Solutions

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

2.1

- both analyse network data to determine whether malicious activity is taking place; a NIDS alerts and the traffic still passes, while a NIPS also blocks it

2.2

- a SIEM collects and analyses data from **multiple sources** - firewalls, NIDS/NIPS, device logs, application logs; so it can correlate events that look harmless in one log but form an attack when seen together, which a single sensor cannot do

2.3

- computers log every user action and every sensor logs all traffic, so a medium-sized network produces far more data than analysts can read; AI algorithms classify these data patterns as malicious or normal at that scale

2.4

(a)

- false positives fall

(b)

- real attacks may go undetected, because anything the model scores below 95% raises no alert

2.5

(a)

- signature-based - it is more efficient at high traffic volume, and the patterns here are not consistent enough for an anomaly baseline

(b)

- anomaly-based - signature-based cannot detect a new attack, and novel techniques are expected

(c)

- anomaly-based - consistent traffic patterns give a reliable baseline, so genuine deviation stands out

2.6

- detection works by matching traffic to a stored signature of a known attack; a novel attack has no signature yet, so there is nothing to match and it passes unremarked

2.7

(a)

- false negative; characteristic of signature-based detection

(b)

- false positive; characteristic of anomaly-based detection, which flags anything outside the baseline

2.8

(a)

- MAC flooding

(b)

- evil twin

(c)

- ARP poisoning

(d)

- smurf attack

3.1 B

- A NIDS only alerts; a SIEM correlates; a packet capture only records

3.2 B

- It needs a stable baseline before a deviation means anything

3.3 B

- A is a false positive; the threshold in C would raise false positives, not negatives

3.4 C

- DNS poisoning is difficult to detect, and this drop in traffic is its documented indicator - visitors are being sent elsewhere

3.5

(a)

- **MAC flooding** - a sudden surge of Ethernet frames with many different MAC addresses; **ARP poisoning** - duplicate MAC address ARP packets

(b)

- MAC flooding overwhelms the switch's MAC address table, so the switch can no longer direct frames to one port and traffic reaches the adversary that would not otherwise; ARP poisoning then associates the adversary's MAC with a legitimate IP, letting them sit between the imaging machines and the record system to read or modify patient data in transit

(c)

- **Signature-based**. Traffic volume is very high, where signature-based is more efficient; and the patterns constantly change, so an anomaly baseline would be unstable and produce endless false positives on a guest network the hospital does not control

(d)

- **Anomaly-based**, or a hybrid. Traffic is highly consistent, which is exactly the condition anomaly-based needs; and the network carries the most sensitive data the hospital holds, so the criticality criterion favours the more thorough method despite its cost. A false positive here means investigating a legitimate imaging transfer - an hour of analyst time - whereas a false negative means patient records altered; on the guest network the same false-positive rate would generate constant alerts for no protective gain

(e)

- The threshold is a trade between false positives and false negatives, and the two networks sit at opposite ends of it. Network B needs a **low** threshold, because a missed attack compromises regulated patient data; Network A needs a **higher** one, because its volume and variability would otherwise bury the team in alerts about guest devices carrying no sensitive data - and an analyst who learns to ignore alerts misses the ones that matter on both networks