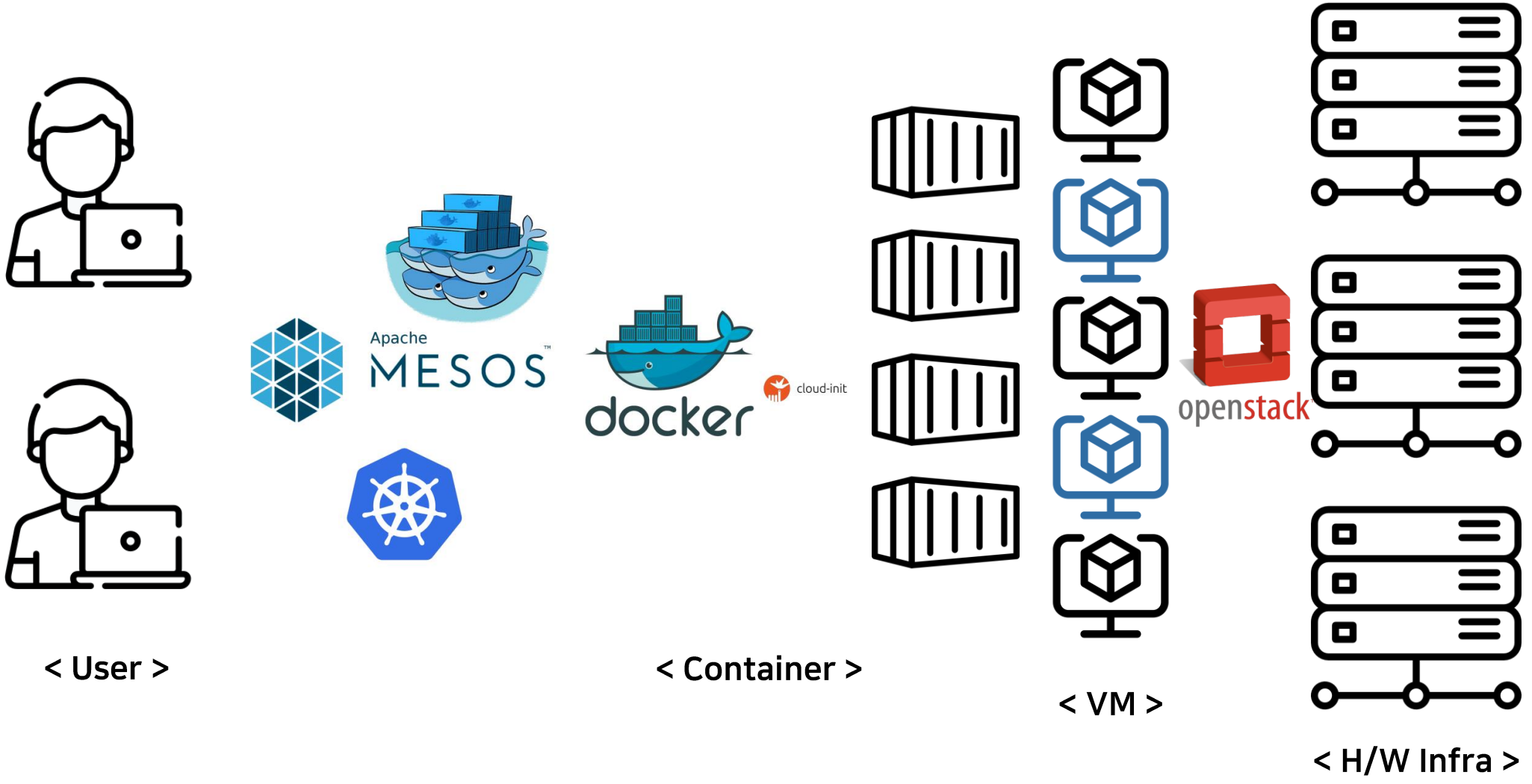
쿠버네티스는 이미지 관리부터

김명섭 / 클라우드기술교육팀

목차

1. 컨테이너 서비스 동향

컨테이너 기술


Apache
MESOS
docker
cloud-init
openstack
< User >
< Container >
< VM >
< H/W Infra >

컨테이너 서비스

컨테이너 기술을 활용한 서비스형 컨테이너 기술

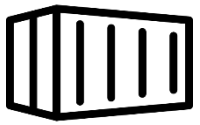
주요 특징

- IT 부서와 개발자가 컨테이너화된 애플리케이션 생성, 관리, 실행할 수 있는 서비스를 지원
- 기업들은 IT 인프라를 현대화하고 클라우드 네이티브 방식을 수용할 필요성을 인식
- 분산 환경에서 애플리케이션을 효율적으로 구축하고, 관리할 수 있도록 해주는 컨테이너 기술이 중요한 원동력으로 부상하며 그 수요가 증가

컨테이너 시장의 주요 키워드

- **컨테이너(Container)**

애플리케이션과 그 종속성(라이브러리, 설정 등)을 격리된 환경에 패키징하여 실행하는 가벼운 가상화 기술

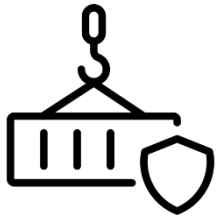


- **이미지**

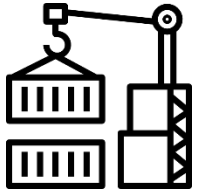
애플리케이션과 그 종속성을 패키징한 파일로, 컨테이너를 생성하는 데 사용

