

Lab Exercises

# Using IBM QRadar SIEM

Course code LSL0231X



## July 2019 edition

### NOTICES

This information was developed for products and services offered in the USA.

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, MD-NC119  
Armonk, NY 10504-1785  
United States of America*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to non-IBM 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 supply in any way it believes appropriate without incurring any obligation to you.

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.

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

### 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](http://www.ibm.com/legal/copytrade.shtml).

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

© Copyright International Business Machines Corporation 2019.

This document may not be reproduced in whole or in part without the prior written permission of IBM.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

**Exercises** ..... 1

    Virtual machines .....1

    Exercise 1 Sending sample data to QRadar SIEM ..... 2

    Exercise 2 Using dashboards and dashboard items ..... 4

    Exercise 3 Leveraging a dashboard item ..... 7

    Exercise 4 Investigating a remote access offense ..... 13

    Exercise 5 Creating a search for RDP connections to your server ..... 19

    Exercise 6 Creating a remote access report template ..... 23

    Exercise 7 Configuring the network hierarchy ..... 31

    Exercise 8 Closing the offense ..... 37

    Exercise 9 Navigating through other tabs ..... 39

---

# Exercises

IBM® Security QRadar® SIEM enables you to 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 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 of 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 into 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.

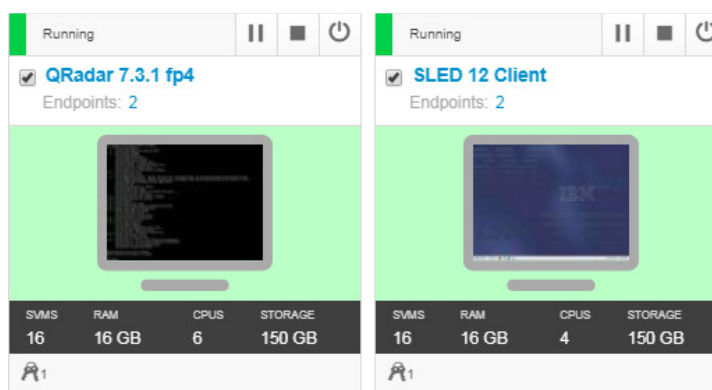
You can run the virtual lab multiple times without restriction.

## Virtual machines

This virtual lab simulates the following environment:

- QRadar 7.3.1 fp4 - a virtual machine running IBM QRadar on Red Hat Enterprise Linux.
- SLED 12 Client - a virtual machine providing a graphical user interface.

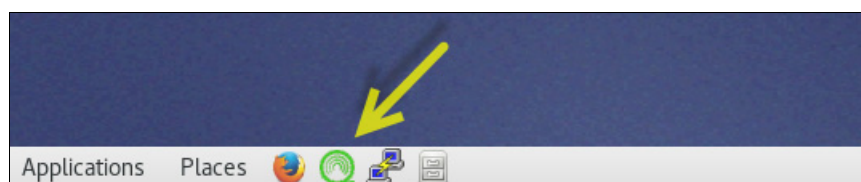
Your interaction with QRadar will be done using this virtual machine. You access this client selecting it in the IBM Security Learning Academy Lab web interface.



## Exercise 1 Sending sample data to QRadar SIEM

Before attempting to create a report, you must first have available data to be displayed by it. From this lab environment, you are able to run scripts that feed prepared sample data to QRadar. To generate a set of logs sample data into QRadar, perform the following steps on the SLED 12 Client machine:

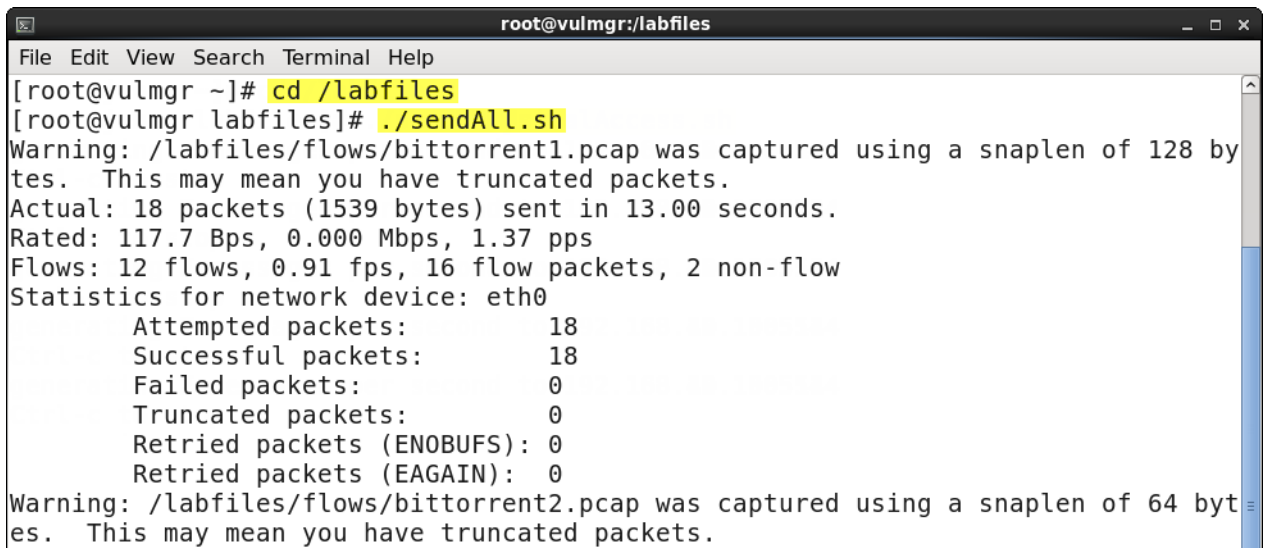
1. To open an SSH session to the QRadar VM, click the icon that resembles the letter **Q** of QRadar, on the bottom panel.



2. To feed prepared syslog messages to QRadar, run the following commands:

```
cd /labfiles  
./sendAll.sh
```

Ignore any warnings that appear in the terminal window.



```
root@vulmgr:/labfiles  
File Edit View Search Terminal Help  
[root@vulmgr ~]# cd /labfiles  
[root@vulmgr labfiles]# ./sendAll.sh  
Warning: /labfiles/flows/bittorrent1.pcap was captured using a snaplen of 128 bytes. This may mean you have truncated packets.  
Actual: 18 packets (1539 bytes) sent in 13.00 seconds.  
Rated: 117.7 Bps, 0.000 Mbps, 1.37 pps  
Flows: 12 flows, 0.91 fps, 16 flow packets, 2 non-flow  
Statistics for network device: eth0  
    Attempted packets:      18  
    Successful packets:     18  
    Failed packets:         0  
    Truncated packets:      0  
    Retried packets (ENOBUFS): 0  
    Retried packets (EAGAIN): 0  
Warning: /labfiles/flows/bittorrent2.pcap was captured using a snaplen of 64 bytes. This may mean you have truncated packets.
```

3. To start the web browser, click the **Firefox** icon on the bottom panel of the desktop.

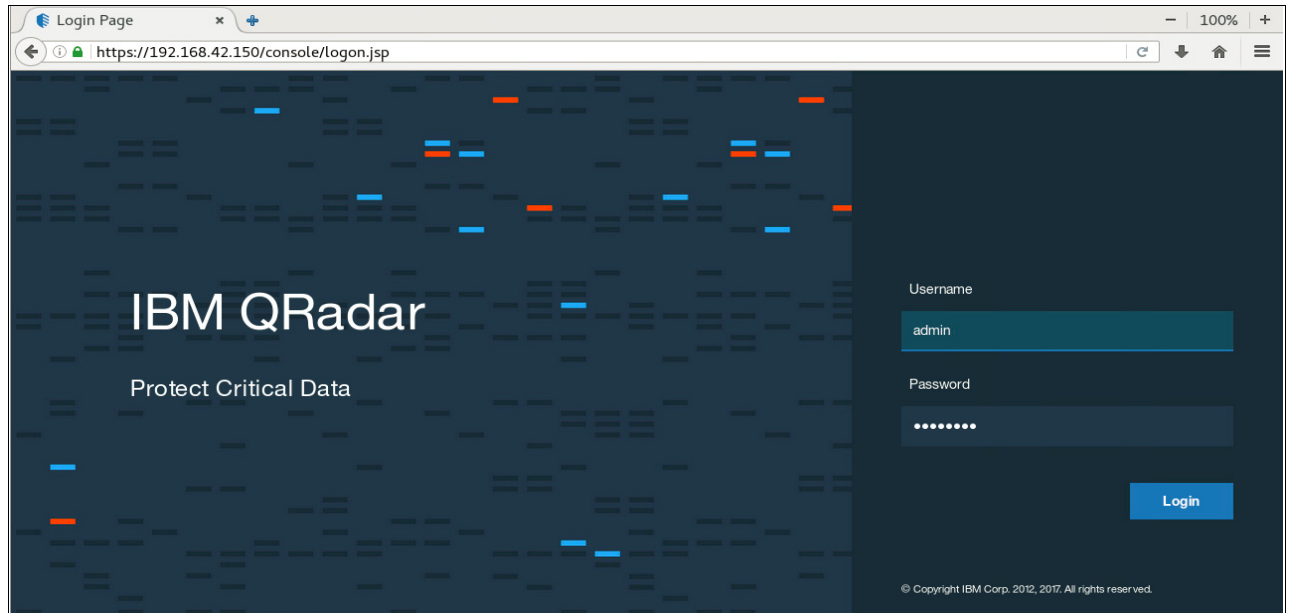


4. On the QRadar login page, the **Username** and **Password** fields should already be populated. If they are not populated, enter the following credentials:

