클라우드 여정을 위한 준비, 컨테이너 표준화 그리고 보안

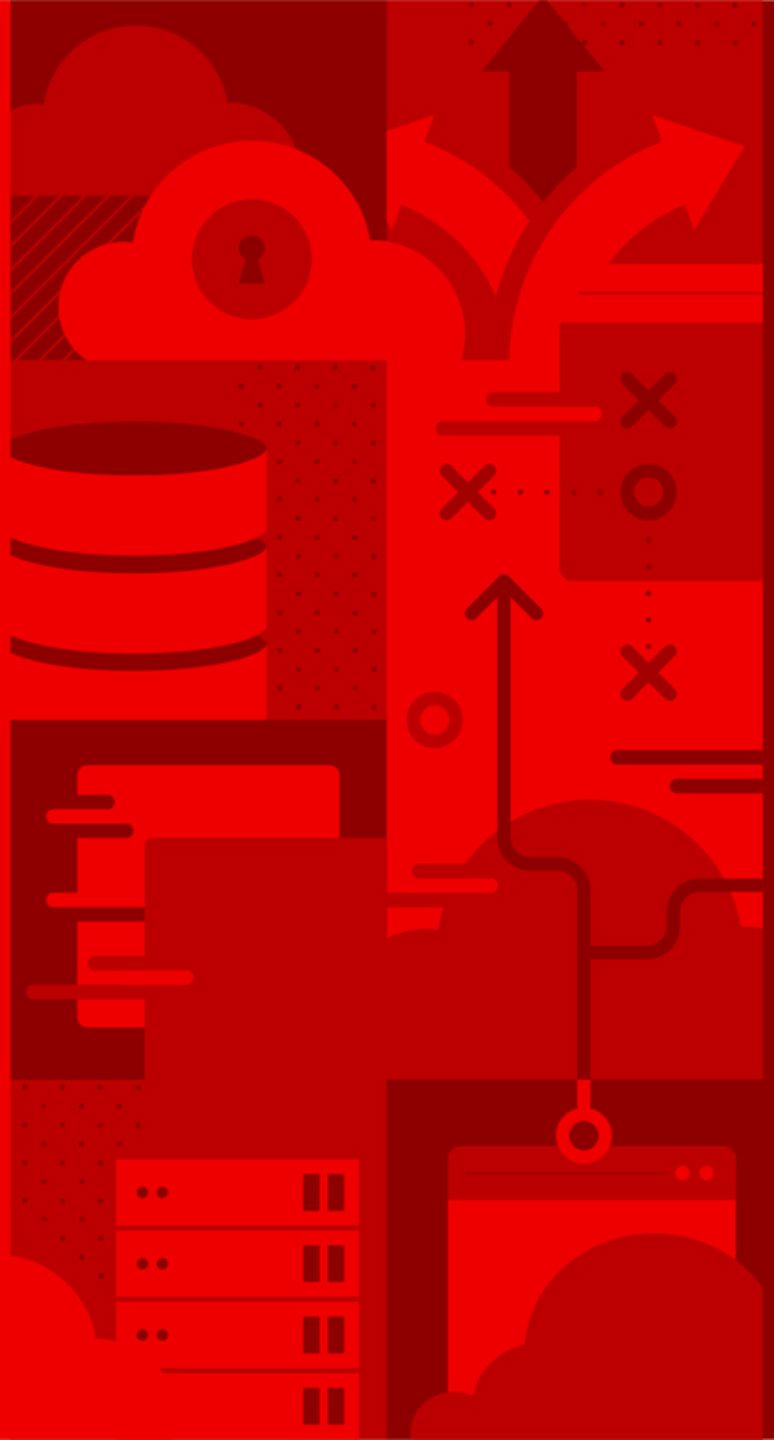
이제는 챙겨야 할 컨테이너 보안 이야기
(NIST SP 800-190 Application Container Security Guide)

Chankyu Song
chsong@redhat.com
Red Hat Solution Architect

Red Hat

Agenda

- 컨테이너 표준화? 보안?
- NIST 800-190 Application Container Security guide
- 컨테이너이미지 위협 요소 및 방안
- 마무리 & 키워드



컨테이너 표준화? 보안?

Red Hat

컨테이너 표준과 보안

표준이 없으면 자동화 할 방법이 없습니다.

상자는 크기가 다르고 각각 규격이 다릅니다.

이런 상태로는 생태계가 활성화 될 수 없습니다.

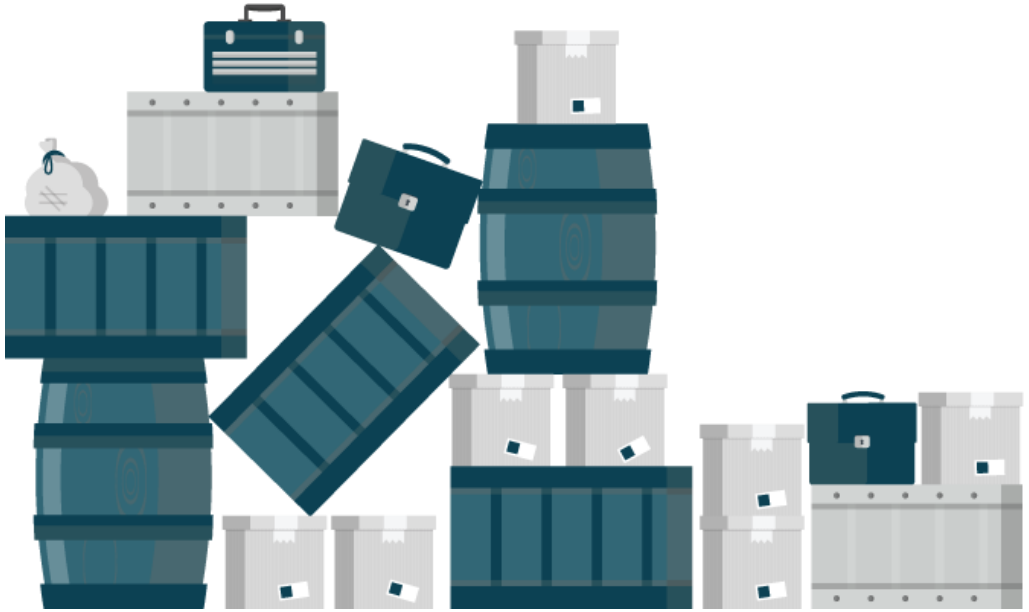
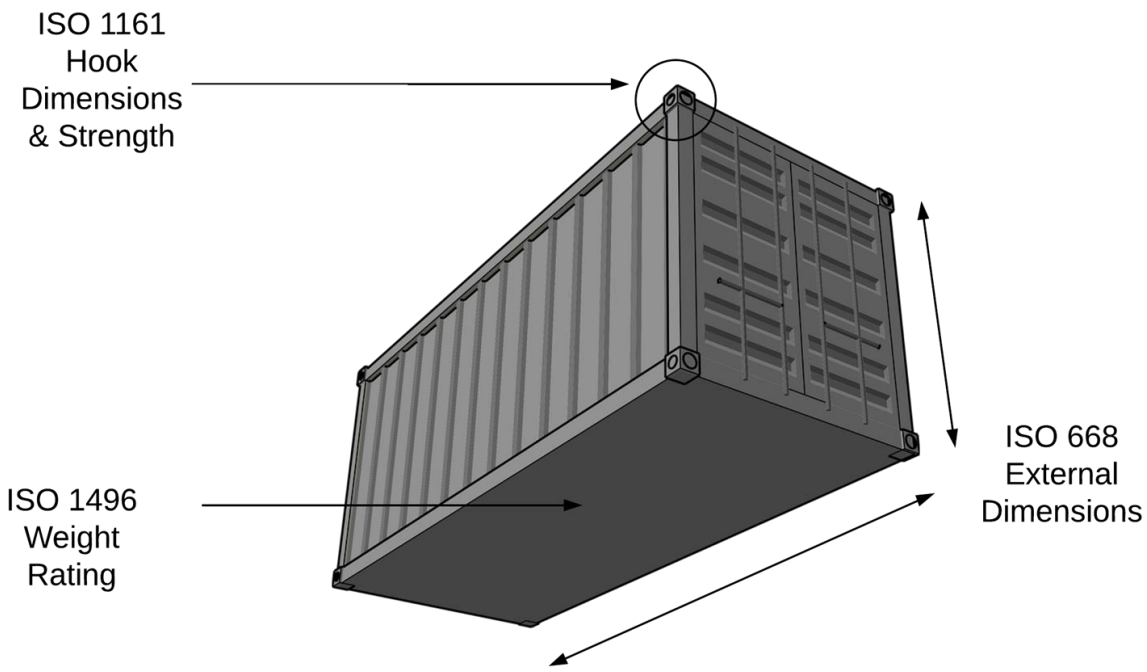


Image: Boxes manually loaded on trains and ships in 1921

실제 컨테이너와 비슷한 부분

- **자동화 : 현대의 컨테이너 항구와 같이 완전히 자동화 된 환경에서 장애는 경제적으로 치명적인 손실 발생** (CI/CD)
- **표준 : 단순한 것, 상호 운용성을 위한 정확한 규격이 필요** (Files & Metadata)
- **복잡한 환경에서 장비와 서비스 인프라에 대한 관리와 투자를 보호하는 유일 한 방법** (container orchestration & build processes)