- **컨테이너 보안**

컨테이너 이미지 및 실행 중인 컨테이너의 보안을 강화하기 위한 기술과 접근 방식

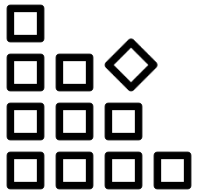


컨테이너 기술 주요 키워드



- **컨테이너 오케스트레이션**

컨테이너화된 애플리케이션을 자동으로 배포, 관리, 스케일링 및 로드 밸런싱하는 자동화 도구



- **이미지 레지스트리**

컨테이너 이미지를 저장하고 관리하는 서버 또는 서비스

- **컨테이너 이미지 서명**

이미지의 무결성을 보장하기 위해 디지털 서명을 사용하는 메커니즘

컨테이너 서비스의 과제

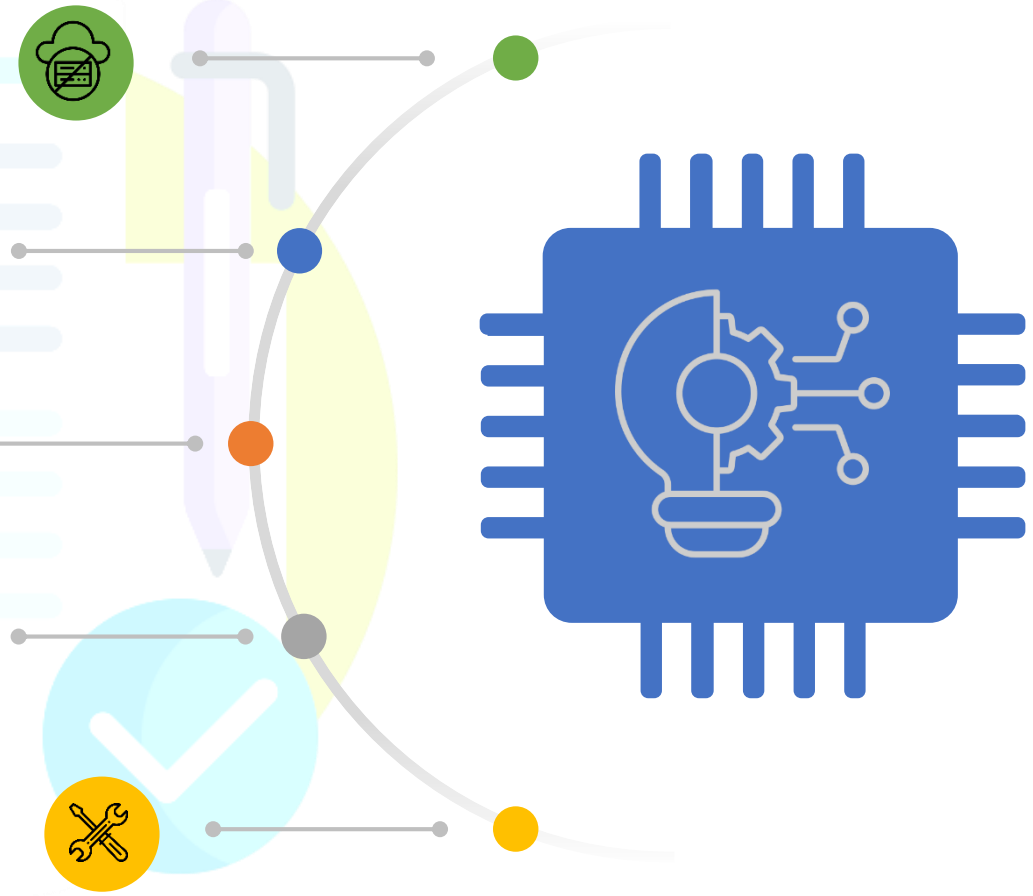
- **서버리스 컨테이너**
  컨테이너 기술을 활용하여 더욱 민첩하고 경제적인 서버리스 환경을 제공

- **보안 강화 및 컨테이너 보안 표준화**
  컨테이너 이미지 스캐닝, 컨테이너 런타임 보안, 네트워크 보안, 이미지 서명 및 접근 제어 강조

- **Edge 및 IoT 컨테이너**
  에지 컴퓨팅 및 사물인터넷(IoT) 환경에서 활용

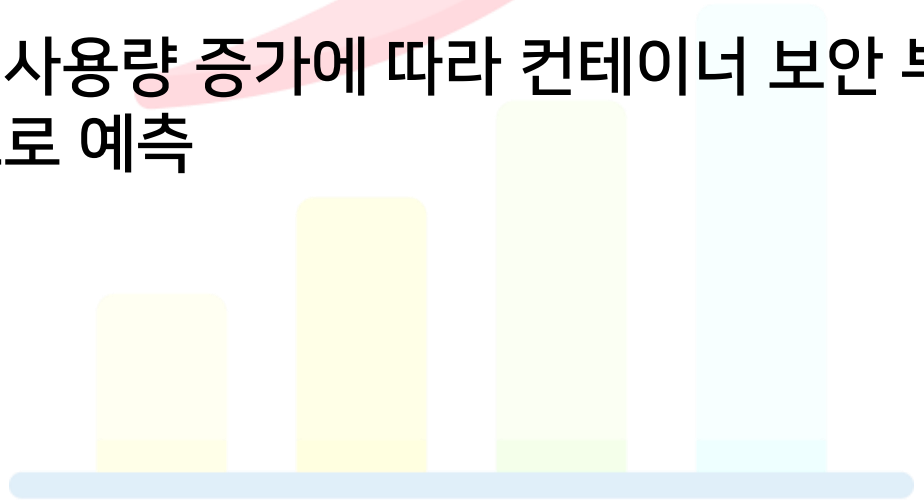
- **하이브리드 및 멀티 클라우드 환경 지원**
  멀티 클라우드 환경과 온프레미스 인프라 혼합 환경에서의 컨테이너 서비스에 애플리케이션 관리 지원

