Aerospace and Defense needs to embrace DevSecOps

Replace traditional V-cycle software development, become more agile

Software development is moving rapidly to DevSecOps. Research predicts that, by 2022, **90 percent of software development projects** will employ DevSecOps practices, up from 40 percent in 2019. DevOps, which integrates security principles into each step of IT development and deployment, enables rapid product engineering delivery and operations, particularly by Agile teams using lean practices. And 60 percent of developers say they are releasing code two times faster than before.

DevSecOps solves the traditional application-development conflict in which security concerns impeded time to market, and which meant security was either weakened or dealt with as an afterthought.

Security should actually live at the intersection of development and operations. This means it is not added after product development or relegated to testing done on a once-per-release schedule.

While DevSecOps emerged from internet and software companies, it can benefit regulated and high-security environments, and it is the path to digital transformation. Aerospace and Defense (A&D) companies need to break from the traditional V-model so they can accelerate software delivery with DevSecOps, reducing the time from code change to production deployment or release while minimizing security risks.

Safety and security challenges

Cloud and mobile technologies have created a hyper-connected world with more cybersecurity attack surfaces and increased security risks. This can be made worse by the use of third-party or open-source software. Folding security into the process of smaller, faster software builds helps fix defects and security issues much earlier in the release cycle. DevSecOps therefore maintains system integrity and enables efficient incident management, governance, and compliance.

The issue for the sector is that A&D companies have been slow to adopt Agile, DevOps, and DevSecOps practices due to their unique, industry-specific challenges. A&D companies must meet complex compliance requirements with multiple regulations and standards. This is the biggest challenge, directly affecting product release velocity and productivity. As companies connect enormous numbers of devices and develop ever more complex data structures, cybersecurity becomes increasingly important.

Held back by tradition

Software complexity is increasing exponentially across industries, while development productivity is stagnating.

A&D companies typically use Model Based Software Engineering (MBSE) in V-cycle SDLC. That provides simplicity and ease of use but is not well suited for Agile. V-cycles are inflexible and encourage a rigid and linear view of software development, similar to a legacy waterfall SDLC. The long development cycles and low level of test automation make the process less flexible in the face of change, setting aside the implicit, slower release cadence. It can work well for smaller applications but the risk of defects not being found early is too high for massive projects.

An issue specific to the A&D sector is that one aircraft, submarine, or military drone needs to be supported for many years, leading to a huge legacy codebase and complex branching strategy. This is made worse when development environments are inconsistent with runtime environments. The result is software that is not necessarily ready to be rolled out because it has not been tested well enough in day-to-day operations.

This results in resource constraints, with less room to compensate for hardware (CPU or memory) variations. Reducing hardware dependencies, accelerating test automation, and providing production-like test environments repeatedly and reliably, without compromising security, is difficult if not impossible to achieve without adopting a DevSecOps approach.

Committing to DevSecOps

Hardware dependencies and long support contracts lead to a huge legacy codebase with siloed software development teams. Regulated software also requires compliance to safety standards like DO-178B/C and ED-12B and security standards such as DO-326A and ED-202A.

The first step to addressing these challenges is adoption of Agile planning and development processes. Moving from a traditional V-model to a hybrid W-model, which embodies the Agile spirit of working on small increments of requirements, is a key enabler for DevSecOps in A&D.

This DevSecOps approach enables companies to plan shorter iterations such as Agile sprints and to build software incrementally, including automated safety, security, and compliance verification.

Initial sprints in a DevSecOps approach focus on requirement and system design modeling, which are iteratively refined based on feedback from automated tests. In each sprint, implementation of particular components or features includes component design, implementation, unit and integration testing, and security and compliance verification.

Adoption of DevSecOps practices in A&D can accelerate software delivery, reducing the time from code change to production deployment or release while reducing security risks. Rigorous, automated security testing, which is key to adopting DevSecOps, can also validate compliance requirements. Bi-directional requirement traceability, document generation, and security tests can be done as part of the CI/CD pipeline.

Embrace DevSecOps

Capgemini Engineering has developed a range of software frameworks that can help clients adopt and improve DevSecOps implementation by performing a number of activities related to CI/CD pipelines including automated testing, simulation, safety, security, and compliance verification.

- **Avert:** Performs continuous security verification in CI/CD pipelines by orchestrating different security testing tools during various stages
- **Atlas:** An intelligent testing framework that uses AI/ML models to optimize different use cases across the test life cycle
- **Beads:** Provides a holistic view of the complete software development process and enforceable policies on software development KPIs using smart contracts
- **DevAgility:** A managed DevSecOps platform which free up resources and bandwidth from routine tasks to focus instead on creating high-value features and new, innovative capabilities.

Capgemini brings deep domain expertise built on decades of work with the A&D industry and consistently delivers tangible business results that exceed customer expectations through innovative integrated solutions and accelerators. The company helps clients comply with regulatory requirements such as DO-178B/C and DO-326A and participates in industry initiatives like SECT-AIR to develop technologies for safety-critical industries, including aerospace. Under this initiative, Capgemini conceptualized and created an open, integrated, model-based toolchain incorporating a standard reference model for the software engineering tool set.

FOR MORE INFORMATION,
PLEASE CONTACT:

Michael Denis

Senior Director –
Aerospace Strategy and
Business Architechture
michael.denis@capgemini.com

Gurpreet S. Sachdeva

Senior Director – Aerospace,
Defense and Naval
gurpreet.sachdeva@capgemini.com

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 325,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion (about $21 billion USD at 2021 average rate).

Get the Future You Want | www.capgemini.com

MACS_2022_PG

The information contained herein is provided for general informational purposes only and does not create a professional or advisory relationship. It is provided without warranty or assurance of any kind.