Red Hat

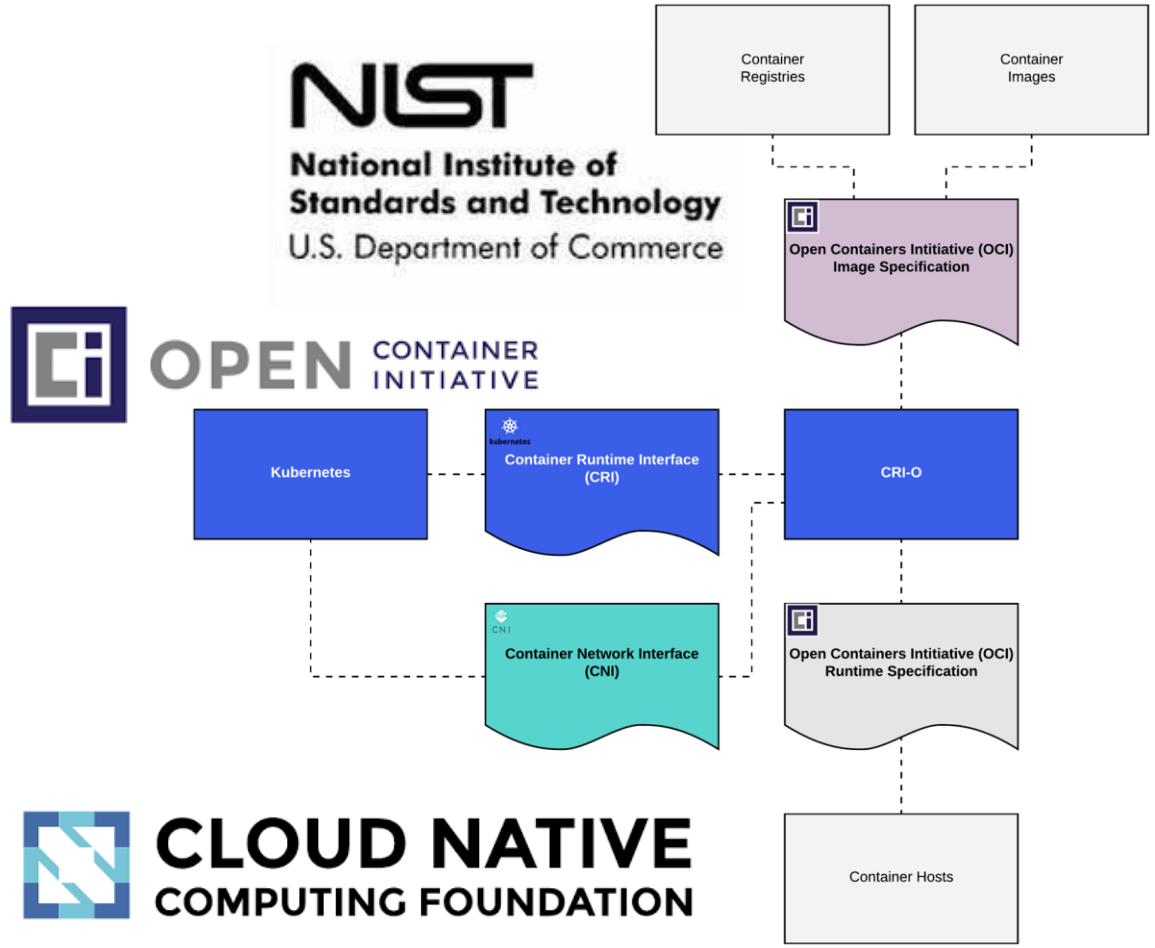
컨테이너와 관련된 다양한 표준

Vendor, Community, and Standards Body driven

컨테이너 표준 + 보안

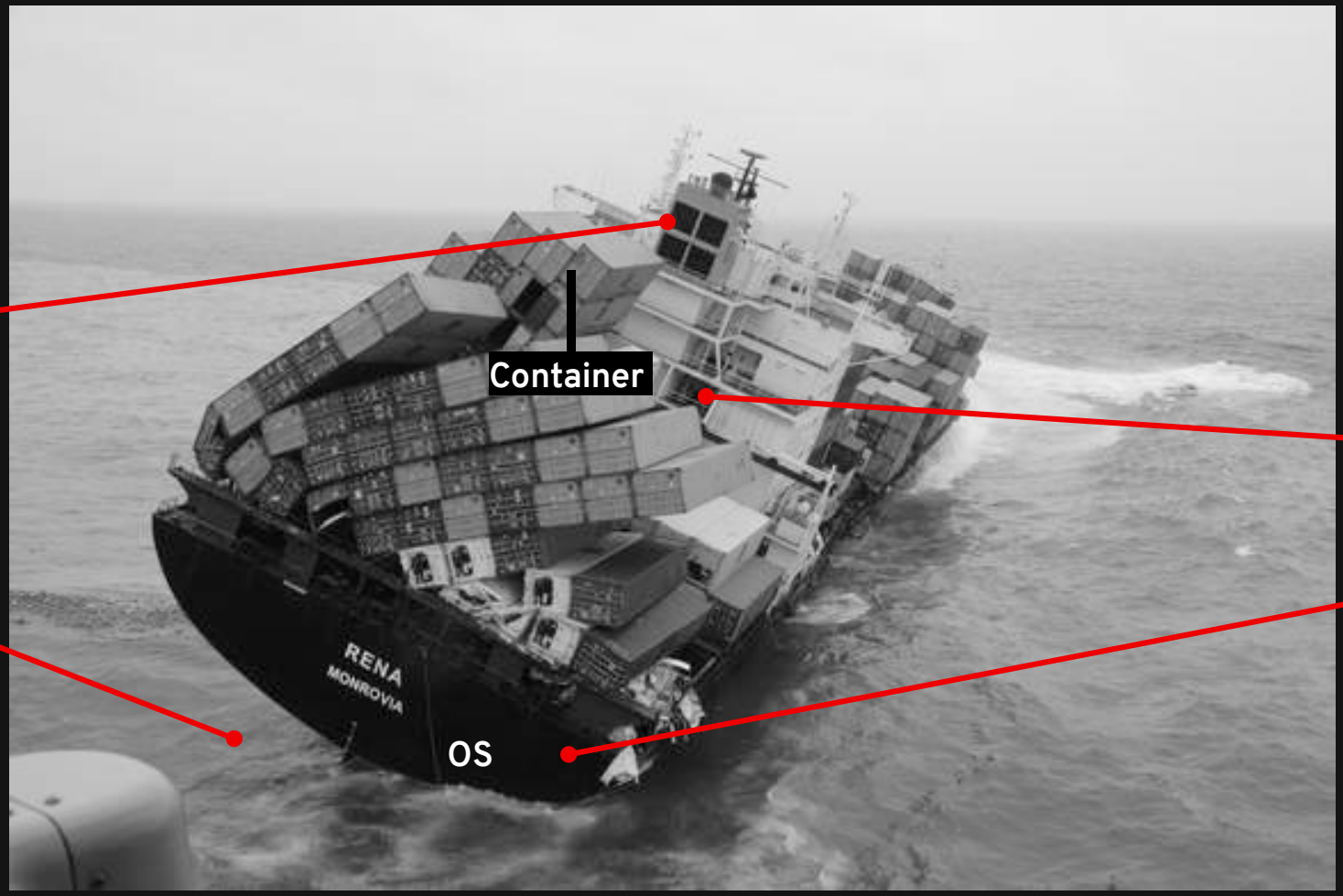
각각의 표준들은 목표가 다름

- **Container Images & Registries**
- **Container Runtimes**
- **Container Networking**
- **Kubernetes security**
- **NIST Container standards**



Red Hat

컨테이너 보안?



