SECURITY ASSESSMENT · WEEK 1 DELIVERABLE

Grand Marina Water Monitoring System

Security Threat Model

Client: The Grand Marina Hotel
Prepared by: Maria Shirin
Classification: Confidential

SECTION 1 OF 6

Executive Summary

The Grand Marina relies on three HYDROLOGIC devices to watch every water line in the hotel. After last year's ignored leak, we analyzed how an attacker could abuse that system.

The most serious risk we found is An attacker could steal an operator's password and gain unauthorized access to the hotel's water management dashboard, potentially taking full control of the water system. Beyond that, the findings that most need attention are An attacker could overwhelm the hotel's cloud service, preventing operators from monitoring water readings across the hotel, or send a fake emergency shutoff command that disrupts the hotel's water supply. We recommend starting with Implementing multi-factor authentication for the water management dashboard, because requiring an additional verification step would make it harder for attackers to gain access using stolen passwords.

SECTION 2 OF 6

System Overview

The Grand Marina is a 500-room hotel. Its water monitoring system runs three HYDROLOGIC flow devices, one per major water line: Main Building, Pool and Spa, Kitchen and Laundry. The devices report pressure and flow readings to a cloud monitoring service (the Cloud API). Operators watch the system through a web dashboard and can send remote commands, including gate control and an emergency shutoff. The hotel commissioned this assessment after an unnoticed leak caused $4.2M in damage.

How the data flows:

- Devices send readings to the **Cloud API**, which feeds the **Dashboard**.
- Devices also receive commands for the **Gate Controls** and the **Emergency Shutoff**.
- The Cloud API writes to the **Database** and generates **Reports**.

SECTION 3 OF 6

Asset Inventory

The six assets below come from the Vault analysis, in their three families, each rated for Confidentiality, Integrity, and Availability.

ASSET	WHAT IT IS	C	I	A
WHAT THE SYSTEM DOES · ACTIONS AN ATTACKER COULD TRIGGER				
Valve commands	Open or close the water lines on each HYDROLOGIC device.	**Med**	**Critical**	**Critical**
Emergency shutoff	Cut water to the whole hotel in one action.	**Low**	**Critical**	**Critical**
WHAT THE SYSTEM KNOWS · DATA AN ATTACKER COULD READ OR FAKE				
Pressure and flow readings	Live numbers from all three water lines.	**Med**	**Critical**	**High**
Consumption history	Months of usage records and reports.	**High**	**High**	**Med**
WHAT THE SYSTEM TRUSTS · THINGS IT BELIEVES WITHOUT QUESTION				
Operator credentials	Logins that unlock the dashboard and remote controls.	**Critical**	**Critical**	**High**
Leak alerts	The warnings operators rely on to act in time.	**Low**	**Critical**	**Critical**

Why these priorities: Integrity is critical almost everywhere, because a faked reading or command is exactly how last year's leak went unnoticed. Availability is critical for the shutoff and the alerts, because they only matter in an emergency. Confidentiality peaks at operator credentials, because one stolen login unlocks everything else.

SECTION 4 OF 6

STRIDE Analysis

Web Dashboard

Where operators watch readings and send commands. The component you rated with Maya, so it carries all six threat families.

S **Spoofing** — **CRITICAL RISK**

An attacker uses a phished operator password to log into the dashboard from outside the hotel and gains full control of the water system.

Likelihood: Medium · Impact: Critical · Risk: Critical

T **Tampering** **CRITICAL RISK**

An attacker with dashboard access raises the leak alert threshold so real leaks never trigger an alert.

Likelihood: Medium · Impact: Critical · Risk: Critical

R **Repudiation** **HIGH RISK**

An operator triggers the emergency shutoff and later denies it, and no log records which account clicked or when.

Likelihood: Medium · Impact: High · Risk: High

I **Information Disclosure** **MEDIUM RISK**

An attacker with dashboard access exports a year of consumption history for the whole hotel in one click.

Likelihood: Medium · Impact: Medium · Risk: Medium

D **Denial of Service** **CRITICAL RISK**

An attacker floods the dashboard login with requests so operators cannot see readings during an active leak.

Likelihood: High · Impact: High · Risk: Critical

E **Elevation of Privilege** **CRITICAL RISK**

A view-only account exploits a bug to send valve commands that should be reserved for admin operators.

Likelihood: Medium · Impact: Critical · Risk: Critical

HYDROLOGIC Devices

The three flow devices on the water lines: Main Building, Pool and Spa, Kitchen and Laundry.

S **Spoofing** **HIGH RISK**

A fake device on the hotel network registers as the Pool and Spa unit and reports normal flow during a leak.

Likelihood: Medium · Impact: High · Risk: High

D **Denial of Service** **HIGH RISK**

An attacker jams the wireless signal near the Kitchen and Laundry line so readings stop for an hour.

Likelihood: Medium · Impact: High · Risk: High

Cloud API

The cloud service every reading passes through, feeding the dashboard, database, and reports.

