Fortune 500 Tech Giant Achieves 40% Faster Deployment and 25% Reduced Security Threats with DevSecOps

Business Overview

Our client is a global technology company engaged in software and hardware development. They provide a wide range of business devices to large enterprises, venturing into critical growth sectors such as server, storage, mobile, software, services, and holistic solutions.

The company's commitment to rapid innovation had previously led to security threats and potential financial risk. With escalating cyber threats and sensitive data at stake, the client recognized the imperative need to adopt DevSecOps to safeguard their business and ensure secure innovation. Given the years of successful collaboration with us and our extensive expertise in cybersecurity, the company approached NIX to strike a balance between rapid software delivery and robust security throughout the whole SDLC.

Challenge

In the past, the need for expedited software delivery frequently resulted in the sidelining of security concerns. This, in turn, gave rise to vulnerabilities that could be taken advantage of, leading to substantial financial losses. As the scale of cyber threats is ramping up, there is a growing awareness of the risks associated with this oversight. Speed without security is a risk few can afford, especially for our client handling sensitive types of data like personal identification information.

Solution

Our primary goal was to embed security from the earliest stages of development—the "shift left" principle in DevSecOps. This allowed us to proactively identify and fix vulnerabilities before they became costly production issues, accelerating the delivery process. Built upon the foundation of DevOps and DevSecOps principles, our methodology and resource selections were geared towards achieving agility without compromising security.

Our approach revolved around the key principles of DevOps, namely rapid delivery, automation, and iterative feedback.

- **Microservice Architecture:** We adopted a microservice architecture for flexibility and agility. This allows teams to work on, test, and release individual components independently, leading to faster innovation cycles and reduced time-to-market.
- **Rapid Feedback and Iterative Development:** With Kubernetes in play, we ensured that every microservice had its own continuous delivery pipeline, enabling faster feedback, swift iterations, and, in turn, rapid deployment.
- **Resilience and Recovery:** Our approach emphasized rapid recovery—in the event of a microservice failure, Kubernetes safeguards the system from disruption.

We designed a highly secure and resilient solution on top of AWS. The architecture utilizes Kubernetes for orchestration, ensuring availability and robust security controls. The DevSecOps team employed Infrastructure as Code to streamline infrastructure management for consistency and accelerated deployment, while Docker containerization guarantees a seamless development-to-production workflow.

We employed a contemporary tech stack perfectly aligned with our project's vision, often surpassing objectives. By harnessing best practices and technologies, we achieved a remarkable 40% acceleration in deployment time—a commendable outcome, especially considering the establishment of highly secure infrastructure with automatic vulnerability fixes.

“Our goal was never just rapid software delivery—it was about delivering software that meets the highest security and performance standards, working as clockwork. “

Viktor, – Lead DevSecOps Engineer

Robust Security Framework for Agility

We integrated a comprehensive security framework within the existing DevOps model, ensuring both speed and security at every stage.

- **CI/CD with Automated Vulnerability Checks**: Security tests with each code change enabled early detection, preventing costly delays and potential breaches.
- **Integrated Security Tools:** A range of tools (SAST, DAST, IAST, etc.) provided continuous monitoring and deep code analysis for a thorough security posture.

- **Jira Integration for Streamlined Response**: Automated ticketing and prioritization within Jira expedited the resolution of security issues.
- **Security Dashboard for Data-Driven Decisions:** The dashboard offers in-depth security metrics, enabling a data-driven approach to identifying, prioritizing, and mitigating system vulnerabilities.

Outcome

The NIX team helped the client strike a balance between rapid software delivery and robust security throughout each step of SDLC. Our strategic DevSecOps implementation empowered the company to transform its development approach, embedding security as a fundamental pillar rather than an afterthought.
This strategic shift safeguarded them from the escalating financial risks of cyberattacks and allowed them to innovate quickly and confidently.

The impact was significant, demonstrating the business value of DevSecOps:

- **40% Deployment Acceleration:** Reduced time-to-market empowered the client to capitalize on new opportunities faster.
- **25% Reduction in Security Incidents:** Significantly strengthened security posture, mitigating costly breaches.
- **Lowered Remediation Expenses:** The "shift left" approach of DevSecOps allows for discovering vulnerabilities early or preventing them, saving money on rework and delays.
- **Elevated Client Trust:** Proactive security measures reinforced the client's reputation as a reliable technology partner.