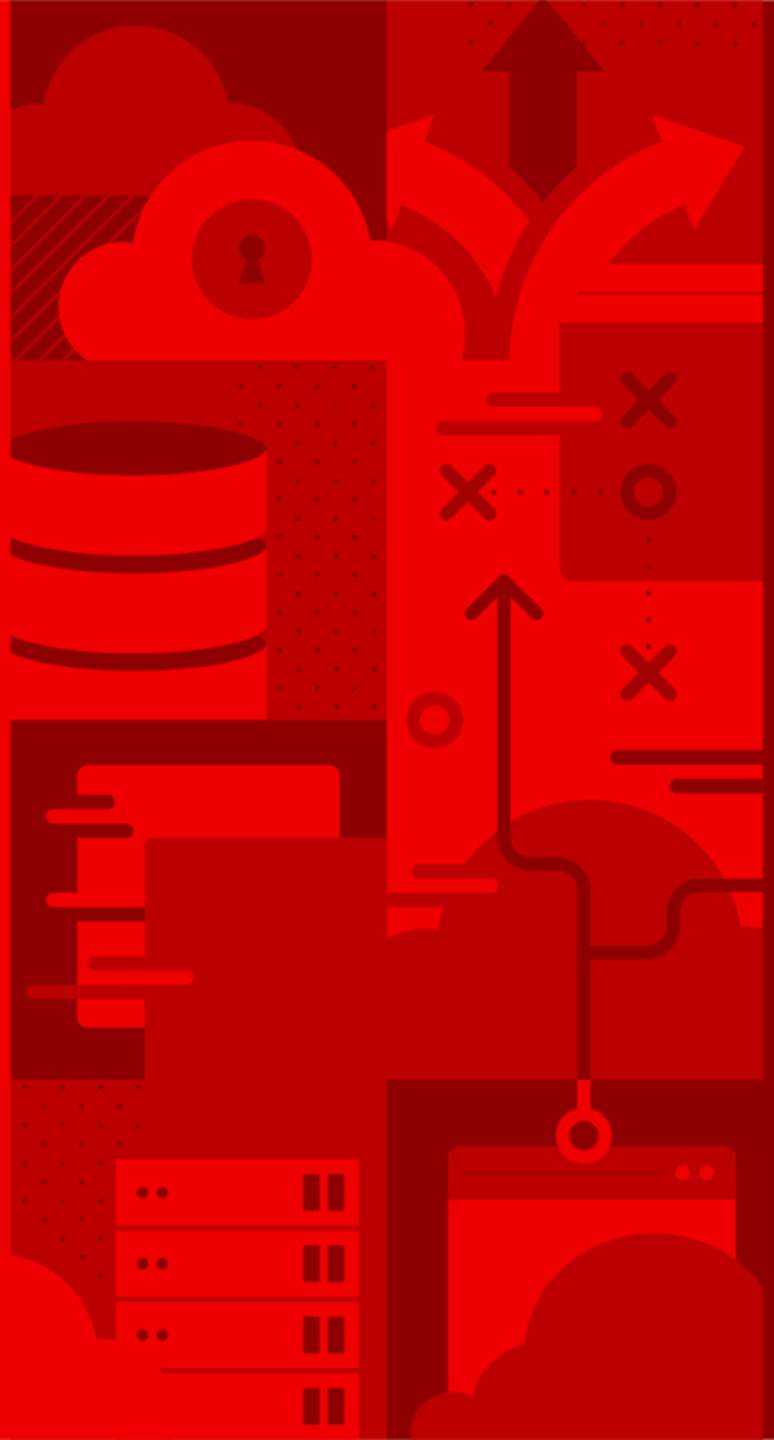
상황 통제

환경&위협

Container

OS

Red Hat



NIST SP 800-190 Application Container Security Guide

Red Hat

Application Container Security Guide Overview

- 특정 컨테이너 기술 호스트 OS 및 클라우드 환경에 의존하지 않는 일반적인 컨테이너 환경의 보안 가이드를 제공
- 컨테이너 이미지, 오케스트레이터, 호스트 OS 등 컨테이너 기술에 관한 핵심 구성 요소의 주요 위험을 대상으로 컨테이너와 이미지 권한 및 컨테이너를 악용 한 다른 컨테이너 호스트 OS 다른 호스트 등의 공격에 분류
- 핵심 구성 요소가 아닌 개발자의 시스템 테스트 및 검증 시스템 관리자의 시스템 호스트 하드웨어 및 가상 머신 관리자를 포함한 비 핵심 컨테이너 기술의 구성 요소에 대한 위험은 포함되지 않음

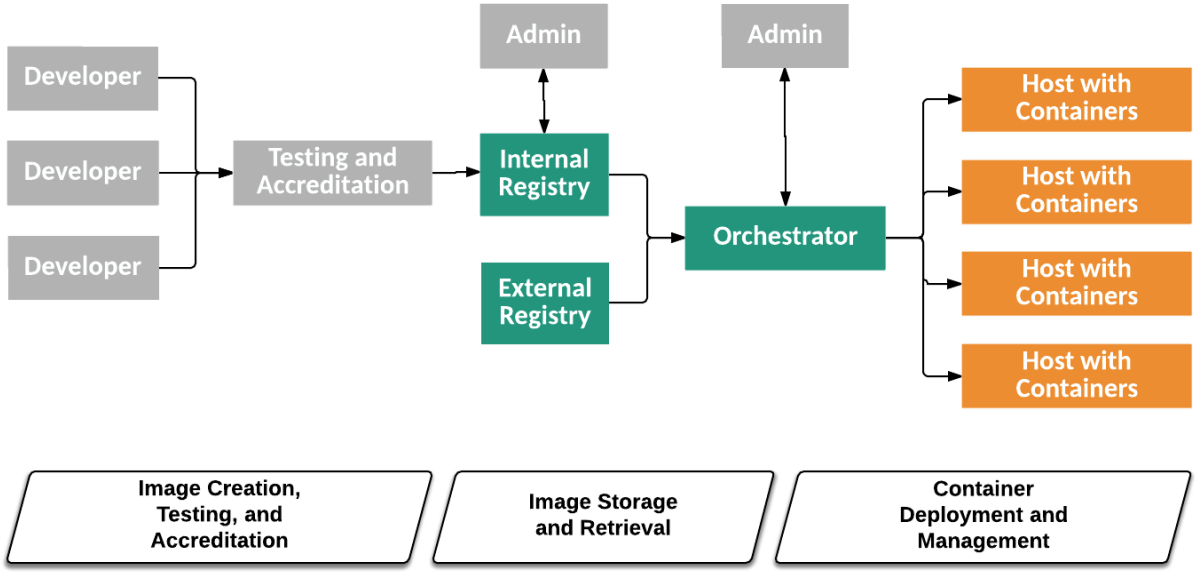


Figure 3: Container Technology Architecture Tiers, Components, and Lifecycle Phases [1]

The five tiers of the container technology architecture

1. Developer systems : 이미지를 구축하고 검증 환경에 배포
2. Testing and accreditation systems : 콘텐츠 검사나 이미지 서명을 하고 레지스트리에 저장
3. Registries : 이미지를 저장하고 오케스트레이터에 배포
4. Orchestrators : 이미지를 컨테이너로 변환, 호스트에 배포
5. Hosts : 오케스트레이터의 지시에 따라 컨테이너를 시작 또는 중지

[1] https://csrc.nist.gov/publications/detail/sp/800-190/final 발췌

Red Hat

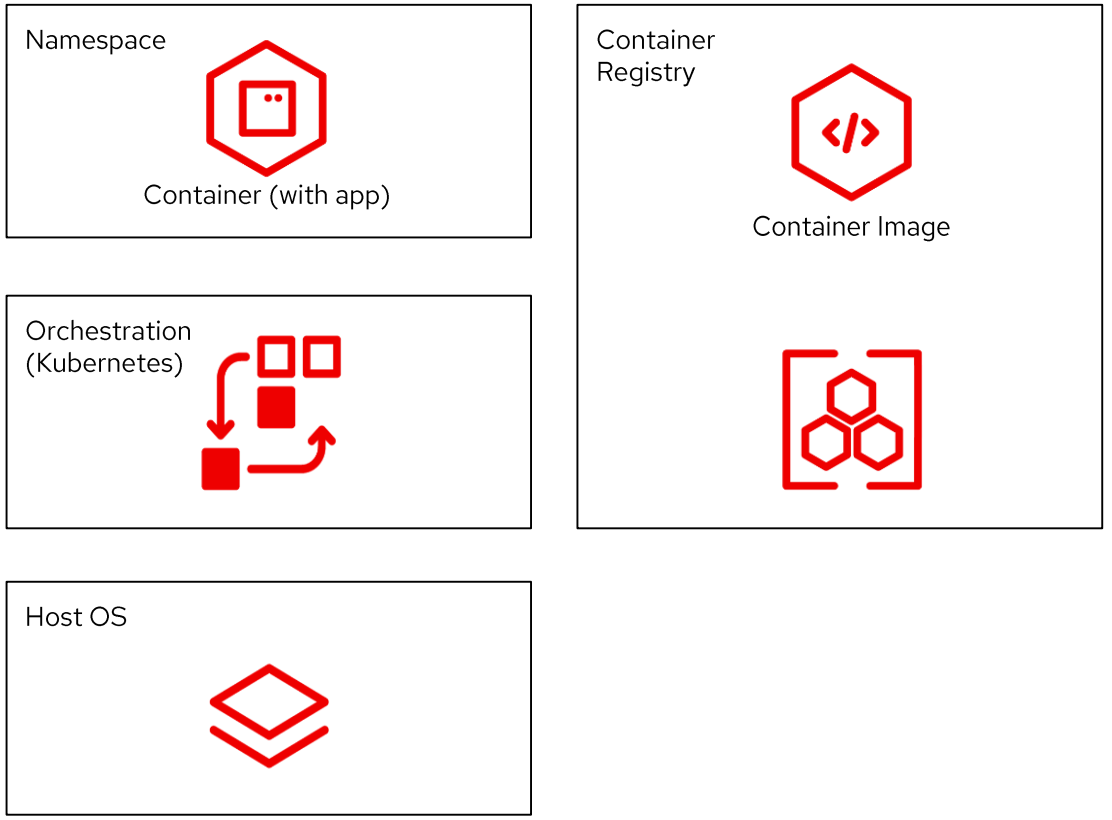
컨테이너 기술의 핵심 구성 요소에 대한 주요 위험 요소

평가의 대상 및 목적

- 컨테이너 기술의 주요 구성 요소 인 이미지 레지스트리 오 케스트 레이터, 컨테이너, 호스트 OS에 대한 주요 위험을 분석 [1]

고려해야 할 위험

- 이미지 또는 컨테이너 권한 [2]
- 컨테이너를 악용 한 다른 컨테이너 호스트 OS 다른 호스트 등의 공격 [3]

