# Containment of Malware Incidents

## Objectives:

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

Understand what the main goal of containment of Malware Incidents should be for the IH&R team.

Explain what are the steps IH&R personnel should follow to contain malware incidents.

## External Resources:

Containment of Malware Incidents

Once a responder validates an incident as a malware incident, the IH&R team should focus on containing it after obtaining approval from concerned authorities.

The main intention of containment of malware is to prevent its further spread and minimize its impact to the organization.

What are the steps IH&R personnel should follow to contain malware incidents? -

▪ Separate the compromised host from the operational network

▪ Gather and analyze network logs of the system to find the events of malware propagation through shared files and connected systems

▪ In case the malware has compromised multiple systems, you must cut the network services of these systems and prioritize them according to the importance of the affected host for business continuity

▪ Use separate virtual local area networks (VLAN) for infected hosts to find the processes the malware employs to join the network when connected

▪ Allow the connections through an access control network or VPN for the non-compromised devices

▪ Analyze the compromised host to find malware signature, pattern, or behavior that you can use to contain the incident

▪ Disable the targeted services, applications, and systems until the exploited vulnerabilities are patched

▪ Block all unnecessary ports at the host and firewall

▪ Run host-based antivirus, firewall, and intrusion detection software

▪ Run registry monitoring tools to find malicious registry entries added by the backdoor

▪ Remove or uninstall the program or application installed by the backdoor Trojan or virus

▪ Remove the malicious registry entries added by the backdoor Trojan

▪ Delete malicious files related to the backdoor Trojan