Software Security as a Force of Nature

Kelly Shortridge
@shortridge@hachyderm.io | @swagitda_ (twitter)

StaffPlus New York 2024

Do we want to deliver secure software?

shortridge@hachyderm.io | @swagitda_

Why is software security so difficult?

shortridge@hachyderm.io | @swagitda_

World is not nice.

shortridge@hachyderm.io | @swagitda_

- World is not nice
- Constant change
- Flaws are *so* common
- Maintenance is continuous
- Procedures don’t match conditions
- Production pressures unbalanced
- New hazards appearing

shortridge@hachyderm.io | @swagitda_

Software cyberorthodoxy assumes the world is nice: closed and linear. That's why it fails.

shortridge@hachyderm.io | @swagitda_

If world not nice, what do instead?

shortridge@hachyderm.io | @swagitda_

In nature, organisms thrive by pursuing a strategy we refer to as resilience.

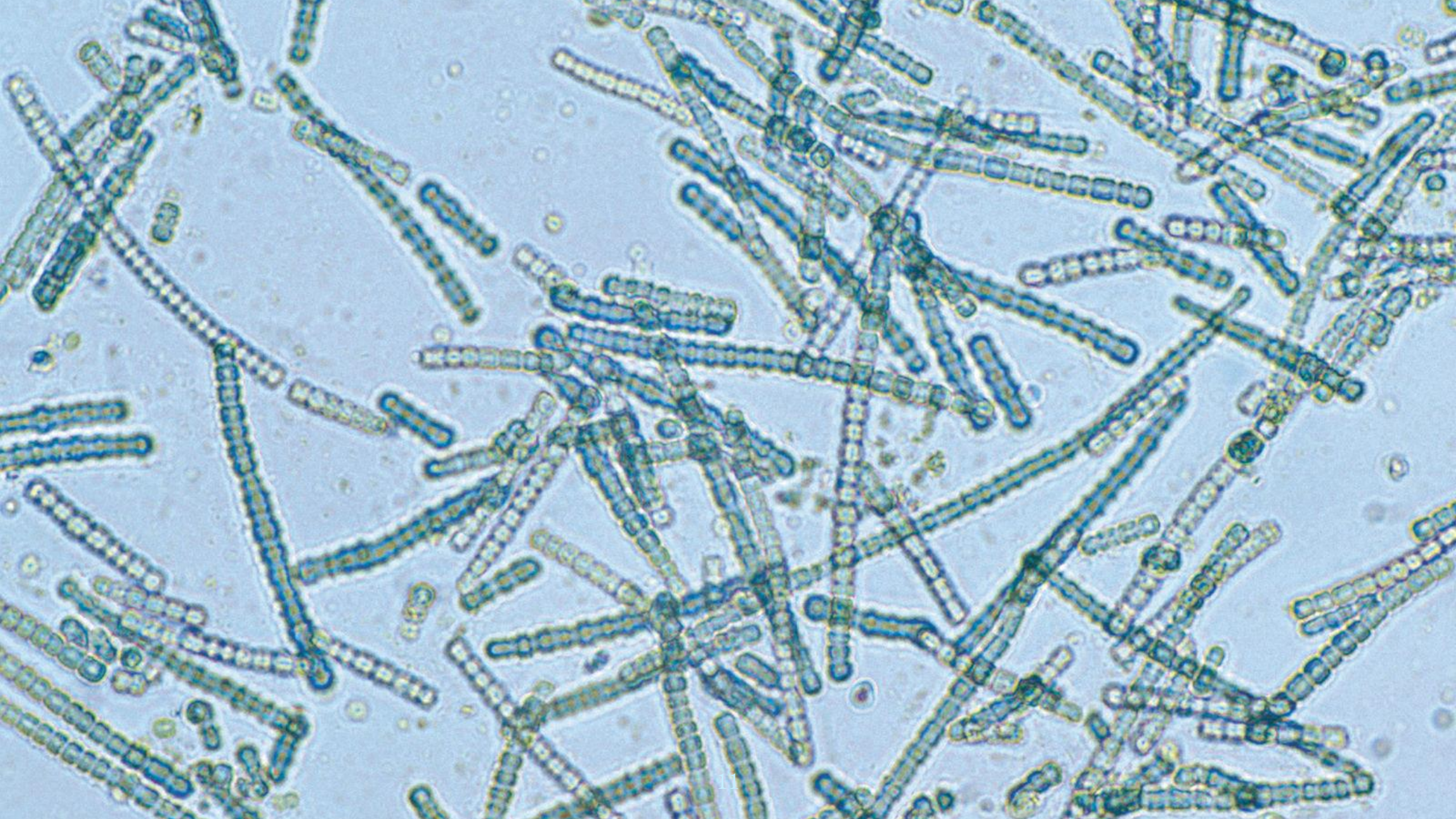
shortridge@hachyderm.io | @swagitda_

Our software has predators (attackers), too

shortridge@hachyderm.io | @swagitda_

Defensive adaptations in nature emerge from successful evasion; only the outcome matters

Source: Steve Harvey



Adaptation is emergent; software security changes should emerge from other initiatives

shortridge@hachyderm.io | @swagitda_

Let’s extend our patterns & practices to apply “natural” defenses to software...

shortridge@hachyderm.io | @swagitda_

Source: Taylor Chausky


© Shannon Guichon

In a similar fashion, we can repurpose automation like CI/CD and IaC for security.

shortridge@hachyderm.io | @swagitda_

With IaC, we generate the same environment every time for reliable & predictable services.

shortridge@hachyderm.io | @swagitda_

- faster incident response
- minimized misconfigurations
- faster patching + security changes
- minimized environmental drift
- catching vulnerable configs
- stronger change control

shortridge@hachyderm.io | @swagitda_

CI/CD enforces invariants: properties we want every time we build + deploy + deliver

shortridge@hachyderm.io | @swagitda_

