Question 1: Summarize the key steps involved in the incident response process, from initial detection to recovery and lessons learned. How does the "prepare, detect, respond, recover, and learn" framework guide incident responders in effectively managing security incidents?

Answer: The steps in the incident response help curate a detailed response. Preparation, identification, containment, eradication, recovery and lessons learned from the event. This framework guides responders in the correct steps to respond to an incident. It acts as a pipeline, there are steps for each stage of the incident. Which ultimately ends in the eradication of the threat and then implementing the lessons that have been learned from the incident.

Question 2: Examine the concept of post-incident analysis and reporting. Why is it essential for organizations to conduct a thorough analysis of security incidents, document findings, and share lessons learned?

Answer: Its important because eventually some of these incidents could be repetitive and used to create an SOP. This could help other organizations that face similar attacks or threats. This could be shared knowledge amongst community and organizations to help create a more secure network.