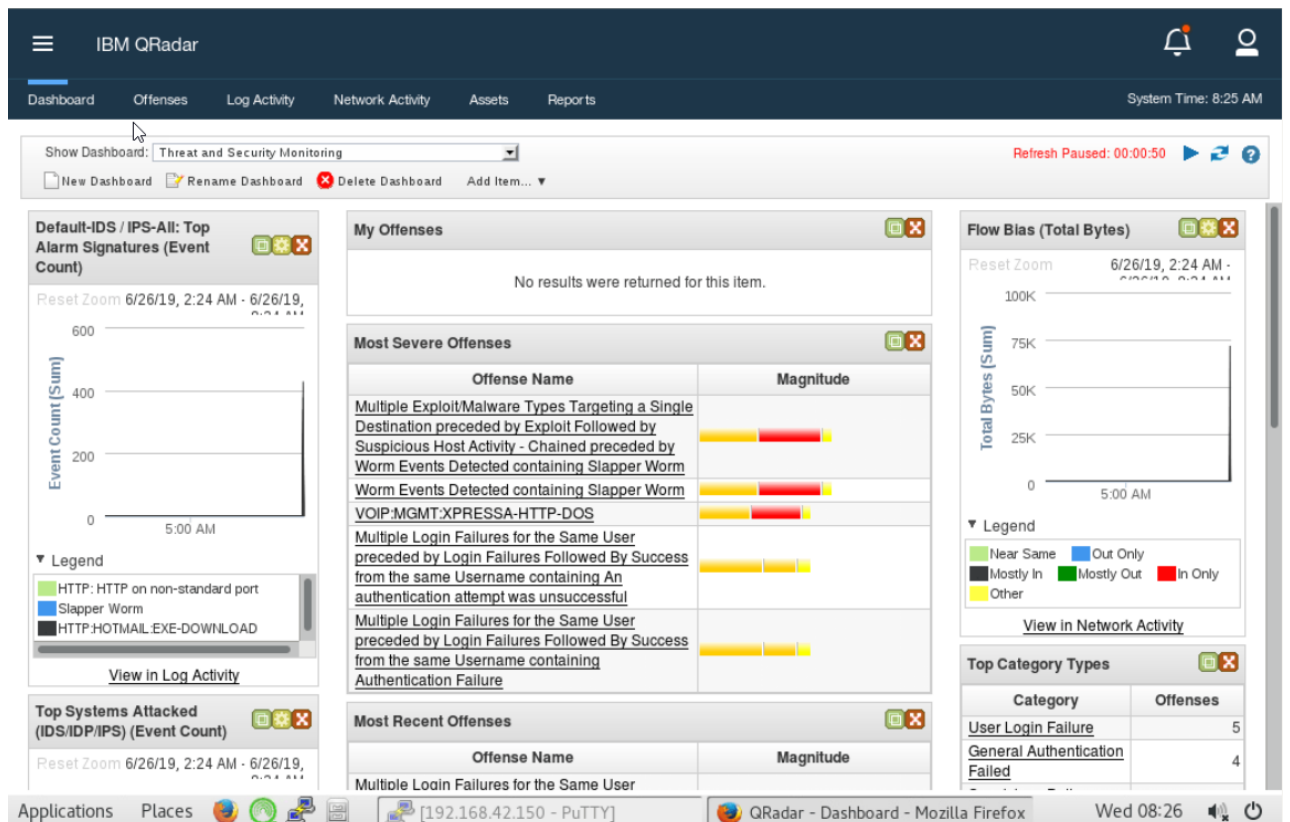
Username: admin

Password: P@ssw0rd      the '0' is the digit zero

5. To access to QRadar Console in the Firefox browser, click **Login**.



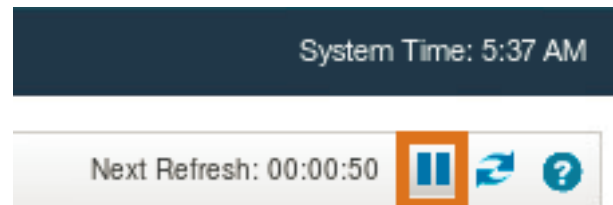
6. After logging in, you see a web interface similar to the one in the following image.



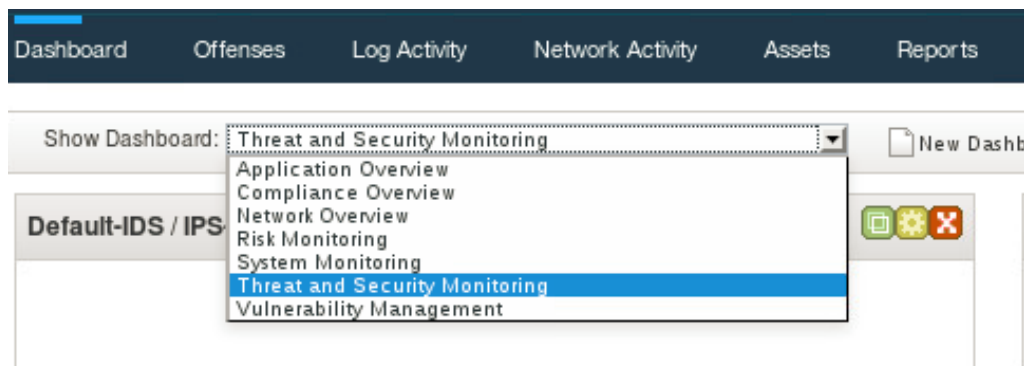
## Exercise 2 Using dashboards and dashboard items

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. The items enable you to 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 derived from the data fed into QRadar SIEM. QRadar SIEM refreshes the information on the **Dashboard** tab every minute. To start sending data into the Dashboard click the Play button located in the upper right-hand section of the toolbar. The button will turn into pause button.



2. QRadar SIEM provides seven pre-configured dashboards. Open the **Show Dashboard** drop-down menu and select one dashboard.

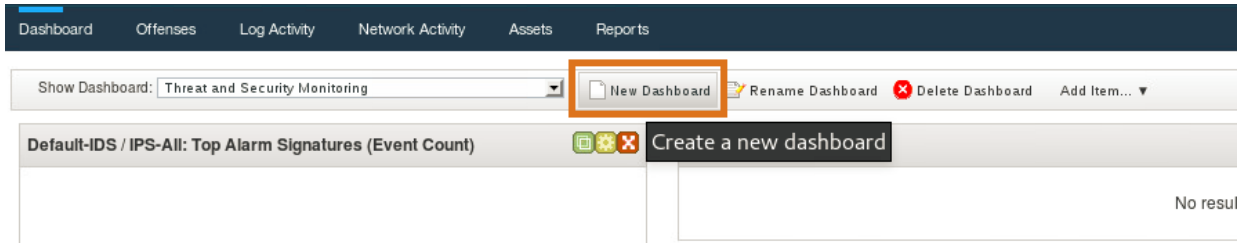


At this point the dashboards do not yet display much information, because the system was just booted and started to receive data. The longer the sample data is fed to QRadar SIEM, the more information the dashboard displays.

3. Once you have reviewed different dashboards, to move to the next step select Vulnerability Management dashboard and review the toolbar provides buttons to perform the following dashboard tasks:
  - Create a new dashboard
  - Rename an existing dashboard
  - Delete a dashboard



- Add an item to an existing dashboard

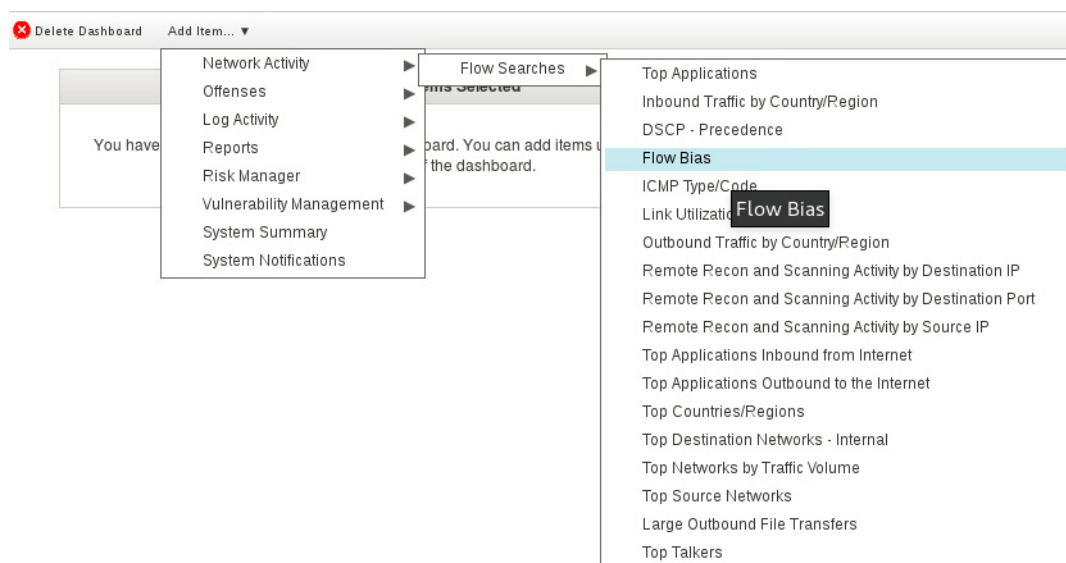


4. To create an additional dashboard, click the **New Dashboard** button.  
The New Dashboard window opens.
5. For **Name**, enter *Watch*.
6. Select **Share**, if you want to provide this dashboard to other users.

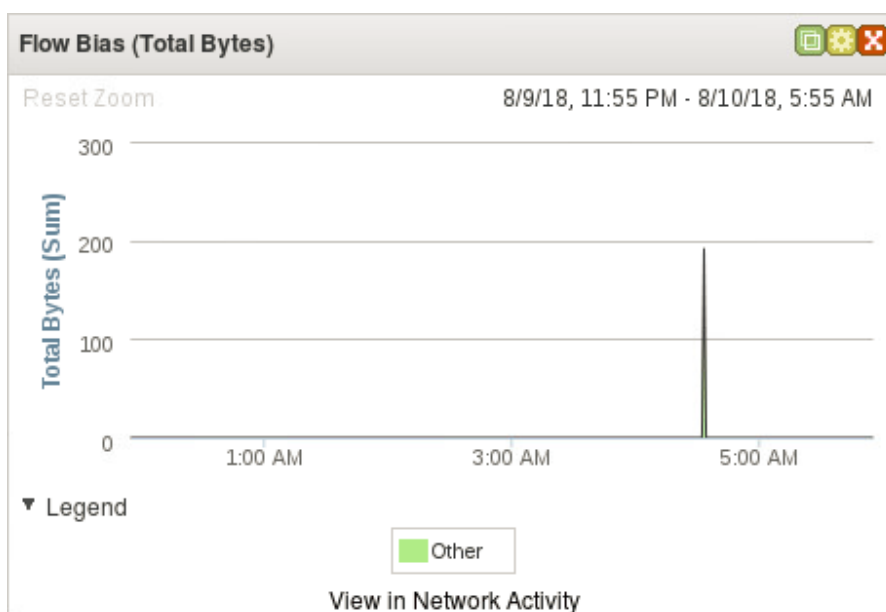
A screenshot of the 'New Dashboard' dialog box. It has a title bar 'New Dashboard'. Below the title bar is a text input field for 'Name' containing the text 'Watch'. Below that is a larger text area for 'Description'. At the bottom, there is a 'Share' checkbox which is checked. At the very bottom are 'OK' and 'Cancel' buttons.

7. To create the Watch dashboard, click the **OK** button.  
The New Dashboard window closes.
8. The **Dashboard** tab displays the new Watch dashboard. It does not display any dashboard items. To add a pre-configured item, click the **Add Item** button in the toolbar.

