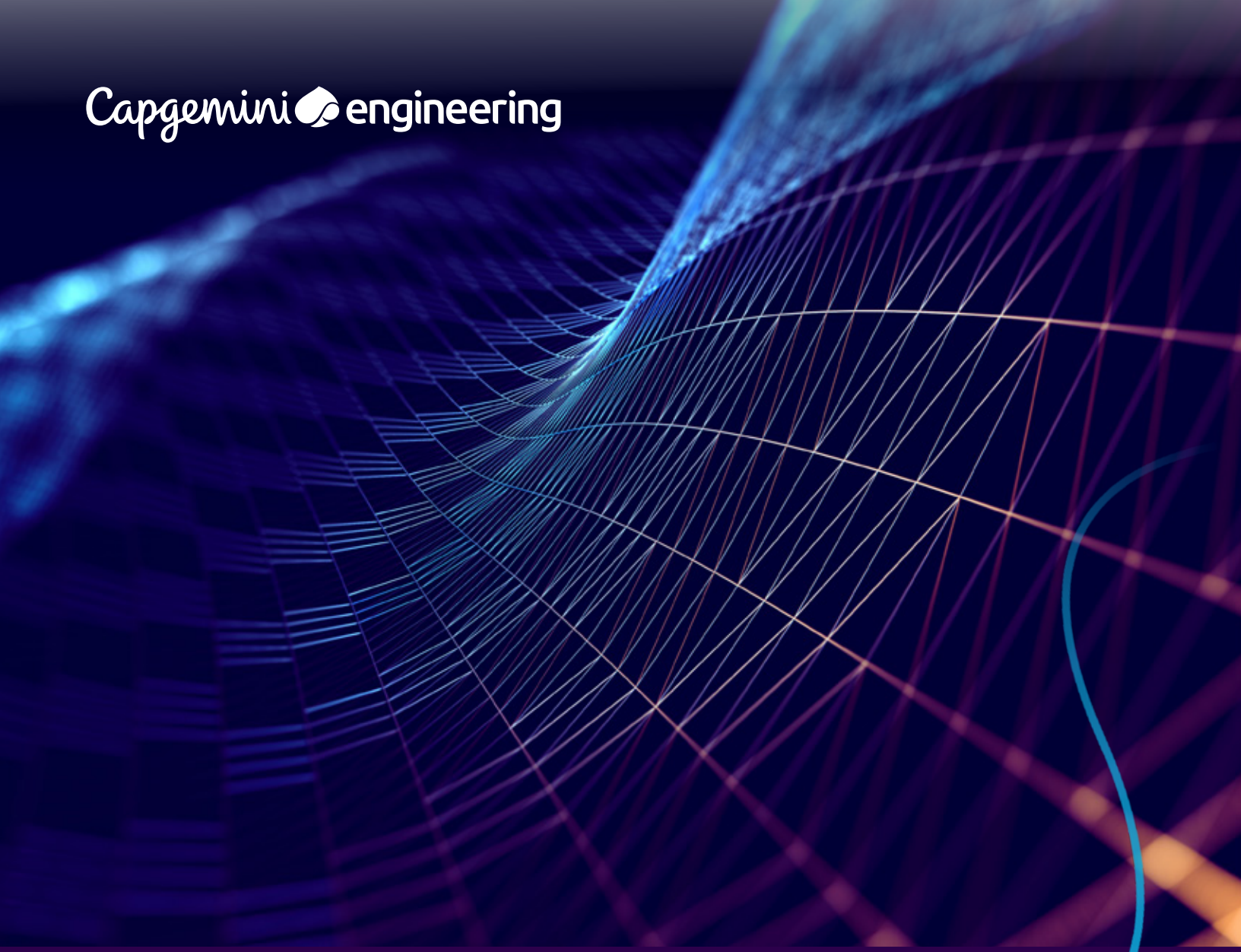
Capgemini engineering



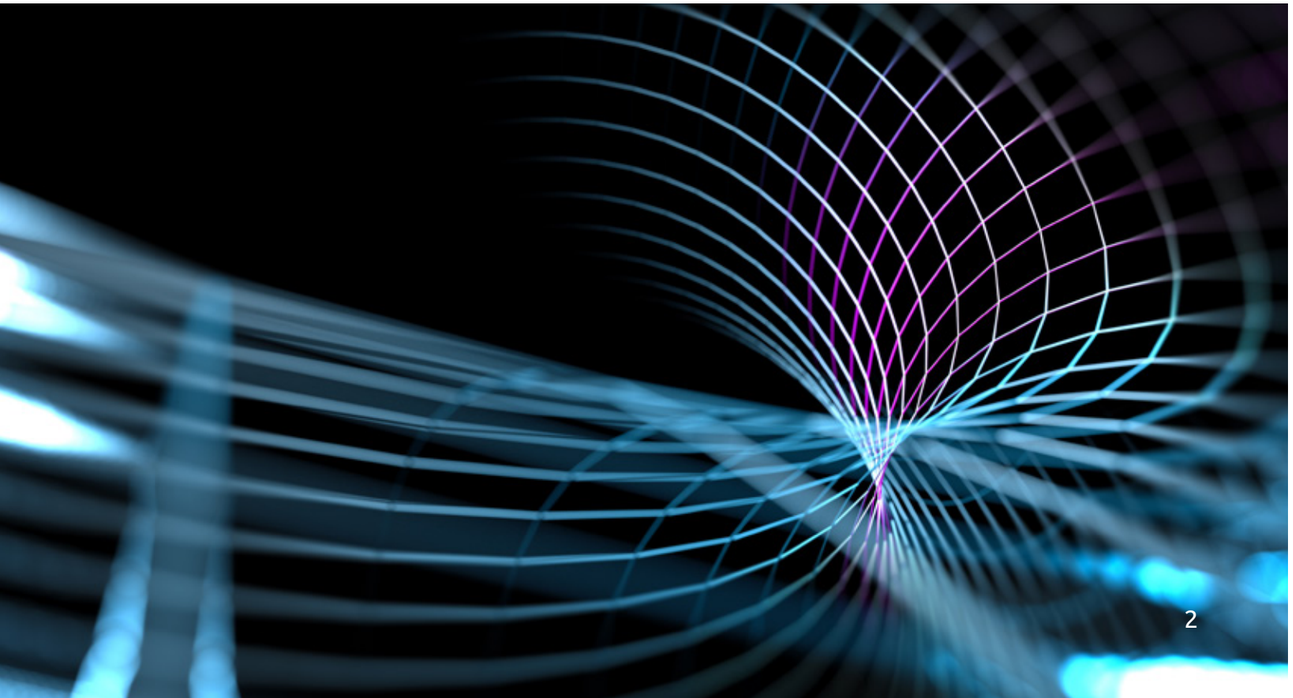
THE ADVANTAGE OF DEVSECOPS TO REGULATED INDUSTRIES

Introduction

DevOps practices enable rapid product engineering delivery and operations, particularly by agile teams using lean practices. But there is a paradigm shift occurring in DevOps to incorporate security in the end to end process. That is because security cannot be added after product development is complete and security testing cannot be a once per release activity. By including security, DevSecOps practices enable faster, more reliable and more secure software.

DevSecOps is particularly relevant for regulated industries like aerospace and automotive that follow the traditional V-shaped development cycle with manual testing and minimal software reusability. V-cycle is the traditional way of development in many industries like aerospace and automotive. It is an extension of the waterfall process, with the difference being that the process steps are bent upwards after the coding phase to form the V shape. Hardware dependencies and long support contracts lead to a huge legacy codebase with siloed software development teams. What's more, regulated software must comply with safety standards such as DO-178C, ED-12B, MISRA, and ISO 26262 and security standards such as DO-326A, ED-202A and SAE J3061.

Internet and software companies have pioneered DevSecOps practices, but they can be adapted to the unique requirements of regulated industries. Indeed, incorporating DevSecOps practices in regulated industries can optimize software development and reduce security risks. Moreover, DevSecOps minimizes the time from code change to production to deployment and release. Rigorous, automated security testing can also validate compliance requirements.



Playbook for DevSecOps adoption in regulated industries

Adopting agile and development processes is the first step to incorporating security into the DevOps process. This requires migrating from a traditional SDLC V-shaped model to a hybrid W-shaped Agile model, working on small increments of the requirements (Figure 1).

