```
WEBVTT
Kind: captions
Language: en-US

00:00:03.975 --> 00:00:06.453
This course is an overview of some of the ways to keep

00:00:06.453 --> 00:00:08.467
the QRadar network hierarchy updated.

00:00:11.563 --> 00:00:14.554
 Update the network hierarchy whenever you make changes that

00:00:14.554 --> 00:00:16.500
QRadar can properly monitor all activities.

00:00:17.231 --> 00:00:20.462
One method for updating your network hierarchy is to use Infoblox,

00:00:20.462 --> 00:00:24.718
or another network management utility that uses the QRadar Restful
API.

00:00:25.071 --> 00:00:28.190
Find information about the QRadar Restful API at this link.

00:00:28.754 --> 00:00:32.238
Also, API information specific to the network hierarchy is available

00:00:32.238 --> 00:00:35.434
in the Interactive API Documentation for Developers.

00:00:35.753 --> 00:00:38.816
View the Interactive Documentation by using this URL:
https://ConsoleIPaddress/api_doc/.

00:00:40.000 --> 00:00:42.352
First, confirm that you are looking at the latest version.

00:00:43.907 --> 00:00:45.192
Expand /config.

00:00:45.904 --> 00:00:47.541
And then expand network_hierarchy.

00:00:48.216 --> 00:00:50.852
Click staged_networks to view API information that is

00:00:50.852 --> 00:00:52.852
specific to updating the network hierarchy.
```

```
00:01:00.767 --> 00:01:03.789
Another method for keeping the network hierarchy up to date is to look for

00:01:03.789 --> 00:01:05.296
remote-to-remote (R2R) traffic.

00:01:06.191 --> 00:01:09.102
Typically, one side of the communication in QRadar events and flows is

00:01:09.102 --> 00:01:10.595
from your environment.

00:01:11.203 --> 00:01:13.846
Remote-to-remote traffic can indicate that the network hierarchy is

00:01:13.846 --> 00:01:14.877
missing a subnet.

00:01:16.128 --> 00:01:18.613
To find remote-to-remote flows, create a search

00:01:18.613 --> 00:01:19.952
and include a column for Flow direction.

00:01:27.727 --> 00:01:29.483
Now that you displayed remote-to-remote flows,

00:01:29.483 --> 00:01:32.669
open the Use Case Manager to view remote-to-remote events.

00:01:33.249 --> 00:01:35.262
In the Use Case Manager app, open the

00:01:35.262 --> 00:01:38.033
tuning interface and display remote-to-remote events.

00:01:45.781 --> 00:01:47.713
Another search that can identify an outdated

00:01:47.713 --> 00:01:50.526
network hierarchy is to filter on unknown networks.

00:01:50.802 --> 00:01:57.302
Other is a hidden network hierarchy address that uses 0.0.0.0/0 as the

00:01:57.302 --> 00:02:00.726
CIDR range to find all addresses that are undefined in a network.
```

00:02:01.344 --> 00:02:04.653
Normally, the source or the destination belongs to a defined network node.

00:02:05.488 --> 00:02:07.680
Filter Source Network equals other.

00:02:15.646 --> 00:02:17.761
And then filter Destination Network equals other.

00:02:25.139 --> 00:02:28.989
If both source and destination are displayed as other, it can indicate that

00:02:28.989 --> 00:02:31.703
either the source or destination IP address belongs to

00:02:31.703 --> 00:02:35.918
a CIDR that is part of your network, but is not defined in the network hierarchy.

00:02:36.762 --> 00:02:39.047
Another method to keep a network hierarchy up to date

00:02:39.047 --> 00:02:43.281
is to notify QRadar administrators as part of the change management process

00:02:43.499 --> 00:02:46.751
so that administrators can reconfigure QRadar as you make changes.

00:02:47.549 --> 00:02:49.077
Thank you for your time and attention.

00:02:49.476 --> 00:02:53.200
Please refer to the IBM Security Learning Academy for more training resources.