Solutions

Each answer shows the steps, then the **result**.

2.1

- accounting is the process of recording and monitoring user activities - devices log when data are accessed and by whom; analysing those logs can reveal unauthorised access to data

2.2

- the volume of logged activity is far larger than analysts can read, so to operate at an effective speed log analysis must be augmented with automation - otherwise detection arrives long after the attack

2.3

- a honeypot is a file that appears to contain valuable data such as credit card details, PII or passwords, but whose contents are fake; no legitimate user has any reason to open it, so any access is by definition suspicious and there is essentially no innocent explanation to rule out

2.4

(a)

- repeatability - the same input always produces the same output for a given hash function

(b)

- the file has been altered

(c)

- any two of: what changed; who changed it; when it changed; whether the change was malicious; whether the file was also copied

2.5

- a hash detects **alteration** only; an adversary who views or copies the file changes nothing, so the hash still matches and the theft goes undetected - a false negative for confidentiality

2.6

(a)

- directory traversal

(b)

- XSS

(c)

- SQL injection

(d)

- buffer overflow

2.7

(a)

- a honeypot, or hash checking - justified on **cost**, since both are inexpensive and the charity has almost no budget

(b)

- automated real-time log analysis, or DLP tooling - justified on **sensitivity/criticality** and **classification**, since healthcare data is highly sensitive and legally regulated

2.8

- data classified as healthcare or financial is usually governed by law or regulation requiring stronger protection, and it is more attractive to adversaries, so both the legal requirement and the higher likelihood of attack justify more expensive controls

3.1 B

- The value is only apparent; the data inside is fake, which is what makes an access unambiguous

3.2 C

- Repeatability is what lets two hashes taken at different times be compared at all

3.3 C

- A false negative: an attack occurred and the control reported nothing

3.4 B

- Honeypots offer near-instantaneous detection and are inexpensive

3.5

(a)

- a **honeypot**. The file looks valuable - bank details - but its contents are fabricated, so nobody has a legitimate reason to open it; the system alerts on any access, and because there is no innocent explanation the alert is essentially certain to be a genuine indicator

(b)

- it proves the file has been **altered** since the previous Friday. It does not prove **who** altered it, **what** was altered, or **when** during the week it happened; nor does it prove the change was malicious - a legitimate grade entry produces exactly the same result

(c)

- copying a file changes nothing about it, so its hash is unchanged and the integrity check reports normal - the classic false negative for confidentiality. The ledger was in any case not among the files being hashed. The access **was** recorded in the accounting logs, but the review is only **monthly** and manual, so detection could not arrive sooner than a month after the event, by which time the data had already been sold - detection that late permits no response

(d)

- Any sensible three, each with a distinct criterion: seminar dates - hash checking only, justified on **cost**, since the data is public and low value; grade records - automated log analysis with alerting, justified on **classification**, since educational data carries a legal protection requirement; grant ledger - a honeypot alongside real-time automated log analysis or DLP, justified on **sensitivity/criticality**, since financial data is both regulated and the most attractive target here

(e)

- DLP would give alerts **as an attack is happening**, which is what was missing - a prompt response can stop an attack rather than record it. But it is expensive, and cost is a real criterion for a university research office; the honeypot and hash checks are inexpensive and already provide near-instant detection and integrity verification respectively. The better proposal is therefore to **keep** the cheap controls, automate the log review so it is continuous rather than monthly, and scope DLP to the financial ledger alone, where the classification justifies the spend