# Software pipelines and Google's Cloud Build

Previously, you learned about software pipelines and how they support DevSecOps culture and workflow. Software pipelines are valued for making the software development lifecycle move efficiently. They also help foster collaboration among DevSecOps professionals. Using continuous integration and delivery (CI/CD), pipelines help automate build, validation, and deployment processes.

In this reading, you'll explore examples of incorporating security into a CI/CD pipeline, and gain insight into Google Cloud's service, Cloud Build.

## Software pipelines

A **software pipeline** is a process that uses automation and tools to facilitate movement through each phase of the software development lifecycle. Software pipelines are useful because they enable developers to release changes quickly. With a software pipeline, developers can work on one piece of the application's code at a time, which means they don't interrupt other parts of the development process.

Automation plays a critical role in software pipelines. First, automation ensures consistency. Software in the pipeline is less prone to human error when tasks like security and functionality testing are automated. Second, testing is incorporated throughout the software development lifecycle, instead of being saved as a final step. This practice supports shifting left, or implementing security checks and practices at the beginning and throughout each phase of the software development lifecycle.

### CI/CD pipelines

The CI/CD pipeline is a commonly used software pipeline. CI/CD is a process DevSecOps teams use to create software and automate updates. Continuous integration, or CI, is when developers continuously create and update code that's uploaded into a shared repository.

Continuous delivery, or CD, continuously releases software builds into a testing environment. CD also stands for continuous deployment, which is an extension of continuous delivery. Continuous deployment automatically deploys builds into a production environment in real time. This means that when developers finish an update, the update is released to end users immediately.

## Security in CI/CD

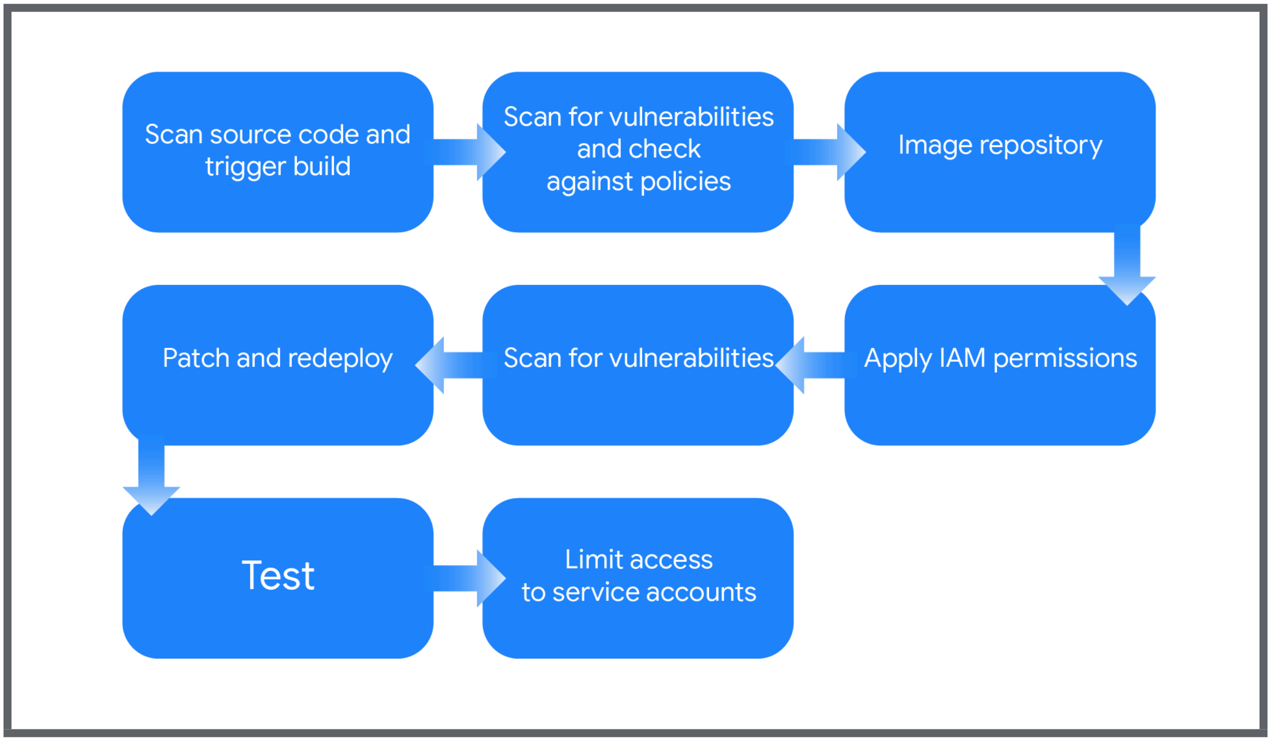
CI/CD pipelines support integrated and automated security testing. There are several steps in the CI/CD pipeline, and automation helps streamline the workflow. With automation, DevSecOps teams can introduce security tests at many points throughout the development process. The application is regularly tested without needing human intervention, which results in a more healthy application, and less time investment from developers.

Consider this example: a DevSecOps team is developing an application using CI/CD pipelines. The security team implements security checks starting at the beginning of the development process.

First, the application's source code is uploaded into the shared repository. Uploading the code triggers a build. Triggering a build is when the code starts taking shape as an actual application. At this stage, the build becomes an image. With the image created, automated scans check for vulnerabilities and policy violations. The image continues into the image, or artifact repository if it passes this round of security tests. The artifact repository is where the images are stored.

With the images in the repository, pre-set identity and access management (IAM) permissions ensure only authorized users are able to access the build image when needed. Automated vulnerability scans make sure the image is secure. If a scan detects a vulnerability, automation triggers a patch and redeploys the image. The redeployed image then undergoes another vulnerability scan.

Finally, automation enables only privileged service accounts access to the deployed builds. Service accounts are identities that are not tied to human users, but are used by an application, virtual machine, or service. They're also granted specific IAM permissions to provide more granular control over the builds. With access limited to service accounts, the builds are less susceptible to human error.


Scan source code and trigger build
Scan for vulnerabilities and check against policies
Image repository
Apply IAM permissions
Scan for vulnerabilities
Patch and redeploy
Test
Limit access to service accounts

The common thread through each phase of the software pipeline is automation. Automation lends expediency and consistency to pipelines, contributing to the efficiency and collaborative efforts of DevSecOps teams. Cloud service providers (CSPs) often offer services like Google's Cloud Build to help them integrate automation and CI/CD pipeline elements into development workflows.

## Google's Cloud Build

Cloud Build is a Google serverless service that helps build and protect software. Users can integrate code from cloud repositories or storage and create builds for applications. These builds can result in artifacts like container images.

Cloud Build strengthens security in several ways. First, it can conduct scans to identify vulnerabilities in container images, and check to ensure compliance requirements are being met. Then, organizations can review provided insights into the health of builds to identify potential bugs and address error messages. The builds are automated, which improves consistency and reduces the chance of human error.

## Key takeaways

Software pipelines are a foundational part of DevSecOps processes, with automation as an integral component of this workflow. Automation is a cornerstone of implementing software pipelines. It enhances the speed and integration of functionality testing, security checks, and build deployments. So, understanding security's role in software pipelines will improve your effectiveness as a cloud security professional.