CYBER SECURITY DIVISION

# Qualizer and DevSecOps: security into DevOps approach

November 2021



LEONARDO

## APPLICATION SECURITY

A faster development of software systems, the compliance with requirements, built through collaborative team relationships, the continuous release of applications - also using tools for release automation - the continuous monitoring and optimization of applications are some of the features that are distinctive of the DevOps approach. An approach to quickly develop flexible systems and applications guaranteeing their quality.

Software systems and applications must also comply with security requirements to deal with increasingly concrete and potentially harmful cyber threats for the correct behaviour of services and, above all, for the security of data.

The application of security policies “a posteriori”, i.e. after the development of software systems, does not allow an optimal management of cyber security and often leads to rewrite entire portions of code, thus generating extra costs, inefficiencies delays in deliveries, low quality and low interventions’ effectiveness.

For this reason, the DevSecOps approach introduces the security management of software applications from the earliest stages of their design thus ensuring high security standards thanks to the continuous integration between security specialists and developers, to the information sharing relating to known vulnerabilities, to the application of best practices and the automation of security controls.

## THE APPROACH TO SECURE DEVELOPMENT

Leonardo's Cyber Security Division offers an approach based on a complete framework to support the design and implementation of secure software systems throughout the development cycle. This approach, on which our Qualizer solution is based, consists of a consolidated methodology, a platform and a portal for project management and access to the knowledge base.

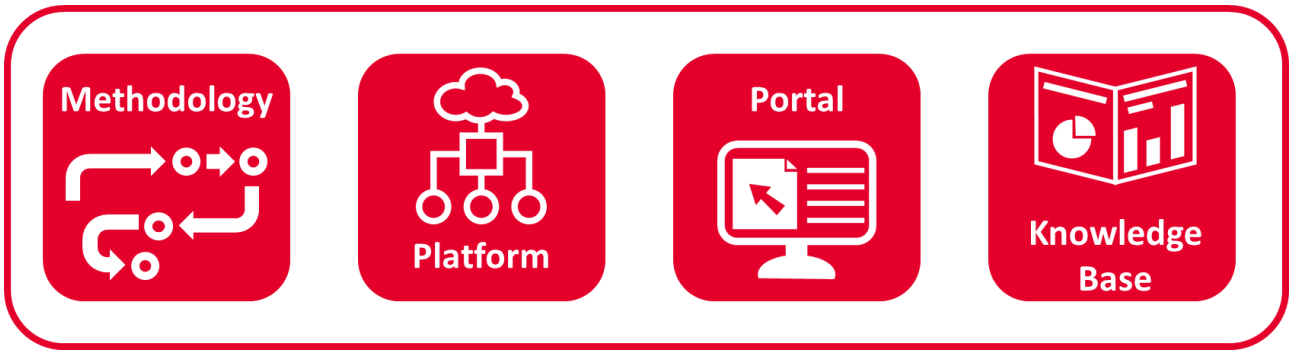


**Figure 1** – Qualizer’s pillars

## The methodology

The methodology is divided into phases that address the Continuous Integration and Continuous Development components of the DevOps approach with the aim of ensuring the software's quality. It is integrated with activities focused on the security of development projects. Risk analysis, threat modelling, static software analysis and dynamic analysis of running applications allow the production of secure source code and applications.

