# AutoSecure Agent – High Level Design (HLD)

## Overview

AutoSecure Agent is an AI-powered GitHub integration designed to automatically detect and remediate vulnerabilities in Java-based enterprise applications.

It leverages static code analysis, Software Bill of Materials (SBOM) scanning, and Large Language Models (LLMs) to identify outdated dependencies, deprecated APIs, and insecure code patterns. It then applies secure upgrades and automatically submits Pull Requests (PRs) to modernize applications—ensuring they remain compliant and secure without breaking existing functionality.

AutoSecure is ideal for financial institutions like Danske Bank seeking to embed secure coding practices and DevSecOps automation in their CI/CD pipelines.

## Architecture Overview

1. GitHub Repo Fetcher: Pulls the codebase via GitHub API.  
2. Static Analyzer: Scans code using OWASP/Snyk for CVEs and deprecated APIs.  
3. AI Assistant (GPT-4): Recommends code upgrades and secure replacements.  
4. Refactoring Engine: Rewrites code using AST/LLM suggestions.  
5. Validator: Builds and tests code to ensure safety and functionality.  
6. GitHub PR Generator: Opens automated pull requests with changelog and fix summary.  
7. Optional UI: CLI/Web interface to trigger and monitor remediation jobs.

## Core Components

🔁 GitHub Integration  
- Authenticates and fetches repository code.  
- Pushes updated branches and creates pull requests.

🧪 Static Analyzer  
- Uses OWASP Dependency Check or Snyk CLI for CVEs.  
- Detects deprecated Spring APIs with JavaParser or Spoon.

🧠 AI Assistant  
- Uses OpenAI GPT-4 for secure refactoring suggestions.  
- Prompts include method migration, security upgrade, etc.

🔧 Refactoring Engine  
- Applies safe changes to code and configuration files.  
- Updates pom.xml/build.gradle for dependency upgrades.

🛡️ Validator  
- Performs Maven/Gradle builds.  
- Runs unit/integration tests to validate code changes.

📦 GitHub PR Generator  
- Automatically opens PR with changelog, summary and labels.

## Tech Stack

| Layer | Technologies |  
|------------------|--------------------------------------|  
| Language | Java, Python |  
| Vulnerability Scan| OWASP Dependency Check, Snyk |  
| Code Parsing | JavaParser, Spoon |  
| AI Suggestions | OpenAI GPT-4 API |  
| Build System | Maven, Gradle |  
| Testing Framework | JUnit, TestNG |  
| GitHub Integration| GitHub API, GitHub Actions |  
| Optional UI | React, Tailwind CSS, Node.js CLI |

## Security Considerations

- Uses scoped GitHub tokens with minimal write access.  
- Does not upload full codebase to external systems.  
- GPT prompts limited to relevant code snippets.  
- Logs and audit trails for every transformation.

## Implementation Roadmap

Phase 1: MVP  
- Input: GitHub repo URL  
- Output: Scan → Fix → PR flow

Phase 2: AI-assisted Refactor  
- Integrate GPT-4 to convert deprecated functions

Phase 3: UI & Jenkins CI Integration  
- Trigger via dashboard or CI events

Phase 4: Multi-language & Plugin Ecosystem  
- Support for Node.js, Python  
- Jenkins/GitHub App

## Summary

AutoSecure Agent addresses a critical DevSecOps need by embedding AI-powered security remediation directly into the GitHub workflow.

It enables proactive vulnerability fixing, saves developer time, reduces compliance risk, and accelerates modernization efforts. For Danske Bank, this agent strengthens secure software delivery, ensuring that Java-based platforms stay resilient, updated, and production-ready.

Tagline: Upgrade. Secure. Repeat — with AutoSecure.