CLOUD NATIVE UNIVERSITY NORTH AMERICA

CLOUD NATIVE THEATER

# Supply Chain, Runtime and SDLC

## A Cloud Native Security Overview

*Dr. Constanze Roedig  fusioncore.ai / SBA-Research*

# Who is talking

CLOUD NATIVE UNIVERSITY NORTH AMERICA

CLOUD NATIVE THEATER

AMBASSADOR

CLOUD NATIVE COMPUTING FOUNDATION



**Dr. Constanze Roedig**

Founder / Key Researcher

*fusioncore.ai / SBA Research*

# Security can be overwhelming

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

01
## Supply Chain
*What is inside the software?*

02
## SDLC: CI/CD and GitOps
*Builds, Config and Deploy*

03
## Runtime
*What is actually alive*

SBOM

Identity

Rules

Signatures

Encryption

Isolation

Attestations

Secrets

Policies

# Security can be overwhelming

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

01
## Supply Chain
*What is inside the software?*

02
## SDLC: CI/CD and GitOps
*Builds, Config and Deploy*

03
## Runtime
*What is actually alive*

**Inventory:**

**- up-to-date**
**- complete**
**- e2e trusted**

**Changes:**

**- who did what**
**- quality assurance**
**- process and controls**

**What is deployed and what is it doing?**
**- live inventory**
**- behavior**
**- debugging**

# 01 Supply Chain

*What is inside the software?*

**Build, patch, store, distribute and clean up: CNCF projects**

- **Buildpacks** — graduated
- **ko** — sandbox
- **Shipwright** — sandbox
- **Dalec** — sandbox
- **Stacker** — sandbox
- **Copa** — sandbox
- **Eraser** — sandbox
- **Harbor** — graduated
- **zot** — sandbox
- **Distribution** — sandbox
- **Dragonfly** — graduated
- **ORAS** — sandbox

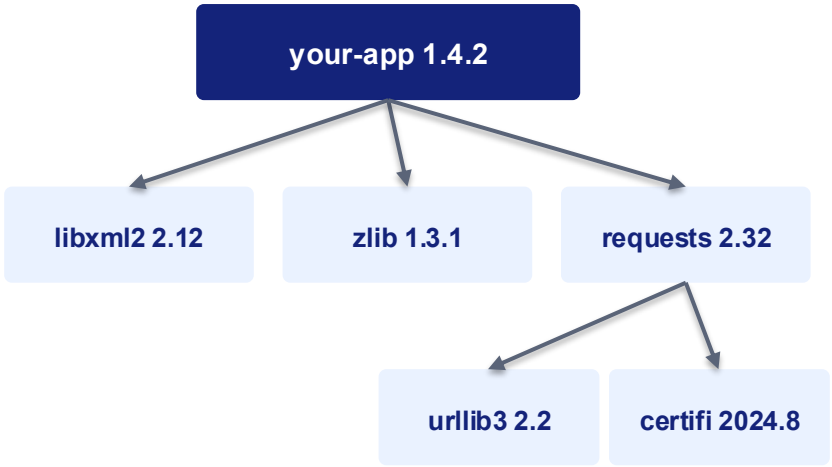
**OpenSSF projects (CNCF friends)**

- **SLSA** — OpenSSF graduated
- **RSTUF** — OpenSSF incubation
- **Zarf** — OpenSSF sandbox

# SBOM minimum elements (NTIA 2021)

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

## Components and their relationships




**CNCF publishes SBOMs for its projects:** github.com/cncf/sbom generates an SPDX SBOM per release; 71 of the 80 CNCF projects in this talk are covered (checked 2026-11-08).

