LINUXKIT

Moby and LinuxKit

What to expect

Lorenzo Fontana - @fntlnz
DevOps @ Kiratech
Docker Captain - Docker Maintainer
https://fntlnz.wtf

KIRATECH
WE DEVOPS IT

What happened?

What to expect?

Governance?

What will change?

What's that LinuxKit?

Will I become a Moby captain?

KIRATECH
WE DEVOPS IT

“A platform is only as secure as **its weakest** components„

KIRATECH®
WE DEVOPS IT

Microsoft Azure

vmware

amazon web services

“I want Docker for whateverplatform!„

— ***Me*** *(whenever I discover any new platform)*

Windows 10

Google Cloud Platform

KIRATECH
WE DEVOPS IT

LinuxKit

a **SECURE** *Linux subsystem*

Only works with containers

- Smaller attack surface
- Immutable infrastructure
- Sandboxed system services
- Specialized patches and configurations

Incubator for security innovations

- Wireguard, Landlock, KSPP
- MirageOS type safe system daemons
- okernel

Community-first security process

- Linux is too big for a single company to secure it
- Participate in existing Linux security efforts

LinuxKit

a **LEAN** *Linux subsystem*

- Minimal size, minimal boot time
- All system services are containers
- Everything can be removed or replaced

LinuxKit

a **PORTABLE** *Linux subsystem*

- Desktop, Server, IoT, Mainframe
- Intel & ARM
- Bare Metal & Virtualized
- On prem & in the Cloud

Everything is a yaml file: `kernel`

```yaml
kernel:
 image: "linuxkit/kernel:4.9.x"
 cmdline: "console=ttyS0 console=tty0 page_poison=1"
```


see: https://github.com/linuxkit/linuxkit/blob/master/docs/yaml.md#kernel

Everything is a yaml file: `init`

```yaml
init:
  - linuxkit/init:1c8cd75ec89313f4058b069449e9bac966cd96b1
  - linuxkit/runc:b0fb122e10dbb7e4e45115177a61a3f8d68c19a9
  - linuxkit/containerd:60e2486a74c665ba4df57e561729aec20758daed
  - linuxkit/ca-certificates:eabc5a6e59f05aa91529d80e9a595b85b046f935
```


see: https://github.com/linuxkit/linuxkit/blob/master/docs/yaml.md#init

Everything is a yaml file: onboot

```yaml
onboot:
 - name: sysctl
   image: "linuxkit/sysctl:2cf2f9d5b4d314ba1bfc22b2fe931924af666d8c"
   net: host
   pid: host
   ipc: host
   capabilities:
    - CAP_SYS_ADMIN
   readonly: true
```


see: https://github.com/linuxkit/linuxkit/blob/master/docs/yaml.md#onboot

Everything is a yaml file: `services`

```yaml
services:
 - name: rngd
   image: "linuxkit/rngd:c42fd499690b2cb6e4e6cb99e41dfafca1cf5b14"
   capabilities:
    - CAP_SYS_ADMIN
   oomScoreAdj: -800
   readonly: true
 - name: nginx
   image: "nginx:alpine"
   capabilities:
    - CAP_NET_BIND_SERVICE
    - CAP_CHOWN
    - CAP_SETUID
    - CAP_SETGID
    - CAP_DAC_OVERRIDE
   net: host
```