- **컨테이너 관리 도구의 혁신**
  컨테이너 관리 도구 및 서비스는 계속해서 혁신될 것이며, 사용자 편의성, 자동화, 모니터링 및 디버깅 기능 등이 향상



서비스형 컨테이너 시장 추이

- 글로벌 서비스형 컨테이너 시장은 2022년 22억 달러 규모로 평가됨
- 2023년부터 연평균 25.3%로 성장해 2032년까지 207억 달러에 이를 것으로 전망
- 컨테이너 서비스의 사용량 증가에 따라 컨테이너 보안 부분이 앞으로 가장 높은 성장률을 보일 것으로 예측



* 출처: Allied Market Research(www.alliedmarketresearch.com) - 서비스형 컨테이너 시장 전망 보고서

비즈니스 성과에 미치는 컨테이너 보안 문제

- **컨테이너 서비스 운용 중 보안 문제로 비즈니스 성과에 영향을 받은 기업들 다수 발생**
  - 컨테이너와 쿠버네티스 보안 사고의 대부분은 런타임 단계에서 발생했지만,
    빌드/배포 단계에도 유사한 수준으로 영향을 미치고 있음을 확인

- **컨테이너 서비스 보안 문제에 따른 고객 사례 조사 결과**
  - 보안 문제로 인한 배포 지연 및 속도 저하
  - 보안 문제로 인한 매출 손실 또는 고객 손실 경험
  - 기존 컨테이너와 쿠버네티스 보안 솔루션으로 인한 개발 속도 저하
  - 보안 구성 오류의 결과로 데이터 삭제 경험

* 출처: 쿠버네티스 보안 현황 리포트 2023 - Red Hat

2. 컨테이너 보안 기술

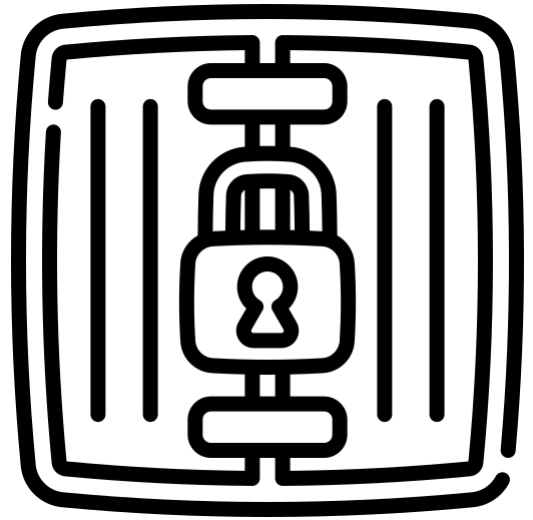
컨테이너 보안 기술의 정의

컨테이너 보안 기술은 컨테이너 기반 애플리케이션 환경에서

보안을 유지하고 강화하는데 사용되는 다양한 기술과 방법을 의미

- 컨테이너 환경에서 보안 취약점을 해결하고 애플리케이션과 데이터를 안전하게 보호하는데 목적
- 컨테이너 기술을 사용하는 조직들이 애플리케이션 및 데이터를 보호하고 보안 취약점을 식별하며,

  보안 정책을 준수하도록 지원



컨테이너 서비스 환경 보안 주 위험 요소

Major Risk Container Environment	Build/Develop	Deploy	Run
1. 이미지 Risk			
2. Registry Risk			
3. Orchestrator Risk			
4. Container Risk			
5. Host OS Risk			
	Shift Left		Shift Right

컨테이너 이미지 보안 관리

- 실제 내/외부 사용자의 영향을 가장 민감하게 받을 수 있고, 컨테이너 서비스의 표면적 접근이 가장 활발히 작용할 수 있는 요소로 볼 수 있음

  (ex. 퍼블릭 레지스트리에서 제공하는 공개용 컨테이너 이미지)

- 올바른 컨테이너 서비스를 활용하기 위해서는 안정적이고 검증된 이미지를 인증하여 관리하고, 인가된 사용자만 인증 받은 이미지를 이용할 수 있도록 구성하는 것이 중요

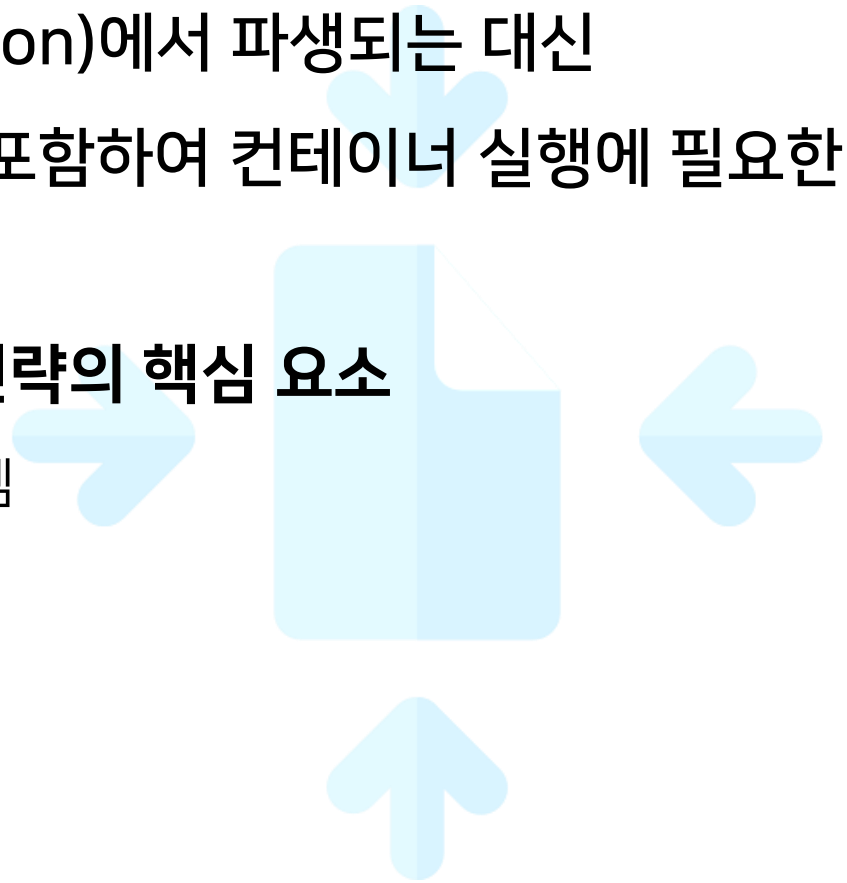
- 이미지는 각 조직별로 보안을 철저히 관리하고 최적화하기 위한 전략 수립 필요