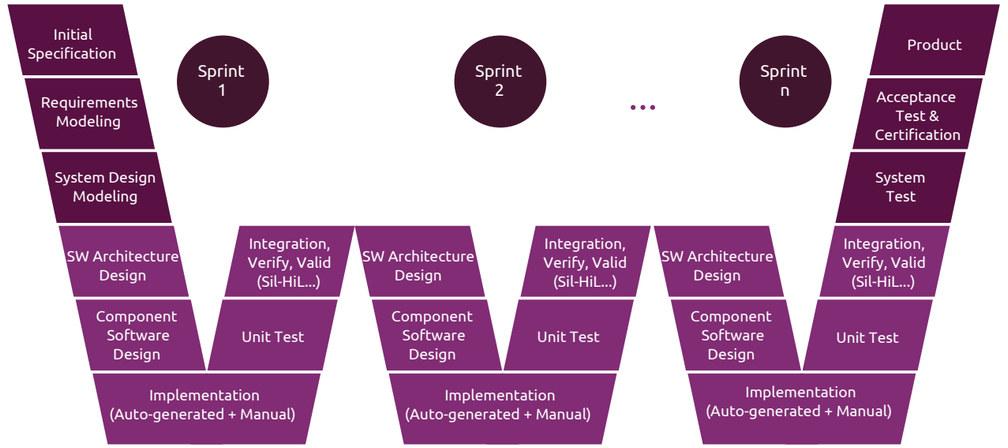


Figure 1: DevSecOps W-Shaped Model

There are eight critical elements necessary for a successful DevSecOps model:

Modern version control systems, such as Git and Bit bucket, enable integration with Continuous Integration/Continuous Delivery (CI/CD) pipelines. Legacy version control systems like clear case are not well suited to CI/CD pipelines and third party tools.

Simplified branching strategies that leverage modern source control systems reduce merge conflicts, save time and streamline support for legacy codebases.

Continuous automated testing is crucial to obtain immediate feedback on a software release candidate. Static code analysis reveals potential vulnerabilities and verifies compliance with standards such as DO-178C and MISRA. Unit testing with adequate coverage verifies individual components. And automated functional testing verifies the integration of different units.

Continuous security testing verifies that systems and applications are analyzed for vulnerabilities in a continuous cycle. Different checks and verifications such as threat modeling, secure coding guidelines, software composition analysis, static analysis, vulnerability testing, and penetration testing help fix flaws incrementally as the features are implemented.

Bidirectional requirements traceability is essential for compliance with standards like DO-178C and can be performed automatically. User stories, tasks, code commits, unit and integration tests, functional tests and production incidents can all be linked to requirements.

Automated documentation generation can be done incrementally in every sprint. Inputs can include requirements, system models, component design models, test plans and source code.

Compliance with standards like do-178c can be performed by developing software in accordance with policies that clearly state quality, safety, security and compliance goals.

Continuous delivery pipeline enables software deployment and automated security verification. After automated unit testing, the generated binaries should be versioned, tagged and stored in a repository. Simulators and virtual prototypes should be used for functional and system testing.

The Capgemini Engineering DevSecOps software accelerators

Agile and DevSecOps practices are Capgemini Engineering's default for software development. DevAgility is our centralized DevSecOps platform, consisting of a curated set of open-source and commercial DevOps tools (See Figure 2). Capgemini Engineering has integrated four inhouse software accelerators in the DevAgility platform: Avert, Atlas, Tantem and Beads. These tools help in various activities such as source code control, build integration, continuous integration and continuous delivery. To date, nearly 600 customer projects consisting of 6,500 engineers have been onboarded to the DevAgility platform in a phased approach. Engineering agility metrics are used to track project adherence to DevOps practices.

Capgemini Engineering's use of DevAgility has delivered the following benefits to our customers:

- **Engineering transformation** using DevSecOps as the default for all customer projects
- **10% To 30% agility improvement** in developer productivity, build frequency and cycle time
- **30% Increase** in DevOps maturity
- **Reduction in release cycle time** from months to a couple of weeks

The four software accelerators that Capgemini Engineering uses make the customer transition to DevSecOps faster and more effective by performing specific activities: automated testing, simulation, safety, security and compliance verification.

