coveros

COVEROS IMPROVES DEVSECOPS CAPABILITIES

FOR FINANCIAL SERVICES FIRM

CASE STUDY

CASE STUDY

Coveros Improves DevSecOps Capabilities for Financial Services Firm

OVERVIEW

A recognized Fortune 100 financial services firm engaged Coveros to improve its DevSecOps capabilities for mission-critical financial applications. The organization was seeking support to shift its application security practices to the left in its existing DevOps process.

CHALLENGES

- The organization's ability to accelerate delivery is significantly slowed by the inability to integrate critical governance and security practices into agile and DevOps processes.
- Teams are unable to deliver value to customers due to late lifecycle security bottlenecks and bureaucracy.
- The Application security team is not fully integrated into emerging containerization, elastic demand, and cloud-based re-platforming initiatives, making their security assurance an out-of-band activity.
- The organization's initial use of open-source application security tools yielded some benefits, but a more robust approach is needed to meet business needs.
- Silos are slowing down the adoption of new technology and security assurance capabilities.

The organization has been pursuing approaches to better integrate application security into the software lifecycle for many years with only a limited amount of success. Existing organizational silos make integrating tools and capabilities difficult. New initiatives to modernize software development and delivery have not been fully embraced and existing application security tools and concepts are not in widespread use.

Software engineering teams are focused solely on speed and often skip security checks during build, integration, and delivery/deployment jobs to meet deadlines.

THE COVEROS APPROACH

To address these challenges, Coveros was retained to assess and improve processes, practices, and capabilities relating to DevSecOps. We followed our DevSecOps transformation process to assess existing DevSecOps capabilities, create an improvement plan, build out

Coveros Improves DevSecOps Capabilities for Financial Services Firm

DevSecOps processes, integrate application security tools, and scale DevSecOps across the enterprise through coaching and training. This work was performed in three phases, as discussed below.

Phase 1: Plan DevSecOps improvements

In the first phase, Coveros used our DevSecOps Maturity ModelTM to evaluate existing DevSecOps capabilities and benchmark the organization's application security posture against other financial services organizations. We conducted interviews with current development teams, IT and security stakeholders, and operational personnel along with strategy sessions to understand the organization's DevSecOps vision, posture, process, practices, and current implementation. Our team evaluated existing DevSecOps tools and technologies for their effectiveness. We evaluated DevSecOps maturity across leadership, process, automation, and engineering and made recommendations for improving overall DevSecOps capabilities. The outcome of our work during phase one was a backlog of recommended DevSecOps improvements, as well as a roadmap for building and scaling DevSecOps within the organization. These recommendations and results were reviewed with the organization's IT personnel and key members of senior leadership.

Phase 2: Build and Validate DevSecOps Capabilities

In the second phase, Coveros worked with the organization to determine where appropriate security assurance processes and tools should reside within their DevOps pipelines. We created an architectural plan for integrating DevSecOps automation capabilities throughout the software development and delivery lifecycle. Initial components of this architecture included:

Static Application Security Testing (SAST): The integration of both lightweight and comprehensive SAST capabilities within continuous integration (CI) and continuous delivery (CD) environments. We integrated lightweight SAST into developer desktops and CI to identify code-based security vulnerabilities as they are introduced. We integrated comprehensive SAST analysis into the existing regression testing jobs performed frequently in quality assurance (QA) environments. We used SonarQube used for lightweight SAST and Fortify for more comprehensive SAST analysis.

Dynamic Application Security Testing (DAST): Dynamic security testing was integrated into the QA environment to allow web security testing and secure API testing to happen as part of existing QA activities. We selected a variety of open-source tools to perform DAST analysis during the process, including OWASP ZAP, Postman, and BurpSuite.

Software Composition Analysis (SCA): SCA capabilities were integrated into the build and integration process to validate that open-source code integrated into applications did not have known critical vulnerabilities and that their licenses were acceptable. We initially integrated Dependency-Check as a stopgap while commercial applications were evaluated. Ultimately Sonatype Lifecycle and Sonatype Firewall were purchased.

Coveros Improves DevSecOps Capabilities for Financial Services Firm

Coveros worked successfully with the organization's Vulnerability Assessment team to integrate SAST and DAST into the existing DevOps process. Once Sonatype products were acquired, we focused our ongoing implementation work on integrating Sonatype Firewall and Sonatype Lifecycle into the software development, continuous integration, and continuous delivery processes. We then built capabilities to measure and report open-source vulnerabilities, integrating these results into an existing business intelligence dashboard. Additionally, we integrated automated quality and security gates into the DevOps process to assure code changes complied with security policies and best practices. We hardened the DevOps pipeline to assure no malicious activity could be performed from within the DevOps pipeline itself.

As the organization shifted to containerization and cloud-based environments, Coveros worked with both the emerging Application Security and Cloud teams to migrate DevSecOps capabilities to Amazon Web Services (AWS) along with their entire DevOps process. All application security analysis was containerized, and we piloted its use on a single customer-facing application undergoing change. In addition, we provided strategic and tactical support to the application security team to ensure the security of all containers and cloud-based platforms used to perform application security testing.

Phase 3: Scale DevSecOps Knowledge

After the completion of our DevSecOps implementation, an organization-wide rollout process began by incorporating automated security capabilities into development teams across the enterprise. Coveros worked closely with the Enterprise Architecture team and development teams to onboard them onto each emerging DevSecOps platform and train them on how to best triage, remediate, and deploy security fixes continuously. We provided ongoing application security assurance to teams as needed and necessary. We provided coaching and training to both software development and application security teams supporting the end-to-end secure software lifecycle. We also provided early lifecycle security analysis, such as threat modeling and secure code review, to teach architecture and development teams how to effectively build security into their applications from the ground up.

BUSINESS RESULTS

Coveros quickly assessed the DevSecOps maturity of the organization and supported necessary changes to integrate security into the existing DevOps processes. This implementation was successfully rolled out across the organization's development teams. Through the combined efforts of our team and key stakeholders from the organization, a roadmap and critical real-time security reporting were put into place to allow the organization to more rapidly respond to zero-day vulnerabilities. Internal studies show that deployment frequency increased by 25% in the first year after adopting DevSecOps principles, and their deployment failure rate fell by about the same amount. In addition, several well-known, public vulnerabilities that impacted the industry were avoided.