Translation from the original.

“We predict that CodeV will represent 10% of 2011's billing volume”

Dognædis launched this week it's program to detect software vulnerabilities and hopes to bill 600 thousand euros in 2011, reveals the start-ups' CEO, Francisco Rente.

Dognædis presented to the market its tool do detect software vulnerabilities, preparing already a version to be made available as a service (SaaS). The companys' CEO, Francisco Rente, expects a turnover of 600 thousand euros with the software until the end of 2011, as he revealed in an interview to ComputerWorld.

The start-up from researchers of the College of Science and Technology of the University of Coimbra shall turnover nearly 600 thousand euros, at the estimates of the executive. The CodeV is presented as an “intelligent inspector-professor that detects software security issues throughout all the phases of its development”. Sends alerts, produces reports and gives instructions to the fast correction of the identified vulnerabilities, says the responsible.

According to the company’s' communicate the software has been tested on the “40 largest free software existent on the market”. Some are used by the Portuguese State and CodeV has identified, in total, 28 vulnerabilities of the “zero-day” kind – security problems yet without known solution. These are problems that Dognædis promises to reveal in a “responsible manner”.

Computerworld – What business goal does the company have by launching this software? What weight can it represent on the company’s' income?

Francisco Rente – Dognædis has its “core business” in the sector of information security, having strategically began its activity as a services company. However, always had as a goal the creation of products through the knowledge and technology developed during the execution of such services.

CodeV is the first result of that cycle. It rises as a response to our “software assurance” teams necessities and aims to help ensure a high level of security to who produces and who acquires custom made software. We believe that CodeV will represent 10% of the billing of 2011, given it has only been launched this week. In 2012 it should represent 25%-35%.

CW – If the CodeV represents 10% of your sales, the rest should come from what? How much do you expect to turnover and grow this year?

FR – The other 90% of the invoice will be related to our range of services. The goal of the business volume for 2011, the first full tax year of activity as Dognædis (having inherited the client base of CERT-IPN), is of 600 thousand euros, being that we attained 70% of this goal at the end of the second trimester.

CW – Which is the business model of the tool?

FR – The business model we designed to CodeV comprehends three strands that will be launched by phases: “freemium”, SaaS, CodeV Appliance.

The first represents a way to give knowledge to the public of CodeV's capacities and receive feedback through an experimentation version, available with no costs. The second, available only a few months from now, represents an online service where the user may submit his software to periodical tests, receiving results focused on different needs (technical, quality control, project management...). And the last, representing the “ex-libris” of the product line, is an appliance to be installed on the clients' infrastructure, ensuring diverse communication channels with several interactions with the development cycle, namely code repositories and IDE.

Currently is available the “freemium” strand and a limited SaaS version (that requires our

validation and coordination).

CW – But in term of business volume, which will be the proportion in relation to the services surrounding the tool, face to the selling of the product?
FR - We believe that some of our services, namely the software architecture audit and consultancy and the Security Development LifeCycle (SDL) Consultancy will suffer a considerable increase, especially since these are services naturally required as a strong support to the work made by CodeV.

CW – When do you predict to have the complete version of the SaaS?
FR – The SaaS version, that basically represents a system to interact with the existent inference motor, shall be ready and presented in a few months.

CW – In the set of vulnerabilities of the "zero day" kind, which are the usually most neglected by programmers in general and the Portuguese in specific? Which are the most easily detected vulnerabilities by CodeV?
FR – One of the main sources of vulnerabilities on software is the incorrect validation of “inputs”. This is the most neglected sort of vulnerability and thus precisely the one that CodeV best detects.

CW – How does the software work? In what technology is it based? Is it opensource?
FR - CodeV works as an “intelligent agent” that analyzes the work and organic of a software, detecting possible points of security flaw (vulnerabilities). It is a technology developed by Dognædis that represents the result of several years of investigation. It is not opensource.

CW – Does CodeV only monitor the development on free software?
FR - CodeV has the capacity to analyze any sort of software developed in one of the programming languages it supports, being that software free or proprietary. The auditing

we made to a set of free software using CodeV arose not only as a form of contributing to the opensource community but also as a proof of efficiency of CodeV itself.

When a system (CodeV) detects vulnerabilities of software already audited by so many experts and several other auditing systems, it naturally proves the increased value it brings to the table. The disclosure of vulnerabilities in opensource software is being made in a responsible manner in the sense that we are articulating with the communities responsible by each of the software a joint disclosure of the vulnerability and its correction, ensuring that when the “problem becomes public” the solution is also known!

CW – CodeV is a direct competition of which other software platforms? How does it differ from them?

FR – There is some direct competition of our software on the global market, although with little expression (3 or 4). It differs from them in two aspects: on the inference motor, the algorithms and mechanisms of analysis and detections are more efficient, effective and capable of a more comprehensive detection of vulnerabilities; in the interaction with the software cycle and its protagonists.

It sustains information channels in real time and is focused on specific needs ensuring thus that only the relevant information gets to whom it should (divided between programmers, project managers, quality control, test team, security team...). These facts will be more expressive in the last strand of the business model described above.

Translation from the original.