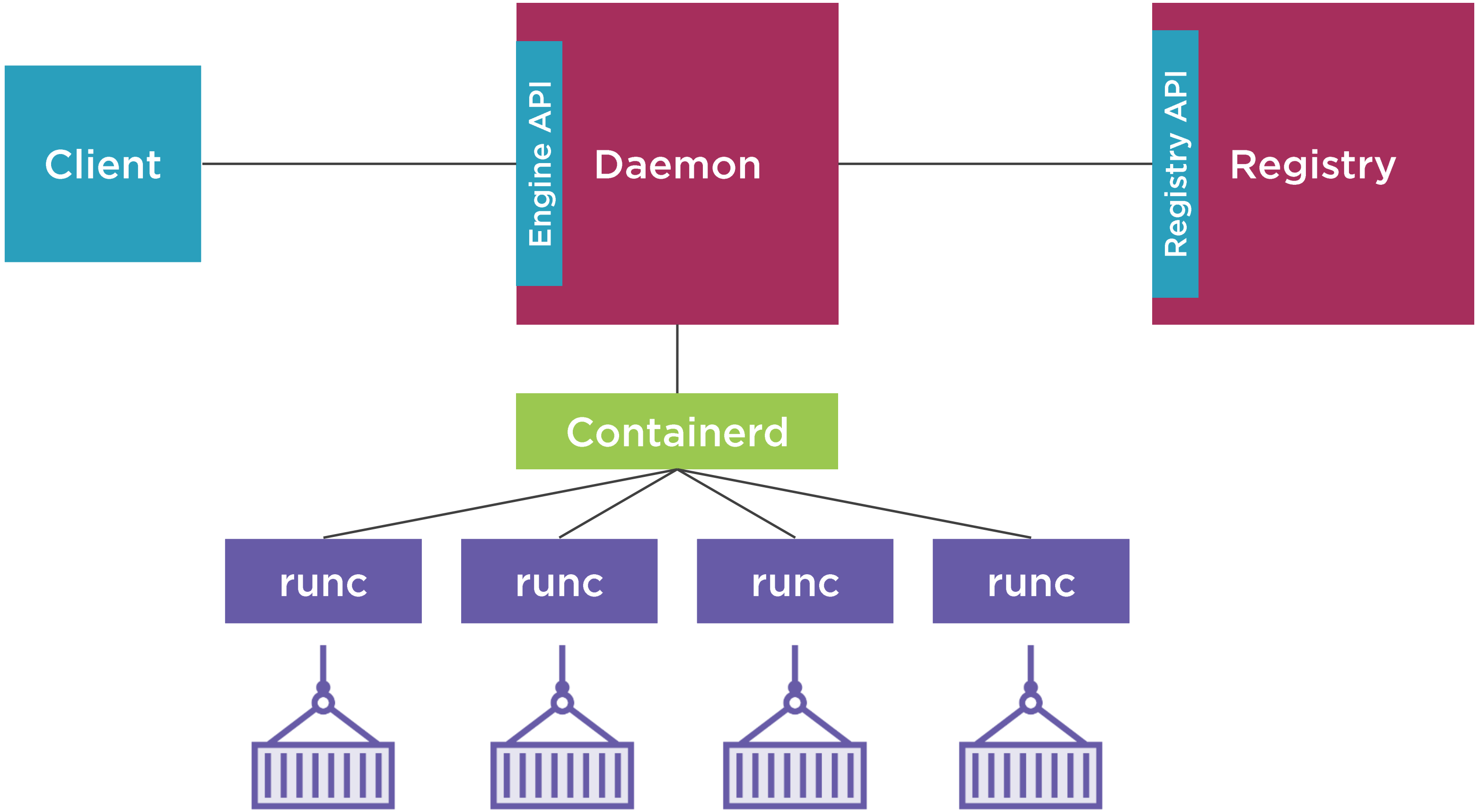
Securing the Docker Platform

ESTABLISHING A BASELINE FOR DOCKER PLATFORM SECURITY

Nigel Brown

@n_brownuk www.windsock.io

Docker Platform