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

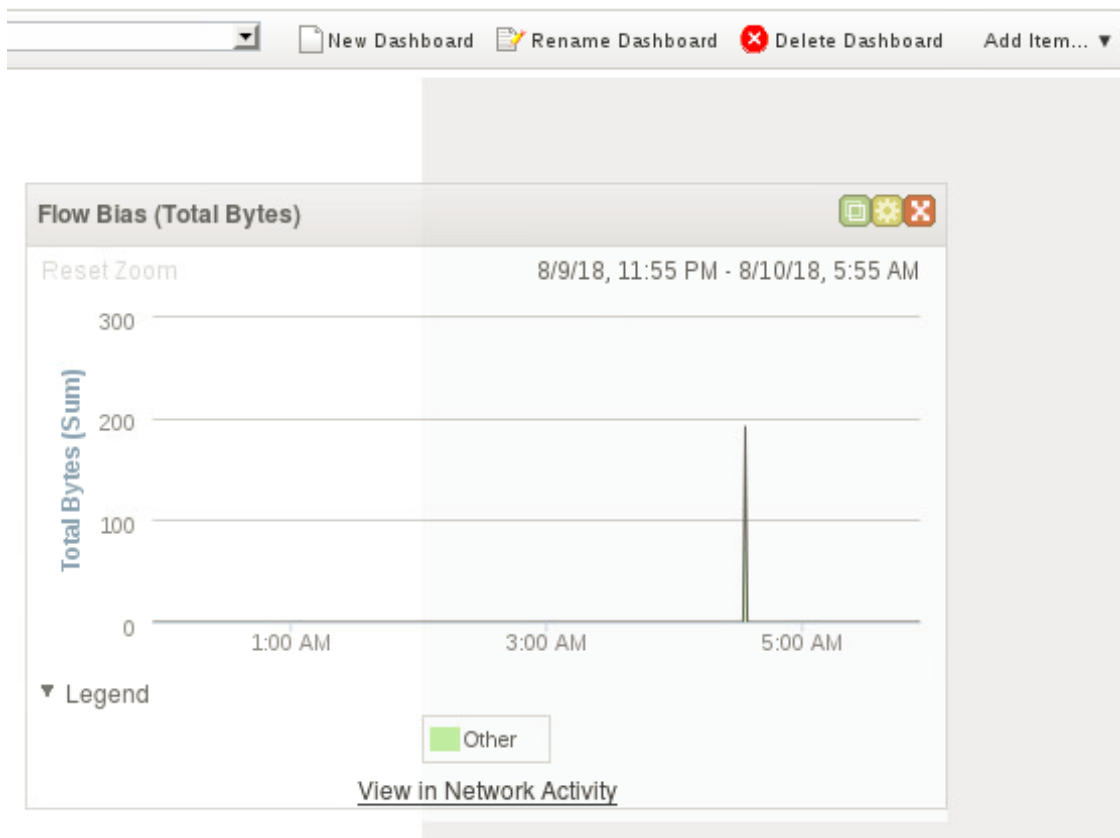


The Flow Bias item displays in the Watch dashboard.





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



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

## Exercise 3 Leveraging 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, the script that is started earlier to generate the data, sends a large number of sample network connections to QFlow in QRadar SIEM.

In the lab environment, QFlow monitors a 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.

## 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 being 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 being blocked by a firewall or a port scan attempt of a publicly reachable IP address of your organization.
- Mostly out: 70% to 99% of bytes outbound  
This bias indicates data leaving 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 end-user machines.
- 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 machines. It can also indicate traffic between two remote machines that either points to a misconfiguration of an organization's network or notifies you that a local network is missing in the network hierarchy of QRadar SIEM.

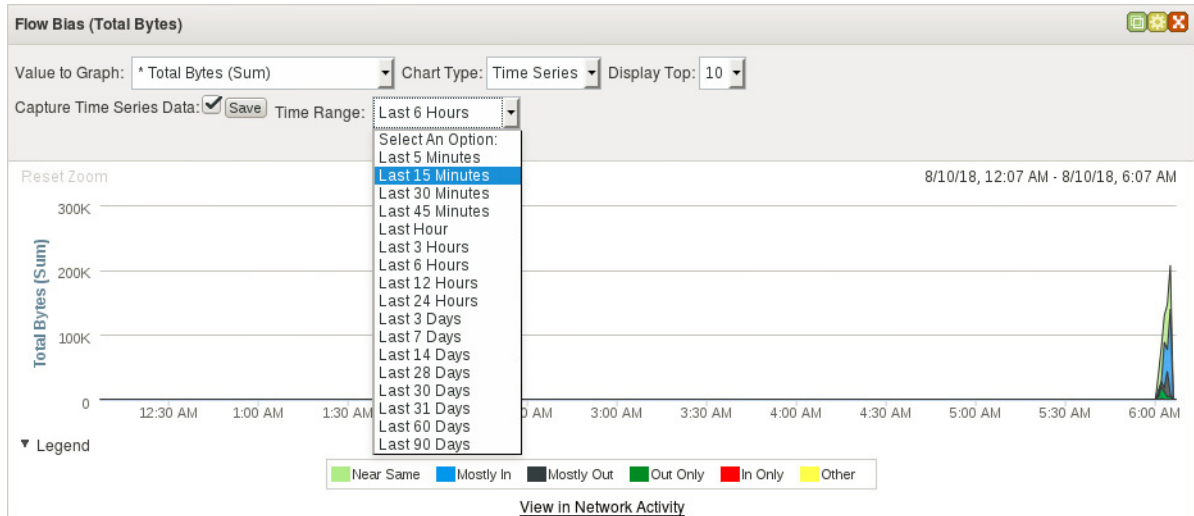
QRadar SIEM considers every network configured in its **network hierarchy** as part of your organization's local network. Therefore, the QRadar SIEM administrator needs to add any network belonging to your organization to the network hierarchy. You perform this task in [Exercise 7, Configuring the network hierarchy](#).

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

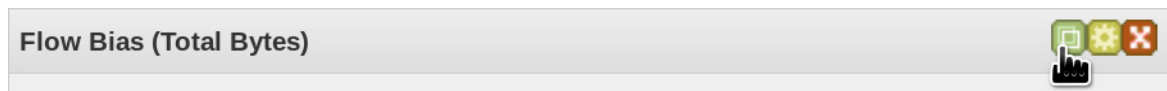
1. To configure what the chart in the item displays, click the yellow icon in the header of the Flow Bias item.



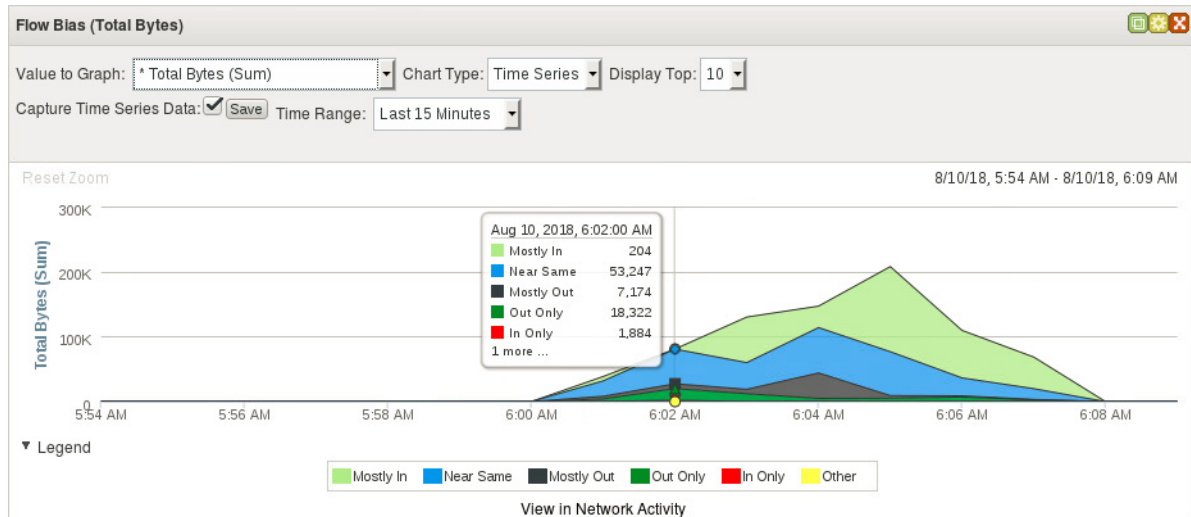
- To focus on the most recent flow biases, select **Last 15 Minutes** for **Time Range**.



- To detach the Flow Bias item, click the green button in the header of the item.  
The item opens in a separate browser window. QRadar SIEM keeps updating the item in the window, even if you would close the main window without logging out from QRadar SIEM. However, do not close the main browser window during this lab.



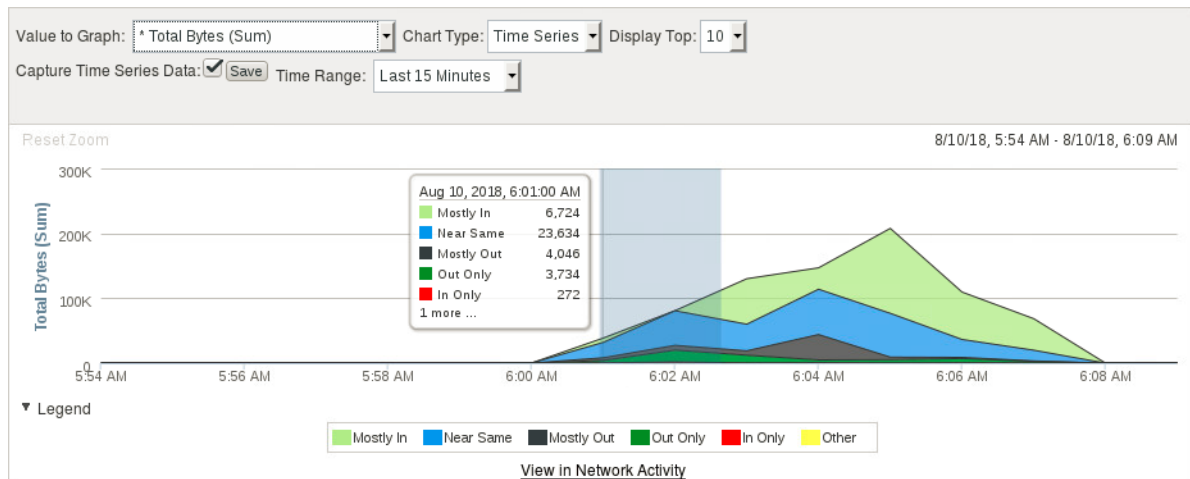
- To learn about the flow biases during a particular one-minute time interval, hover the mouse pointer over the chart.



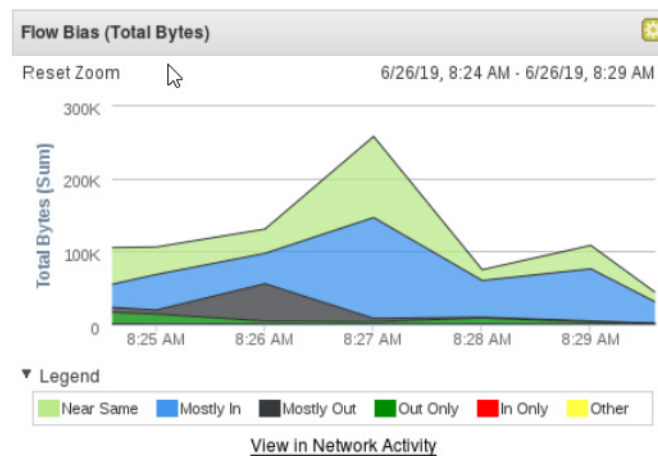
- To zoom in to a shorter chart interval, hold the left mouse button pressed while moving the mouse pointer to the left or right. Release the mouse button when you have highlighted the

interval that you want to zoom in to.

