algosec

Secure application connectivity.
Anywhere.

Implementing security as code in the SDLC
Enhanced guidelines

To effectively implement security as code, security practices must be implemented throughout the entire software development lifecycle (SDLC). Here's a set of guidelines to help achieve this:

1. Planning

- ☐ Security requirements documented, reviewed and prioritized
- ☐ Threat analysis completed and risks assessed
- ☐ Compliance with relevant regulations verified
- ☐ Team alignment on security objectives established

2. Development

- ☐ Threat modeling completed and vulnerabilities identified
- ☐ Secure design principles applied throughout the architecture
- ☐ Security testing strategy defined and integrated into the SDLC

3. Implementation

- ☐ Secure coding standards followed and enforced
- ☐ SAST and other code analysis tools integrated into the CI/CD pipeline
- ☐ Third-party libraries and dependencies regularly assessed for security