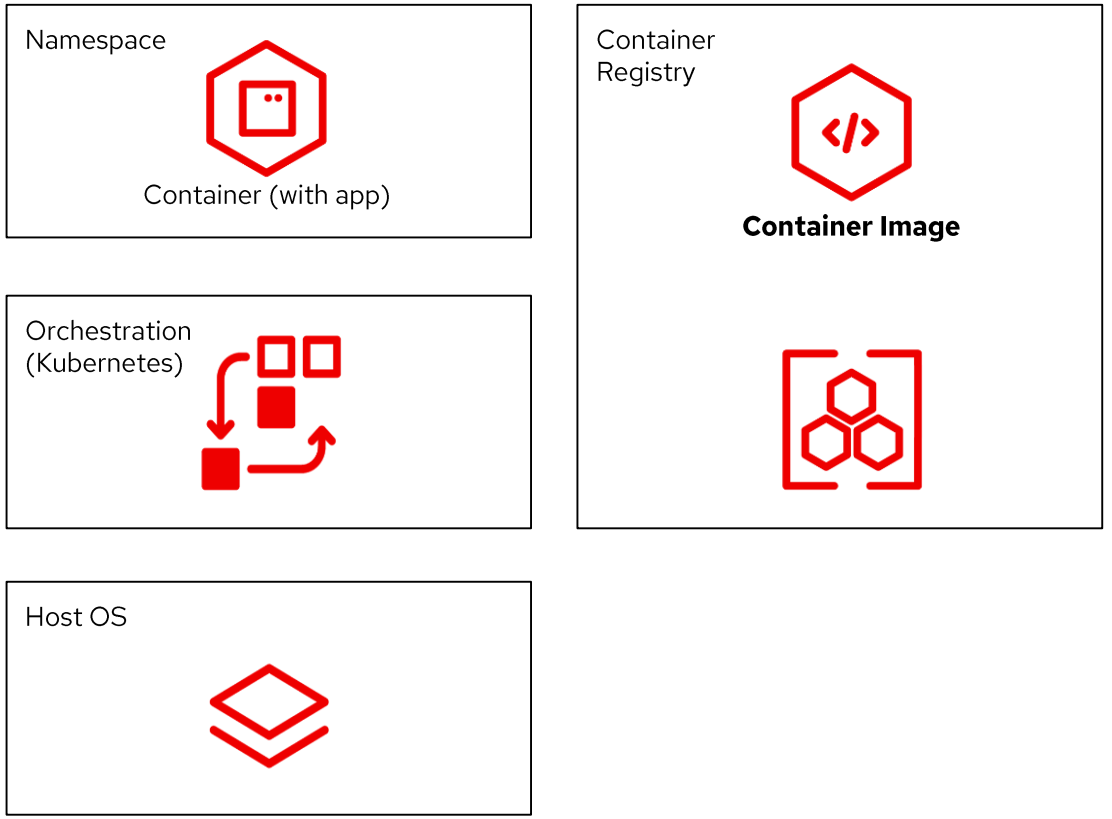


[1]이 분석은 핵심 구성 요소에만 초점을 충당하기 위해 컨테이너 기술 호스트 OS 플랫폼 또는 퍼블릭 클라우드와 프라이빗 클라우드 등의 위치뿐만 아니라 대부분의 컨테이너의 배치에 적용 할 수 있다는 생각에 기초한다.
[2] NIST SP 800-154에서 데이터를 중심으로 한 시스템 위협 모델에 의해 평가되어 보호해야 할 데이터 이미지와 컨테이너가 해당한다. 전자는 애플리케이션의 속성 파일 데이터를 포함한 파일, 후자는 메모리, 스토리지 및 NIC와 같은 호스트에서 공유 된 자원을 보유하고있는 컨테이너의 데이터가 해당한다.
[3] 개발자의 시스템 테스트 및 검증 시스템 관리자의 시스템 호스트 하드웨어 및 가상 머신 등 비 컨테이너 기술의 구성 요소에 대한 위험은 포함되지 않는다.

