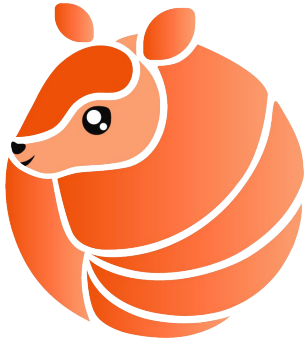
Confidential computing with Kairos

The immutable edge Kubernetes

Kairos

Summary

- Introduction
- Kairos and Confidential computing
  - Architecture
  - Current state



Introduction

Kubernetes Immutable Edge Infrastructure

Introduction - Confidential computing

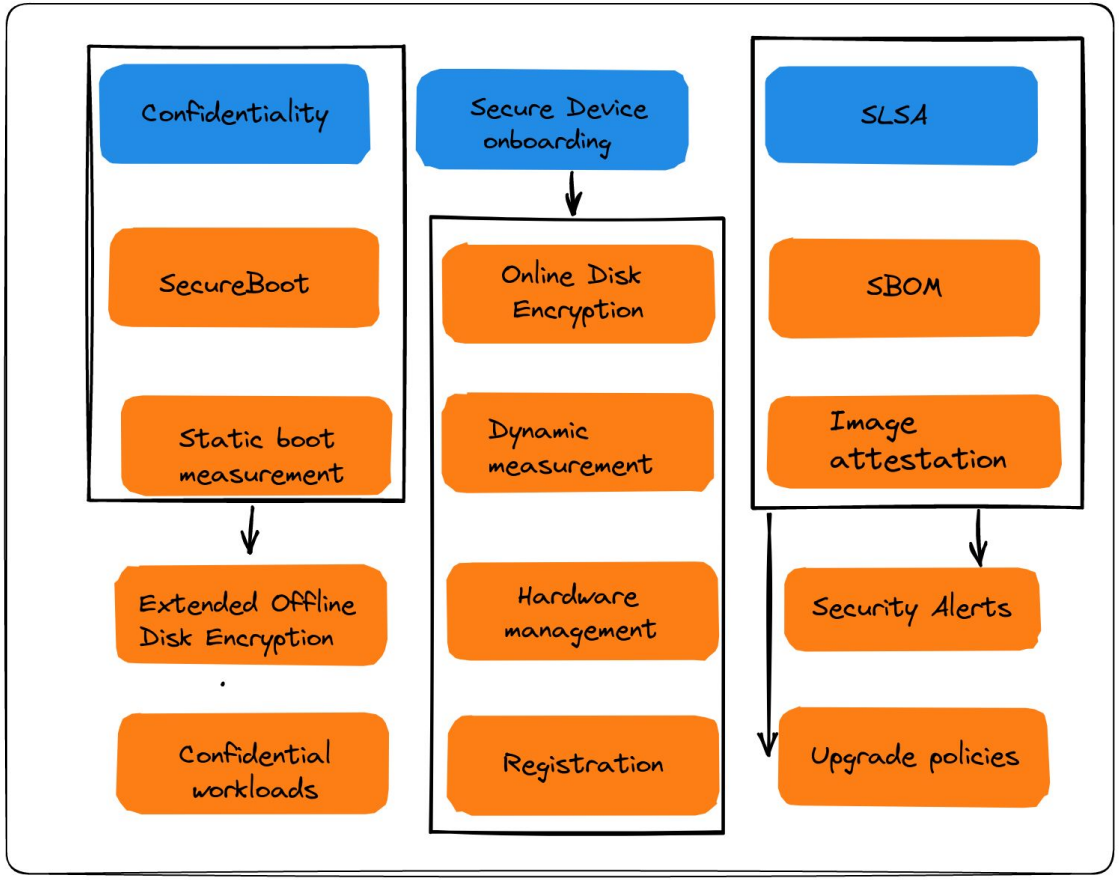
- Why?
  - Securely provision devices
  - Securely control and identify devices
  - Remote assessment of system's state
  - Secure data at rest
  - Secure workload isolation
  - Secure upgrade policies
  - Secure supply chain
  - Security Image and CVEs reports analysis

