Exercise walk-through

Leveraging AI in Cyber Defense ▪ 1.5

eXercise

You must be able to

- explain how AI recommends safer configurations (with human review)
- explain how AI handles the scale of network events for faster detection

Method — AI at scale

A network produces millions of events daily - too many for people to read. AI sorts likely-malicious events from harmless ones, alerts staff, or acts automatically, cutting response from days to seconds.

Method — Human in the loop

AI advice is a recommendation, not a command. A knowledgeable human must review a suggested firewall rule or code fix before it is applied, because AI is probabilistic.

Practice 2.1 ▪ 2 marks

Explain why AI is useful for analysing network logs.

Solution 2.1

Worked steps

a network logs millions of events daily B1 that humans cannot read, but AI can sort them quickly B1.

Practice 2.2 ▪ 2 marks

Give one benefit and one limitation of AI-powered threat detection.

Solution 2.2

Worked steps

benefit: responds in seconds not days B1; limitation: it is probabilistic and needs human review B1.

Practice 2.3 ▪ 2 marks

Why must a human review an AI's security recommendation before applying it?

Solution 2.3

Method: Human in the loop

Worked steps

AI guesses are probabilistic and can be wrong B1; a bad rule could block real users or miss a threat B1.

Exam-style 3.1 ▪ 1 mark

The main advantage of AI for threat detection is that it can

A remove all false alarms

B respond in seconds instead of days

C replace every analyst

D delete the logs

Solution 3.1

A remove all false alarms

B respond in seconds instead of days ✓

C replace every analyst

D delete the logs

Worked steps

B. speed of response is AI's key advantage.

Exam-style 3.2 ▪ 1 mark

Which task is best left to a human, not the AI?

A sorting millions of events

B flagging likely threats

C making the final risk-acceptance decision

D matching known signatures

Solution 3.2

A sorting millions of events

B flagging likely threats

C making the final risk-acceptance decision ✓

D matching known signatures

Worked steps

C. the final risk decision is a human/policy call.

Exam-style 3.3 ▪ 1 mark

A hospital's network logs 20 million events a day.
(a) Explain why human staff alone cannot review all these events.
(b) Describe how AI helps and what role the human keeps.

Solution 3.3

Method: AI at scale

Worked steps

(a) the volume is far too large for people to read B1. (b) AI sorts and flags the likely-malicious events B1; a human reviews and decides on the flagged cases B1.