“Services must communicate over TLS and validate remote certificates.”

shortridge@hachyderm.io | @swagitda_

“Only images built by our CI/CD system may run on the production Kubernetes cluster.”

shortridge@hachyderm.io | @swagitda_

Source: Julian @PhotasticLab

Caching more content makes us more resilient to Layer 7 DDoS attacks

shortridge@hachyderm.io | @swagitda_

Source: Andrey Tikhonovskiy

We can make our systems immutable as a form of temporal amputation (ie isolation).

shortridge@hachyderm.io | @swagitda_

Time-based access tokens are another form of temporal isolation that frustrates attackers

shortridge@hachyderm.io | @swagitda_


Life quite literally emerged due to isolation.

Nature was the original architect of nested isolation, long before we made the transistor.

shortridge@hachyderm.io | @swagitda_

Sources: ANIRUDH; Kate Storey & Marios Stavridis (Wellcome Collection); Robina Weermeijer; Joe Green; Guillermo Ferla

Modularity is a system property reflecting the degree components can be decoupled.

shortridge@hachyderm.io | @swagitda_

Allows distinct parts to retain autonomy during stress & easier recovery from loss

shortridge@hachyderm.io | @swagitda_

Source: UNESCO

We should similarly treat modularity and isolation as essential for software.

shortridge@hachyderm.io | @swagitda_

Isolation is an invisible foundation of your lives as software engineers.

shortridge@hachyderm.io | @swagitda_

We want to make security invisible, too.

shortridge@hachyderm.io | @swagitda_

In nature, adaptation does not involve reinventing from scratch; it involves iteration using common components.

Source: National Cancer Institute

We can standardize middleware like authN so we don’t have to think about it.

shortridge@hachyderm.io | @swagitda_

Source: Landon Martin

We must adopt deception in software more.

shortridge@hachyderm.io | @swagitda_

Agility and stamina help prey evade predators, like gazelles vs. cheetahs.

shortridge@hachyderm.io | @swagitda_

Source: Hu Chen (Unsplash)