Architecture

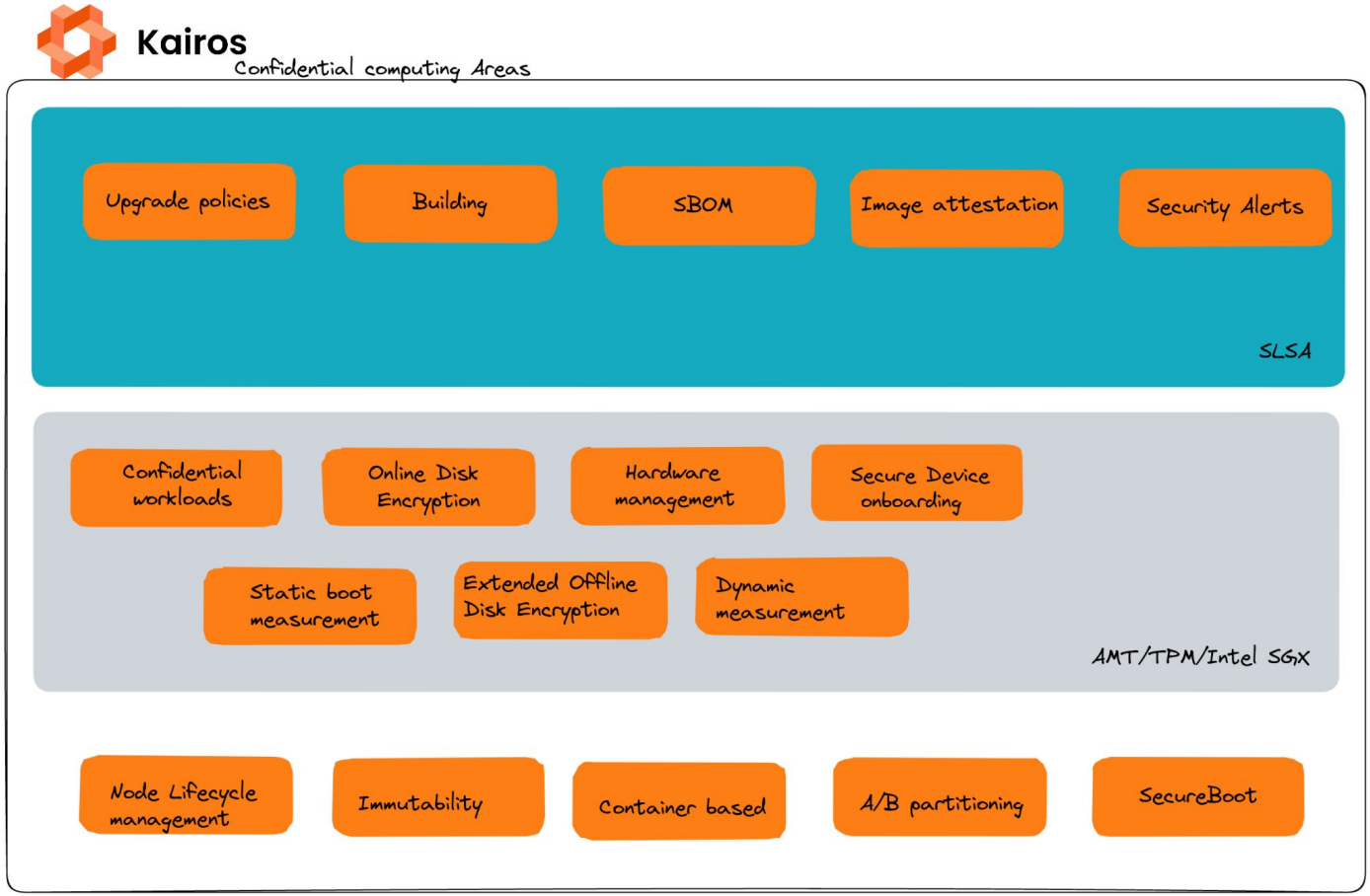
Kubernetes Immutable Edge Infrastructure