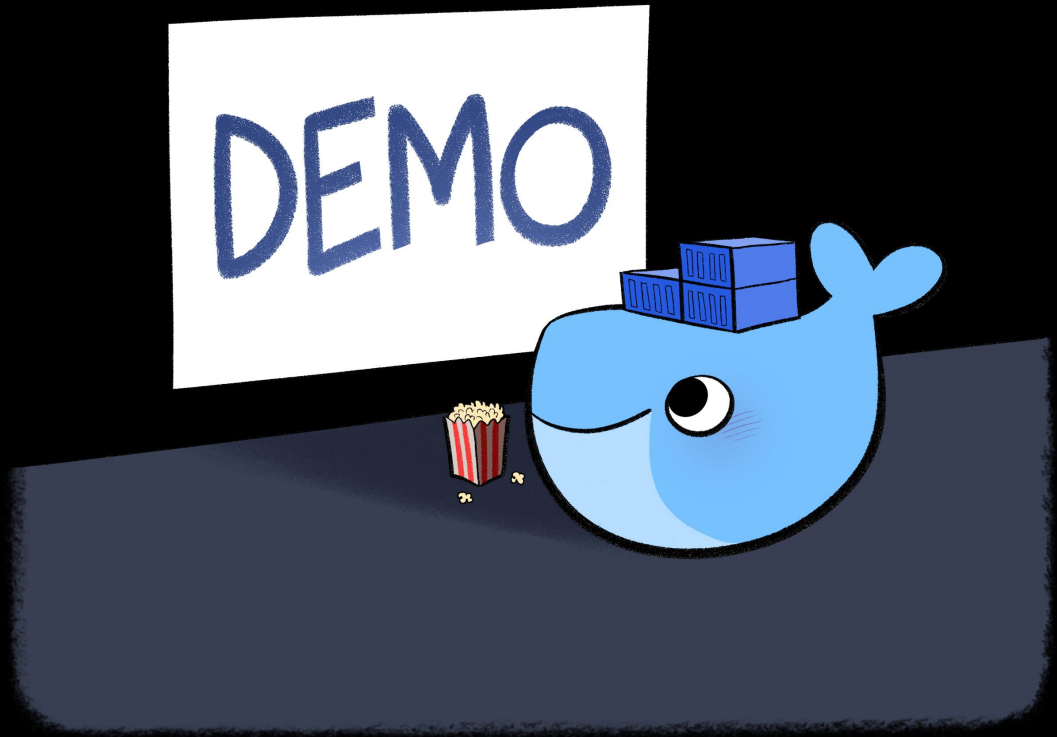
KIRATECH® WE DEVOPS IT

see: https://github.com/linuxkit/linuxkit/blob/master/docs/yaml.md#services

Everything is a yaml file: `output`

