PARASOFT®

CASE STUDY

Aerospace/Defense Company Deploys Parasoft to Support DevSecOps for Major DoD Initiative

SUMMARY

Since 2012, Parasoft has been working with a U.S. Department of Defense contractor in the aerospace and defense industry to improve the quality and security of their software. The contractor is a significant contributor to a major, long running defense initiative. The nature of the project has evolved drastically during the tenure of Parasoft's relationship with the contractor. Most recently, the DoD has announced plans to stand up DevOps pipelines to support the initiative.

A DevOps pipeline is an automated infrastructure that processes the code contributed to the project from various teams. As the code is checked in and pushed through the pipeline, test execution and code analysis jobs are continuously triggered. The continuous code quality activities provide feedback to software engineers and testers so that the build at the end of the pipeline meets the organization's quality, security, and compliance goals. DevSecOps integrates security testing activities into the process.

The size and complexity of the project poses a significant challenge for all vendors involved. The purpose of this case study is to describe the company's DevOps journey and highlight the technologies and processes that characterize DevOps and DevSecOps. To comply with the company's privacy policy, identifying information has been removed.

PHASE 1: STATIC CODE ANALYSIS

The contractor's DevOps journey began in 2012 when it started working with Parasoft to implement an automated static code analysis solution. The contractor's existing static code analysis solution lacked automation capabilities necessary to delivering mission-critical software on time and in compliance with safety-critical guidelines.

The ability to automate code quality is central to running a DevOps pipeline, but it would be a few years before discussions taking place within software development would center on DevOps, much less DevSecOps. At this stage, the contractor wanted more efficient automated static analysis technology to reduce the costs and risks associated with its development process—and do so in a way that enabled it to achieve compliance with JSF and DO-178.

The contractor, furthermore, was not considering changes to its software security approach at this time. Security testing was a separate phase of the development lifecycle with its own set of processes that, for many companies, had little to do with static code analysis. A DevSecOps pipeline, however, integrates software security activities into the workflow. As the code passes through different gates, different techniques can automatically be applied to validate other aspects of the code, such as security.

Parasoft's approach has always been to build security into the software engineering process. This is accomplished by enabling checkers that report violations when patterns that are known to result in security-related defects are detected. In fact, for approaches such as Parasoft's, analyzing code for quality and analyzing code for security follow the exact same process. The only difference is which checkers are enabled. Because of this approach, automating quality and security within a DevOps pipeline is simple.

The investments made at this stage helped the contractor lay the groundwork toward the DevOps initiative that it would begin planning more recently.

PHASE 2: UNIT TESTING AND COVERAGE

The next phase of the contractor's journey was to extend its unit testing capabilities, also with the goal of enabling greater automation. Unit testing is a foundational software quality activity that engineers and developers across all industries struggle to implement consistently and efficiently. It is a notoriously expensive activity in terms of engineering resources for several reasons, including:

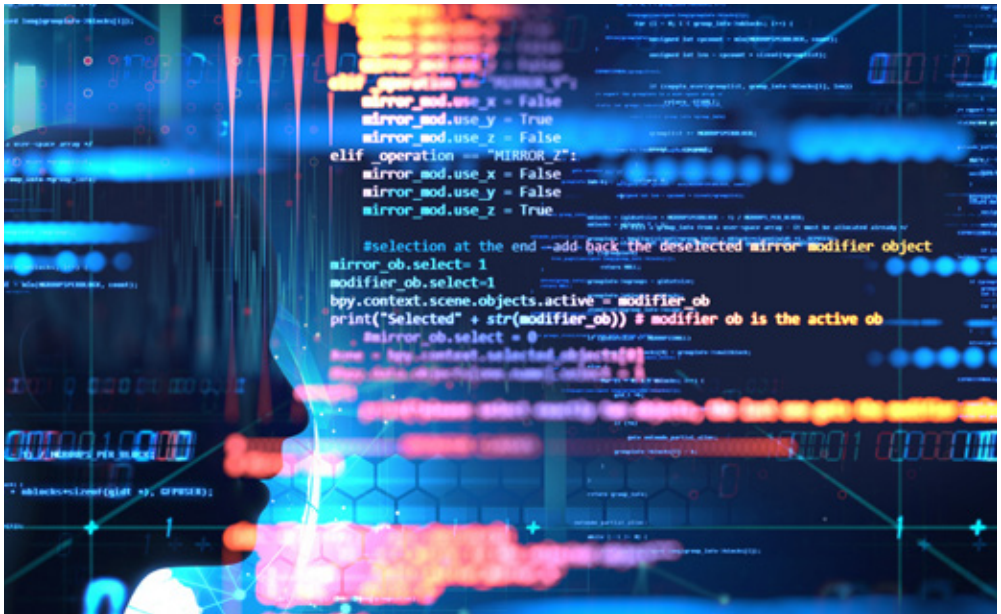
- Time and expertise required to create tests.
- Time and computing resources required to execute the tests.
- Knowledge and technical skills required to maintain unit tests.
- Ability to identify which tests to run after code changes.