- **Avert:** Performs continuous security verification in CI/CD pipeline 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
- **Tantem:** An Automation-as-a-Service platform that uses a behavior driven development approach and unified portal for test environment creation and end-to-end automation
- **Beads:** Provides a holistic view of the complete software development process and enforceable policies on software development KPIs using smart contracts

Source: Compiled by Capgemini Engineering

Capgemini Engineering can support DevSecOps adoption by regulated industries with our full spectrum of DevSecOps practices that are very similar to practices used by software and internet companies. Combined with our managed DevSecOps platform, Capgemini Engineering can free up clients' resources and bandwidth from routine tasks so they can focus on creating high value features and new, innovative capabilities.

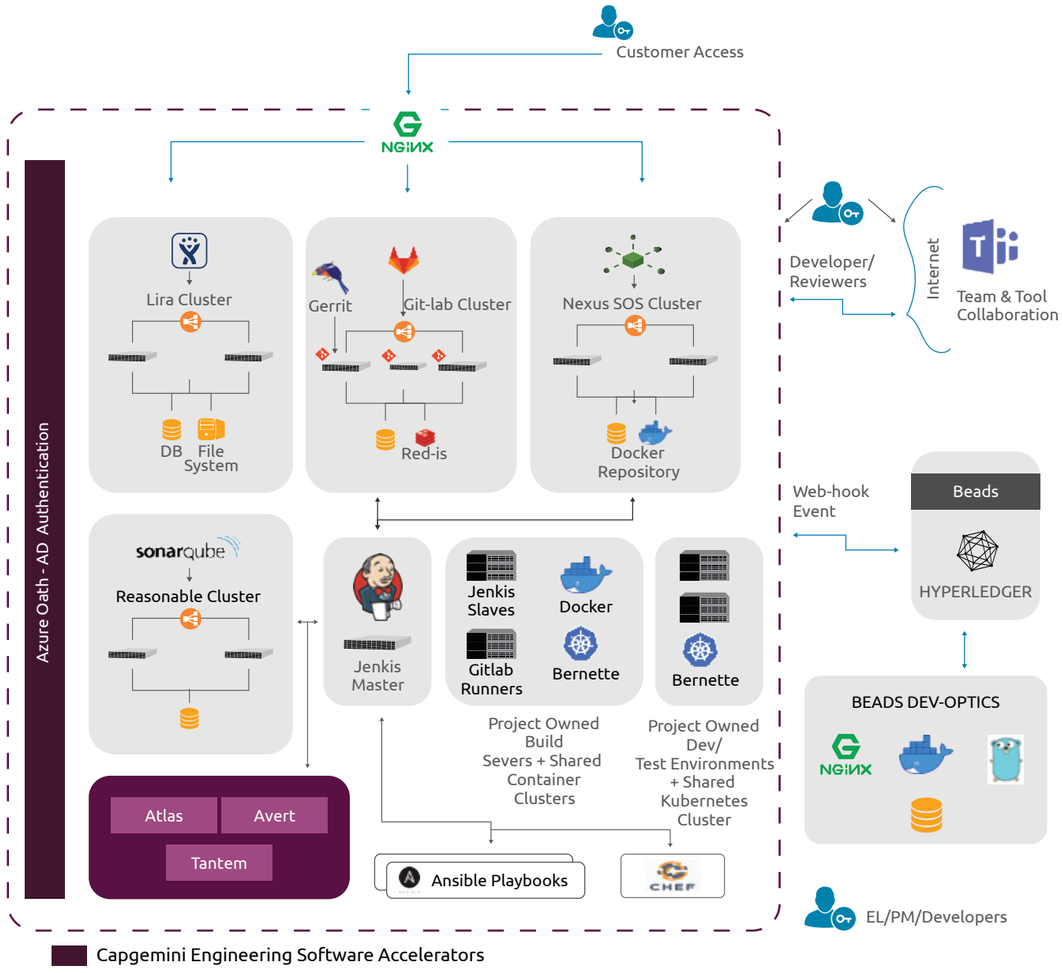


Figure 2: DevSecOps W-Shaped Model

Why Capgemini Engineering?