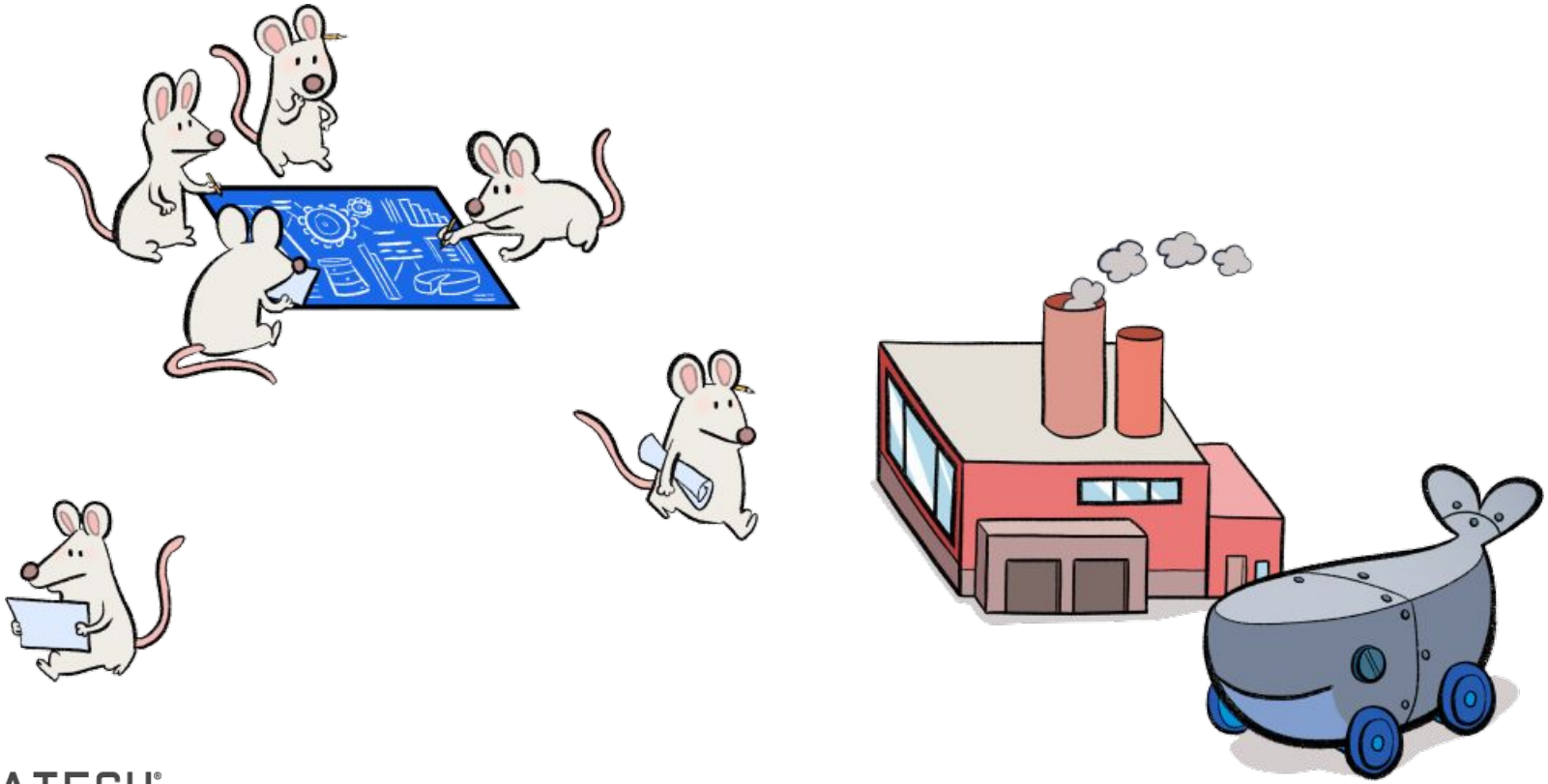
```yaml
outputs:
  - format: kernel+initrd
  - format: iso-bios
  - format: iso-efi
  - format: vhd
  - format: vmdk
```