Again, the contractor approached Parasoft about replacing their existing unit testing solution with Parasoft because it needed to create, execute, and maintain its unit tests more efficiently. While each testing vendor has their advantages and limitations, Parasoft's flagship embedded testing solution, Parasoft C/C++test, places emphasis on test coverage and requirements traceability as an integral part of the unit testing workflow. The ability to efficiently execute unit tests across frameworks and collect concise coverage information traced back to requirements helped the contractor efficiently meet their safety-critical and compliance objectives at this stage.

Whether producing their own applications or integrating downstream code into their projects, organizations that deliver software for safety-critical DoD initiatives must be able to demonstrate traceability from requirement to test, as well as report testing completeness. The software integrator is responsible for any negative affects if an uncovered compilation unit leads to produces unexpected behavior in the application, such as a crash or an exploitable surface.

Continuous and complete information about the state of the application enabled the contractor to confidently deliver software devoid of critical errors. The "feedback loop," as it is commonly referred to, is paramount for teams to meet the rigorous release cycles promised by DevOps. This is because the ideal feedback loop returns thorough and accurate test, code analysis, coverage, and traceability data as early as possible so that software engineers can fix issues without wasted iterations. The feedback loop made possible by C/C++test enabled the contractor to find defects and identify uncovered code critical to the safety and security of the application before the cost of fixing those issues became exorbitant.

More recently, the company has turned to Parasoft to measure code coverage at the assembly level, which enables the company to meet its DO-178B/C compliance objectives. While many of the processes that mark a true DevOps pipeline are yet to be implemented, much of the infrastructure has been deployed. Furthermore, the government department running the initiative has decreed that all contractors contributing to the project follow the DevOps model.



PHASE 3: SUSTAINABILITY

Long-running government projects eventually reach a phase in which the focus shifts from new development to sustainability. This means that although development continues, software and maintenance becomes the primary objective as hardware is refreshed. The push toward sustainability means an even greater emphasis on software testing efficiency.

The contractor at the center of this case study is currently developing a DevOps pipeline to support the sustainability phase of the program. The pipeline is intended to process code not only contributed by the primary contractor, but several other vendors responsible for different parts of the codebase. The goal is to standardize and automate testing activities using Parasoft's solutions.

Ultimately, the DevOps pipeline will run in a secure, containerized environment, which has been deemed best practice by the head of DevSecOps for all of the U.S. Department of Defense. This enables the organization to implement shift-left testing policies that focus on security and quality.

CULTURAL CHANGE

One of the key differences between a DevOps pipeline and an automated testing infrastructure is that DevOps requires cultural changes within the organization. Automated testing and build activities are a part of moving toward DevOps, but sometimes new technologies must be deployed that require certain practices to be done in different ways. The changes enable the organization to achieve the same goals more efficiently and with better results.

For instance, one of the ways Parasoft supports DevSecOps is by providing actionable data at every stage of the development cycle—this is the feedback loop characteristic of DevOps workflows. Not only is the data thorough and actionable, but in many cases Parasoft enables remediation workflows that are a click away. Code analysis findings link directly to the code violation and documentation to help engineers quickly fix defects and immediately rerun the analysis.

It is still a work in progress, but the aerospace and defense contractor has committed to making the cultural changes necessary to implement DevOps and standardize on Parasoft solutions.

CONCLUSION

As of the writing of this paper, the contractor has implemented automated static code analysis and automated unit testing with integrated coverage and traceability, as well as assembly-level coverage. Implementing these technologies are a critical step toward standing up a true DevOps pipeline because they enable complete and accurate data about the state of the application to continuously be fed back to the software engineers.

The path toward true DevSecOps pipeline will be even shorter because the contractor is standardizing on Parasoft C/C++test. In a traditional software engineering model, security testing is a separate standalone process that begins after most of the application has been programmed and tested for quality. Parasoft C/C++test is designed to integrate security testing activities into the normal workflow. Switching from static code analysis that targets quality to a set of checkers that target security is simple and can even run in parallel.

Robust unit testing, coverage, and traceability capabilities from Parasoft C/C++test are also easily automated, enabling any software engineering team to quickly get the feedback they need to deliver on the promise of a DevSecOps model.

TAKE THE NEXT STEP

Build security into your software development process from the beginning.

Talk to one of our experts to get started today.

ABOUT PARASOFT

Parasoft helps organizations continuously deliver quality software with its market-proven, integrated suite of automated software testing tools. Supporting the embedded, enterprise, and IoT markets, Parasoft's technologies reduce the time, effort, and cost of delivering secure, reliable, and compliant software by integrating everything from deep code analysis and unit testing to web UI and API testing, plus service virtualization and complete code coverage, into the delivery pipeline. Bringing all this together, Parasoft's award winning reporting and analytics dashboard delivers a centralized view of quality enabling organizations to deliver with confidence and succeed in today's most strategic ecosystems and development initiatives—cybersecure, safety-critical, agile, DevOps, and continuous testing.