云原生安全30分钟导赏团

汇报人：Donald Liu, Developer Evangelist, CNCF

目录

CONTENTS

CNCF

who is CNCF? projects, TOC, Security TAG and Cloud Native Security Whitepaper

Kubernetes

training and certification helpful for deploying in production

CNCF Landscape

聚焦安全与合规性

CLOMonitor

how good a project is

OpenSSF

advance open source security for all

1

CNCF

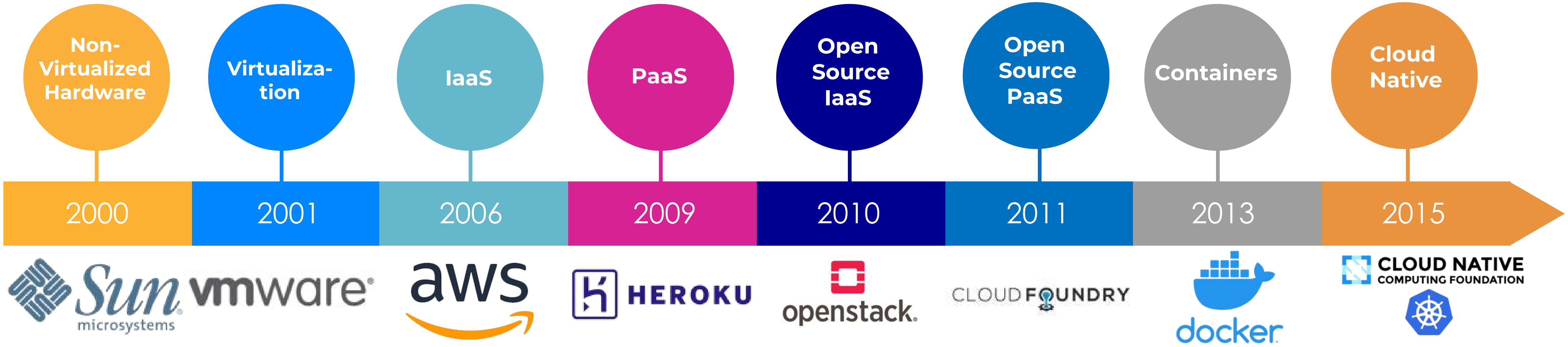
who is CNCF?

From Virtualization to Cloud Native

CLOUD NATIVE
COMPUTING FOUNDATION

kubernetes

- Cloud native computing uses an *open source software (OSS)* stack to:
  - segment applications into *microservices*,
  - package each part into its own *container*
  - and dynamically *orchestrate* those containers to optimize resource utilization



CNCF is part of the Linux Foundation

The Linux Foundation is much more than Linux today

Security

OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Networking

We are creating ecosystems around networking to improve agility in the evolving software-defined datacenter.

LF NETWORKING

Cloud

We are creating a portability layer for the cloud, driving de facto standards and developing the orchestration layer for all clouds.

CLOUD NATIVE COMPUTING FOUNDATION

Automotive

We are creating the platform for infotainment in the auto industry that can be expanded into instrument clusters and telematics systems.

AUTOMOTIVE GRADE LINUX

Blockchain

We are creating a permanent, secure distributed ledger that makes it easier to create cost-efficient, decentralized business networks.

HYPERLEDGER

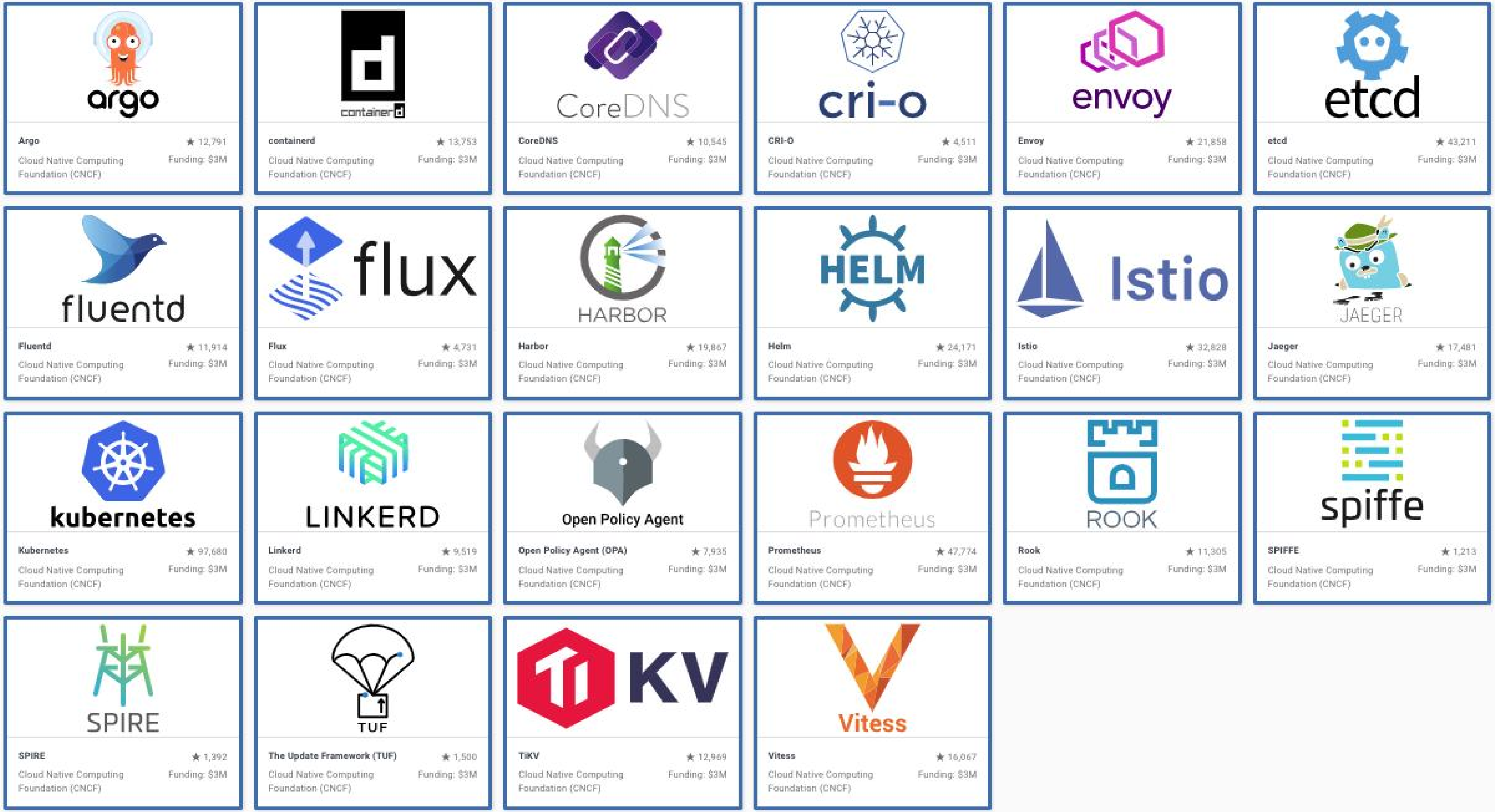
Web

Node.js and other projects are the application development framework for next generation web, mobile, serverless, and IoT applications.

