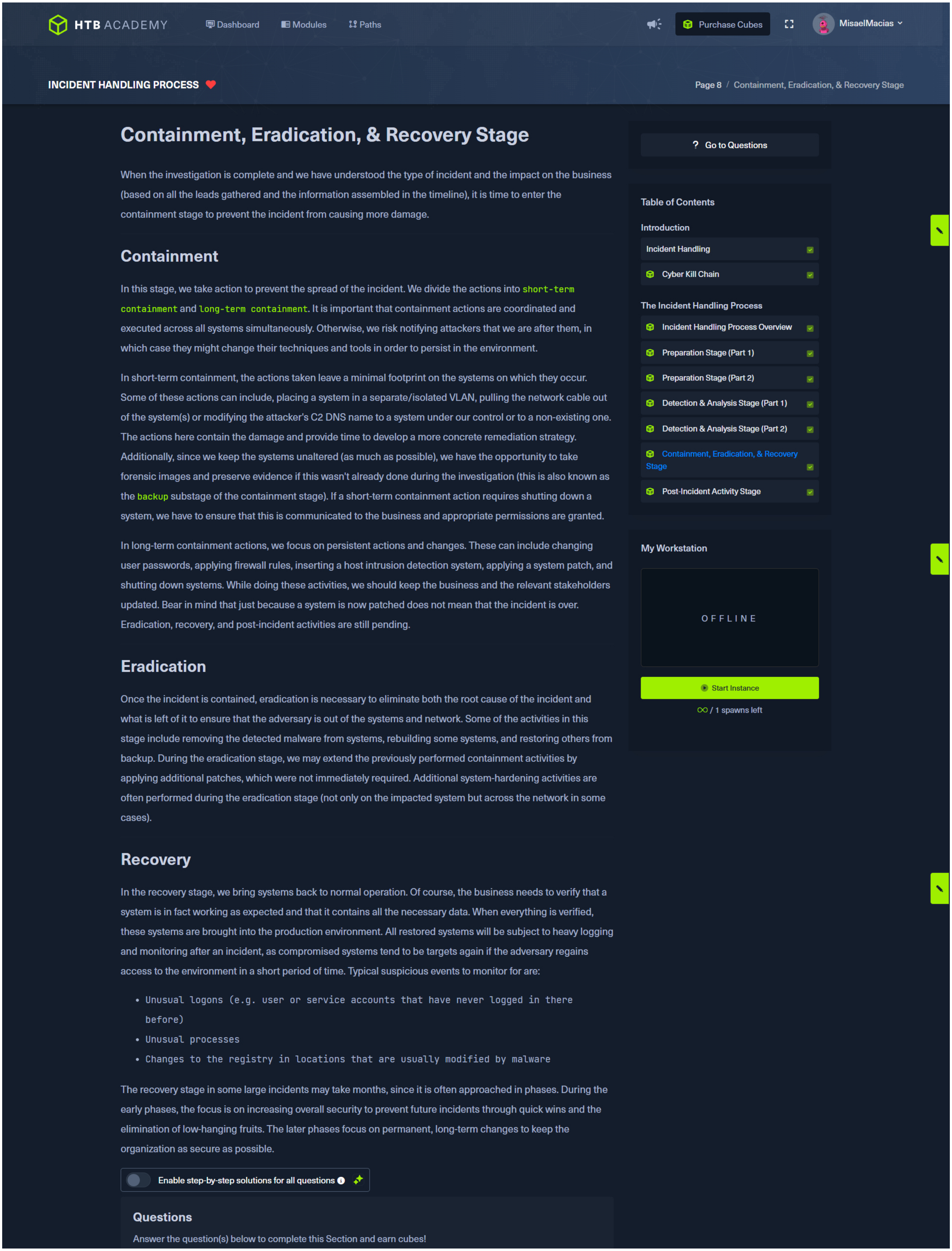


Containment, Eradication, & Recovery Stage

When the investigation is complete and we have understood the type of incident and the impact on the business (based on all the leads gathered and the information assembled in the timeline), it is time to enter the containment stage to prevent the incident from causing more damage.

Containment

In this stage, we take action to prevent the spread of the incident. We divide the actions into `short-term containment` and `long-term containment`. It is important that containment actions are coordinated and executed across all systems simultaneously. Otherwise, we risk notifying attackers that we are after them, in which case they might change their techniques and tools in order to persist in the environment.

