Qualia

Qualia’s Secure Product Lifecycle

Overview

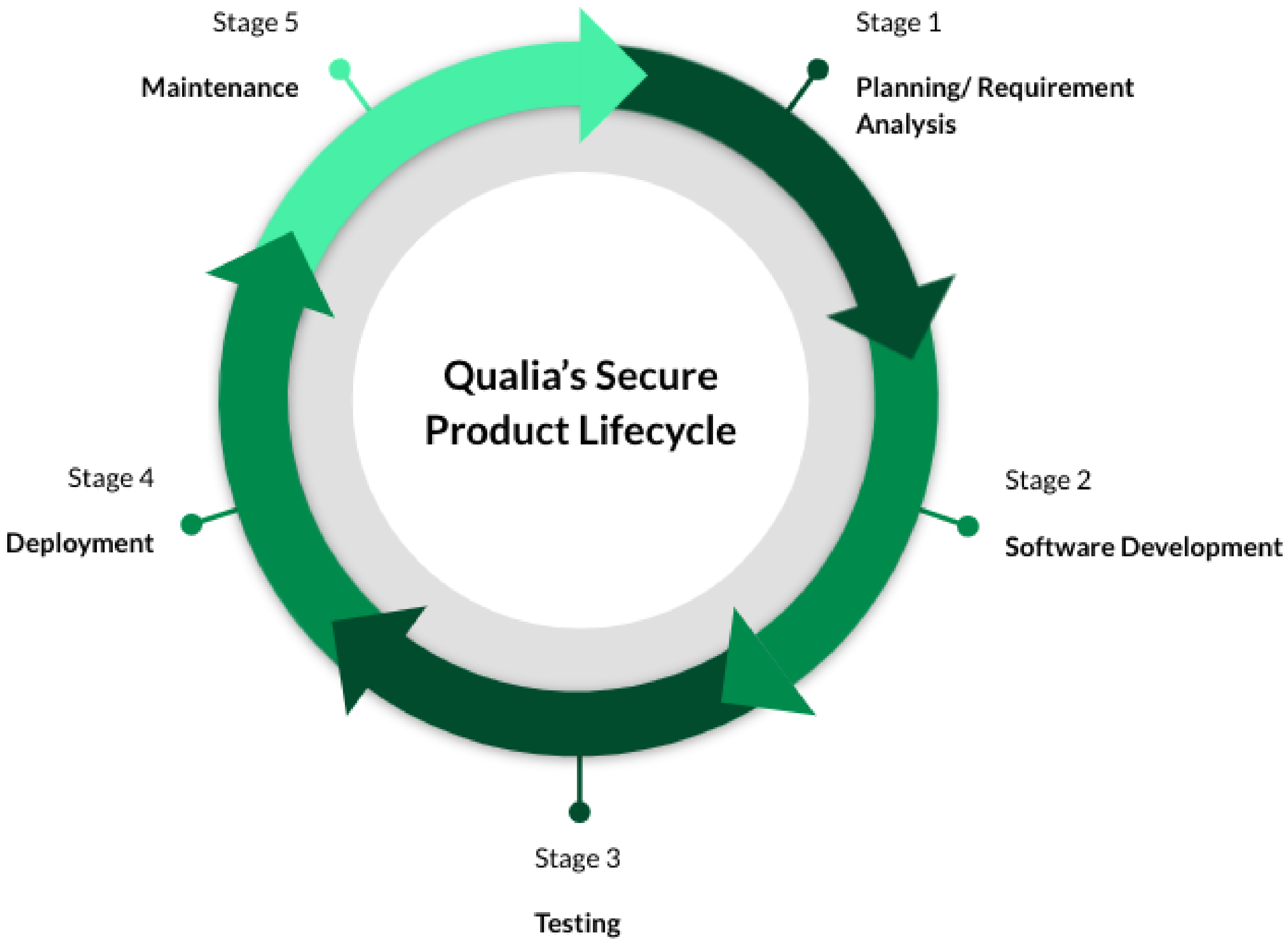
Security is embedded into every phase of Qualia’s product development lifecycle. Qualia has, from our early beginnings, committed extensive time, resources, and focused energy on the security of our users’ data and accounts. Before engineers wrote the first line of code at Qualia, they had already thought about security and the necessary architectural design.

The product and engineering teams at Qualia strive to develop technology that is scalable and future-proof to ongoing change. To achieve this, Qualia fully embraces agile development principles. This enables development and feature releases at a rapid pace as well as the ability to quickly adapt to changes in our customers’ business needs and the market. New functionality development and bug fixes are prioritized based on a combination of customer feedback and the company roadmap.