컨테이너 이미지 보안 솔루션

컨테이너 이미지 보안 전략 - Distroless 이미지 전략

Linux 배포판(Distribution)에서 파생되는 대신

최소한의 파일 시스템만 포함하여 컨테이너 실행에 필요한 최소한의 요소로 구성



Distroless 이미지 전략의 핵심 요소

- 최소한의 파일 시스템
- 취약점 감소
- 이미지 최적화
- 다중단계 빌드
- 강력한 보안

컨테이너 이미지 보안 전략 - Distroless 이미지 전략(Cont.)

NHN Container Registry(NCR) > 관리

관리 복제 이미지 캐시

레지스트리 > nhn-ncr > nhn-ncr/distroless-nodejs

아티팩트 삭제 스캔 스캔 중지

아티팩트 유형	아티팩트	크기	인증	Push 시간	Pull 시간	취약점
docker	sha256:e14eeae8	51.72MB	✕	2023-09-19T16:24:00+09:00	2023-09-19T16:24:07+09:00	Critical (total 27 / fix 0)

VS.

NHN Container Registry(NCR) > 관리

관리 복제 이미지 캐시

레지스트리 > nhn-ncr > nhn-ncr/normal-nodejs

아티팩트 삭제 스캔 스캔 중지

아티팩트 유형	아티팩트	크기	인증	Push 시간	Pull 시간	취약점
docker	sha256:c2ed73be	380.17MB	✕	2023-09-19T16:23:39+09:00	2023-09-19T16:23:45+09:00	Critical (total 776 / fix 32)

컨테이너 보안 주요 기술 정리

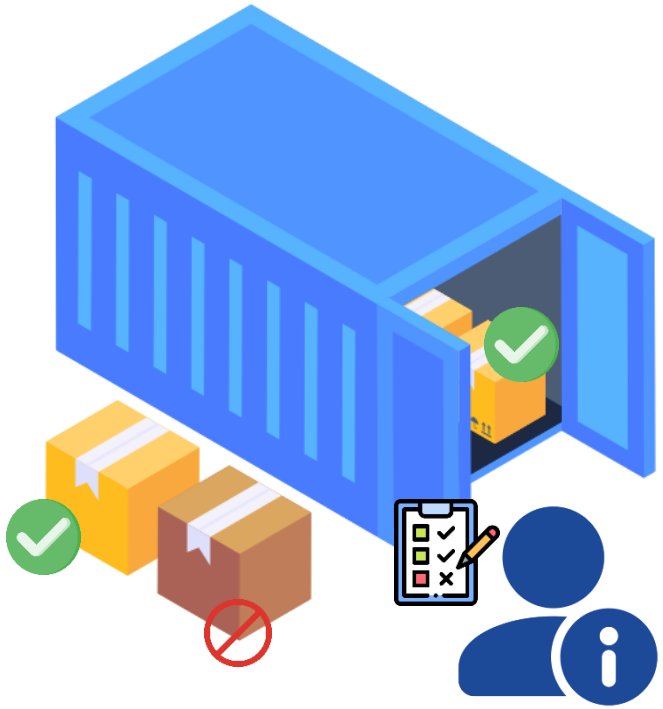
- 이미지 스캐닝
- 접근 제어 및 권한 관리
- 서명 및 인증
- 런타임 모니터링
- 네트워크 보안
- 로그 및 감사
- 규정 준수 및 보고

3. 이미지 서명 관리 기술

컨테이너 이미지 서명

컨테이너 이미지 서명(Container Image Signing) 기술

- 이미지의 무결성과 신뢰성을 보장하기 위한 보안 기술 중 하나
- 이미지 변경 여부 검증, 이미지가 원본 소프트웨어 제공자에 의해 생성되었음을 확인하는데 사용



컨테이너 이미지 서명 관리 기술

- **디지털 서명**
  - 이미지를 생성한 소프트웨어 공급업체나 개발자가 이미지에 디지털 서명을 적용하여 이미지 무결성을 보장
  - 공개 키, 개인 키 Pair를 사용하여 생성하며, 무결성 검증을 위해 사용

- **서명 검증 프로세스**
  - 이미지를 사용하는 사용자나 컨테이너 오케스트레이션 솔루션이 이미지와 함께 제공된 서명 검증
  - 이미지 서명 확인을 위한 공개 키와 서명 생성에 사용된 개인 키, 내용(Hash) 일치 여부 확인
  - 일치할 경우 이미지를 안전하게 실행하거나 배포하도록 구성

컨테이너 이미지 서명 관리 기술(Cont.)

