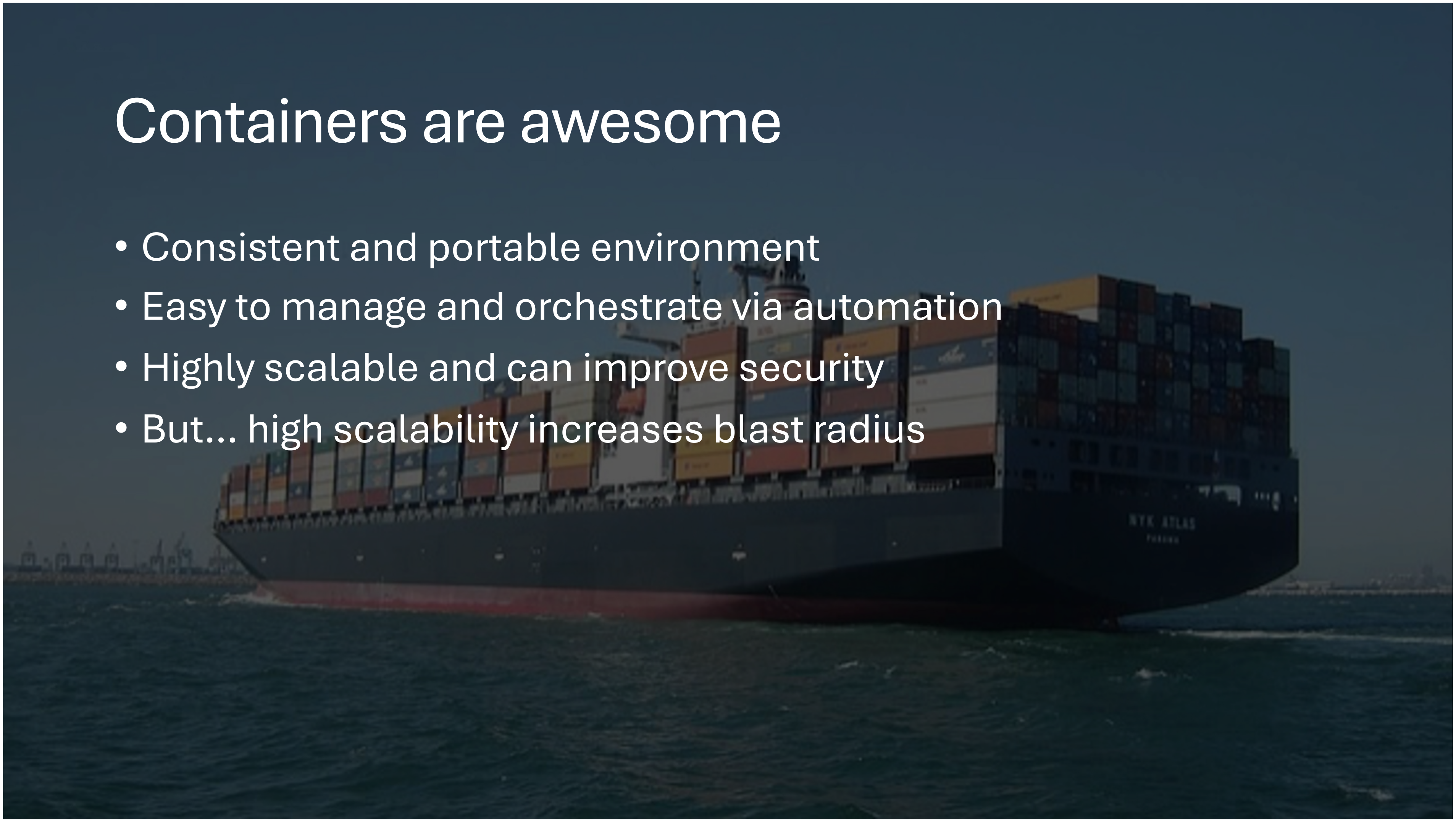
Strengthening the Secure Supply Chain with Open-Source Tools

