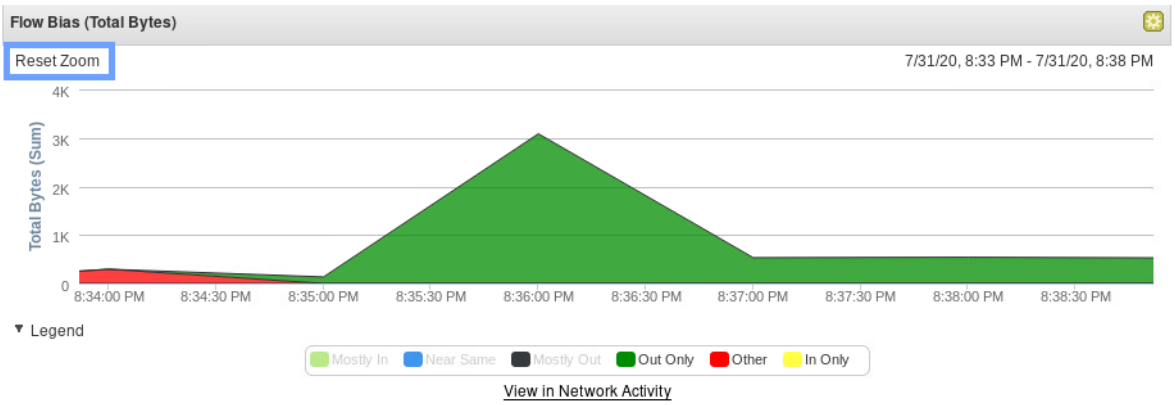


6. To focus on the less prevalent flow biases, hide dominating flow biases from the chart. To hide them, click the legend that is named **Mostly In**.

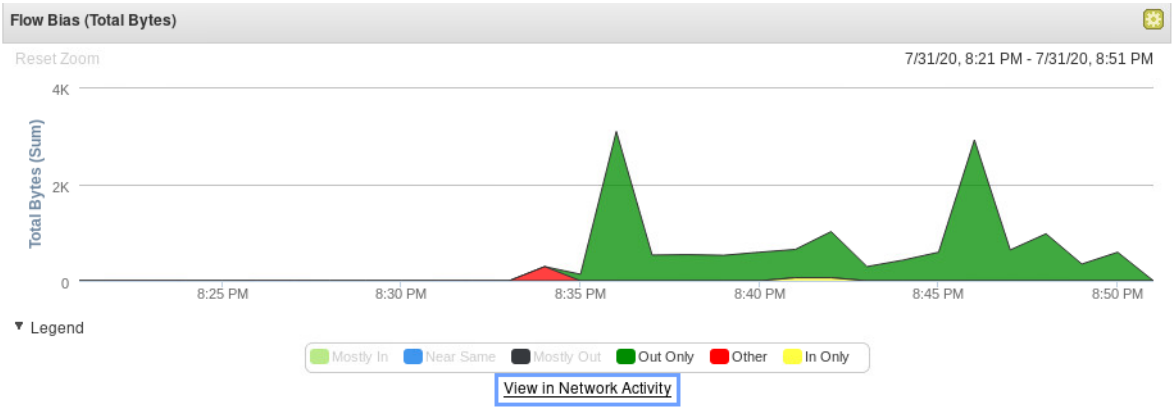



Notice how the chart changes as specific flow biases are hidden. Click the label in the legend named **Near Same**, followed by the label named **Mostly Out**.

7. To return to the original time range, click **Reset Zoom** in the upper left.




8. To investigate the flows further, on the **Network Activity** tab of the QRadar SIEM web interface, click the **View in Network Activity** link.




9. The **Network Activity** tab opens on the main window with the result of the search query that produces the Flow Bias dashboard item.

10. Close the Flow Bias window.

11. Scroll down and review the graphs in the main QRadar Console window.

**Hint:** In a real environment, if QRadar SIEM does not display a table of flow biases or the right chart, click **Update Details**.

**Hint:** The same way as with the charts in the dashboard items, you can zoom in, hide graphs, and hover the mouse pointer over the chart to look at the recorded bytes in 1-minute intervals. If you want to configure what is displayed on the chart, click the **Settings** icon in the header. Those options are not available in this virtual environment.

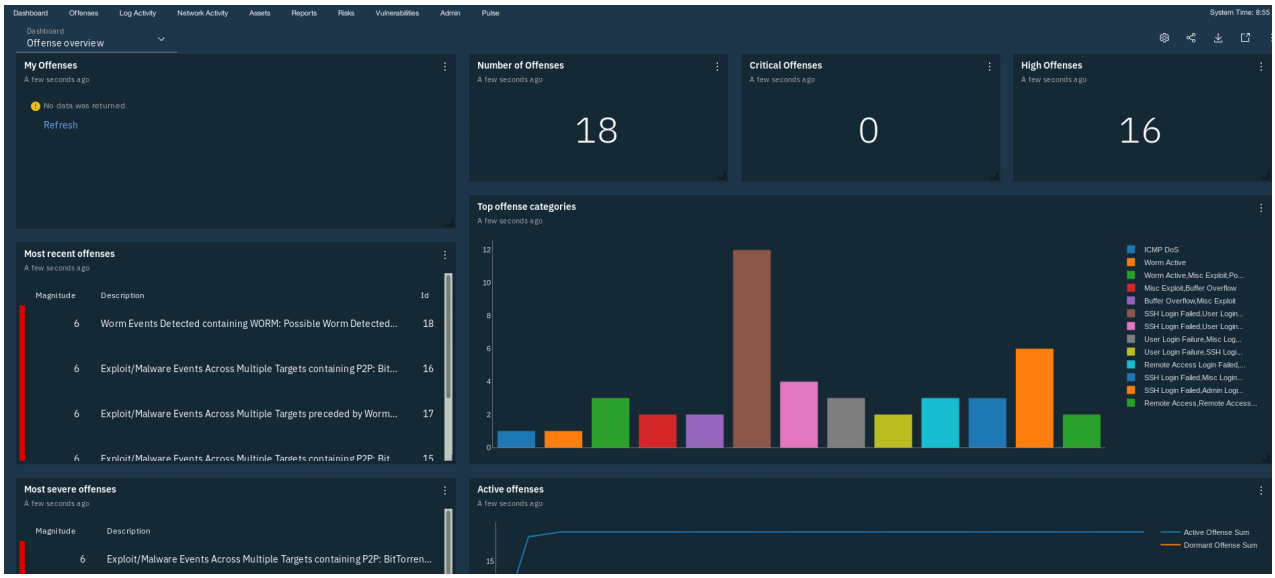
# Exercise 4 Using Pulse and widgets

IBM® QRadar® Pulse is a dashboard app that you can use to communicate insights and analysis about your network. Like the Dashboard tab, the Pulse app has different dynamic real-time dashboards that provide meaningful insights into your security posture and threat landscape. You can use it to visualize offenses, network data, threats, malicious user behavior, and cloud environments from around the world in scatter and choropleth geographical maps, a 3D threat globe, and autoupdating charts that you can customize.

QRadar SIEM 7.4 comes with this app. In this exercise, you walk through the Pulse app and its default dashboards. As a comparison and to learn the differences and advantages between the Pulse and the Dashboard tab, you then create a new dashboard and add a Flow Bias graph similar

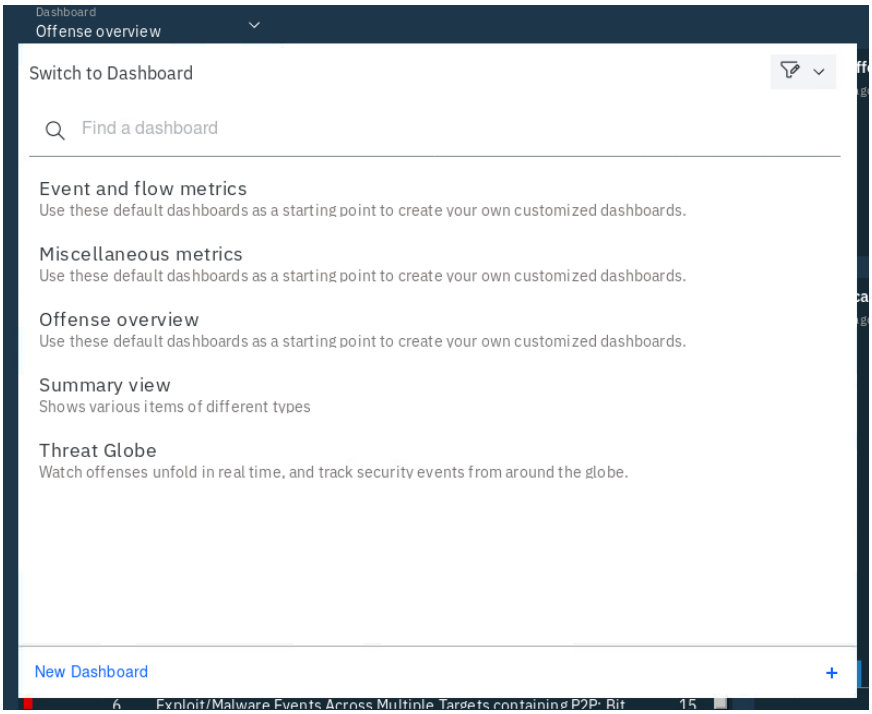
to Exercise 2. The objective of this exercise is to teach you about the most used terms in Pulse, such as items, widgets, AQL queries, and more; and how to create a graph widget.

1. To view the Pulse app, click the **Pulse** tab.



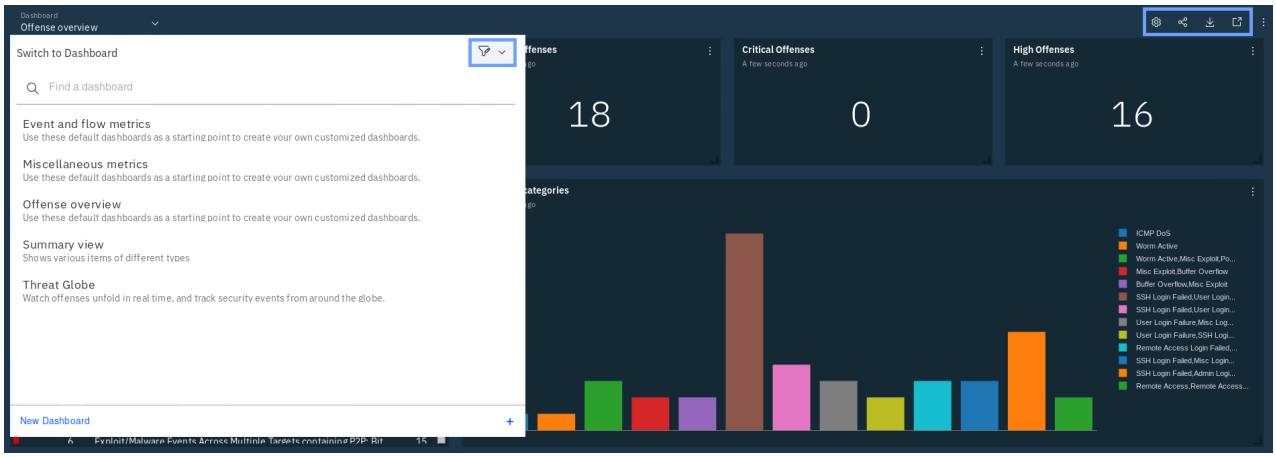

Like the Dashboard tab, each dashboard in Pulse displays items that provide information that is derived from the data that is fed automatically into QRadar SIEM. QRadar SIEM refreshes the information on the Pulse dashboards every minute. Unlike the Dashboard tab, you cannot pause the dashboards in Pulse. However, you can share it with other Pulse users, export it in JSON format, and open it in a new window if needed for your daily activities.

2. QRadar SIEM provides five preconfigured dashboards for Pulse. Open the **Dashboard** menu and select every dashboard, one at a time. Review each dashboard, scroll down, and select the next one.



The dashboards do not yet display much information because the system was just started and began receiving data. The longer the sample data is fed to QRadar SIEM, the more information that is displayed. The data displayed is enough for you to know the great potential that each dashboard has to help you identify threats.

3. After you review the different dashboards, double-click the **Pulse** tab to refresh the dashboard view. Then, review the additional options of the dashboard menu on the upper left and the icons on the upper right of each dashboard.




These options perform the following dashboard tasks:

- Create a new dashboard
- Filter dashboards by those shared by me, shared with me, and the ones with an update available
- Configure the current dashboard
- Share the dashboard with another QRadar user
- Export the dashboard in JSON format
- Open dashboard in a new window

**Hint:** Double-clicking resets the tab to its default settings.

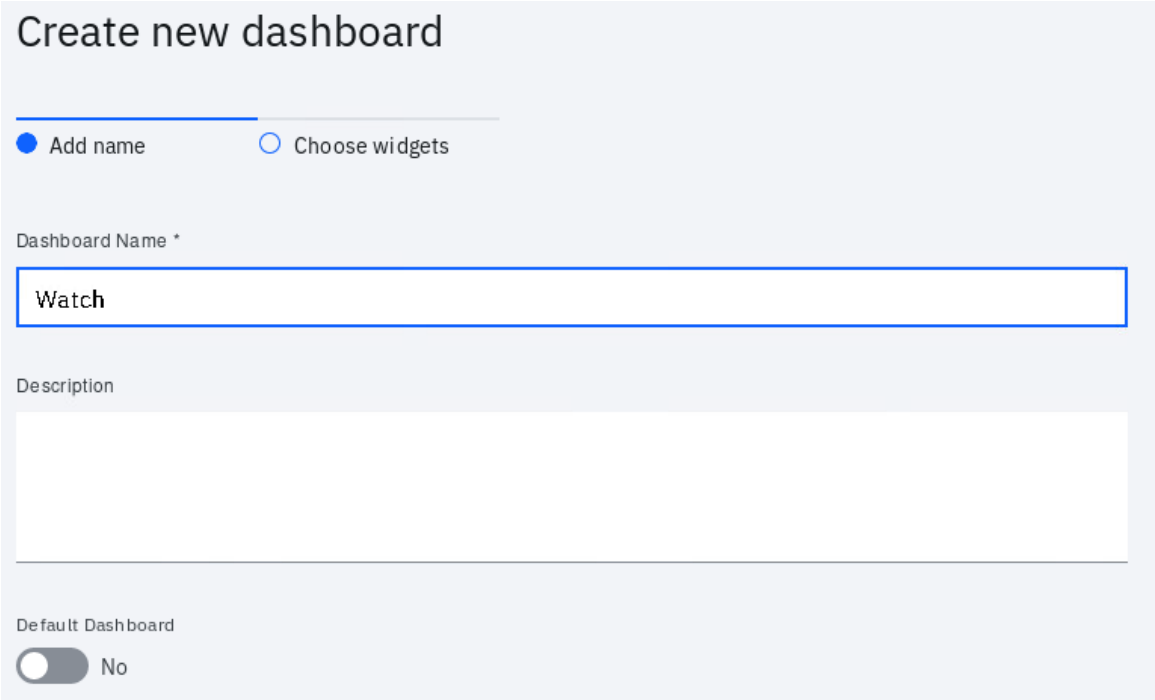
4. To create an additional dashboard, from the Dashboard menu, click **New Dashboard**.
5. Click **Blank Dashboard**.