## NTIA minimum data fields

- **Supplier Name** entity that creates, defines and identifies components
- **Component Name** designation assigned by the original supplier
- **Version of the Component**
- **Other Unique Identifiers** look-up key for other databases
- **Dependency Relationship** upstream component X is included in software Y
- **Author of SBOM Data**
- **Timestamp**

# SBOM (Software Bill of Materials)

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

*“A formal record containing the details and supply chain relationships of various components used in building software.”*

NIST SP 800-161r1, from E.O. 14028 §10(j)

## CNCF projects



Buildpacks.io
**Buildpacks**
graduated

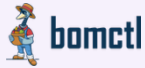


Dalec
**Dalec**
sandbox

## OpenSSF projects (CNCF friends)



GUAC
**GUAC**
OpenSSF incubation



**bomctl**
OpenSSF sandbox



**BOMHort**
OpenSSF sandbox



**CVE Binary Tool**
OpenSSF sandbox



**OpenVEX**
OpenSSF sandbox



**Protobom**
OpenSSF sandbox

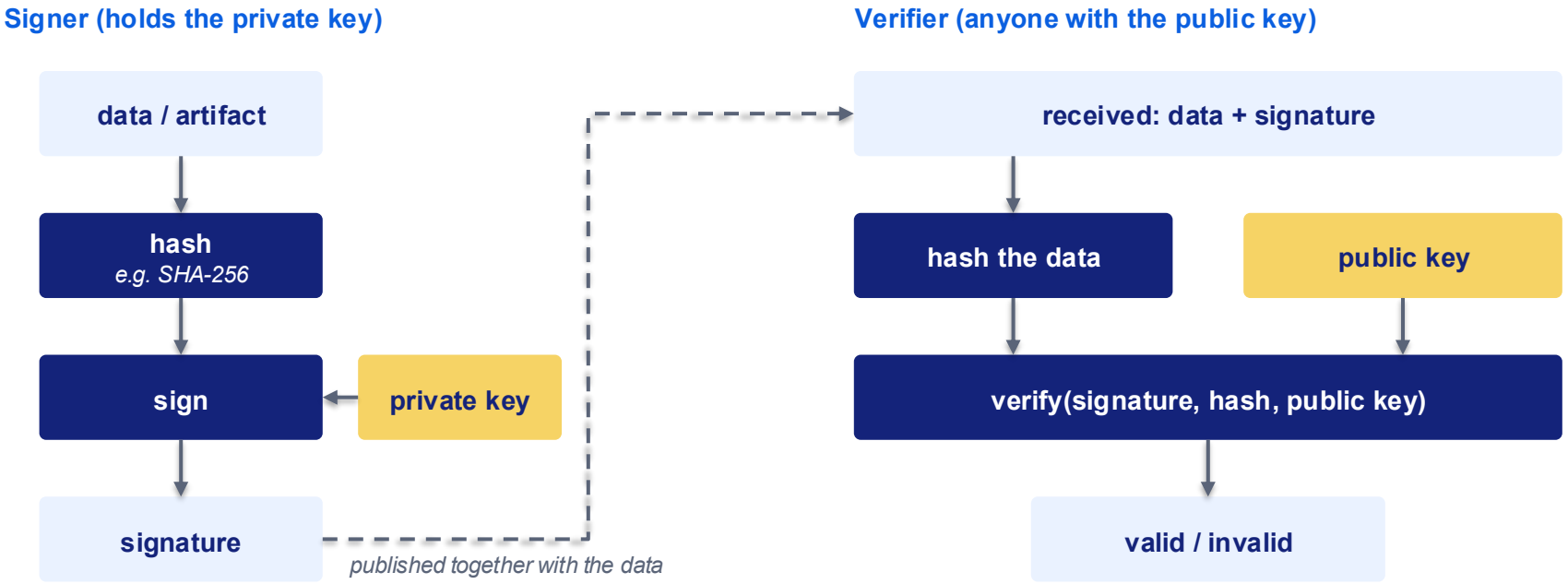


**SBOMit**
OpenSSF sandbox



**OSV Schema**
OpenSSF TBD

# How a digital signature works




data integrity | source authentication | identity authentication | supports non-repudiation

*Sources: FIPS 186-5 (signature algorithms); services as listed in NIST SP 800-175B Rev. 1, Sec. 4.2.3.*

# Signatures

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

> *"The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation."*
>
> FIPS 186-5, "digital signature"

