Task (File Submission)

*Answers are highlighted in **bold***

1. What are the indicators that an incident has occurred? Select all that apply
   a. A hunch.
   b. Mando & Co.'s website was unavailableplus there was an increase intraffic causing a slow performance.
   c. Mando & Co.'s external mailboxes locked due to unsuccessful login attempts.
   d. A mail from ShadowSquirrels requesting for 200BTC.
   e. Mando & Co.'s Active Directory being compromised.

2. What kind of attack do you suspect this to be? Select all that apply
   a. Phishing.
   b. Distributed Denial of Service (DDOS).
   c. Password Attack.
   d. Ransomware.
   e. Cross-site Scripting.

3. After determining that an incident has occurred, as a cybersecurity analyst, what are the next steps to take? Select all that apply
   a. Begin documenting the investigation.
   b. Prioritise handling the incident based on factors such as; functional impact, information impact and recoverability effort.
   c. Start gathering evidence. Get confirmation of the breach and whether any information was exposed.
   d. Find out how the attacker got into Mando & Co.'s network.
   e. Find out if any data was stolen.
   f. Change and strengthen all logins, passwords, and security Q&As.

4. What steps would you take to contain, eradicate & recover from this incident? Select all that apply

   a. Identify and mitigate all vulnerabilities that were exploited.
   b. Attempt to remove malware from all hosts affected.
   c. Return affected systems to an operationally ready state.
   d. Confirm that the affected systems are functioning normally.
   e. Stay alert and continue to monitor for any future related activity.

5. What activity should be performed post-incident? Select all that apply

   a. Shut down all systems.
   b. Follow-up report detailing everything thing that occurred.
   c. Close incident immediately when everything is back up and working normally.
   d. **Hold lessons learnt meeting.**

e. **Educate: Create a cyber-awareness program for employees.** This helps employees to know how to identify phishing emails. Also, when something suspicious occurs, it should be reported immediately.