Case Study

Docs.ai provide a AI chat-bot that is trained on your own data. Customers upload their business documents (like annual reports, sales presentations, meeting records etc.) which are used as dataset for training an AI model. In the first stage, training is done automatically, then in in 2nd stage model fine-tuning is done by machine learning experts at the company. Once training is complete, customers can start chatting with the AI agent and ask for any business-related information.

Question Group A

1. For the above information system, identify and discuss a possible threat against (a) integrity (b) confidentiality (one threat each). Be specific to the case study!
   Secondly, propose and briefly discuss a security measure against each threat.
2. Define the term 'incident'. List down any three incident indicators, and discuss two incident containment strategies.

[(8 + 4) + 6 marks]

Question Group B

1. For the above information system, identify and discuss a possible threat against (a) accountability (b) availability (one threat each). Be specific to the case study!
   Secondly, propose and briefly discuss a security measure against each threat.
2. Difference between attack and threat.
3. What are social engineering attacks, give a real life example.

[(8 + 4) + 2 + 4 marks]