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

00:00:03.720 --> 00:00:06.465
This course is an overview of the QRadar network hierarchy.

00:00:06.874 --> 00:00:09.635
The network hierarchy, which is located on the Admin Console,

00:00:09.920 --> 00:00:12.291
is where you define the CIDR ranges that make up your network.

00:00:12.880 --> 00:00:15.670
You do this, so that QRadar can distinguish what is part of your
network,

00:00:15.670 --> 00:00:16.987
also known as local,

00:00:17.149 --> 00:00:19.915
and what is not part of your network, also known as remote.

00:00:22.558 --> 00:00:24.596
The network hierarchy allows administrators to segment

00:00:24.596 --> 00:00:26.632
their network into logical groups.

00:00:28.504 --> 00:00:31.974
Each network object contains one or more CIDR ranges, or IP addresses.

00:00:33.488 --> 00:00:36.648
A CIDR can belong to only one network object per domain.

00:00:38.027 --> 00:00:42.000
However, some sets of CIDR ranges can belong to multiple network
objects.

00:00:42.244 --> 00:00:48.484
For example, the CIDR range 102.0.0.0/8 can exist in only

00:00:48.484 --> 00:00:50.000
one network object per domain.

00:00:50.517 --> 00:00:55.951
However, the CIDR 192.0.0.0/16 can exist in another

00:00:55.989 --> 00:00:58.218
network object on the same domain.
```

```
00:00:58.526 --> 00:01:03.314
The same is true
of 192.0.2.0/24.

00:01:03.723 --> 00:01:07.604
Network traffic matches the most precise CIDR range where a singular
IP address

00:01:07.604 --> 00:01:08.940
is the most precise option.

00:01:09.372 --> 00:01:12.177
In QRadar, many default building blocks and rules use

00:01:12.177 --> 00:01:14.807
the default network hierarchy groups and objects.

00:01:14.940 --> 00:01:18.000
Before you can remove or restructure any of the default network
hierarchy

00:01:18.000 --> 00:01:21.792
 groups or objects, search the rules and building blocks to understand

00:01:21.792 --> 00:01:25.595
how QRadar uses the group or object, and which rules and building
blocks

00:01:25.595 --> 00:01:28.134
require adjustments after your modifications.

00:01:31.593 --> 00:01:37.260
The net-10-172-192 group is used to include commonly used private CIDR
ranges.

00:01:37.840 --> 00:01:40.906
Even if these private ranges do not currently exist within a network,

00:01:40.906 --> 00:01:44.162
they are used to find private ranges that were added to the network

00:01:44.162 --> 00:01:45.489
without the administrator's knowledge.

00:01:46.120 --> 00:01:51.210
The net-10-172-192 group can also be used to detect scan attempts
against

00:01:51.210 --> 00:01:53.696
```

these common, private, nonexistent CIDR ranges.

00:01:53.953 --> 00:01:55.953
To create a new entry within a network hierarchy,

00:01:55.993 --> 00:01:58.887
on the Admin Console, click the Network Hierarchy icon.

00:01:59.718 --> 00:02:01.852
To add a network object, click Add and then

00:02:01.852 --> 00:02:04.260
type a unique name and description for the object.

00:02:05.677 --> 00:02:08.338
From the Group list, select the group to which you want to add

00:02:08.338 --> 00:02:09.120
the network object.

00:02:10.116 --> 00:02:11.522
Or, to add a group,

00:02:11.522 --> 00:02:14.446
click the icon next to the group list and type the name for the group.

00:02:15.096 --> 00:02:18.331
Create subgroups by typing the name of the parent group, followed by

00:02:18.331 --> 00:02:20.489
a period and then the name of the subgroup.

00:02:20.860 --> 00:02:24.903
Create multiple layer subgroups by separating each subsequent subgroup with a period.

00:02:25.588 --> 00:02:29.668
Select the domain that the network object belongs to, and then click Save.

00:02:32.159 --> 00:02:36.200
Type a CIDR range or IP address for the network object and then click Add.

00:02:39.386 --> 00:02:43.633
Continue to add CIDR ranges and IP addresses for this object as required.

00:02:43.880 --> 00:02:46.664
After adding all CIDR ranges to the object, click Create.

00:02:49.260 --> 00:02:52.005
Repeat these steps for any other required network objects.

00:02:52.053 --> 00:02:55.404
Or click Edit or Delete to work with an existing network object.

00:02:55.661 --> 00:02:58.678
After you add network objects, or modify the network hierarchy,

00:02:58.678 --> 00:03:00.678
deploy changes on the Admin Console.

00:03:04.452 --> 00:03:06.159
Thank you for your time and attention.

00:03:06.340 --> 00:03:10.052
Please refer to the IBM Security Learning Academy for more training resources.