

Secure Software Development Lifecycle (SSDL) Statement

At ReConfirm, we are committed to integrating security into every phase of our Software Development Lifecycle (SDLC). Our Secure Software Development Lifecycle (SSDL) approach is designed to identify, mitigate, and address security risks from the initial stages of design and development through to deployment and maintenance. The goal is to deliver secure, reliable, and compliant software that meets the highest security standards.

Key Principles of Our SSDL:

1. **Security by Design:** We embed security requirements from the outset by incorporating security-focused design principles and threat modeling in the architecture and design phases. Security requirements are treated as first-class citizens alongside functional requirements.
2. **Risk Assessment and Threat Modeling:** Before development begins, we conduct risk assessments and threat modeling exercises to identify potential vulnerabilities and attack vectors. This allows us to proactively address risks early in the lifecycle.
3. **Security Training and Awareness:** All developers, testers, and key stakeholders are provided with continuous security training to stay up to date with evolving threats, best practices, and secure coding standards.
4. **Secure Coding Practices:** Our development teams follow secure coding guidelines and industry standards such as OWASP and CWE. We ensure that code reviews include a focus on identifying and mitigating security vulnerabilities.
5. **Automated Security Testing:** Security testing is embedded in our CI/CD pipeline, incorporating static and dynamic analysis, dependency scanning, and automated security testing tools like SAST, DAST, and IAST to detect and fix vulnerabilities early.
6. **Vulnerability Management:** We maintain a robust vulnerability management process that includes regular scans, monitoring, and patching of software dependencies. We also integrate automated vulnerability detection tools into our testing workflows.
7. **Continuous Monitoring and Incident Response:** After deployment, we continuously monitor for potential security threats and vulnerabilities, ensuring rapid detection and response to any incidents. A dedicated security team manages this process, coordinating remediation efforts as needed.

8. **Compliance and Governance:** Our SSDL aligns with industry regulations, standards, and best practices such as ISO 27001, GDPR. We also conduct regular security audits and maintain documentation to ensure full compliance.
9. **Third-Party Security Assessments:** We regularly engage external security experts to perform penetration testing and code reviews to validate the security of our applications.
10. **Post-Release Review and Maintenance:** We ensure that security is maintained even after the release through continuous patching, updates, and security assessments. Any vulnerabilities discovered post-release are handled according to our incident response policies.

By adhering to the SSDL, we aim to continuously improve the security, reliability, and quality of our software solutions, protecting both our customers and stakeholders from potential security threats.

Revision #3

Created 28 October 2024 15:32:47 by Raphael

Updated 28 October 2024 15:34:10 by Raphael