Step 7: Eradication

Objectives:

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

Understand what eradication is.

Explain what Step 7, Eradication, of the IH&R process is.

Identify what the process flow for Eradication should be for the IH&R team.

Define the role that eradication plays for the IH&R team.

External Resources:

Step 7 Eradication

What is the Process Flow for Eradication? -

1. Perform a vulnerability analysis to determine if the network is still vulnerable to attacks.

2. If the root cause of the incident is still present/active, try to eliminate it, if elimination is not possible, escalate the incident to the appropriate department(s)/specialist(s) for further action.

3. If the root cause of the incident is no longer present/active, verify if the issue exists in other systems.

4. After identifying and eliminating any/all threats, updating/correcting the security posture of the affected infrastructure has to be performed.

5. Implement protection tools and techniques, such as firewalls, routers, and router filtering, to allow network security devices and applications to block the identified attack paths, as well as patching all identified vulnerabilities to prevent further exploitation.

6. If necessary, change externally visible network component addresses to remove an established attack path.

7. Perform an internal audit of all resources before initiating the recovery process (Step 8) in order to ensure recovery will be successful.