1 CheatSheet: Container Compliance **SECURITY**

- PDF Link: cheatsheet-compliance-A4.pdf, Category: security
- Blog URL: `https://cheatsheet.dennyzhang.com/cheatsheet-compliance-A4`
- Related posts: Cheatsheet: Kubernetes Security, Cheatsheet: Linux Security #denny-cheatsheets

File me Issues or star this repo.

1.1 Compliance Scan Tools

Name	Comment
Clair	Vulnerability Static Analysis for Containers
Dive	A tool for exploring each layer in a docker image
Tern	Open Source compliance for containers from VMware

1.2 Terminology

Name	Comment
OSS	Open Source Software
OSS/TP	Open Source Software/Third Party
CVE	Common Vulnerabilities and Exposures
OSM	Open-source & Security Manager System
OSL	Open Source License file
ODP	Open source Disclosure Package
SBR	Source, Build and Replace

1.3 Common Docker Registry

Name	Comment
Docker hub	
Google container registry	
Self-maintained registry	JFrog, Nexus

1.4 Docker Scan

Name	Comment
Detect wasted space in docker image via dive	`dive <docker_tag>`, `dive golang:1.12`
Analysis of the dockerfile is manual	

1.5 Container Compliance Principles

Name	Comment
Avoid pulling from external sources	Need to mirror the repo for apt-get, wget, etc
Avoid using un-versioned packages	Reproducibility
Choose container base images	No authroized or insecured base images
Avoid installing package with latest version	Insecure because the process is not reproducible
Build from source code	Good for the overall goverance
Pin the package version	Make the build re-entrant and stable
In Dockerfile, use `COPY`, instead of `ADD`	

1.6 More Resources