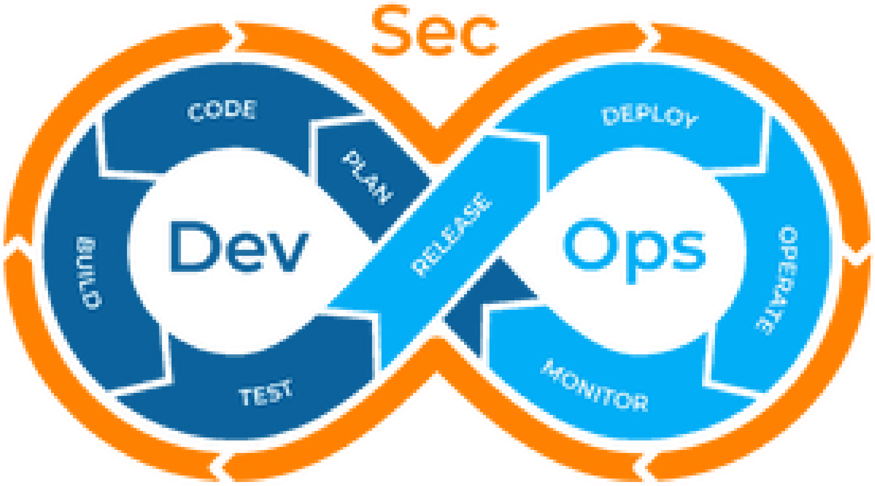
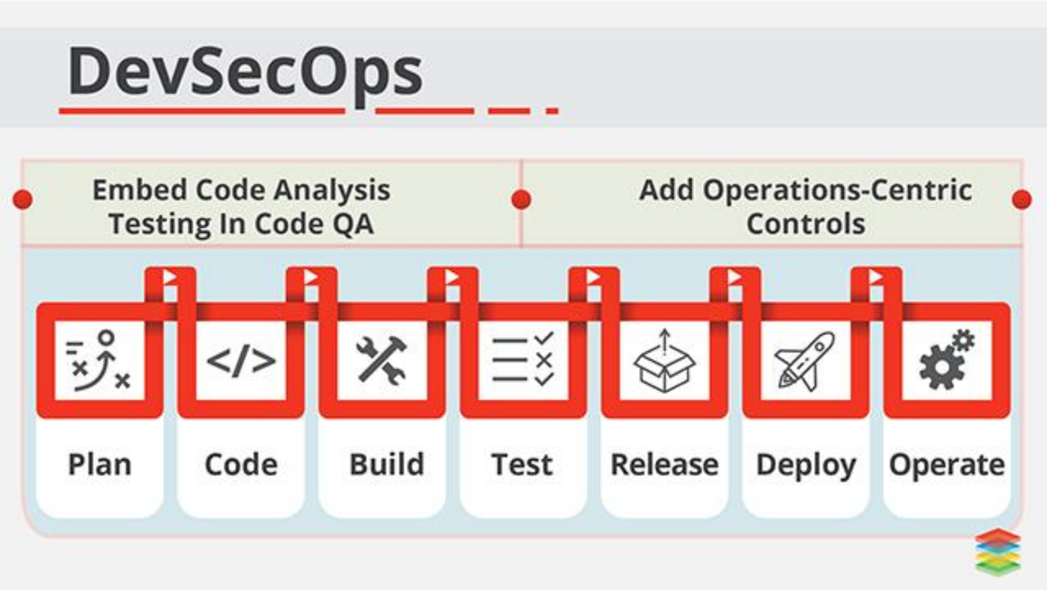
DevSecOps

DevSecOps = Development + Security + Operation
We can also say Securing DevOps. Securing DevOps is making sure that organizations operate securely and protects data of their customers. This works on a model called "Continuous Security" which focuses and provide security to various components of DevOps Strategy.
DevSecOps is also called DevOps Security which is a practice to make sure about security of infrastructure and applications from start. It means automating security gates to prevent DevOps workflow from slowing down. DevOps Security is basically built for Container and Microservices. DevOps teams automate security to protect the overall environment and data, including continuous integration/continuous delivery process which are the goals that include the security of microservices in containers. It works on CIA tried i.e. Confidentiality, Integrity, and Availability. Confidentiality means keeping sensitive information private. This involves ensuring that only who have authority to access and preventing that are not authorized.
Integrity means ensuring the quality. This ensures that data has not been tempered and can be trusted. Integrity includes hashing, digital signature, and audition and version control.
Availability means that system, network and applications are running. It ensures that application is available for users who all have authority.



