Step 5: Containment

Objectives:

At the end of this episode, I will be able to:

Understand what incident containment is.

Explain what Step 5, Containment, of the IH&R process is.

Identify what key containment activities should be for the IH&R team.

Define what some of the common techniques used in the containment phase are.

External Resources:

Step 5 Containment

What is Incident Containment? -

The IH&R team plays a significant role in this stage by taking actions that
reduce a threat or incident’s magnitude or complexity to prevent further damage
to the organization.

Some of the key activities of an IH&R team in containing a security incident are:

```
▪ The IH&R team in partnership with the technical and management personnel
```

must create a containment strategy.

```
▪ The strategy should incorporate feedback from external sources if required.

▪ The IH&R team should validate the type of response(s) required to contain
```

the incident and then assigns the task(s) to the technical, management, or
legal teams as appropriate.

```
▪ Once the relevant team(s) have completed their assigned task(s), the IH&R
```

team must validate that containment was successful.

```
▪ If incident containment failed, then the IH&R team must escalate the
```

process, review and update the containment strategy, and engage with the
necessary resources to seek successful containment.

What are some of the common techniques used in the containment phase? -

```
▪ Disabling of systems
▪ Changing of passwords
▪ Locking/Disabling of accounts
▪ Create full backups of affected systems
▪ System restoration
```