Module Outline

Defining the Docker platform

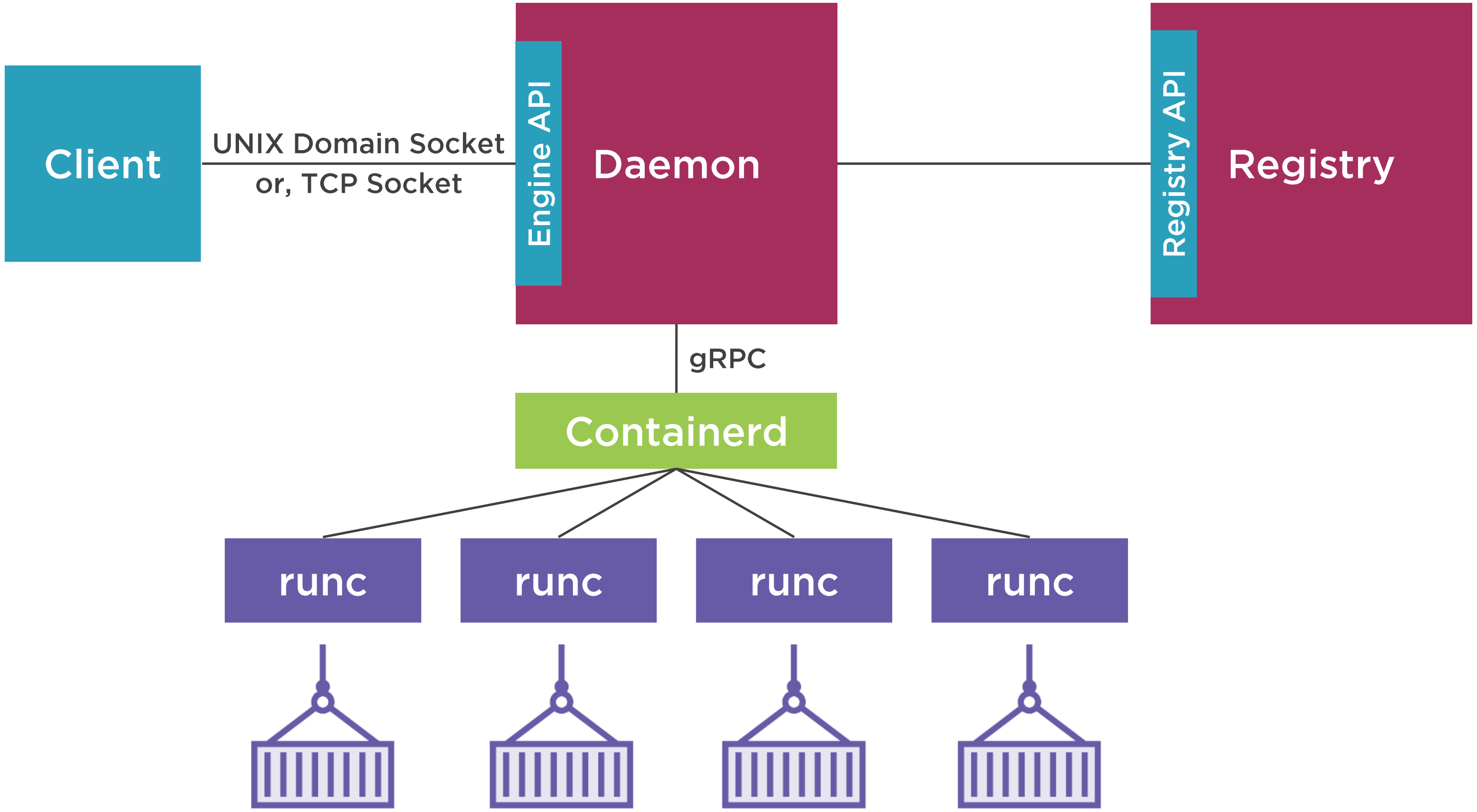
Finding information on vulnerabilities

Determining what needs securing