   The Create a new dashboard window opens.

**Note:** In addition to a blank dashboard, you can also import existing dashboards in JSON format, and add templates, which are available in your QRadar Console. An administrator must install and synchronize the content extensions that contain Pulse dashboard templates.

6. For **Dashboard Name**, enter `Watch`.

**Hint:** Type an optional description and if you want to set this dashboard as the default dashboard when you open the Pulse tab, set **Default Dashboard** to Yes. You cannot edit these options in this virtual lab.




7. To view the available widgets from the library that you can add to your new dashboard, click **Next** and scroll to see all widgets.
8. To create the Watch dashboard, click **Create**.
   The new Watch dashboard is displayed. It does not display any dashboard items yet.

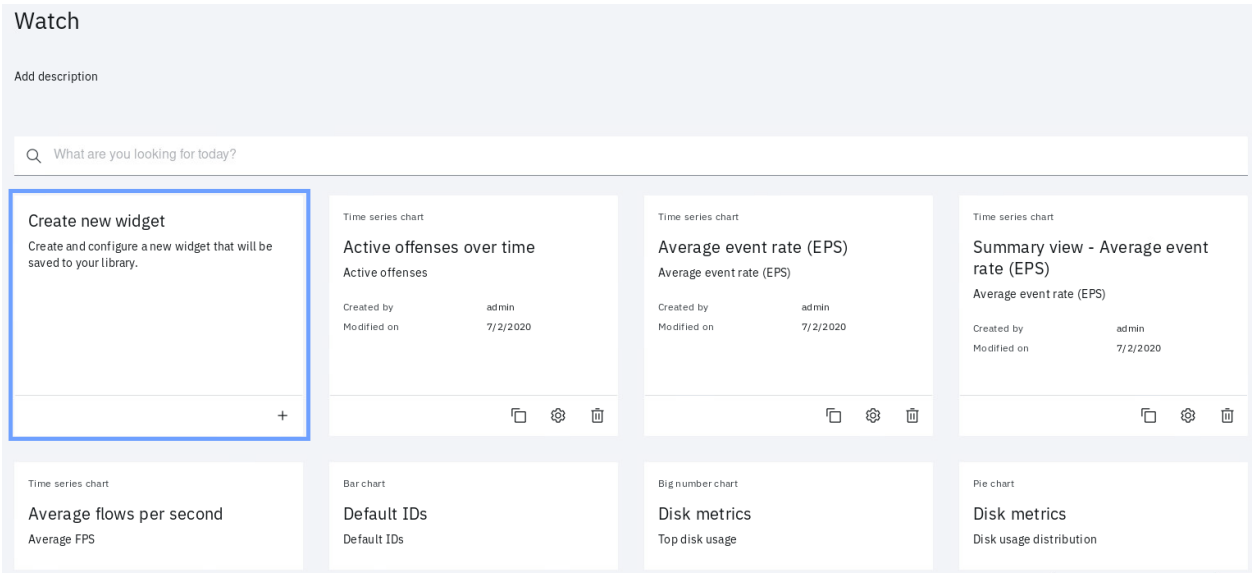
**Note:** In the Pulse app, widgets are the equivalent of dashboard items.

You can now add your first widget to your newly added dashboard.

9. To add a preconfigured widget, click the **Click here to get started** link in the center of the dashboard.

**Important:** After you add your first widget, you can add more by clicking **Configure Dashboard** in the upper right of the dashboard.

10. Select **Create new widget**.




The New dashboard item window opens.

11. In the **Name** field, type `Flow Bias`.

12. In the **Data source** menu, select AQL. Leave the Refresh Time at its default of Every Minute.

**Note:** You can also create widgets from an offense API, which means you can select specific fields of an offense and apply filters to them, and also from a generic API, provide the URL endpoint and JSON path to results.

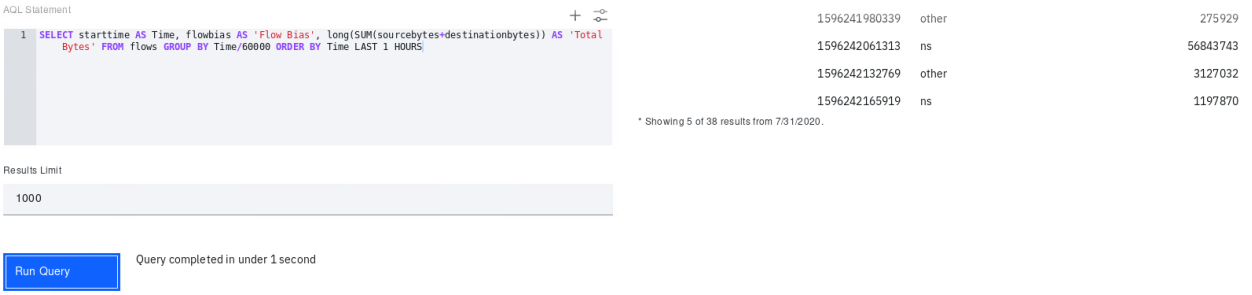
13. In the **AQL Statement** field, type the following query:

```
SELECT starttime AS Time, flowbias AS 'Flow Bias',
long(SUM(sourcebytes+destinationbytes)) AS 'TotalBytes' FROM flows GROUP BY
Time/60000 ORDER BY Time LAST 1 HOURS
```

This query retrieves the start time, the flow bias, and the total bytes from the flows database for the last hour. The data is grouped by the time of the flows and this is used as the basis of the graph.

**Hint:** To learn about the Ariel Query Language (AQL) that you use in QRadar Pulse to create dashboard items, read the **Overview of Ariel Query Language** and **Event, flow, and simarc fields for AQL queries** articles in the IBM Knowledge Center.

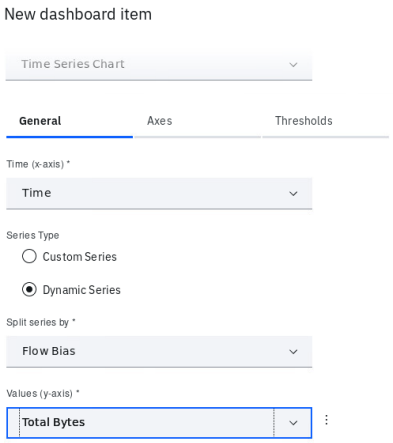
14. Scroll down.
15. Leave the Results Limit field at its default 1000 value, scroll down, and click **Run Query**. Make sure a sample of the results is displayed next to the AQL statement.

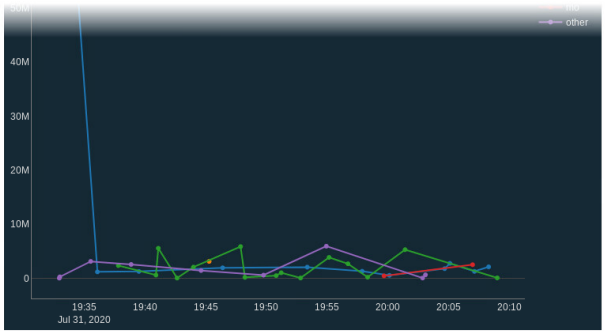



**Note:** The AQL Statement field has an autocomplete feature that suggests parameters based on the text you type. This feature facilitates the creation of queries for a quick customization. This feature is not available in this virtual lab.

16. Scroll down to the Views section.
17. In **View Name**, type `Flow Bias`.
18. In **Chart Type**, select **Time Series Chart** and scroll down.
19. Under General, in **Time (x-axis)**, select **Time**.
20. In **Series Type**, select **Dynamic Series**.
21. In **Split series by**, select **Flow Bias**.
22. In **Values (y-axis)**, select **Total Bytes**.
    A sample graph is displayed on the right. Scroll down.
23. Set the **Area Chart** and **Show Legend** buttons to On and Yes.

24. Scroll down.




25. In **Legend Orientation**, select **Bottom**.

26. In the **New dashboard item** and then in the **Configure Dashboard** window, click **Save**.

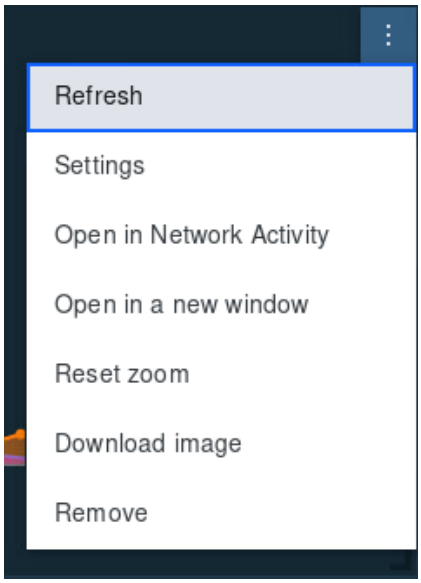
    The Flow Bias graph is displayed in the Watch dashboard.

# Exercise 5 Using a Pulse widget

This exercise shows you how to work with widgets in Pulse dashboards. You learn how to navigate and adjust the graph that you created in Exercise 4 so you can compare how useful this widget is to your work as an analyst compared to the procedure you followed in Exercise 3.

1. To detach the Flow Bias item, click **More options...** (the three-dotted icon) in the header of the widget.

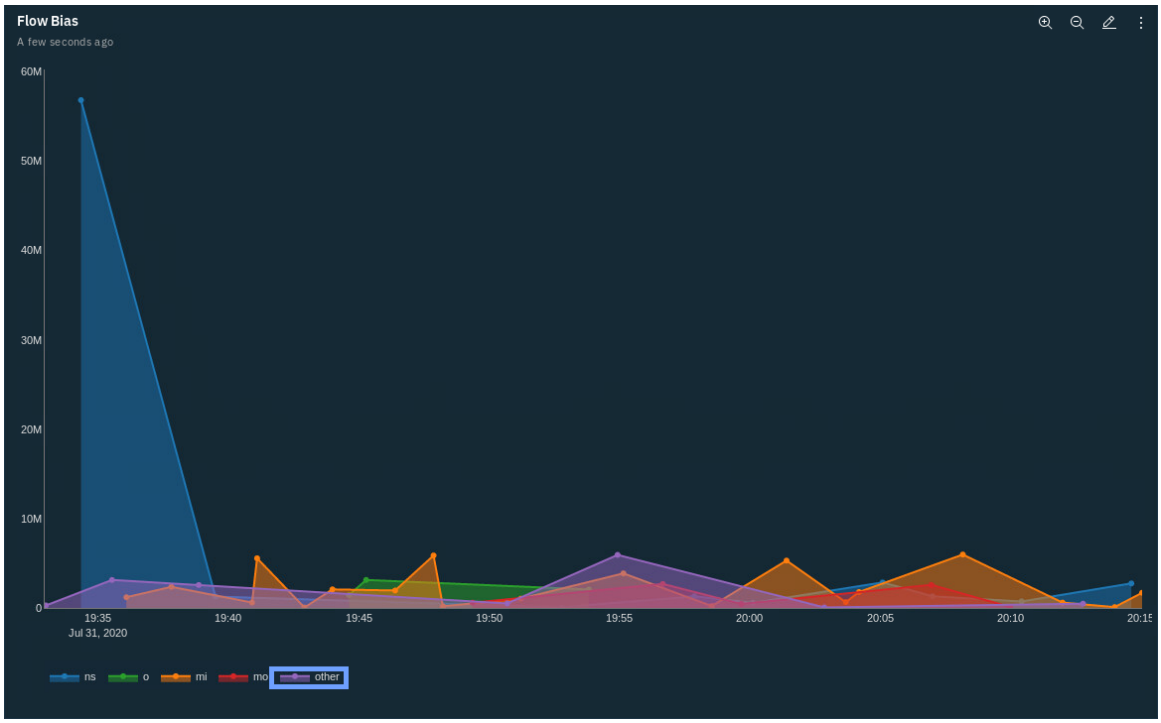
2. Select **Open in a new window**.



The graph opens in a separate browser window. QRadar SIEM continues to update the widget in the window, even if you close the main window without logging out of QRadar SIEM. However, do not close the main browser window during this lab.

**Hint:** To learn about the flow biases during a particular 1-minute time interval, hover your mouse pointer over the chart. This action is not supported in this virtual environment.

