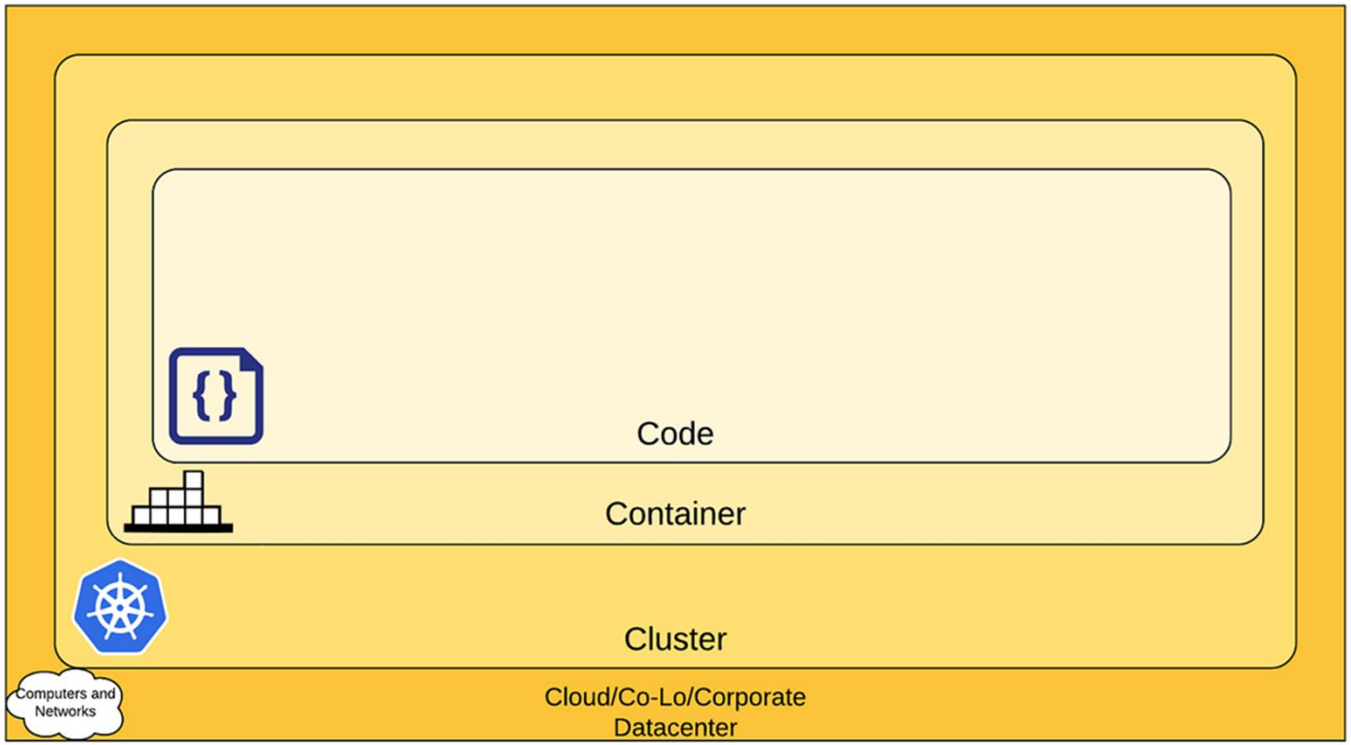
K8S 보안

Kubernetes 4C 보안 모델



Kubernetes 4C 보안 모델

	의미	보안 요소와 포인트	
Cloud	K8s가 올라가는 기반 인프라 - 퍼블릭 클라우드(AWS/GCP/Azure) - 온프레미스 VM	네트워크(VPC, Subnet) 방화벽 / 보안그룹/IAM 계정 물리 서버 / 하이퍼바이저	API 서버 외부 노출 차단 관리 포트 제한 (6443, 22) IAM 최소 권한 노드 간 통신 제한
Cluster	Kubernetes 제어 영역	kube-apiserver etcd Scheduler / Controller RBAC Audit Log	API Server TLS 인증(Authentication) 권한(RBAC) Admission Control Audit Log 활성화
Container	Pod / 컨테이너 환경	Docker / containerd Pod 설정 Linux Kernel (공유)	root 사용자 금지 privileged Pod 차단 Capability 최소화 readOnlyRootFilesystem Pod Security Admission
Code	개발자가 작성한 애플리케이션 코드	소스 코드 라이브러리 설정 값	시큐어 코딩 입력값 검증 인증/인가 로직 Secret 하드코딩 금지 취약 라이브러리 제거

K8s 5계층 보안 모델

	의미
Cluster	API Server 보호 etcd 보안
인증과 권한	인증(authentication) **RBAC(Role-Based Access Control)** - 누가(User/ServiceAccount), 어떤 리소스(Resource)에, 어떤 행위(Verb)를 할 수 있는지”를 정의 하는 권한 통제 방식
Network	CNI NetworkPolicy
Pod & Container	Pod Security Container 보안 규칙
Image & CI/CD	개발자가 만든 코드가 안전한 Image로 만들어져 검증된 경로(CI/CD)를 통해서만 K8s에 배포되도록 통제하는 보안