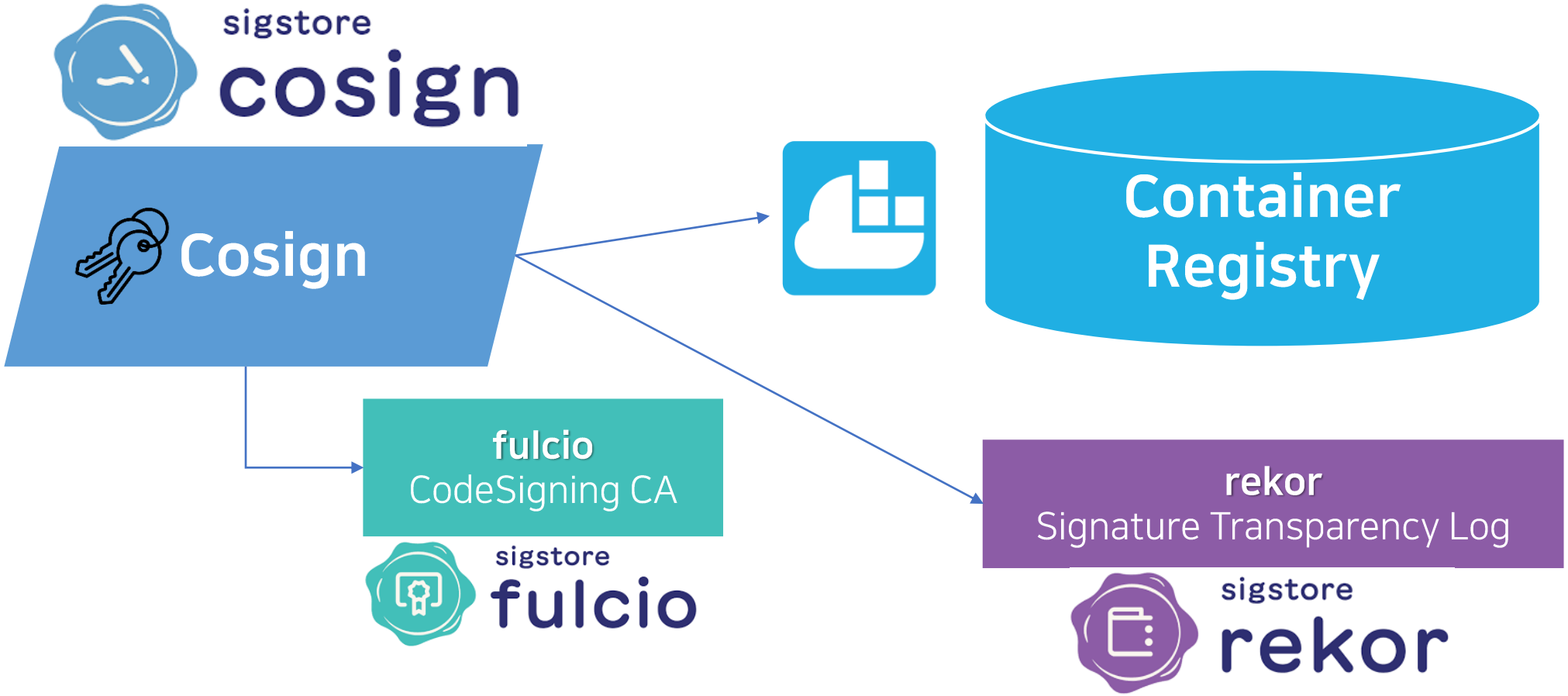
- **서명 범위**
  - 이미지 전체 또는 특정 이미지 레이어에 적용 가능
  - 이러한 유연성은 이미지 생성 및 관리 프로세스를 개선하고 보안을 강화하는데 도움

- **이미지 보안 강화**
  - 서명관리 기술을 사용하면 이미지가 원본에서 생성되었으며, 변경되지 않았음을 확인
  - 이를 활용하여 악성 이미지의 사용을 방지하고 신뢰할 수 있는 이미지를 배포/실행하는데 도움