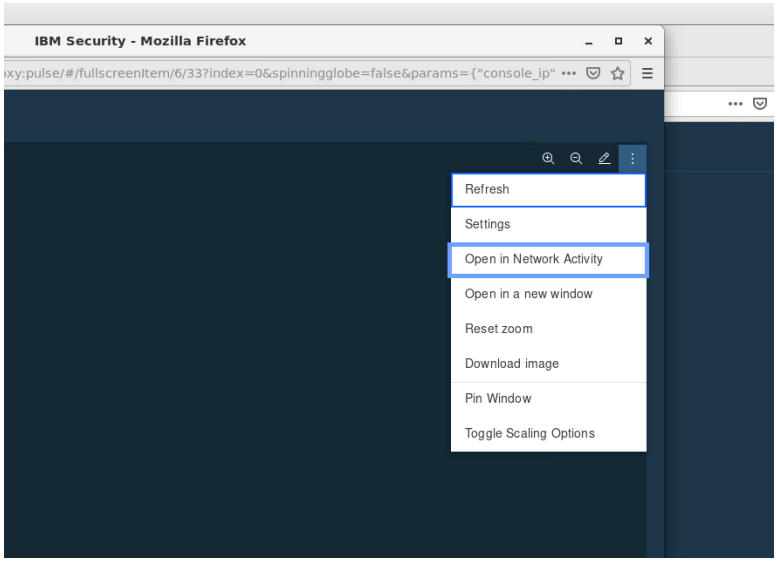
3. To zoom in to a shorter chart interval, click the zoom icon in the upper right once.
4. To focus on the less prevalent flow biases, hide dominating flow biases from the chart. To do this, in the legend, click **other**.



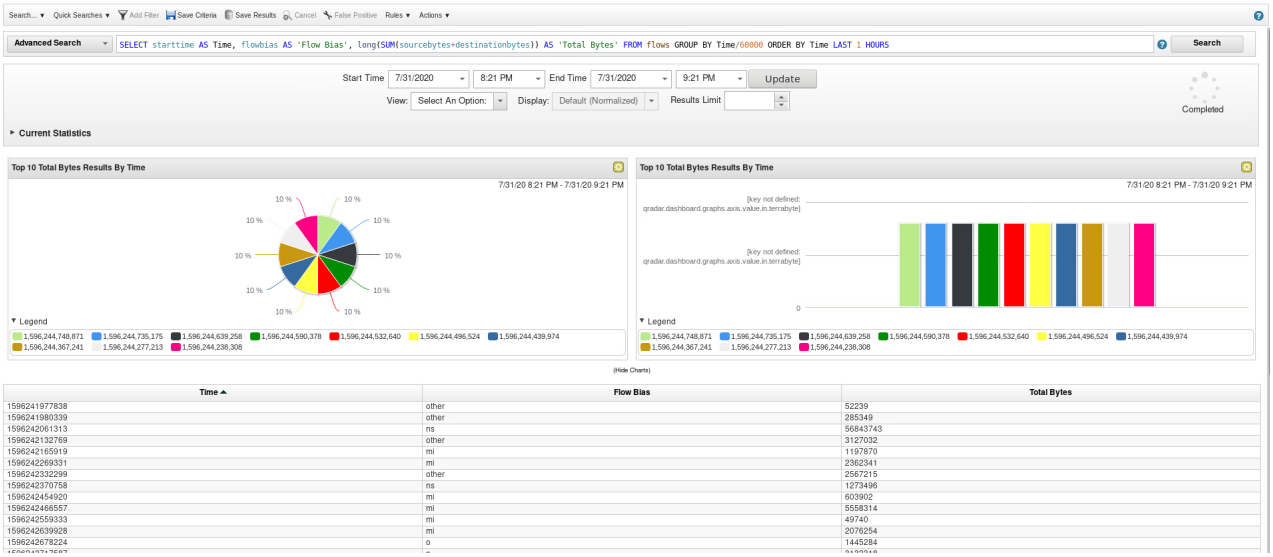

In the legend, click **mi** (mostly in), then click **o** (out).

**Hint:** To return to the original time range, click **Reset zoom** in the **More options...** menu in the upper right. This action is not supported in this virtual environment.

5. To investigate the flows further on the **Network Activity** tab of the QRadar SIEM web interface, click **More options** > **Open in Network Activity.**




The **Network Activity** tab opens on the main window with the result of the AQL query that produces the Flow Bias dashboard widget you created.




6. From the browser taskbar, select the Flow Bias widget window and close it.

7. Review the graphs in the **Flow List** tab and then close it.

**Hint:** Like the charts in the dashboard items, you can zoom in, hide graphs, and hover the mouse pointer over the chart to look at the recorded bytes in 1-minute intervals. If you want to configure what is displayed on the chart, click the **Settings** icon in the header. Those options are not available in this virtual environment.

# Exercise 6 Investigating a remote access offense

The **rules** of QRadar SIEM correlate events, flows, and other information to detect indicators of compromise or attacks. If the test conditions of the rule are met, a rule can create an **offense** or add information to an existing offense. An offense alerts to suspicious activity and links to information helpful to investigate it.

QRadar SIEM comes with preconfigured rules. Extensions can add more rules. You can build your own rules to watch for specific indicators, or look at behavioral changes or anomalies. This exercise relies on a rule from an extension and teaches you how rules are structured, how they are triggered, and the different responses and actions that you can customize when they are triggered.

**Hint:** If you want to explore the rules of QRadar SIEM, navigate to the **Offense** tab and then click **Rules** in the left pane. This action is not supported in this virtual environment.

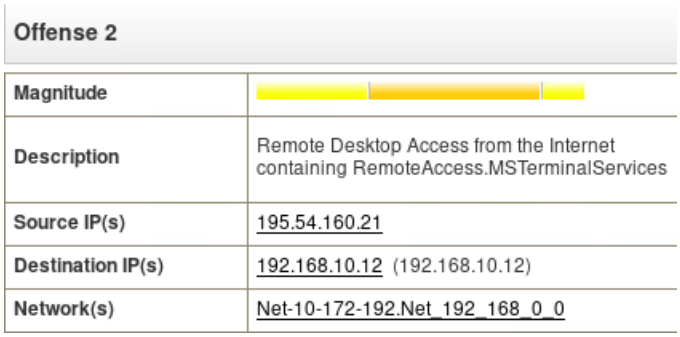
Follow these steps to navigate to an example offense and investigate it:

1. To display all offenses that are generated by the sample data that was sent before the beginning of this lab, click the **Offenses** tab.

2. To open the offense summary, double-click the offense number 2 with the description of **Remote Desktop Access from the Internet containing RemoteAccess.MSTerminal Services**.

| | Id | Description | Offense Type | Offense Source | Magnitude | Source IPs | Destination IPs | Users |
|---|---|---|---|---|---|---|---|---|
| | 18 | Worm Events Detected containing WORM: Possible Worm Detected in... | Source IP | 10.106.48.158 | | 10.106.48.158 | 103.192.75.27 | N/A |
| | 23 | Possible Local Worm Detected preceded by Excessive Firewall Denie... | Source IP | 10.126.50.42 | | 10.126.50.42 | Multiple (1,031) | N/A |
| | 15 | Exploit/Malware Events Across Multiple Targets containing P2P: BitTor... | Source IP | 10.105.8.215 | | 10.105.8.215 | Remote (14) | N/A |
| | 16 | Exploit/Malware Events Across Multiple Targets containing P2P: BitTor... | Source IP | 10.107.120.211 | | 10.107.120.211 | Remote (10) | N/A |
| | 17 | Exploit/Malware Events Across Multiple Targets preceded by Worm Ev... | Source IP | 10.107.43.71 | | 10.107.43.71 | Local (20) | N/A |
| | 10 | Login Failures Followed By Success from the same Username preced... | Username | root | | Multiple (2) | 10.64.2.13 | root |
| | 21 | Excessive Firewall Denies Across Multiple Hosts From A Local Host c... | Source IP | 10.26.72.208 | | 10.26.72.208 | Multiple (52) | N/A |
| | 22 | Excessive Firewall Denies Across Multiple Hosts From A Local Host c... | Source IP | 10.26.72.218 | | 10.26.72.218 | Multiple (72) | N/A |
| | 29 | Local ICMP Scanner preceded by Excessive Firewall Denies Across ... | Source IP | 10.127.27.34 | | 10.127.27.34 | Multiple (63) | N/A |
| | 7 | Multiple Login Failures for the Same User containing Authentication F... | Username | administrator | | Multiple (2) | 10.64.2.13 | administrator |
| | 8 | Multiple Login Failures for the Same User containing Bad Username | Username | mail | | Multiple (2) | 10.64.2.13 | mail |
| | 9 | Multiple Login Failures for the Same User containing Bad Username | Username | operator | | Multiple (2) | 10.64.2.13 | operator |
| | 11 | Multiple Login Failures for the Same User containing Bad Username | Username | sys | | Multiple (2) | 10.64.2.13 | sys |
| | 12 | Multiple Login Failures for the Same User containing Bad Username | Username | ftp | | Multiple (2) | 10.64.2.13 | ftp |
| | 13 | Multiple Login Failures for the Same User containing Bad Username | Username | mysql | | Multiple (2) | 10.64.2.13 | mysql |
| | 14 | Multiple Login Failures for the Same User containing Bad Username | Username | admin | | Multiple (2) | 10.64.2.13 | admin |
| | 24 | Local ICMP Scanner preceded by Excessive Firewall Denies Across ... | Source IP | 10.127.15.37 | | 10.127.15.37 | Multiple (252) | N/A |
| | 25 | Excessive Firewall Denies Across Multiple Hosts From A Local Host c... | Source IP | 10.127.27.40 | | 10.127.27.40 | Multiple (141) | N/A |
| | 26 | Local TCP Scanner Detected preceded by Excessive Firewall Denies ... | Source IP | 10.126.54.92 | | 10.126.54.92 | Multiple (177) | N/A |
| | 27 | Local ICMP Scanner preceded by Excessive Firewall Denies Across ... | Source IP | 10.127.27.28 | | 10.127.27.28 | Multiple (120) | N/A |
| | 3 | Login Failures Followed By Success to the same Destination IP prece... | Destination IP | 10.64.2.13 | | Multiple (2) | 10.64.2.13 | Multiple (10) |
| | 4 | Multiple Login Failures for the Same User preceded by Multiple Login ... | Source IP | 10.64.2.13 | | 10.64.2.13 | 10.64.2.13 | Multiple (10) |
| | 5 | Multiple Login Failures for the Same User containing Authentication F... | Username | nobody | | Multiple (2) | 10.64.2.13 | nobody |
| | 6 | Multiple Login Failures for the Same User containing Check password | Username | unknown | | 10.64.2.13 | 10.64.2.13 | unknown |
| | 20 | Local DNS Scanner containing Invalid DNS | Source IP | 10.152.247.69 | | 10.152.247.69 | Local (153) | N/A |
| | 28 | Excessive Firewall Denies Between Hosts containing Firewall Drop | Source IP | 192.168.1.193 | | 192.168.1.193 | Multiple (3) | N/A |
| | 19 | Large ping | Event Name | Large ping | | Multiple (87) | Multiple (46) | N/A |
| | 2 | Remote Desktop Access from the Internet containing RemoteAccess.... | Source IP | 195.54.160.21 | | 195.54.160.21 | 192.168.10.12 | N/A |

The **offense summary** displays and links to a wide range of evidence that is helpful for investigating the suspected attack or policy violation.



**Offense 2**

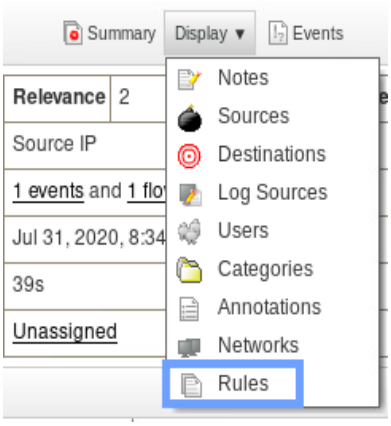
| | |
|---|---|
| **Magnitude** | |
| **Description** | Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices |
| **Source IP(s)** | 195.54.160.21 |
| **Destination IP(s)** | 192.168.10.12 (192.168.10.12) |
| **Network(s)** | Net-10-172-192.Net_192_168_0_0 |

The Magnitude specifies the relative importance of the offense.

Scroll down to explore the information the offense summary provides. Afterward, scroll up to the beginning of the offense summary.

**Note:** The example offense is simple and therefore its offense summary contains little information. For most offenses, the offense summary provides more information.

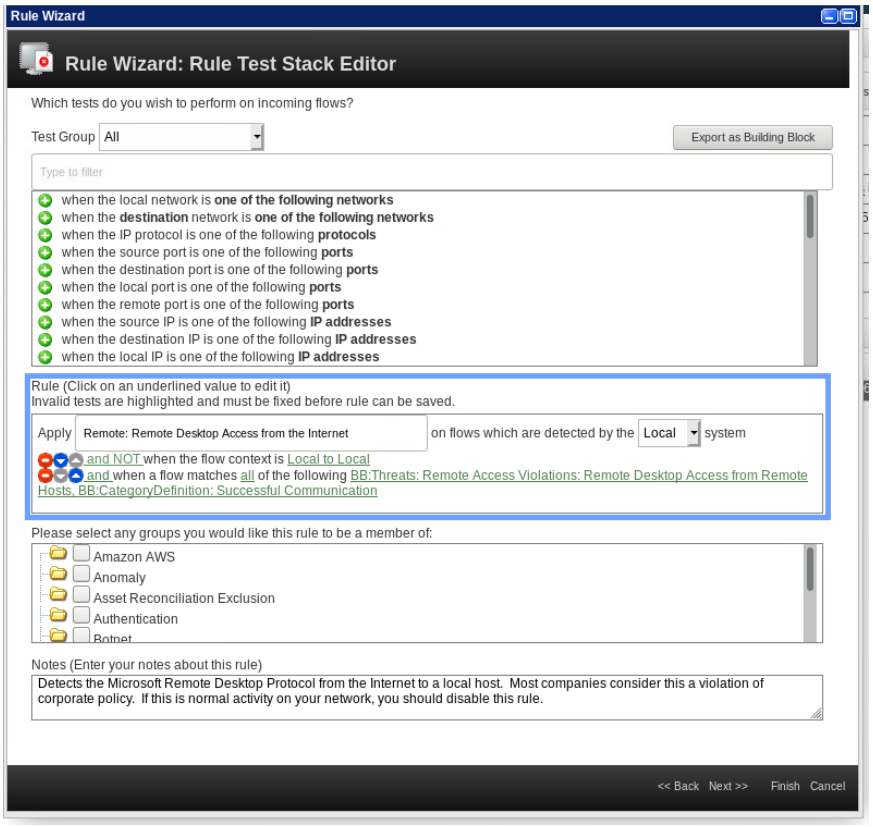
3. To view the rules that contribute to this offense, select **Rules** from the **Display** menu.




