AP CYBERSECURITY • EXERCISE SHEET

1.5 Leveraging AI in Cyber Defense

Name: _____ Class: _____ Date: _____ **Total: 11 marks**

Objective

Build the skills to answer exam questions on how defenders use AI to protect networks, applications, and data.

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

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ 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.

■ 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.

2 Practice

2.1 Explain why AI is useful for analysing network logs. [2]

2.2 Give one benefit and one limitation of AI-powered threat detection. [2]

2.3 Why must a human review an AI's security recommendation before applying it? [2]

3 Exam-style questions

3.1 The main advantage of AI for threat detection is that it can [1]

- **A** remove all false alarms
- **B** respond in seconds instead of days
- **C** replace every analyst
- **D** delete the logs

3.2 Which task is best left to a human, not the AI? [1]

- **A** sorting millions of events
- **B** flagging likely threats
- **C** making the final risk-acceptance decision
- **D** matching known signatures

3.3 A hospital's network logs 20 million events a day.

(a) Explain why human staff alone cannot review all these events. [1]

(b) Describe how AI helps and what role the human keeps. [2]

Solutions

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

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

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

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

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

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