

DevSecOps

Process improvement through secure automation and collaboration



Modern software is disrupting entire industries and forcing organizations to change how they think about their development activities. While today's development teams focus on the speed of delivering new features, operations teams concentrate on stability and reliability. This conflict delays releases and business agility is lost. Additionally, with this laser focus on speed-to-market comes increased vulnerabilities and risk.

Using development operations (DevOps) concepts, based on effective collaboration between development and operations teams and extensive automation, Perspecta builds in a security component, early in the development life cycle, to securely expedite the delivery of mission capabilities.

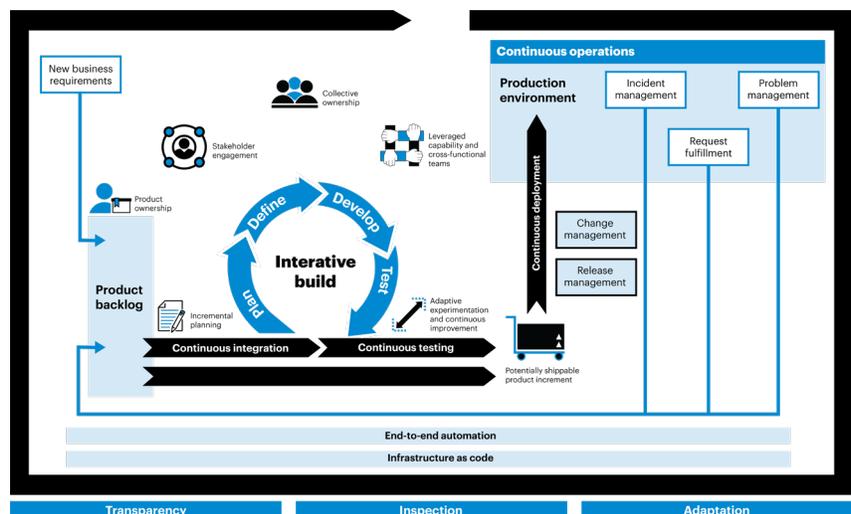
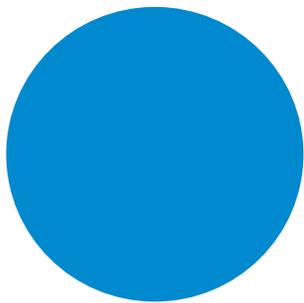
Defining DevSecOps

DevSecOps is all about people, process, and technology, and applying lean principles and automation to drive better collaboration between your applications delivery and IT operations teams. Defining organizational goals as focused and shared metrics that are tied to benchmarked stages to share

successful patterns to continuously improve the organizational efficiency. It extends the agile mindset incorporating operations and security into the process.

Perspecta's DevSecOps solution provides an environment for both development and operations teams to collaborate and automate software delivery life cycle processes securely. By leveraging open-source tools we are able to integrate the software delivery pipeline and automate software delivery end-to-end. The open-source tool integration accelerates the continuous integration process, and our built-in security processes ensure you identify critical security requirements when it's most effective and efficient—early in the development life cycle. The DevSecOps solution can be deployed in a public or private cloud or at on-premise data centers.

Perspecta partners with you in your DevSecOps journey to securely drive delivery efficiency and relevance of technology solutions. Trusted advice, cost-efficient implementation and flexible governance maximize the end-to-end value enable agility and realization of your digital strategy.



Maximizing the value of DevSecOps

Adaptive automation

- We develop the most effective customer-specific automation solution that maximizes quality and efficiency and is easily deployed through code. Our expertise in application programming interface-centric integration allows us to leverage your existing technical environment and maximize ROI

Human-centric design

- Design thinking and user experience practices are embedded in our methodologies. This assists in operationalizing innovation and delivering accessible, hyper-personal solutions to maximize the adoption, use and relevance of cross-platform solutions

Industrialized continuous delivery

- Our industrialized delivery model employs the best talent, methodologies, tools and industry assets across multiple geographies. This capability can be scaled and distributed to effectively align with your business cycles and strategies
- Continuous testing, end-to-end quality management, and collective ownership of security through the DevSecOps pipeline ensure continuous delivery of high quality and secure solutions

Accelerated transformation

- We use a proven and repeatable approach to transformation to quickly jumpstart and accelerate digitalization. We leverage the latest technology and apply lean, agile and DevSecOps components appropriately and with careful consideration of the existing environment

Responsive governance

- Value management dashboards that provide predictive and prescriptive analytics complement our portfolio, program and project governance processes to amplify feedback, monitor value delivery, and provide guidance for relentless improvement and continuous business alignment

Security built in

- Early integration of quality and security
- Solutions designed with the 'defense in layers' principal to minimize exposed surfaces and prevent an entire system from being compromised
- Automated security assessments to detect potential vulnerabilities to static and dynamic code and runtime patterns