CGI

Simplifying AppSec Results with Black Duck® Software Risk Manager

Company overview

Founded in 1976, CGI is one of the world's largest IT and business consulting services firms, delivering end-to-end services and solutions. CGI consultants partner with clients in large enterprises and public sector agencies around the world to help them advance their business and technology strategies. CGI was recognized in 2023 by TIME magazine as one of the world's best companies based on its achievements in the areas of employee satisfaction, revenue growth, and sustainability.

CGI has used Software Risk Manager (formerly Code Dx) since 2018 within its U.S. business to integrate its security activities across over 100 software projects. Software Risk Manager is an on-premises application security posture management solution that enables security and development teams to simplify and strengthen their application security programs.

The challenge: Consolidate vulnerability reporting across AST tools

"My role is to identify, understand, and communicate threats and mitigations in order to help our development teams protect CGI software," said Rajesh Subramani, application security engineer at CGI. "CGI uses a variety of tools for application management, including an application portfolio management solution, an open source code quality analysis tool, a cloud-native application protection platform, and several others."

CGI isn't unusual in its use of multiple application security testing (AST) tools. A report by the Enterprise Strategy Group, "Cracking the Code of DevSecOps," notes that over 70% of enterprises are using more than 10 AST solutions.

"Within our U.S. application security testing scope, we have well over 100 software projects underway," Subramani continued. "With that many projects in development through deployment, all being examined by a spectrum of security testing tools, it was important that we start getting consolidated reports with results in one place."

There was more than one business priority driving CGI's decision to provide a single, consolidated view of security-related information from its AST tools. It needed to understand how effective its AppSec tools actually are, as well as gain complete visibility into process and performance across teams. And CGI development and operations teams wanted a centralized view of all issues so they could identify the security activities that have the most impact. Those whose focus is on security, such as Subramani, wanted to be able to identify and prioritize critical issues quickly.

The solution CGI selected to answer those business priorities was Software Risk Manager™.

The solution: Simplify AppSec management with Software Risk Manager

Supporting over 125 integrations with security testing tools, Software Risk Manager is a unified, on-premises application security posture management (ASPM) solution that enables security and development teams to prioritize risk and focus on what matters most to them.

Software Risk Manager brings together policy, orchestration, correlation, and built-in static application security testing (SAST) and software composition analysis (SCA) engines to integrate security activities intelligently and consistently across the software development life cycle.

With Software Risk Manager, security and development teams can make informed security decisions from a single source of truth. By connecting security data, software resources, policies, and insights, CGI can make quick, informed decisions to immediately bolster its security posture.

Software Risk Manager is the only ASPM solution to offer industry-leading, built-in engines for SAST and SCA to quickly achieve source code and open source testing, and onboard necessary scanning with little disruption to existing pipelines. Software Risk Manager also provides contextual risk scoring of vulnerabilities and escalates critical issues, pushing these defects to developers directly within the tools they use. And it provides support for bidirectional syncing with issue-tracking systems. With centralized policy management, Software Risk Manager can define, enforce, and track adherence to policies that set criteria for testing, triage, and remediation.

The results: A complete picture of security risks

"We've found Software Risk Manager very helpful with static code analysis, since it uses the same SAST engine that powers Coverity® Static Analysis," said Subramani. "I concentrate mainly on security issues—how well we're performing against benchmarks such as the OWASP Top 10 and SANS Top 25."

"One of the things I like about Software Risk Manager is its ability to filter out everything except what is important to you. It can produce information from the AST tools on everything related to the code they're scanning—code quality and code "smell," for instance. But if what you want is a strict focus on security vulnerabilities, Software Risk Manager will provide a laser focus on that and only that. Noise was an issue we had with several of the tools we use; that is, they throw out data in quantity, and it's easy for the information you're looking for to get lost in the noise. Software Risk Manager answers that problem."

"Black Duck and Software Risk Manager have provided the results we're looking for," Subramani continued. " We can get results from all the tools we use consolidated into one place, and get the results filtered down to only the information we need. We found Software Risk Manager easy to configure, and its dashboard provides a great user experience. I've been very satisfied with the results we've seen."

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.