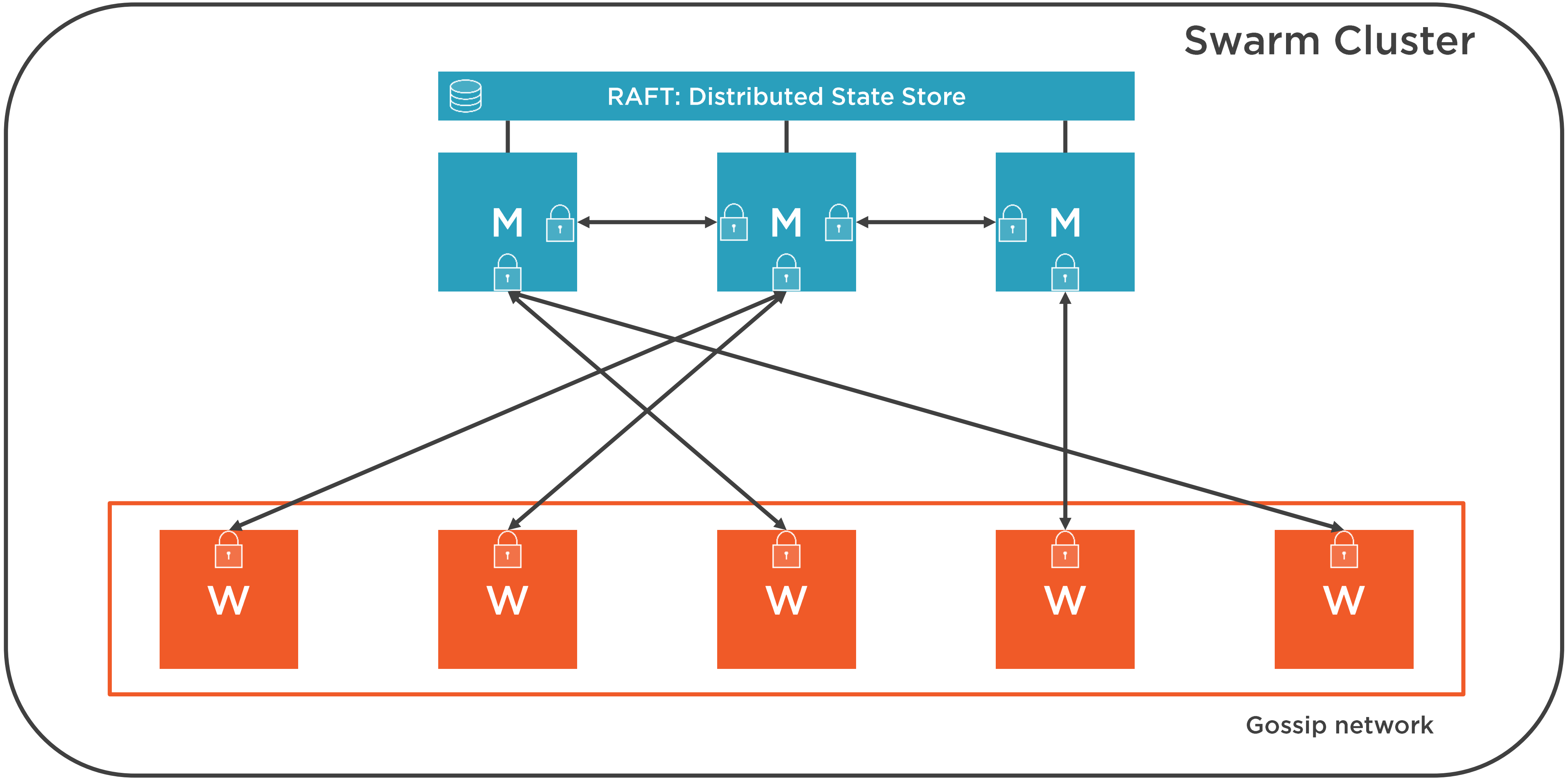
Tools for measuring security compliance

Using a benchmark to test compliance

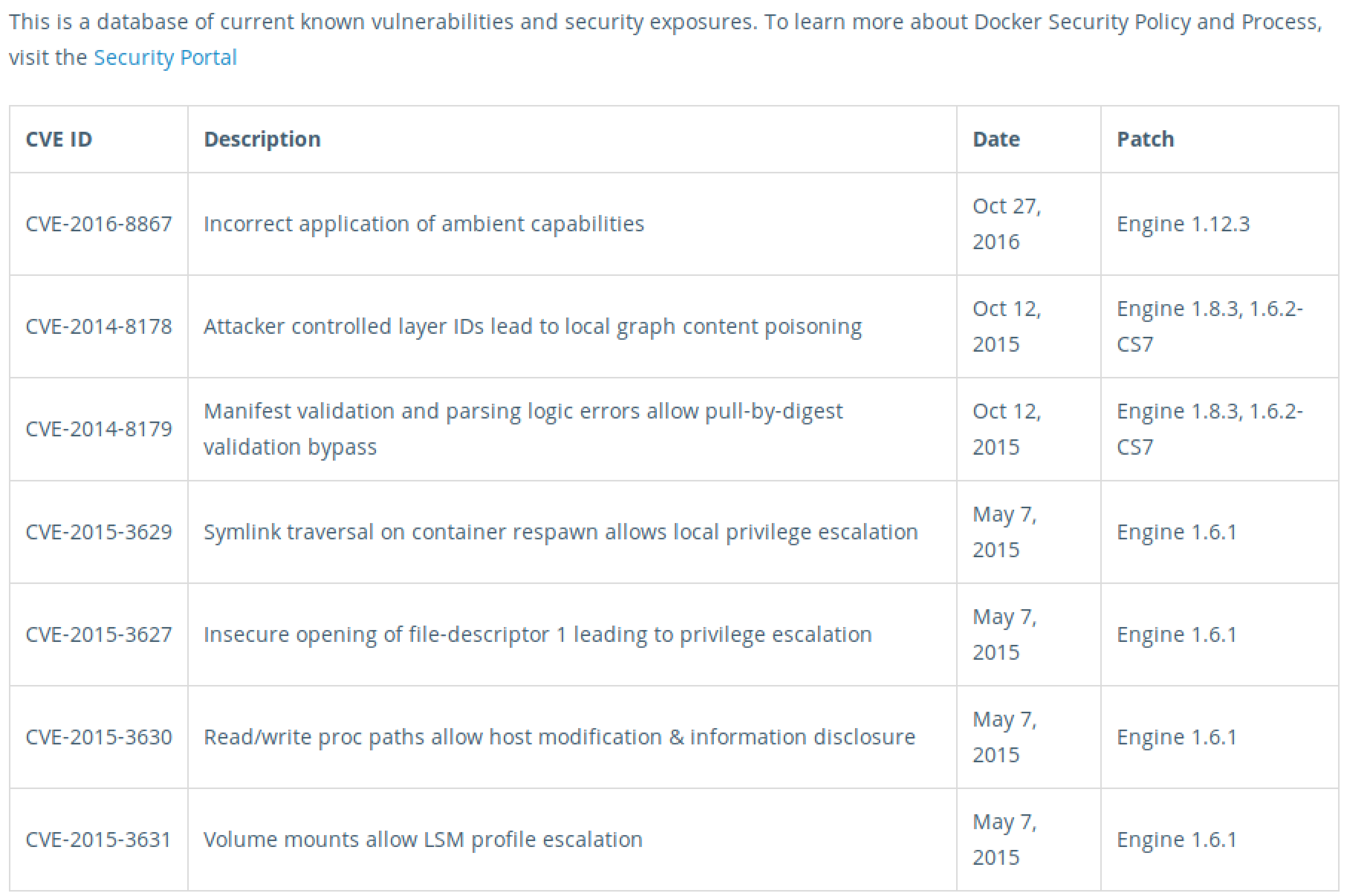
Docker Platform



Docker Swarm Mode



Docker CVE Database



This is a database of current known vulnerabilities and security exposures. To learn more about Docker Security Policy and Process, visit the Security Portal

