Optimizing the Configuration of the Docker Host

Nigel Brown

@n_brownuk www.windsock.io

Module Outline

Employing a minimal operating system

Hardening the host operating system

Keeping the Docker platform current

Auditing important Docker artifacts

Operating System Choice

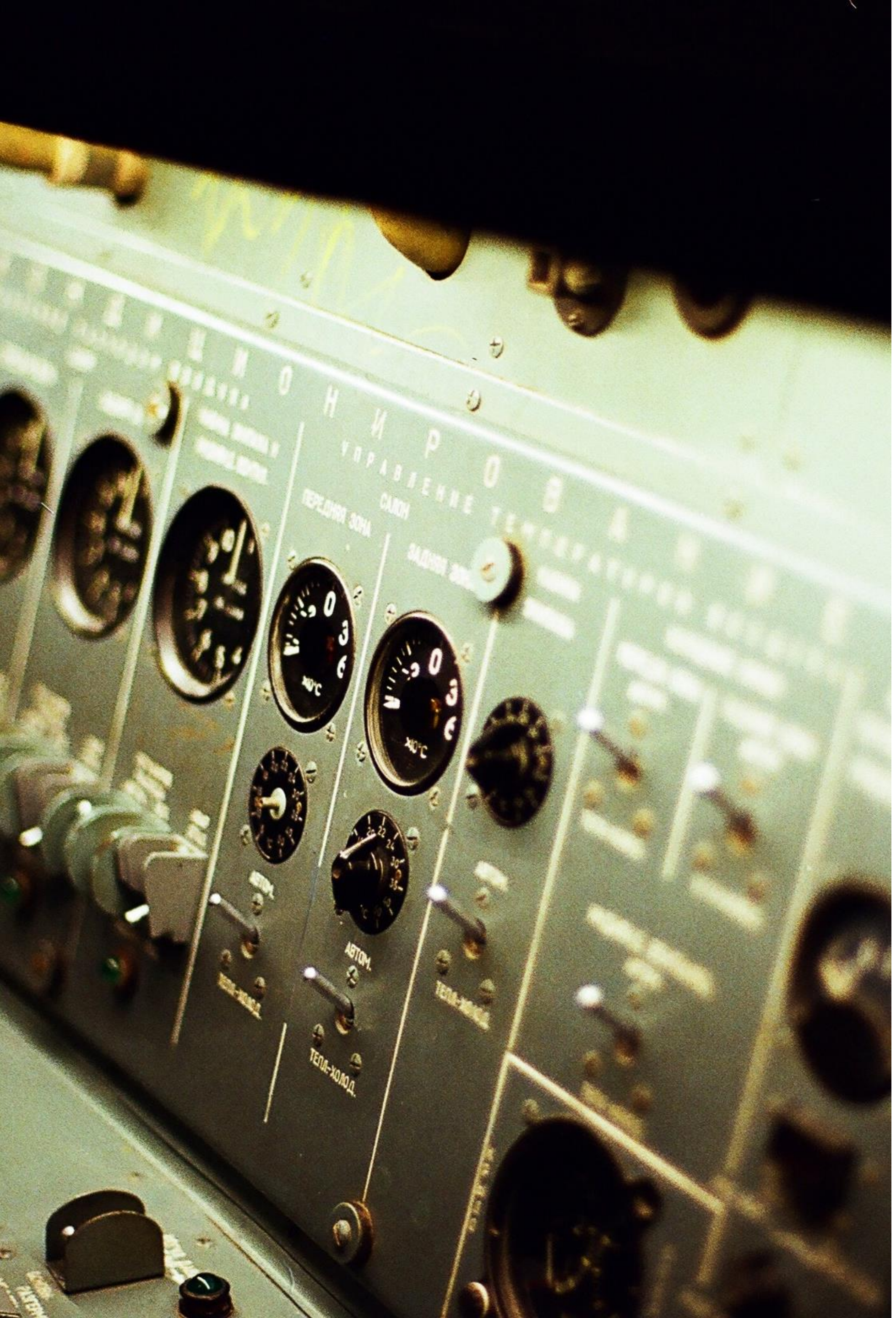
Which operating system is the best choice for hosting a Docker platform?

Lots of factors may influence the eventual decision of operating system provider

The cloud native era heralds a new breed of minimal operating system

Traditional vs. Minimal

Traditional	Minimal
General purpose	Purpose specific
Large, and resource hungry	Minimal, with a small footprint
Incremental updates	Atomic, transactional updates
Read-write partitions	Read-only OS partition
Bigger attack surface	Inherently more secure