Organizations are adopting DevOps as early as possible. As DevOps makes our development and deployment of a project more quickly. Because of fast delivery, forget about the security aspect involved with the changes. DevOps require more security at each phase and has to be taken seriously. Proper security check at each phase of DevOps makes sure error free deployment. Satisfying customer needs and better quality is the goal of any organization but not forget to secure the customer data.
In software development field, CI/CD pipeline is used for continuous Integration/Continuous Development which makes possible rapid changes according to demand and customer feedback.


DevSecOps
Embed Code Analysis Testing In Code QA
Add Operations-Centric Controls
Plan
Code
Build
Test
Release
Deploy
Operate

Security is important from the beginning as we need to shift our security in beginning of DevOps cycle to make sure we don't have anything at the end that may delay from moving fast.
Security and compliance within DevOps. In such a distributed environment and fast delivery companies need to adopt more micro level security across application and infrastructure and have multiple line of Defense.

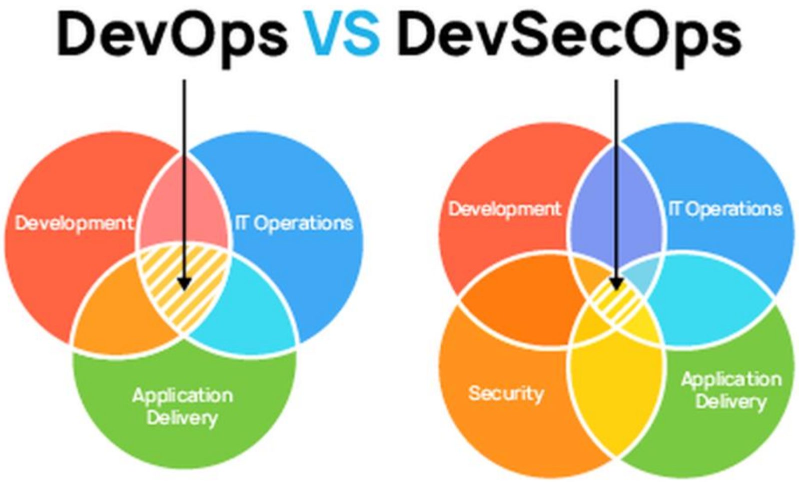
Why Security important for DevOps

- DevOps secrets include SSH Keys, API Tokens which is used by Human and Machines. Inadequate Security measures can lead to providing vulnerabilities for attackers which will help them to steal information of project as well as organization.
- As different teams involved like development, deployment, QA and Operation. Since many people involved, there are chances of errors. So security should be highlighted in the beginning of DevOps implementation else it could be dangerous for the whole plan.
- DevOps is about automation and speed, Number of tools used, and tools you selected might be vulnerable which leads to security issue which make the app exposed to malicious attack. So, it is important to choose tools with the security concerns and policies. Tools Like Chef, Puppet and Salt need security managements.
- Each phase needs security check to ensure deployment error free. Focus on Security makes more frequent control, so the error can be reduced easily.
- Rising DevSecOps is adding security in DevOps cycle which tends to minimizing vulnerabilities and make product more secure. This model ensures that everyone is responsible for Security not only one person. Its objective is to implement security decisions on the same scale as Development and Operation, and make everyone responsible for security.

IT security must also play an integrated role in the full life cycle of your apps to take full advantages of the agility and responsiveness of a DevOps approach.

