# Risk Register

**Atlas Industrial LLC – Risk Register (Stage 3: Risk & Threat Modeling)**

## 1. Web Application Attack Surface (Tryton)

**System:** Tryton
**Source:** Tryton documentation cites brute-force login, SQL injection, and XSS as primary risks for browser-based ERP systems.

Tryton Documentation

| Item | Details |
|---|---|
| **Threat** | Web-based attacks (brute force, XSS, SQL injection) |
| **Vulnerability** | Public-facing login page, weak input validation, outdated web components |
| **Likelihood** | **High** |
| **Impact** | **High** — ERP manages inventory, production workflows, customer data |
| **CIA Impact** | **C: High, I: High, A: Medium** |
| **Risk Level** | **High** |
| **Mitigation** | MFA, rate limiting, WAF rules, hardened Docker configuration, encrypted communication, secure coding settings |

## 2. Database Service Exposure

**System:** PostgreSQL Database
**Source:** PostgreSQL documentation describes this as a major risk if port 5432 is exposed publicly.

PostgreSQL Documentation

| Item | Details |
|---|---|
| **Threat** | External attacker exploiting exposed database port (5432) |
| **Vulnerability** | Open port exposure, brute-force attacks, SQL injection attempts |
| **Likelihood** | **Medium** (common attack vector) |
| **Impact** | **High** — Database holds financial, inventory, and customer data |
| **CIA Impact** | **Confidentiality: High**, **Integrity: High**, **Availability: Medium** |

| Item | Details |
| --- | --- |
| **Risk Level** | **High** |
| **Mitigation** | Firewall rules, network segmentation, disable remote access, enable TLS, strong passwords, change default port |