## CNCF projects

- **Notary Project** incubating
- **TUF** graduated
- **Ratify** sandbox

## OpenSSF projects

- **Sigstore** OpenSSF graduated
- **gittuf** OpenSSF incubation
- **RSTUF** OpenSSF incubation
- **Model Signing** OpenSSF sandbox

## Sigstore tools

- **Cosign** Sigstore · OpenSSF
- **Fulcio** Sigstore · OpenSSF
- **Rekor** Sigstore · OpenSSF

# Attestation: statement vs. hardware evidence

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

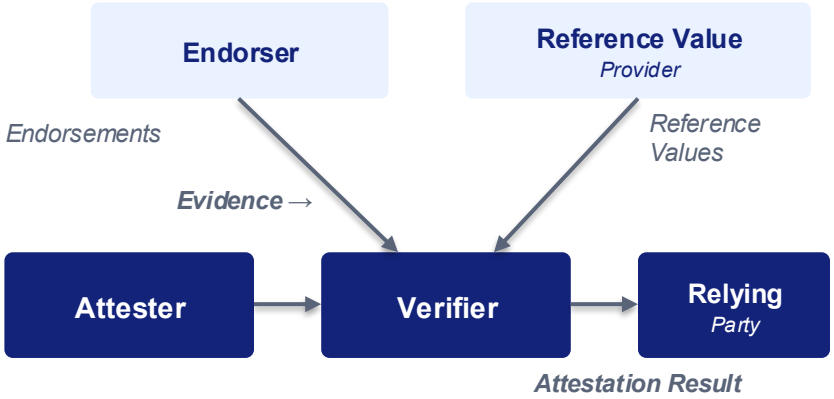
## Software supply chain: in-toto attestation layers

**Envelope:** authentication and serialization (signature over the payload)

**Statement:** binds to the subject: artifact name + digest, and the predicateType

**Predicate:** the actual claims, e.g. SLSA provenance: who built it, from which source, with which steps

## Hardware / remote attestation: RATS roles




**Evidence:** a set of claims the Attester generates about itself, e.g. TPM measurements.

**Verifier** appraises Evidence against Reference Values and its appraisal policy; the Relying Party decides based on the Attestation Result.

*Sources: in-toto Attestation Framework spec (github.com/in-toto/attestation); IETF RFC 9334, Remote ATtestation procedureS (RATS) Architecture.*

# Attestations

*“The issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated.”*

ISO/IEC 17000:2020, via NIST EO 14028 guidance

*“The process of providing a digital signature for a set of measurements securely stored in hardware, and then having the requester validate the signature and the set of measurements.”*

NIST SP 1800-19B

## CNCF projects: software supply chain

- **in-toto** — graduated
- **Dalec** — sandbox
- **Ratify** — sandbox

## CNCF projects: hardware / remote attestation

- **Keylime** — sandbox
- **Confidential Containers** — incubating
- **Inclavare Containers** — sandbox

## OpenSSF projects (CNCF friends)

- **SLSA** — OpenSSF graduated
- **GUAC** — OpenSSF incubation
- **Ampel** — OpenSSF sandbox
- **SBOMit** — OpenSSF sandbox

# 02 SDLC: CI/CD and GitOps

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

*Who built it, and who may change it?*

**Identity** | **Secrets** | **Policies**

### CI/CD, GitOps, packaging and IaC: CNCF projects

- **Argo** — graduated
- **Flux** — graduated
- **Flagger** — Flux subproject
- **Tekton** — incubating
- **PipeCD** — sandbox
- **werf** — sandbox
- **OpenGitOps** — sandbox
- **Atlantis** — sandbox
- **OpenTofu** — sandbox
- **Helm** — graduated

### OpenSSF projects

- **Best Practices Badge** — OpenSSF graduated
- **gittuf** — OpenSSF incubation
- **Scorecard** — OpenSSF incubation
- **OSPS Baseline** — OpenSSF incubation
- **Darnit** — OpenSSF sandbox
- **Minder** — OpenSSF sandbox
- **Security Insights** — OpenSSF sandbox
- **Criticality Score** — OpenSSF TBD

# Identity

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

*“An attribute or set of attributes that uniquely describes a subject within a given context.”*

NIST SP 800-63-4, “digital identity”

