Eradication of Malware Incidents

Objectives:

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

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

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

External Resources:

Eradication of Malware Incidents

Eradication of malware implies removing malware completely from infected hosts. However, it involves more than this, it also includes elimination of vulnerability in the host/network that caused the infection.

Eradication should also ensure that there are no further chances of similar infection.

What are some of the steps an incident responder should follow to eradicate malware security incidents? -

```
▪ Content Filtering Tools - Use the static characters of the malware, such as
```

strings and loaders, as filters to block the malware from entering systems

```
▪ Network Security Devices - Add the malware signature to the network security
```

devices such as firewalls and IDPSs to stop it from breaching the organization perimeter

```
▪ Blacklist - Block the harmful URLs, IP addresses, email-Ids, services,
```

programs, applications, and executables that install malware onto the system

```
▪ Antivirus Tools - Update the antivirus tools to detect the newly found
```

malware using signature, string, or heuristics-based techniques

```
▪ Manual Scan - Run a full scan of the compromised system with an updated
```

antivirus program to remove the malicious codes, binaries, and the related registry entries

```
▪ Usage Policy - Organizations must define malware prevention concerns while
```

defining policies such as acceptable usage policies; The organization should include the following:

```
    o Scan all types of media before connecting it to the internal systems
    o Scan all email attachments before opening
    o Restrict users from installing unknown programs
    o Prohibit the use of removable media devices


▪ Employee Awareness  - Organizations should make their employees aware of
```

best practices regarding malware such as:

```
    o Not opening suspicious emails or attachments or click hyperlinks
    o Not clicking on web browser pop-up windows
    o Not opening files with file extensions such as .bat, .com, .exe, .pif, .vbs
o Enabling security applications such as antivirus & content filtering
    o Not allowing unauthorized personnel to use administrator-level accounts
    o Not downloading or execute applications from third-party sources
```