Section Introduction, CER

This section of the Incident Response domain will cover how to contain an incident to prevent it from affecting additional assets, collecting digital evidence, removing any malicious artifacts such as backdoors, and addressing any issues that led to the incident occurring, as well as fixing damage occurred during the attack.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand different containment measures and when they are appropriate.
- Understand how digital forensics plays a part in incident response, regarding taking forensic copies of affected systems for later analysis and evidence collection.
- Removing malicious artifacts such as backdoors, scripts, malware and files generated by the attacker.
- Identifying the root cause of the incident and recovering any affected systems, and ensuring the incident shouldn't occur again.