Overview

The secure Software Development Lifecycle (SDLC) at ROAR outlines the procedures, policies, and security measures that govern how software changes are managed, implemented, and deployed within the ROAR platform. The SDLC process ensures that changes to the system are tracked, reviewed, tested, and implemented in a manner that prioritizes security, confidentiality, and compliance with industry best practices.

Changes to ROAR are managed via GitHub, where GitHub Issues, Projects, and Pull Requests serve as the core tools for ticketing, prioritizing, and tracking change requests throughout the SDLC process.

Environment Segregation

To maintain the integrity, security, and stability of the ROAR platform, separate environments are used throughout the SDLC process.

- Emulated Environment: This ephemeral environment exists only on ROAR developers' local machines during development.
- Development Environment: Used by developers for implementing and testing code changes.
- Staging Environment: A controlled environment where QA testing occurs, and the security review is conducted.
- Production Environment: The live environment where only authorized personnel can deploy changes. Developers do not have direct access to this environment.

Environment segregation ensures that development, testing, and production activities occur in isolated, controlled spaces. This approach minimizes the risk of unauthorized changes, enhances the accuracy of testing, and protects the production environment from potential disruptions.

Roles and Responsibilities

The ROAR development team comprises the following roles:

- Developer: Responsible for developing the changes according to specifications in the ticket and ensuring all tests pass.
- QA Team: Responsible for testing the change in the Staging environment.
- Information Security Officer: Responsible for reviewing the security checklist and ensuring the change meets all security and compliance requirements.
- Director of Technology and Innovation: Responsible for authorizing and approving changes before deployment to the production environment.

SDLC Process

The following steps outline the full SDLC process for managing code changes:

1. Change Request:
    - Any change, whether a new feature requests or a bug fix, begins with the creation of a ticket.
    - Tickets are logged and prioritized using GitHub Issues in the centralized ROAR repository. Each ticket should document the required change, the impact of the change, and any relevant security, confidentiality, and privacy considerations.
    - ROAR maintains issue templates to assist issue authors in providing required information.
2. Change Development:
    - Code changes are first developed in either the Emulated environment (local developer machines) or the Development environment.
    - Before changes can be merged into the main branch, they must:
        1. Pass automated tests that run in either the Emulated or Development environment to ensure code correctness.
        2. Pass automated security vulnerability scanning managed by GitHub's CodeQL tool.
        3. Undergo a line-by-line code review by at least two authorized developers.
        4. Pass acceptance testing that validates the relevant behavior of the feature or bug fix.
    - Once the above steps are completed, the code can be merged into the main branch via a pull request.
    - After merging, the code is automatically deployed to the Staging environment for further testing.
3. Change Testing:

    In the staging environment, changes undergo

    - Quality Assurance (QA) testing to validate functionality and performance.
    - A security review to assess potential impacts on security, confidentiality, and privacy.
    - Automated pre-deployment tests that verify the code's readiness for production. Vulnerabilities must be addressed before changes can move from staging to production.
4. Change Approval and Deployment:
    - Approval for code changes is required before they can be merged into production.
    - The ROAR Director of Technology and Innovation or their designee reviews and authorizes changes. Individual developers cannot deploy code directly to the production environment.
    - Approval is recorded by minting a new version number tag and release on GitHub. These actions then trigger deployment through GitHub actions.

5. Post-Deployment Monitoring:

   Once in production, changes are monitored to ensure the system operates as expected, with a focus on identifying any security or operational issues that may arise.

Security Controls

The SDLC process integrates the following security controls to ensure the safety and integrity of the ROAR platform:

1. Access Control

   Access to ROAR GitHub repositories is restricted to authorized personnel only. All users must use two-factor authentication (2FA).

2. Code Review

   - All pull requests must undergo code review before being merged into the master branch.
   - ROAR repositories are configured to enforce code reviews by designated code owners. Code cannot be merged without an approving review.

3. Code Vulnerability Scanning

   - CodeQL scanning is integrated into GitHub to detect vulnerabilities and coding errors in the source code.
   - Dependency Review via GitHub's Dependabot tool automatically detect vulnerabilities in third-party dependencies.
   - High or critical issues must be remediated before a change can proceed through the SDLC.

4. Automated Tests

   - Automated tests are run via GitHub Actions for each pull request. These tests include:
     - Code linters to check for style and formatting issues.
     - Security checks to ensure the codebase remains free from vulnerabilities.
     - Functional tests to verify code correctness.
   - All tests must pass before proceeding to the next stage in the SDLC process.
   - Branch protection rules are applied to prevent merging changes with failed tests.

5. Change Approval

   - All code changes must be approved by the ROAR Director of Technology and Innovation or a designated reviewer.
   - Approval is required before deploying the change to production.

Conclusion

The ROAR Secure SDLC process ensures that all code changes are properly documented, tested, and reviewed, with security considerations integrated into each step of the lifecycle. By maintaining rigorous access controls, automated testing, vulnerability scanning, and structured approval processes, ROAR can protect the integrity and security of its platform throughout development and deployment.