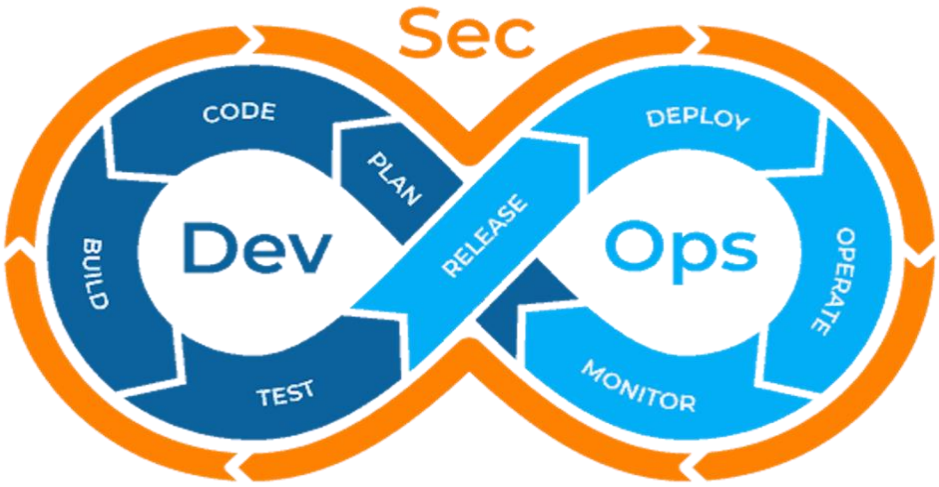
۱. مقدمه

توسعه عملیات (DevOps) مجموعه‌ای از روش‌ها و فرایندها و ابزارهایی است که با تمرکز بر ارتباطات و همکاری و یکپارچگی بین تیم‌های توسعه نرم‌افزار و عملیات فناوری اطلاعات، ارزش‌های تولیدشده را به‌طور سریع و مداوم به مشتریان نهایی می‌رساند. ادغام کلمات اختصاری «Dev» و «Ops» به این موضوع اشاره می‌کند که توسعه و عملیات، دو تیم سابقاً مستقل و کاملاً جدای از هم، جای خود را به تیم‌های چندتخصصی با مهارت‌ها و روش‌ها و ابزار یکپارچه داده است. در کنار DevOps مفهوم توسعه، امنیت و عملیات (DevSecOps) به عنوان نسخه تقویت شده معرفی شده است تا امکان ادغام اقدامات امنیتی در رویکرد DevOps را فراهم کند. هدف این رویکرد یکپارچه سازی امنیت به عنوان یک مسئولیت مشترک در کل چرخه حیات فناوری اطلاعات (برخلاف مدل سنتی تیم امنیتی متمرکز) می‌باشد.

فرآیند DevSecOps شامل چندین مرحله می‌باشد که در نمودار زیر نمایش داده شده است. لازم به ذکر است که از لحاظ فنی، امنیت در هر جنبه ای از چرخه DevOps یکپارچه شده است و مانند توسعه و عملیات از هم جدا نیست.



شکل ۱ – چرخه DevSecOps

۲. ساعت اول: بررسی چرخه DevOps و DevSecOps

در این کارگاه در ابتدا چرخه DevOps که شامل مراحل زیر است بررسی می‌گردد:

- طرح ریزی(Planning)
- توسعه(Development)
- تست(Testing)
- گسترش یا استقرار(Deployment)
- نگهداری(Maintenance)

در این کارگاه ابتدا فرآیندها و رویه‌های هر یک از موارد بالا بررسی می‌گردد. روندهای بررسی امنیتی و نحوه تضمین امنیت در هر مرحله بر اساس best practiceها معرفی می‌شود.

۳. ساعت دوم: بررسی ابزارهای مورد استفاده در هر یک از گام‌های چرخه DevSecOps

در واقع DevSecOps با استفاده از استانداردهای امنیتی سختگیرانه در هر مرحله از روش‌های مرسوم تولید نرم افزار به دنبال تضمین امنیت می‌باشد. مراحل اصلی چرخه حیات توسعه نرم افزار (SDLC) شامل برنامه ریزی، کدنویسی، ساخت، آزمایش، انتشار و استقرار است. بعد از معرفی چرخه DevSecOps و دلایل اهمیت و نیاز به این pipeline در هر خط تولید نرم‌افزاری نوبت به معرفی ابزارها و الزامات اصلی برای ایجاد یک pipleline ساده از این چرخه بررسی می‌گردد.

در این ساعت ابزارهای امنیتی که برای تکمیل چرخه DevSecOps معرفی می‌گردد. ابزارها، تست‌ها و نحوه پذیرش/عدم پذیرش هر یک از قدم‌های چرخه از نظر امنیتی بررسی می‌گردد. برای هر یک از مراحل فوق ابزارهای امنیتی محبوب‌تر و همراه با ویژگی‌های آن‌ها معرفی می‌گردد.

۴. ساعت سوم: ایجاد یک CI/CD pipeline با استفاده از خدمات AWS

در انتهای این قسمت یک pipeline کامل که تمامی مراحل امنیتی در آن رعایت شده است معرفی می‌گردد.

هدف اصلی این کارگاه نشان دادن نحوه ترکیب ابزارهای مختلف و ایجاد یک CI/CD pipeline برای توسعه برنامه های کاربردی با ملاحظات امنیتی است.

در ادامه این کارگاه DevSecOps CI/CD pipeline ایجاد می‌گردد تا یک نمونه برنامه جاوا را در یک AWS Elastic Beanstalk (EB) مستقر کند. برای پیاده سازی این DevSecOps pipeline از خدمات AWS و ابزارهای امنیتی منبع باز استفاده خواهد شد. خدمات AWS برای ارائه چارچوب اصلی CI/CD و ابزارهای منبع باز برای انجام اسکن آسیب پذیری برنامه استفاده می شود.

برای انجام اسکن SCA، SAST و DAST به ترتیب از ابزارهای منبع باز "OWASP dependecy-check"، "Sonarqube" و "OWASP ZAP" استفاده خواهد شد.