Asset CIA Analysis (10 minutes)

Asset	Confidentiality (1-5)	Integrity (1-5)	Availability (1-5)	Justification *Why did you rate it this way?*
Pressure/flow readings	3	5	5	Need accurate readings to avoid water issues- wrong or missing data can cause bursts.
Gate control commands	4	5	5	Controls water flows- if tampered with, it could flood or cut off areas.
Emergency shutoff capability	4	5	5	Critical for safety, it must work and be accurate, attackers know how bad it would be
Dashboard login credentials	5	5	4	If stolen, someone can control the whole system, Integrity matters to trust users.
Consumption/savings data	4	4	3	Show guest usage, privacy is important, accuracy matters, availability is less critical.
Leak detection alerts	4	5	5	Need alerts to prevent damage- accurate and timely info is very important.

Attack Mapping

For each attack type you learned, identify **one specific scenario** at The Grand Marina:

Attack Type	Specific Scenario	Which Asset Is Targeted	CIA Impact
Eavesdropping	Sniffing MQTT traffic from flow sensors on the network	Pressure/ flow readings	Confidentiality
Spoofing	Sending fake flow readings to the cloud pretending to be a sensor	Pressure/ flow readings	Integrity
Replay Attack	Replaying a previously sent gate open/ close command	Gate control commands	Integrity/ availability

Man-in-the-Middle	Intercepting and changing dashboard commands to devices	Gate control commands/ emergency shutoff	Integrity/ confidentiality
Denial of Service	Flooding the MQTT broker or cloud server to block commands	Dashboard/ Sensor	Availability
Unauthorized Access	Stealing dashboard login credentials to control the system	Dashboard login credentials	Confidentiality/ Integrity/ Availability

Priority Ranking

Based on your analysis, rank the six attacks from **most dangerous** to **least dangerous** for The Grand Marina:

1. Unauthorized Access-> an attacker can control everything once inside
2. Man- in- the- middle -> attacker sees and change commands
3. Spoofing -> can trick the system, cause wrong adjustments
4. Replay attack-> old commands mess up water flow
5. Denial of Service -> blacks access, but doesn't give it full control
6. Eavesdropping -> only sees data, it doesn't allow them to act