

Mock Exam: Scenario-based Questions

Please read and research the following scenarios and then answer the questions as best as you can – 60 mins

Scenario 1:

A computer fraud has been reported by one of the local banks. The fraudsters were able to steal a large sum of money by issuing an unauthorised bank transfer. The Bank IT security team has requested the help of the national CIRT to handle the incident. The initial investigation carried out by the Bank's IT security team has not led to any substantial result, and the national CIRT has been contacted to help lead the investigation. The CIRT team has been given the results of the initial investigation and is being asked to validate those results and continue with the investigation.

1. How should the bank identify the extent of data exposure and the specific information during unauthorised bank transfers in computer fraud?
2. Regarding data governance, what steps should be taken to change the bank credentials and secure them?
3. To handle incidents in a dynamic environment, what procedures can be put in place to prevent fraudsters in the future by the Bank's IT security team?
4. Analyse the different types of operating systems and application logs when the CIRT team has been given the results of the initial investigation.

Scenario 2: Log Analysis – Website Defacement

The national CIRT has received notification about a defacement of the website of the Revenue Authority. Upon discovering the incident, the IT Team from the Revenue Authority was able to reinstall the website from a backup. However, a few minutes later, the website was once again defaced. The Revenue Authority has requested help from the CIRT team to analyse the logs from the website and understand the root cause of the incident so that appropriate corrective actions can be put in place and the attack stopped.

1. What security controls should be in place to detect, investigate and respond to web attacks?
2. How will you communicate this incident internally and externally with data governance principles?
3. How can the organisation identify and analyse the web server logs from the website of the Revenue Authority?
4. To prevent the website defacement, describe different attack vectors for the exploitation of web vulnerabilities.

Please understand the main point/issue of the scenario before you answer the question