Northwell Health partners with Code Dx Enterprise for Application Security

Information security is a top priority for healthcare providers, as they manage large amounts of protected health information (PHI). Northwell Health, one of the nation's largest health care systems, turned to the Code Dx Enterprise Application Vulnerability Manager to ensure that applications developed internally were reviewed for security vulnerabilities prior to release.

With locations spanning the NY Metro area, Northwell has more than 1,800 team members focused on IT delivery for the organization - with over 100 individuals focused on application development. The application development team manages hundreds of applications, including both commercial off-the-shelf (COTS) and those built in-house, which are subject to stringent HIPAA (Healthcare Insurance Portability & Accountability Act) regulations and PCI-DSS standards.

To ensure consistency and best practices in the application security development process, Northwell's Information Services Security team formed a Secure Software Development Governance committee to establish standards and guidelines for the Application Security (AppSec) review process. This included establishing requirements to ensure that all applications developed in-house went through rigorous security testing and that remediation of identified vulnerabilities were completed before going into production. Although daunting, this is an essential task considering the rapid expansion of the health system.

As a result, the Applications Development (AppDev) team in collaboration with Information Security, explored technologies for testing, managing, and remediating security weaknesses during the development of source code. Code Dx Enterprise was selected as the cornerstone to minimize vulnerabilities and improve the security of in-house developed applications.

As part of the AppDev teams' CI/CD (Continuous Integration/Continuous Delivery) process, Code Dx is used to run static application security testing (SAST) tools on Northwell's source code. Running these tools at least once a week allows security vulnerabilities to be detected and remediated early in the software development lifecycle (SDLC), avoiding costly rewrites and delivery delays.

With many applications written in diverse programming languages, using best practice methodology requires development teams to apply several different application security testing (AST) tools to discover weaknesses in software. Northwell relies on Code Dx Enterprise to automatically run more than 15 open source SAST tools across different languages, incorporate the results of manual code reviews and any other AST tools, then correlate and merge the results into a single consolidated data set. The AppDev team also checks on the vulnerability status of open source components that have been incorporated into each code base — part of the recommended practice of Software Composition Analysis.

The AppDev team then takes the results and triages them into priority categories for remediation. Similar to a hospital emergency room, triage is critical, and the most severe cases must be addressed first. To do this on software, the AppDev team uses Code Dx's built-in system for tagging software weaknesses that are deemed severe or critical, based on industry standards such as the OWASP Top 10 or SANS 25.

Since 2016, Northwell has transformed and standardized their testing and reporting processes. They have integrated Code Dx Enterprise into their CI/CD process enabling them to look at more applications in less time, ensure their code is secure, and properly protect the personal health information of their patients and employees. "Today's healthcare environment can be extremely vulnerable, and our priority is to ensure our software applications and patient data are secure", said David Luft, AVP Software Engineering and Development. "Northwell's use of Code Dx has enabled us to better detect security vulnerabilities and optimize our Continuous Integration/Continuous Delivery process."

As Northwell's software development practices are maturing, standards on AppSec tools and practices are maturing as well. Northwell envisions leveraging Code Dx's ability to interface directly with their developers' Integrated Development Environments and the automated build servers to further streamline their AppSec practices in the future.

6 Bayview Avenue, Northport, NY 11768-1502
631.759.3933
www.CodeDx.com
info@codedx.com