Paul Yu

Developer Advocate

Microsoft

@pauldotyu | /in/yupaul

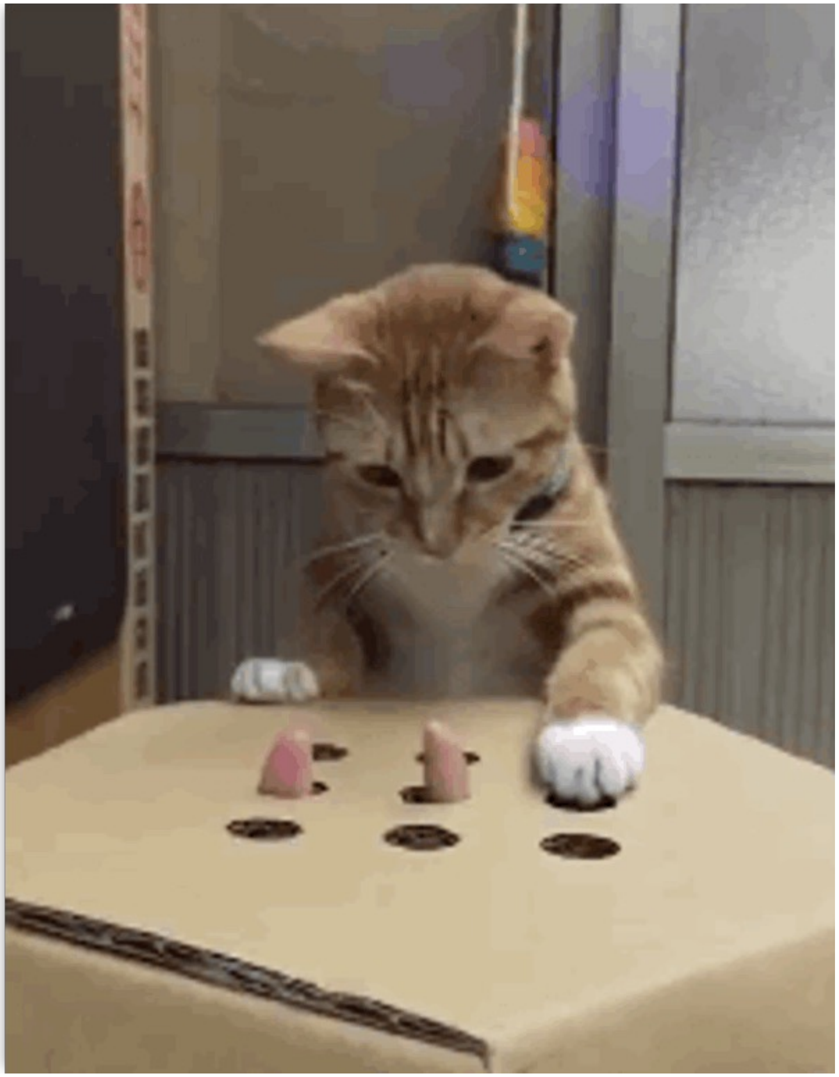


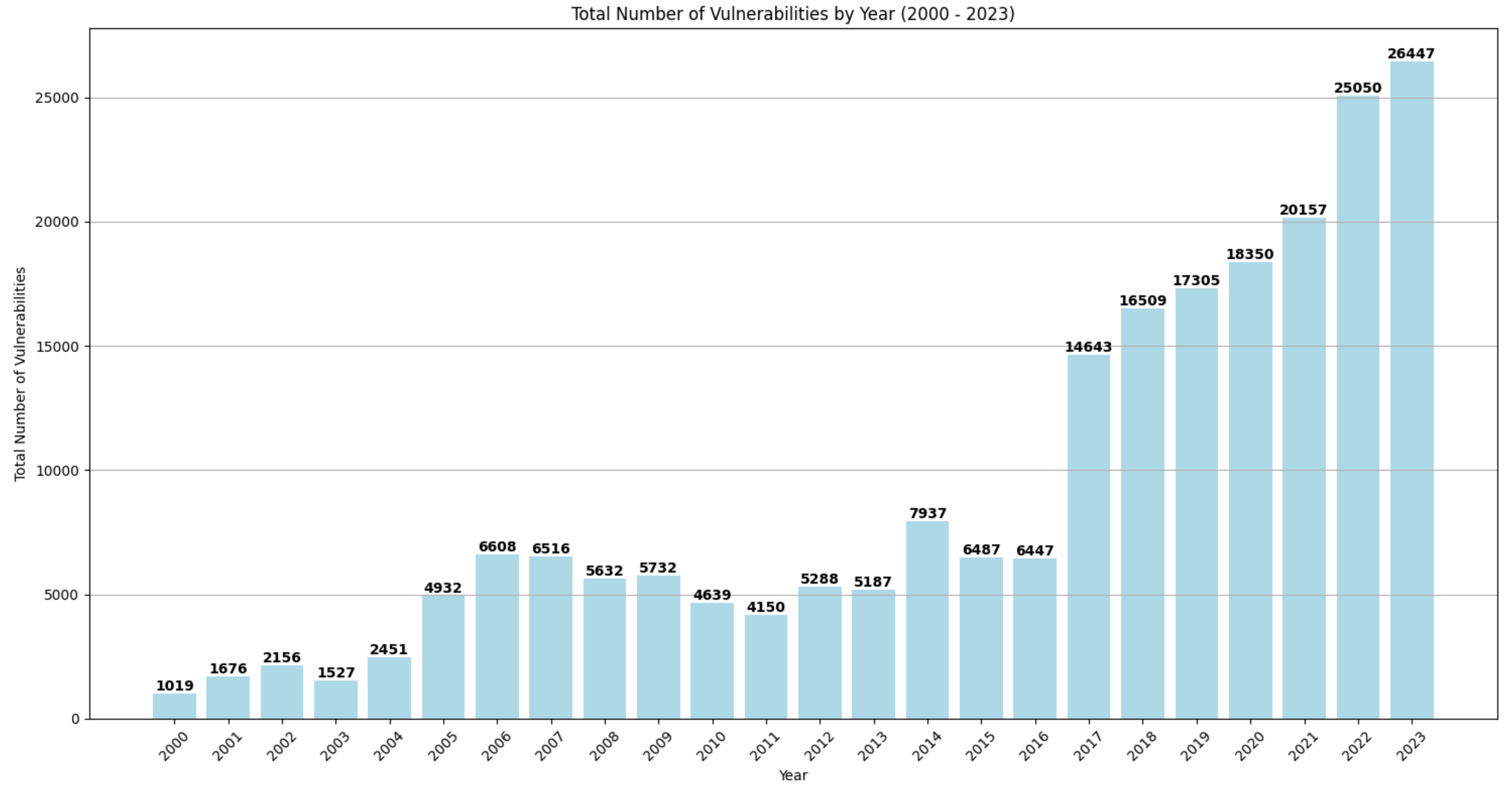
Containers are awesome

- Consistent and portable environment
- Easy to manage and orchestrate via automation
- Highly scalable and can improve security
- But… high scalability increases blast radius