We should keep software components small and nimble so they can “evade,” too

shortridge@hachyderm.io | @swagitda_

Source: Lorna Ladril

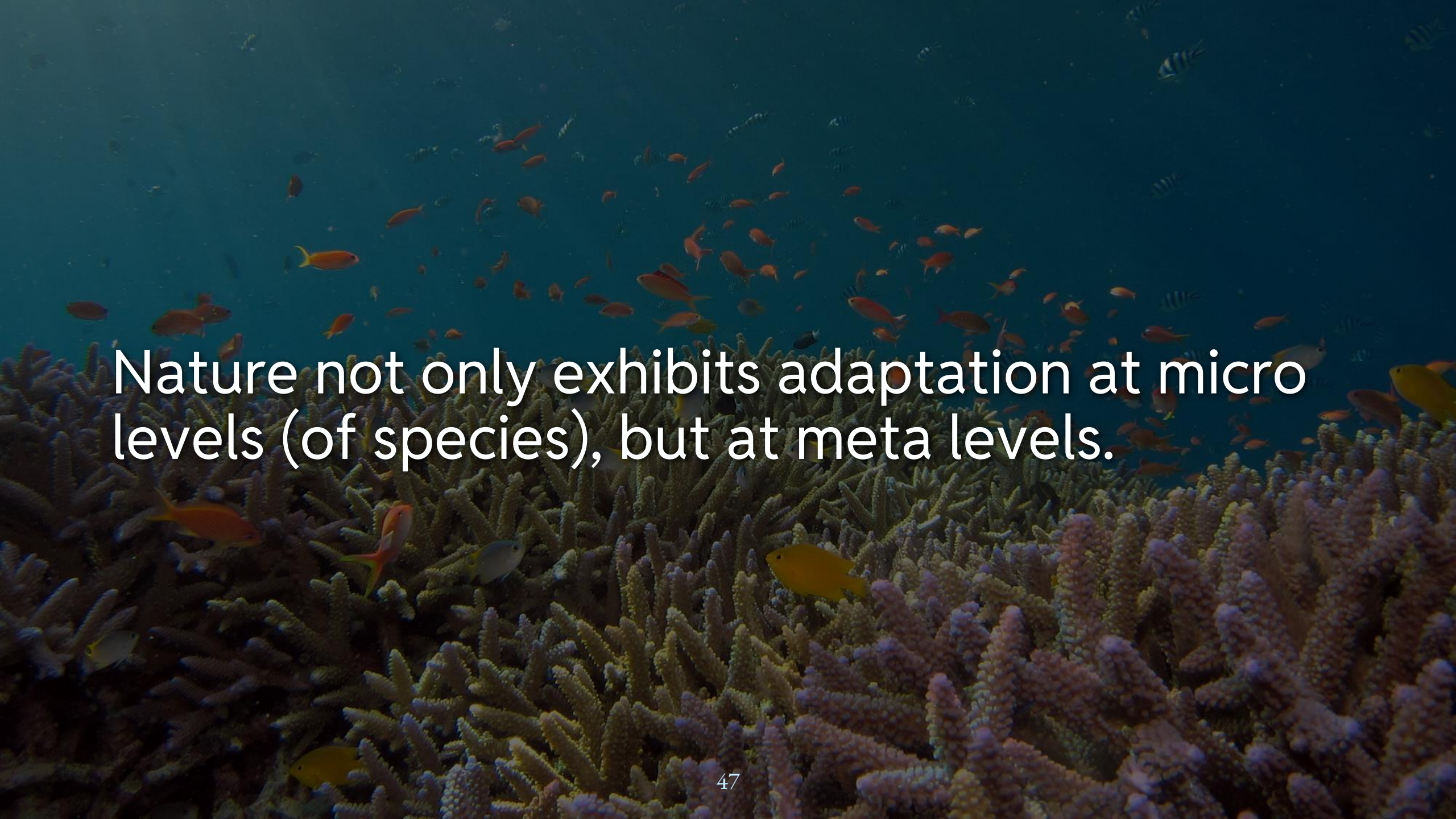
We should similarly use autoscaling against attackers for availability resilience.

shortridge@hachyderm.io | @swagitda_

Source: Shannon Potter

Adopting ephemerality similarly introduces unreliability against attackers.

shortridge@hachyderm.io | @swagitda_


Nature not only exhibits adaptation at micro levels (of species), but at meta levels.

