Shift Left Security: What, Why & How

Matthew Barker, Solution Architect, Twistlock

What we're covering today:

- What is shift-left security?
- Why is it important?
- How do you enable it?
- Q & A

Software is eating the world

- Every org is becoming a software org
- Software orgs need modern tools
- DevOps, containers, and cloud native are those tools

The world is dangerous

- ‘Democratization’ of sophisticated attacks
- Security teams and SOCs overloaded
- Your own software is the softest target

Only 20% of organizations following DevOps practices consistently integrate security into the development process.

Source: HPE | True State of Application Security & DevOps

Only 15% of organizations can remediate security vulnerabilities or address compliance violations as they arise.

Source: Chef | 2017 Community Survey

Shift Left Security

Moving security practices left into the software development lifecycle with the goal of shifting from a reactive to a proactive security posture

Simple concept – difficult execution.

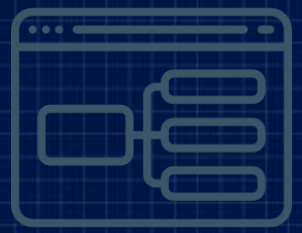
- Traditional security practices are manual and time-consuming
- Developers and security have very different domain expertise
- Security tooling doesn’t surface information in a dev-friendly fashion

1. Security by design – establish criteria up front
2. Automate, automate, automate
3. Control gates are your friend
4. Share tooling – don’t silo information
5. Use dev learns for better production protection

Containers empower security teams to shift left more successfully than traditional architectures

Minimal

Typically single process entities



Declarative

Built from images that are machine readable

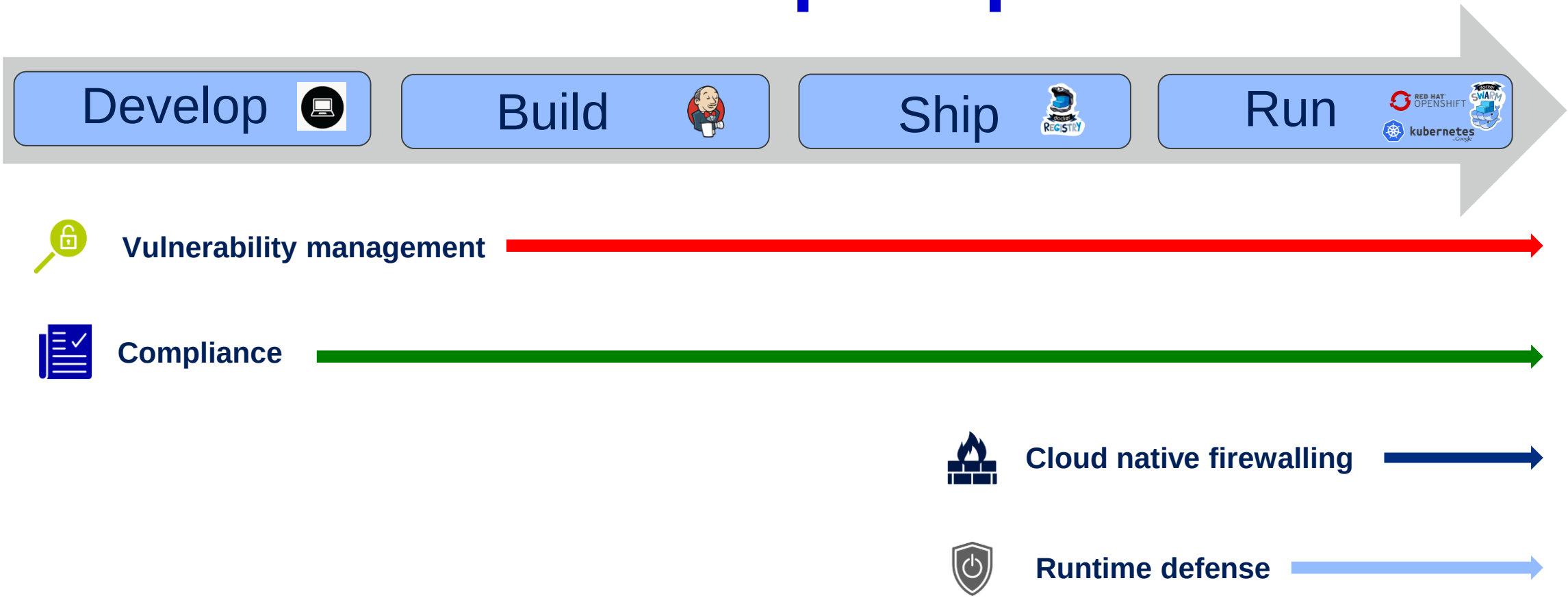
Predictable

Do exactly the same thing from **`run`** to **`kill`** **`(immutable)`**

1. The minimal nature simplifies security requirements for each artifact
2. The declarative nature allows automated analysis of vulnerabilities and compliance
3. The predictable nature simplifies automation of policy creation and enforcement

