

Section 1: Executive Summary

Hydroficient is an IoT company that makes water flow management devices for commercial properties. The Grand Marina is a 500-room luxury hotel that uses Hydroficient's HYDROLOGIC system. They have 3 HYDROLOGIC devices installed (Main Building, Pool/Spa, Kitchen/Laundry). The system includes cloud-based monitoring, a web dashboard, and remote shutoff capability. Recently, a \$4.2M water damage incident occurred when a leak alert was ignored – this is why security matters

This threat model identifies security risks that could affect availability, integrity, reputation, and hotel operation. IoT hotel devices are increasingly targeted by attackers – the 2025/2026 Tourism sector, with IoT devices serving as common entry points.

Our analysis identified three critical concerns requiring immediate attention:

- Weak security on the hotel's water management system could allow unauthorized people to access it, change important settings, or control water valves, leading to water supply disruptions or delayed responses to leaks.
- If information sent between the water sensors and the monitoring system is not properly protected, someone could intercept or change it. This could cause the system to display incorrect information, miss leaks, or trigger the wrong actions.
- The hotel's water monitoring system relies on a central control system. If this central system fails or is compromised, the hotel could lose visibility of all connected water sensors, preventing staff from detecting leaks and responding to water-related emergencies in time.

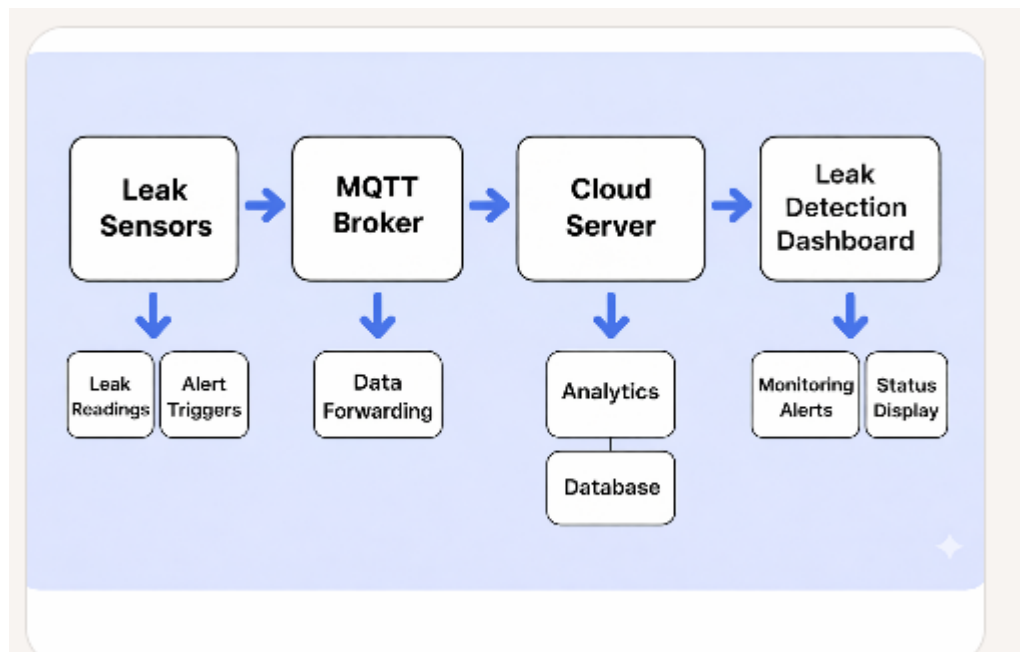
We recommend prioritizing multi-factor authentication, encrypted communications, and server redundancy.

Section 2: System Overview

Grand Marina Threat Detection Deployment:

- Hotel water monitoring system
- Pressure and flow sensors installed throughout the property
- MQTT-based communication gateway
- Cloud-based monitoring and analytics platform
- Maintenance dashboard for monitoring and response
- Leak detection alerts and emergency shutoff capability
- Historical water consumption reporting

Data Flow Diagram:



How It Works:

1. Water sensors measure pressure, flow rates, and water usage continuously throughout the hotel.
2. Sensor data is transmitted through the hotel's IoT network to the MQTT gateway/broker for processing.
3. The MQTT broker forwards sensor information to the central water monitoring dashboard.
4. The monitoring system analyses readings, compares them against predefined thresholds, and identifies unusual activity such as leaks or abnormal water pressure.
5. The dashboard displays real-time water system status, sensor readings, and alerts to hotel maintenance staff.
6. Critical alerts are sent to maintenance personnel, who can investigate the issue or remotely activate the emergency shutoff valve to prevent further damage

Section 3: Asset Inventory

Asset	Description	C Priority	I Priority	A Priority
-------	-------------	------------	------------	------------

