phase pacific
A subsidiary of CoverTel Telecommunications Group

CASE STUDY

Improving Software Security for Public Transportation

Business Problem

A government public transport department in Australia was facing a critical challenge: securing the software that manages its vast rail network. This software plays a vital role in daily operations, from scheduling and signaling to real-time monitoring and safety controls. A single vulnerability could disrupt operations, jeopardise passenger safety, and result in costly compliance failures.

As cyber threats evolved, the department recognised the need for a proactive security solution. Their objective was not only to identify vulnerabilities but to address them swiftly before they could affect operations. They sought a solution that would integrate seamlessly with their existing development processes, without hindering performance or innovation.

Solution Provided

To address these security concerns, the department chose **Black Duck Coverity**, a **Static Application Security Testing** (SAST) solution known for identifying security flaws early in the development lifecycle. Unlike traditional tools that often find issues too late, Coverity provided immediate, actionable insights, enabling developers to resolve vulnerabilities as they wrote and tested code.

Coverity's deep code analysis, along with its support for multiple programming languages, allowed it to seamlessly integrate with the department's CI/CD pipelines. Developers were able to scan code automatically during their daily workflows, receiving prioritised reports that pinpointed high-risk vulnerabilities for immediate resolution. This proactive security approach ensured that issues were identified and addressed early, rather than after they had escalated into more severe risks. This commitment to proactive security empowered developers to focus on their coding tasks with greater efficiency, ultimately strengthening the department's security posture while ensuring compliance with public infrastructure regulations.

Business Outcome

Since implementing Black Duck Coverity, the department has transformed its approach to software security. They now detect and resolve vulnerabilities early in the development cycle, preventing potential risks from escalating. This change has led to a 30% reduction in vulnerabilities during pre-deployment, compared to the previous process. Developers are now able to focus more on innovation, rather than fixing security issues late in the cycle.

The department's shift has also streamlined compliance reporting, with Coverity's detailed reports demonstrating adherence to security best practices. The result is a more efficient development process that enhances both security and operational efficiency.

Business Benefits

Integrating Black Duck Coverity into the department's development pipeline has delivered several long-term advantages. First, security has been greatly enhanced. Vulnerabilities are now identified and resolved long before they can pose risks, dramatically reducing the chances of any disruptions to the rail network. This proactive approach has ensured that critical vulnerabilities are addressed early, which keeps the network secure and operational.

The department has also seen a more streamlined compliance process. With Coverity's automated tracking and detailed reports, preparing for audits has become significantly easier. This has reduced the time spent on compliance tasks, allowing the team to focus on other critical areas. These improvements have ensured the department is always in line with the stringent cybersecurity standards required in the industry.
Operational stability has greatly improved as well. Prior to implementing Coverity, security issues often delayed software updates, affecting the timely rollout of necessary system enhancements. Now, updates can be deployed with confidence, knowing that security vulnerabilities will not cause new disruptions. This has not only increased the reliability of services but has also led to greater customer satisfaction due to more consistent, on-time operations.

Finally, the department has seen substantial cost savings. The proactive security measures have helped avoid costly emergency fixes, downtime, and penalties from non-compliance. These savings have allowed the team to reallocate resources toward long-term improvements and innovations, further strengthening the department's overall security posture.

Conclusion

Black Duck Coverity has played a pivotal role in securing the department's software, ensuring the safety and efficiency of its rail network. By embedding security into every stage of development, the department is better equipped to handle cybersecurity challenges. These challenges are growing in critical infrastructure.
As public transportation systems continue to digitise, the need for robust software security will only increase. With Coverity as a trusted partner, the department is prepared to tackle emerging threats. Passengers can now travel safely, knowing that their safety is backed by the highest standards of software security.

Looking forward, the department will adopt new technologies. Coverity will evolve alongside them. It will provide the flexibility and depth needed to secure next-generation infrastructure. It will also meet future security challenges head-on.

As the need for robust security solutions continues to grow across critical infrastructure sectors, Black Duck Coverity stands ready to help organisations safeguard their software and meet the ever-evolving cybersecurity challenges. If you're looking to strengthen your security posture, streamline compliance, and improve operational stability, reach out today to discover how Coverity can seamlessly integrate into your development pipeline. Secure your future with proactive security—contact us now to learn more and get started.

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