Image Risk

3.1 Image Risks

- 이미지의 취약점
- Dockerfile 및 이미지 설정의 미비
- 악성 코드 포함
- 인증 정보 포함
- 신뢰할 수없는 이미지의 사용

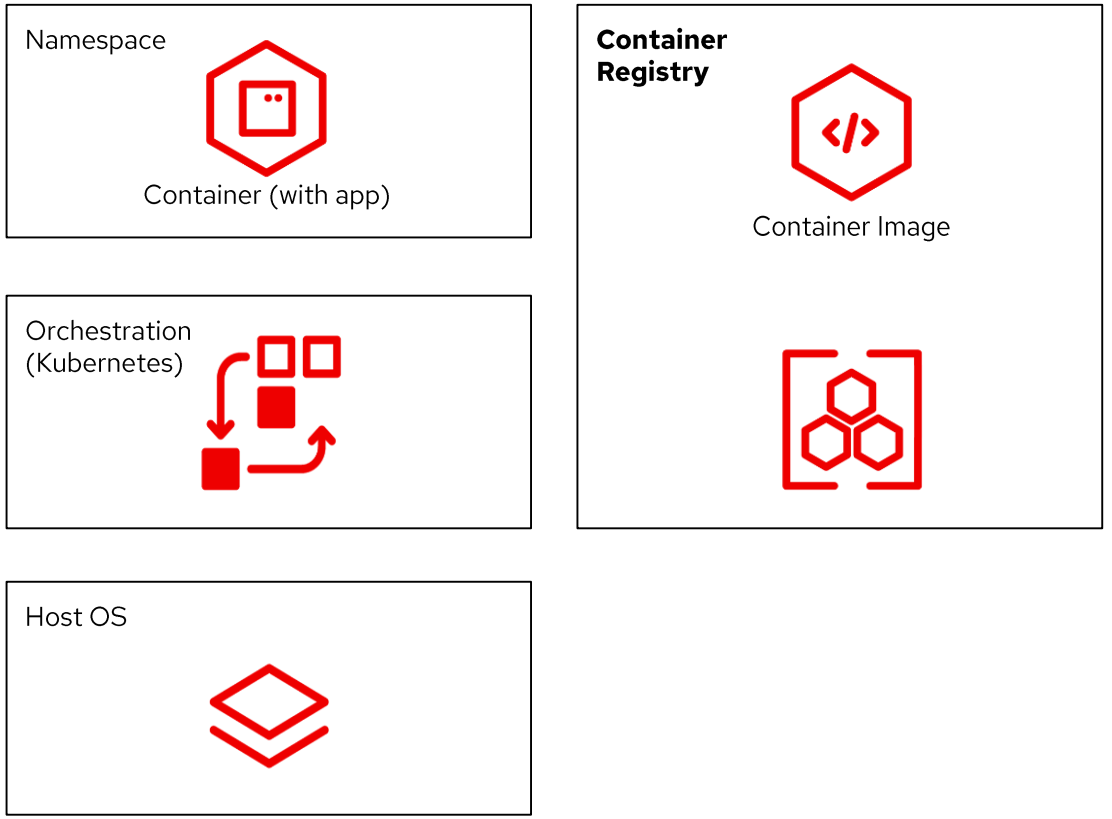


Red Hat

Registry Risks

3.2 Registry Risks

- 비보안 통신의 이용
- 사용하지 않는 이미지의 취약점
- 인증 및 승인의 미비

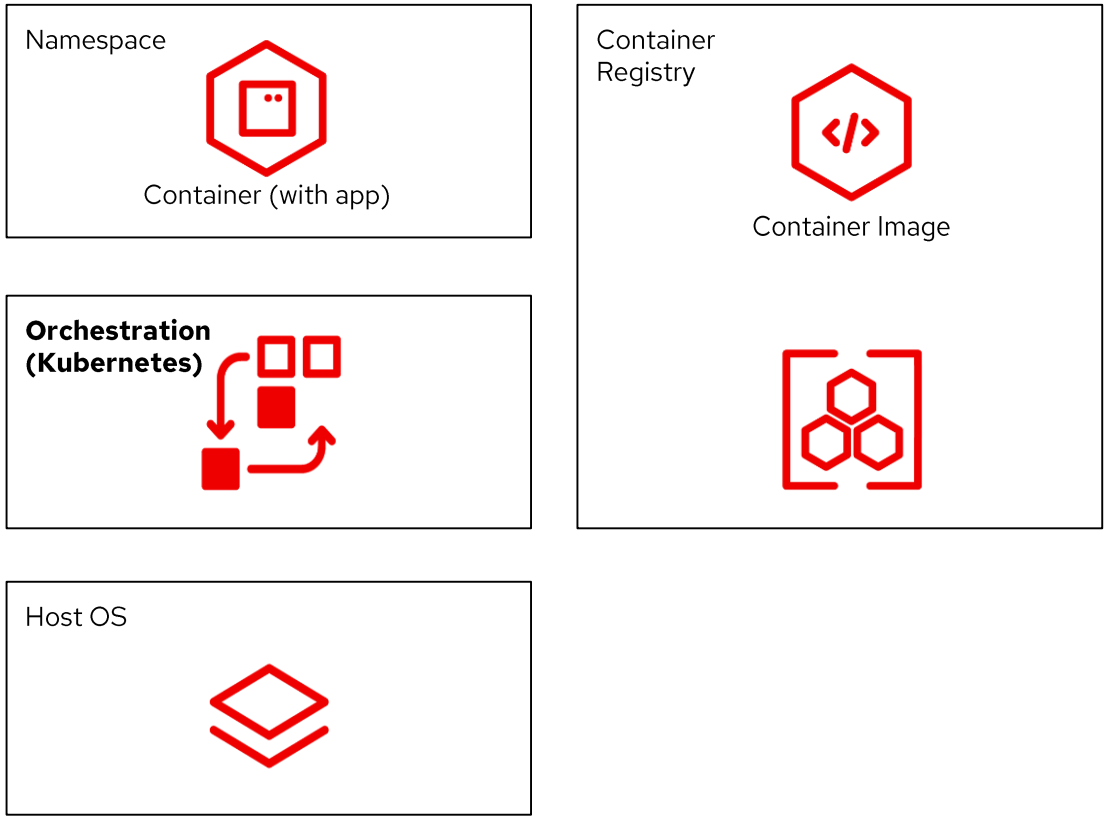


Red Hat

Orchestrator Risks

3.3 Orchestrator Risks

- 사용자 계정 및 권한관리 미비
- 잘못된 컨테이너 네트워크 분리
- 서로 다른 수준의 워크로드 혼재
- Master와 Node의 신뢰성

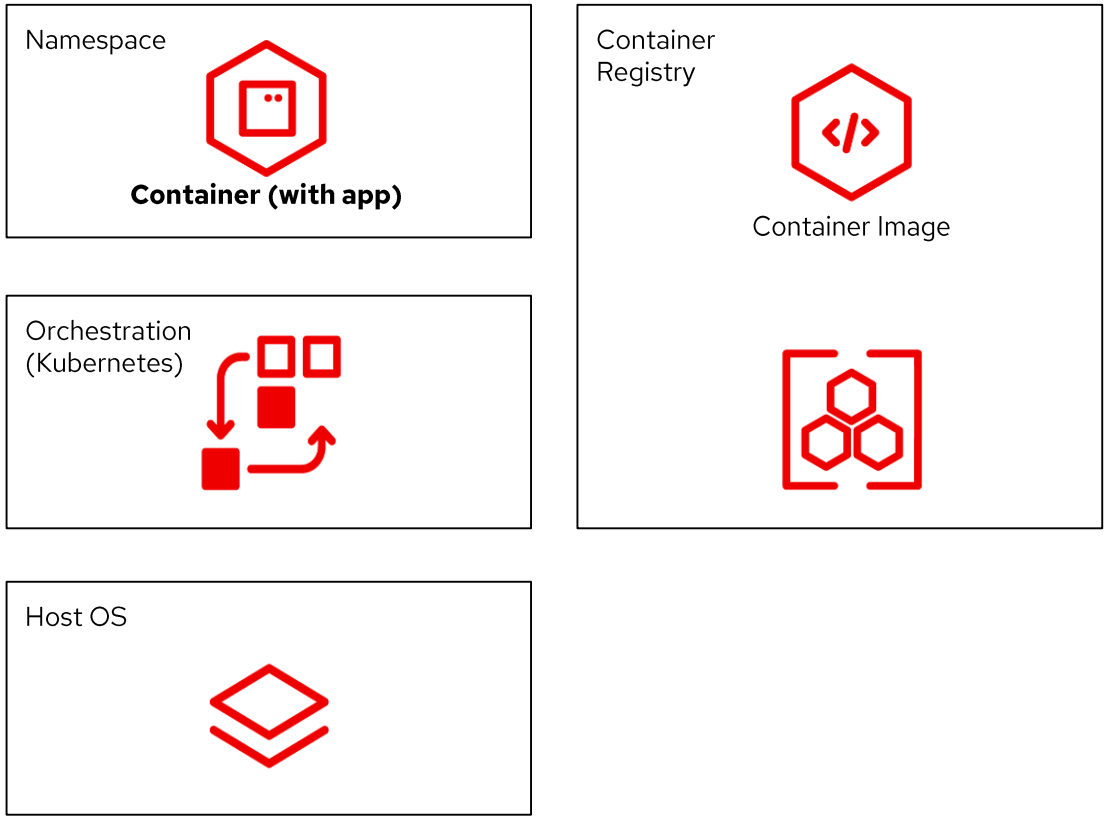


Red Hat

Container Risks

3.4 Container Risks

- 런타임 소프트웨어의 취약점
- 제한없는 네트워크 접근
- 안전하지 않은 컨테이너 런타임 설정
- 어플리케이션의 취약점
- 잘못된 컨테이너의 방치