Water Monitoring Sensors	Pressure, flow, and leak detection devices installed throughout the hotel	Medium	Critical	Critical
Water Monitoring Dashboard	Interface used by hotel staff to view water system status, sensor readings, and alerts	High	High	Critical
MQTT Broker / IoT Gateway	Central communication service that receives sensor data and forwards information to the monitoring system	High	Critical	Critical
Water System Data	Pressure readings, flow measurements, consumption data, and historical water usage records	Medium	Critical	High
Leak Detection Alert System	System responsible for identifying abnormal conditions and notifying maintenance staff	Medium	Critical	Critical
Emergency Shutoff System	Automated or manual controls used to close water valves during major leaks or emergencies	Medium	Critical	Critical

Priority Rationale:

- **Integrity-** The data being provided needs to be accurate. False information / reading can lead to the water being shut off /or a false emergency leading to a water crisis. Secondly, there could be a leak that has not been detected resulting in significant property damage
- **Availability-** you need to have the systems up and running at all times . Residents cannot be without water.
- **Confidentiality-** equally as important as the command signals being sent to the sensors and access to the dashboard that is used to control the system

Section 4: STRIDE Analysis

Component 1: Grand Marina Devices

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attackers impersonates a legitimate water sensor and send false readings to hide leaks or trigger incorrect responses.	Medium	High	High
Tampering	Attacker modifies water control commands, preventing correct valve operation during an emergency.	Low	Critical	High
Repudiation	The system lacks sufficient logs to prove who issued water control commands or when actions occurred.	Medium	Medium	Medium
Information Disclosure	Attacker captures unencrypted IoT communications and obtains sensor data or system information.	High	High	Critical
Denial of Service	Attacker disrupts IoT communication, preventing sensors, alerts, and emergency controls from operating.	Medium	Critical	Critical
Elevation of Privilege	Attacker exploits dashboard vulnerabilities to gain administrator access and control water system functions.	Low	Critical	High

Component 2: Water Sensor Dashboard

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker impersonates a legitimate pressure or flow sensor and sends false readings to the monitoring dashboard, causing the system to hide a leak or trigger a false alarm.	Medium	Critical	High
Tampering	An attacker with access to the monitoring dashboard modifies leak detection thresholds or alters emergency shutoff commands, preventing the system from responding correctly to a water leak.	Medium	Critical	Critical
Repudiation	A maintenance operator claims they never received or acknowledged a leak alert, but the system lacks audit logs showing who viewed the alert, when it was received, or whether commands were successfully sent and executed.	Medium	Medium	Medium
Information Disclosure	An attacker gains unauthorized access to the monitoring dashboard and exports water consumption records, sensor locations, system configurations, and maintenance logs, exposing sensitive operational information.	Medium	High	High
Denial of Service	An attacker floods the MQTT broker or monitoring dashboard with network traffic, preventing maintenance staff from receiving real-time sensor readings, leak alerts, or using the emergency shutoff system.	Medium	Critical	Critical
Elevation of Privilege	A maintenance technician exploits a software vulnerability to gain administrator privileges, allowing them to modify system configurations, disable alerts, or remotely control water valves without authorization.	Low	Critical	High

Component 3: Cloud Server

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	An attacker creates a fake cloud endpoint or impersonates a legitimate MQTT broker, causing the hotel gateway to send sensor data to the attacker's server or accept false sensor readings.	Medium	Critical	High
Tampering	An attacker gains unauthorized access and modifies live sensor readings, leak detection thresholds, or emergency shutoff commands, causing incorrect system decisions or delayed responses to leaks.	Medium	Critical	High
Repudiation	A maintenance operator claims they never received or acknowledged a leak alert, but the system lacks audit logs showing who viewed the alert, when it was received, or whether commands were successfully sent and executed.	Medium	High	High
Information Disclosure	An attacker gains unauthorized access to the monitoring dashboard and exports water consumption records, sensor locations, system configurations, maintenance logs, and control settings, exposing sensitive operational information.	Medium	Critical	High
Denial of Service	An attacker floods the MQTT broker or monitoring dashboard with malicious traffic, preventing maintenance staff from receiving real-time sensor readings, leak alerts, or issuing emergency shutoff commands.	Medium	Critical	Critical

Component 4: Alert System

Threat	Scenario	Likelihood	Impact	Risk
Spoofing	Attacker sends fake critical alerts for devices, causing alert fatigue and wasted response time	Medium	Medium	Medium
Tampering	Attacker intercepts and blocks real critical alerts before they reach central dashboard stations	Low	Critical	High
Repudiation	Alert was generated but no proof it was delivered to the operator on duty	Medium	High	High
Info Disclosure	Alert messages contain patient room and condition; attacker intercepts to learn who is critically ill	Medium	Medium	Medium
Denial of Service	Attacker floods alert system with false positives; real alerts get buried or ignored	Medium	Critical	Critical
Elevation of Privilege	Standard user discovers they can modify their own alert preferences to receive all sensor alerts	Low	Medium	Low