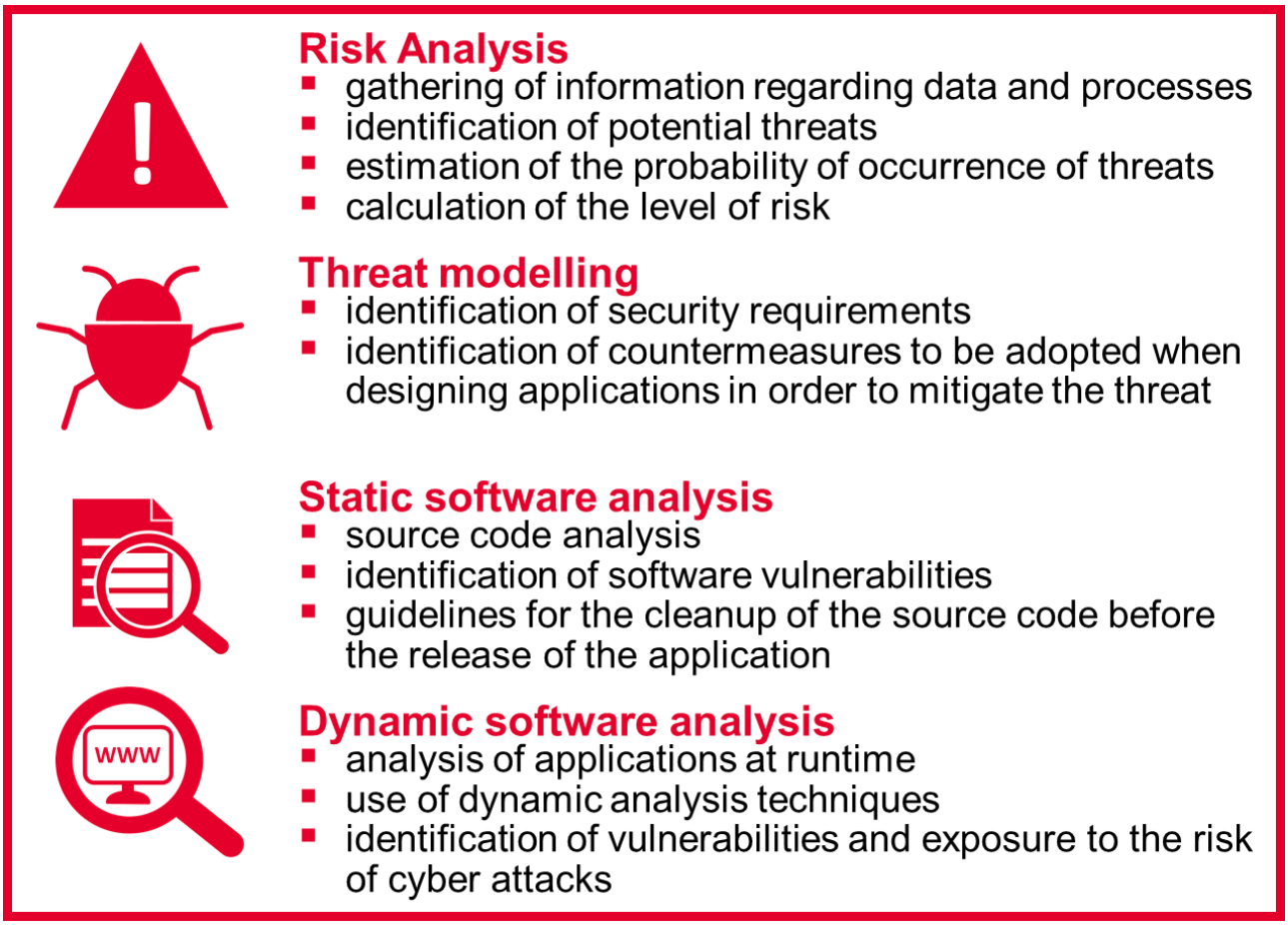


**Figure 2** – Qualizer's methodology

Leonardo's Cyber Security Division also supports the verification, monitoring and management process of application compliance (in the security and privacy field), through a specific tool to measure the "as is" maturity level of the application security and privacy requirements and suggests the most suitable action plan of to achieve the level of compliance required by the reference regulatory context.

## The platform

The platform, available on premises, in cloud or in hybrid mode, allows to perform all the activities needed to manage software development projects, from planning to code compilation up to results' validation.

Through specific functions it is possible to carry out a wide range of tests, also in an automated way, in order to verify the compliance with functional requirements, performance, accessibility of the solutions developed, integration with other systems and correct functioning on different devices. The platform provides quality indicators and KPIs – that can be consulted through the portal – for the quality assessment of software projects and of the tests performed.