Kairos

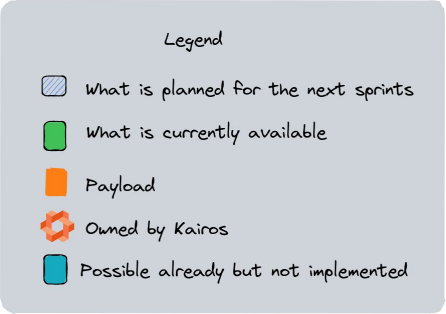
Confidential computing Areas



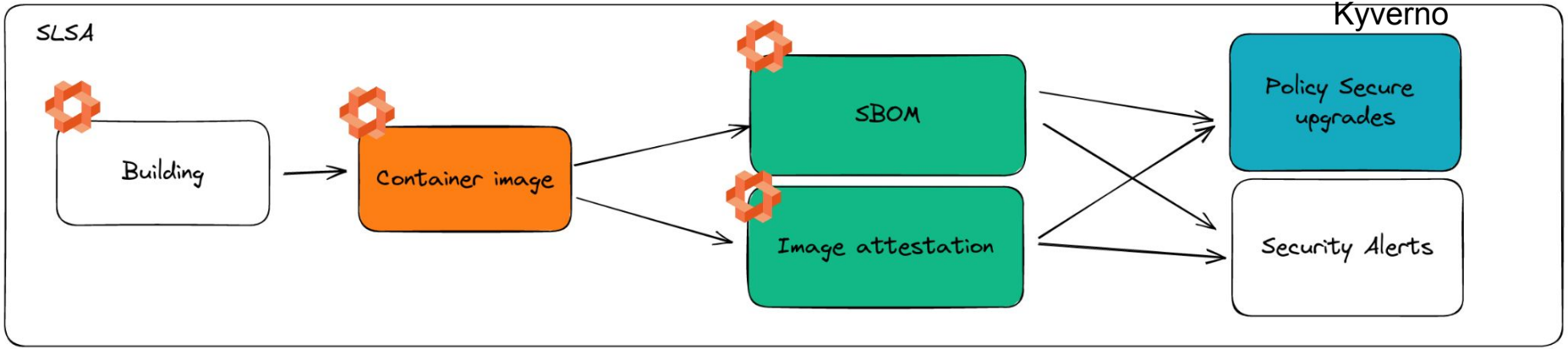
Areas


Kairos
Confidential computing Areas
Upgrade policies
Building
SBOM
Image attestation
Security Alerts
SLSA
Confidential workloads
Online Disk Encryption
Hardware management
Secure Device onboarding
Static boot measurement
Extended Offline Disk Encryption
Dynamic measurement
AMT/TPM/Intel SGX
Node Lifecycle management
Immutability
Container based
A/B partitioning
SecureBoot

SLSA



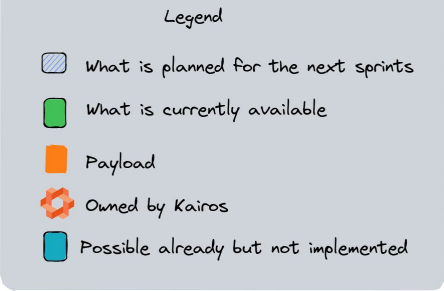
What are we installing/Upgrading?



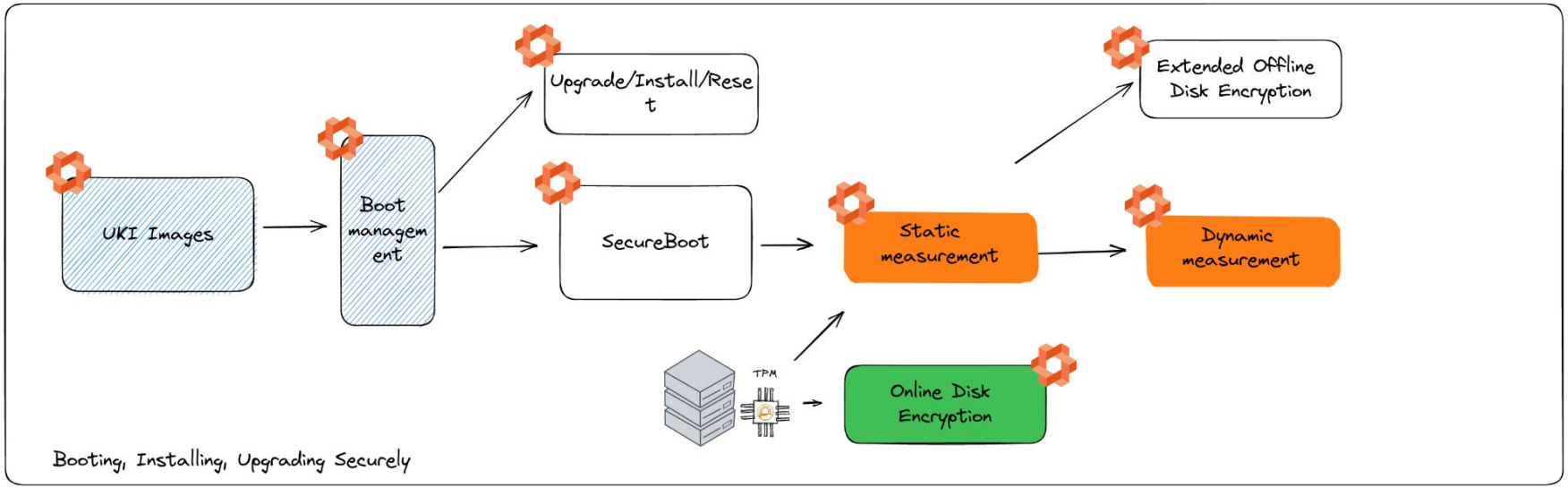
We currently use: cosign, trivy, syft, and grype