Section 5: Risk Summary

1. **Unencrypted device communications (Information Disclosure)** – Sensor readings, water consumption data, and system communications are transmitted over the hotel's network without sufficient encryption. An attacker connected to the network could intercept sensitive operational information, identify water usage patterns, or gather information that could assist future attacks.
2. **Weak dashboard authentication (Spoofing)** – A single compromised password could provide unauthorized access to the water monitoring dashboard, allowing attackers to view sensor data, modify alert settings, or issue unauthorized commands. Phishing and credential theft present a significant risk in hotel environments.
3. **Alert system flooding (Denial of Service)** – The alert system lacks sufficient protection against excessive requests or false alerts. An attacker could overwhelm the system with fake notifications, causing genuine leak alerts to be overlooked and delaying response to critical water issues.
4. **Dashboard tampering (Tampering)** – Users with dashboard access may modify leak detection thresholds or system settings. A malicious insider or compromised account could increase thresholds, preventing alerts from triggering during actual leaks and increasing the risk of property damage.

5. **Cloud service single point of failure (Denial of Service)** — All connected water monitoring devices depend on the Grand Marina cloud monitoring service. A cloud outage or compromise could prevent the hotel from receiving sensor data, monitoring water conditions, and responding to emergencies. No local fallback mechanism exists.

High Risks:

Risk	Description
Device network pivot (Elevation of Privilege)	A compromised water monitoring device could provide an attacker with access to the hotel's IoT network and potentially allow movement toward other connected systems.
Water usage data export (Information Disclosure)	The monitoring dashboard allows access to historical water consumption data, sensor locations, and operational records without additional authorization controls.
Firmware tampering (Tampering)	Physical access to water sensors or IoT devices could allow attackers to modify firmware, causing false readings or unauthorized device behaviour if firmware integrity is not verified.
Alert delivery gaps (Repudiation)	The system does not provide sufficient confirmation that critical leak alerts were delivered, received, or acknowledged by maintenance personnel.

Medium Risks:

- **Device spoofing on the network** — An attacker could introduce a fake sensor or impersonate a legitimate device to send false readings.
 - **Dashboard action audit gaps** — Lack of detailed logging may prevent the hotel from determining who changed settings or issued commands.
 - **Alert interception** — Attackers may intercept communications between sensors, the MQTT broker, and the dashboard.
 - **False alert injection** — Attackers may generate fake leak alerts, causing unnecessary responses and potentially hiding real incidents.
-

Section 6: Recommended Mitigations

For Critical Risks:

Risk	Proposed Mitigation	Implementation Complexity
Weak dashboard authentication	Enable multi-factor authentication (MFA) for all hotel staff accessing the water monitoring dashboard. Implement role-based access controls to limit who can modify settings or issue commands.	Low – configuration and access policy changes
Unencrypted device communications	Implement TLS encryption for MQTT communication between sensors, MQTT broker, and dashboard. Use certificate-based authentication to verify trusted devices.	Medium – network and device configuration changes
Alert system flooding	Implement rate limiting, alert thresholds, and anomaly detection to prevent excessive false alerts from overwhelming maintenance staff.	Medium – application/cloud configuration
Dashboard tampering	Require approval workflows for changing leak detection thresholds or emergency settings. Maintain logs of all configuration changes and administrator actions.	Low – application update
Cloud single point of failure	Implement a local gateway fallback mode that allows temporary local monitoring, alert storage, and emergency control if the cloud service becomes unavailable.	High – architecture redesign

For High Risks:

Risk	Proposed Mitigation	Implementation Complexity
Device network pivot	Segment IoT water devices onto a dedicated VLAN separate from hotel corporate systems and guest WiFi. Apply firewall rules limiting unnecessary communication.	Medium – network configuration

Water data export	Require additional authentication before exporting historical water usage reports. Restrict export permissions based on user roles.	Low – application update
Firmware tampering	Enable secure boot, signed firmware verification, and controlled firmware update processes to prevent unauthorized modifications.	High – hardware/firmware update
Alert delivery gaps	Implement alert delivery confirmation, acknowledgement tracking, and escalation procedures if maintenance staff do not respond within a defined timeframe.	Medium – application update
Unauthorized cloud access	Implement zero-trust access controls, strong identity management, privileged access reviews, and comprehensive audit logging for all dashboard activity.	Medium – policy and technical changes

Key Alignment With Grand Marina Risks

The highest priority controls should focus on:

1. **Availability** – ensuring the hotel can continue monitoring water systems and responding to leaks.
2. **Integrity** – ensuring sensor readings and control commands cannot be manipulated.
3. **Confidentiality** – protecting dashboard access, system configurations, and operational data.

This mitigation plan directly addresses the major risks identified in the STRIDE assessment:

- DoS → Cloud dependency and alert flooding
- Tampering → Dashboard changes and firmware attacks
- Spoofing → Fake sensors and unauthorized access
- Information Disclosure → Exposed operational data
- Elevation of Privilege → Unauthorized administrative control
- Repudiation → Missing audit trails and accountability.