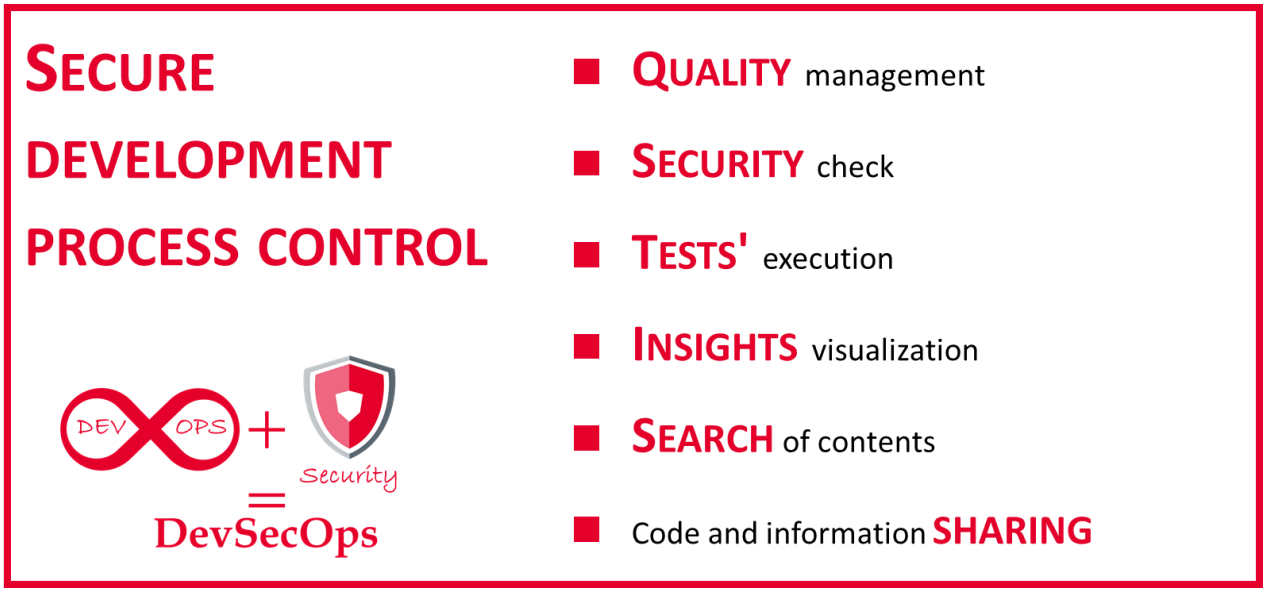


**Figure 3** – Qualizer's platform main functions

## The knowledge base

The knowledge base allows users to share information and to access sections containing tips, videos and tutorials for managing the DevSecOps process also through an advanced search feature available on mobile devices.

## The portal

The portal is the main access point to the platform functions and to the knowledge base. It allows the management of single software development projects, the verification of the project status, the sharing of the source code, the tracking of the activities carried out, the approvals of the various phases, the display of defects and indicators of quality, productivity, efficiency as well as those relating to the results of the tests performed.

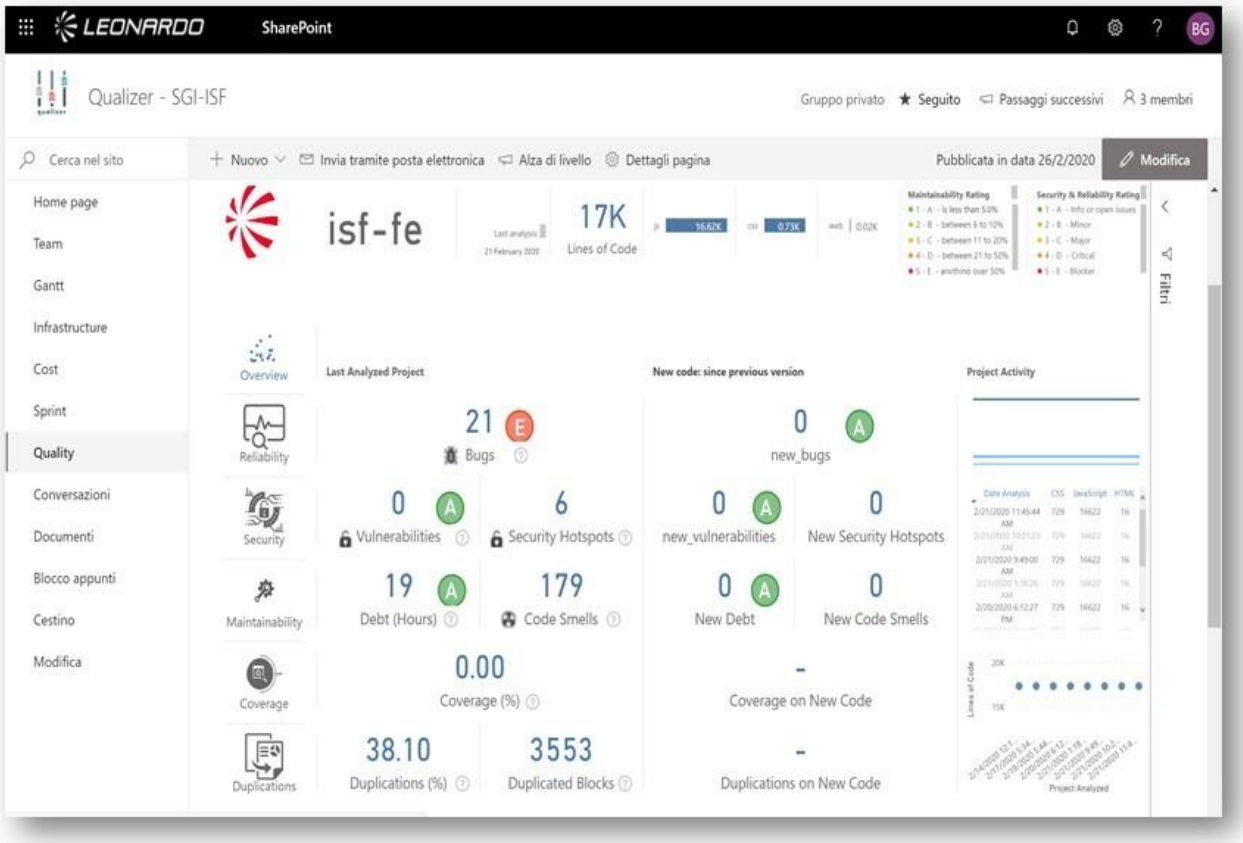


**Figure 4** – Qualizer's portal

Piazza Monte Grappa, 4
00195 Rome
T +39 06324731
F +39 063208621

**leonardocompany.com**