CASE STUDY

A Fintech Company Elevates it AppSec Program by Collaborating with Security Champions in Development Team

Company Description

This financial technology company helps its customers accelerate their financial contract work through its extensive integration with industry ecosystem players. It has revolutionized the sector by unifying financial contracts from multiple industries and providing a fast, seamless experience for its users. The company deals with confidential information that has to be protected, but also must maintain a competitive edge by innovating quickly.

The Challenges

The company utilized hundreds of applications and microservices that generated an overwhelming number of alerts. The Product Security team had set up an expansive structure for manual processing of alerts, software updates, report generation, etc. While the manual process got the job done, it was unscalable and slowed their product security activities. This stop-gap solution also created friction within the development team that needed to be addressed. Developer productivity suffered as a result of not having clear visibility into the issues requiring attention. Since the industry was highly regulated, achieving compliance on time was a must.

The small team found it hard to keep up with the volume of security issues coming from Pentesting, Threat Modelling, SAST, SCA, DAST, Bug Bounty, and RASP. There was no clear visibility into SLAs across teams, nor insights into how these could be improved.

The ArmorCode AppSecOps Solution

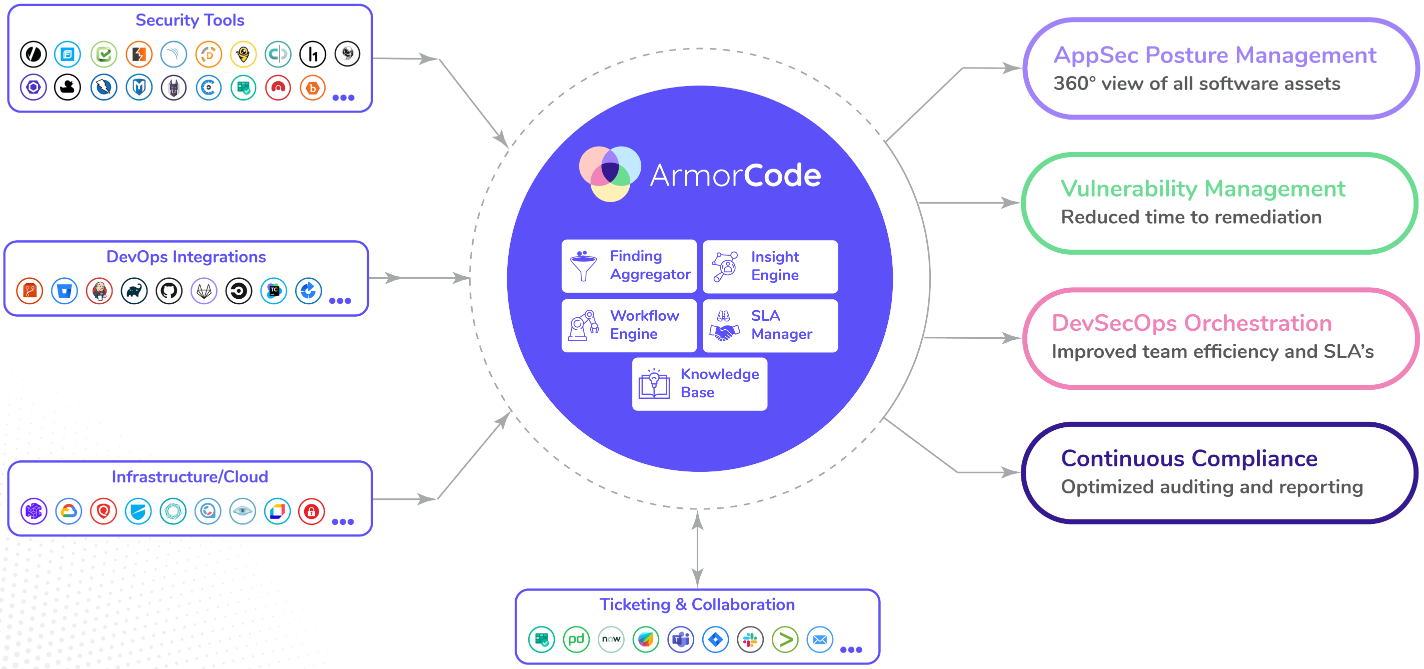
The company selected ArmorCode as a solution to help:

1. Implement a new AppSecOps process that would work closely with security champions on the development team.
2. Migrate from monolith to microservices using a modern platform that could incorporate the architectures of both.
3. Reuse an in-house customer reporting tool to combine AppSec data with revenue, sales, and other organizational data; as well as with critical APIs and data integrations.

ArmorCode's AppSecOps platform provides the team a single-pane-of-glass to gain application and alert visibility to quickly identify important issues, and work with developers to get them fixed. Issues are automatically assigned to developers using automation capabilities, contributing to improved Service Level Agreements. New repositories are automatically detected, and unused ones deprioritized.

The team's AppSec program multiplied in force without changing people or tools, and within a short period. This has allowed them to ship their software faster and more securely while accelerating overall operations.

Platform Overview-How ArmorCode Works



Results

1. Continuous and efficient AppSec monitoring from a single AppSecOps Platform that combines AppSec Posture Management, DevSecOps Workflow Automation, and Continuous Compliance.

2. Improved cohesion between AppSec and development teams.

3. Seamless orchestration of different workflows via integrations with SAST, DAST, RASP, CI/CD, Bug Bounty, and Pentesting.

4. Creation, sharing, management, and tracking of SLAs and automated DevSecOps workflows using SLA Automation.

5. Successful scaling of AppSec processes.

What is AppSecOps?

> AppSecOps is the process of identifying, prioritizing, remediating, and preventing Application Security breaches, vulnerabilities and risks - fully integrated with existing DevSecOps workflows, teams, and tools.

An AppSecOps platform enables an application security team to scale its ability to identify, remediate and prevent high priority security issues, vulnerabilities, and compliance issues. It also helps identify and eliminate coverage gaps. It automates, manages, and orchestrates workflows enabling developers to fix issues faster and more effectively without specialized training and skills. In short, **AppSecOps 10X force multiplies your AppSec program.**