

Tugas Kelompok
Analisis dan Perancangan Sistem Informasi
“Metodologi DevSecOps”



Oleh Kelompok 2 (IS-04-01) :

Aisyah Nabila Zahra	1204210122
Ardatika Dwi Cahyani	1204210052
Cindy Gracya Vortis	1204210026
Yuyun Ayunda Kurniawati	1204200060

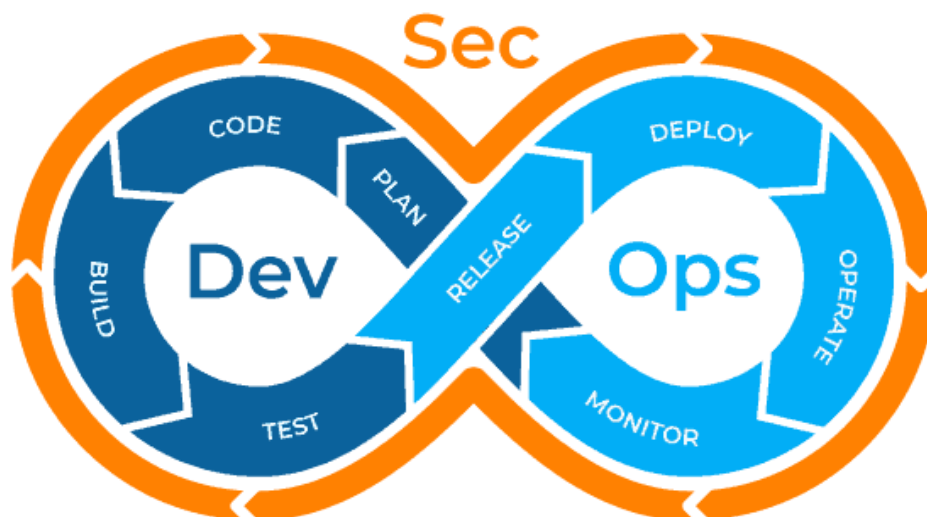
Institut Teknologi Telkom Surabaya
Fakultas Teknologi Informasi dan Bisnis
Program Studi Sistem Informasi
2023

1. Deskripsi Metodologi

DevSecOps adalah integrasi proses dan implementasi pengembangan perangkat lunak, operasi TI, dan keamanan informasi menjadi satu kesatuan dengan tujuan membangun perangkat lunak yang lebih aman dan andal. Cakupan implementasi DevSecOps meliputi *Continuous Testing, Security as Code, Threat Modelling, Risk Analysis, Monitoring and logging*, dan *Red Team Security Drills*[1].

- a. Continuous Testing atau Pengujian Berkelanjutan merupakan salah satu siklus pengembangan perangkat lunak yang memiliki kontrol keamanan dengan melakukan deteksi cacat atau error pada perubahan kode program dengan kemungkinan rollback otomatis jika diperlukan.
- b. Security as Code atau Keamanan sebagai Kode merupakan kebijakan keamanan berupa konfigurasi jaringan yang dikodifikasi dan terintegrasi dengan software development life cycle.
- c. Threat Modelling atau Pemodelan Ancaman merupakan aktivitas untuk mengidentifikasi, menjelaskan, dan mengkategorikan ancaman atau threat pada sistem aplikasi.
- d. Risk Analysis atau analisis risiko adalah siklus yang menjelaskan kegiatan untuk membuat spesifikasi desain keamanan dari awal perancangan aplikasi. Tujuan dari siklus ini adalah menemukan permasalahan dari keamanan dan membantu untuk menemukan solusi.
- e. Monitoring and logging atau Praktik Pemantauan merupakan siklus untuk mengamati parameter serta mengukur kualitas terkait dengan kontrol yang digunakan pada aplikasi.
- f. Red Team Security Drills digunakan untuk menguji keamanan dengan menirukan ancaman secara nyata dimana menggambarkan bagaimana *attacker* melakukan serangan. Simulasi ini diketahui aktivitasnya hanya oleh beberapa pihak agar hasil dari pengujian tersebut menjadi efektif dan maksimal.

2. Deskripsi Alur Implementasi DevSecOps



Penjelasan alur metodologi DevSecOps[2]:

- a. Plan yaitu merencanakan dan merancang kebutuhan aplikasi yang akan dikembangkan dengan menggunakan beberapa tools seperti Asana, Jira, dan ClickUp.
- b. Code yaitu mengetik kode untuk aplikasi yang akan dibuat dengan menggunakan tools seperti VSCode. Kemudian dilakukan proses pemeriksaan kode ke dalam repository terpusat seperti GitHub.
- c. Build yaitu proses membangun aplikasi dengan mencari feedback dan mereview terlebih dahulu terhadap code. Kemudian mengonversi file ke gambar atau file terkompresi dengan menggunakan tools seperti Docker.
- d. Test adalah langkah pengujian aplikasi yang sudah dibangun. Pengujian dilakukan secara terus-menerus hingga aplikasi mampu memenuhi kriteria tertentu. Jika sudah sesuai maka aplikasi dapat melakukan rilis.
- e. Release merupakan fase ketika aplikasi yang diuji sudah berhasil memenuhi kriteria pengujian dan siap untuk dirilis.
- f. Deploy yaitu melakukan penerapan terhadap aplikasi sehingga aplikasi dapat digunakan oleh pengguna menggunakan tool seperti AWS CodeDeploy, Jenkins dan lain lain.
- g. Operate yaitu tahap memastikan bahwa sistem yang dioperasikan sudah memenuhi kebutuhan keamanan dengan cara mengintegrasikan pemantauan keamanan, *logging*, dan dapat melalui umpan balik pengguna jika menemukan kesalahan atau *bug*.
- h. Monitor yaitu tahap untuk melakukan self assesment atau evaluasi dan memantau aplikasi yang sedang dikembangkan terhadap hambatan di masa mendatang.
- i. Tahap terakhirnya yaitu mengintegrasikan aspek keamanan ke semua tahap di atas. Sehingga dapat mengurangi resiko yang akan terjadi dan meningkatkan kepercayaan pelanggan terhadap aplikasi yang sedang dikembangkan.

Referensi :

- [1] S. Wrycza and J. Maślankowski, Eds., *Information Systems: Research, Development, Applications, Education: 12th SIGSAND/PLAIS EuroSymposium 2019, Gdansk, Poland, September 19, 2019, Proceedings*, vol. 359. in *Lecture Notes in Business Information Processing*, vol. 359. Cham: Springer International Publishing, 2019. doi: 10.1007/978-3-030-29608-7.
- [2] S. Riyadi, “Adopsi Metode DevOps Sebagai Acuan Pengembangan Aplikasi Bantuan Hukum”.