Life is cyclic, not linear; we must replenish soil and deadhead blooms to nourish growth.

shortridge@hachyderm.io | @swagitda_

Our software must prepare for, recover from, and adapt to (corporate) cycles.

shortridge@hachyderm.io | @swagitda_

Functional diversity is a critical factor for resilience in ecological systems.

shortridge@hachyderm.io | @swagitda_

shortridge@hachyderm.io | @swagitda_


Flask
web development, one drop at a time
ANSIBLE
kafka
GitHub
Symfony
django
JUnit
redis
RAILS
OPENSHIFT
amazon S3
OpenSSL
Cryptography and SSL/TLS Toolkit
Couchbase
authentik
LOG4J
fastly
incident.io
APACHE HTTP SERVER PROJECT
Maven
MySQL
CHEF
replit
GitLab
Grafana
puppet
ClickHouse
spring
new relic
SALT PROJECT
HIVE
elastic
Kong
AWS CLOUDFORMATION
netlify
splunk>
NumPy
VMware Tanzu
Avro
Parquet
protobuf
Google Cloud Deployment Manager
cassandra
kubernetes
docker
Bamboo
fluentd
SQLite
Google Kubernetes Engine
presto
Amazon EKS
pandas
CLOUDFOUNDRY
Istio
HELM
gRPC
curl://
AXIOS
Terraform
envoy
DATADOG

Swappability is inherent in functional diversity (like blackbirds vs. thrashers).

shortridge@hachyderm.io | @swagitda_

We desperately need swappability (easy substitutions) in software systems.

shortridge@hachyderm.io | @swagitda_

Source: Traci O’Connor

Only collect data with a clear purpose.

shortridge@hachyderm.io | @swagitda_

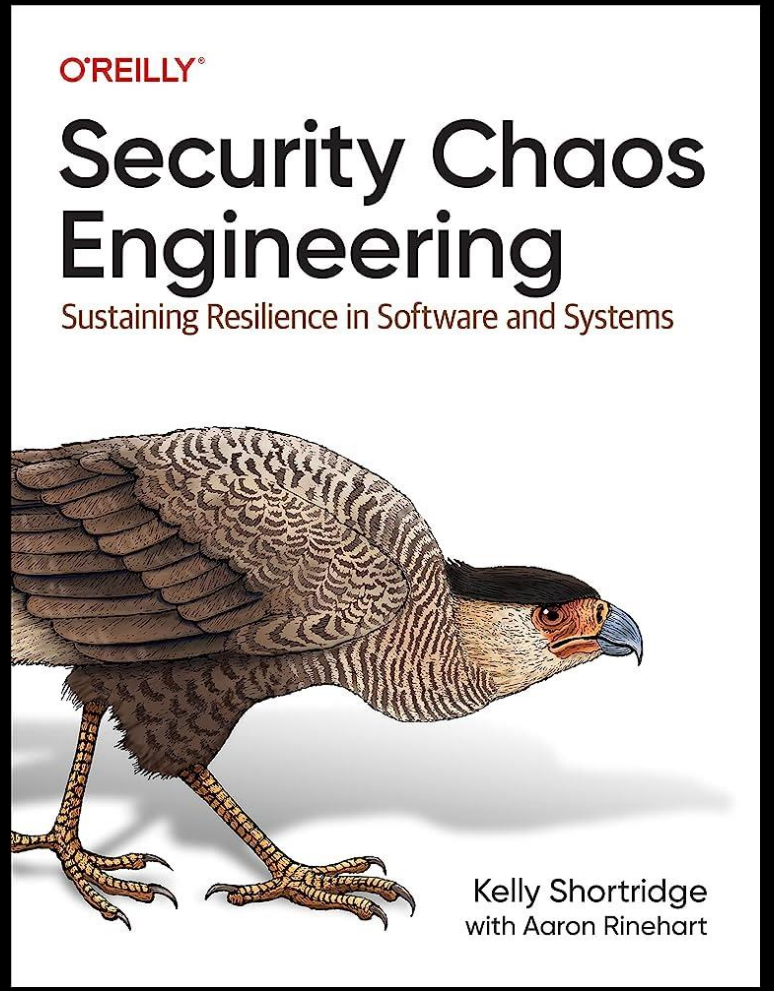
FD reflects true redundancy: the system has multiple paths to reach a goal outcome.

shortridge@hachyderm.io | @swagitda_

Life, uh, finds a way. And we can, too.

shortridge@hachyderm.io | @swagitda_

Order the book today:
Amazon
Bookshop
& other major retailers



shortridge@hachyderm.io | @swagitda_

/in/kellyshortridge

@swagitda_

shortridge@hachyderm.io

@shortridge.bsky.social

chat@shortridge.io