Section 1: Executive Summary

The Grand Marina Hotel relies on Hydroficient's HYDROLOGIC system to manage water flow across three critical zones: the Main Building, Pool/Spa, and Kitchen/Laundry. Following a historical incident involving a $4.2 million loss due to an ignored leak, this assessment was conducted to identify vulnerabilities in the system.

The goal of this report is to prevent future catastrophic financial losses, ensure guest safety, and protect the Grand Marina's reputation by securing the physical infrastructure against both cyber-attacks and human error. Based on our threat modeling, we have identified three critical risk categories:

- □ Operational Ransomware: Malicious actors could compromise the web dashboard to remotely shut off water to the hotel, pool, and laundry facilities. Attackers could hold the hotel's water supply hostage, demanding payment to reopen the valves, resulting in immediate revenue loss and guest evacuation.
- □ The "Human-in-the-Loop" Failure= The previous $4.2M loss occurred because a human ignored an alert. Currently, the system relies too heavily on manual intervention. If staff become desensitized to frequent "low-level" alerts, they are likely to ignore a critical "high-level" warning again.
- □ Dependency on Connectivity: If the hotel's internet goes down, the current system configuration may lose the ability to send alerts or receive shutoff commands. A leak occurring during an internet outage could be catastrophic if the devices lack "local intelligence" to act on their own.

Section 2: System Overview

The Grand Marina's HYDROLOGIC system includes the following:

- 500-room luxury hotel (Hydroficient customer)
- 3 HYDROLOGIC flow management devices (one per water service line)
- Cloud-based monitoring and control
- Web dashboard for operators and management
- Remote shutoff and gate control capability

How it works

- The three hydrologic device sends real-time water measurements in psi, and pushes the data to the Message Queue Telemetry Transport (MQTT) broker.
- The MQTT broker sends the data to the Hydroficient cloud server.
- The data in the Cloud server can be viewed on the dashboard through HTTPs requests.

None

```
[HYDROLOGIC Devices] → [Cloud API] → [Dashboard]
        ↓                   ↓
  [Gate Controls]      [Database]
  [Emergency Shutoff]  [Reports]
```

The communication Path

```
[HYDROLOGIC Devices] → [Cloud API] → [Web Dashboard]
                      ↓              ↓
                   WiFi           HTTPs
```

Section 3: Asset Inventory

List the key assets and their CIA priorities (use your work from Step 2):

Asset	Description	C Priority	I Priority	A Priority
HYDROLOGIC Devices	3 flow management units	Medium	Medium	High
Web Dashboard	Operator monitoring interface	Medium	Critical	Medium
Cloud API	Device-to-cloud communication	High	High	High
Remote Controls	Gate adjustments, emergency shutoff	High	Critical	High
Consumption Data	Savings reports, billing records	Medium	High	Medium

Priority Rationale:

- **Integrity is Critical** for remote control and Web dashboard — wrong readings could lead to incorrect decisions.
- **Availability is High** for most assets because they need to be available at any point— downtime during an emergency could incur costs.
- **Confidentiality is High** for remote control— If anyone could access it, then it can be triggered and cause ruckus.

Section 4: STRIDE Analysis

This is the core of your threat model. For **each major component**, analyze all six STRIDE categories:

Component 1: HYDROLOGIC Devices

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attackers introduce fake devices and send fake alerts to the dashboard. For example, Device 04 from Common room.	Medium	High	High
Tampering	Attackers with physical access to the building can tamper with the settings e.g the angle of pipe, inflow and outflow etc.	Medium	High	Critical
Repudiation	The device sent an alert but no logs were able to trace the fact that data was sent from the device.	Medium	High	High
Info Disclosure	Attacker views consumption data or commands sent over unencrypted WiFi.	High	High	Critical
Denial of Service	Attacker jams the Wifi Signal used in transmitting data from the devices	High	High	Critical

	to the cloud server.			
Elevation of Privilege	Physical access to the devices without authorization is a potential cause of damage.	Medium	Medium	Medium