I **Information Disclosure** — HIGH RISK

An unencrypted API connection lets an attacker on the network read every pressure reading in transit.

Likelihood: High · Impact: Medium · Risk: High

D **Denial of Service** — CRITICAL RISK

A flood of junk requests takes the Cloud API down, cutting the dashboard off from every device at once.

Likelihood: Medium · Impact: Critical · Risk: Critical

Remote Controls

Gate controls and the emergency shutoff. What the system DOES, the highest-stakes surface.

S **Spoofing** — CRITICAL RISK

An attacker sends a forged shutoff command that the gate accepts as if a real operator sent it.

Likelihood: Medium · Impact: Critical · Risk: Critical

E **Elevation of Privilege** — CRITICAL RISK

An attacker who reaches the gate controller pivots from it into the hotel internal network.

Likelihood: Medium · Impact: Critical · Risk: Critical

SECTION 5 OF 6

Risk Summary

CRITICAL **7 findings**

Web Dashboard, Spoofing: An attacker uses a phished operator password to log into the dashboard from outside the hotel and gains full control of the water system. — TOP 3 FOR MARCUS

Web Dashboard, Tampering: An attacker with dashboard access raises the leak alert threshold so real leaks never trigger an alert.

Web Dashboard, Denial of Service: An attacker floods the dashboard login with requests so operators cannot see readings during an active leak.

Web Dashboard, Elevation of Privilege: A view-only account exploits a bug to send valve commands that should be reserved for admin operators.

Cloud API, Denial of Service: A flood of junk requests takes the Cloud API down, cutting the dashboard off from every device at once. TOP 3 FOR MARCUS

Remote Controls, Spoofing: An attacker sends a forged shutoff command that the gate accepts as if a real operator sent it. TOP 3 FOR MARCUS

Remote Controls, Elevation of Privilege: An attacker who reaches the gate controller pivots from it into the hotel internal network.

HIGH 4 findings

Web Dashboard, Repudiation: An operator triggers the emergency shutoff and later denies it, and no log records which account clicked or when.

HYDROLOGIC Devices, Spoofing: A fake device on the hotel network registers as the Pool and Spa unit and reports normal flow during a leak.

HYDROLOGIC Devices, Denial of Service: An attacker jams the wireless signal near the Kitchen and Laundry line so readings stop for an hour.

Cloud API, Information Disclosure: An unencrypted API connection lets an attacker on the network read every pressure reading in transit.

MEDIUM 1 finding

Web Dashboard, Information Disclosure: An attacker with dashboard access exports a year of consumption history for the whole hotel in one click.

SECTION 6 OF 6

Recommended Mitigations

Remote Controls, Spoofing CRITICAL RISK TOP 3 FOR MARCUS

Device certificates with mutual TLS, plus timestamps and nonces on commands. The gate only accepts commands from an authenticated sender (Week 6), and a captured command cannot be replayed later (Week 7).

Web Dashboard, Spoofing CRITICAL RISK TOP 3 FOR MARCUS

Strong authentication for operator logins, plus network segmentation and audit logs. The unauthorized access defense from the Attack Lab: a stolen password alone stops being enough, and every login leaves a record.

Cloud API, Denial of Service CRITICAL RISK TOP 3 FOR MARCUS

Rate limiting and redundancy. The denial of service defense from the Attack Lab: the API sheds junk traffic and stays up for the real devices.

Web Dashboard, Tampering CRITICAL RISK

Strong authentication and audit logs. Changing an alert threshold requires a verified operator, and the change is recorded, so a silent edit stops being silent.

Web Dashboard, Repudiation HIGH RISK

Audit logs for every action. Every shutoff and valve change records which account acted and when, so a denied action can be settled by the record.

Web Dashboard, Denial of Service CRITICAL RISK

Rate limiting and redundancy. The denial of service defense from the Attack Lab: junk traffic gets throttled before it can lock operators out.

Web Dashboard, Elevation of Privilege CRITICAL RISK

Strong authentication and audit logs. Command permissions are checked on every request, not just at login, and every command leaves a record.

HYDROLOGIC Devices, Spoofing HIGH RISK

Device certificates with mutual TLS. The spoofing fix you will build in Week 6: a device proves who it is before the system believes a single reading.

HYDROLOGIC Devices, Denial of Service HIGH RISK

Redundancy across water lines and alert paths. With overlapping coverage, one jammed device cannot blind the system to a leak. Rate limiting still guards this path against network floods.

Cloud API, Information Disclosure HIGH RISK

TLS encryption on the connection. The eavesdropping fix you will build in Week 4: readings travel encrypted, so an attacker on the network sees nothing useful.

Remote Controls, Elevation of Privilege CRITICAL RISK

Network segmentation, plus strong authentication. Reaching one controller stops meaning reaching everything: the controls live on their own network slice, behind their own logins.