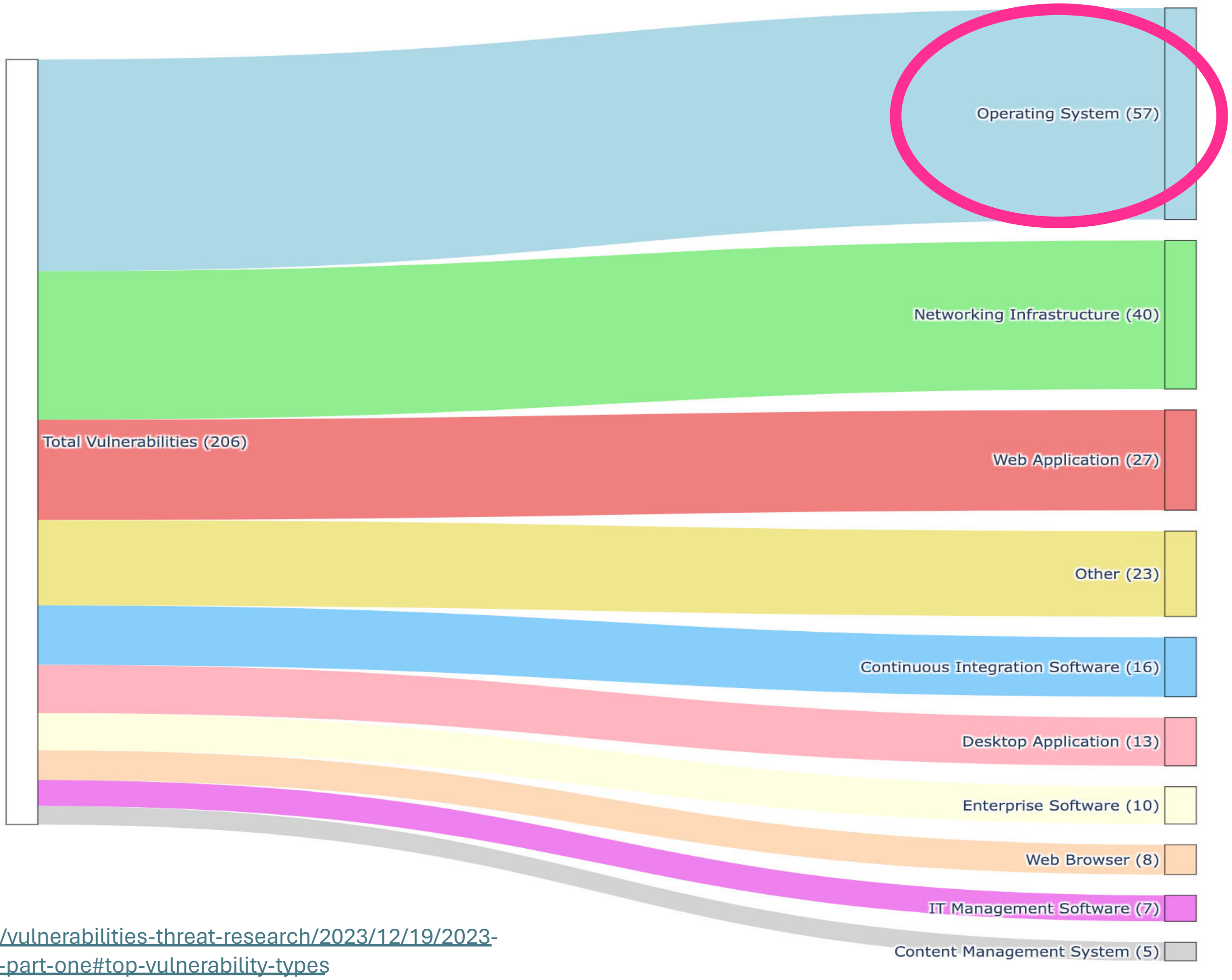
Security vulnerabilities galore

- 50+ CVEs reported daily
- Never ending game of whack-a-mole

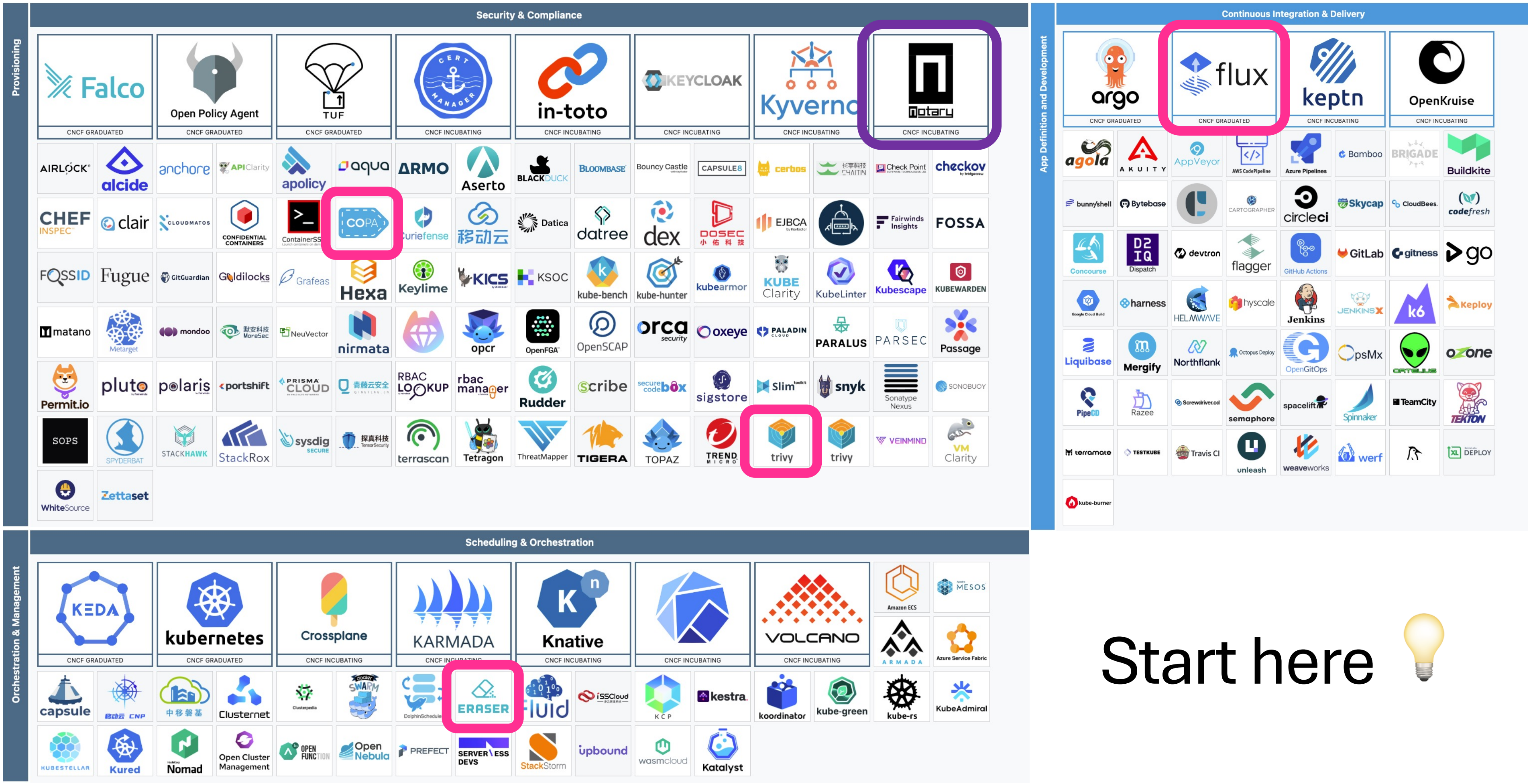




Source: https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one



Source: https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one#top-vulnerability-types