CVE ID	Description	Date	Patch
CVE-2016-8867	Incorrect application of ambient capabilities	Oct 27, 2016	Engine 1.12.3
CVE-2014-8178	Attacker controlled layer IDs lead to local graph content poisoning	Oct 12, 2015	Engine 1.8.3, 1.6.2-CS7
CVE-2014-8179	Manifest validation and parsing logic errors allow pull-by-digest validation bypass	Oct 12, 2015	Engine 1.8.3, 1.6.2-CS7
CVE-2015-3629	Symlink traversal on container respawn allows local privilege escalation	May 7, 2015	Engine 1.6.1
CVE-2015-3627	Insecure opening of file-descriptor 1 leading to privilege escalation	May 7, 2015	Engine 1.6.1
CVE-2015-3630	Read/write proc paths allow host modification & information disclosure	May 7, 2015	Engine 1.6.1
CVE-2015-3631	Volume mounts allow LSM profile escalation	May 7, 2015	Engine 1.6.1

https://www.docker.com/docker-cve-database

Responsible Disclosure

A vulnerability disclosure model, in which a vulnerability is disclosed only after a period of time, that allows for the vulnerability to be patched.

Inform and Be Informed

Be a good citizen, and responsibly report any discovered security vulnerabilities, to security@docker.com

Join the Docker Community Forum (https://forums.docker.com), and follow the 'Announcements' category

Monitor the #docker-security Slack channel, by signing up to participate in the Docker community (https://community.docker.com)

Docker Documentation

- http://dockr.ly/2oVM2Cr

Understanding and Hardening Linux Containers

- http://bit.ly/2G7dRz7

Center for Internet Security Benchmark

- http://bit.ly/2fiNTg8

CIS Docker Benchmark

Benchmark	Version	Docker Version	Date
CIS Docker Benchmark	1.2.0	Docker CE/EE 17.09	Draft
CIS Docker CE Benchmark	1.1.0	Docker CE 17.06	06 Jul 2017
CIS Docker 1.13.0 Benchmark	1.0.0	Docker 1.13.0	19 Jan 2017
CIS Docker 1.12.0 Benchmark	1.0.0	Docker 1.12.0	15 Aug 2016
CIS Docker 1.11.0 Benchmark	1.0.0	Docker 1.11.0	14 Apr 2016

Benchmark Content

Recommendations

Best practices for
providing a secure
Docker platform

Profiles

Categories defining the
effect of applying
security measures

Scoring

Individual test scores
contribute to overall
benchmark score

Example Recommendation for Logging Level

Recommendation Detail	Narrative
Profile applicability	Level 1 – Docker
Description	Set Docker daemon log level to `info`
Rationale	Log events for later review
Audit	`ps –ef	grep docker`
Remediation	`dockerd --log-level=“info”`
Impact	None
Default value	Log level set to `info`

InSpec

InSpec is an open source auditing and testing framework, created by Chef (https://www.inspec.io/)

InSpec uses a Ruby-based DSL, for defining the controls for testing infrastructure

Community provided InSpec profiles are available at the Chef Supermarket (https://supermarket.chef.io/)

An InSpec profile is available, which implements the CIS Docker Benchmark (https://git.io/vxftx)

Docker Bench for Security

A script-based audit system

Open source implementation

- (https://git.io/vxnOO)

Maintained by Docker

Conforms to the CIS Docker CE Benchmark

Container-based for convenience

Module Summary

Defined the components of the Docker platform

Identified pertinent sources of security information

Discovered open source, community tools for auditing