## CNCF projects

- **SPIFFE** — graduated
- **SPIRE** — graduated
- **Keycloak** — incubating
- **Dex** — sandbox
- **Athenz** — sandbox
- **OAuth2 Proxy** — sandbox
- **Tokenetes** — sandbox
- **Paralus** — sandbox
- **cert-manager** — graduated

## OpenSSF projects

- **Sigstore** — OpenSSF graduated
- **Fulcio** — Sigstore · OpenSSF

# Secrets

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

> *"A Secret is an object that contains a small amount of sensitive data such as a password, a token, or a key."*
>
> Kubernetes documentation, Concepts › Configuration › Secrets

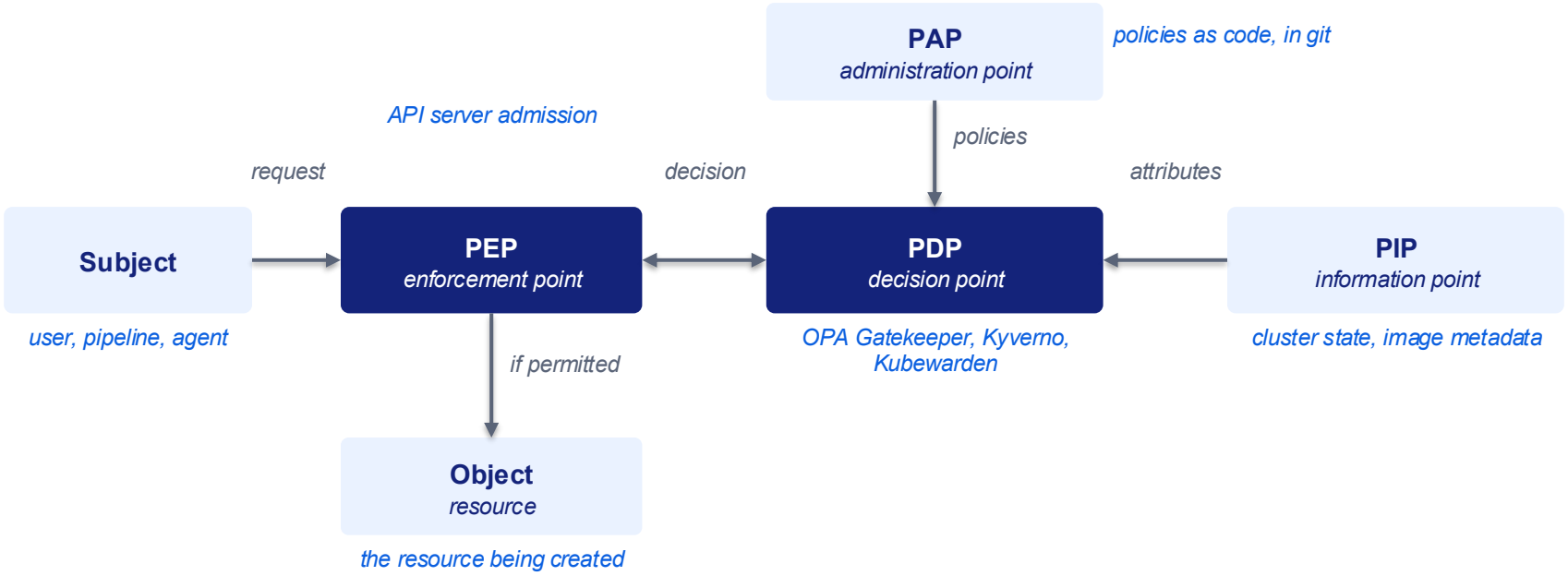
## CNCF projects

- **external-secrets** sandbox
- **SOPS** sandbox
- **Bank-Vaults** sandbox
- **cert-manager** graduated
- **Parsec** sandbox

## OpenSSF projects (CNCF friends)

- **OpenBao** OpenSSF sandbox

# Policy decision and enforcement (SP 800-162)



# Policies

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

*"Statements, rules or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component."*