Provisioning
Security & Compliance
Falco
CNCF GRADUATED
Open Policy Agent
CNCF GRADUATED
TUF
CNCF GRADUATED
CERT MANAGER
CNCF INCUBATING
in-toto
CNCF INCUBATING
KEYCLOAK
CNCF INCUBATING
Kyverno
CNCF INCUBATING
notary
CNCF INCUBATING
AIRLOCK
alcide
anchore
APIClarity
apolicy
aqua
ARMO
Aserto
BLACKDUCK
BLOOMBASE
Bouncy Castle
CAPSULE8
cerbos
Check Point
checkov
CHEF INSPEC
clair
CLOUDMATOS
CONFIDENTIAL CONTAINERS
ContainerSSH
COPA
curiefense
Datica
datree
dex
DOSEC
EJBCA
Fairwinds Insights
FOSSA
FOSSID
Fugue
GitGuardian
Goldilocks
Grafeas
Hexa
Keylime
KICS
KSOC
kube-bench
kube-hunter
kubearmor
KUBE Clarity
KubeLinter
Kubescape
KUBEWARDEN
matano
Metarget
mondoo
NeuVector
nirmata
opcr
OpenFGA
OpenSCAP
orca security
oxeye
PALADIN CLOUD
PARALUS
PARSEC
Passage
Permit.io
pluto
polaris
portshift
PRISMA CLOUD
RBAC LOOKUP
rbac manager
Rudder
scribe
secure codebox
sigstore
Slim toolkit
snyk
Sonatype Nexus
SONOBUOY
SOPS
SPYDERBAT
STACKHAWK
StackRox
sysdig SECURE
terrascan
Tetragon
ThreatMapper
TIGERA
TOPAZ
TREND MICRO
trivy
trivy
VEINMIND
VM Clarity
WhiteSource
Zettaset
App Definition and Development
Continuous Integration & Delivery
argo
CNCF GRADUATED
flux
CNCF GRADUATED
keptn
CNCF INCUBATING
OpenKruise
CNCF INCUBATING
agola
AKUITY
AppVeyor
AWS CodePipeline
Azure Pipelines
Bamboo
BRIGADE
Buildkite
bunnyshell
Bytebase
CARTOGRAPHER
circleci
Skycap
CloudBees
codefresh
Concourse
Dispatch
devtron
flagger
GitHub Actions
GitLab
gitness
go
Google Cloud Build
harness
HELMWAVE
hyscale
Jenkins
JENKINS X
k6
Keploy
Liquibase
Mergify
Northflank
Octopus Deploy
OpenGitOps
OpsMx
ORTELIUS
ozone
PipeCD
Razee
Screwdriver.cd
semaphore
spacelift
Spinnaker
TeamCity
TEKTON
terramate
TESTKUBE
Travis CI
unleash
weaveworks
werf
XL DEPLOY
kube-burner
Orchestration & Management
Scheduling & Orchestration
KEDA
CNCF GRADUATED
kubernetes
CNCF GRADUATED
Crossplane
CNCF INCUBATING
KARMADA
CNCF INCUBATING
Knative
CNCF INCUBATING
CNCF INCUBATING
VOLCANO
CNCF INCUBATING
Amazon ECS
MESOS
ARMADA
Azure Service Fabric
capsule
CNP
中移磐基
Clusternet
Clusterpedia
docker SWARM
DolphinScheduler
ERASER
Fluid
iSSCloud
KCP
kestra
koordinator
kube-green
kube-rs
KubeAdmiral
KUBESTELLAR
Kured
Nomad
Open Cluster Management
OPEN FUNCTION
Open Nebula
PREFECT
SERVERLESS DEVS
StackStorm
upbound
wasmcloud
Katalyst

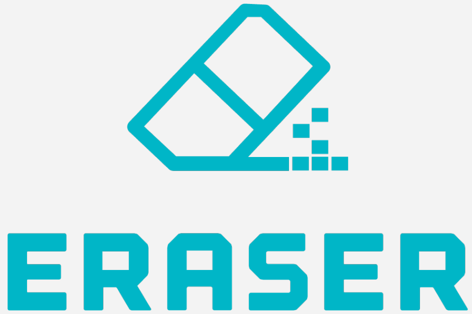
Start here 💡

GitHub Actions

- Continuous integration and continuous delivery platform
- Workflows trigger off an event
- Runners can be GitHub provided or self-hosted