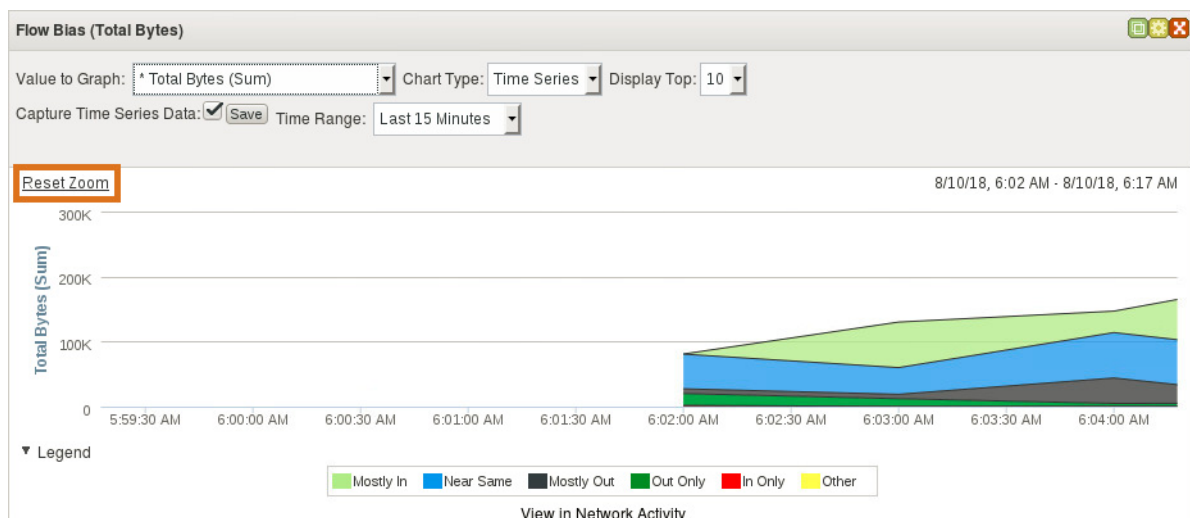
In this virtual environment, this step is simplified. To zoom in, click the graph.



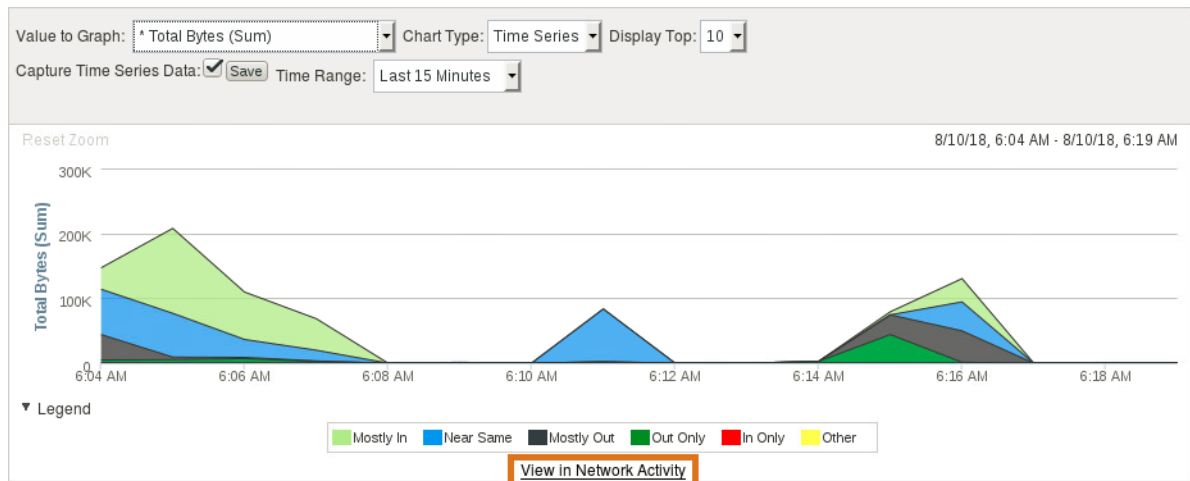
- To focus on the less prevalent flow biases, hide dominating flow biases from the chart. To do this, click the button in the legend with the green color.



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



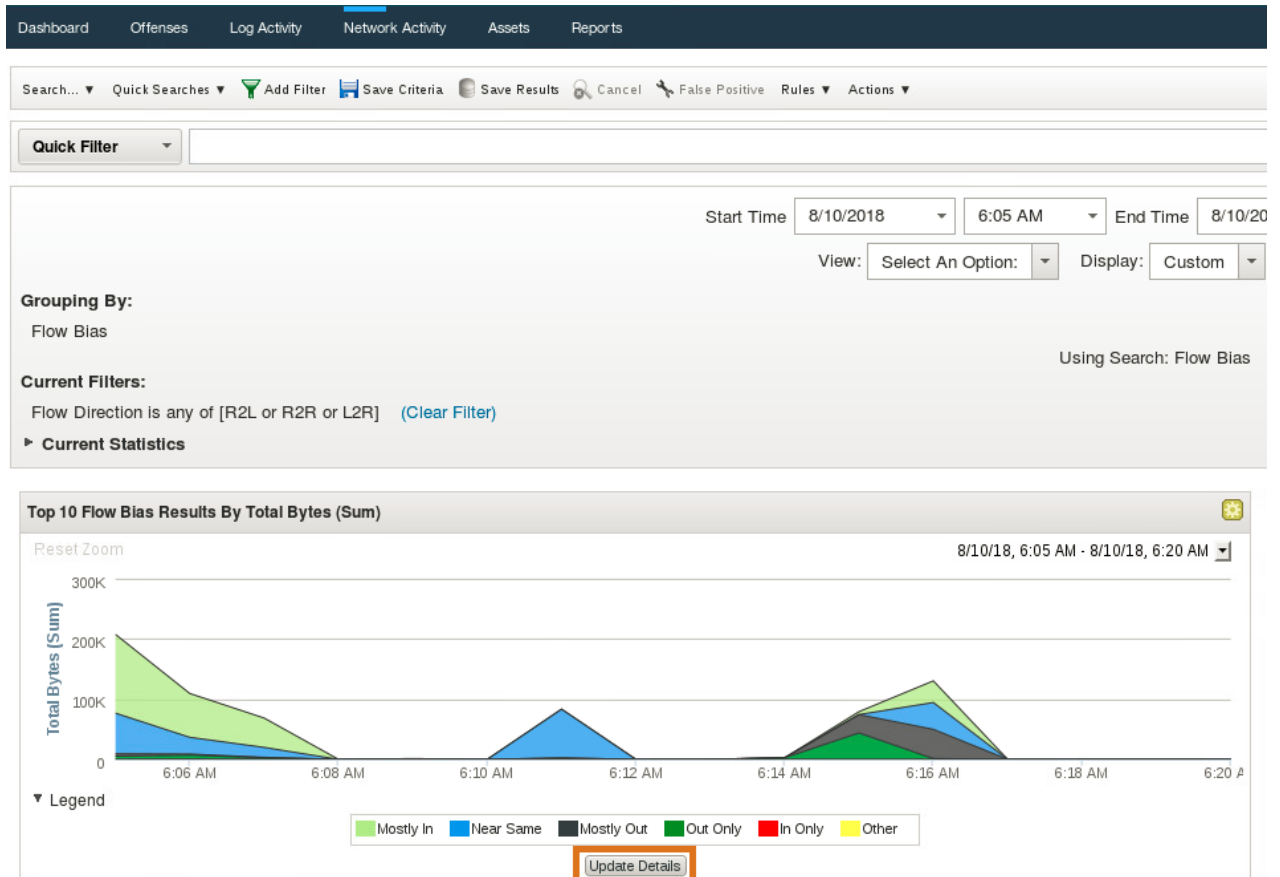
- To investigate the flows further on the **Network Activity** tab of the QRadar SIEM web interface, click the **View in Network Activity** link at the bottom.



- The **Network Activity** tab opens on the main window with the result of the search query that produces the Flow Bias dashboard item.
- Close the Flow Bias window.
- Scroll down and review the graphs in the main QRadar Console window.



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



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

12. In the beginning of the lab, the Dashboard did not display much data. As time progresses, the QRadar receives more data. To observe the new data, perform the following steps:
  - a. Navigate to the **Dashboard** tab.
  - b. Select the **Threat and Security Monitoring** dashboard.
  - c. Because the refresh of the **Dashboard** tab is paused, press the **Play** button in the upper-right corner of the toolbar.



## Exercise 4 Investigating a remote access offense

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

QRadar SIEM comes with pre-configured 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.



**Note:** 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, navigate to the **Offenses** tab.
2. Double-click the offense number 11 with the description of **Remote Desktop Access from the Internet containing RemoteAccess.MSTerminal Services** to open the offense summary.

Dashboard Offenses Log Activity Network Activity Assets Reports

Offenses

Search... Save Criteria Actions Print

My Offenses

**All Offenses**

By Category

By Source IP

By Destination IP

By Network

Rules



Current Search Parameters:

Exclude Hidden Offenses (Clear Filter) Exclude Closed Offenses (Clear Filter)

	Id	Description
	1	Multiple Exploit/Malware Types Targeting a Single Destination preceded by Exploit Follow...
	2	Worm Events Detected containing Slapper Worm
	8	Login Failures Followed By Success from the same Username preceded by Multiple Login ...
	3	VOIP:MGMT:XPRESSA-HTTP-DOS
	4	Multiple Exploit/Malware Types Targeting a Single Destination containing Web Exploit
	9	Multiple Login Failures for the Same User containing An authentication attempt was unsuc...
	7	Multiple Login Failures for the Same User preceded by Login Failures Followed By Succes...
	6	Multiple Login Failures for the Same User containing An authentication attempt was unsuc...
	5	Multiple Login Failures for the Same User preceded by Login Failures Followed By Succes...
	10	IRC Connections containing Firewall Permit
	12	Client Based DNS Activity to the Internet containing Misc.domain
	11	Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices

3.

4. Double-clicking an offense opens the **offense summary**. It displays and links to a wide range of evidence that is helpful for investigating the suspected attack or policy violation.

All Offenses > Offense 11 (Summary)	
Offense 11	
Magnitude	
Description	Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices
Source IP(s)	 <a href="#">9.9.8.42</a>
Destination IP(s)	<a href="#">192.168.10.12</a> (192.168.10.12)
Network(s)	<a href="#">Net-10-172-192.Net</a> 192_168_0_0

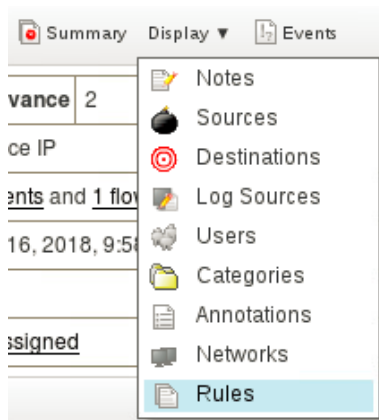
The **Magnitude** specifies the relative importance of the offense.