NIST SP 800-95

## CNCF projects

- **OPA** graduated
- **Kyverno** graduated
- **Kubewarden** sandbox
- **Cedar** sandbox
- **OpenFGA** incubating
- **Open Policy Containers** sandbox
- **Cloud Custodian** incubating
- **KCL** sandbox
- **Kubescape** incubating
- **Capsule** sandbox
- **OSCAL-COMPASS** sandbox

## OpenSSF projects (CNCF friends)

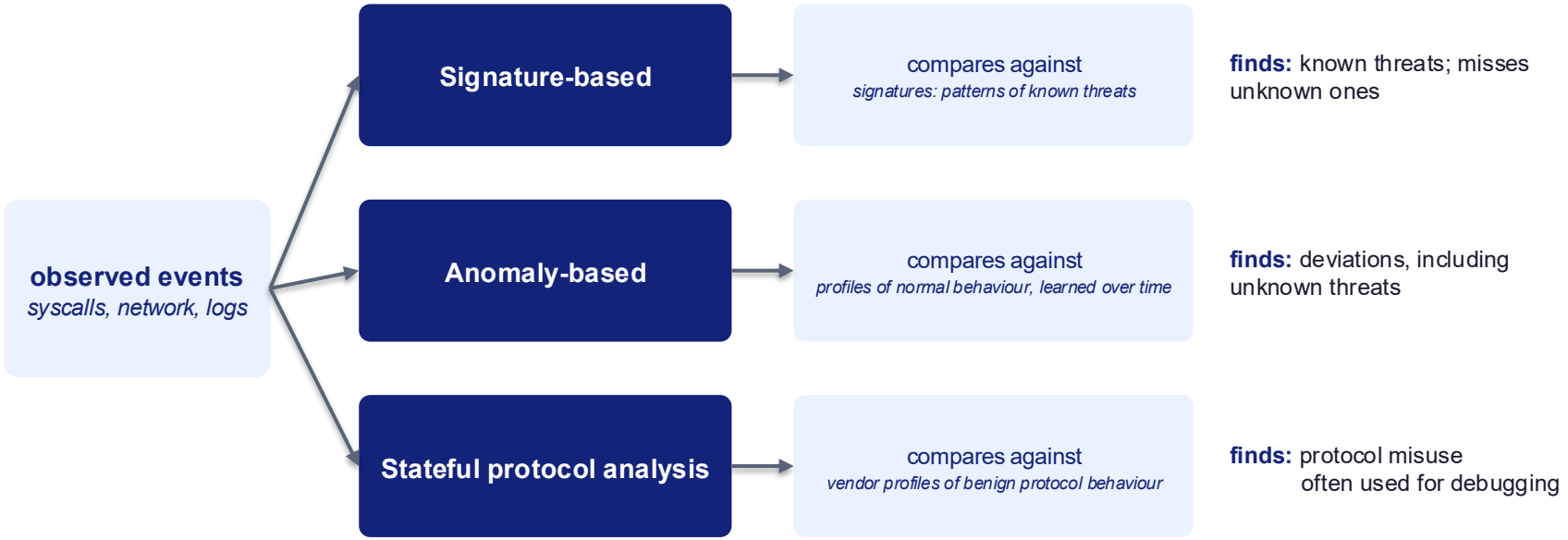
- **OSPS Baseline** OpenSSF incubation
- **Ampel** OpenSSF sandbox
- **Darnit** OpenSSF sandbox
- **Gemara** OpenSSF sandbox
- **Minder** OpenSSF sandbox
- **Privateer** OpenSSF sandbox

# 03 Runtime



*What does it actually do?*

# Detection methods (NIST SP 800-94)




*Source: NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems, Sec. 2.3.1–2.3.3.*

# Rules

*“A text string (algorithm or expression), used to configure intrusion detection systems and sensors, describing characteristics, patterns or other identifying information of cyber threat activity.”*

CNSSI 4009-2022, “signature” (same word as on the Signatures slide)

**CNCF projects**

| Falco | tetragon | kubearmor | Kubescape | Cloud Custodian |
|---|---|---|---|---|
| **Falco** graduated | **Tetragon** Cilium subproject | **KubeArmor** sandbox | **Kubescape** incubating | **Cloud Custodian** incubating |

