

CASE STUDY

Enhancing Software Security in Mining Technology

Business Problem

A leading provider of Mining Software faced growing challenges in ensuring their applications were secure enough to meet client demands. Their software powers critical mining operations, where any security lapse could lead to significant downtime, data breaches, or even reputational damage.

Like many companies in the mining sector, they were navigating an evolving landscape of cybersecurity threats and tightening regulatory requirements. While their existing cybersecurity infrastructure included standard protective measures, they lacked a solution to address vulnerabilities at the development stage. Security checks occurred late in the process, often creating delays or leaving gaps that could have been addressed earlier. They needed a solution that wouldn't replace their existing defenses but would strengthen their ability to identify and resolve vulnerabilities as part of their development workflow.

Solution Provided

To address these challenges, the company implemented **Black Duck Seeker**, an interactive application security testing (IAST) tool. This addition wasn't intended to replace their existing cybersecurity strategy but to complement it by providing visibility into security issues during the software development lifecycle. What set Seeker apart was its developer-friendly design. It didn't just highlight issues; it provided context and actionable recommendations, helping developers understand what went wrong and how to fix it. Importantly, this all happened in real-time, integrated into the tools the team was already using.

Additionally, the tool's automation capabilities aligned perfectly with their workflows, conducting continuous security tests without creating bottlenecks. This made it easier to ensure that security was a priority at every stage of development while still meeting tight deadlines. While Seeker focused on application-level security, its ability to generate detailed compliance reports also proved crucial. These reports streamlined their efforts to meet regulatory requirements, saving time and providing an added layer of accountability.

Business Outcome

The introduction of **Black Duck Seeker** made an immediate impact. The company was able to proactively detect and address vulnerabilities much earlier in the development process. Instead of scrambling to fix issues after release, the team resolved them as part of their regular workflows.

This proactive approach didn't just improve security, it also enhanced productivity. Developers could focus on building innovative solutions rather than being bogged down by manual security checks or last-minute fixes. Projects moved faster, and releases became more reliable. For their clients, this was a significant reassurance. The mining industry relies on stable, secure software to operate efficiently. Demonstrating a commitment to improving cybersecurity instilled greater trust in the company's offerings and strengthened relationships with existing and new clients.

Business Benefits

The benefits of Black Duck Seeker went beyond identifying vulnerabilities. By integrating the tool into their development process, the company saw a reduction in costs associated with late-stage bug fixes. Catching problems early meant fewer post-release patches, which translated into significant savings.

Regulatory compliance, which had been a time-consuming and complex process, also became simpler. With Seeker's automated reporting capabilities, the company could quickly demonstrate adherence to industry standards, reducing the stress and effort of audits.

Perhaps the most important benefit was its impact on the company's reputation. By adding Seeker to their cybersecurity infrastructure, they showed a proactive approach to protecting their clients' interests. This wasn't about relying on a single tool to solve all security problems; it was about building a comprehensive and resilient security framework.

Their development team, too, felt the difference. Seeker empowered them with the insights needed to address issues effectively, boosting confidence and fostering a culture of security-focused innovation.

A Holistic Approach to Cybersecurity

This success story underscores an important lesson: no single solution can address all cybersecurity challenges. Black Duck Seeker wasn't a replacement for firewalls, endpoint protection, or other traditional measures. Instead, it filled a critical gap by providing visibility and actionable insights during development—something their existing tools couldn't fully deliver.

By integrating Seeker into its broader security strategy, the company created a more robust defense against evolving threats. This layered approach, combining traditional infrastructure with advanced application-level security, positioned them to address risks from multiple angles.

For their clients, this means greater assurance that the software they rely on is not only functional but also secure. For the company, it's a step toward building trust and maintaining leadership in a competitive industry.

As cyber threats continue to evolve, having a multi-faceted security strategy is more important than ever. Black Duck Seeker proved to be a vital piece of the puzzle, complementing their existing defenses and helping the company deliver secure, reliable software for the mining industry.

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](#)