4. Double-click the rule that is displayed in the **List of Rules Contributing to Offense** table.

   The Rule Wizard opens with the rule **Remote: Remote Desktop Access from the Internet**.

The tests that are evaluated by this rule are displayed in the middle section of the Rule Wizard: Rule Test Stack Editor window. The first test tests whether the flows are detected by the local system.




**Note:** Within the rule, all hyperlinks represent variables that you can select to modify the behavior of the tests and therefore, the conditions under which the rule is triggered.

a. What is the second test?

_____

b. How many variables are there in the second test?

_____

c. What is the third test?

_____

d. How many variables are there in the third test?

_____

**Note:** You can find all answers to the questions in this guide in the Appendix on page 49.

5. You can modify some variables in the tests by clicking them. Click the **and NOT** logic operator variable from the second test. Notice that it changes to **and**, which is the only alternative for this variable.
6. Click it again to revert to **and NOT**.
7. You can modify some variables by selecting different options from a list. Click the **Local to Local** context variable from the second test.

   The context window opens.

   a. What are the available options for this context?

   _____

   Close the context window.
8. Click the Building Block variables from the third test.

**Hint:** Building blocks are preceded by **BB:** in their names.

The rules to match window opens.

a. What are the two selected building blocks for this variable in the Selected Items list?

_____

**Note:** Building blocks perform tests against many variables when events and flows are received by QRadar. They are useful because they simplify the logic of some tests and can be used as part of rules. They are configured similarly to rules, but do not contain actions or responses.

Close the rules to match window.

9. In the Rule Wizard, click **Next**.
10. In Rule Action, notice which actions can be taken when the rule is triggered.
    a. Which action is enabled by default?

    _____

    b. Based on which variable is the offense indexed?

    _____

Notice the different variables on which the offense can be indexed.

**Note:** Indexing based on a variable helps identify an offense uniquely because this variable can specify information about the offense that is common across all events that trigger a rule's tests.

11. In Rule Response, notice which responses can be made when the rule is triggered.
    a. How many responses can be enabled in total?

    _____

    b. Which response is enabled by default?

    _____

    c. What are the low-level and high-level categories defined for the new dispatched event?

    _____

    d. Based on which variable is the offense indexed?

    _____

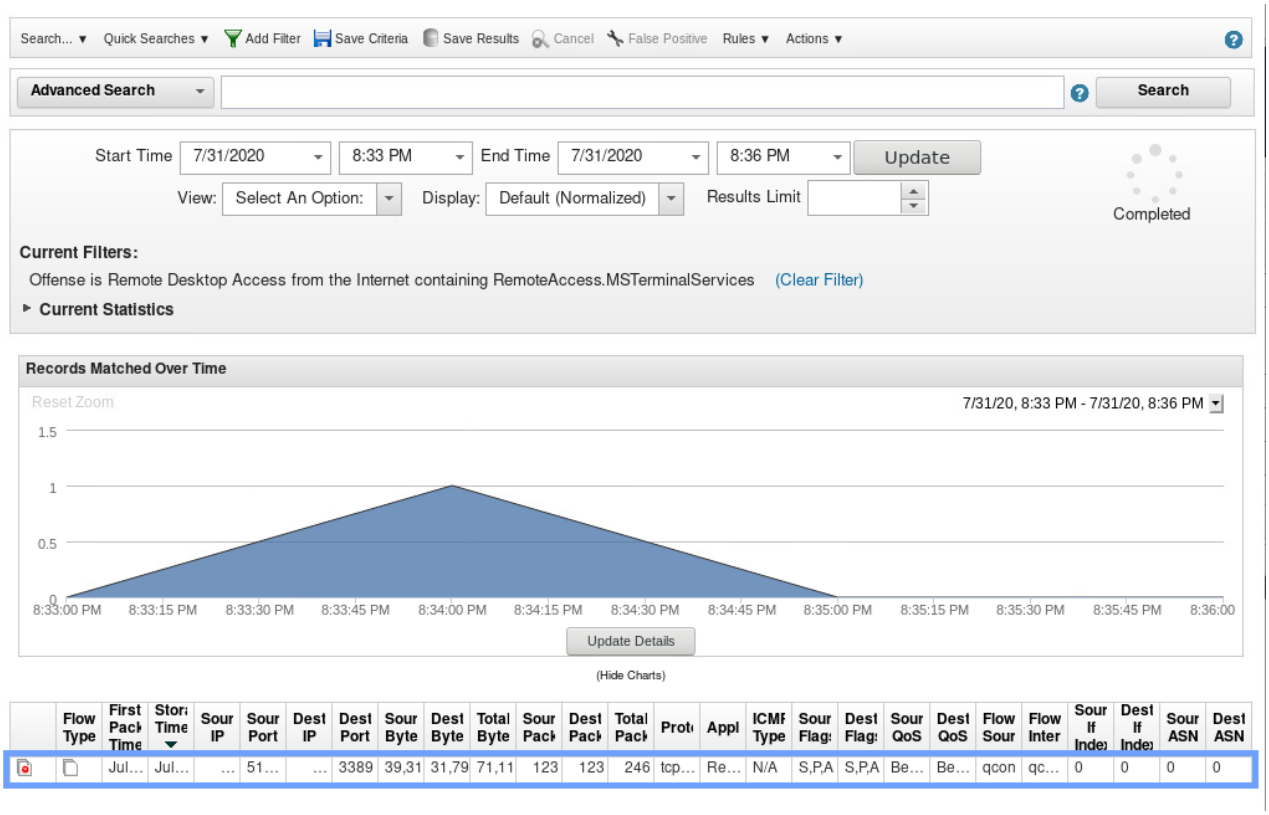
12. Click **Next**.
13. Review all the information that was specified in the previous sections of the Rule Wizard. To avoid saving any inadvertent changes to the rule, click **Cancel**, then click **OK**.

**Important:** Modifying the rule can have an unexpected behavior when the offenses trigger. Therefore, modify rules with caution.

14. To view the flow that triggered the rules that created the offense, in the **Event/Flow count** field, click **1 flows**.

| Status | | Relevance | 2 |
|---|---|---|---|
| Offense Type | | Source IP | |
| Event/Flow count | | 1 events and 1 flows in 2 categories | |
| Start | | Jul 31, 2020, 8:34:15 PM | |
| Duration | | 39s | |
| Assigned to | | Unassigned | |

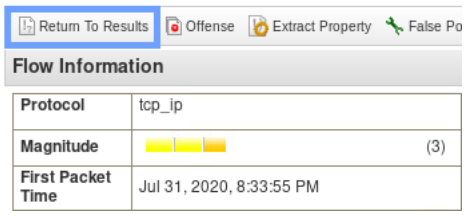
The Flow List window opens. The table contains only one flow in this example.




15. Double-click the flow in the table to navigate to the Flow Details window.

    To investigate the flow further, look at the Flow Information, Source and Destination Information, and scroll down to view the Source Payload and Additional Information. All this information is useful when you investigate a suspicious connection.

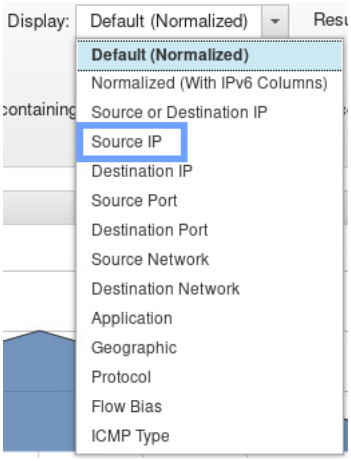
16. Click **Return To Results** in the upper left of the Flow Details window.
    You return to the Flow List window.



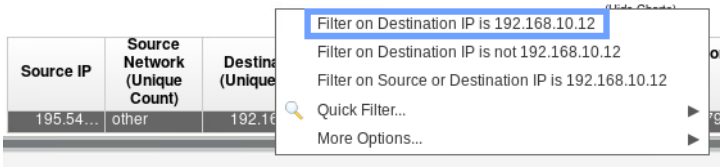
# Exercise 7 Creating a search for RDP connections to your server

So far, QRadar SIEM recorded only one RDP connection to your server, but more flows might occur soon. The Flow List displays the results of a search. Follow these steps to refine and save this search to monitor additional recent RDP connections to your server:

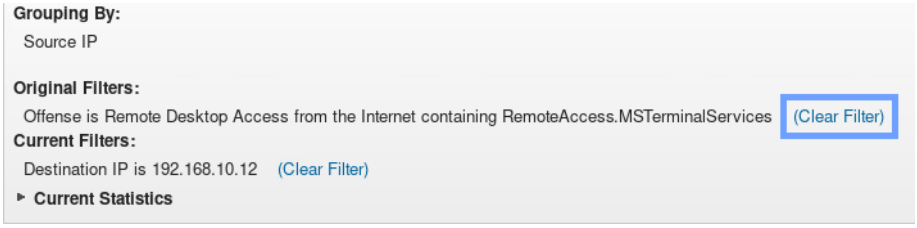
1. To make the Flow List display the flows as summarized by source IP address and prepare it for a report template, from the **Display** menu, select **Source IP**.




2. Still in the Flow List window, in the Destination IP column, right-click **192.168.10.12** and select **Filter on Destination IP is 192.168.10.12**.



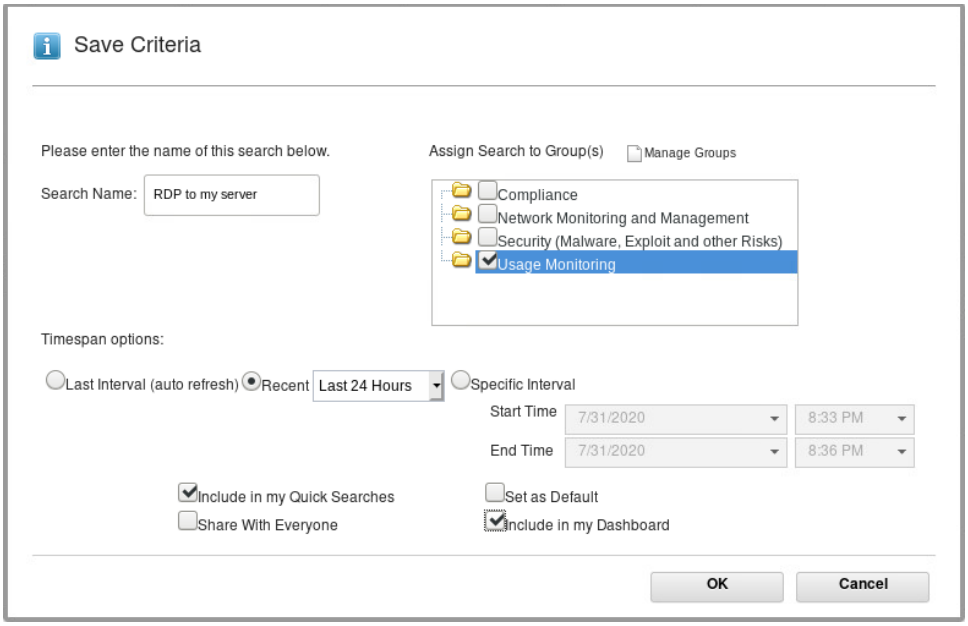

3. Because you opened the Flow List from an offense summary, it filters for flows that contribute to this particular offense. To remove the filter on the offense, click **Clear Filter** next to **Offense is Remote Desktop Access from the Internet**.




4. To save the search, click **Save Criteria** in the toolbar.

5. Provide the following criteria in the **Save Criteria** fields.

| Field | Setting |
|---|---|
| Search Name | RDP to my Server |
| Timespan Option | Recent: Last 24 Hours |
| Assign Search to Group(s) | Usage Monitoring |
| Include in my Quick Searches | Yes |
| Include in my Dashboard | Yes |

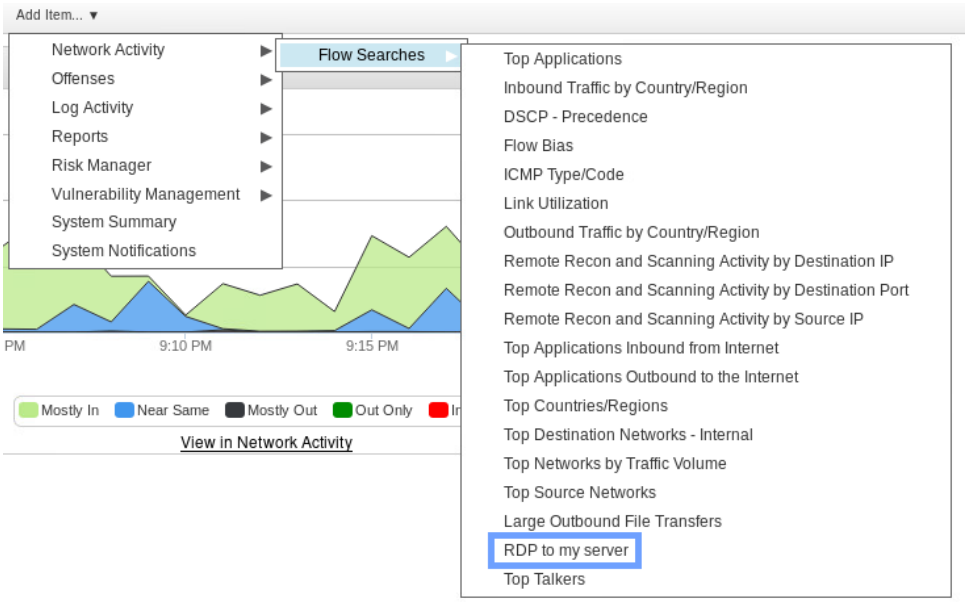



6. Click **OK**.
7. In the Search Saved confirmation window, click **OK** again.
8. Close the Flow List window.

**Note:** Any search with a grouping and saved with the option **Include in my Dashboard** enabled becomes available as a dashboard item after you refresh the **Dashboard** tab.

