### **AirWatcher Security Risk Analysis**

| **Asset** | **Vulnerability** | **Attack Type** | **Potential Risk** | **Impact Level** | **Countermeasures** |
| --- | --- | --- | --- | --- | --- |
| Recovered air condition data | Inadequate password policies | Brute-force attack | Unauthorized account access | High | Enforce strong password policies and regular rotations |
| Data transfer to databases | Lack of secure transmission | Man-in-the-middle attack | Data interception and manipulation | High | Implement SSL/TLS encryption and digital certificates |
| Sensor and user data in the database | Insufficient access controls | Unauthorized access | Data leakage or unauthorized modification | Medium | Apply principle of least privilege, encrypt data at rest, and monitor for unusual access patterns |
| System operability | Single point of failure (server) | Power outage | System downtime and potential data loss | High | Deploy backup power solutions and redundant systems |
| Sensor data integrity | Malicious data tampering by users | Data corruption | Ingestion of false data | High | Implement anomaly detection systems and user behavior analysis |
| Unencrypted data | Unsecured data storage and transmission | System intrusion | Uncompensated data exposure | Medium | Utilize end-to-end encryption for data transmission and storage |
| Input data validation | Lack of input sanitization | Injection attacks | Storage and processing of erroneous data | High | Enforce strict input validation and sanitization processes |

### 

| **Level** | **Description** |
| --- | --- |
| **High** | 1. Very costly loss of major tangible assets or resourcesA 2. Significant violation of, or harm or impediment to, an organization's mission, reputation, or interest |
| **Medium** | 1. Costly loss of tangible assets or resources 2. Violation of, or harm or impediment to, an organization's mission, reputation, or interest |
| **Low** | 1. Loss of some tangible assets or resources 2. A noticeable effect on an organization's mission, reputation, or interest |

| System | Asset | Vulnerability | Attack | Risk | Impact level | Countermeasures |
| --- | --- | --- | --- | --- | --- | --- |
| AirWatcher | Recovered air condition data | Weak password are allowed | the attacker can guess the password | the attacker hold the access to account | High | Weak password are not allowed |
| data transfer to databases | man in the middle | Information leakage or manipulation | High | Use digital certificates to validate the identity of sensors and the central server |
| sensor data and user data stored on database | Unauthorized access to functions or data | The attacker can leak data are modify them | Medium | data encryption, access management and suspicious activity monitoring |
| server dependency | power outage | lost of data not saved | High | use an emergency generator |
| unusable application |
| Recovered data may not correspond to reality | Private user may act maliciously and corrupt their sensor | Data are false | High | User with corrupted data are flagged in our database |
| Data transmission and storage without encryption | a user enters the system | an unauthorized user gains access to the data | Medium | Encryption of data |
|  |  | The data entered is not validated | Private user may act maliciously and corrupt their sensor | saved data are wrong | High |  |

| **Level** | **Description** |
| --- | --- |
| **High** | 1. Very costly loss of major tangible assets or resourcesA 2. Significant violation of, or harm or impediment to, an organization's mission, reputation, or interest |
| **Medium** | 1. Costly loss of tangible assets or resources 2. Violation of, or harm or impediment to, an organization's mission, reputation, or interest |
| **Low** | 1. Loss of some tangible assets or resources 2. A noticeable effect on an organization's mission, reputation, or interest |

Liste de questions :

1. L’application tourne en local mais ducoup niveau sécurité nous avons pas à gérer les données? serveur
2. L'application est elle sur un serveur donc on peux avoir des attaques réseaux?
3. Les données sont-elles cryptées ?
4. Les fichiers sont-ils protégés par des mots de passe ?
5. Il n'y a pas de requête au serveur pouvant être atteinte ?
6. Pas de base de données que des fichiers ?
7. Où se trouve le centrale de application ?
8. L’utilisateur peut-il se connecter sur un appareil ? yes need to know who is connectedno