Container Linux

- https://coreos.com/why

Atomic Host

- https://www.projectatomic.io

RancherOS

- https://rancher.com/rancher-os

Ubuntu Core

- https://www.ubuntu.com/core

Photon OS

- https://vmware.github.io/photon

LinuxKit

- https://github.com/linuxkit/linuxkit

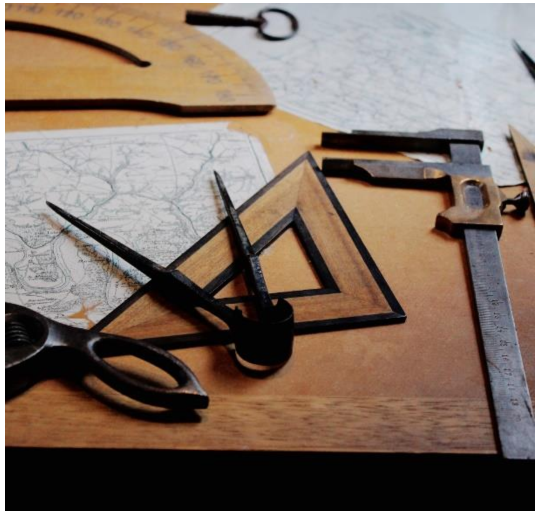
Hardening the Host Operating System

Plan of Action

Hardening a Linux host requires planning

Information Sources

Sources of information are innumerable



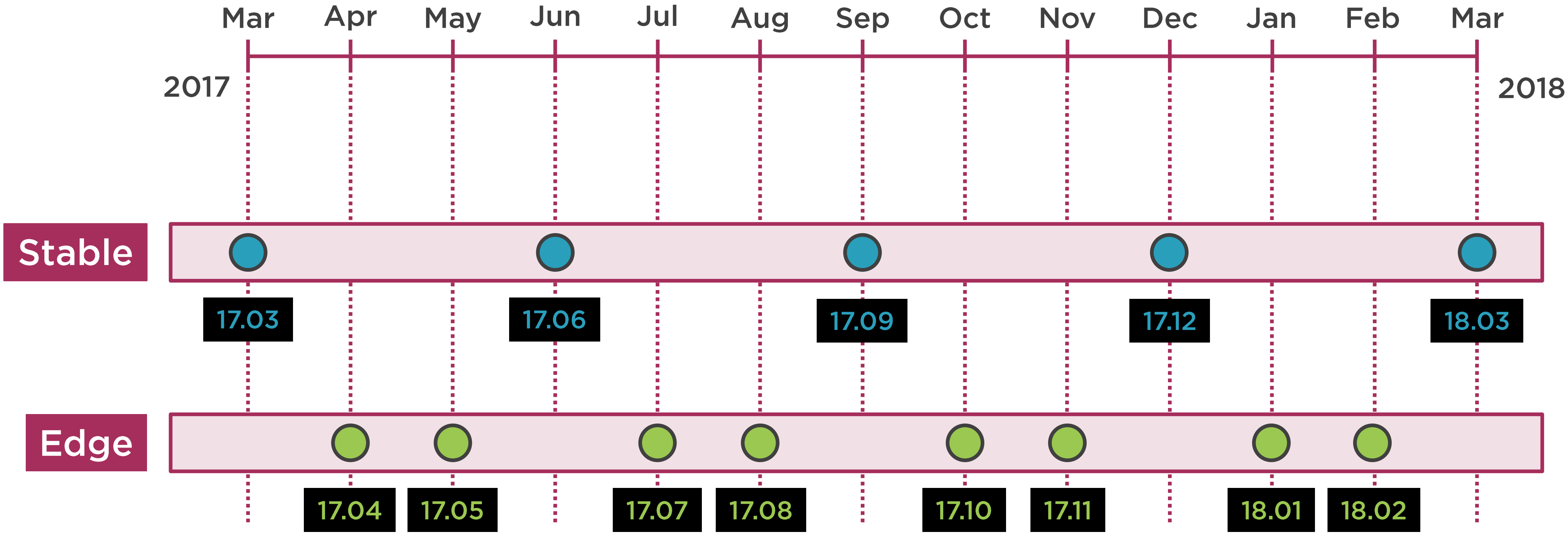
CIS Benchmarks

CIS provides distro-specific benchmarks

CIS Benchmarks for Linux

Distro	Benchmark	Version	URL
n/a	Distribution Independent Linux	1.1.0	https://bit.ly/2uQWZe0
Debian	Debian Linux 8	1.0.0	https://bit.ly/2EjTxYN
Ubuntu	Ubuntu Linux 16.04 LTS	1.1.0	https://bit.ly/2JkyQjc
Amazon	Amazon Linux	2.1.0	https://bit.ly/2uNZgXp
CentOS	CentOS Linux 7	2.2.0	https://bit.ly/2GBm1nb
Oracle	Oracle Linux 7	2.1.0	https://bit.ly/2HbABP4
Red Hat	Red Hat Enterprise Linux 7	2.2.0	https://bit.ly/2q7etxY
SUSE	SUSE Linux Enterprise 12	2.0.0	https://bit.ly/2H1d8CN