OpenJS Foundation

We are regularly adding projects; for the most up-to-date listing of all projects visit tlfprojects.org

Graduated Projects (for your OSS stack consideration)



Argo ★ 12,791
Cloud Native Computing Foundation (CNCF) Funding: $3M

containerd ★ 13,753
Cloud Native Computing Foundation (CNCF) Funding: $3M

CoreDNS ★ 10,545
Cloud Native Computing Foundation (CNCF) Funding: $3M

CRI-O ★ 4,511
Cloud Native Computing Foundation (CNCF) Funding: $3M

Envoy ★ 21,858
Cloud Native Computing Foundation (CNCF) Funding: $3M

etcd ★ 43,211
Cloud Native Computing Foundation (CNCF) Funding: $3M

Fluentd ★ 11,914
Cloud Native Computing Foundation (CNCF) Funding: $3M

Flux ★ 4,731
Cloud Native Computing Foundation (CNCF) Funding: $3M

Harbor ★ 19,867
Cloud Native Computing Foundation (CNCF) Funding: $3M

Helm ★ 24,171
Cloud Native Computing Foundation (CNCF) Funding: $3M

Istio ★ 32,828
Cloud Native Computing Foundation (CNCF) Funding: $3M

Jaeger ★ 17,481
Cloud Native Computing Foundation (CNCF) Funding: $3M

Kubernetes ★ 97,680
Cloud Native Computing Foundation (CNCF) Funding: $3M

Linkerd ★ 9,519
Cloud Native Computing Foundation (CNCF) Funding: $3M

Open Policy Agent (OPA) ★ 7,935
Cloud Native Computing Foundation (CNCF) Funding: $3M

Prometheus ★ 47,774
Cloud Native Computing Foundation (CNCF) Funding: $3M

Rook ★ 11,305
Cloud Native Computing Foundation (CNCF) Funding: $3M

SPIFFE ★ 1,213
Cloud Native Computing Foundation (CNCF) Funding: $3M

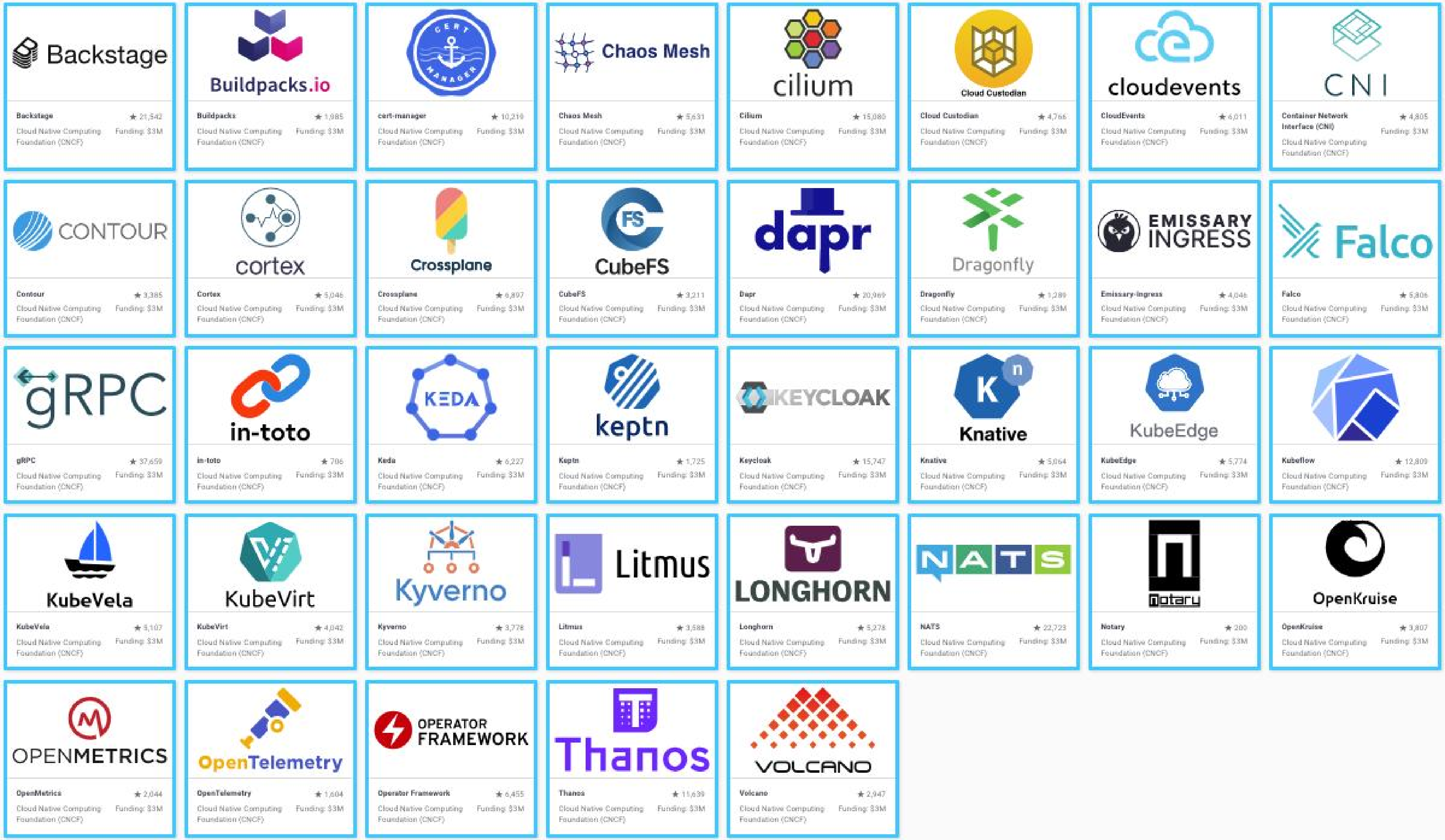
SPIRE ★ 1,392
Cloud Native Computing Foundation (CNCF) Funding: $3M

The Update Framework (TUF) ★ 1,500
Cloud Native Computing Foundation (CNCF) Funding: $3M