Component 2: Web Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attackers use stolen credentials through phishing to access the dashboard.	High	High	Critical
Tampering	Attackers modify alerts as they enter e.g. when water leaks are detected.	Medium	High	High
Repudiation	Operation manager or Technician can claim they did not trigger remote shutoff command.	Medium	Medium	Medium
Info Disclosure	By analyzing water flow data in the "Main Building" vs. "Pool/Spa," a sophisticated attacker (or competitor) could infer hotel occupancy rates or guest habits	Medium	Medium	High

Denial of Service	Attackers use botnets to send a lot of traffic to the dashboard during night shifts and staff couldn’t see them.	High	Critical	Critical
Elevation of Privilege	The Head of security account is compromised, then attackers modify configurations.	Medium	High	High

Component 3: Cloud API

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker creates fake cloud endpoint; sends all water data records to attacker's server.	Medium	High	High
Tampering	Attacker with database access modifies historical water usage records, corrupting consumption details.	Medium	Medium	Medium
Repudiation	Hydroficient claims trigger alert was sent; the hotel claims it was not seen.	Medium	High	Medium
Info Disclosure	The database breach can expose	Medium	High	Medium

	how water was efficiently or poorly managed.			
Denial of Service	DDoS attack on the cloud takes down monitoring for all devices simultaneously and the hotel management might start panicking.	High	High	Critical
Elevation of Privilege	An intern employee from Hydroficient access Marina Hotel Cloud database without authorization.	Medium	Low	Medium

Component 4: Remote Controls (Gate/Shutoff)

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attackers introduce fake devices and send fake alerts to the dashboard.	Medium	Medium	High
Tampering	Attackers can tamper with the minimum or maximum psi levels to which remote shutoff can be triggered.	Medium	High	Critical
Repudiation	An attacker can remotely use the login credentials of a staff without	Medium	High	High

	his knowledge to trigger remote shutoff			
Info Disclosure	Attackers views and reveals shutoff commands.	Medium	Medium	High
Denial of Service	DDos attacks can render the remote commands or shutoff inaccessible.	Medium	High	High
Elevation of Privilege	Attacker can use stolen credentials with admin privileges to access the remote control	Medium	High	High

Section 5: Risk Summary

1. Operational / Process Alert Fatigue & Human Error: Staff ignore or mute "Leak Detected" notifications due to frequent false positives, leading to unchecked flooding (Repeat of previous incident).
2. Denial of Service: attack: An external attacker compromises the cloud dashboard to shut off valves in all 3 zones (Main, Pool, Kitchen), demanding payment to restore water flow.
3. Architecture: Loss of Connectivity (Fail-Open): Internet/Cloud outage occurs during a leak event. If the device relies on the cloud for instructions, it fails to act, resulting in physical damage.
4. Network Security: Lateral Movement: Attackers use the compromised IoT water devices as a gateway to pivot into the Hotel's corporate network to steal Guest Data or Credit Card info (PCI).
5. Integrity: Audit Trail Repudiation: A lack of immutable logs allows staff to deny seeing alerts or modifying settings, preventing the hotel from enforcing accountability or insurance claims.
6. Unencrypted device communications — Vital data transmitted over WiFi without encryption. Any attacker on the network can capture sensitive water consumption information.

7. Dashboard tampering (Tampering) — Users with dashboard access can modify alert thresholds. A malicious insider or compromised account could raise thresholds so critical alerts never trigger.

Medium Risks:

1. Device spoofing on the network
2. Dashboard action audit gaps
3. Alert interception
4. False alert injection

Section 6: Recommended Mitigations

Risk	Proposed Mitigation	Implementation Complexity
Alert system flooding	Add rate limiting and anomaly detection for alert generation	Medium — cloud configuration
Unencrypted device communications	Implement TLS encryption for all device-to-gateway communication	Medium — firmware update required
Weak dashboard authentication	Enable multi-factor authentication for all logins.	Low — configuration change
Dashboard tampering	Require admin approval for threshold changes; add confirmation dialogs	Low — application update
Wifi hijacking	Make the HYDROLOGIC devices to be on a separate VLAN, isolated from the Guest Wi-Fi and the Hotel Payment systems.	Low - Separate VLAN
Repudiation	Every alert, login, and acknowledgement must be written to a log that cannot be deleted by standard users.	Low - Activate logging on devices

Water consumption data export	Add re-authentication requirement for bulk data exports	Low — application update