see: https://github.com/linuxkit/linuxkit/blob/master/docs/yaml.md#output

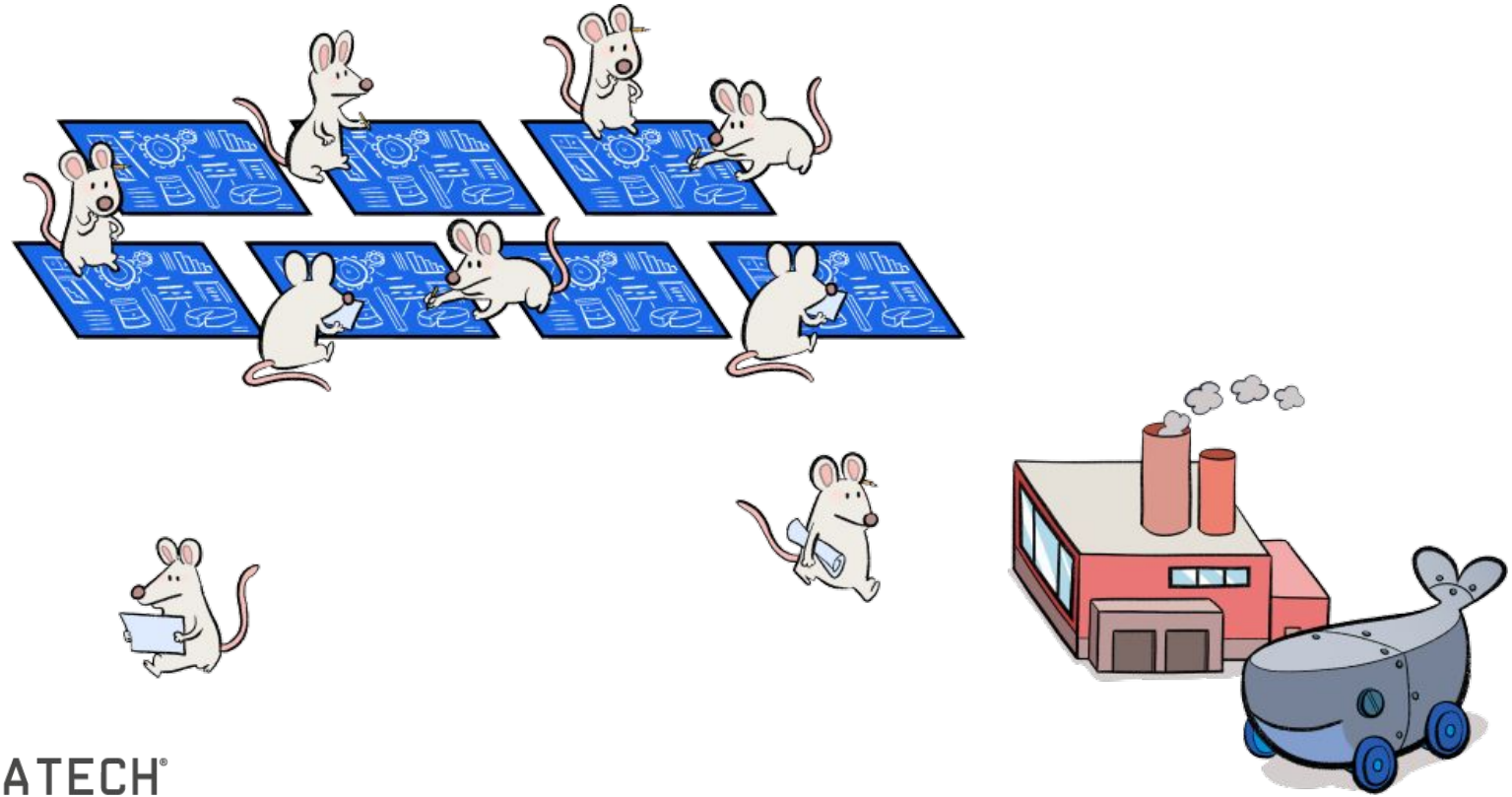


KIRATECH
WE DEVOPS IT