TiKV ★ 12,969
Cloud Native Computing Foundation (CNCF) Funding: $3M

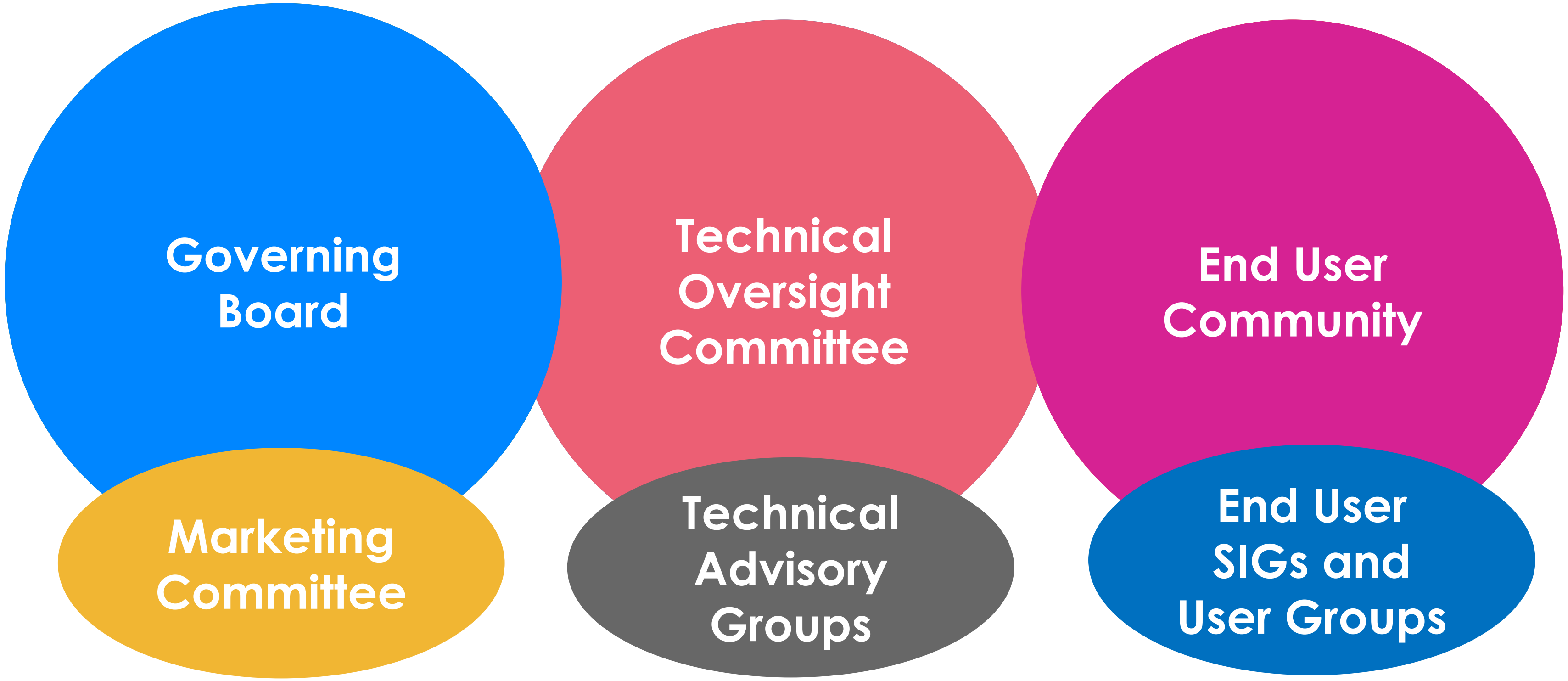
Vitess ★ 16,067
Cloud Native Computing Foundation (CNCF) Funding: $3M

Incubating Projects (for your OSS stack consideration)



Backstage	★ 21,542	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Buildpacks	★ 1,085	Cloud Native Computing Foundation (CNCF)	Funding: $3M
cert-manager	★ 10,210	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Chaos Mesh	★ 5,631	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Cilium	★ 15,080	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Cloud Custodian	★ 4,766	Cloud Native Computing Foundation (CNCF)	Funding: $3M
CloudEvents	★ 6,011	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Container Network Interface (CNI)	★ 4,805	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Contour	★ 3,385	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Cortex	★ 5,046	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Crossplane	★ 6,897	Cloud Native Computing Foundation (CNCF)	Funding: $3M
CubeFS	★ 3,211	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Dapr	★ 20,969	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Dragonfly	★ 1,289	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Emissary-Ingress	★ 4,046	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Falco	★ 5,806	Cloud Native Computing Foundation (CNCF)	Funding: $3M
gRPC	★ 37,659	Cloud Native Computing Foundation (CNCF)	Funding: $3M
in-toto	★ 706	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Keda	★ 6,227	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Keptn	★ 1,725	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Keycloak	★ 15,747	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Knative	★ 5,064	Cloud Native Computing Foundation (CNCF)	Funding: $3M
KubeEdge	★ 5,774	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Kubeflow	★ 12,809	Cloud Native Computing Foundation (CNCF)	Funding: $3M
KubeVela	★ 5,107	Cloud Native Computing Foundation (CNCF)	Funding: $3M
KubeVirt	★ 4,042	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Kyverno	★ 3,778	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Litmus	★ 3,588	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Longhorn	★ 5,278	Cloud Native Computing Foundation (CNCF)	Funding: $3M
NATS	★ 22,723	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Notary	★ 200	Cloud Native Computing Foundation (CNCF)	Funding: $3M
OpenKruise	★ 3,807	Cloud Native Computing Foundation (CNCF)	Funding: $3M
OpenMetrics	★ 2,044	Cloud Native Computing Foundation (CNCF)	Funding: $3M
OpenTelemetry	★ 1,604	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Operator Framework	★ 6,455	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Thanos	★ 11,639	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Volcano	★ 2,947	Cloud Native Computing Foundation (CNCF)	Funding: $3M

CNCF Structure



Governing Board

Marketing Committee

Technical Oversight Committee

Technical Advisory Groups

End User Community

End User SIGs and User Groups

- Mainly vendors
- Fund the organization
- Marketing and strategic direction

- 11 top technical architects
- Admit new projects
- Acts as a resource to projects

- Real end users of the technologies
- Communicate back requirements
- and good and bad experiences

CNCF Security Technical Advisory Group

secure access, policy control, privacy, auditing, explainability and more!

- The CNCF Security Technical Advisory Group facilitates collaboration to discover and produce resources that enable secure access, policy control, and safety for operators, administrators, developers, and end-users across the cloud native ecosystem.
- TAG Security Publications (examples)
  - Cloud Native Security Whitepaper: ensure the cloud native community has access to information about building, distributing, deploying, and running secure cloud native capabilities.
  - Supply Chain Security
    - Software Supply Chain Best Practices
      - ensure the cloud native community has access to information about building, distributing, deploying, and running secure software supply chains.
    - Evaluating your supply chain security
      - A framework for supply chain evaluation
    - Secure Software Factory
      - A reference architecture for securing the software supply chain
  - Use Cases & Personas: enable secure access, policy control and safety for users of cloud native technology

Cloud Native Security Whitepaper

Application lifecycle with 4 continuous phases

- Develop
  - Cloud native tools are meant to introduce security early in the application lifecycle.
- Distrbute
  - Software supply chain safety is especially critical in models that enable faster software iteration.
- Deploy
  - Deploy time checks provide the last chance to validate, correct, enforce these checks before the workload starts running to serve its intended business needs.
- Runtime Environment
  - e.g. hardware, host, operating system, network, storage, container image runtime, orchestration.

