|  |  |
| --- | --- |
| Course | MGMT-1212-04- Incident Handling & response |
| Assignment 3 | Incident Response Scenario |
| Student ID | 100899259 |
| Student name | Maisha Khatoon |

# Incident Response Scenario 7: Disappearing Host

## Question 1 - Preparation: What measures should be in place to attempt to prevent this type of incident from occurring or to limit its impact?

The association should have many strategies in place to either limit the impact of such an incident or prevent it from occurring in the first place, including:

* Security measures for the organization and endpoints: The association should have security measures in place to detect and stop unauthorized access to and use of the organizations and endpoints.
* Access control measures: The organization needs strong access control measures to make sure that only authorized faculty access the organization and its systems.
* The association should have a documented incident reaction strategy in place to guide the response to security events.
* The incident response team should be able to identify the gaps and play a key role in risk assessment.

## Question 2 - Detection and Analysis: What does the incident response team look at during the initial analysis of a validated incident?

The incident response team should look at a few factors during the fundamental examination of an authorized occurrence, such as:

* The action's origin and character: The team should investigate the origin of the action to identify any potential threat entertainers or attack vectors. To determine the incident's anticipated outcome, they must also decide on the action's purpose.
* The hosts and frameworks that were harmed: To understand the scope of the issue, the team must identify which hosts and frameworks were affected by the action.
* The action's timeline: To understand how long the incident may have been ongoing, the group must decide the action's course of events.
* To make the detection analysis easy, the incident handling team can profile networks and systems, understand normal behaviours and create a log retention policy.

## Question 3 - Containment, Eradication, and Recovery: What should be done to contain the incident? Why?

The incident response team needs to take certain actions, such as:

* Disconnecting impacted systems: In order to prevent further issue, spread, the group should isolate impacted systems from the organization.
* Collecting evidence: In order to determine the cause and scope of the occurrence, the group should gather evidence.
* Watching for future action: The team should keep an eye out for any subsequent activity that could point to a continuing or continued threat in the company and its systems.
* Containment is essential to prevent additional injury or unauthorized entry, as well as to give the team time to collect evidence and analyze the situation.

## Question 4 - Post-Incident Activity: Who should be invited to attend the lessons learned meeting regarding this incident? And when should the lessons learned meeting be held?

Agents from the incident response team, IT personnel, senior administration, and any other partners involved in the incident response should be present at the lessons learned meeting. After the situation has been planned for, the meeting should be convened as soon as possible to ensure that everyone's minds are still fresh with the details. The group should discuss areas for improvement, what went well during the incident response, and any changes that need to be made to the arrangements or processes to prevent future occurrences of incidents similar to this one.