Role of DevSecOps in Digital Transformation

Organizations are transitioning to a new era of security policies as cloud migration becomes more common. Infrastructure is being considered as if it were a piece of software. This enables DevOps teams to quickly create and provision a development environment (servers, storage, and network) at scale. This is all done through an automated script, which cuts down on the cost and time it takes to deploy application services.

While continuous integration and continuous code development are both relatively well practiced and understood, security testing is not. Security specialists must have abilities in web development, cloud infrastructure deployment, architecture, and, of course, security to manually test or assess an application on a cloud platform. The security issues involved can be foreseen and resolved with DevSecOps.

DevSecOps is in the early phases of widespread adoption, according to the Gartner Hype Cycle for Agile and DevOps, 2020. Gartner estimates a 20-50 percent market penetration among DevSecOps' target audience, placing it on the Hype Cycle's "Slope of Enlightenment."

DevSecOps addresses an organization's development, operations, and security needs. The basic goal of DevSecOps is to get everyone in an organization to take security seriously. It intends to make security decisions as simple as development and operations. Businesses must first adopt DevSecOps and adjust their culture before they can adapt digitally.

Using DevSecOps technology, it is possible to include security into applications early in the development process. Establishing business-critical security services and recognizing potential security concerns are examples of this. Continuous integration can aid in the reduction of compliance costs and the acceleration of product delivery.

How does DevSecOps add value to digital transformation projects?

Enhanced performance: DevOps applications boost the performance, speed, functionality, and scale of your mission-critical application to new levels. These apps, however, are usually slow due to a lack of compliance and strong security. DevSecOps comes in handy in this situation. DevSecOps combines development, security, and operations when it's implemented into your software development cycle.

Increased security: In the absence of stringent security, malware that was mistakenly introduced into your application during the development stage could be transmitted to your customers. This is detrimental not only to your brand's reputation but would result in a loss of customer loyalty. Hence, it is important to ensure tight security throughout the development and operational phases. Using DevSecOps, every developer and operations administrator can prioritize security at every level of the development and delivery of mission-critical apps.

Faster delivery: Speed of product delivery is increased by incorporating automated security tests versus adding security testing at the end of the lifecycle. This leads to faster detection

and recovery of threats. By discovering and correcting security concerns earlier in the development lifecycle rather than in production environments, the pace of delivering products is accelerated.

DevSecOps helps organizations achieve speed and resilience in their agile development and cloud migration processes while also increasing compliance and security. It enables businesses to rethink development models and re-architect collaborative security-by-design procedures. Instead of waiting till the development phase to examine and find security issues, developers must use DevSecOps technology early in the CI/CD process to find code problems. This technique will assist developers in fixing security gaps and lowering security dangers before they reach production infrastructure.