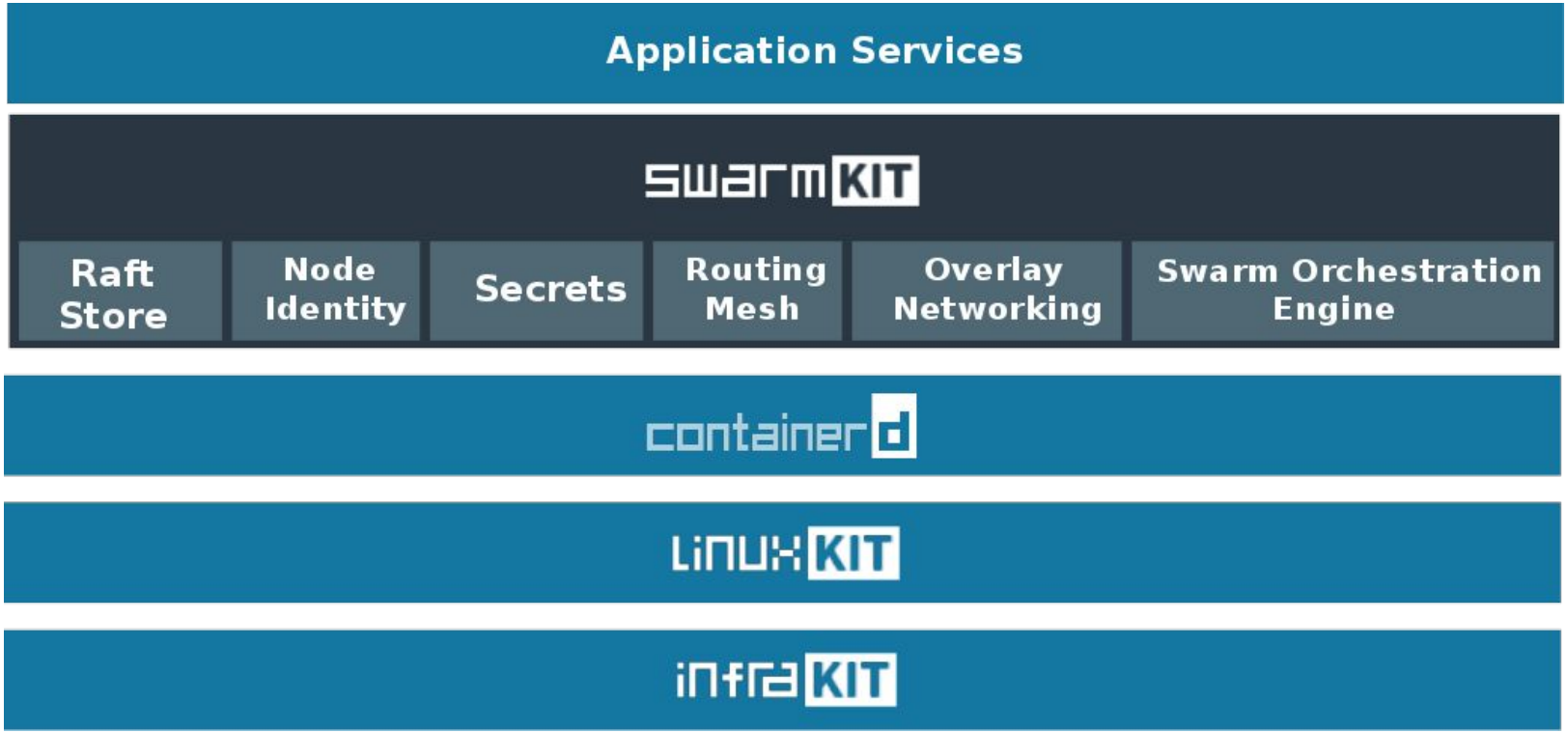
Production model: **Open Source**



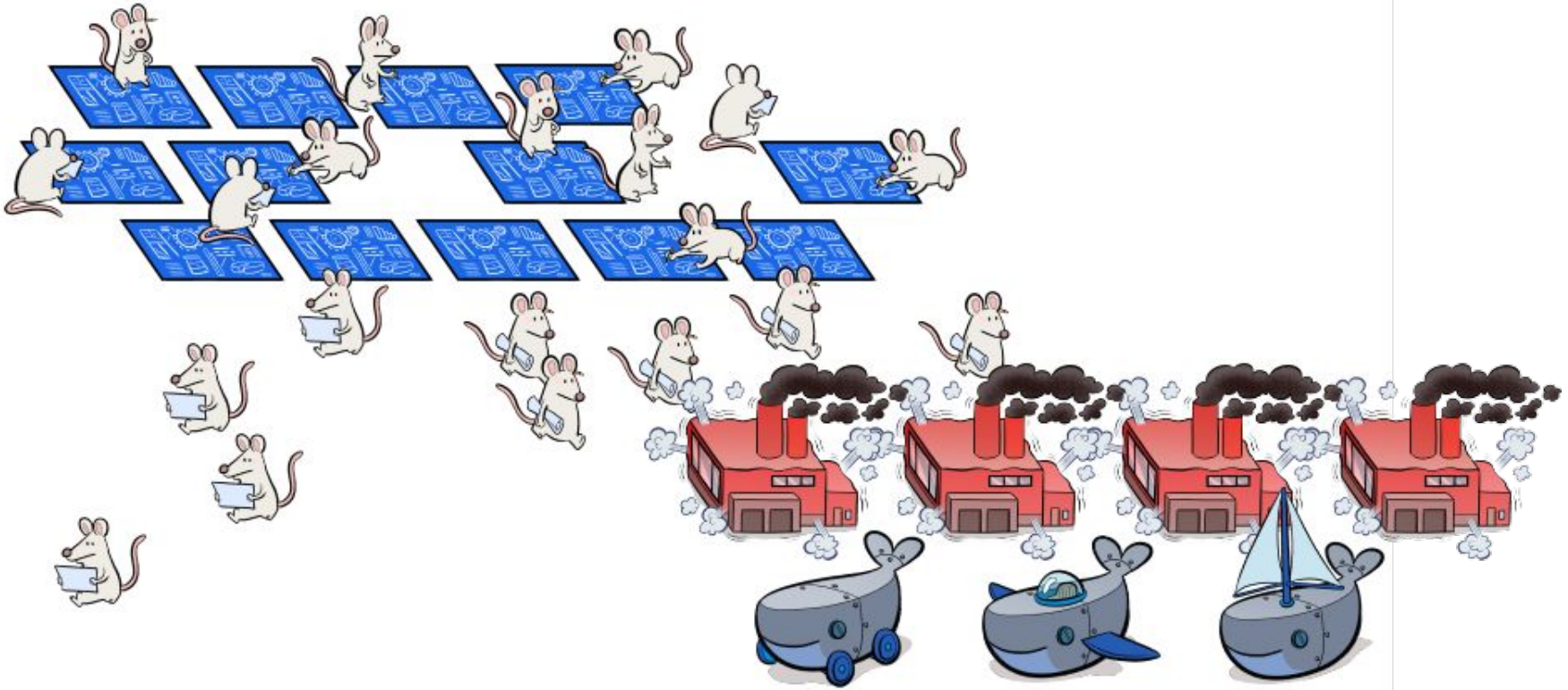
Production model: **Open components**



