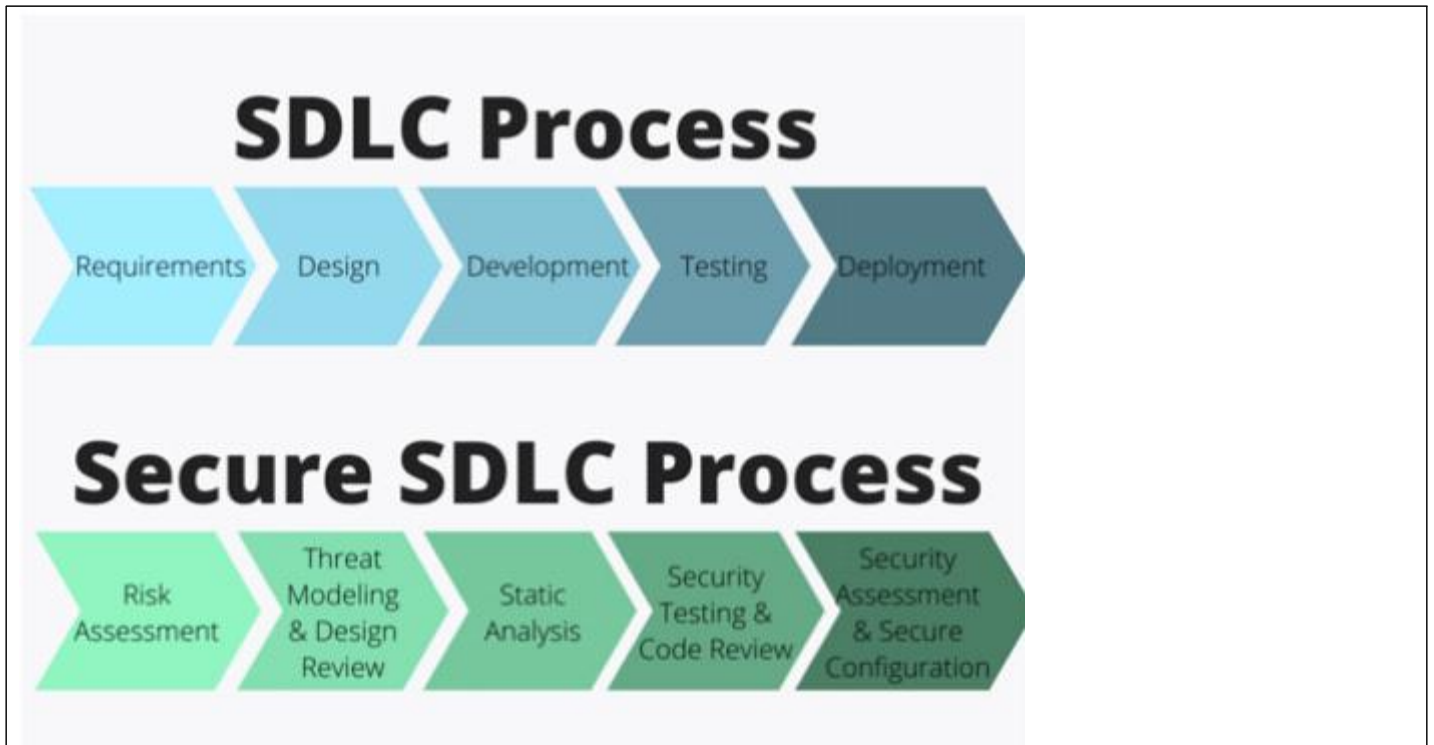


## Secure(시큐어) SDLC

### [1] Secure SDLC



요구분석 => 설계 => 구현 => 테스트 => 유지보수

### [2] SDLC 단계별 보안 활동



### [3] 소프트웨어 개발 보안 요소

[4] 시큐어 코딩 (Secure Coding)

	입력값 검증	보안기능	에러처리	세션통제		
입력 데이터 검증 및 표현	SQL 삽입	경로 조작 및 자원 삽입	크로스사이트 스크립트	운영체제 명령어 삽입	위험한 형식 파일 업로드	신뢰되지 않은 URL 주소로 자동 접속 연결
	XQuery 삽입	XPath 삽입	LDAP 삽입	크로스사이트 요청 위조	HTTP 응답 분할	정수형 오버플로우
	보안기능 결정에 사용되는 부적절한 입력값	메모리 버퍼 오버플로우	포맷 스트링 삽입			
보안 기능	적절한 인증 없는 중요 기능 허용	부적절한 인가	중요한 자원에 대한 잘못된 권한 설정	취약한 암호화 알고리즘 사용	중요정보 평문 저장	중요정보 평문전송
	하드코딩된 비밀번호	충분하지 않은 키 길이 사용	적절하지 않은 난수값 사용	하드코딩된 암호화 키	취약한 비밀번호 허용	사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출
	주석만 안에 포함된 시스템 주요정보	솔트 없이 일방향 해쉬 함수 사용	무결성 검사 없는 코드 다운로드	반복된 인증시도 제한 기능 부재		
시간 및 상태	검사시점과 사용시점	종료되지 않은 반복문 재귀함수				
에러 처리	오류메시지를 통한 정보 노출	오류 상황 대응 부재	부적절한 예외 처리			
코드 오류	Null Pointer 역참조	부적절한 자원해제	해제된 자원 사용	초기화되지 않은 변수 사용		
캡슐화	잘못된 세션에 의한 데이터 정보노출	제거되지 않고 남은 디버그 코드	시스템 데이터 정보 노출	Public 메서드로부터 반환된 Private 배열	private 배열에 public 데이터 할당	
API 오용	DNS Lookup에 의존한 보안 결정	취약한 API 사용				