In short-term containment, the actions taken leave a minimal footprint on the systems on which they occur. Some of these actions can include, placing a system in a separate/isolated VLAN, pulling the network cable out of the system(s) or modifying the attacker's C2 DNS name to a system under our control or to a non-existing one. The actions here contain the damage and provide time to develop a more concrete remediation strategy. Additionally, since we keep the systems unaltered (as much as possible), we have the opportunity to take forensic images and preserve evidence if this wasn't already done during the investigation (this is also known as the `backup` substage of the containment stage). If a short-term containment action requires shutting down a system, we have to ensure that this is communicated to the business and appropriate permissions are granted.

In long-term containment actions, we focus on persistent actions and changes. These can include changing user passwords, applying firewall rules, inserting a host intrusion detection system, applying a system patch, and shutting down systems. While doing these activities, we should keep the business and the relevant stakeholders updated. Bear in mind that just because a system is now patched does not mean that the incident is over. Eradication, recovery, and post-incident activities are still pending.

Eradication

Once the incident is contained, eradication is necessary to eliminate both the root cause of the incident and what is left of it to ensure that the adversary is out of the systems and network. Some of the activities in this stage include removing the detected malware from systems, rebuilding some systems, and restoring others from backup. During the eradication stage, we may extend the previously performed containment activities by applying additional patches, which were not immediately required. Additional system-hardening activities are often performed during the eradication stage (not only on the impacted system but across the network in some cases).

Recovery

In the recovery stage, we bring systems back to normal operation. Of course, the business needs to verify that a system is in fact working as expected and that it contains all the necessary data. When everything is verified, these systems are brought into the production environment. All restored systems will be subject to heavy logging and monitoring after an incident, as compromised systems tend to be targets again if the adversary regains access to the environment in a short period of time. Typical suspicious events to monitor for are:

- `Unusual logons (e.g. user or service accounts that have never logged in there before)`
- `Unusual processes`
- `Changes to the registry in locations that are usually modified by malware`

The recovery stage in some large incidents may take months, since it is often approached in phases. During the early phases, the focus is on increasing overall security to prevent future incidents through quick wins and the elimination of low-hanging fruits. The later phases focus on permanent, long-term changes to keep the organization as secure as possible.

Questions

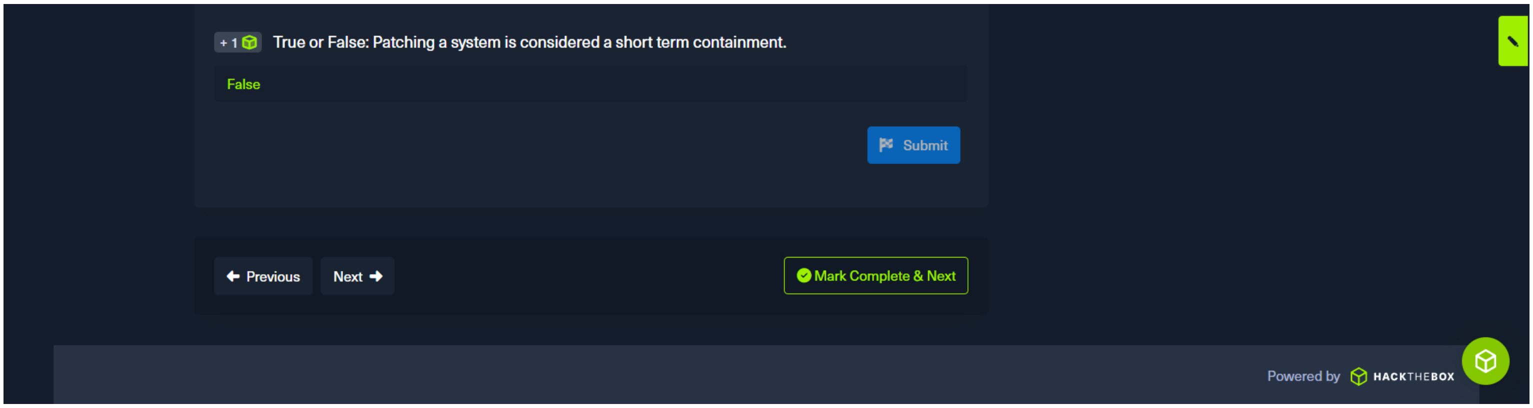
Answer the question(s) below to complete this Section and earn cubes!

Table of Contents

Introduction

The Incident Handling Process

My Workstation



+ 1 True or False: Patching a system is considered a short term containment.

False