Step 2: Incident Recording and Assignment

Objectives:

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

Understand what needs to be done to define Incident Escalation Procedures for employees.

Explain what Step 2, Incident Recording and Assignment, of the IH&R process is.

Identify what the role of IT Support and / or the Help Desk is as part of the IH&R process.

Define what a ticketing system is, and the advantages using one provides as part of the IH&R process.

External Resources:

Step 2: Incident Recording and Assignment

Define Incident Escalation Procedures for Employees -

The incident handling and response process should define a proper incident escalation plan or procedure.

The plan should:

```
▪ Allow victims, customers, clients, and other people to report an incident
easily

▪ Enable the incident handler to assign tasks to team members, verify the
process, and obtain reports about the progress

▪ Allow the incident responders to discuss the steps, communicate the response
```

results, and provide result data with proper evidence

```
▪ Communicate results and report to management and stakeholders
```

NOTE: The escalation plan depends on the organization type, size, and types of attacks it might face

Role of IT Support and / or the Help Desk -

IT support receives a call from users regarding issues with systems, network, applications, etc...

IT support will record the call and try to identify the issue using a questionnaire based on the type of incident

If IT support suspects the issues to be a security incident, then they will assign it to the IH&R team using a ticketing system

What is a Ticketing System?

Simplifies incident response and handling process by tracking details of incidents in a centralized location easily accessible by ALL IH&R team members

Organizations MUST USE the ticketing system to keep track of all the incident response activities

What are the Advantages of using ticketing systems?

```
▪ Can generate tickets automatically on discovering suspicious patterns from
```

firewall, IDS, and SIEM, etc…

```
▪ Systematically collects details about the incident

▪ Helps in assigning priority to incidents based on the compromised system,
type of incident, etc...

▪ Alerts the responsible person(s) and distributes tasks automatically

▪ Stores details of the incidents, solutions, and results
```