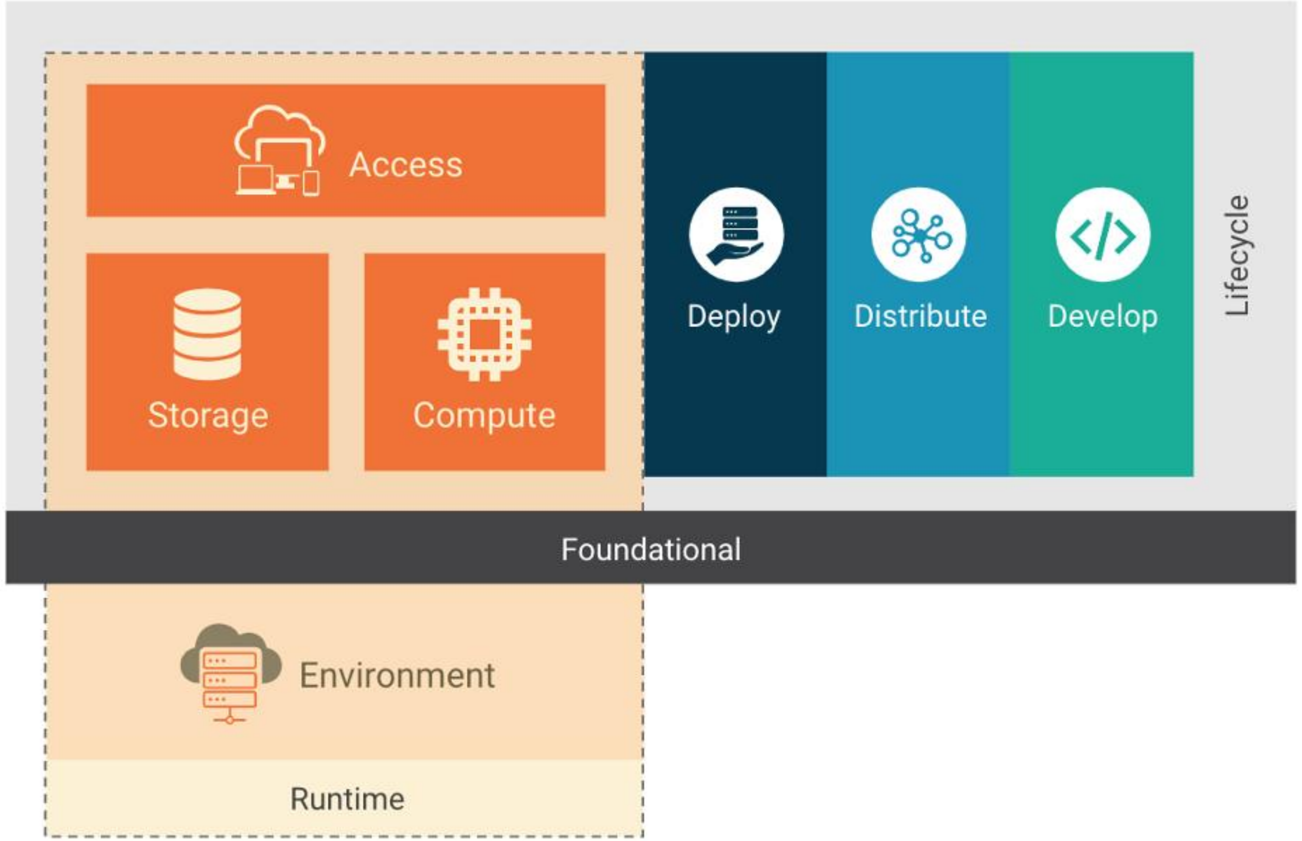


Figure 1: Cloud Native Layers, Cloud Native Security Whitepaper

2

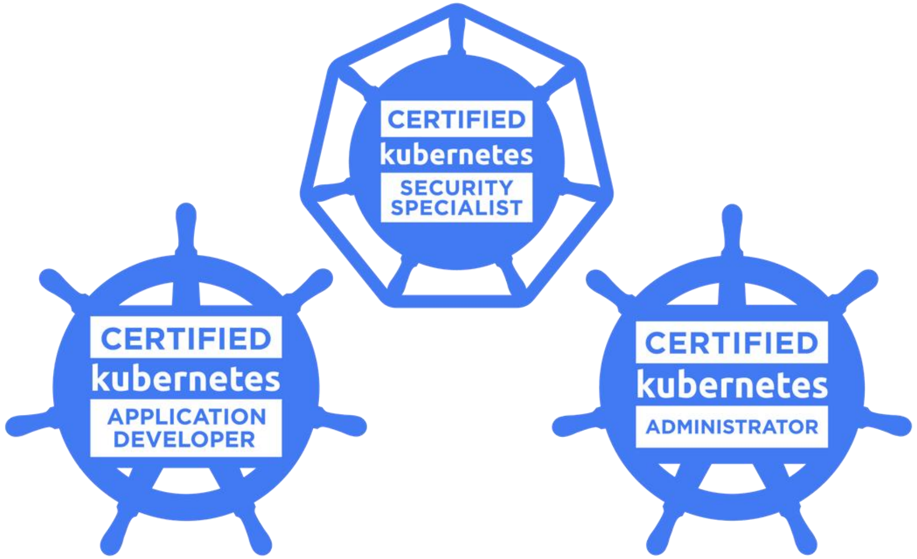
Kubernetes

training and certification helpful for deploying in production

Millions of Trained and Certified Professionals

training and certifications

- Kubernetes MOOC hit 285,000 enrollments
- Certified Kubernetes Administrator (CKA) exam hit 101,000 enrollments
- Certified Kubernetes Application Developer (CKAD) hit 47,000 exam registrations
- Certified Kubernetes Security Specialist (CKS) exam hit 17,000 registrations
- Kubernetes and Cloud Native Associate Exam (KCNA) exam reached 3,800 registrations
- Additional Courses include:
  - Service Mesh Fundamentals
  - Manager Kubernetes Applications with Helm
  - Cloud Native Logging with Fluentd
  - Intro to Service Mesh with Linkerd
  - Intro to Serverless on Kubernetes
  - Intro to WebAssembly



KCSP, KTP, Certified Kubernetes Conformance

services provider and software conformance

- Kubernetes Certified Service Provider (KCSP)
  - A pre-qualified tier of vetted service providers who have deep experience helping enterprises successfully adopt Kubernetes through support, consulting, professional services and/or training.
- Kubernetes Training Partners (KTP)
  - A tier of vetted training providers who have deep experience in cloud native technology training.
- Certified Kubernetes Conformance
  - Software conformance ensures that every vendor’s version of Kubernetes supports the required APIs, as do open source community versions.

