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

00:00:03.600 --> 00:00:06.859
In this course, you learn how to structure your&nbsp; network
hierarchy.

00:00:07.296 --> 00:00:10.000
When you develop a network&nbsp;&nbsp;hierarchy, consider the most
effective&nbsp;

00:00:10.000 --> 00:00:12.305
method for viewing your network activity.&nbsp;&nbsp;

00:00:13.117 --> 00:00:15.021
The network hierarchy does not need to resemble&nbsp;the

00:00:15.021 --> 00:00:16.232
physical deployment of your network.

00:00:16.560 --> 00:00:18.513
Instead, create groups within QRadar based&nbsp;on

00:00:18.513 --> 00:00:20.513
how you search and test the system.

00:00:21.107 --> 00:00:23.632
To view the network hierarchy, on the Admin&nbsp; Console,

00:00:23.632 --> 00:00:25.178
click the Network Hierarchy icon.

00:00:25.803 --> 00:00:29.113
Typically, administrators group the network&nbsp; hierarchy by using a
combination of

00:00:29.113 --> 00:00:32.270
system functions, business units,&nbsp;and geographic locations.

00:00:36.933 --> 00:00:40.440
Some administrators compare a business unit in&nbsp; one geographic
location

00:00:40.440 --> 00:00:43.174
against the business unit&nbsp;in another geographic location.

00:00:43.299 --> 00:00:46.882
For example,&nbsp; you might expect all Active Directory servers in
your Cincinnati
```

```
00:00:46.921 --> 00:00:50.652
finance department to&nbsp;exhibit similar behaviors and
patterns&nbsp;&nbsp;

00:00:50.652 --> 00:00:52.598
to those in your Belfast finance department.

00:00:53.629 --> 00:00:56.809
Defining the expected behaviors in network objects&nbsp;allows you to

00:00:56.809 --> 00:01:01.005
write rules to detect deviations&nbsp;from one another and take
specific actions.

00:01:01.553 --> 00:01:04.742
Some administrators write rules to take actions&nbsp;when there is

00:01:04.742 --> 00:01:08.132
communication between network object&nbsp;&nbsp;A and B outside of a
certain hour.

00:01:08.812 --> 00:01:11.569
So, network&nbsp; objects need to be properly defined and grouped

00:01:11.569 --> 00:01:13.327
based on how you plan to use them.

00:01:13.772 --> 00:01:16.643
Consider&nbsp;the following guidelines when you define
your&nbsp;network hierarchy:

00:01:17.033 --> 00:01:20.392
Include both the private and&nbsp;public CIDR ranges that make up your
network.&nbsp;

00:01:20.498 --> 00:01:23.705
Name network groups and objects to describe&nbsp;exactly what they
represent.

00:01:24.412 --> 00:01:28.136
Define&nbsp;all-encompassing groups so that the appropriate&nbsp;
behavior monitors are

00:01:28.136 --> 00:01:30.434
applied to all subgroups and&nbsp;network objects.

00:01:30.504 --> 00:01:34.160
If specific security policies&nbsp;are required, be as precise as
possible.
```

```
00:01:34.480 --> 00:01:36.385
The more&nbsp;precise you are with your network hierarchy,&nbsp;the
more

00:01:36.385 --> 00:01:40.687
easily you can write rules, searches,&nbsp;and reports for specific
network objects.

00:01:40.827 --> 00:01:44.584
However, adding detail also increases the&nbsp;&nbsp;amount of
maintenance required

00:01:44.584 --> 00:01:46.982
to keep the&nbsp;list up to date with changes.

00:01:47.061 --> 00:01:51.222
For example, if you&nbsp;&nbsp;have a network object for mail servers
with a list&nbsp; of specific &nbsp;

00:01:51.222 --> 00:01:55.624
IP addresses defined instead of CIDR ranges, each time a network mail
server is

00:01:55.624 --> 00:01:58.369
edited&nbsp;or added, you must update the network hierarchy.

00:02:00.305 --> 00:02:02.146
Thank you for your time and attention.

00:02:02.295 --> 00:02:06.112
Please refer to the IBM Security Learning Academy for more training
resources.
```