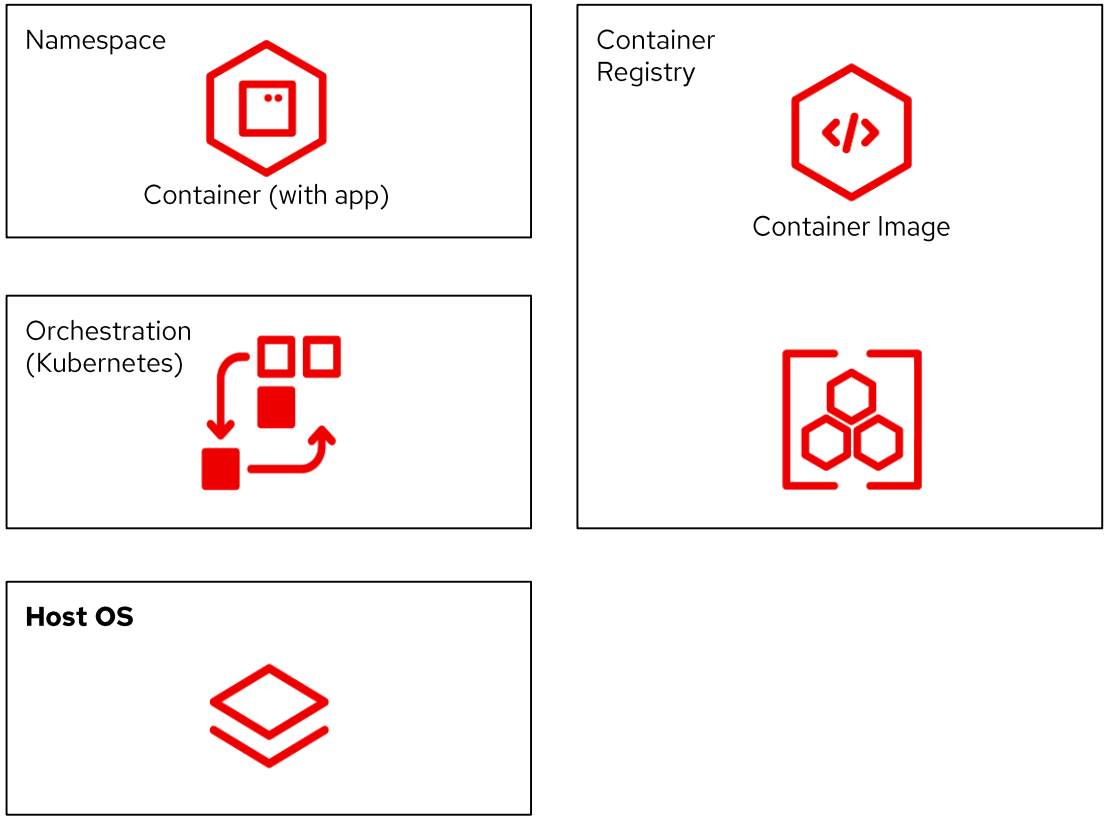


Red Hat

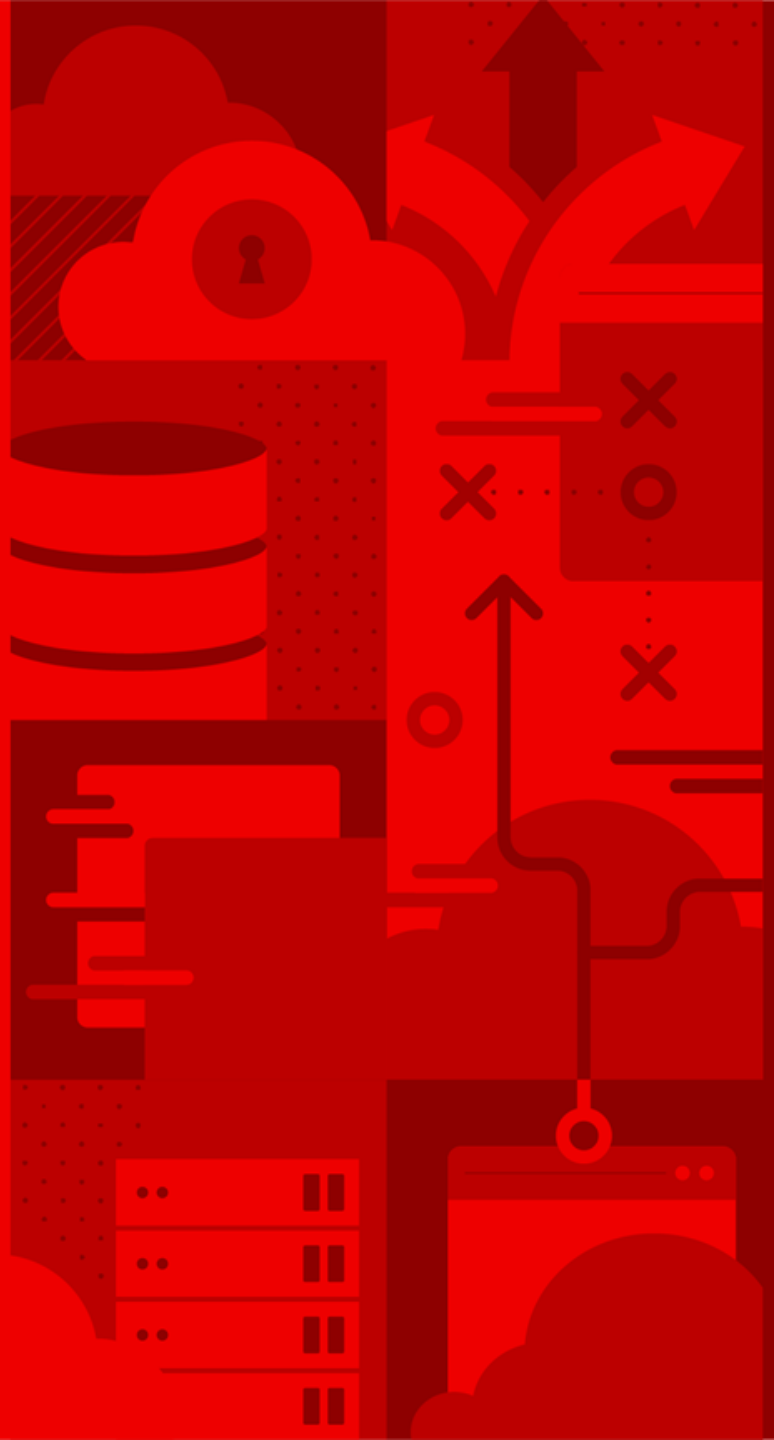
Host OS Risks

3.5 Host OS Risks

- 호스트 OS의 취약점 여부
- 커널 공유
- 불필요한 사용자 권한 부여
- 파일 시스템의 변조



Red Hat

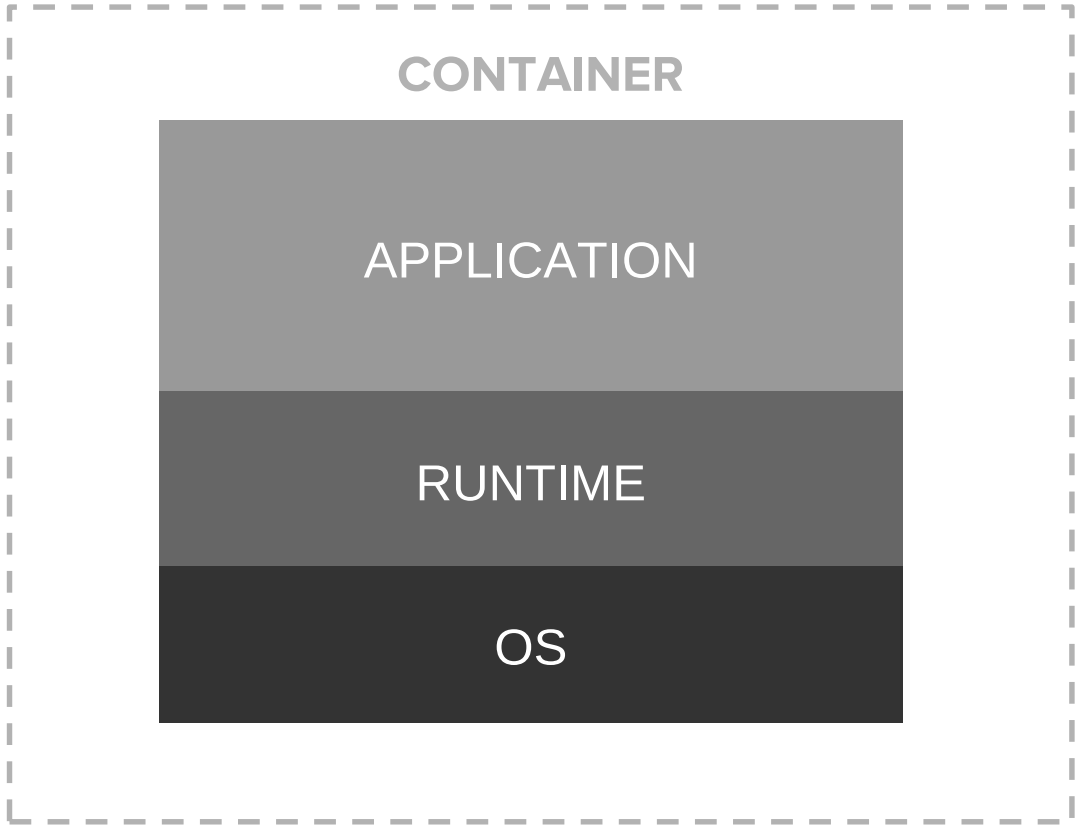


컨테이너 이미지 위협요소 및 방안

Red Hat

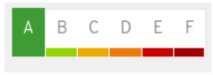
WHAT'S INSIDE?

- 컨테이너를 통해 인프라 시스템 전체를 파괴할 수 있다는 걸 알고 있나요?
- 혹시 애플리케이션에 알려진 취약점이 있는지 확인하셨나요?
- 런타임과 OS는 최신 상태인가요?



CONTENT: Container Health Index

The following grades and icons are used with a brief explanation of how they are calculated.



Grade A: This image does not contain known unapplied errata that fix Critical or Important flaws.

Grade B: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 7 days and no missing Important flaw is older than 30 days.

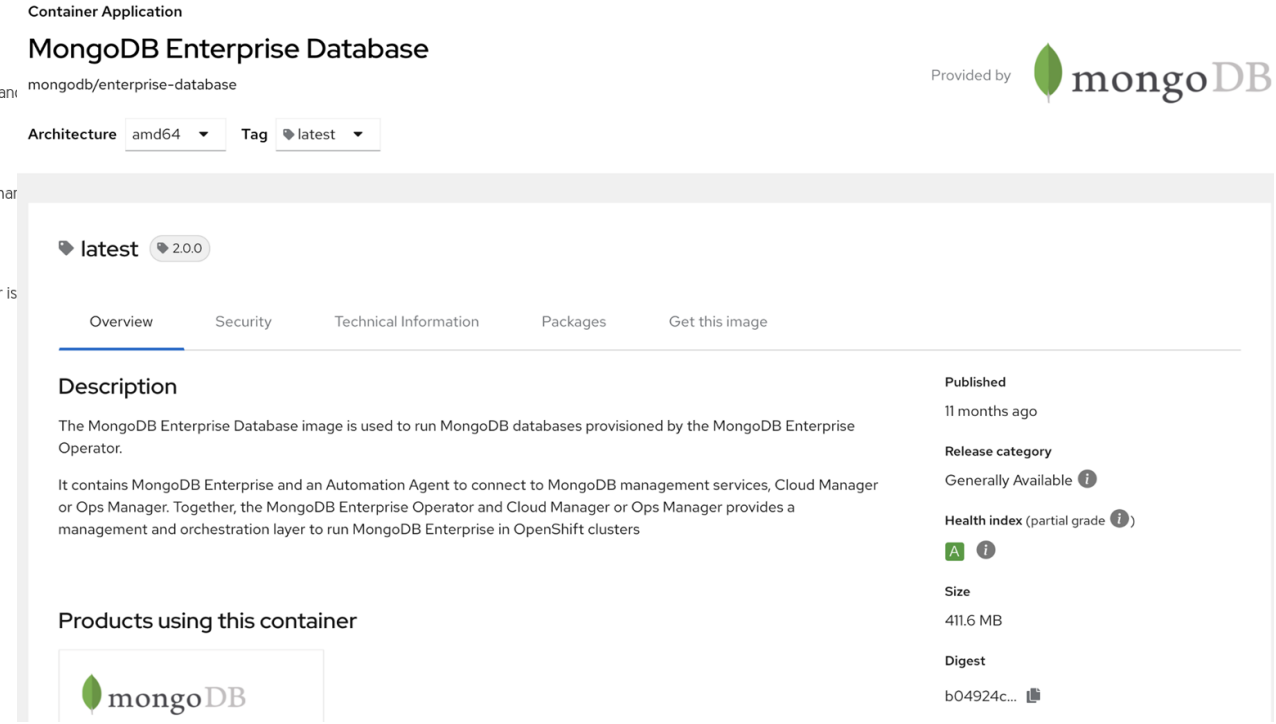
Grade C: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 30 days and no missing Important flaw is older than 90 days.

Grade D: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 90 days and no missing Important flaw is older than 365 days.

Grade E: This image may be missing Critical or Important security errata, but no missing Critical or Important flaw is older than 365 days.

Grade F: This image may be missing Critical or Important security errata, and they are older than 365 days. Or the container is of its lifecycle.

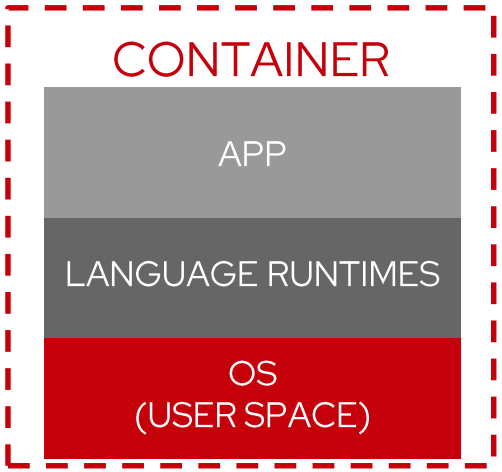
Grade Unknown: This image cannot be scanned as it is missing metadata required to perform the Container Health Index calculation.



Red Hat

컨테이너 이미지 보안

레드햇 공식 이미지 레지스트리 registry.redhat.io 에서 보안성 및 안정성이 검증된 UBI(Universal Base Image) 제공



Red Hat Universal Base Image는 RHEL에 기반하였으며 새로운 end user license agreement에 의해 무료로 사용 가능합니다.

