Software Risk Manager: Building a Secure SDLC for a State Government IT Agency

Company overview

This state IT agency services the business operations of employees in more than 700 locations, supporting statewide data center, help desk, and IT security strategy initiatives. Among its other responsibilities, the agency aids other departments in the development and implementation of the state's overall strategic IT direction.

The challenge: Establishing a secure SDLC across state agencies

Like many IT departments overseeing statewide technology needs, the agency faced significant challenges in helping its client departments establish a unified secure software development life cycle across a wide range of applications and systems. In 2022, the state solicited software security tool vendors for a solution that would help expand its agency-wide secure application development framework to reduce application security risk. The goal was to ensure that security practices were used throughout the development life cycle, from planning to deployment.

Key challenges included developer adoption of the new automated security tools and processes, and ensuring that those tools integrated smoothly into the existing DevOps pipeline. "We knew that the key to success would be how open developers would be to this new initiative," noted an application security architect deeply involved with the implementation. "Adoption would be dependent upon how easily the new tools and processes fit into our DevOps pipelines."

The solution: Coverity SAST and Black Duck SCA, unified with Software Risk Manager

After evaluating vendor proposals, the state selected Black Duck's industry-leading application security testing (AST) tools Coverity® Static Analysis and Black Duck® SCA, unified into a comprehensive testing solution through Black Duck's Software Risk Manager.

Software Risk Manager is an application security posture management solution that enables development teams to manage their application security programs at any scale. It integrates with 135+ industry-leading static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), interactive application security testing (IAST), network security, and developer tools to provide a single AppSec source of record. Software Risk Manager allows developer teams to easily track security initiatives using dashboards that deliver KPIs and productivity analytics.

Software Risk Manager provides a uniform software risk assessment of all components—custom code, third-party, and open source—as well as related components like APIs, containers, and microservices. Support for 20+ compliance standards including HIPPA, NIST, and OWASP Top 10 enables both public and private entities to map specific findings to regulatory standards to shorten time to audit.

"We knew that the key to success would be developer adoption, and that adoption would be dependent upon how easily the new tools and processes fit into our DevOps pipelines."

The results: Measuring success with Software Risk Manager

By implementing Software Risk Manager, the state gained the ability to manage its application security programs at an enterprise scale. Software Risk Manager provided a centralized view of security issues, helped identify impactful security activities, and streamlined security activities across 19 state agencies.

"We established a compliance framework for new and modified applications centered around an overall reduction of vulnerabilities in each of the respective agency's systems," noted a team member involved with implementing the new tools and processes.

"The success of the initiative was measured using key performance indicators. Those KPIs included measurements of overall reduction in identified vulnerabilities per application/system/agency, and a measurable reduction in resolution time."

The agency has seen other improvements as well. Software Risk Manager improved issue-tracking due to its ability to integrate results from different data sources, according to the implementation team. "The Black Duck team has also been instrumental in helping accelerate cultural change within the organization toward a security mindset for both operations and developers."

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.