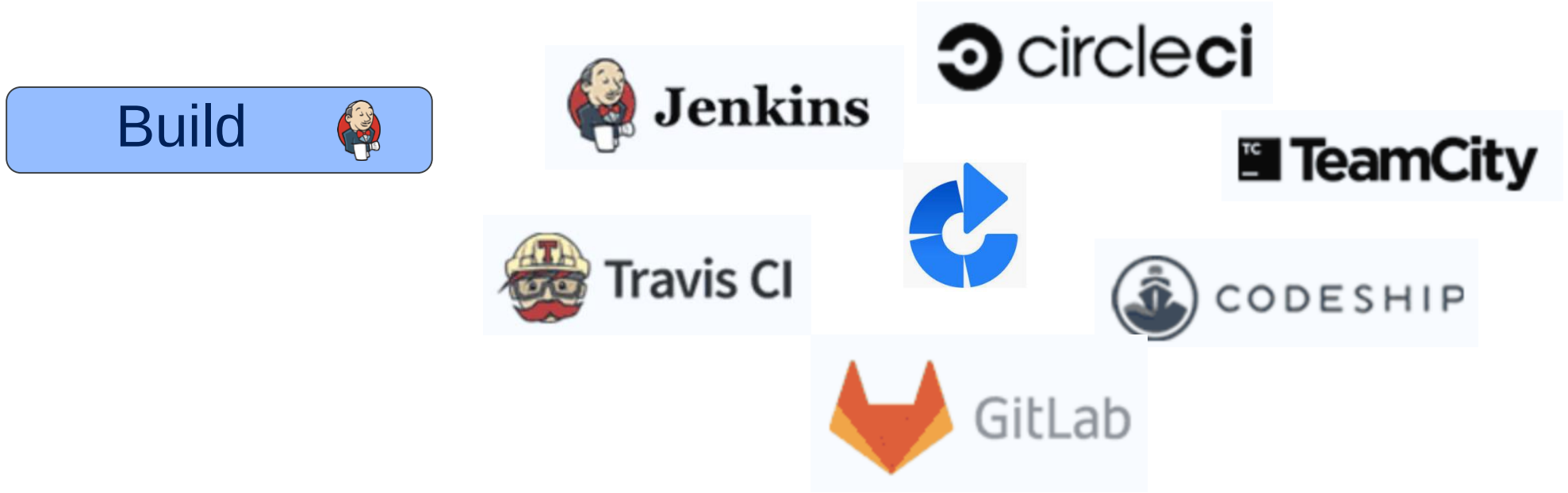
1. Security by design – establish criteria up front
2. Automate, automate, automate
3. Control gates are your friend
4. Share tooling – don’t silo information
5. Use dev learns for better production protection

Twistlock Enables Shift Left + Across Entire Devops Pipeline



Develop

- FAR Left Shift (on developer desktop)
  - Enable vulnerability and compliance checks for base images
    - particularly when pulled from public repositories
  - Developers also scan their custom image
  - Remediate security and compliance issues ***before*** code check in
  - Developers integrate security into build



- Left Shift – In Build
  - Automate scan for vulnerabilities and compliance at build
  - Set thresholds and optionally fail the build
  - Continuously remediate security and compliance issues

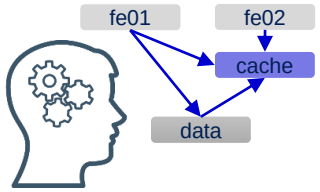
- Continuously monitor docker registries
  - Maintain a clean inventory of images
  - Alert when new vulnerable images are pushed to registry
  - Alert when new CVE’s are reported for images in registry
  - Enable trusted repositories

- Provide and active defense for your containerized work loads
- IDS
  - Containers and hosts
  - Protect against suspicious activities in following categories
    - process, network, file system, and system calls

Shift Left Shifts Protection Right

```
/var/cache/apt/archives/partial/*.deb /var/cache/apt/*.bi
echo 'Acquire::Languages "none";' > /etc/apt/apt.conf.d/d
RUN sed -i 's/^#\s*\(deb.*universe\$/\1/g' /etc/apt/sourc
CMD "/bin/bash"
RUN apt-get -y update && apt-get install -y git
RUN git clone https://github.com/moxiegirl/cowsay.git
WORKDIR /cowsay
RUN git reset --hard origin/master
RUN sh install.sh
ENV PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/u
RUN apt-get -y update && apt-get install -y fortunes
CMD "/bin/sh" "-c" "/usr/games/fortune -a | cowsay"
```

+



=

+

```
ip, category, score, first_seen,
last_seen, ports
74.88.8.7,31,65,2016-04-16,2016-
04-16,
23.16.9.49,35,125,2016-04-
11,2016-04-20,80
82.16.9.65,35,127,2016-04-
09,2016-04-21,80
```

=

Static analysis

Machine learning

Predictive model

Threat intelligence

Automated defense

Questions?

@twistlocklabs

@twistlockteam

matthew@twistlock.com

matthewabq twitter/linkedIn

Thank you