

1 AI in attack and defence – Part 2

—Answers

Answers

Work through these after you have tried the questions yourself.

2.1 AI writes in perfect, native-sounding language, removing the bad grammar that used to reveal a scam.

2.2 a shared secret question only the two people know; the deepfake cannot answer it, exposing the fake.

2.3 some AI tools feed input back into training, and an adversary could later extract that data.

2.4 a network logs millions of events daily that humans cannot read, but AI can sort them quickly.

2.5 the final risk decision (or approving a firewall change), because AI is probabilistic and can be wrong. \