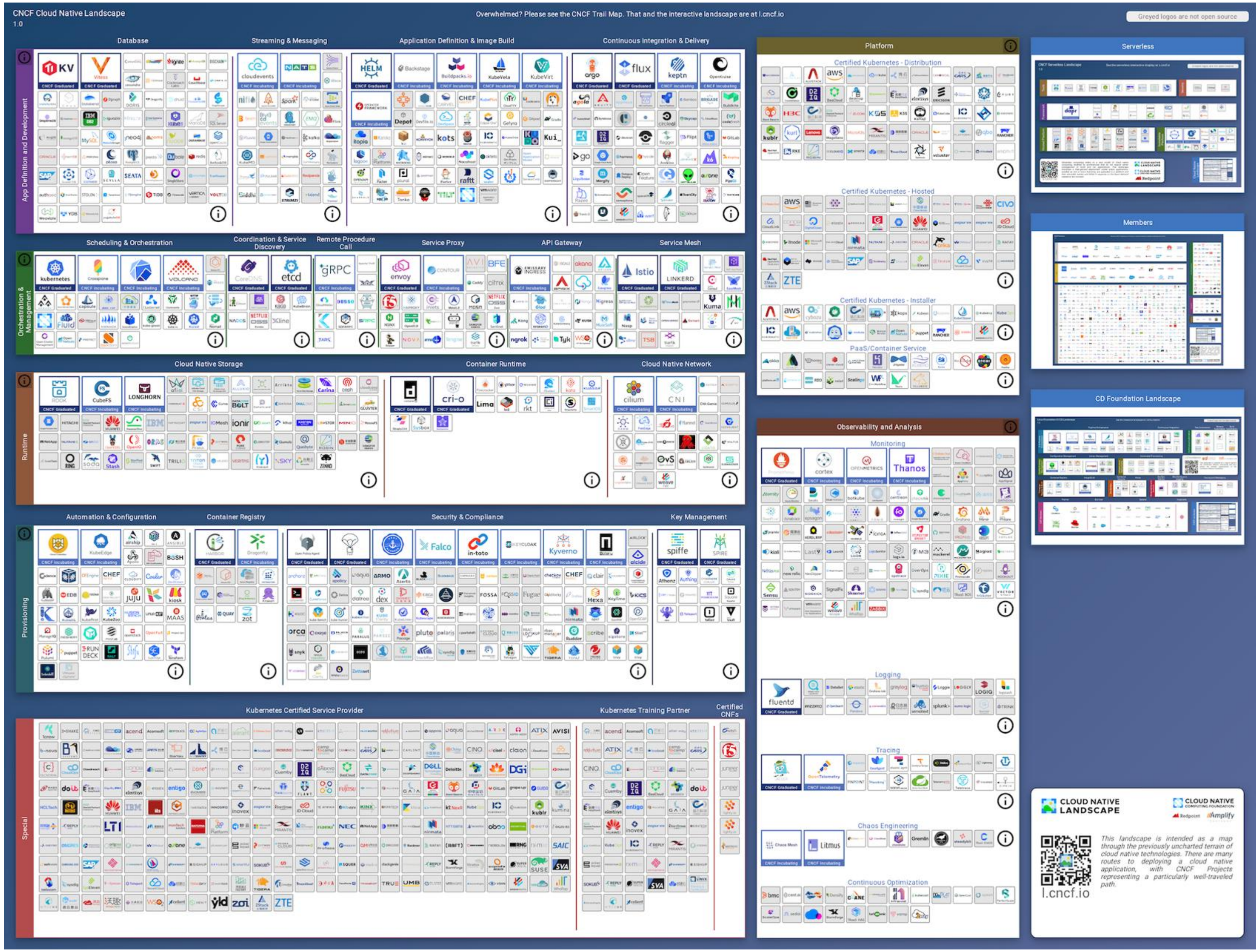
3

CNCF Landscape

聚焦安全与合规性

CNCF Cloud Native Interactive Landscape

https://landscape.cncf.io/


CNCF Cloud Native Landscape
1.0
Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io
Greyed logos are not open source
App Definition and Development
Database
Streaming & Messaging
Application Definition & Image Build
Continuous Integration & Delivery
Orchestration & Management
Scheduling & Orchestration
Coordination & Service Discovery
Remote Procedure Call
Service Proxy
API Gateway
Service Mesh
Runtime
Cloud Native Storage
Container Runtime
Cloud Native Network
Provisioning
Automation & Configuration
Container Registry
Security & Compliance
Key Management
Special
Kubernetes Certified Service Provider
Kubernetes Training Partner
Certified CNFs
Platform
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Observability and Analysis
Monitoring
Logging
Tracing
Chaos Engineering
Continuous Optimization
Serverless
Members
CD Foundation Landscape
CLOUD NATIVE LANDSCAPE
l.cncf.io
This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

The goal of the cloud native landscape is to compile and organize all cloud native open source projects and proprietary products into categories, providing an overview of the current ecosystem.

CNCF Landscape Guide

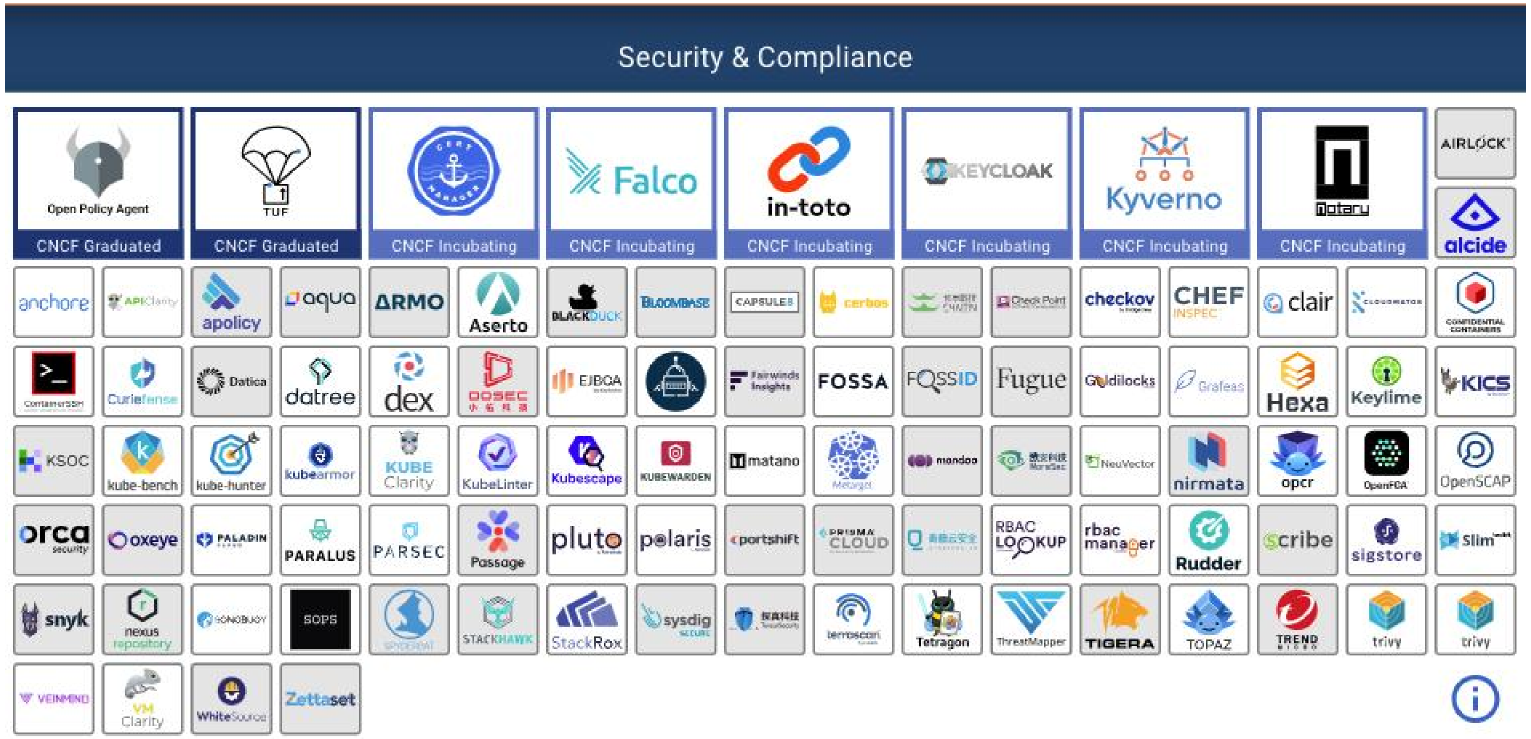
- Provisioning
- Runtime
- Orchestration & Management
- App Definition and Development
- Observability and Analysis
- Platform

Security & Compliance

harden, monitor, and enforce platform and application security.

