Qualitest Implements Shift-Left Cyber Security for Leading Medical Devices Company

Challenge

Bringing in security in the early stage of development lifecycle.

Automating cyber security test cases just like any other functional test cases.

Solution

Identified security requirements and started designing security test cases at the early stages of the SDLC.

Identified the candidates for test automation and automated using the test automation framework.

Results

The Client was able to perform cyber security testing at a much earlier stage of development.

The Client was able to automate cyber test cases and execute to identify any vulnerabilities as part of regression.

The Client is a German-based multinational biomedical technology company. It offers equipment for diagnosis, treatment, and therapy support in the areas of cardiac rhythm management, electrophysiology and vascular intervention.

The company’s extreme high standards of quality and the safety of its end-customers demand flawless development and results. The Client always strives to be at the forefront of development and innovation, as well as improving its processes.

With more than 9,000 employees around the world in over 100 countries, the company invests heavily into R&D as well as produce all critical components of its products in-house.

Healthy Security = Secured Health

The Client wanted to introduce cyber security solutions at the early stage of the development lifecycle. Since the Client develops medical devices, cyber security is one of their key concerns in order to protect Patient PII and the safety of patients.

The Client had a traditional testing approach, employing penetration testing of applications to identify any vulnerabilities, which wasn’t very efficient or effective as the cost to fix issues is high and also doesn’t provide complete coverage of cyber security for all aspects of the product.

Qualitest proposed a solution to the customer to address cyber security requirements as early as possible in the development lifecycle and to automate cyber requirements to reduce the effort, without reducing the coverage as part of the cyber security activity.

The objective was to go through all the cyber security requirements and identify tests that could be automated. Qualitest designed all the test cases as per the requirements and automated the majority of the test cases, executing some tests manually in parallel to functional testing to identify vulnerabilities. The test cases included static code inspection as well to enable better coverage for many requirements.

> **“Since the Client develops medical devices, cyber security is one of their key concerns in order to protect Patient PII and the safety of patients.”**

Qualitest worked with the Client to build a strong cyber security testing plan that would accommodate cyber security test automation, code inspection and manual execution of the cyber security test cases.

The Client wanted to:

- Establish a QA partner that has extensive knowledge and experience on shift-left cyber security implementation.
- Translate cyber security requirements into automated tests.
- Perform code inspection and manual test execution to identify vulnerabilities at the early stage of development lifecycle.
- Execute automated test cases regularly to identify any vulnerabilities as part of the regression pack.

Shifting-Left Security Makes a World of Difference

The Client was following agile methodology with the release-based approach for developing their medical device product. Qualitest began work in three phases:

- **Phase 1** – Completion of 50% of the test cases with the majority of the tests being automated.
- **Phase 2** – Performing the remaining 50% of the test case execution with the majority of the tests being automated.
- **Phase 3** – Executing the automation test cases as part of the regression pack to identify any vulnerabilities.

Phase 1 – Completion of 50% of test cases

In this phase, Qualitest reviewed all the requirements defined for the product to identify requirements that can be automated, needed code inspection or to be manually tested. We created a detailed test plan for the entire project, which detailed the approach we take for testing, the risks, the mitigation plans, and more.

Qualitest then designed the manual test cases for 50% of the requirements and identified the test cases that could be automated, as well as the tools required to execute the cyber test cases.

We leveraged the functional test automation framework and automated the cyber security testing requirements and executed the automated tests as part of the Client's build pipeline in the cloud environment.

Phase 2 – Performing remaining 50% of the test case

In this phase, Qualitest took the remaining 50% of the requirements and designed the test cases for it. The tests that could be automated were identified and test scripts were designed accordingly.

There were many tests that required code inspection to validate the implementation, especially the requirements on cryptography, Bluetooth communications, Debug Logs verification, code obfuscation, etc. The code inspection tests were designed for these requirements and the source code validation was performed accordingly.

All the identified cyber test cases were automated and executed on a regular basis to identify any vulnerabilities that application might have. Executing the automation test, performing code inspection and manually execution of the cyber security tests had resulted in identifying vulnerabilities in earlier stage of development lifecycle.

Phase 3 – Regression Test Execution

In this phase, Qualitest executed all the tests as part of the regression testing on a regular basis. Any vulnerabilities identified during the execution were shared with the Client to fix. Since more than 50% of the test cases were automated, the regression testing effort was reduced predominantly for cyber security testing.

> **“Qualitest enabled identification of vulnerabilities at the early stage of the development lifecycle.”**

Key Benefits

Qualitest was able to meet all the Client's stated goals within the allotted time frame:

- **Automated more than 50%** of cyber security test cases.
- **Identified and designed the code inspection and manual test cases** for cyber security testing requirement.
- **Enabled identification of vulnerabilities** at the early stage of the development lifecycle.
- **Leveraged the functional automation framework** to perform cyber test case automation.
- **Executed cyber automation test cases** on all the new builds.
- **Reduced regression testing effort** on cyber security through automation.
- **Enabled performing cyber security testing** at both static and dynamic level.
- **Fixed vulnerabilities** with the developers.

> **“Qualitest worked with the Client to build a strong cyber security testing plan that would accommodate cyber security test automation, code inspection and manual execution of the cyber security test cases.”**

QUALITEST

Connect with Us

www.qualitestgroup.com

https://www.linkedin.com/company/qualitest
https://www.instagram.com/lifeatqualitest
https://twitter.com/Qualitest
https://www.facebook.com/Qualitestgroup