Customer Success Story

Security

Vital Images

Vital Images completes DIACAP package with Micro Focus® Fortify Static Code Analyzer. Medical imaging software company leverages leading application security solution to penetrate DoD market.

Overview

Vital Images provides advanced visualization solutions for the healthcare industry. The company's software enables radiologists, cardiologists, oncologists, and other clinical specialists to view and analyze 2D, 3D, and 4D images of anatomy and physiological functions using computed tomography (CT) and magnetic resonance (MR) scan data. Advanced visualization enhances diagnostic confidence by enabling the care team to see more information and make more efficient measurements.

Challenge

Gold Standard

It's a slightly unusual use of Fortify Static Code Analyzer (SCA). Since its inception in 1988, Vital Images (now a subsidiary of Toshiba Medical Systems Group) has built a strong business through sales to clinics, hospitals, and other medical facilities across the country and around the world. Last year the company decided to expand its market to include the healthcare operations of the U.S. Department of Defense (DoD). Because the Department requires its vendors to achieve DoD Information Assurance Certification and Accreditation Process (DIACAP) certification for products sold to the Federal government—and because application security is a critical component of this complex accreditation package—Vital Images implemented Fortify SCA to scan its code base.

DIACAP is the DoD's process to demonstrate activity toward continuous improvement on the security front, helping to ensure that the information assurance posture of the system is maintained throughout its lifecycle. Among other things, it requires the vendor to have a baseline software assurance policy in place to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities.

In a nutshell:

- **It works**—Fortify finds vulnerabilities and helps developers be effective at remediating issues.
- **Language coverage**—Fortify covers 25 programming languages.
- **Updates**—Micro Focus Security Research translates cutting-edge security research into security intelligence that powers Fortify SCA, among other products in the Micro Focus Enterprise Security Products portfolio, through regular software security content feeds.
- **Support**—Fortify provides plug-ins which work with the most common IDEs (Visual Studio, Eclipse, etc.).

VITAL

A Toshiba Medical Systems Group Company

At a Glance

- **Industry**

  Healthcare

- **Location**

  United States

- **Challenge**

  Implement an approved code scanning process on key software to enable compliance with the DoD Information Assurance Certification and Accreditation Process (DIACAP).

- **Products and Services**

  Fortify Static Code Analyze

- **Results**

  + Compliance with DIACAP guidelines enables Vital Images to sell its medical imaging software to the U.S. Department of Defense
  + Brand protection through a formal commitment to software security assurance (SSA), with a downward trend in the number of vulnerabilities identified by Fortify
  + Competitive advantage from having built a formal SSA step into their software development lifecycle, resulting in enhanced code security

Solution

Enlightening

The primary development language at Vital Images is C++—arguably one of the harder languages to develop under and build, according to Tim Dawson, Senior Director of Software Engineering at Vital Images— and the company's code base is complex. That said, Principal Software Engineer Jeff Shuberg says Fortify SCA is now doing what it needs to do. "Fortify flagged some things as vulnerabilities that honestly I would not have seen had it not been for the tool, things where a complex combination of factors comprised the vulnerability. The average developer would probably not be able to see that particular vulnerability without some sort of tool that could analyze the code at that level." Vital Images currently runs scans in a centralized build location, and also ad hoc on developer machines as needed.

Vital Images has been running a weekly code scan for the past six months. Shuberg comes in to work on Monday and looks at the results, works with them, and sees what vulnerabilities have fallen out of the scan because they have been properly remediated. If something needs to be fixed, he and another team member generally do it themselves with input from the group that is most familiar with the code. Some of the code dates back a long time, and there isn't necessarily someone with first-hand knowledge, so it may take some research to ensure that the vulnerabilities are properly remediated. The following Monday, he looks at everything that was checked in and fixed from the previous week to verify that it has fallen off of the scan.

The results are encouraging. "Overall we are seeing a downward trend in the number of vulnerabilities that Fortify identifies as we work through the product," says Shuberg. "As we continue to refine our developer awareness and education, this trend should accelerate."

A process to help developers write more secure code, using the findings and remediation suggestions from Fortify scans, is in the works. According to Dawson, Vital Images will be scanning its entire code base, identifying the primary security issues, and providing guidance on alternate coding techniques to reduce introduction of new vulnerabilities.

Going forward, Vital Images plans to extend its use of Fortify SCA to other applications in its product suite. The company is currently using Fortify for VitreaAdvanced; VitreaWorkstation and VitreaView will likely be added in the future, along with modality workstations. Increased scan automation is also in scope. "We plan to actively use Fortify in our software development lifecycle and hope to have it fully automated into our processes," says Dawson. "We are currently devoting effort to making the scanning process fully automated with Fortify."

Results

Benefits

The broad language coverage of Fortify SCA is of particular importance at Vital Images. "What I like most about Fortify is the fact that it can scan pretty much anything," says Dawson. "That is absolutely critical for us. Even though we code primarily in C++, there are other languages that we use for development. It's nice to know that Fortify can be applied to everything."

Product enhancements continue to drive performance improvement. Initially, using version 3.x of Fortify SCA on the company's massive code base, a full scan of the company's imaging suite would take up to nine days. Since the introduction of v4.x with parallelization, the scan times have been reduced by as much as 66%. To take advantage of the new software architecture, Vital Images utilizes a dedicated HPE GL380p G8 server with dual Xeon processors (10 physical cores each). "Since increasing the RAM to 128GB on this server, we've seen an even more dramatic decrease in scan times," says Shuberg.

Authority to Operate

Summarizing the overarching benefit that Fortify has provided at Vital Images, Dawson says: "Fortify helps us find and remediate security vulnerabilities in Vital Images medical imaging software before they go to market. It is directly responsible for an improvement to the security posture of our software. We have a desire that Vital Images be known for producing software which is secure and can be used in high security environments. This is a competitive advantage because certain customers require that security be part of our SDLC and that we show compliance with their security processes."

Vital Images has gone through almost the entire DIACAP process with the Army and is about mid-way through a similar exercise with the Air Force. Ultimately DIACAP certification will result in an Authority to Operate (ATO), meaning that Vital Images can sell its product to facilities in the Army and Air Force. "There are hospitals and other medical facilities within the Army and Air Force that want to install and use our products," says Dawson. "Fortify has made it possible for us to target this important new opportunity."

The benefit goes beyond economic opportunity. "Fortify helps us build a more secure product," concludes Shuberg. "By remediating and removing security vulnerabilities, our software is better; basically, that's the whole point of running the code scans. Selling to the DoD is great, but at the end of the day the main purpose of the tool is so that we can have a better application. That is what Fortify is doing for us."

Learn More At

www.microfocus.com/securitysolutions

> “Fortify helps us find and remediate security vulnerabilities in Vital Images medical imaging software before they go to market. It is directly responsible for an improvement to the security posture of our software.”
>
> **TIM DAWSON**
> Senior Director, Software Engineering
> Vital Images

Contact us at:
www.microfocus.com

MICRO® FOCUS