Flux

- CNCF Graduated project (2022)
- Continuous delivery solution via GitOps
- Image update automation to detect and deploy new images



Eraser

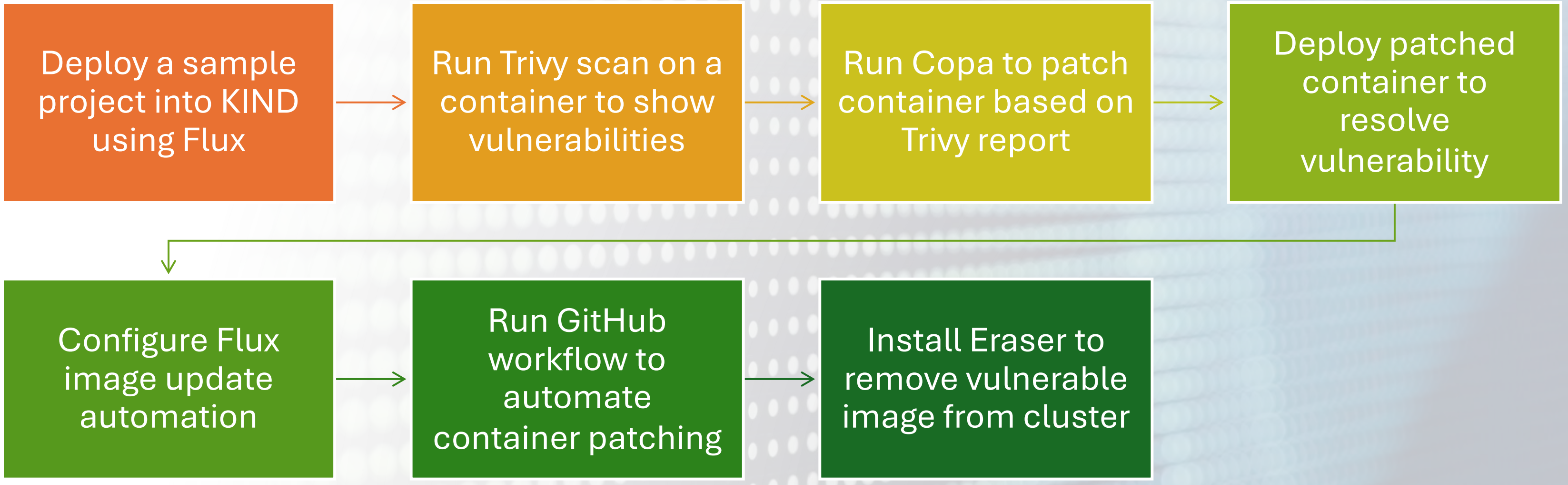
- CNCF Sandbox project (2023)
- Removes non-running images based on vulnerability scans
- Supports Trivy but can integrate with others

COPA

Project Copacetic

- CNCF Sandbox project (2023)
- Patch container images based on vulnerability scans
- Supports Trivy but can integrate with others