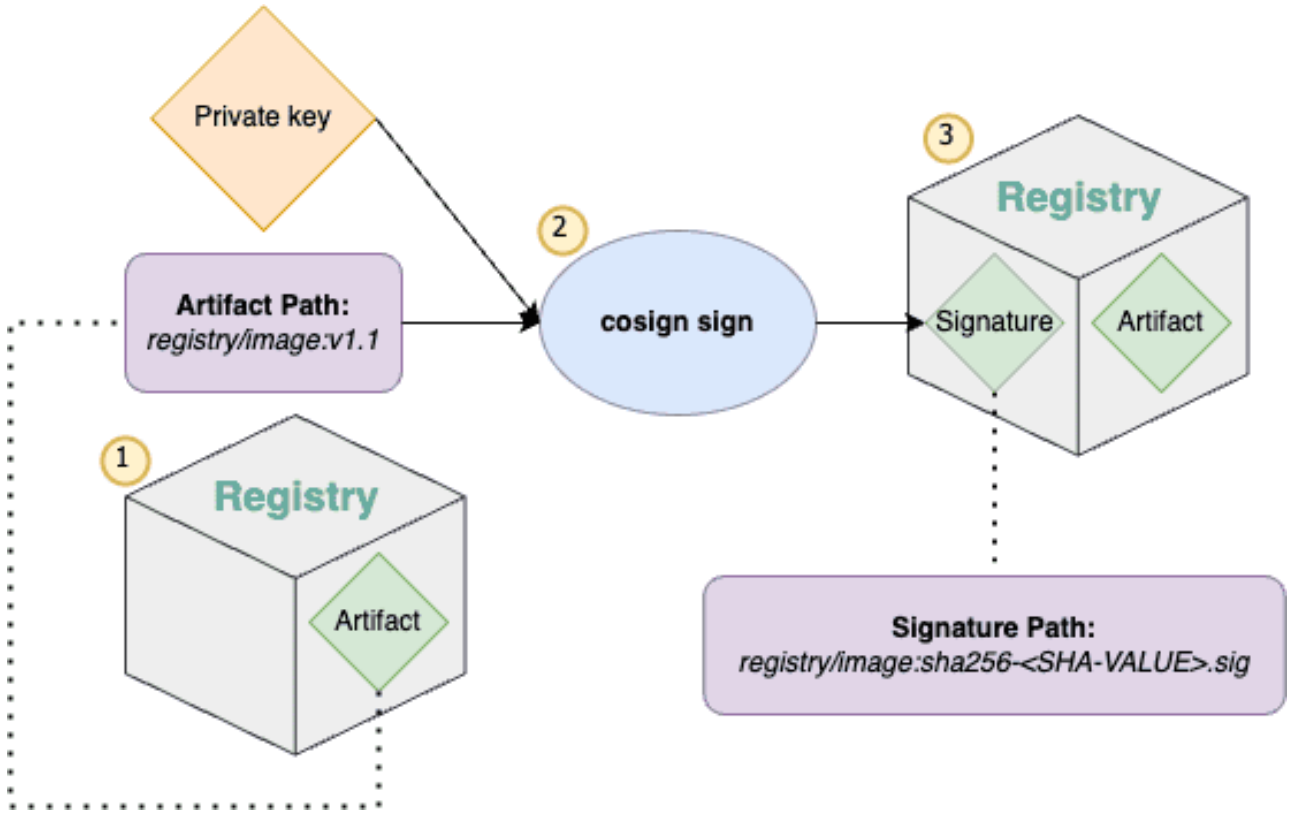
Sigstore cosign

- **Sigstore 오픈 소스 프로젝트**(https://docs.sigstore.dev/)
  - 소프트웨어 공급업체와 개발자들이 소프트웨어 서명 및 이미지 서명 관리를 향상시키기 위한 도구와 서비스를 제공하는 프로젝트
- **cosign**(https://docs.sigstore.dev/signing/quickstart/)
  - Sigstore 프로젝트의 일부로 개발된 도구 중 하나
  - 컨테이너 이미지 서명 및 검증을 위한 도구
  - 무결성을 보장하고 이미지의 출처를 확인하기 위한 디지털 서명을 관리