Kairos

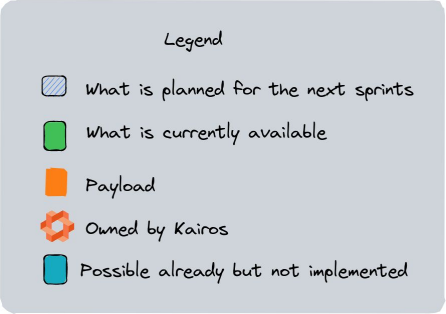
Booting securely

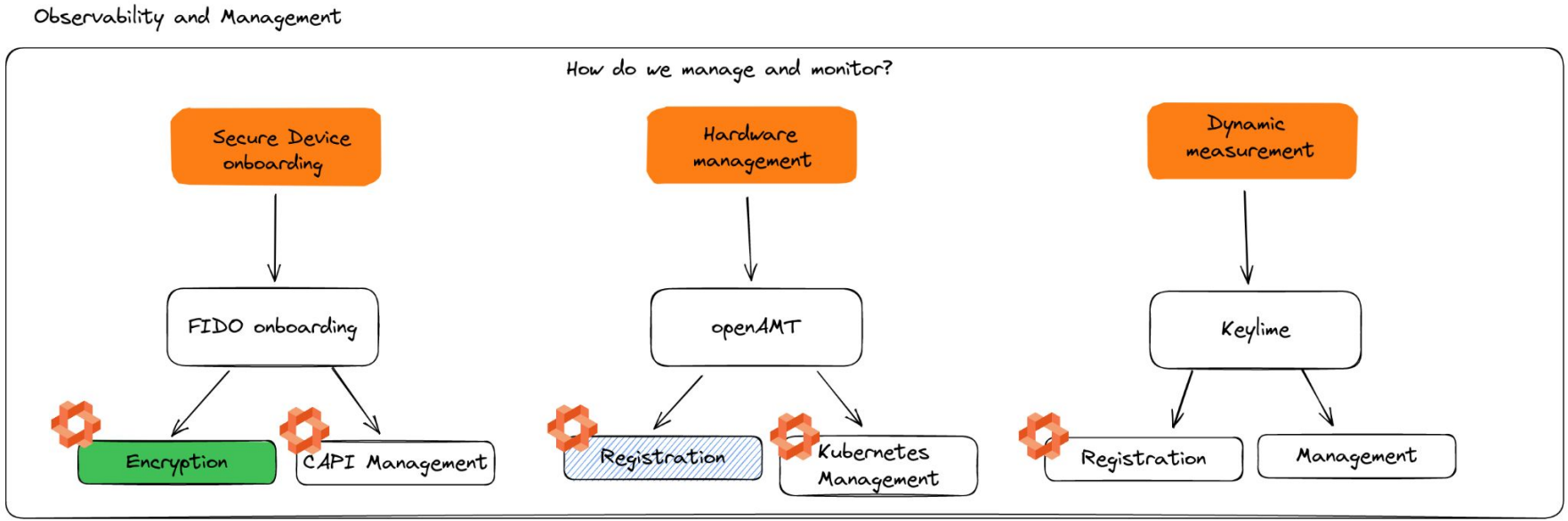


How are we Booting/Upgrading securely?



Observability and management





Kairos

Want to know more or try it out?

Learn more about Kairos at https://kairos.io/

Check out the code at
https://github.com/kairos-io/kairos

Download a release
https://github.com/kairos-io/kairos/releases

Matrix: #kairos-io:matrix.org

GitHub Discussions: https://github.com/kairos-io/kairos/discussions

Office Hours (Wednesdays 17:30-18:00 CET): https://meet.google.com/aus-mhta-azb

Thanks!

Kairos