DevOps Advanced

DevSecOps, Continuous Testing & Delivery

Security is everyone's responsibility as demonstrated in the rising trend in enterprise interest in DevSecOps. Security is integral to protect the business and enforce internal and external policies of the company. The operating models such as DevSecOps and SecOps might be confusing at first, but at a closer look, the most important thing to know is that they are somewhat similar philosophies. While DevSecOps makes security an equal consideration alongside development and operations, SecOps focuses more on integrating the security and operations teams. According to the third Upskilling DevOps survey participants, DevSecOps achieved a must-have percentage vote of 56% in the automation tool category. DevSecOps is a critical domain. According to a survey conducted by SecurityCompass, 75% of enterprises in the US and UK have adopted DevSecOps in 2020.

Continuous integration is a DevOps software development practice where developers regularly merge their code changes into a central repository, after which automated builds and tests are run. Continuous integration most often refers to the build or integration stage of the software release process and entails both an automation component (e.g. a CI or build service) and a cultural component (e.g. learning to integrate frequently). The key goals of continuous integration are to find and address bugs quicker, improve software quality, and reduce the time it takes to validate and release new software updates.