

CASE STUDY

Securing Government Software with a Unified Application Security Solution

Business Problem

An Australian government department was facing mounting challenges in managing their application security processes. Their software development team, responsible for creating critical public services, was struggling with a fragmented security approach. Multiple disjointed tools led to silos of information, making it difficult to gain a clear view of vulnerabilities. Developers frequently encountered false positives, wasting time on non-issues, while critical vulnerabilities sometimes slipped through the cracks until late in the development cycle. This resulted in costly rework and delays, impacting both productivity and security. The department needed a solution to streamline their security processes and reduce the burden on their development teams.

Solution Provided

The department turned to Phase Pacific for guidance. After a thorough assessment of their needs, Phase Pacific recommended a comprehensive suite of tools that would provide end-to-end application security coverage. The proposed solution included Black Duck **Seeker** for Interactive Application Security Testing (IAST), **Coverity** for Static Application Security Testing (SAST), Software Composition Analysis (SCA) for managing open-source risks, and Software Risk Manager (SRM) to automate vulnerability triage and prioritisation.

Black Duck Seeker allowed the department to detect vulnerabilities in real-time during application runtime, providing immediate feedback to developers. Coverity integrated directly into their development environment, enabling the team to catch code-level vulnerabilities early in the process. SCA ensured that the department had full visibility into open-source components used in their applications, identifying potential risks and ensuring compliance with licensing requirements. Finally, SRM automated the process of triaging security findings, reducing the noise created by false positives and allowing the team to focus on high-priority issues.

Business Outcome

The implementation of this unified solution had a transformative impact on the department's software security processes. Developers reported a significant reduction in the amount of time spent on rework, as vulnerabilities were now identified and addressed earlier in the development lifecycle. The automated triage provided by SRM ensured that only valid, high-priority issues were brought to their attention, allowing them to focus their efforts where it mattered most.

With these tools in place, the department achieved continuous, comprehensive security testing. The integration of security tools within their existing workflows meant that security was no longer a bottleneck but an integral part of the development process. This shift enabled the department to deliver secure applications faster, without compromising on quality.

Business Benefits

One of the most significant benefits was the reduction in false positives, which had previously bogged down the development team. The automated triage provided by SRM ensured that developers were no longer wasting time on non-issues, improving both productivity and morale. This streamlined approach to securing government software made it easier for teams to focus on critical tasks. By catching vulnerabilities early, the department minimised rework and reduced the risk of security issues making it into production.

The unified Application Security Posture Management (ASPM) platform also provided the department with full visibility into their risk landscape. This comprehensive view allowed them to proactively address potential threats, improving their overall security posture. Additionally, the solution helped the department maintain compliance with stringent government regulations, reducing the risk of penalties and ensuring that public services remained secure.

Phase Pacific continues to provide ongoing support and consultation, ensuring that the department's security practices evolve alongside emerging threats. This partnership highlights how government organisations can achieve both security and agility by adopting a unified application security approach.

A Modern Blueprint for Government Software Security

The Australian government department's journey toward a modernised application security framework demonstrates the value of a unified solution. The department partnered with Phase Pacific and implemented Black Duck Seeker, Coverity, SCA, and SRM. This helped streamline their security processes. It also reduced false positives and allowed for faster delivery of secure applications. This case study underscores the importance of integrating security into the development lifecycle to achieve both compliance and efficiency in the public sector.

About Us

We streamline network labs, software development environments, and IT Operations with advanced automation and orchestration. Additionally, we bolster application security with cutting-edge solutions that focus on efficiency and protection.

Contact Us

Phase Pacific
114 Bakehouse Rd,
Kensington, VIC, 3031
enquiries@phasepacific.com
Ph: +61 3 9381 7818

For more information, go to www.phasepacific.com

[Download our Cybersecurity and Application Test Services brochure here](#)