**OpenSSF projects (CNCF friends)**



**Malicious Packages**
OpenSSF sandbox



**Package Analysis**
OpenSSF TBD

# Where the isolation boundary sits

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

### Containers

app

bins / libs

container runtime

**host OS kernel (shared)**

hardware

**boundary:** kernel namespaces, cgroups, seccomp

*containerd, CRI-O*

### Sandboxed containers

app

bins / libs

**guest kernel per pod**

sandbox monitor (VMM)

host OS kernel

hardware

**boundary:** per-pod kernel or unikernel

*Kuasar, urunc, Hyperlight, gVisor*

### Virtual machines

app

bins / libs

guest OS

**hypervisor**

hardware

**boundary:** hypervisor

*KubeVirt*

### Confidential

app

bins / libs

guest OS

hypervisor (not trusted)

**hardware with TEE**

**boundary:** hardware TEE, memory encrypted

*Confidential Containers*

# Isolation

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

> *"The ability to keep multiple instances of software separated so that each instance only sees and can affect itself."*
>
> NIST SP 800-190, Application Container Security Guide

**CNCF projects: container runtimes and sandboxes**

- **containerd** graduated
- **CRI-O** graduated
- **youki** sandbox
- **Kuasar** sandbox
- **urunc** sandbox
- **Hyperlight** sandbox
- **Confidential Containers** incubating
- **Inclavare Containers** sandbox

**CNCF projects: VMs, tenants, network, agents**

- **KubeVirt** graduated
- **Capsule** sandbox
- **Cilium** graduated
- **Antrea** sandbox
- **Agent Substrate** sandbox
- **OpenShell** sandbox

# Encryption

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

*“The process of changing plaintext into ciphertext using a cryptographic algorithm and key.”*

NIST SP 800-57 Part 1 Rev. 5

## CNCF projects

- **cert-manager** graduated
- **Istio** graduated
- **Linkerd** graduated
- **Cilium** graduated
- **Kuma** sandbox
- **Envoy** graduated
- **Antrea** sandbox
- **Submariner** sandbox
- **SOPS** sandbox
- **Confidential Containers** incubating

## OpenSSF projects (CNCF friends)

- **OpenBao** OpenSSF sandbox

# What changed in 2026?

CLOUD NATIVE UNIVERSITY NORTH AMERICA
CLOUD NATIVE THEATER

## AI agents

Agents hold credentials and act in pipelines and clusters: a new non-human identity.

Untrusted text (issues, docs, tool output) becomes input to privileged actions.

Generated code pulls in (whatever) dependencies

## Zero-days

AI-assisted vulnerability discovery finds more, faster.

The window between disclosure and exploitation keeps shrinking.

CVE matching only finds what is already known.

PROTECT YOUR KEYS/SECRETS like never before

**Exposure shifts from “known vulnerable package” towards “unexpected behaviour”, which puts more weight on identity and runtime.**

### AI agents in the CNCF landscape

- **Agent Substrate** — sandbox
- **OpenShell** — sandbox
- **kagent** — sandbox
- **HolmesGPT** — sandbox
- **K8sGPT** — sandbox

### OpenSSF: model signing, bugs

- **Model Signing** — OpenSSF sandbox
- **OSS-CRS** — OpenSSF sandbox
- **Fuzz introspector** — OpenSSF TBD

### Agent identity

- **SPIFFE** — graduated
- **SPIRE** — graduated

# What still holds

Supply chain

Pin images by digest and verify signatures at admission.

Supply chain

Know what you run: keep SBOMs current,

check if your inventory is up-to-date

SDLC

Least privilege and short-lived identity, for humans, pipelines and agents.

SDLC

Make sure you can rotate leaked secrets FAST!

Runtime

Default-deny

Defense in depth

Zero Trust (no that's not a contradiction)

Runtime

Identity on everything

CLOUD NATIVE UNIVERSITY
NORTH AMERICA
CLOUD NATIVE THEATER

# Thank you

*Questions? · Dr. Constanze Roedig · billofbehavior.com*

