Step 3: Incident Triage

Objectives:

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

Understand what Incident Analysis and Validation is.

Explain what Step 3, Incident Triage, of the IH&R process is.

Identify what Incident Classification & Incident Prioritization activities are as part of IH&R process.

Define what the three categorization levels of Incident priorities are.

External Resources:

Step 3: Incident Triage

Incident Analysis and Validation -

Incident responders need to analyze the indicators of a reported issue to verify if it is an information security incident or an error in the hardware or software components

The IH&R team must find the different sources of indicators, examine the security solutions, verify the system, device logs, and identify the incident and its vectors

Analysis and validation will help in determining the affected resources and data, systems, networks, servers, services; impact on the business; and different types of losses

Some of the steps included in incident analysis and validation to verify any data modification are:

```
▪ Log Analysis: Information related to incident might be available in several
```

places such as IDPS, firewall, application, and router logs.

```
▪ Event Correlation: Used to assign/find meaning(s) for relating a set of
```

events that occur over a fixed amount of time.

```
▪ Network and System Profiling: Identifying changes made to the various
```

characteristics of expected activity by establishing a baseline and measuring against it.

What is Incident Classification?

Once the incident is detected, it needs to be categorized appropriately for Type, Severity and Impact so that necessary response actions can be taken.

Incident Classification has two major parts to it –

1. Categorization assists in putting the events into a common bucket for better coordinated and consistent handling.
2. Severity ratings assist in assigning a “sense of urgency” to the Incident detected.

What is Incident Prioritization?

The prioritization must depend on the severity of impact, importance of the compromised resources, operations disrupted, and losses incurred due to the incident.

It is the responsibility of the incident handler to prioritize the compromised elements and sort them according to the most important devices or applications required for business continuity.

Prioritization will also help incident handlers to manage the available incident response staff and resources.

The incident handler assigns the level of priority, predefined criteria and requirement as well as urgency in restoring the compromised resource.

Working on the most severe incidents will also help the organization to minimize business disruption and help reduce financial and reputational loss; it can also reduce the amount and time spent on incident response functions such as containment, eradication, and recovery.

It will help in scheduling the tasks and ease the process of reporting the status to stakeholders and customers.

Incident priorities are mainly categorized into three different levels:

1. Low-level Incidents - the least harmful incidents that pose minimal threat to the organization.

The reported low-level incident might not be severe but still have the potential to act as a predecessor to other major security incidents.

NOTE: It is essential to address these incidents as they can escalate to medium-or high-level incidents.

2. Middle-level Incidents - pose moderate threat to the organization.

These incidents can result in a false positive and might interrupt the organizational operations to some extent.

NOTE: It is essential for the incident handlers to handle such incidents within a few hours on the same day of their occurrence.

3. High-level Incidents - the most severe kind of incidents that can threaten the business operations of the organization.

High-level incidents can have a huge impact on services that are provided to large number of customers.

Incident Prioritization Approaches -

The IH&R team must prioritize incidents based on the following factors:

```
▪ Impact on the Business Functionality
▪ Sensitivity of the Affected Information
▪ Ability to Handle and Recover
```

Incident Prioritization Categories:

```
▪ Critical
▪ Very High
▪ High
▪ Medium
▪ Low
▪ Irrelevant
```

Best Practices -

```
▪ Focus on high-priority security concerns first
▪ Prioritize recommendations for mitigating risks to applications
▪ Develop strategies to achieve short-term and long-term security postures
▪ Decide on the required and available resources to maintain a consistent
```

level of information security