Sigstore cosign - Architecture



Sigstore cosign logic



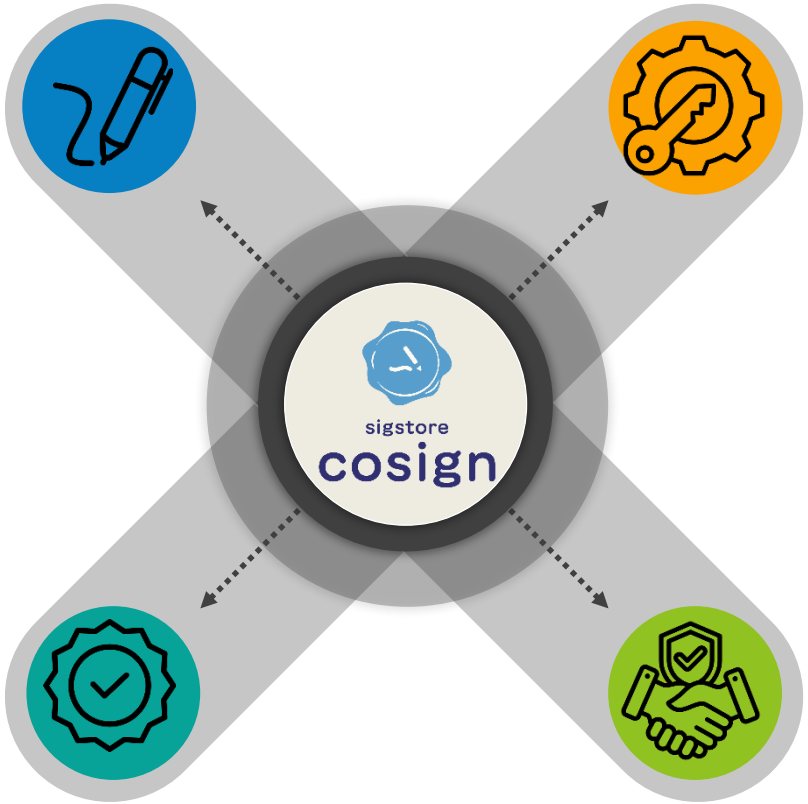
Sigstore cosign 주요 기능 및 특징

- **이미지 서명**

컨테이너 이미지에 디지털 서명을 적용하여 이미지 무결성을 확인하고 변경되지 않음을 보장

- **이미지 검증**

이미지 다운로드 후 배포하기 전 이미지 서명을 검증할 수 있도록 하여 이미지 신뢰 여부 확인



- **공개 키 관리**

이미지 서명을 생성하고 관리하기 위한 공개키/ 개인키 생성 관리를 지원

- **이미지 호환 및 관리체계 통합**

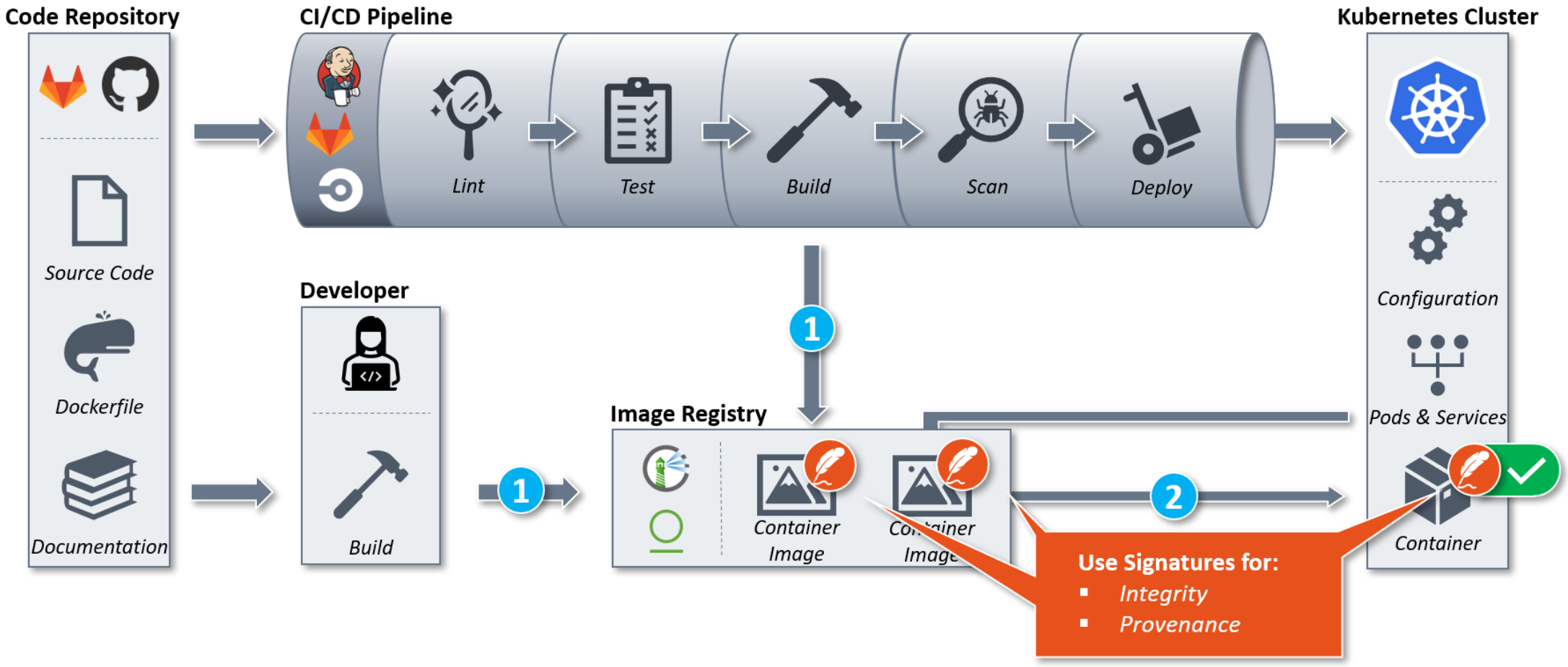
OCI(Open Container Initiative) 이미지 스펙에 준수한 컨테이너 런타임에 사용 가능하며, 다양한 이미지 공급업체(Docker Hub 등)와 통합되어 이미지 서명을 관리하고 검증 가능

Connaisseur

- 컨테이너 이미지에 디지털 서명을 적용하고 이미지의 신뢰성을 검증하는 데 사용하는 Kubernetes 승인 컨트롤러
- Kubernetes 클러스터에서 컨테이너 이미지의 무결성과 출처를 보장
- 클러스터로 전송된 리소스 생성 또는 업데이트 요청을 중간에 확인하며, 모든 컨테이너 이미지를 사전 구성된 공개 키 기반 서명으로 식별 후 컨테이너 생성을 수락하거나 거부
- Sigstore / Cosign 인증 이미지 지원

* 출처: https://sse-secure-systems.github.io/connaisseur/v3.0.0/

Connaisseur Process



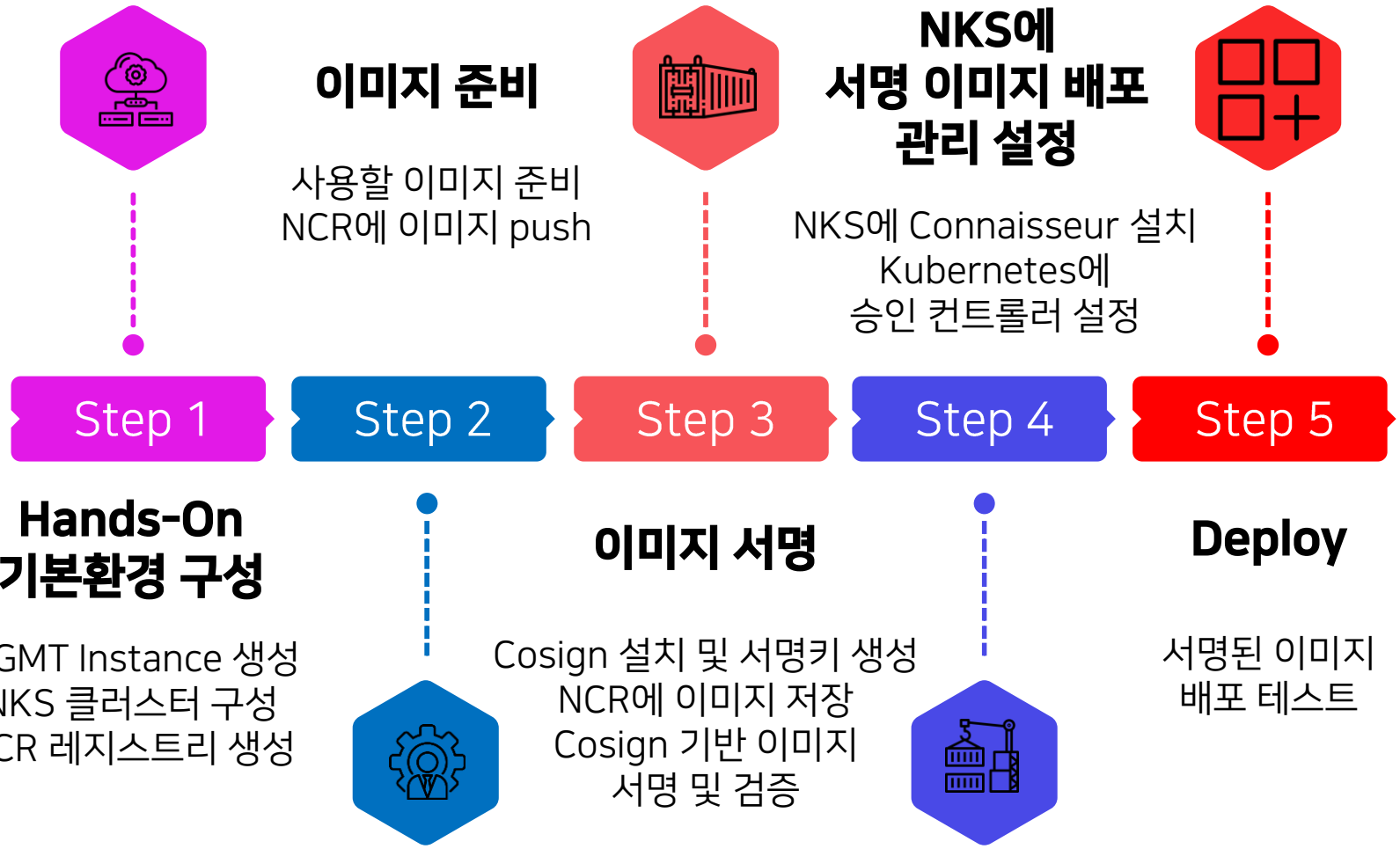
* 출처: https://sse-secure-systems.github.io/connaisseur/v3.0.0/