Docker CE Release Schedule



Sourcing Docker Platform Software

Package Sources

Linux distro packages are often out of date

Docker Repos

Docker provides its own set of packages

Edge Channel

Fixes provided up until the next release

Stable Channel

Fixes for a month following new release

Point Releases

Patches and updates via point releases

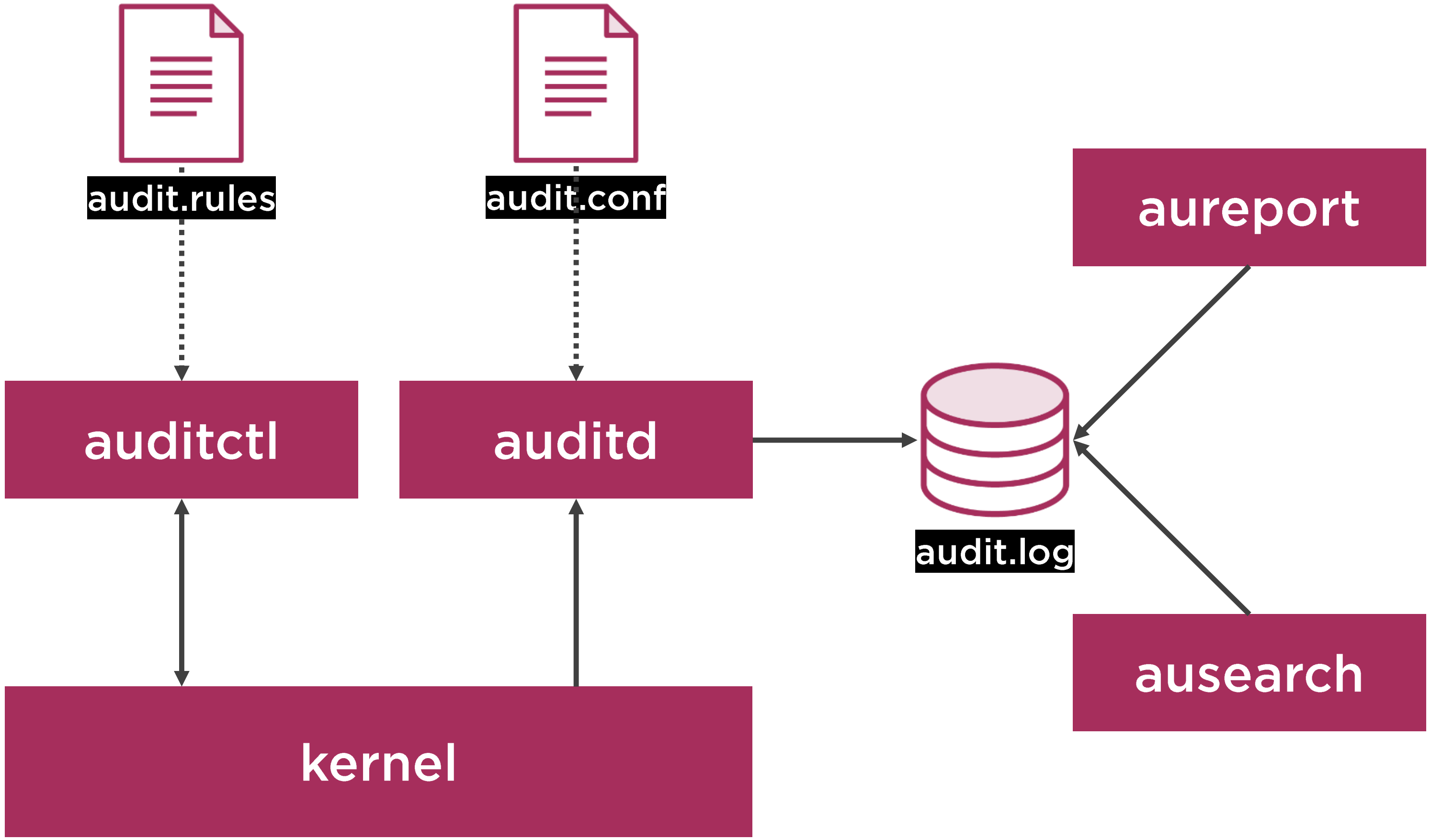
The Linux Audit Framework

Provides a means for analyzing the activity that occurs on the host system

The audit framework is not a real-time preventative security mechanism

It can be used to identify potential security weaknesses or policy violations

Using the Audit Framework



Important Artifacts

Binaries

- */usr/bin/dockerd* **(F)**
- */usr/bin/docker-containerd* **(F)**
- */usr/bin/docker-runc* **(F)**

Config Files

- */etc/default/docker* **(F)**
- */etc/docker/daemon.json* **(F)**

Systemd Unit Files

- *docker.service* **(F)**
- *docker.socket* **(F)**

Execution Root

- */var/lib/docker* **(D)**

TLS Artifacts

- */etc/docker* **(D)**

Module Summary

Take steps to harden the host platform against attack

If possible, use a minimal Linux host operating system

Audit key components, with the Linux audit framework