Docker is a platform made of components



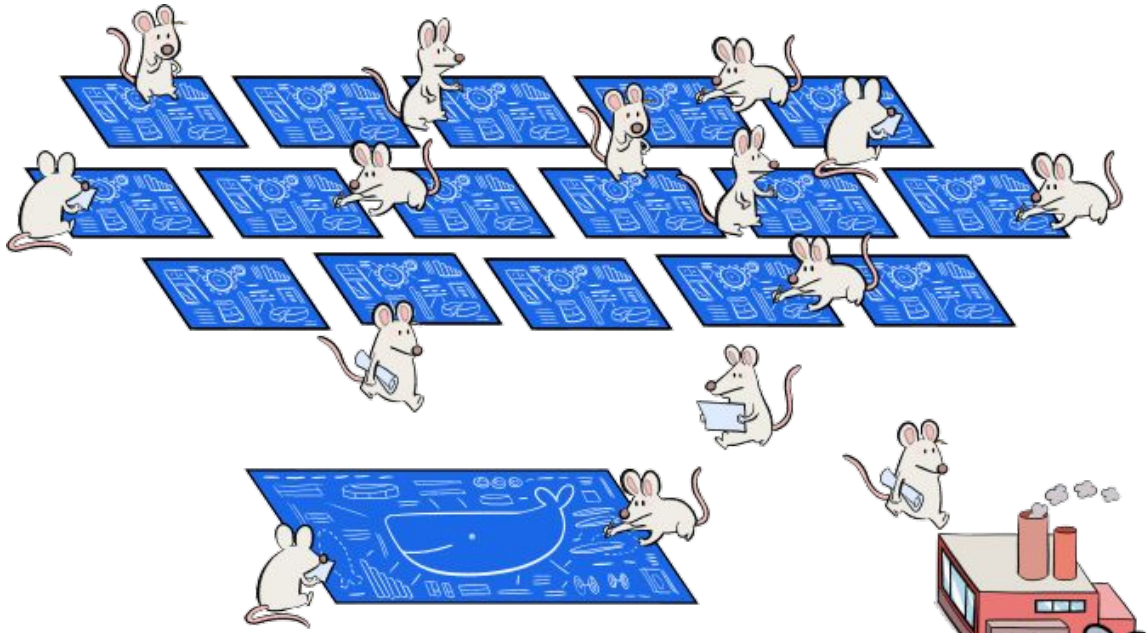
The open components model shows its limits...

