

2.4 Detecting Physical Attacks

Name: _____ Class: _____ Date: _____

Total: 10 marks

Objective

Build the skills to answer exam questions on detecting physical attacks and placing detection controls well.

You must be able to:

- list controls that detect physical attacks: cameras, guards, motion sensors
- explain why placement (entrances, low-traffic areas) matters
- read entry logs (door-open times) for signs of piggybacking

1 Worked examples

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

■ Placement matters

Cameras belong at points of ingress and egress. Motion sensors belong in low-traffic sensitive areas like server rooms - in a busy hallway they cause constant false alarms and get ignored.

■ Reading entry logs

A door that normally opens for 2 seconds but stayed open 15 seconds is a clue that someone piggybacked through behind an authorised employee.

2 Practice

2.1 State two controls that DETECT (rather than prevent) physical attacks. [2]

2.2 Explain why a motion sensor should not be placed in a busy hallway. [2]

2.3 An entry log shows a secure door was held open for 20 seconds, far longer than

normal.

- (a) State what this could indicate. [1]
- (b) Explain your reasoning. [1]
-
-

3 Exam-style questions

3.1 Where are cameras MOST useful for detecting physical attacks? [1]

- **A** inside a locked safe
 - **B** at points of ingress and egress
 - **C** facing a blank wall
 - **D** in an empty closet
-

3.2 A stationary guard is best placed [1]

- **A** patrolling a large perimeter
 - **B** at a point that funnels traffic, like a main entrance
 - **C** in a distant unused room
 - **D** outside the property boundary
-

3.3 A company installs cameras and motion sensors.

- (a) State one advantage of pairing cameras with motion sensors. [1]
- (b) State the best placement for the motion sensors. [1]
-
-

4 Go further

- work through the **2.4 Detecting Physical Attacks** lesson on the **Learn** page;
- read the **Securing Spaces** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 any two of: cameras; security guards; motion sensors.

2.2 constant movement causes many false alarms, so staff stop taking the alerts seriously.

2.3 (a) piggybacking / tailgating. (b) a door held open unusually long suggests an extra person passed through.

3.1 B. entrances and exits capture who comes and goes.

3.2 B. a fixed guard is effective where traffic is funnelled.

3.3 (a) when a sensor triggers, defenders can use the camera to verify a real breach. (b) in low-traffic sensitive areas such as server rooms.