Capgemini Engineering brings deep domain expertise to customer engagements built on decades of work with regulated industries, including aerospace, automotive, industrial equipment and life sciences. We consistently deliver tangible business results that exceed customer expectations through our innovative and comprehensive integrated solutions and accelerators. Capgemini Engineering's software development experience includes compliance with regulatory requirements such as DO-178C and MISRA. Also, we provide the methodologies and tools to ensure compliance with all relevant safety and security standards (See Figure 3).

Capgemini Engineering participates in industry initiatives like SECT-AIR to develop technologies for safety-critical industries like aerospace. Under this initiative, we conceptualized and created an open, integrated, model based toolchain incorporating a standard reference model for the software engineering tool set. Also, Capgemini Engineering is working towards reducing the use of formal methods for developing and maintaining requirements.

Capgemini Engineering's best practices are built on our cross industry experience and unique combination of software skills and domain expertise in regulated industries.

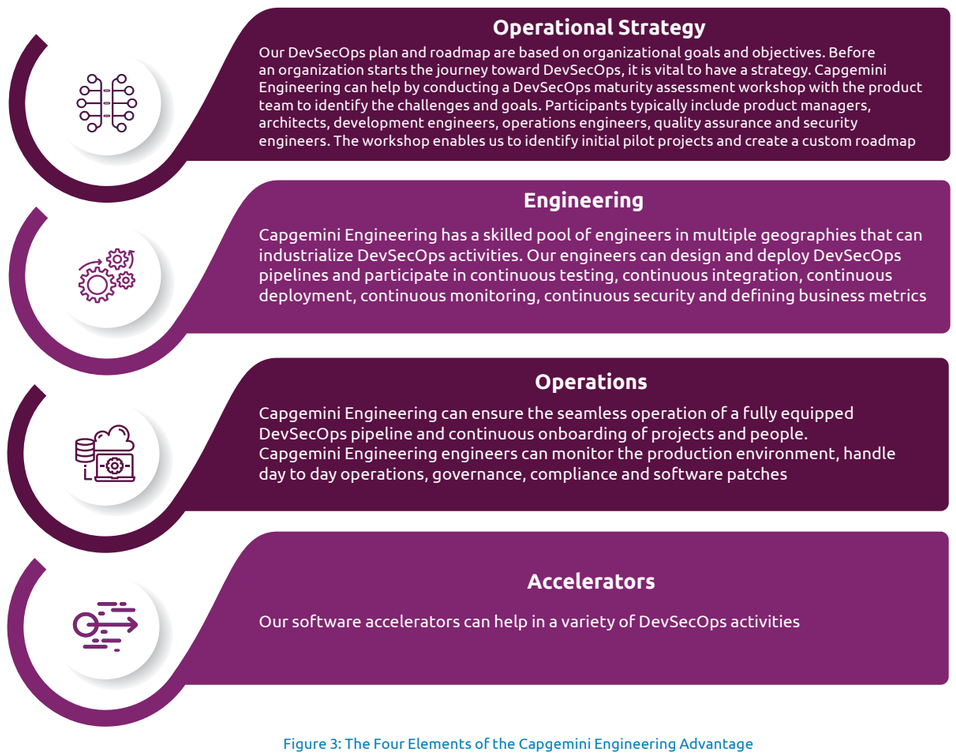


Figure 3: The Four Elements of the Capgemini Engineering Advantage

Capgemini engineering

About Capgemini Engineering

Capgemini Engineering combines, under one brand, a unique set of strengths from across the Capgemini Group: the world leading engineering and R&D services of Capgemini Engineering – acquired by Capgemini in 2020 – and Capgemini's digital manufacturing expertize. With broad industry knowledge and cutting-edge technologies in digital and software, Capgemini Engineering supports the convergence of the physical and digital worlds. We help clients unleash the potential of R&D, a key component of accelerating their journey towards Intelligent Industry. Capgemini Engineering has more than 52,000 engineer and scientist team members in over 30 countries across sectors including aeronautics, space and defense, automotive, railway, communications, energy, life sciences, semiconductors, software, and internet and consumer products.

For more details, contact us:

www.capgemini-engineering.com

Write to us at:

engineering@capgemini.com