How to Ensure Security

- Focus on security in life-cycle
- Developers should be aware of security principles and consequences
- Make sure that Developers use specific tools to keep DevOps System secure
- Make sure to set up monitoring and alerting system to avoid errors at the end
- Maintain proper report to assure everything under control and it almost makes further analysis easier.
- Use identity access management and role-based access control
- Scan APIs, Codes and applications regularly
- Monitor everything regularly



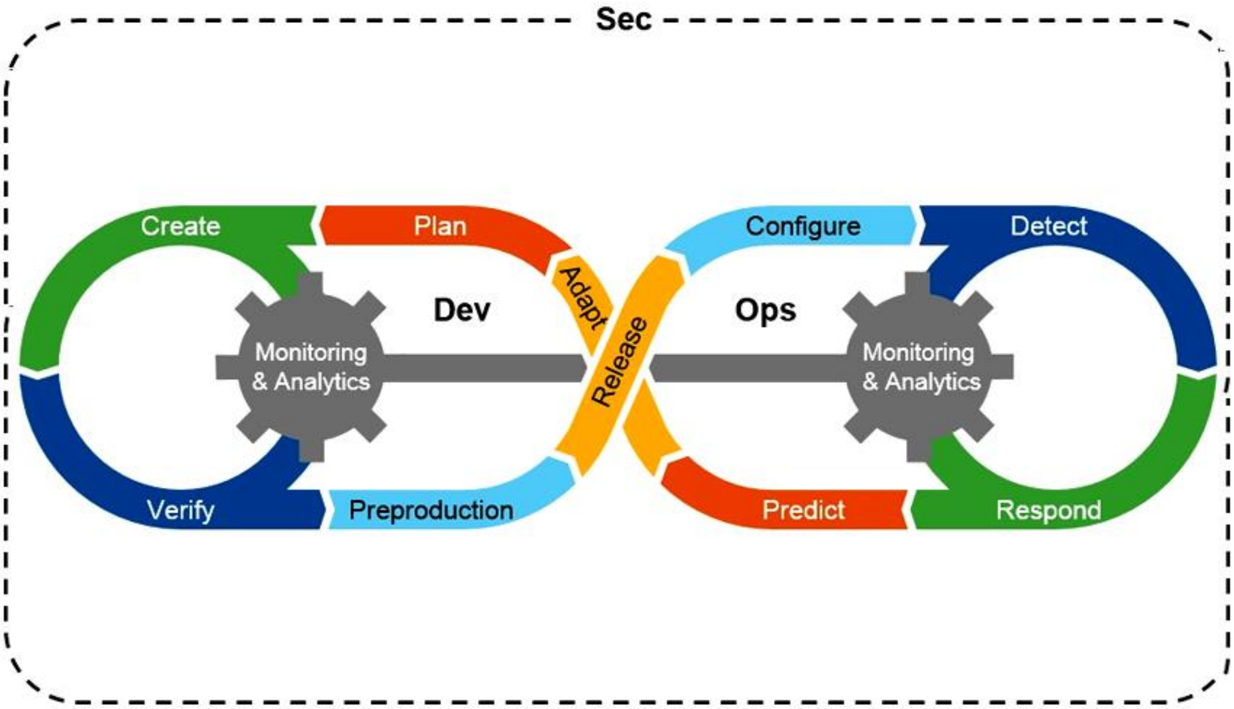
Earlier there was a security team at the final stage of the development which used to take large time months or even year but now with DevOps it is possible in weeks and by applying older security practice can lead to some disadvantage. so, it’s important to share security end to end. Which is DevOps + Security = "DevSecOps".

Security plays important role for any organization. Customers is all you have to satisfy and if there is lack of security and error occurred which makes them to feel not to trust again which will be the biggest lost for any organization, and it's not easy to gain trust again. There are hackers who are ready to breach data from your application. How will they trust you if they are sure you are keeping secure.

CONTINUOUS SECURITY

Continuous Security is a model that focuses and provides security to various components of DevOps Strategy. It composed of three areas. Each area focused on different aspects of DevOps Pipeline.

1. Test-Driven Security (TDS) – TDS Cover security control like configuration of Linux or security header the web application must implement. Applying set of controls on application and infrastructure of the organization and test continuously. These is possible by disabling SSH root login on the system, by using HTTPS by web application, latest versions must be patched of system and applications and by protecting administration interfaces behind a VPN.
2. Monitoring and Responding to attacks - It is analyzing the attacks and how to handle when occurred. This is possible by Logging and fraud detection, Detection intrusion and by responding to incidents.
3. Security Testing – Ability to evaluate how well doing. Some of these strategies can help in security i.e. by using Security techniques like vulnerabilities scanning or code analysis or by establishing bug bounty program.


Sec
Create
Plan
Adapt
Configure
Detect
Dev
Ops
Monitoring & Analytics
Release
Monitoring & Analytics
Verify
Preproduction
Predict
Respond