iQuila Security Development Lifecycle
Effective Date: 19-September-2019

1. Planning

The purpose of this phase is to find the scope of the problem and determine solutions. Costs, Resources, time, and benefits. Security is our top priority. We use industry standard tools that assist in finding vulnerabilities in source code or discovering vulnerabilities in a running instance of the product or application.

2. Analysis & Requirements

Our team work out the functional requirements of the solution. System analysis takes place, analyzing the needs of the end users to ensure the new system will meet expectations. Requirements exist to define the functional security requirements implemented in the product. Threat modeling is the process of thinking through how a feature or system will be attacked, and then mitigating those potential issues.

3. Systems Design

Detailing the specifications, features and operations satisfying the functional requirements. We use standard approach to securing our products.

4. Development

Process to determine the best way of satisfying requirements.

5. Integration & Testing

Integration of solutions with Quality Assurance of the proposed design changes to determine satisfaction of the functional requirements.

6. Implementation

Code is written and tested. Implementation tools include static application security testing (SAST) and dynamic application security testing (DAST) software. With DAST checking the application's runtime instantiation. Vulnerability scanning uses industry-standard tools to determine if any system-level vulnerabilities exist with the application, product, and operating system.

7. Maintenance Release

Release occurs when all the security activities are confirmed against the final build and the software is sent to customers (or made available for download).