Development

- 최소한의 리소스 점유 (~90 to ~200MB)
- 프로그래밍 언어 (Modularity & AppStreams)
- 단일 CI/CD chain 가능

Production

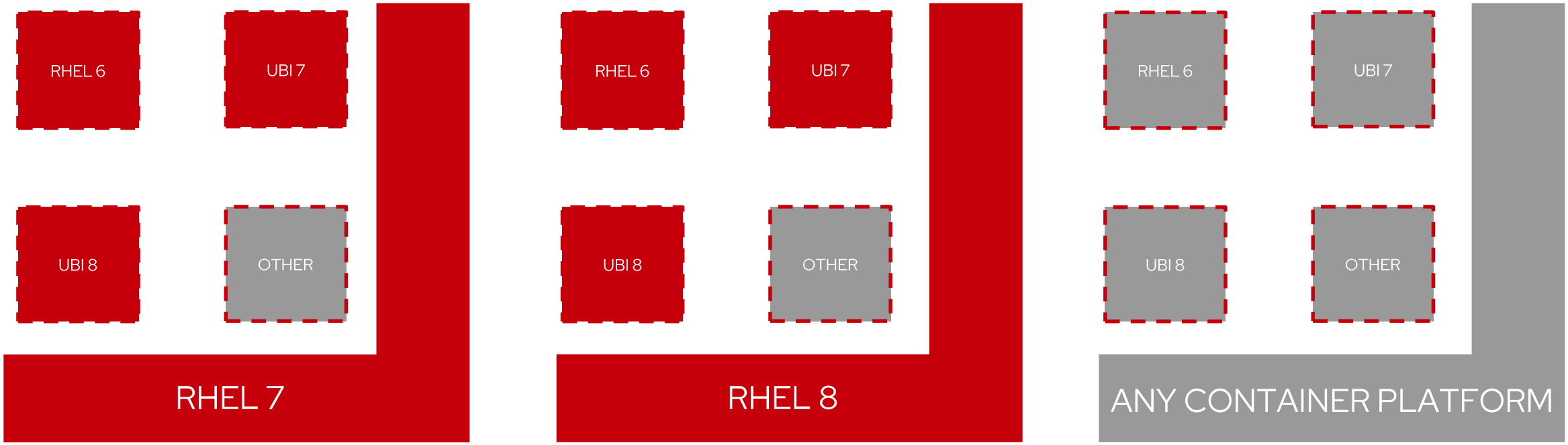
- RHEL 위에서 구동될 경우에는 RHEL처럼 지원됨
- RHEL과 동일한 성능, 보안성, 라이프사이클
- RHEL 지원 서브스크립션 적용 가능

https://catalog.redhat.com/software/containers/explore

Red Hat

Red Hat Container Base Image

검증된 UBI를 Base Image로 활용해 다양한 Upstream Image 빌드 가능



Red Hat Enterprise Linux 7

Red Hat Enterprise Linux 8

Like any upstream project

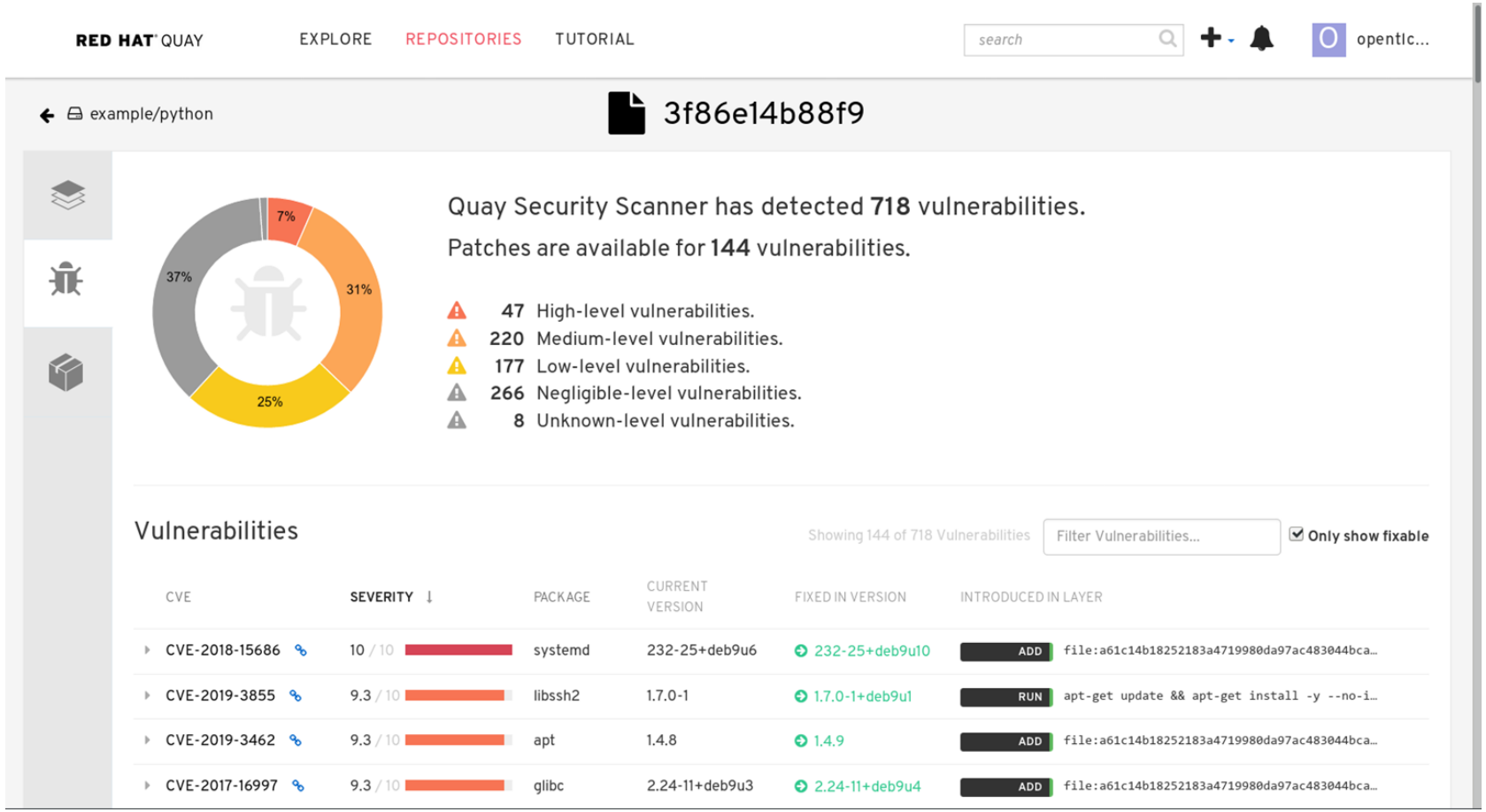
RED HAT SUPPORT

COMMUNITY SUPPORT

Red Hat

Container Image 취약점 검사
Red Hat Quay 이미지 레지스트리의 컨테이너 레이어의 보안 검증

- Self-Managed Service 제공
- 취약점 검사 (Clair)
- Geographic Replication
- Build Image Triggers
- 이미지 롤백 (with Time Machine)