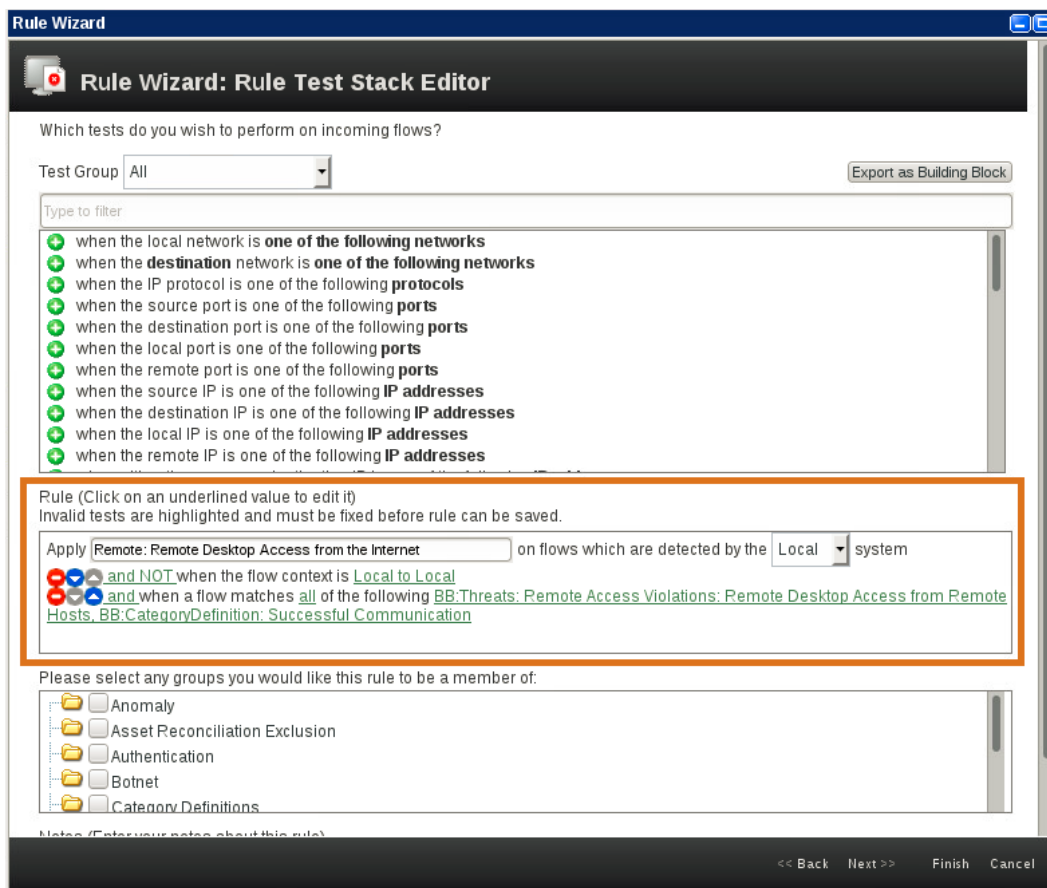
**Note:** Scroll down to explore which kinds of information the offense summary provides. Afterwards, scroll up to the top of the offense summary.

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

5. To view the rule(s) contributing to this offense, select **Rules** from the **Display** drop-down menu.



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



7. The tests evaluated by this rule are displayed in the middle section of the window. The first test is if the flows are detected by the local system.



**Note:** Within the rule, all green hyper links represent variables that can be selected 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?

---

8. 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.
9. Click it again to revert back to **and NOT**.
10. 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.

11. 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.

What are the two selected building blocks for this variable in the bottom 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.

12. Click **Next** on the Rule Wizard.
13. On 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.

14. On 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?

---

15. Click **Next**.

16. Review all the information specified on the previous sections of the Rule Wizard. Click **Cancel** to avoid saving any inadvertent changes you may have done to the rule.

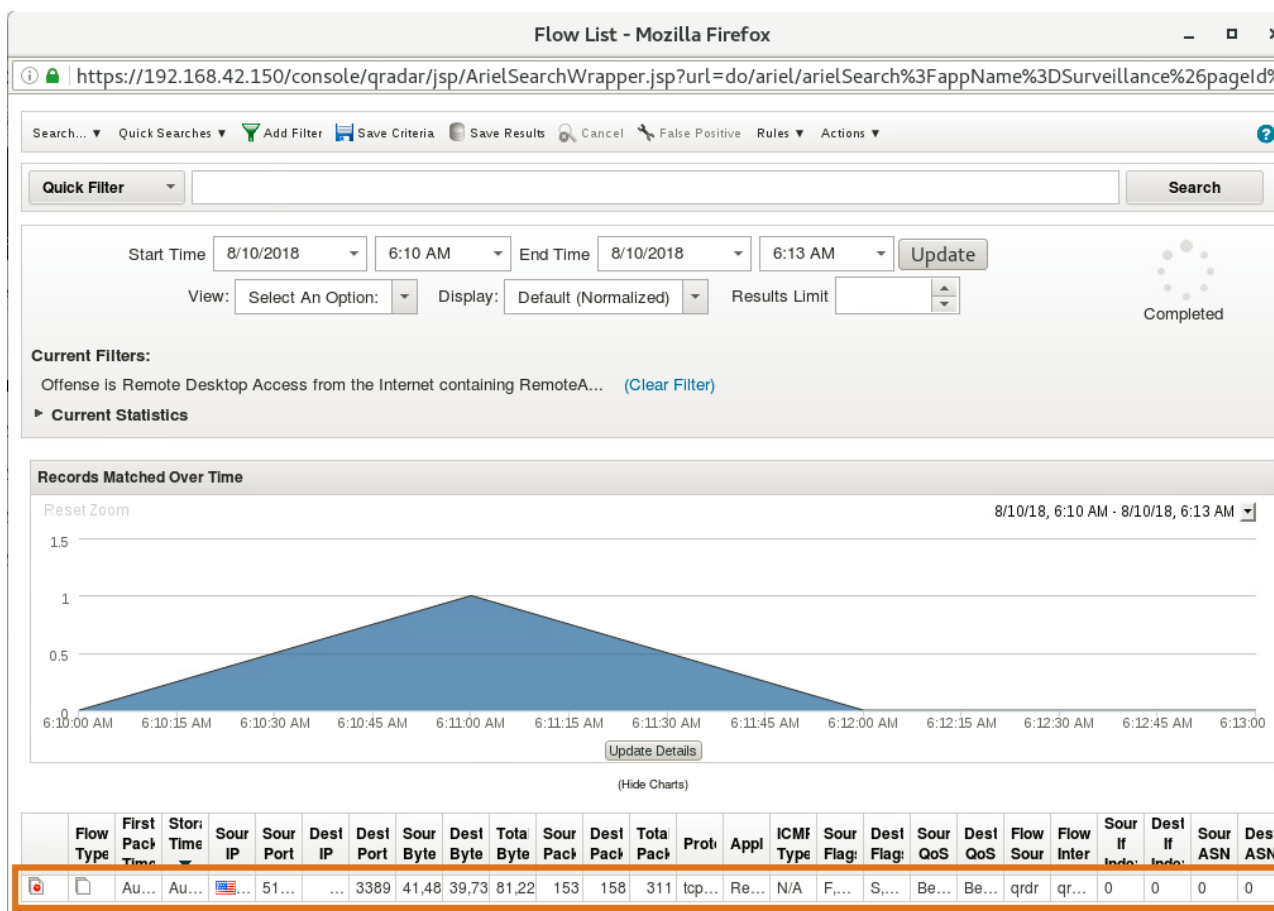


**Important:** Modifying the rule can have an unexpected behavior on the triggering of offenses. Do this with caution.

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

Status		Relevance	2	Severity
Offense Type	Source IP			
Event/Flow count	1 events and 1 flows in 2 categories			
Start	Aug 10, 2018, 6:11:07 AM			
Duration	24s			
Assigned to	Unassigned			

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



19. If you want to investigate the flow further, double-click the flow in the table to navigate to the Flow Details window.

20. When you are finished with your flow details investigation, click **Return To Results** in the upper-left corner of the Flow Details window. This brings you back to the Flow List window.

Return To Results

Offense

Extract Property

False Positive

Previous

Next

Print

File

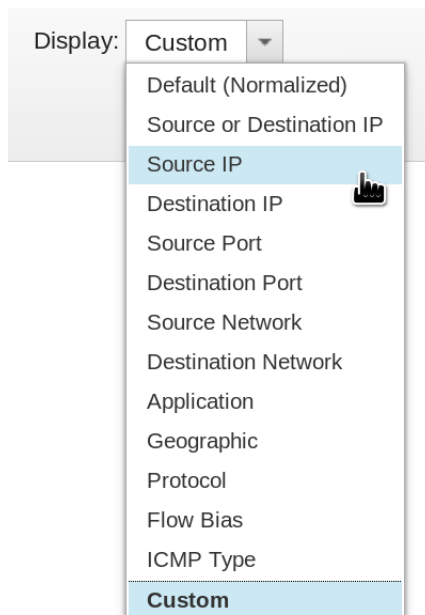
Return To Results

Protocol	tcp_ip			Application	RemoteAccess.MSTerminalServices		
Magnitude	<div> <div></div> <div></div> <div></div> </div> (3)			Relevance	3		Severity
First Packet Time	Aug 10, 2018, 6:10:31 AM			Last Packet Time	Aug 10, 2018, 6:10:39 AM		Storage Time
Event Name	RemoteAccess.MSTerminalServices						
Low Level Category	Remote Access						
Application Determination Algorithm	QRadar port based mapping (4)						

## Exercise 5 Creating a search for RDP connections to your server

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

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



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

Source IP	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Application (Unique Count)
9.9.8.42	other	192.168.10.12	3389	Net_192_168_0_0	RemoteAccess.MSTerminalServices

Filter on Destination IP is 192.168.10.12

Filter on Destination IP is not 192.168.10.12

Filter on Source or Destination IP is 192.168.10.12

Quick Filter...

More Options...

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**.



**Grouping By:**  
Source IP

**Original Filters:**  
Offense is Remote Desktop Access from the Internet containing RemoteA... [\(Clear Filter\)](#)

**Current Filters:**  
Destination IP is 192.168.10.12 [\(Clear Filter\)](#)

► **Current Statistics**

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

Search... ▾ Quick Searches ▾ Add Filter  Save Results  False Positive Rules ▾ Actions ▾

Quick Filter ▾  Save the criteria for the current search

5. Provide the following criteria in the **Save Criteria** fields and click **OK**.

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



**Save Criteria**

Please enter the name of this search below.

Search Name:

Assign Search to Group(s) [Manage Groups](#)

- ☐ Compliance
- ☐ Network Monitoring and Management
- ☐ Security (Malware, Exploit and other Risks)
- ☒ Usage Monitoring

Timespan options:

☐ Last Interval (auto refresh)
 ☒ Recent Last 24 Hours
☐ Specific Interval

Start Time:

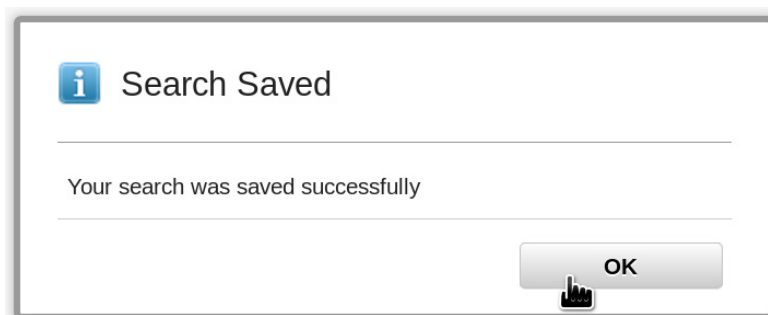
End Time:

☒ Include in my Quick Searches
 ☐ Set as Default

☐ Share With Everyone
 ☒ Include in my Dashboard

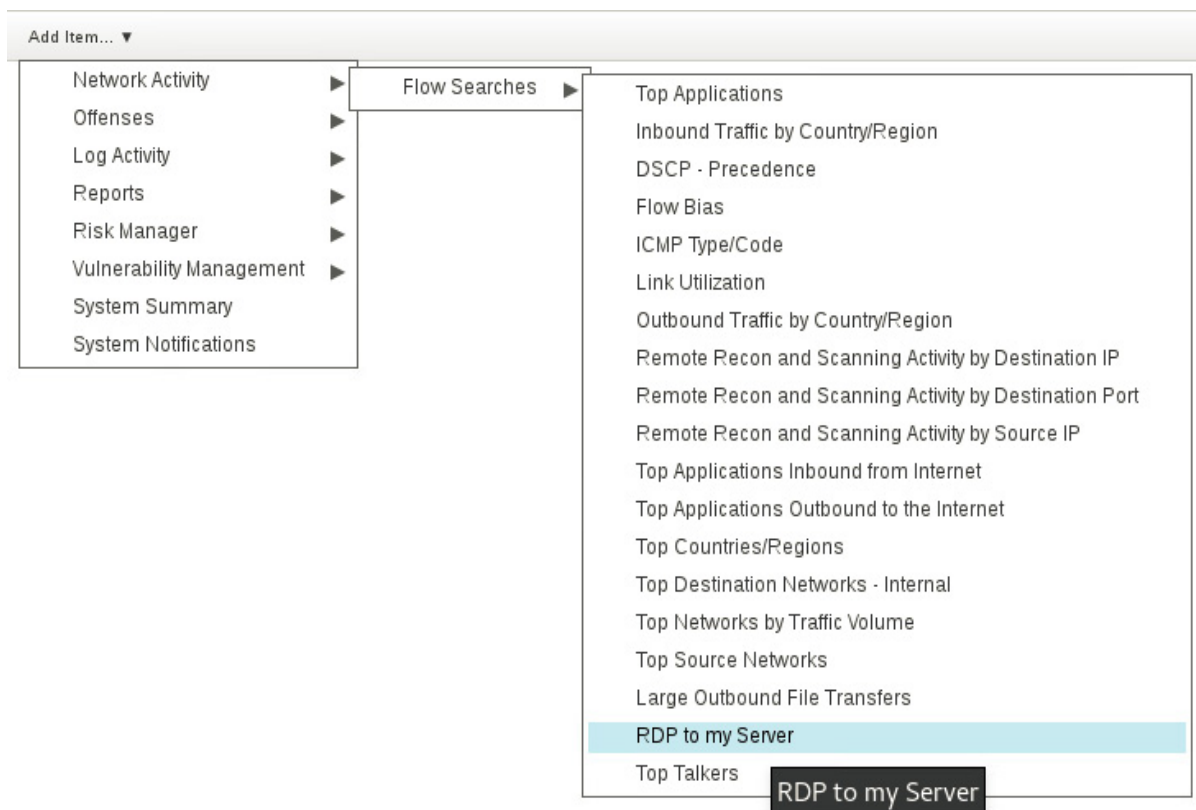
**OK** **Cancel**

- In the Search Saved pop-up window, click **OK** again.



- Close the Flow List window.
- 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.
- 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**.

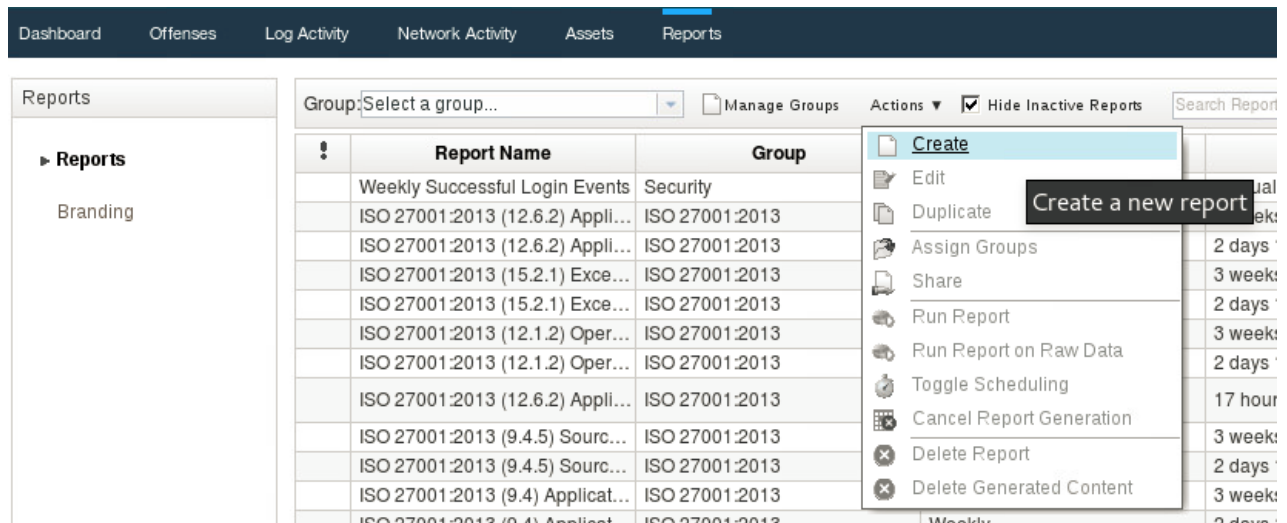


11. Scroll to the bottom of the Dashboard and confirm that the item is added at the bottom of the dashboard.

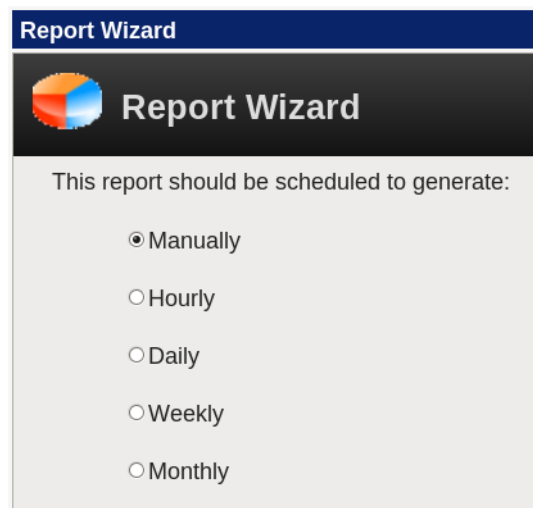
## Exercise 6 Creating a remote access report template

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 **Create** from the **Actions** menu.



2. Click **Next**. QRadar SIEM allows you to 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 would not include the flow that you received earlier. To include the latest flows, leave **Manually** selected as the schedule for the report generation. In a later step, you specify the time frame for the report.





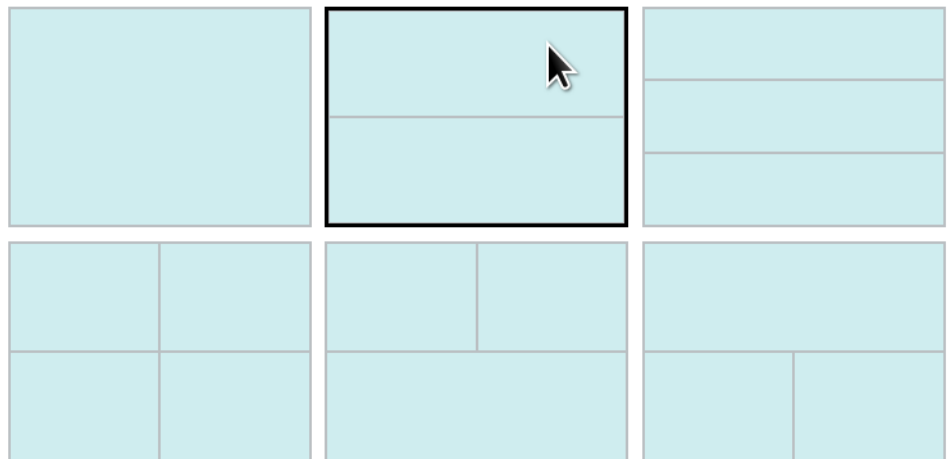
**Note:** A QRadar SIEM report template is a means of scheduling and automating one or more saved searches.

3. Click **Next**.
4. For the report layout, select the double-container layout as is shown in the following image and click **Next**.

Choose a Layout

Each divided section holds one chart. Click the layout that represents the size and number of charts required.

Orientation: Landscape ▾



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

6. For the **Chart Type** of the upper container, select **Flows**.

Specify Report Contents

Enter a report title and choose a logo. Select a chart type and click 'Define' for each chart you wish to configure. Configured charts become highlighted. Click Next.

The screenshot shows the 'Specify Report Contents' window. At the top, there are two input fields: 'Report Title:' with the value 'RDP to my Server' and 'Logo:' with the value 'default.png'. Below these is a large dashed rectangular area representing the report content. In the center of this area, a 'Chart Type:' dropdown menu is open. The menu lists the following options: 'None', 'None', 'Asset Vulnerabilities', 'Assets', 'Events/Logs', 'Flows' (which is highlighted with a blue background and a mouse cursor), 'Log Sources', 'Offenses Over Time', 'Top Destination IPs', 'Top Offenses', 'Top Source IPs', 'Vulnerabilities', and 'Vulnerability Compliance'. Below the list of options is a button labeled 'Define'.

7. The Report Wizard automatically displays the Container Details. Complete the following steps:

- For **Chart Title**, enter `Chart`.
- For **Start Date** and **Time**, and **End Date** and **Time**, select a time frame that includes the time when you captured the flow. In this case, leave default values.
- Scroll down.
- To find and select the search that you created in the previous exercise, into the **Type Saved Search**, enter `rdp` and press Enter.

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

The screenshot shows the 'Report Wizard' dialog box with the following sections:

- Container Details - Flows**: This report displays collected the flow data.
  - Chart Title:
  - Chart Sub-Title: ☒ Automatically Specified
- Manual Scheduling**:
  - Graph data from the following time span
    - Start Date:  Start Time:
    - End Date:  End Time:
  - Timezone:
  - ☐ Targeted Data Selection
- Graph Content**:
  - Saved Searches**: Group:
  - Type Saved Search or Select from List:
  - Available Saved Searches:
    - RDP to my Server** (highlighted)
- 
- 

- f. To finish, click **Save Container Details**.
8. The Report Wizard displays the page to specify the chart type again.

9. In the lower container, for the **Chart Type**, select **Flows**.

Specify Report Contents

Enter a report title and choose a logo. Select a chart type and click 'Define' for each chart you wish to configure. Configured charts become highlighted. Click Next.

Report Title:

Logo:

**Chart Type:**

Flows

**Define**

**Chart Type:**

- None
- None
- Asset Vulnerabilities
- Assets
- Events/Logs
- Flows**
- Log Sources
- Offenses Over Time
- Top Destination IPs
- Top Offenses
- Top Source IPs
- Vulnerabilities
- Vulnerability Compliance

Pagination Options:

Report Classification:

10. 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**.
- For **Chart Title**, enter *Details*.
  - For **Start Date** and **Time**, and **End Date** and **Time**, leave default values.
  - To find and select the search that you created in the previous exercise, into the **Type Saved Search** enter `rdp` and press Enter.

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

**Container Details - Flows**  
*This report displays collected the flow data.*

Chart Title:

Chart Sub-Title: ☒ Automatically Specified

**Manual Scheduling**

Graph data from the following time span

Start Date:  Start Time:

End Date:  End Time:

Timezone:

☐ Targeted Data Selection

**Graph Content**

**Saved Searches** Group:

Type Saved Search or Select from List

Available Saved Searches

**RDP to my Server**

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

**Additional Details**

Graph Type:

Limit Flows to Top: ☐

☐ Enable column widths based on search settings

**Response Details**

☐ Generate Offense

On each scheduled run

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



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

Choose the report format

- ☒ **PDF**  
An easily printable and transferable document
- ☐ **HTML**  
Useful displaying reports on the web in your browser
- ☐ **RTF**  
Report data in Rich Text Format

The following formats are available for single table templates only

- ☐ **XML**  
Extensible Markup Language
- ☐ **XLS**  
Excel

12. 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**.

- c. Scroll down and confirm that **Yes - Run this report when the wizard is complete** is selected.

#### Finishing Up

You're almost finished creating your report.

#### Report Description:

Monitor RDP to my Server

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

- ☐ Compliance
- ☐ Configuration and Change Management
- ☐ Executive
- ☐ Network Management
- ☐ Security
- ☒ Usage Monitoring
- ☐ Vulnerability Management
  - ☐ CIS Benchmark Reports
  - ☐ Scan Reports

#### Execute Report

Would you like to run the report now?

☒ Yes - Run this report when the wizard is complete


13. Click **Next** again.

14. Click **Finish**.

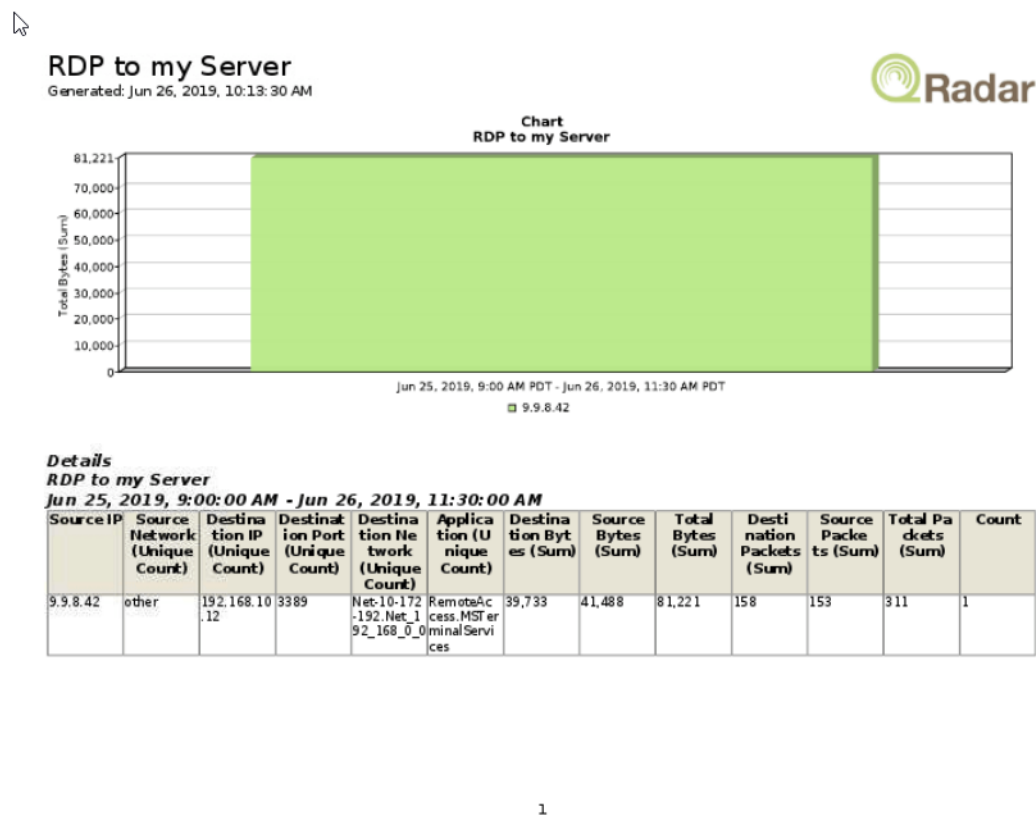
15. In the **Search Reports** field, type **RDP** and click the **Search Reports** icon to filter the report list. QRadar SIEM starts to generate the report. This takes about one minute in the real environment to complete the report.

16. When finished, QRadar SIEM displays a **PDF** icon for the new report template in the right-most column on the **Reports** tab. To view the generated report, click the **PDF** icon.

Group: Reporting Groups Manage Groups Actions ☒ Hide Inactive Reports rdp View the IBM App Exchange for more...

Report Name	Group	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports
RDP to my Server	Usage Monitoring	Manual	Manual	Aug 10, 2018, 9:16 AM	admin	admin	Aug 10, 2018, 9:17 AM 

The report is displayed.



1

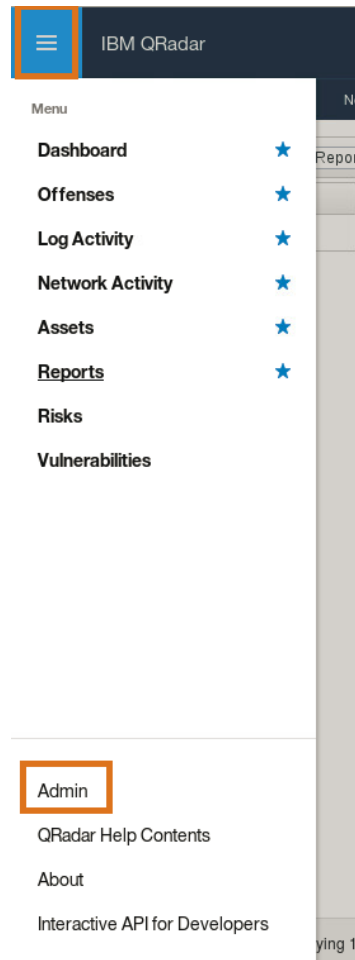
17. Close the report tab and return into the main QRadar console screen.

## Exercise 7 Configuring the network hierarchy

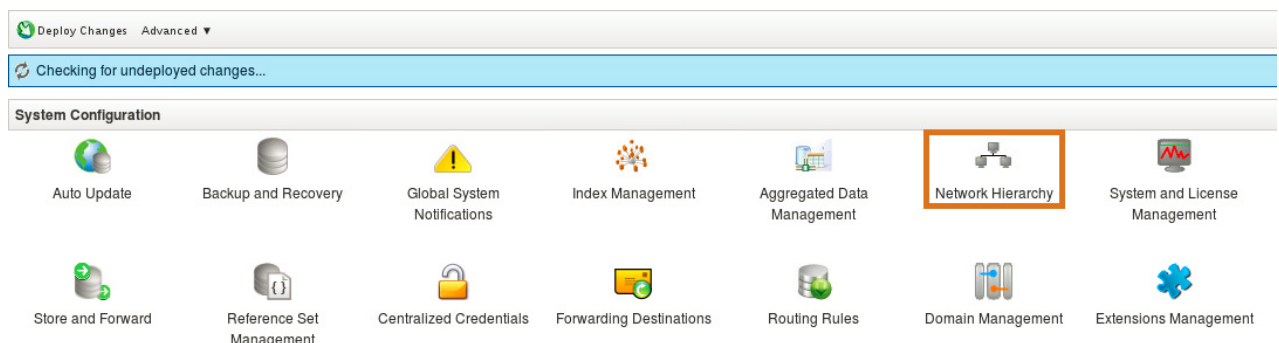
You have confirmed that the source IP address of the RDP connection belongs to your organization. QRadar SIEM created an offense because it considered the source IP address a remote address. Therefore, you need to add the IP address to the network hierarchy of QRadar

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:

1. To open the Network Hierarchy window, navigate to the **Admin** menu by clicking the three bars icon on the top left of the screen and clicking **Admin** on the bottom.



2. Click the **Network Hierarchy** icon in the System Configuration section.



The Network Hierarchy window opens

3. To create a new network object, perform the following steps:
  - a. Click the **Add** button.


The Add Network window opens.



- b. For **Name**, enter Europe.

Default Domain

### Add Network

Name:

Group:  

IP/CIDR(s):   

Description:

Country:

Longitude:  Latitude:

- c. To create a new network group object, click the yellow icon on the right.  
The Add a new group window opens.

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

The screenshot shows the 'Add Network' form. The 'Name' field contains 'Europe'. The 'Group' field is highlighted with a red box. A modal window titled 'Add a new group' is open in the foreground, with the 'Name' field containing 'Jumpbox.Support'. The modal has 'Save' and 'Cancel' buttons. The background form also shows 'IP/CIDR(s)', 'Description', and 'Country' fields.

- e. Click the **Save** button.  
The Add a new group window closes.
- f. For **IP/CIDR(s)**, enter `9.9.8.42`.

The screenshot shows the 'Add Network' form. The 'Name' field contains 'Europe'. The 'Group' field now shows 'Jumpbox.Support' as the selected option. The 'IP/CIDR(s)' field contains '9.9.8.42/32'. The form also shows 'Description' and 'Country' fields.

- g. Click the green plus button.

h. Click the **Create** button.

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 shown in the following table.

Name	Group	IP/CIDR(s)
Asia	Jumpbox.Support	9.9.6.0/24 9.9.7.0/24

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.

**Add Network**

Name: Asia

Group: Jumpbox.Support

IP/CIDR(s): 9.9.7.0/24  
9.9.6.0/24

Description:

Country: Select Country...

Longitude: Latitude:

Create Cancel

5. To close the window, click **Create**.

6. To display the network objects that you created, click the plus buttons next to **Jumpbox** and **Support** in the Network Hierarchy window.

Name	IP/CIDR
DMZ	
Jumpbox	
Support	
Asia	9.9.6.0/24 9.9.7.0/24
Europe	9.9.8.42/32
NAT_Ranges	
Net-10-172-192	
Net_10_0_0_0	10.0.0.0/8
Net_172_16_0_0	172.16.0.0/12
Net_192_168_0_0	192.168.0.0/16

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



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

Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports

Admin

Deploy Changes
Advanced ▼

There are undeployed changes. Click 'Deploy Changes' to deploy them. [View Details](#)

System Configuration

- User Management
- Assets





**Note:** QRadar SIEM considers all networks 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 8 Closing the offense

Assume that the RDP connection was legitimate and you have updated the network hierarchy accordingly. Follow these steps to close the offense:

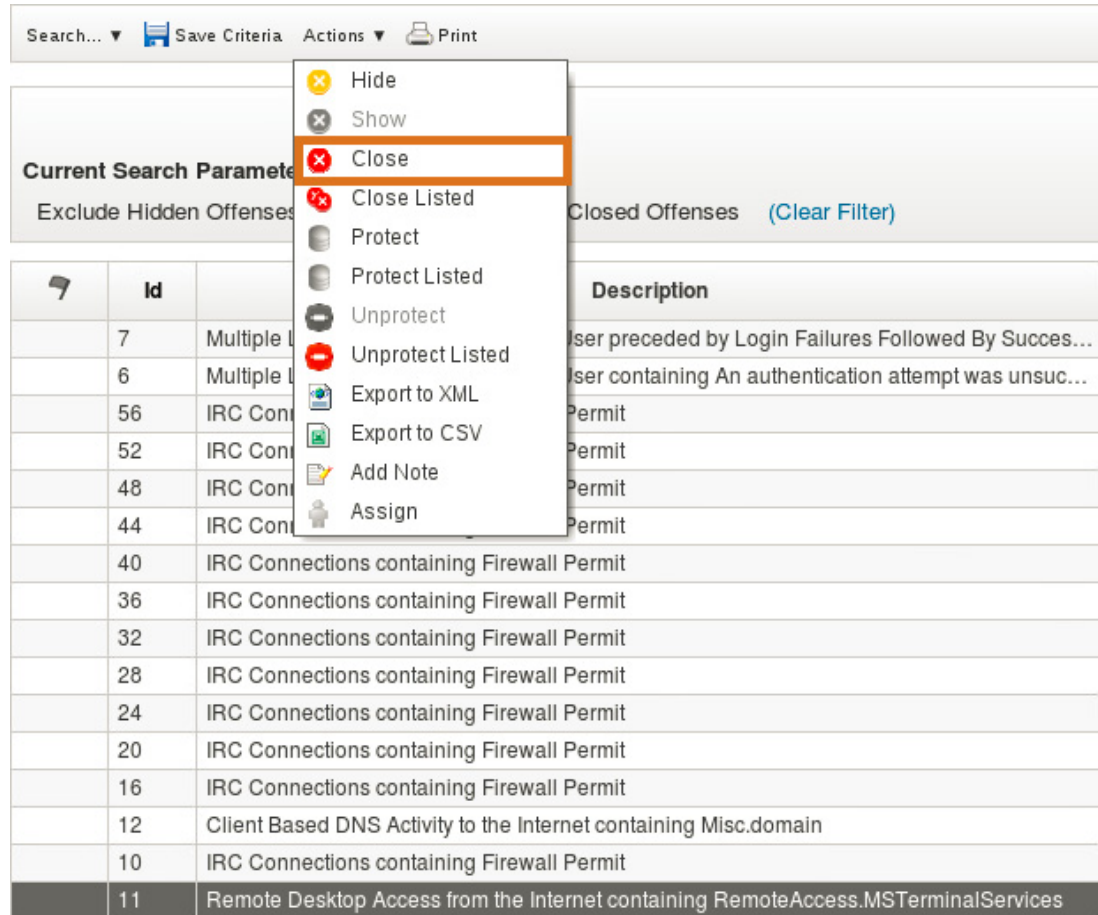
1. Double-click the **Offenses** tab.



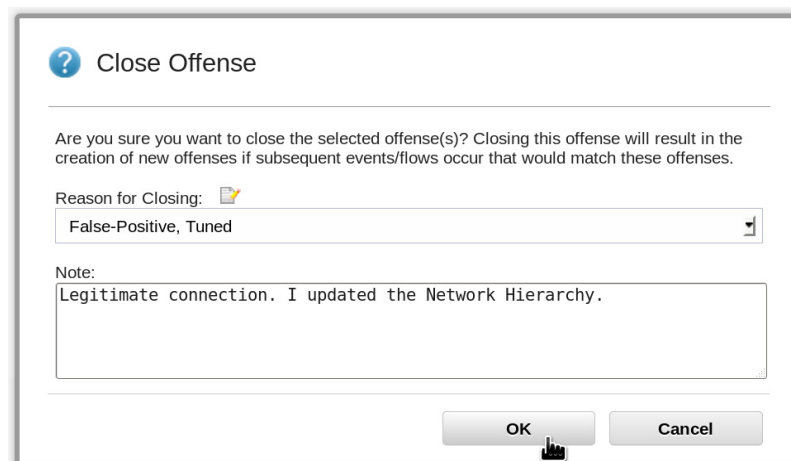
**Hint:** Double-clicking resets the tab to its default settings.

2. Select the offense number 11 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.

## Exercise 9 Navigating through other tabs

Follow these steps to explore QRadar SIEM further:

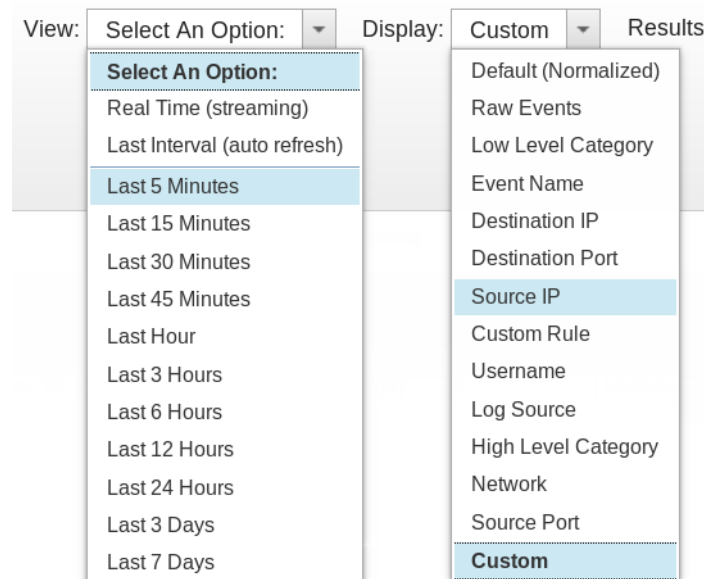
1. QRadar SIEM automatically creates asset profiles for your local machines. If the source or destination IP address of a flow or event falls into one of the networks configured in the network hierarchy, QRadar SIEM creates an asset profile.

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

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

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

You can view events flows from different perspectives. Select options from the **View** and **Display** menus, and check the results.



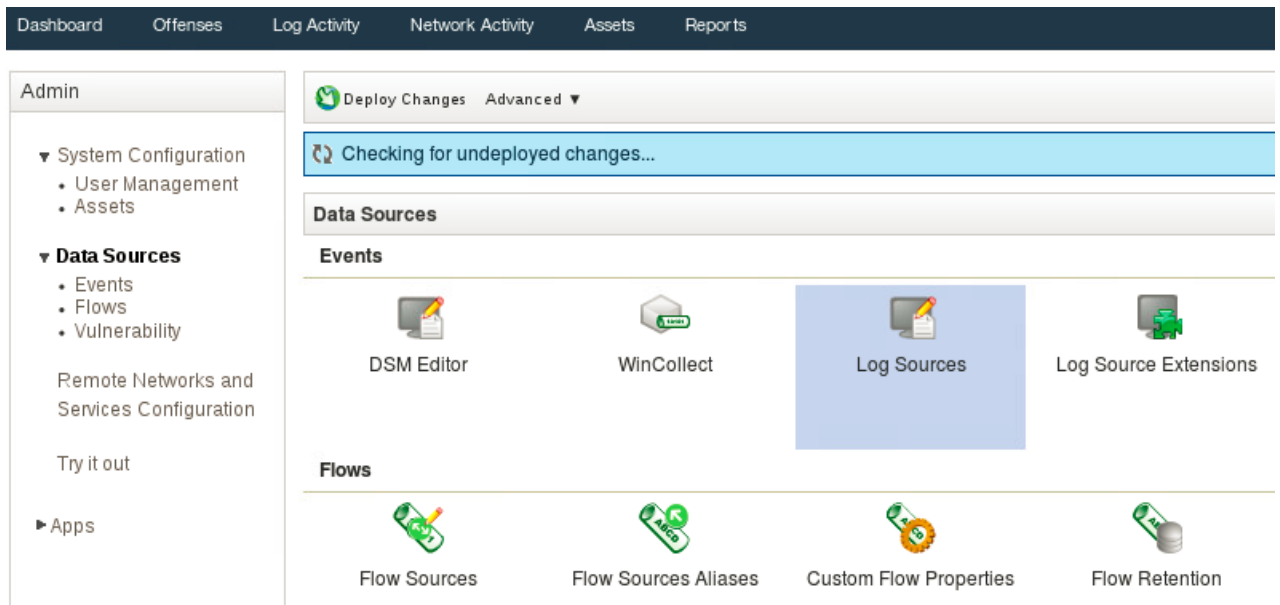
QRadar SIEM groups the flows by your selection in the Display list. In this example, grouping by **Source IP** displays a column of all the unique source IPs and summary information of the other columns, such as the number of unique destination ports for each source IP.



**Note:** A red icon in the left-most 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 red icon.

4. 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. Navigate to the **Admin** menu and then click the **Log Sources** icon to open the Log Sources window.



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.

Search For: Group All Log Source Groups Go Add Edit Enable/Disable Delete Bulk Actions Extensions Pasing Order ?														
Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Destinat	Credibility	Autodisc	Last Event Time	Creation Date	Modificati Date	Average EPS (Last Minute)
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
ASA @ ...	ASA de...	Success	Syslog		Cisco A...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Check P...	Check P...	Success	Syslog		Check P...	True	accept	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	4
Check P...	Check P...	Success	Syslog		Check P...	True	authcrypt	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Check P...	Check P...	Success	Syslog		Check P...	True	drop	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	5
Check P...	Check P...	Success	Syslog		Check P...	True	keyinst	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
Endpoint...	Endpoint...	Success	Syslog		Symant...	True	10.0.109.8	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
IBM i @ ...	IBM i De...	Success	Syslog		IBM i	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	1
IBM i @ ...	IBM i De...	Success	Syslog		IBM i	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A
IBM i @ ...	IBM i De...	Success	Syslog		IBM i	True	10.0.10...	eventcol...	5	True	Aug 10, ...	Aug 10, ...	Aug 10, ...	N/A

5. Close the Log Sources window.

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



# IBM Training

