Præcipio Consulting
Good process, well practiced. ™

DevSecOps

DevOps is the name given to a philosophy where the development team and operations team actively communicate and are often part of the same cross functional product team. DevSecOps includes the security team and security practices into the development process. In this way every developer, operator, and other team member considers security implications in their work. There are myriad combinations of the term, which for simplicity is called DevOps, meaning the practices and processes used to ensure that all stakeholders are a part of the process from ideation to release into production.

> ⓘ DevSecOps is practiced by governments around the world. This is a necessary change to be successful in your mission. The focus on continuous improvement allows teams to aggregate small changes over time. This yields better results than waiting to implement large changes. You can take your first step today.

DevSecOps is an approach to improving communication and integration between teams and the processes that they use. Often the term DevSecOps is construed as a bespoke configuration of technologies yielding complete ephemeral virtualization of your entire tech stack. While everything-as-code is the goal, this framing of DevSecOps ignores the majority of the value that DevSecOps provides to an organization. Until a team has mastered constructive cross-function communication, and the technical domain in which they work, then automation and containerization/virtualization add complexities that the team is not equipped to manage. Imagine a calculator that claimed 2+3=6. Without understanding arithmetic you would accept this incorrect answer and every action built on it would move you farther and farther from your goal. *Without mastering the basics, quality will suffer.*

> *DevSecOps stresses secure communication, collaboration, and integration between software developers and other stakeholders in the software delivery lifecycle.*

"https://wwwqasympohy.com/blog/understanding-devops-simple-matury-model/

At Praecipio Consulting, we work with our customers to model their processes, improve communication, and finally to begin to automate away areas in which the team has achieved mastery.

Security at the forefront

> It is not about ***if*** but ***when*** a system will be compromised. Damage is reduced when a system is designed to minimize the attack surfaces, slow a determined attacker down with layers of defense, and uses active monitoring to notify first responders.

DevSecOps stresses the consideration of security posture at every point in the process. For Praecipio Consulting customers, this means security in people, process, and technology. People are the best attack vector and one of the hardest to defend against. Process provides assurance that the correct actions are being taken and provide a mechanism to slow down design and decision making to include security, quality, and not just functionality. In terms of security best practices, the technology layer is one of the most well defined. Still, with the complex technology stacks and pace of change, there is ample room for exploitable vulnerabilities to put a system at risk. Below are some of the areas that Praecipio Consulting considers in DevSecOps engagements.

- **People:** Build defensively, every team member focuses on security in design, build, and release. Enable everyone with security awareness training, and simulated social engineering penetration tests
- **Process:** A common understanding of the relevant metadata and flow of work through a pipeline ensures all levels of the team understands what to do. Routinely review the process for risk and efficiency (e.g. IT Risk Management Program, and business analysts to ensure the pipeline is minimizing risk while being effective for the team).
- **Technology:** Reduce the attack surface. Whether hardening static infrastructure or containers, the goal is to apply many layers of security to slow an attacker down, and monitor every level to know when an attack is occurring.
  - Static code analysis and security scanners like Snyk identify issues in the code base and its dependencies (most vulnerabilities are introduced via 3rd party dependencies)
  - All traffic is blocked other than the minimum required traffic between systems on specified ports (e.g. a web application only exposes port 443 to the public internet)
  - All systems adhere to standards and best practices such as OWasp Top Ten, FedRAMP

Why should your agency care?

Software and Cybersecurity pervades all aspects of any agencies' mission and being reactive could mean more than falling behind. China, Russian, and North Korea are just a few who have begun implementing DevOps.

Contact federalsales@praecipio.com[1] for further discussion around best next steps to start implementing DevSecOps.

[1] mailto:federalsales@praecipio.com