Demo



Deploy a sample project into KIND using Flux

Run Trivy scan on a container to show vulnerabilities

Run Copa to patch container based on Trivy report

Deploy patched container to resolve vulnerability

Configure Flux image update automation

Run GitHub workflow to automate container patching

Install Eraser to remove vulnerable image from cluster

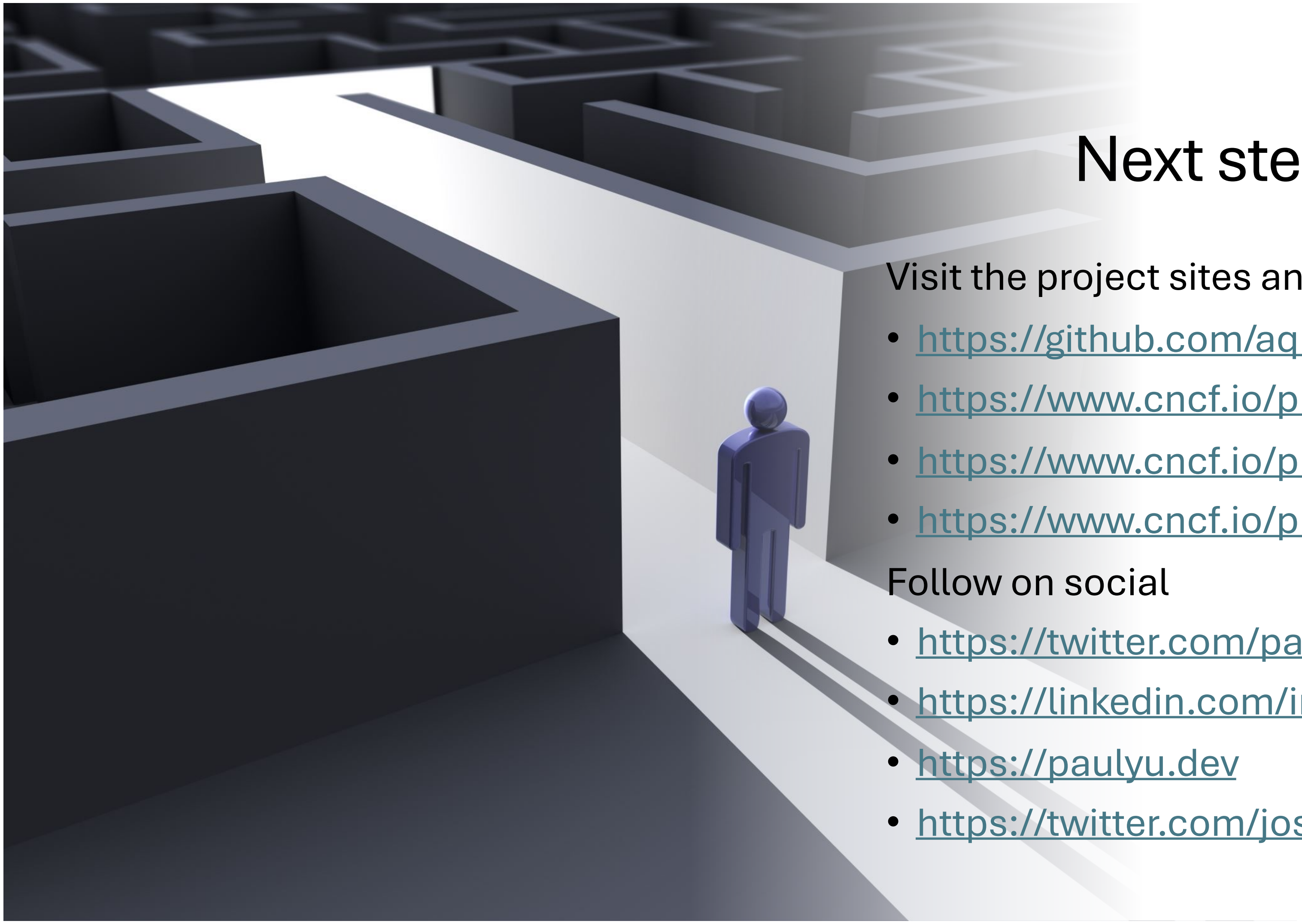
Summary

✓ Containers are the best thing since sliced bread

Keeping up with container security is challenging

Open-source tools can help to strengthen the secure supply chain

Supply chain security is just one aspect



Next steps

Visit the project sites and contribute

- https://github.com/aquasecurity/trivy
- https://www.cncf.io/projects/copa
- https://www.cncf.io/projects/flux
- https://www.cncf.io/projects/eraser

Follow on social

- https://twitter.com/pauldotyu
- https://linkedin.com/in/yupaul
- https://paulyu.dev
- https://twitter.com/joshduffney

https://aka.ms/cloudnative/JoinOSSDiscord