# How LTP and Apiiro Together Forge a Stronger, Resilient Framework

## Background

Digital asset prime brokers like LTP depend on a complex suite of interconnected applications to better serve their clients and further innovation in the digital asset marketplace. As their security team sought to place greater emphasis on identifying and managing vulnerabilities across these applications, they turned to Apiiro. Our team offered a solution to help streamline their security processes, reduce vulnerability management times, and enhance their overall application security posture.

## Highlights

### Challenge

LTP's diverse and complex business operations require robust support from external experts to assist in identifying, managing, and addressing vulnerabilities, including common weakness enumerations (CWE) and CVEs in application code. This collaboration with external teams is crucial to ensure the comprehensive validation of application vulnerabilities, such as those identified by Apiiro, and to maintain smooth and secure operations across our extensive systems.

### Solution

Apiiro, with the support of Aerowave Technologies, provided LTP with a unified AppSec platform, offering full support of supply chain levels for software artifacts (SLSA – which includes SAST, SCA, and pipeline security) and a high-level, consolidated view of their application security.

### Result

LTP developed capabilities to build an SLA/MTTR framework for code security, prioritize vulnerabilities via filtering in software composition analysis (SCA), and reduce their reliance on multiple security tools, resulting in significant time savings and improved DevSecOps processes.

## The Challenge: Managing Vulnerabilities with Complex Business Operations Duties

The complexity and breadth of LTP's operations demand a multi-faceted approach to reducing vulnerability exposure. Success is measured by two key performance indicators: external vulnerability discovery post-launch and internal discovery pre-launch. These metrics, evaluated by the number and severity of vulnerabilities, present a challenge given the scale and complexity of LTP's operations.

Each day, LTP's security team reviews the previous night's security events, analyzes them, and optimizes alarm rules. They also conduct baseline scans and assess business risks to ensure smooth operations. Given the complexity and scale of their applications, the team continuously seeks to enhance their capabilities by leveraging external expertise and support, further reinforcing their robust security

framework.

Given the scale and demands of their business, LTP sought external tools and expert teams to assist in identifying and managing vulnerabilities, particularly those with business-critical risks. These tools needed to streamline security processes, consolidate key features like SAST, SCA, and secret detection, and ensure seamless integration with ticketing systems like JIRA.

## **The Solution: A Unified Platform with Comprehensive Security Capabilities**

LTP chose Apiiro after a successful proof of concept (POC), recognizing its comprehensive support for single supply chain levels for software artifacts (SLSA), including SAST, SCA, and pipeline security. Apiiro's ability to provide a well-rounded view of application security complemented LTP's already robust security practices, further strengthening their overall security posture.

With the assistance of Aerowave, Apiiro helped LTP consolidate their security tools into a single platform. This consolidation provided LTP with multiple filters in their SCA processes, allowing them to prioritize vulnerabilities based on factors like whether they were used in code or exploitable. Additionally, Apiiro's integration capabilities with Github, JIRA, and future CNAPP solutions were crucial in streamlining LTP's security processes.

## **Result: Streamlined Processes and Improved DevSecOps**

Apiiro's solution empowered LTP to build an SLA/MTTR framework for their code security, which in turn helped them demonstrate the value of their security team. The ability to easily view security checks based on each repository allowed LTP to prioritize their work efficiently.

By streamlining vulnerability management and enhancing their DevSecOps processes, LTP was able to optimize their security efforts, allowing the team to allocate resources more efficiently while maintaining their strong focus on security. Apiiro's unified platform eliminated the need for multiple tools, saving LTP considerable time and effort in learning and integrating different systems.

Moreover, Apiiro's continuous code monitoring enabled LTP's developers to not only see and detect risks in their components, but also to download a fixed version, which greatly accelerates the process of reducing security risk.

In the future, Apiiro's strong integration capabilities will enable the LTP team to integrate AppSec workflows with their Aqua CNAPP, deepening the holistic view of security across multiple layers.

## **Conclusion**

Security is a core principle and a non-negotiable priority for LTP. They consistently dedicate substantial resources and effort to building and maintaining a robust security framework, ensuring that every aspect of their operations is safeguarded. LTP's proactive investment in advanced technologies and expert teams reflects their commitment to not just meeting but exceeding industry standards. By partnering with Apiiro, LTP further enhances their capabilities, leveraging Apiiro's solutions to streamline processes, reduce MTTR, and lower vulnerability discovery scores. This collaboration, built on LTP's foundational focus on security, has strengthened their overall security posture, enabling them to effectively manage risks, ensure business continuity, and achieve growth.