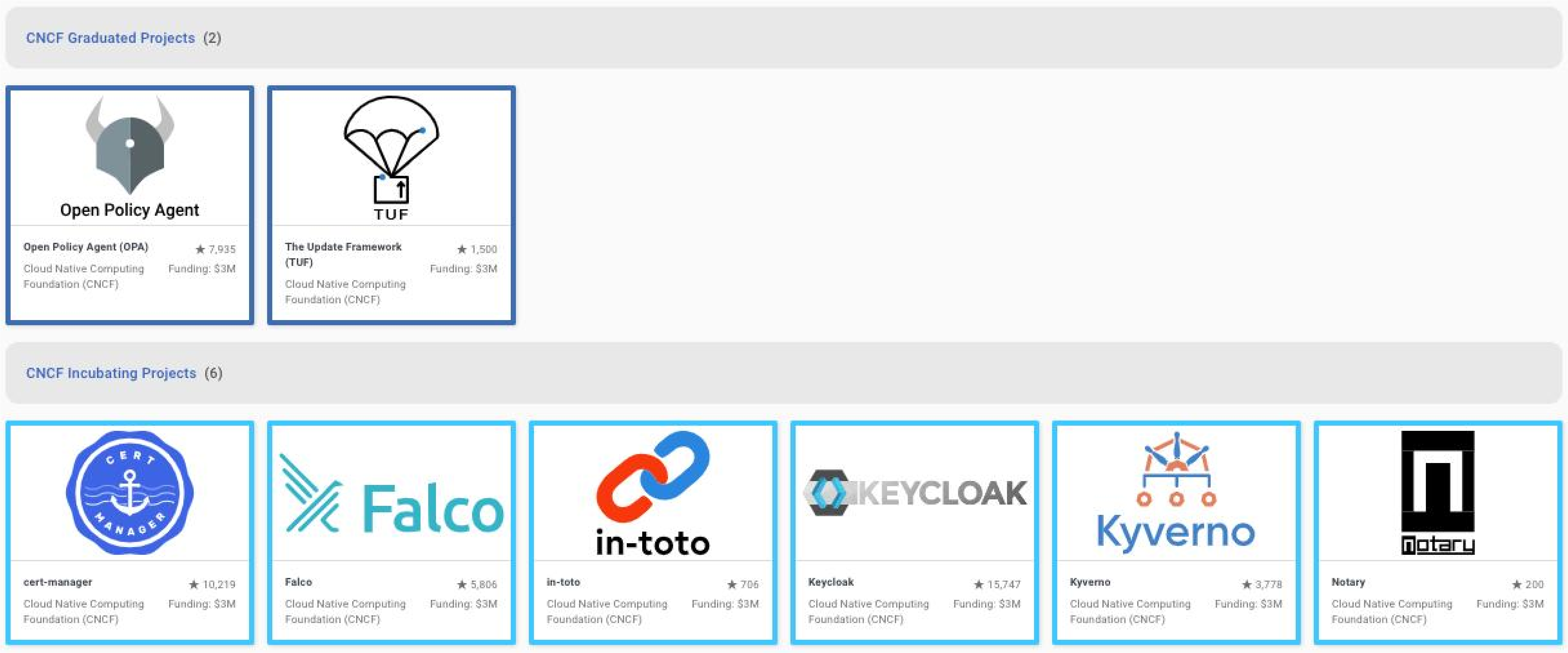
Technical 101/Buzzwords

- Audit and compliance
- Path to production
  - Code scanning
  - Vulnerability scanning
  - Image signing
  - Policy creation and enforcement
  - Network layer security



Security & Compliance (Graduated, Incubating)

harden, monitor, and enforce platform and application security.



CNCF Graduated Projects (2)

Open Policy Agent (OPA) ★ 7,935
Cloud Native Computing Foundation (CNCF) Funding: $3M

The Update Framework (TUF) ★ 1,500
Cloud Native Computing Foundation (CNCF) Funding: $3M

CNCF Incubating Projects (6)