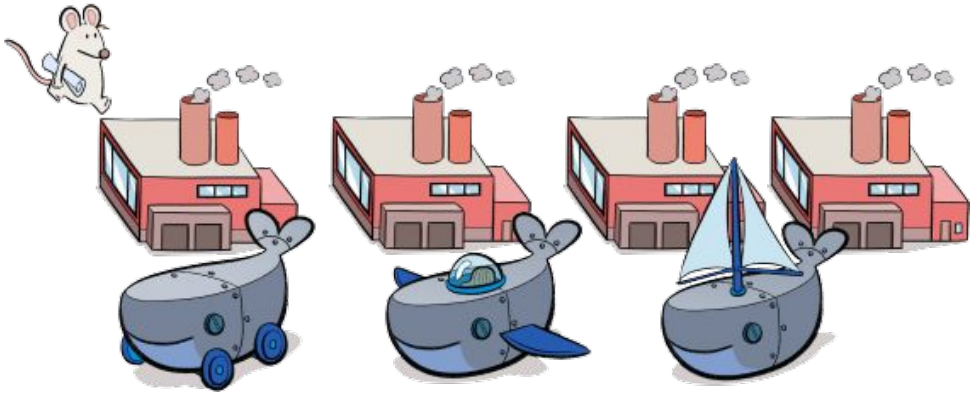


The auto industry has already solved this problem:
COMMON ASSEMBLIES

KIRATECH
WE DEVOPS IT

Next level: **Collaborating on components and Assemblies**

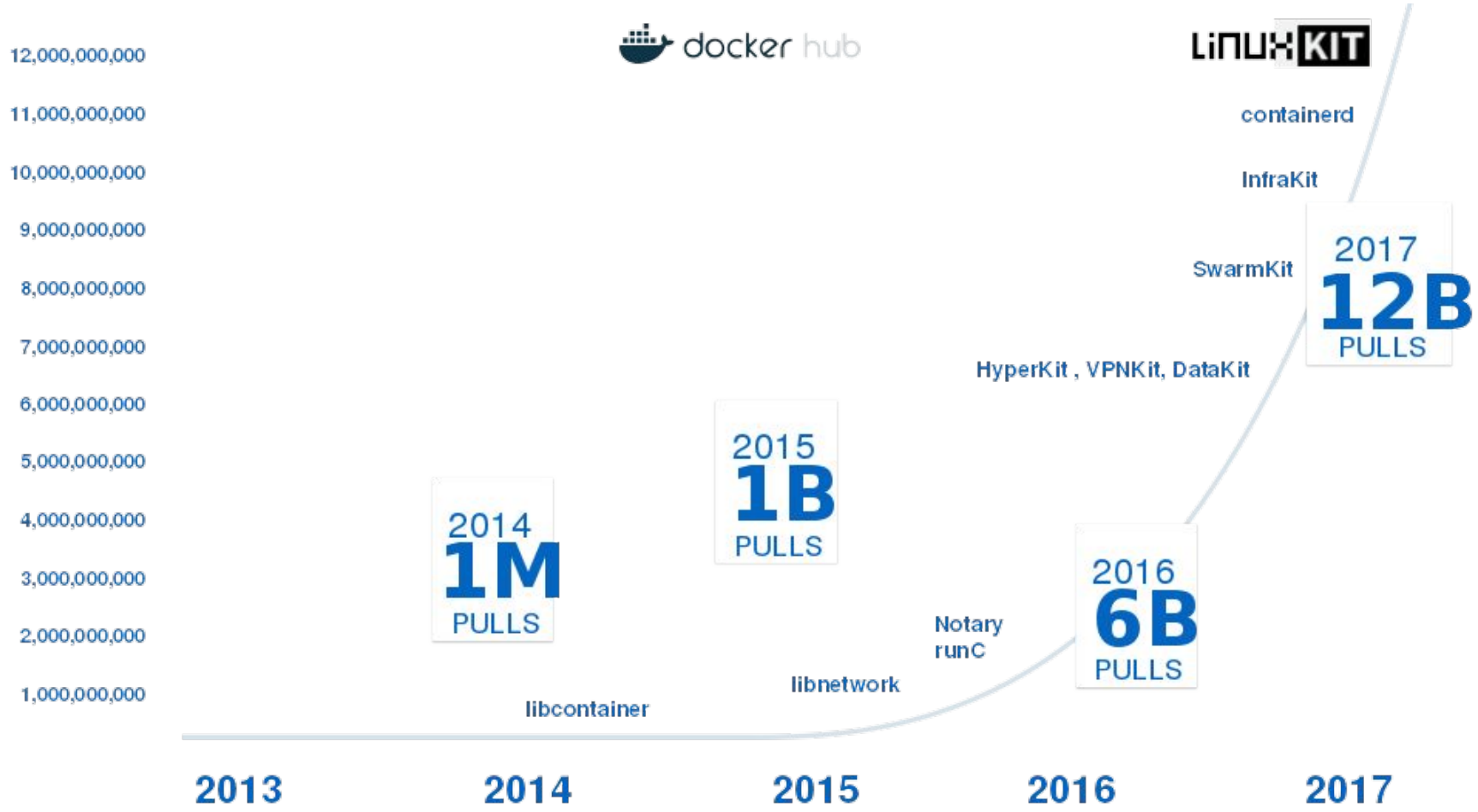




“With going mainstream comes **great responsibilities**„

— Solomon Hykes


The world needs
tools of mass
innovation



KIRATECH
WE DEVOPS IT

“A framework to assemble specialized container systems without reinventing the wheel”

- Library of 80+ components
- Package your own components as containers
- Reference assemblies deployed on millions of nodes
- Create your own assemblies or start from existing ones

KIRATECH
WE DEVOPS IT

What Moby means for you as a:

DOCKER USER

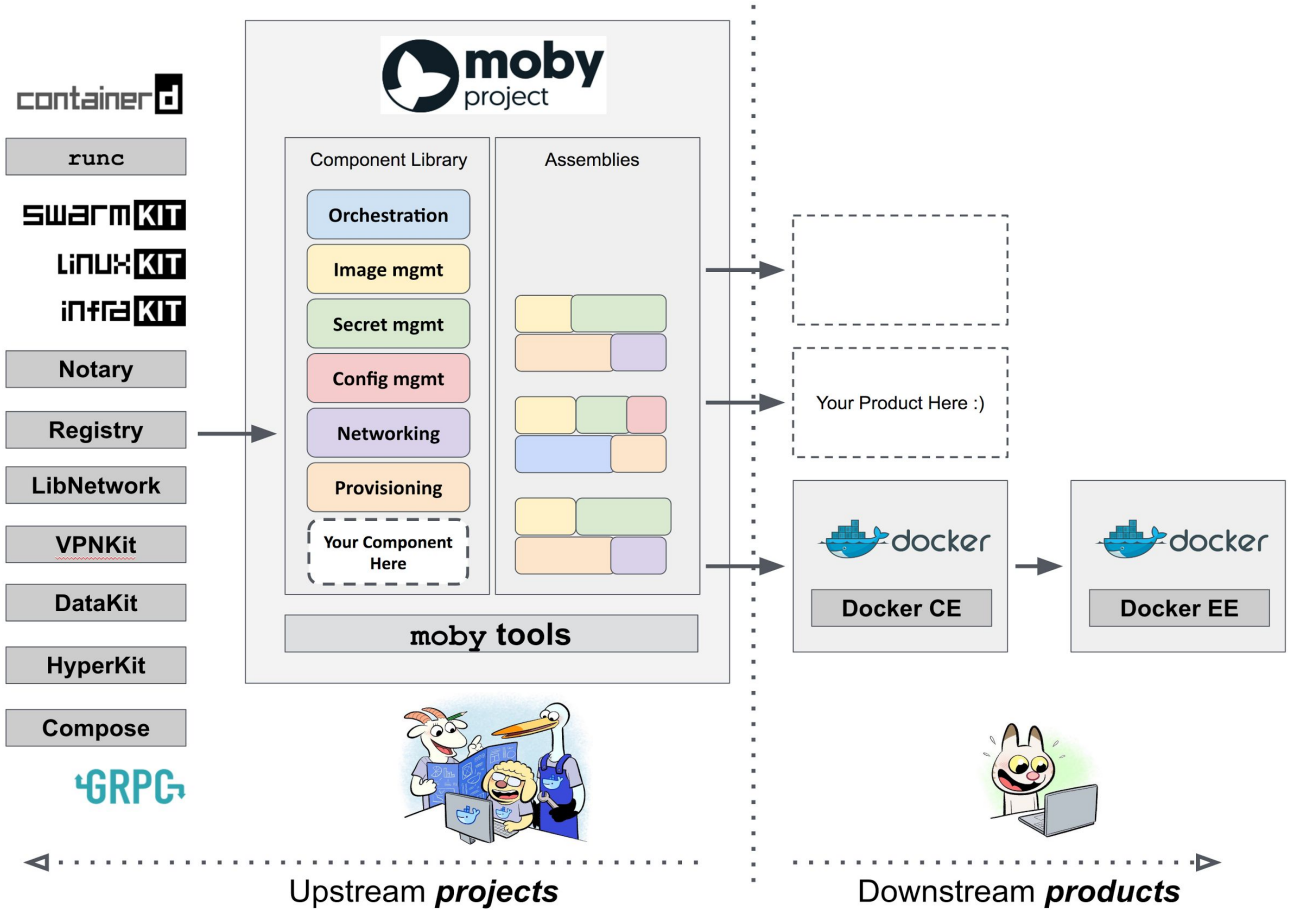
Nothing changes for you, your command line remains the same and also anything else.

It’s just that now Docker can leverage the ecosystem to innovate faster for you

SYSTEM BUILDER

Moby helps you to innovate without tying you to Docker

“The **Moby Project** is to Docker what **Fedora** is to Red Hat Enterprise Linux„



KIRATECH
WE DEVOPS IT

Future plans

- Moby **IS NOT** going to be donated to an **external organization**
- **Moby** will develop a community-driven governance model inspired by **Fedora**
- As **LinuxKit** `outputs` we will have also **deb** and **rpm**

Thank you!

containerday

#containerDay2017

https://fntlnz.wtf

lo@linux.com

@fntlnz