9. Double-click the **Dashboard** tab to reset it.

10. To add the new search to the currently selected dashboard, click **Add Item > Network Activity > Flow Searches > RDP to my Server**.




11. Confirm that the item is added to the dashboard.

**Note:** The new graph is currently empty because the sample data sent to QRadar only had one RDP connection, so another occurrence of the RDP connection is yet to happen.

# Exercise 8 Investigating a remote access offense with the Analyst app

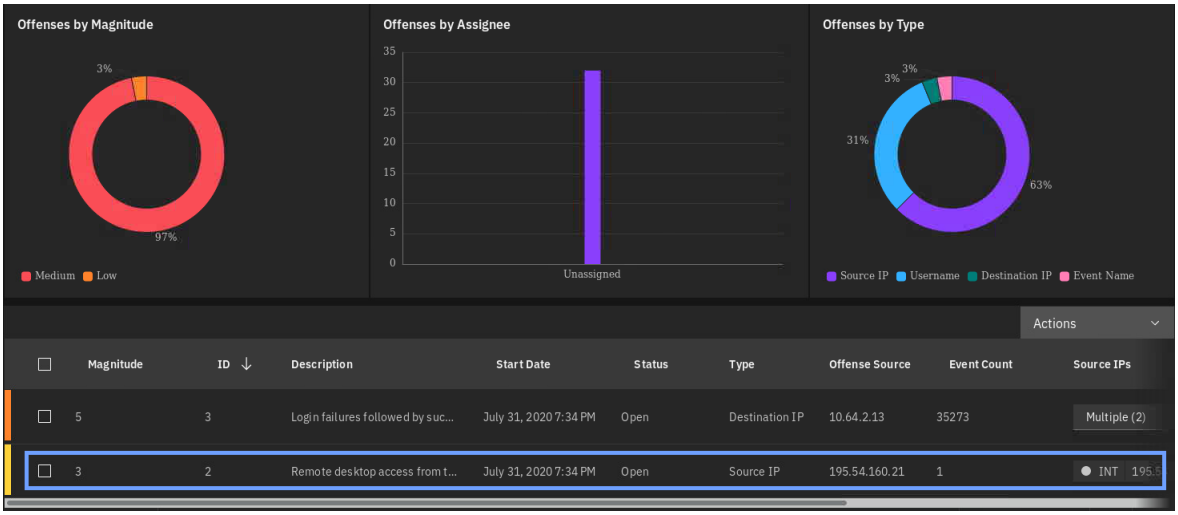
IBM® QRadar® Analyst app is a user interface (UI) designed for the analysts in your organization to help them in their daily activities. It simplifies and expedites the investigation of offenses with a streamlined workflow and is meant to be used along with the regular Offense tab.

This UI is supported in QRadar SIEM 7.4 and later. In this exercise, you investigate the same offense as in Exercise 5. You compare both interfaces and experience the advantages that the Analyst app offers.

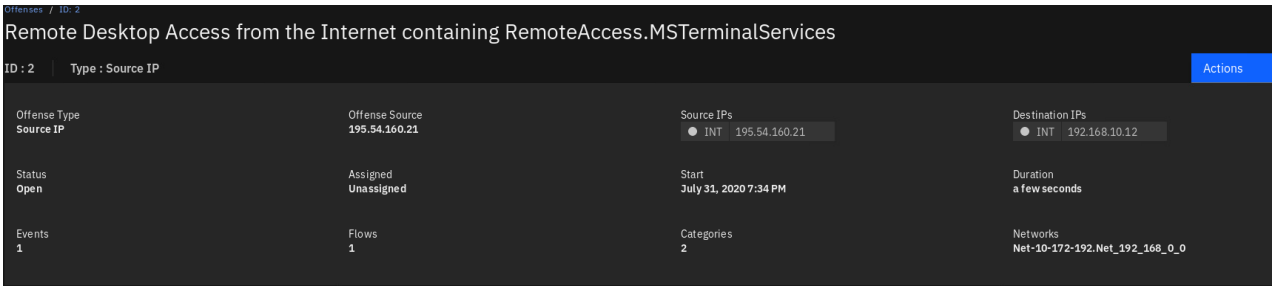
**Important:** Because the Analyst app UI is designed for quick and simplified analysis of offenses, you cannot edit the rules, their responses, and their actions, as with the Rule Wizard.

Follow these steps to navigate to an example offense and investigate it:

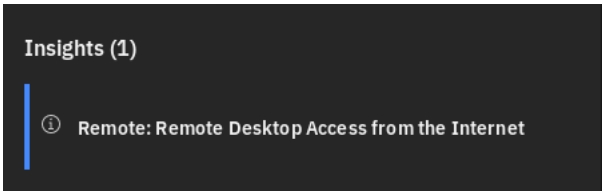
1. To open the main menu, click the menu icon in the upper left of the QRadar Console.
2. Click **Try the New UI**.
   The Analyst app opens in a new tab.
3. Scroll down and go to the last page of displayed offenses.
4. Click the offense number 2 with the description of **Remote Desktop Access from the Internet containing RemoteAccess.MSTerminal Services**.




The offense summary opens. Here you can see an overview of the details of the offense that are helpful for investigating the suspected attack or policy violation.




5. Click the Magnitude image.
   In the Offense Magnitude pane, you can see the magnitude calculation and a definition of each of its components. Scroll down to explore these definitions and then close the Magnitude pane.
6. One or more rules contributing to an offense are displayed to the left, under **Insights**. For this offense, there is only one rule; click **Remote: Remote Desktop Access from the Internet**.



In the pane that opens on the right you can see the following information about the rule. Scroll down to view all items and compare them to what you saw in the Rule Wizard in Exercise 6:

- A description of what this rule does
- One or more groups to which this rule belongs
- The tests evaluated by this rule
- The rule actions and the variables associated to them
- The details of the rule
- The responses enabled for the rule

7. Close the rule insight details pane.

**Note:** The Analyst app doesn't support the investigation of flows that are associated with an offense.

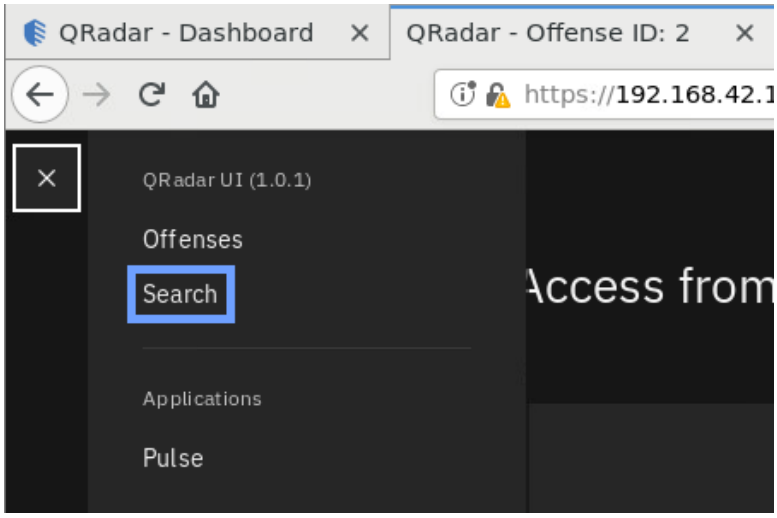
# Exercise 9 Creating a search for RDP connections to your server in the Analyst app

Although you cannot explore the flows associated with the offense in the Analyst app, you can perform advanced searches based on any variable available in the QRadar database. In this exercise, you create a search for the same RDP connections for which a search was created in exercise Exercise 7, so you follow up the offense that you investigated in the previous exercise.

1. In the offense details of the Analyst app, take note of the destination IP.

_____

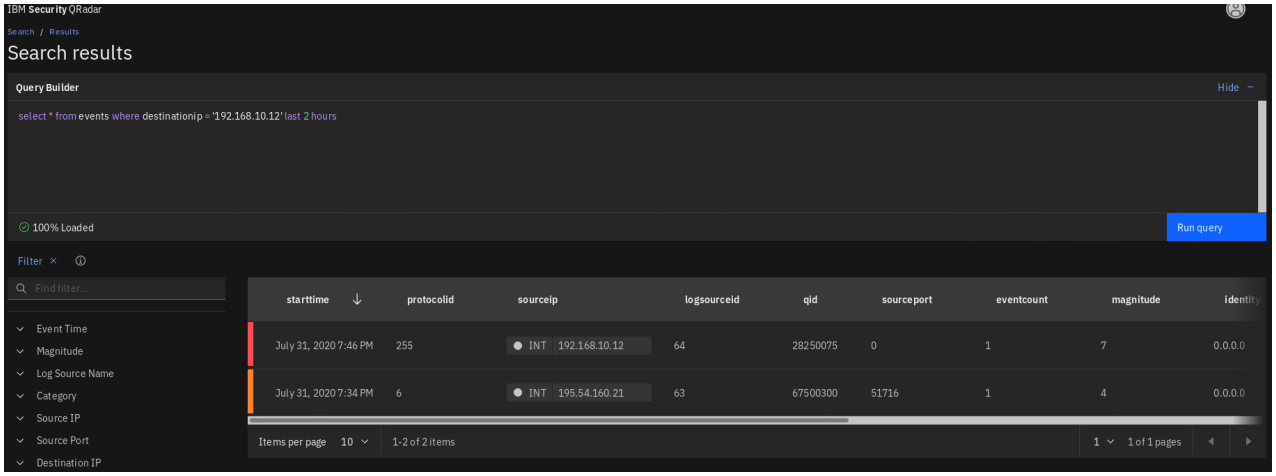
2. From the Analyst app main menu on the upper left, click **Search**.




3. In the Query builder field, type `select * from events where destinationip = '192.168.10.12' last 2 hours`.

   This displays the fields from the events table with the same destination IP as the event and flow that is involved in the RDP offense in the last 2 hours.

4. Click **Run Query** to display the results.

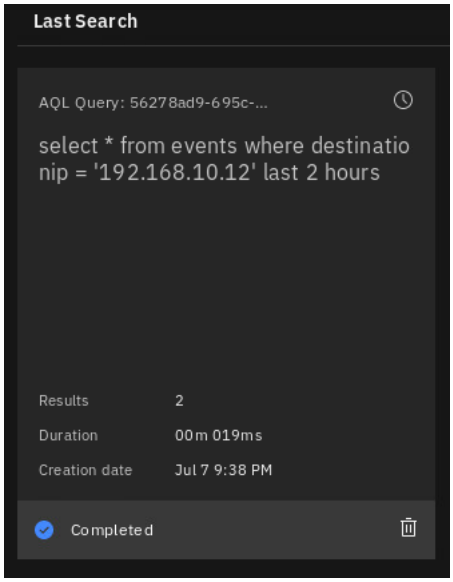



**Note:** The Query Builder field also has an auto-complete feature that suggests parameters based on the text you are typing. This feature is not available in this virtual lab.

Although you cannot save this result as a search, you can view a recent search.

5. From the Analyst app main menu, click **Search** again.

   The recent query is displayed in the Last Search section; Click **select * from events where destinationip = '192.168.10.12' last 2 hours**.



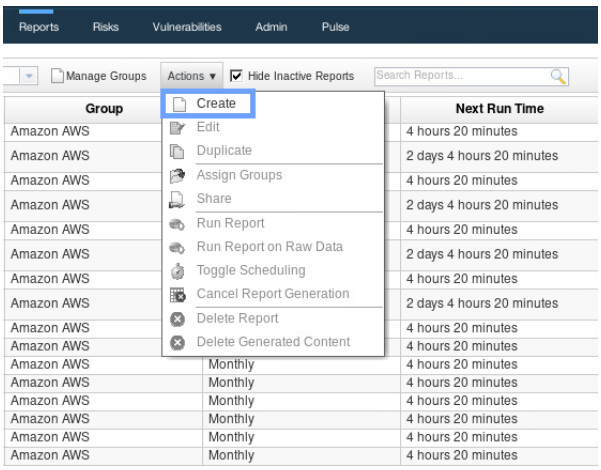

You can run this query multiple times to verify whether the targeted IP address is attacked again or not, thus helping you quickly search for recent RDP connections.

6. Close the **Analyst app** tab.

# Exercise 10 Creating a remote access report template

In the previous exercise, you applied a filter to flows and saved the search. Based on this saved search, you follow these steps to create a report template. To monitor remote access to your server, you use the template to generate a report.

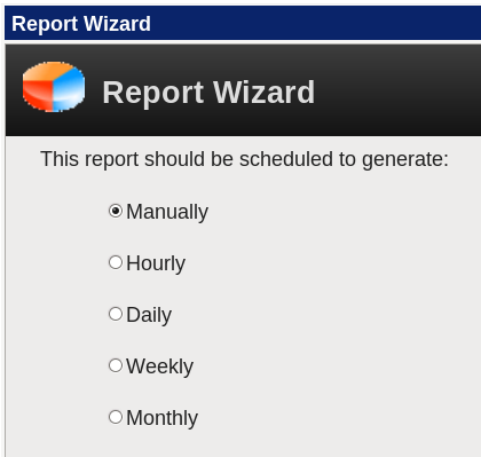
1. Navigate to the **Reports** tab and choose **Actions > Create**.