cert-manager ★ 10,219
Cloud Native Computing Foundation (CNCF) Funding: $3M

Falco ★ 5,806
Cloud Native Computing Foundation (CNCF) Funding: $3M

in-toto ★ 706
Cloud Native Computing Foundation (CNCF) Funding: $3M

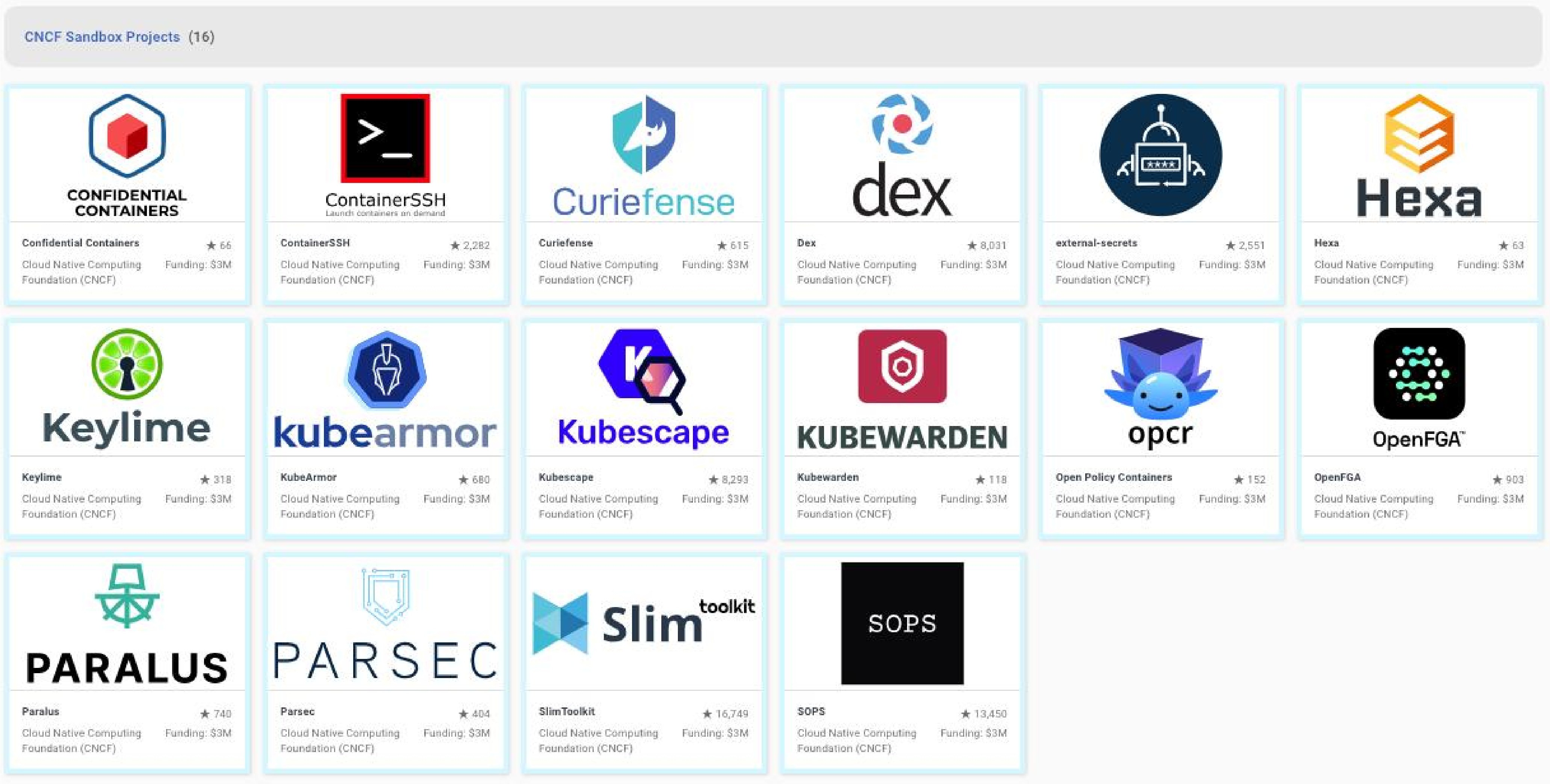
Keycloak ★ 15,747
Cloud Native Computing Foundation (CNCF) Funding: $3M

Kyverno ★ 3,778
Cloud Native Computing Foundation (CNCF) Funding: $3M

Notary ★ 200
Cloud Native Computing Foundation (CNCF) Funding: $3M

Security & Compliance (Sandbox)

harden, monitor, and enforce platform and application security.



CNCF Sandbox Projects (16)

Confidential Containers	★ 66	Cloud Native Computing Foundation (CNCF)	Funding: $3M
ContainerSSH	★ 2,282	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Curiefense	★ 615	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Dex	★ 8,031	Cloud Native Computing Foundation (CNCF)	Funding: $3M
external-secrets	★ 2,551	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Hexa	★ 63	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Keylime	★ 318	Cloud Native Computing Foundation (CNCF)	Funding: $3M
KubeArmor	★ 680	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Kubescape	★ 8,293	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Kubewarden	★ 118	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Open Policy Containers	★ 152	Cloud Native Computing Foundation (CNCF)	Funding: $3M
OpenFGA	★ 903	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Paralus	★ 740	Cloud Native Computing Foundation (CNCF)	Funding: $3M
Parsec	★ 404	Cloud Native Computing Foundation (CNCF)	Funding: $3M
SlimToolkit	★ 16,749	Cloud Native Computing Foundation (CNCF)	Funding: $3M
SOPS	★ 13,450	Cloud Native Computing Foundation (CNCF)	Funding: $3M

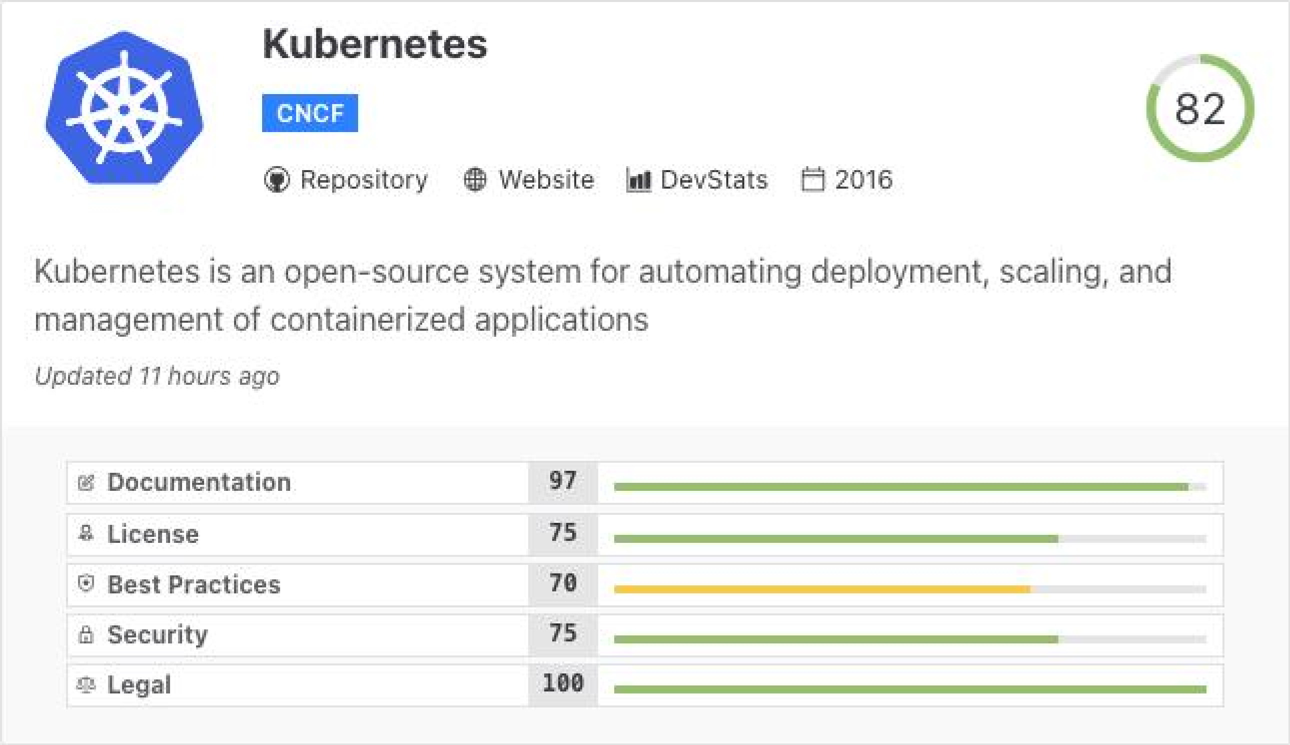
4

CLOMonitor

how good a project is

Project score

https://clomonitor.io/
based on Documentation, License, Best Practices, Security and Legal



Kubernetes

CNCF

Repository · Website · DevStats · 2016

82

Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications

Updated 11 hours ago

Documentation	97
License	75
Best Practices	70
Security	75
Legal	100

Documentation
- Contributing
- Maintainers
- Readme

License
- Approved
- Scanning

Best Practices
- CLA
- DCO
- OpenSSF best practices badge
- OpenSSF Scorecard badge
- Recent release