NCR(NHN Container Registry) 이미지 신뢰 기능

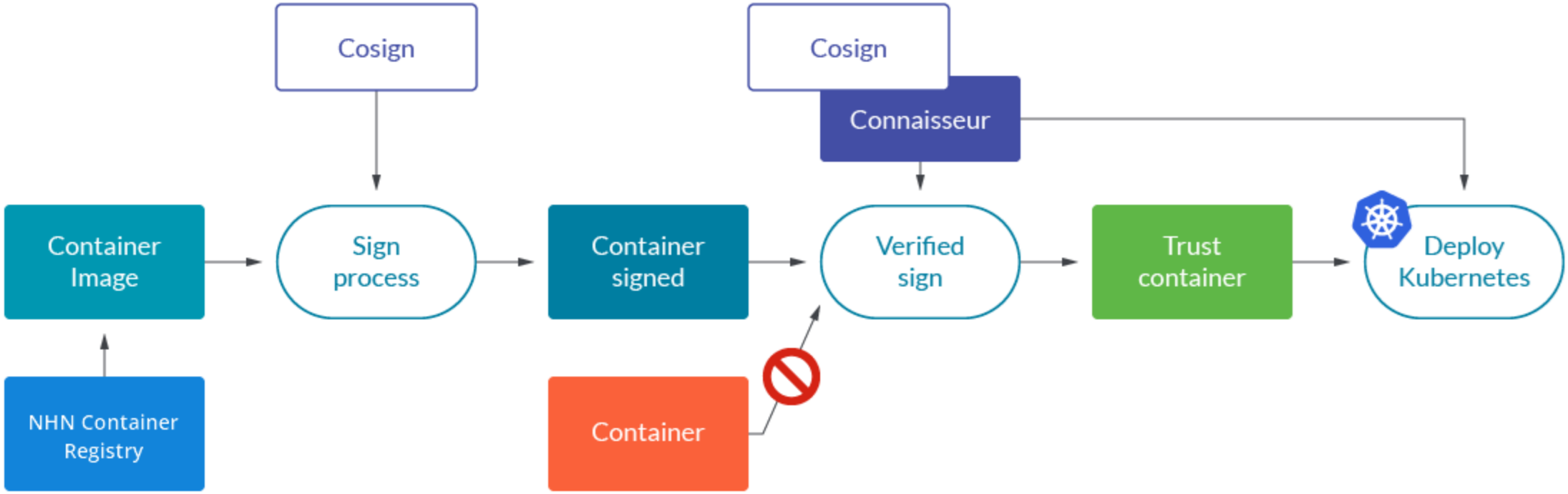
- **디지털 서명 및 검증**
  - 컨테이너 이미지에 디지털 서명을 적용하고 이미지를 검증하는 기능 제공
  - 이미지 다운로드 후 배포할 때 서명을 검증하여 이미지 신뢰성을 확인 가능
- **이미지 업로드 및 다운로드 보안**
  - 이미지 업로드 및 다운로드 과정에서 보안 프로토콜을 사용하여 데이터를 암호화하고 이미지의 무결성을 보호
- **이미지 취약점 스캐닝**
  - 이미지 관련 활동사항에 대한 스캐닝을 통해 이미지 보안 위협요소 체크와 이미지 사용 기록을 모니터링하고 식별 가능

4. 이미지 서명을 활용한 NKS Hands-on Demo

Hands-on Demo Step



Hands-on Process



Summary

Summary

컨테이너 서비스 보안 이것만!

- 다양한 보안 도구와 서비스 활용
- 보안 업데이트 적용 환경 조성
- 전문적인 컨테이너 이미지 보안 관리 체계 구성을 통해 보안요건 검증, 검수, 유지 관리 환경 강화
- 컨테이너 이미지 및 애플리케이션 스캐닝 활용
- 다양한 보안 사고 사례 확인
- 컨테이너 이미지 접근은 최소한의 권한을 부여하여 사용
- 컨테이너 이미지에는 최소한의 애플리케이션 구동 라이브러리만 적용
- 보안정책 규정 준수

NHN Cloud

유연하게, 안전하게
비즈니스에 힘이 되다.