2. Click **Next**.
With QRadar SIEM,you can schedule reports so that they generate automatically at specified

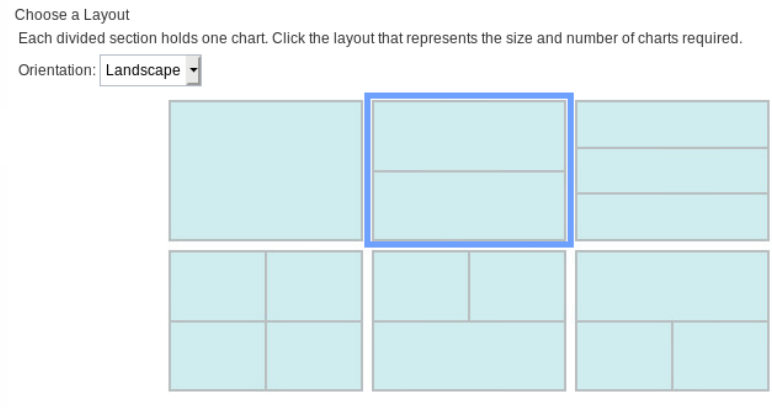
times. For example, the schedule *Daily* would include all flows from the previous day. Therefore, such a report does not include the flow that you received earlier.

3. To include the latest flows, leave **Manually** selected as the schedule for the report generation. In a later step, you specify the timeframe for the report.



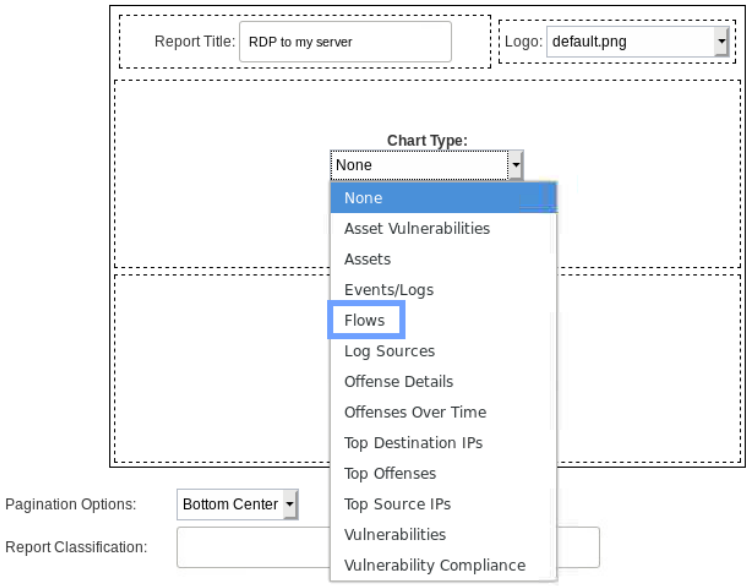

**Note:** A QRadar SIEM report template is a means of scheduling and automating one or more saved searches.

4. Click **Next**.
5. For the report layout, select the double-container layout as is shown in the following image. This layout displays a chart on the first container and a table on the second one.
6. Click **Next**.




7. In the **Report Title** field, enter `RDP to my Server`.

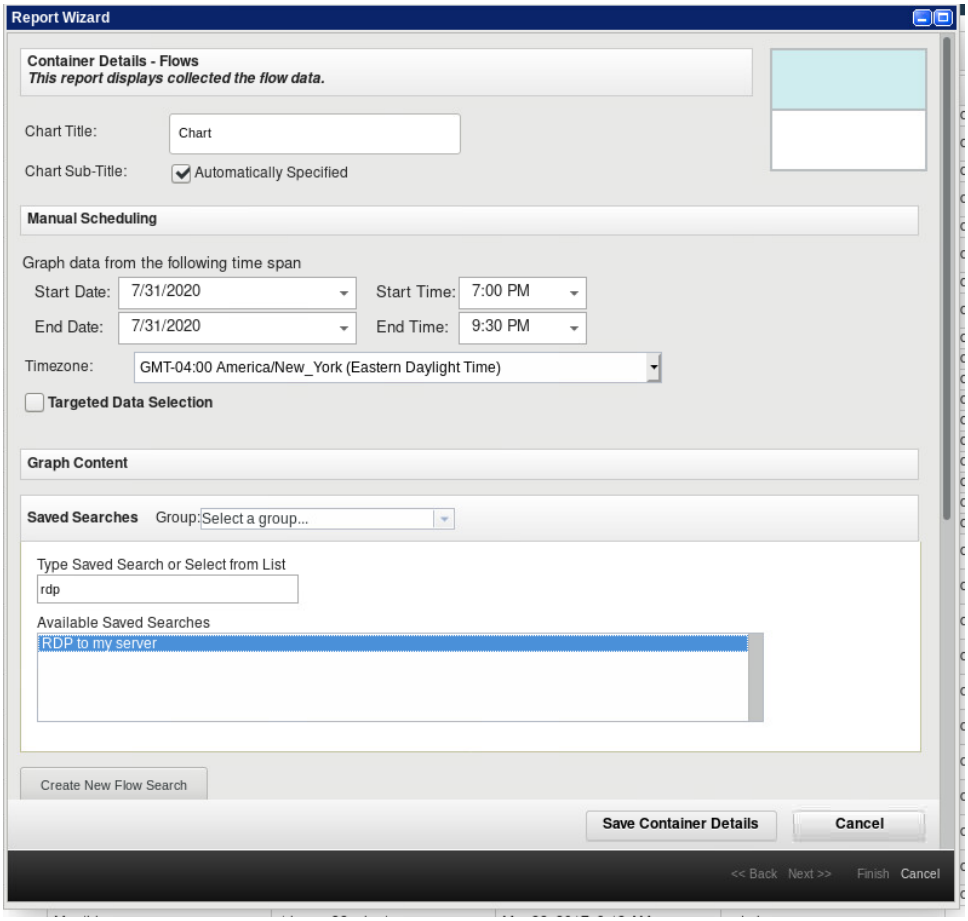
8. For the **Chart Type** menu in the upper container, select **Flows**.




9. The Report Wizard automatically displays the Container Details. Complete the following steps:
   a. For **Chart Title**, enter `Chart`.
   b. For **Start Date** and **Time**, and **End Date** and **Time**, select a timeframe that includes the time when you captured the flow. In this case, select 7:00 PM as the **Start Time** and 9:30 PM as the **End Time**.
   c. To find and select the search that you created in the previous exercise, in **Type Saved Search**, type `rdp` and press **Enter**.

**Note:** You must press Enter in this virtual environment to narrow down the search result.

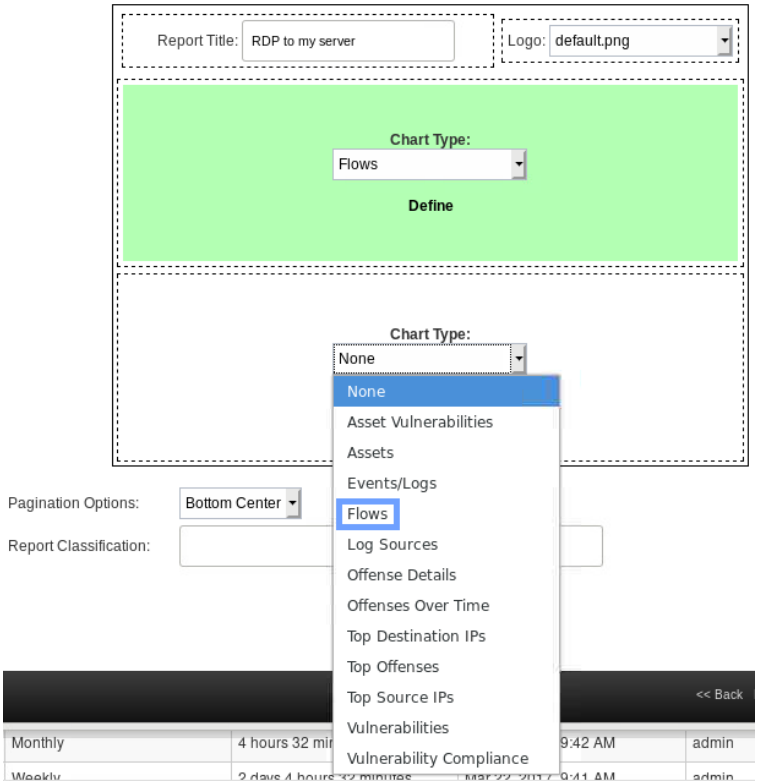
d. Double-click your **RDP to my Server** search.




e. To finish, click **Save Container Details**.

The Report Wizard displays the page to specify the chart type again.

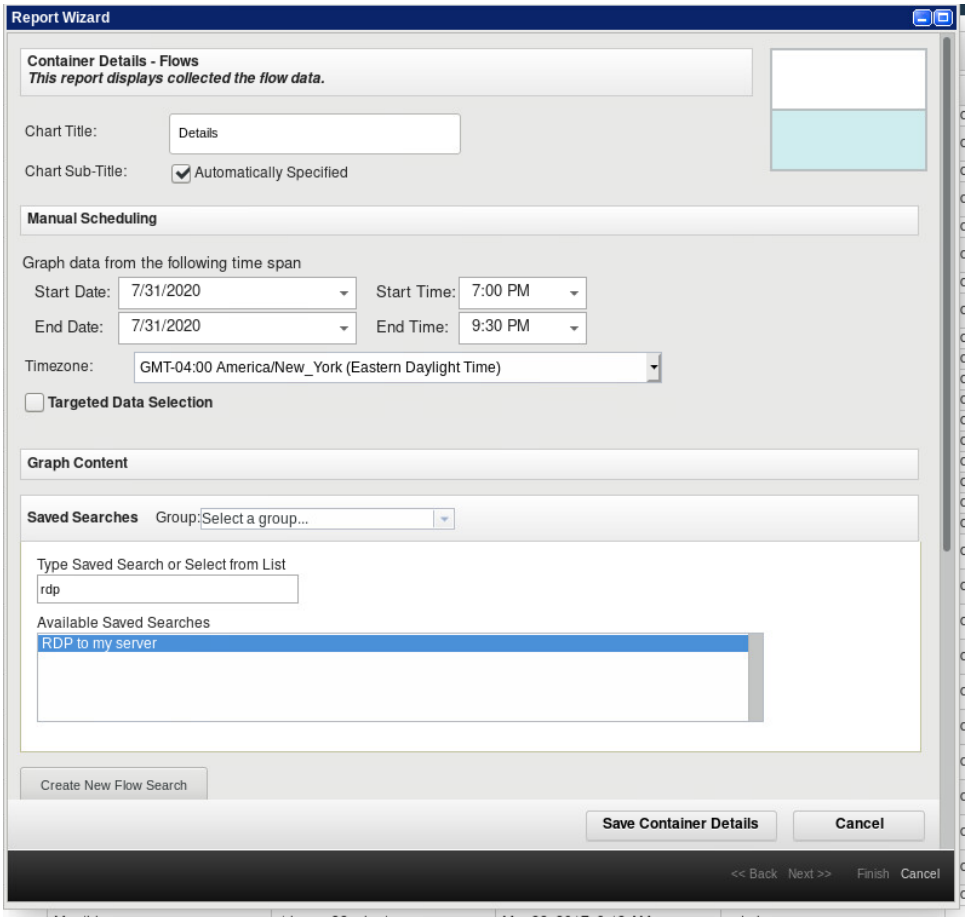
10. After you configure the first container, use the following steps configure the second container. The process is similar, but has one important difference. For the **Chart Type** menu in the lower container, select **Flows**.



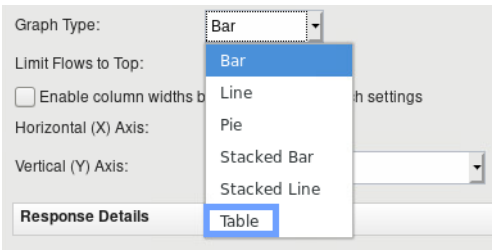

11. The Report Wizard automatically displays the Container Details for the lower container. Complete the same steps as for the upper container, but change the **Graph Type** to **Table**.
    a. For **Chart Title**, enter `Details`.
    b. For **Start Date** and **Time**, and **End Date** and **Time**, leave default values.
    c. To find and select the search that you created in the previous exercise, in **Type Saved Search**, type `rdp` and press Enter.

**Note:** You must press Enter in this virtual environment to narrow down the search result.

d. Double-click your **RDP to my Server** search.

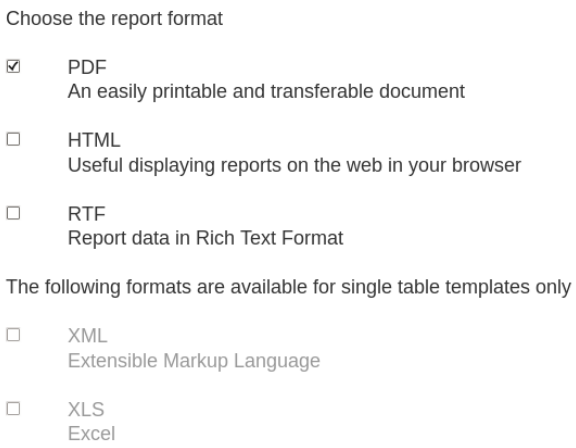



e. Scroll down. For **Graph Type**, select **Table**.

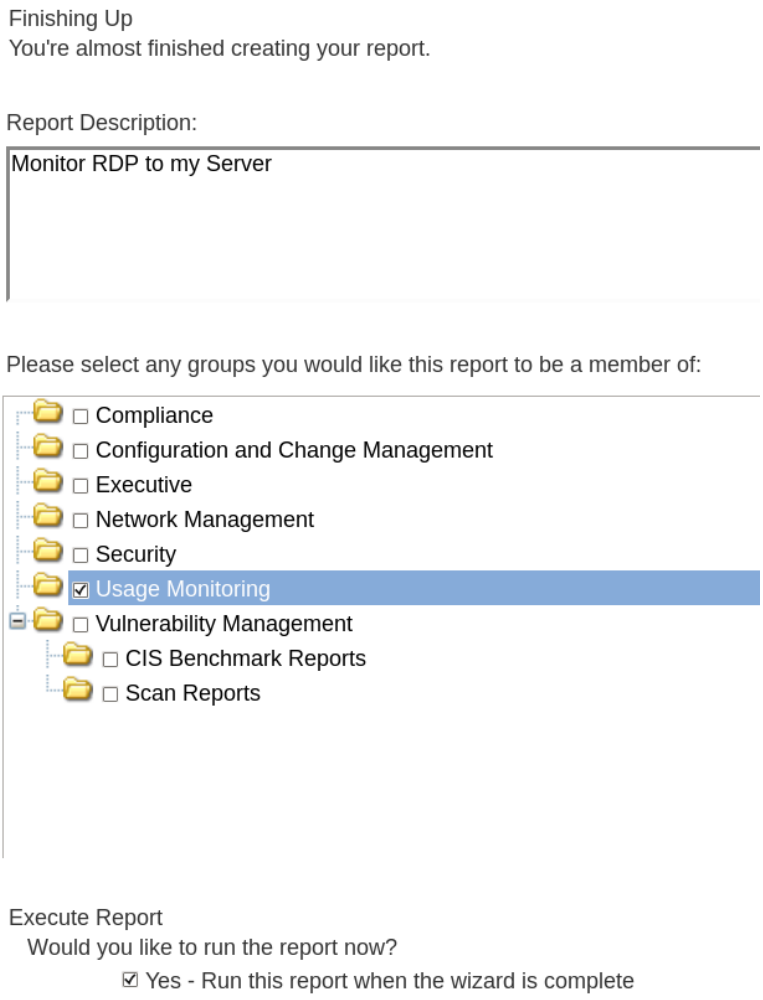



f. To finish, click **Save Container Details**.

12. Click **Next** until you reach the **Choose the report format** step.
    **PDF** is preselected.




13. Click **Next** until you reach the **Finishing Up** step:
    a. For **Report Description**, enter `Monitor RDP to my Server`.
    b. For **Groups**, scroll to the end of the list and select **Usage Monitoring**.
    Confirm that **Yes - Run this report when the wizard is complete** is selected.

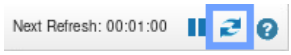


14. Click **Next** again.

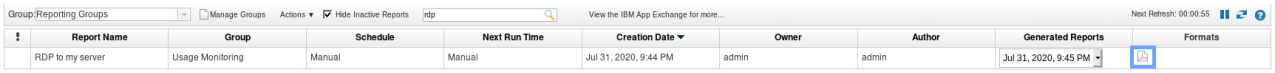
15. Click **Finish**.

16. In the **Search Reports** field, type RDP and click the **Search Reports** icon to filter the report list. QRadar SIEM starts to generate the report. This takes about one minute in the real environment to complete the report.

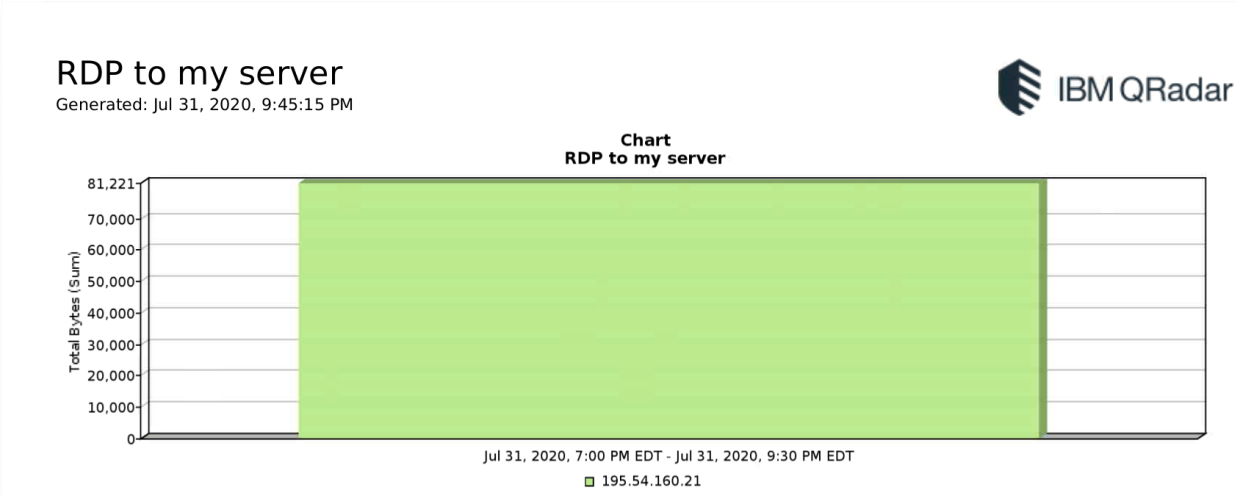
17. Click the **Refresh** icon on the upper right.




18. When you are finished, QRadar SIEM displays a **PDF** icon for the new report template in the rightmost column on the **Reports** tab. To view the generated report, click the **PDF** icon.




The report is displayed.




***Details***
***RDP to my server***
***Jul 31, 2020, 7:00:00 PM - Jul 31, 2020, 9:30:00 PM***

| Source IP | Source Network (Unique Count) | Destination IP (Unique Count) | Destination Port (Unique Count) | Destination Network (Unique Count) | Application (Unique Count) | Destination Bytes (Sum) | Source Bytes (Sum) | Total Bytes (Sum) | Destination Packets (Sum) | Source Packets (Sum) | Total Packets (Sum) | Count |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 195.54.160.21 | other | 192.168.10.12 | 3389 | Net-10-172-192.Net_192_168_0_0 | RemoteAccess.MSTerminalServices | 39,733 | 41,488 | 81,221 | 158 | 153 | 311 | 2 |

1

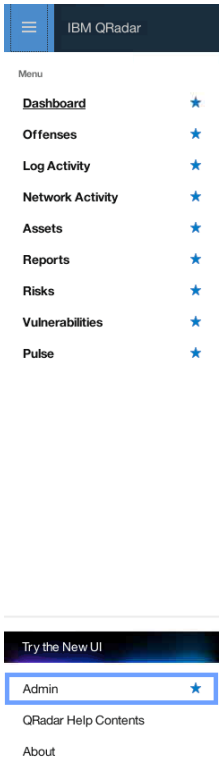
19. Close the report window and return into the main QRadar console.

# Exercise 11 Configuring the network hierarchy

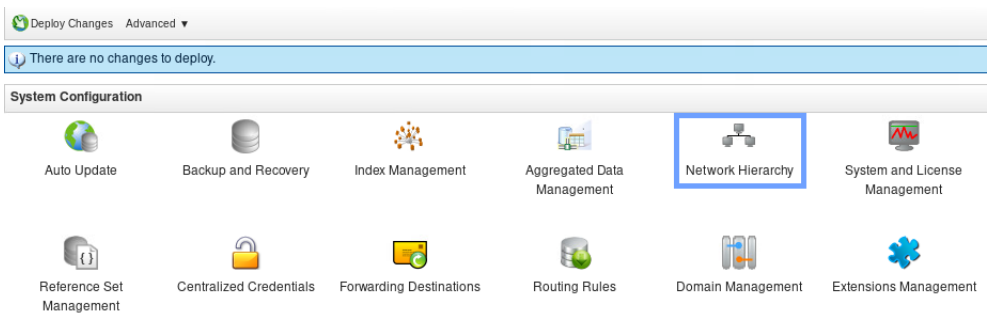
You confirmed that the source IP address of the RDP connection belongs to your organization. QRadar SIEM created an offense because it considered the source IP address a remote address. Therefore, you need to add the IP address to the network hierarchy of QRadar SIEM, which is the only way QRadar SIEM can identify an IP address as local. Follow these steps to add an IP address to the network hierarchy and avoid generating the RDP offense from the same IP again:

1. To open the Network Hierarchy window, navigate to the **Admin** tab.

**Note:** If the Admin tab is not displayed in your Console, open the menu by clicking the menu icon in the upper left, then locate and click “Admin”from the menu.

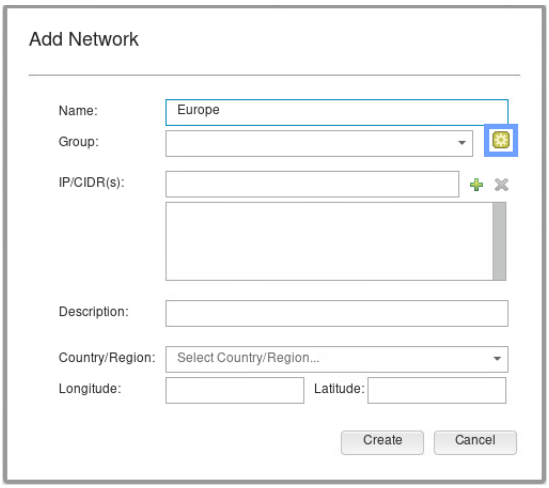



2. In the System Configuration section, click the **Network Hierarchy** icon.



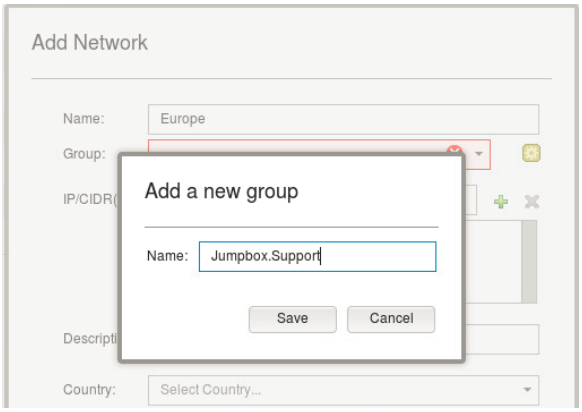
The Network Hierarchy window opens.

3. To create a new network object, perform the following steps:
   a. Click **Add**.
      The Add Network window opens.
   b. For **Name**, enter `Europe`.
   c. To create a new network group object, click the **Settings** icon next to the Group field.



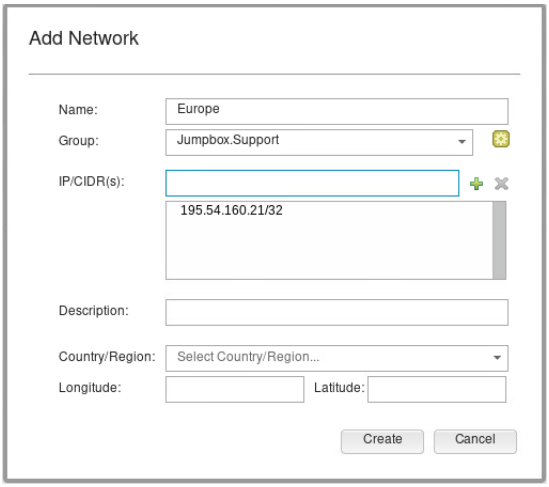

The Add a new group window opens.

   d. For **Name**, enter `Jumpbox.Support`. Make sure that you enter the period between Jumpbox and Support.




   e. Click **Save**.
      The Add a new group window closes.

f. For **IP/CIDR(s)**, enter `195.54.160.21`.




g. Click the **Add** icon next to the IP/CIDR(s) field.

h. Click **Create**.

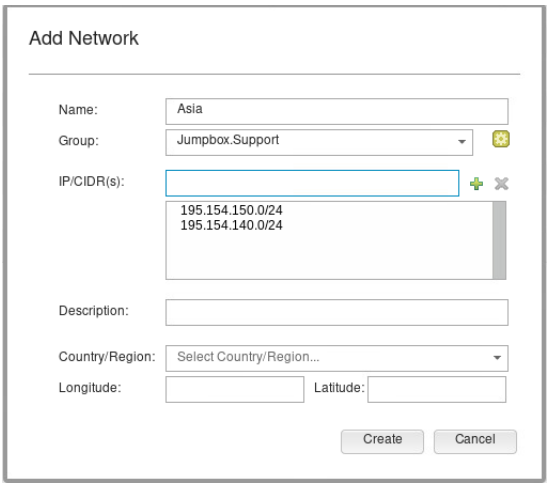
The Add Network window closes.

4. You created a network object with the single IP address from the offense. To create a new network object with two subnets, repeat the previous steps with the values that are shown in the following table.

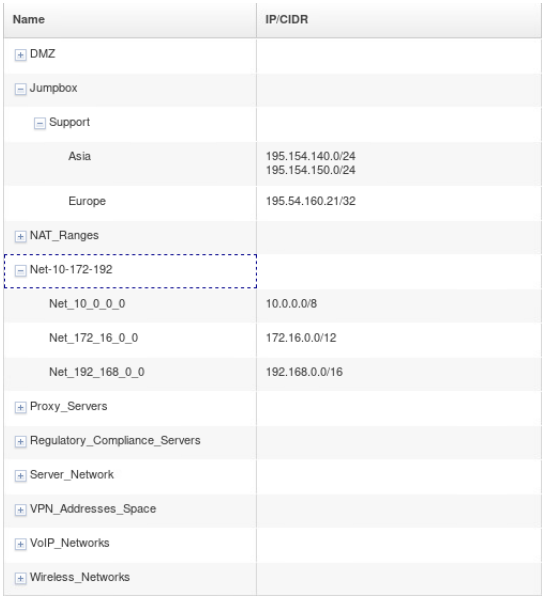
| Name | Group | IP/CIDR(s) |
|---|---|---|
| Asia | Jumpbox.Support | 195.154.140.0/24<br>195.154.150.0/24 |

**Note:** Because you already added the Jumpbox.Support group, you don't have to add it again. Instead, select it from the Group list.

**Important:** For **IP/CIDR(s)**, enter the subnets with the **/24** suffix. If you do not enter a suffix, QRadar SIEM defaults to the **/32** suffix.



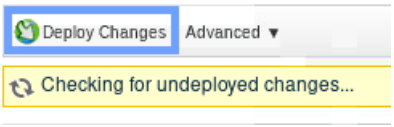

5. To close the window, click **Create**.
6. To display the network objects that you created, click the **Add** icons next to **Jumpbox** and **Support** in the Network Hierarchy window.




7. Click the Add icons next to **Net-10-172-192**.

   The private IP address ranges reserved by the Internet Assigned Numbers Authority (IANA) are displayed. The network hierarchy has these preconfigured ranges because they cannot be routed through the public Internet and therefore the private IP address ranges can be only local.
8. Close the Network Hierarchy window.
9. To apply your modifications, on the **Admin** tab, click **Deploy Changes**.

**Hint:** If clicking **Deploy Changes** does not do anything, double-click the **Admin** tab. The double-click resets the tab to its default settings. Click **Deploy Changes** again.




**Note:** QRadar SIEM considers all networks that are configured in the network hierarchy as local to your organization. Rules use this information to determine whether they suspect an attack or policy violation.

# Exercise 12 Closing the offense

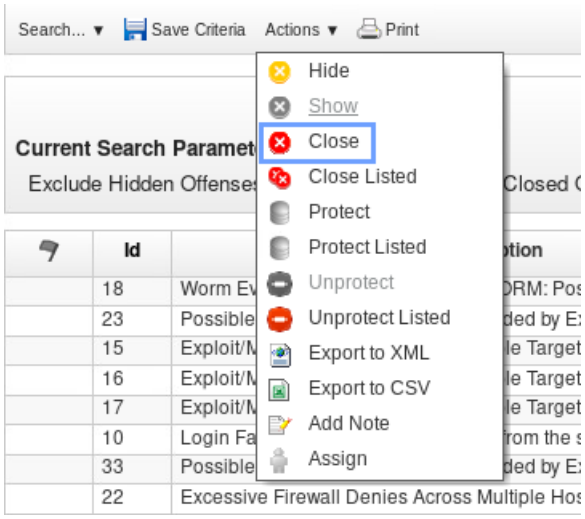
After you assume that the RDP connection was legitimate and you update the network hierarchy, follow these steps to close the offense:

1. Double-click the **Offenses** tab.

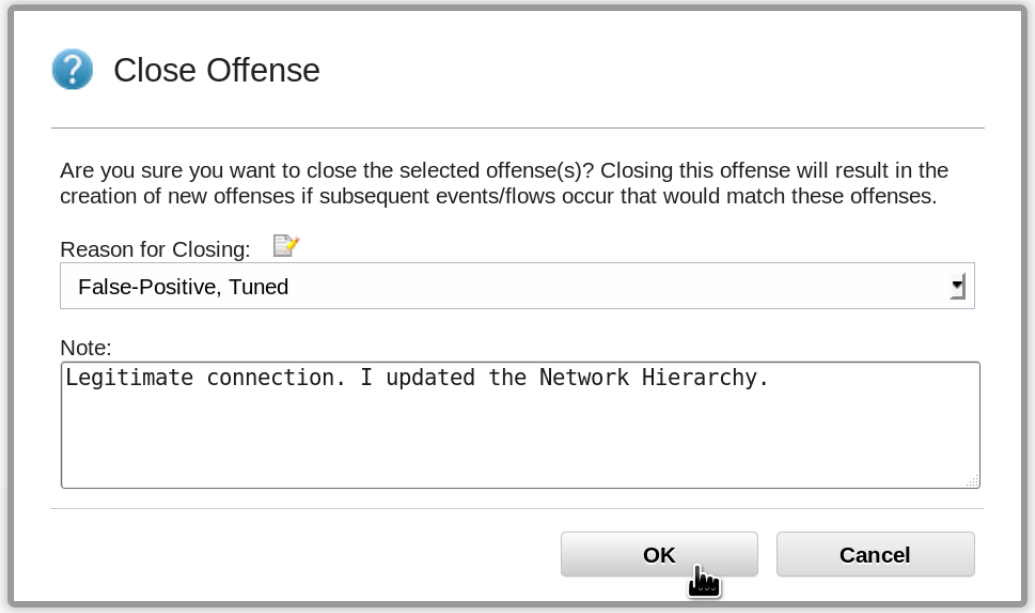
**Hint:** Double-clicking resets the tab to its default settings.

2. Select the offense number 2 with the description of **Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices**.

3. From the **Actions** menu, select **Close**.




4. The Close Offense window opens. In the **Note** field, enter a reason for closing the offense and click **OK**.




**Note:** Notice that the offense is no longer displayed in the Offenses tab. Also, because you updated the network hierarchy, this offense is no longer generated based on the same IP.

# Exercise 13 Navigating through other tabs

Follow these steps to explore QRadar SIEM further:

1. QRadar SIEM automatically creates asset profiles for your local computers. If the source or destination IP address of a flow or event falls into one of the networks that are configured in the network hierarchy, QRadar SIEM creates an asset profile.

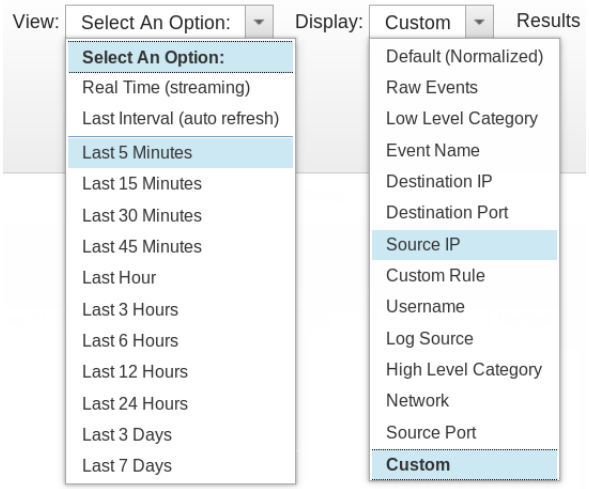
   In the QRadar SIEM web Interface, click the **Assets** tab to see which asset profiles are created.

2. To watch incoming events, double-click the **Log Activity** tab.

**Note:** An icon in the first column of the **Log Activity** and **Network Activity** tabs indicates that the event or flow contributes to an offense. You can navigate to the offense by clicking the icon. This action is not supported in this virtual environment.

3. To watch incoming flows, double-click the **Network Activity** tab.

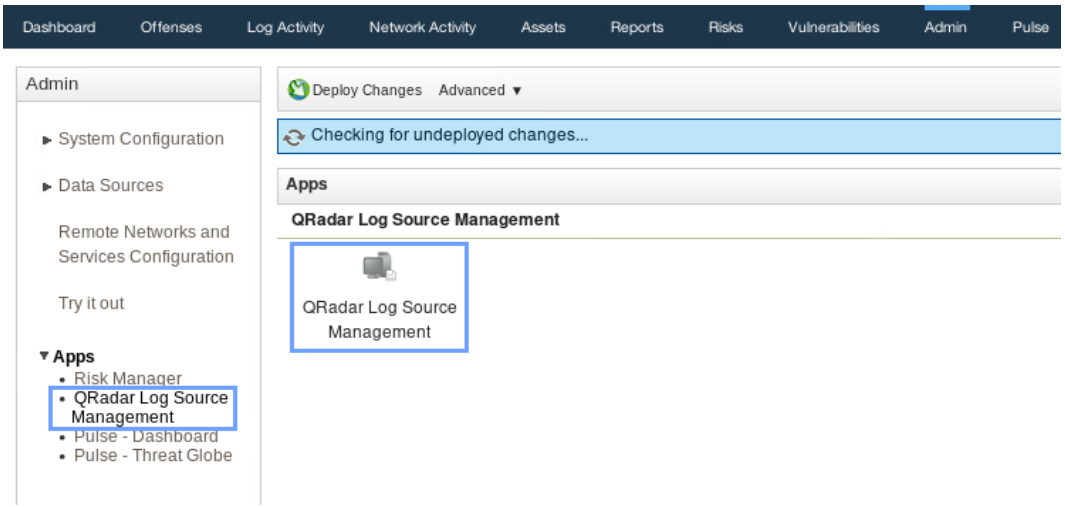
4. You can view events flows from different perspectives. Select **Last 5 Minutes** from the **View** menu, then select Source IP, Application, and Protocol from the **Display** menu, and check the results.




QRadar SIEM groups the flows by your selection in the Display list. In this example, grouping by **Source IP** displays a column of all the unique source IPs and summary information of the other columns, such as the number of unique destination ports for each source IP.

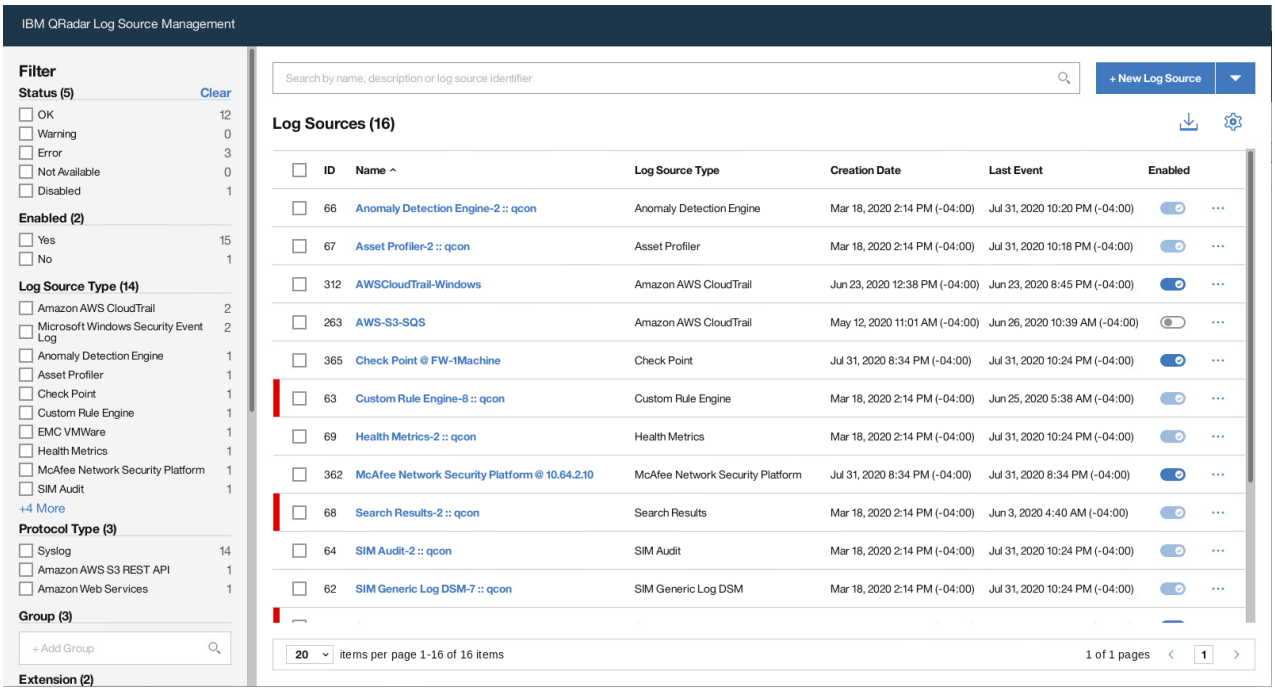
5. The **Log Sources** of QRadar SIEM receive the raw events. QRadar SIEM identifies many log sources automatically by analyzing the format of the incoming raw events. If QRadar SIEM identifies the source of raw events, it creates a log source object. To open the Log Source

Management window, navigate to the **Admin** menu and then click the **Apps** > **QRadar Log Source Management**.




The Log Sources window opens. It lists the log sources that QRadar SIEM automatically created from analyzing the incoming raw events. You can also import or create log source objects manually.

**Hint:** To learn about the Log Source Management app, watch the **QRadar Log Source Management** course in the Security Learning Academy.




6. **Close** the Log Source Management window.

You used QRadar SIEM to separate signal from noise to detect and investigate suspicious activities.

# Appendix

Exercise 6, “Investigating a remote access offense,” on page 19

**Step 4 on page 21**

Step a: What is the second test?

*and NOT when the flow context is Local to Local*

Step b: How many variables are there in the second test?

*Two: “and NOT” and “Local to Local”*

Step c: What is the third test?

*and when a flow matches all of the following BB:Threats:R emote Access Violations: Remote Desktop Access from Remote Hosts, BB:Category Definition: Successful Communication*

Step d: How many variables are there in the third test?

*Three: “and”, “all”, and “BB:Threats:R emote Access Violations: Remote Desktop Access from Remote Hosts, BB:Category Definition: Successful Communication”*

**Step 7 on page 22**

Step a: What are the available options for this context?

*Local to Local, Local to Remote, Remote to Local, and Remote to Remote*

**Step 8 on page 22**

Step a: What are the two selected building blocks for this variable in the Selected Items list?

*BB:Threats:R emote Access Violations: Remote Desktop Access from Remote Hosts,*

*BB:Category Definition: Successful Communication*

**Step 10 on page 23**

Step a: Which action is enabled by default?

*Ensure the detected flow is part of an offense*

Step b: Based on which variable is the offense indexed?

*Source IP*

**Step 11 on page 23**

Step a: How many responses can be enabled in total?

*Eleven: Dispatch New Event, Email, Send to Local SysLog, Send to Forwarding Destinations, Notify, Add to a Reference Set, Add to Reference Data, Remove from a Reference Set, Remove from Reference Data, Trigger Scan, and Execute Custom Action*

Step b: Which response is enabled by default?

*Dispatch New Event*

Step c: What are the low-level and high-level categories defined for the new dispatched event?

*Low-Level: Remote Access Policy Violation*

*Hight-Level: Policy*

Step d: Based on which variable is the offense indexed?

*Source IP*