Security
- Binary artifacts
- Code review
- Dangerous workflow
- Dependency update tool
- Maintained
- SBOM
- Policy
- Signed releases
- Token permissions

5

OpenSSF

advance open source security for all

Open source is critical to the software supply chain

97%

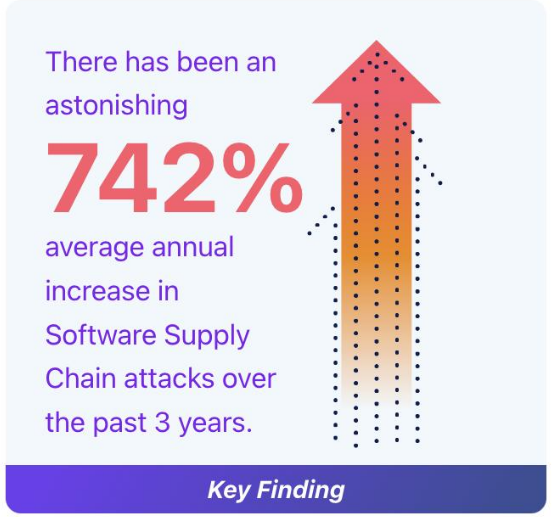
of audited commercial codebases contain OSS

78%

of code in codebases is OSS

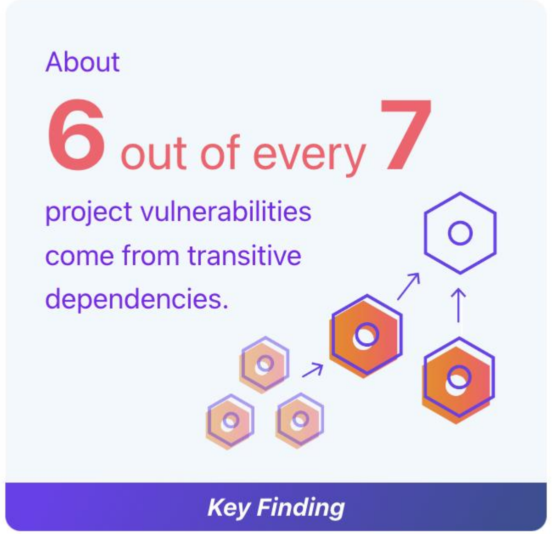
85%

of codebases contain open source that is more than four years out of date



There has been an astonishing **742%** average annual increase in Software Supply Chain attacks over the past 3 years.

Key Finding



About **6** out of every **7** project vulnerabilities come from transitive dependencies.

Key Finding

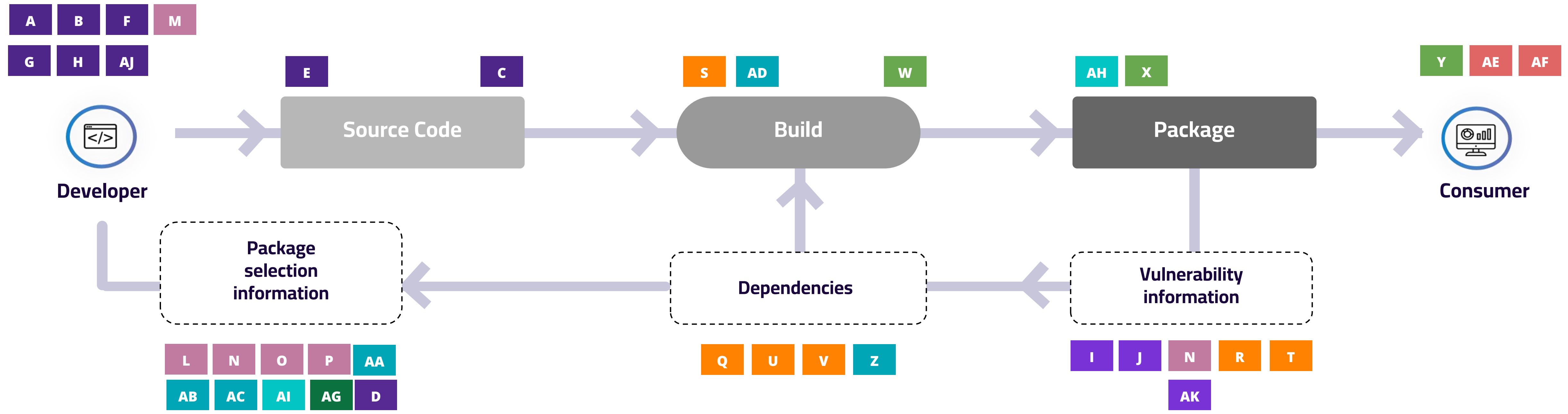
[Sonatype2022]

Source:
[Synopsys2022] "2022 Open Source Security and Risk Analysis Report" by Synopsys
[Sonatype2022] "2022 State of the Software Supply Chain" by Sonatype

Purpose

To inspire and enable the community to secure the open source software we all depend on, including development, testing, fundraising, infrastructure, and support initiatives driven by Working Groups (non-software focused) and Projects (software focused), each a “Technical Initiative”.

How OpenSSF Projects & SIGs Work Together



Best Practices WG

A. Secure Software Development Fundamentals courses SIG

B. Security Knowledge Framework (SKF) project

C. OpenSSF Best Practices Badge project

D. OpenSSF Scorecard project

E. Great MFA distribution SIG

F. Common Requirements Enumeration **(CRE)** project

G. Concise & Best Practices Guides SIGs

H. Education SIG - Mob. Plan

AJ. Memory Safety SIG - Mob. Plan

Vulnerability Disclosures WG

I. CVD Guides SIGs

J. OSS-SIRT SIG - Mob. Plan

K. Open Source Vuln Schema (OSV) project

AK. OpenVEX SIG

AL.**Vuln Autofix** SIG

Identifying Security Threats WG

L. Alpha & Omega project

M. Office Hours SIG

N. Security Insights

O. Security-Metrics: Risk Dashboard

P. Security Reviews project

Security Tooling WG

Q. SBOM Everywhere SIG - Mob. Plan

R. False-Positive Suppression Spec SIG

S.*[Guide to Security Tools SIG]*

T. *[cve-benchmark SIG]*

U. OSS Fuzzing SIG

V. DAST scanning & web app definitions SIG

End Users WG

AE. **Supply Chain Attack taxonomy** SIG

AF. **Supply Chain Attack RefArch** SIG

Supply Chain Integrity WG

W. Supply-chain Levels for Software Artifacts (SLSA) **SIG**

X. Factory for Repeatable Secure Creation of Artifacts (FRSCA) SIG

Y. Secure Supply Chain Consumption Framework (S2C2F) SIG

Securing Software Repositories WG

AG. Survey of OSS Repos SIG

Securing Critical Projects WG

Z. List of Critical Open Source Projects, components, & Frameworks SIG

AA. criticality_score project

AB. Harvard study SIG

AC. package-feeds / package-analysis project

AD. allstar project

Associated Projects

AH. sigstore

AI. **Core Toolchain Infrastructure (CTI) support**

关注公众号

CNCF

OpenSSF

THANKS