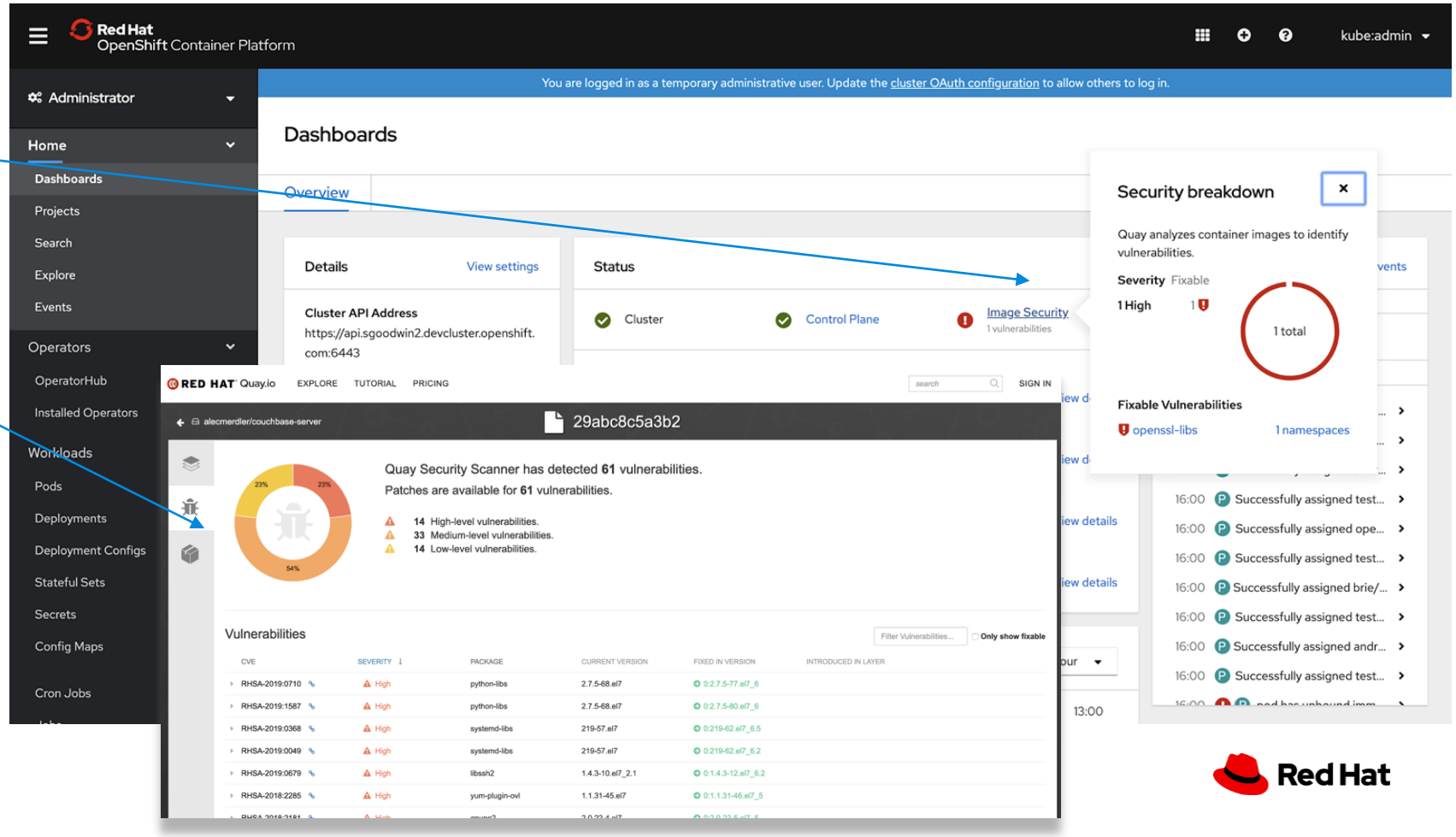
Red Hat

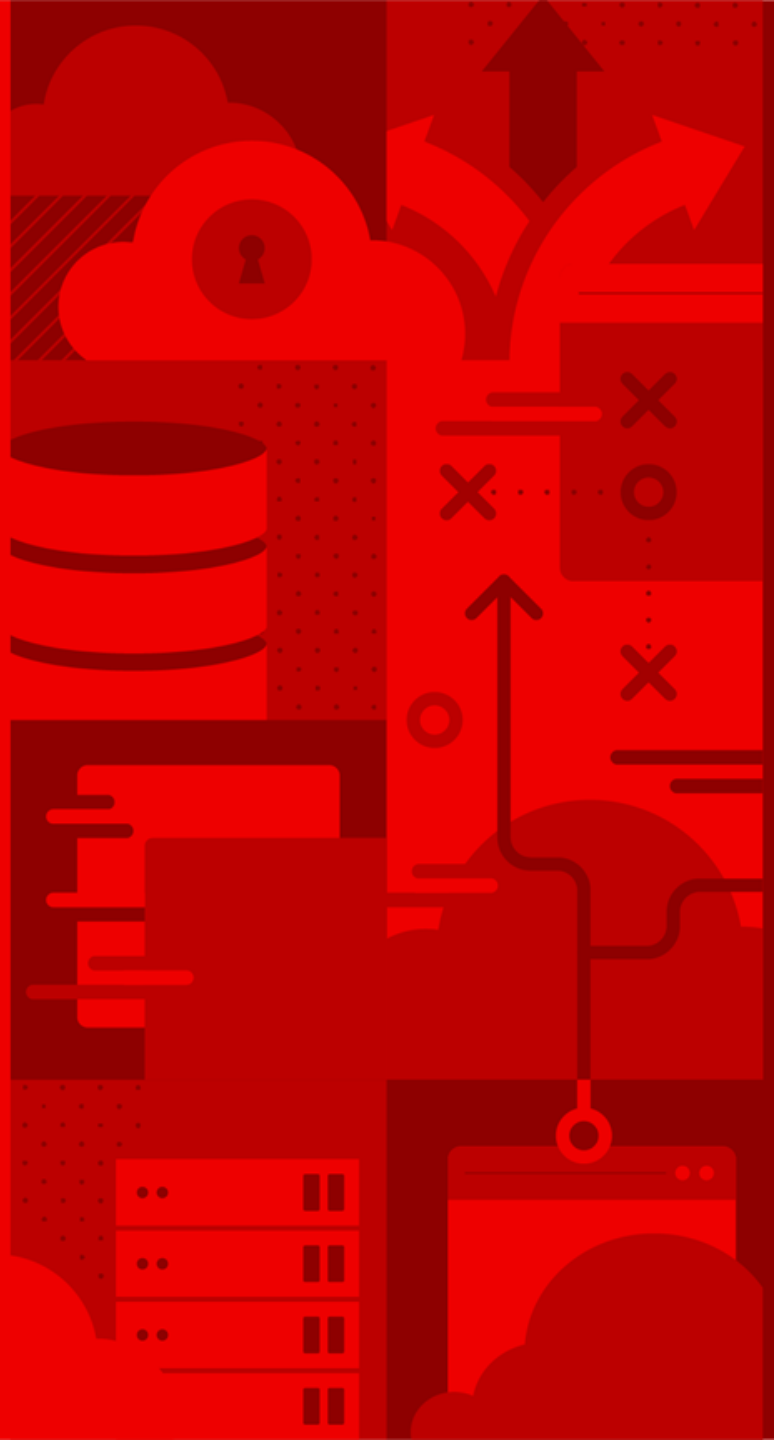
Container 취약점 관리

Red Hat Quay로 Security Vulnerabilities 기능 구현

모든 컨테이너 취약점을 콘솔 대시보드에서 바로 확인 가능

- **Red Hat Quay**를 통해 더 자세한 정보 확인 가능(link out)
- Quay Operator는 **On-premise와 External** Quay Registries를 모두 지원
- 현재 **보안 검사도구로 Clair 사용**; 차후 다른 벤더로 확장 계획 (TwistLock, Aqua 등)
- *Quay로 관리되는 이미지에 대해서만 동작*





마무리 & 키워드

Red Hat

Red Hat Training and Certification

Assess

무료 온라인 기술 평가를 통해 Red Hat 기술에 대한 지식과 능력을 평가하고 추천 커리큘럼을 확인해 보세요

Train

솔루션 중심 과정과 숙련된 공인 인증 강사와 함께 학습하세요. 원격, 셀프 모드의 온라인 학습도 가능합니다.

Validate

실습 기반의 Red Hat 자격 인증 시험을 통해 성공적인 학습 능력을 검증하세요.

과정코드	과정명	개요
RH415	Red Hat Security: Linux in Physical, Virtual, and Cloud	베어메탈(bare metal), 가상 및 클라우드 환경에 배포된 Red Hat Enterprise Linux 시스템의 보안 관리 학습 과정

레드햇 교육 문의:
korea-training@redhat.com, 02-3490-2949/5205

Red Hat

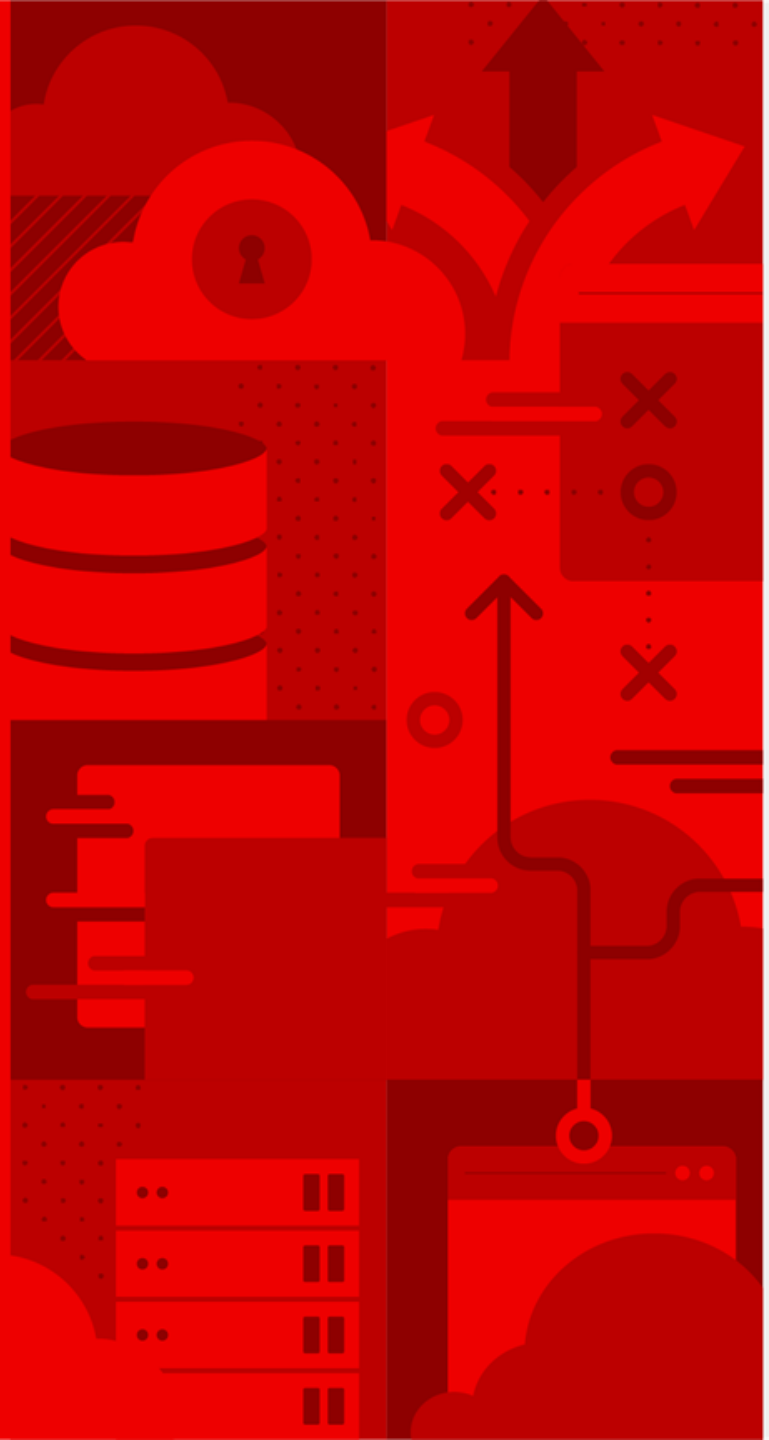
키워드

NIST 800-190

Attitude

보안성/ 안정성 측면을 고려한 UBI 사용하기

Red Hat



Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat