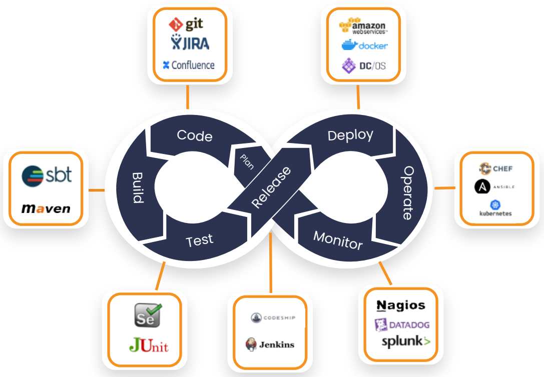
An article on

ADOPTING DEVSECOPS

WHAT IS DEVOPS

With a rapid increase in public cloud, microservices and, containers, Organizations need to adopt the DevOps culture to develop, operate, and maintain applications and IT infrastructure, both onsite and in cloud environments. DevOps proves to be a solution that can easily blend both IT development and IT operations to aggregate several functions like specifications and requirements, coding, testing, operational readiness, implementation, and more. For organizations that employ an agile approach, DevOps is just an extension to the agile software development process to expedite market deliveries with less human interaction. With Continuous Development and Integration (CD/CI), DevOps bridges the gaps between development and operation activities.



But is your App secured? Are you one of those organizations that rely on successful launch and expect profitability or are you one of them who can take a risk by compromising on the security and ready to deliver a product that can be easily attacked by cyber criminals? The choice is yours!

While DevOps is the preferred solution, mitigating security risks and vulnerabilities is also equally important. With today's changing IT world and so many uncertainties', DevOps is often at risk due to the rapid development of code and releases.

The traditional security challenges are also involved where people think that if security is implemented, there would be a delay in the development cycles. There are also a lot of threats involved if security is unseen just for the sake of speedy deliveries. With increasing cyber-attacks and frauds, negligence, or a compromise with the security of DevOps environment can risk the entire software development and delivery.

The question is, how to integrate security?

The answer is DevSecOps

A bit of the conversation I had with one of my IT friends:

Me: Hey Chris, have you heard about the latest trends in IT Development?

Chris: Oh! Do you mean DevSecOps?

Me: Wow! It is really catching up some pace. So, hope you know everything about it

Chris: Yeah, I have read about it, but we have not implemented it yet. Is it really that important or just a hype?

Me: Chris, you should really read my article and get in touch with me if in case you ready to implement it. My organization will surely do it for you.

WHAT IS DEVSECOPS? LET US KNOW WHAT IT IS.

DevSecOps is nothing but Development, Security and Operations. It is an automated framework with a shared objective of everyone involved in the DevOps lifecycle or the software development lifecycle to inherit best practices that can safeguard the entire DevOps environment through strategies, policies, processes, and technology. Every member of the product lifecycle is allocated responsibilities to ensure improved collaboration and accountability for security.

Unfortunately, DevSecOps is still not widely implemented today, and it certainly needs to be considered.

WHY SHOULD YOU CONSIDER DEVSECOPS?

Considering DevSecOps is to seek:

- Best alternative to the traditional security practices. Security risks and vulnerabilities are caught at a very rapid and early stages of development.
- Automated Security means security is not applied at the final stage of development cycle.
- No more a siloed team to manage development, operations and security which also results in reduced cost and faster delivery.
- Ensures strict governance and compliance. Which means everyone working in the product development cycle are accountable.

IMPLEMENTING DEVSECOPS

While DevSecOps brings development, security, and operations teams together, it is difficult to implement this initiative unless there is a proper teamwork and understanding of security practices. The foundation of successful DevSecOps initiatives is an effective, enterprise-wide automation strategy. To implement this, consider the below checklist:

- **Workflows and Processes:** Different tools, practices and several processes can disrupt collaboration, visibility, and productivity in cross-functional initiatives like DevSecOps. Standardizing workflows can allow various teams to come together easily and share their ideas, information, and best practices. Automating your life-cycle operations provides an ideal opportunity to create consistent, repeatable processes that simplify interactions between development, IT infrastructure, and security teams. Create an automation tool that can deliver a unified, user-friendly automation foundation that promotes collaboration, transparency, and consistency across all aspects of your IT environment, including applications, security, networks, and infrastructure.
- **Team Collaboration**: Brining teams together to work on a common objective is important. Teams with contrasting goals cannot collaborate effectively. Assigning responsibilities for the overall outcome of the development must be considered. A platform where teams can collaborate and share ideas to work together should be built. This in-turn helps in designing workflows that can help in streamlining the process. A proper team alignment ensures best and faster results.
- **Automate Security throughout the application lifecycle:** Automating security throughout the application lifecycle ensures security checks at every stage of the application development or customization.
- **Security Trainings:** Security trainings will ensure that every member of the team is aware of the security guidelines and compliance is monitored.

- **Scale with Cloud Technologies:** Cloud technologies - including containers, Kubernetes, and public cloud services—can help you implement DevSecOps at scale. Deploy these technologies alongside cloud-ready, container-specific security and management tools, certified container images, and trusted third-party security products to protect your DevSecOps environment and organization. Adopt an application programming interface (API) first approach to ensure interoperability. Use Artificial Intelligence (AI) and Machine Learning (ML) technologies to address security decisions and adapt your infrastructure security and application development processes.

DEVSECOPS – BEST PRACTICES

Building secure software while keeping up with the speed and scale requirements of the market is a paradox for modern IT organizations. Companies often face a common set of challenges when moving from DevOps to DevSecOps, and they can be addressed by employing these DevSecOps best practices.

- Foster a DevSecOps culture and mindset
- Enable teams to build security in
- Choose When first, not Which
- Automate tools and processes
- Start early and start small
- Be in a continuous state of compliance.
- Always be prepared for threats.
- Invest in advanced training.
- Threat security vulnerabilities as software defects
- Measure every step & Learn from failures
- Pursue scalable governance

Published on: 05 July 2021