Qualia’s agile development process allows for code changes to be released every two weeks in a rolling deployment schedule. This regular release cycle is intended to help the engineering team manage new functionality development, fix bugs, ensure code fidelity and stability, prevent erroneous commits, facilitate peer code review and quality assurance (QA) testing, and ensure timely deployments.

As Qualia continues to build new features with our agile development process, our team prioritizes security during every step of the lifecycle development process planning to deployment and ongoing maintenance.

The 5 Stages of the Product Lifecycle



Stage 1: Planning and requirement analysis

Qualia builds features with a focus on customer success and security best practices. By continuously evaluating our current product offering, and comparing it to the expectations of our customers and the guidance of security standards, we can maximize our ability to deliver functional, intuitive, and secure products.

At Qualia, we want feedback—it helps our team understand our customers' challenges in order to provide them innovative, future-proof solutions that drive meaningful value to their business and the real estate industry as a whole. Security standards, such as those published by the National Institute of Standards and Technology (NIST), provide guidance on the ever-changing security landscape, allowing us to prioritize features and controls to improve the security of the product. Market forces also play an important role in shaping our product priorities. For example, local economic factors, legislative updates, and shifting consumer preferences.

As part of the "requirement analysis" phase of our product development lifecycle, our product team collaborates directly with customers, Qualia's customer-facing teams, and internal Qualia teams (such as our Security team) to identify pain points and opportunities for Qualia to optimize our products. Then, Qualia's teams determine what will be developed to meet these needs.

Stage 2: Software development

Qualia's engineers are extensively trained in best practices for software development, both during onboarding and continually throughout their employment at Qualia. Continuing education happens via code reviews, participation in educational efforts from the broader software development community on the latest security threats and tactics used to mitigate them.

When Qualia engineers are ready to start work on a new feature or bug fix, they open a new Pull Request (PR). The PR must contain a thorough description of the feature or bug fix that is being proposed, instructions on how to test the change for quality and security, and an estimated release date for the change.

Once a PR is in Review/QA, it will be reviewed and tested. All new features and bug fixes must undergo code review, QA, and design review (if appropriate). Additionally, Static Application Security Testing (SAST) is performed during this stage, in which the modified code is automatically analyzed for software bugs or security flaws. If identified, these items are flagged for review and improvement before the Testing phase can begin.

Stage 3: Testing

Every two weeks, a release candidate (RC) is cut from the contents of the development branch, and testing begins by the team of QA engineers. Any issues that arise during RC testing are immediately triaged and appropriate engineering resources are pulled in to resolve the issues.

As part of the testing phase, Qualia undergoes vulnerability assessments and source code reviews to determine the security of our application, architecture, and implementation. Dynamic Application Security Testing (DAST) is a form of vulnerability assessment that can be conducted during this phase, during which a version of the application running in a test environment is provided intentionally-malicious input, and its responses are examined for evidence of security flaws.

Qualia works closely with external security experts, periodically commissioning penetration tests to review the security of the platform and applications and to apply best practices. This includes testing for vulnerabilities in the Open Web Application Security Project (OWASP) Top Ten, which ranks the top ten most critical web application security risks based on the consensus of the leading security experts around the world. This regularly updated, online report on OWASP's website provides developers and web application security teams with guidance on how to mitigate security risks in the software.

Stage 4: Deployment

Once RC issues have been resolved and the lead QA engineer signs off on the build of the feature or bug fix, the process of deploying to production begins.

At this stage, the engineer who developed the code cannot deploy it into production. This Separation of Duties (SoD) ensures that unauthorized code cannot be either maliciously or accidentally pushed into production. Two to three team members other than the code engineer push the feature or bug fix into production in waves over the course of several days. If issues are identified with the new release at any point, the issues are immediately triaged. Qualia's standards require that a fix must be made before the new release is sent to the next wave of deployments.

Stage 5: Maintenance

Once a new release takes place, it is then monitored for quality assurance and any security risks. Every individual service component in Qualia logs activity and security events to a centralized logging service which is actively monitored by our engineering staff. Security logs are kept for at least one year. Identified incidents are treated with the utmost priority and are worked on 24/7 until resolution.

For additional information, see *How Qualia Protects Against & Responds to Security Threats*, here.

© 2022 Qualia Labs, Inc. All rights reserved.