

(this document)



DevSecOps Strategy Guide

- Executive Summary
- Guiding Principles
- Governance Processes

DevSecOps Fundamentals

Topic Specific Guidebooks

- Industry Recognized Best Practices
- Standardized Nomenclature
- Technology Tool & Activity Mappings
- SMART Performance Metrics

Topic Specific Playbooks

DoD Enterprise
DevSecOps
Reference Design

CNCF Kubernetes

- Specific CNCF Kubernetes Tools & Technologies
- Specific Architecture Requirements

DoD Enterprise
DevSecOps
Reference Design

...

- Additional Reference Designs

DoD Enterprise
DevSecOps
Reference Design

Low Code-No Code

DoD Enterprise
DevSecOps
Reference Design

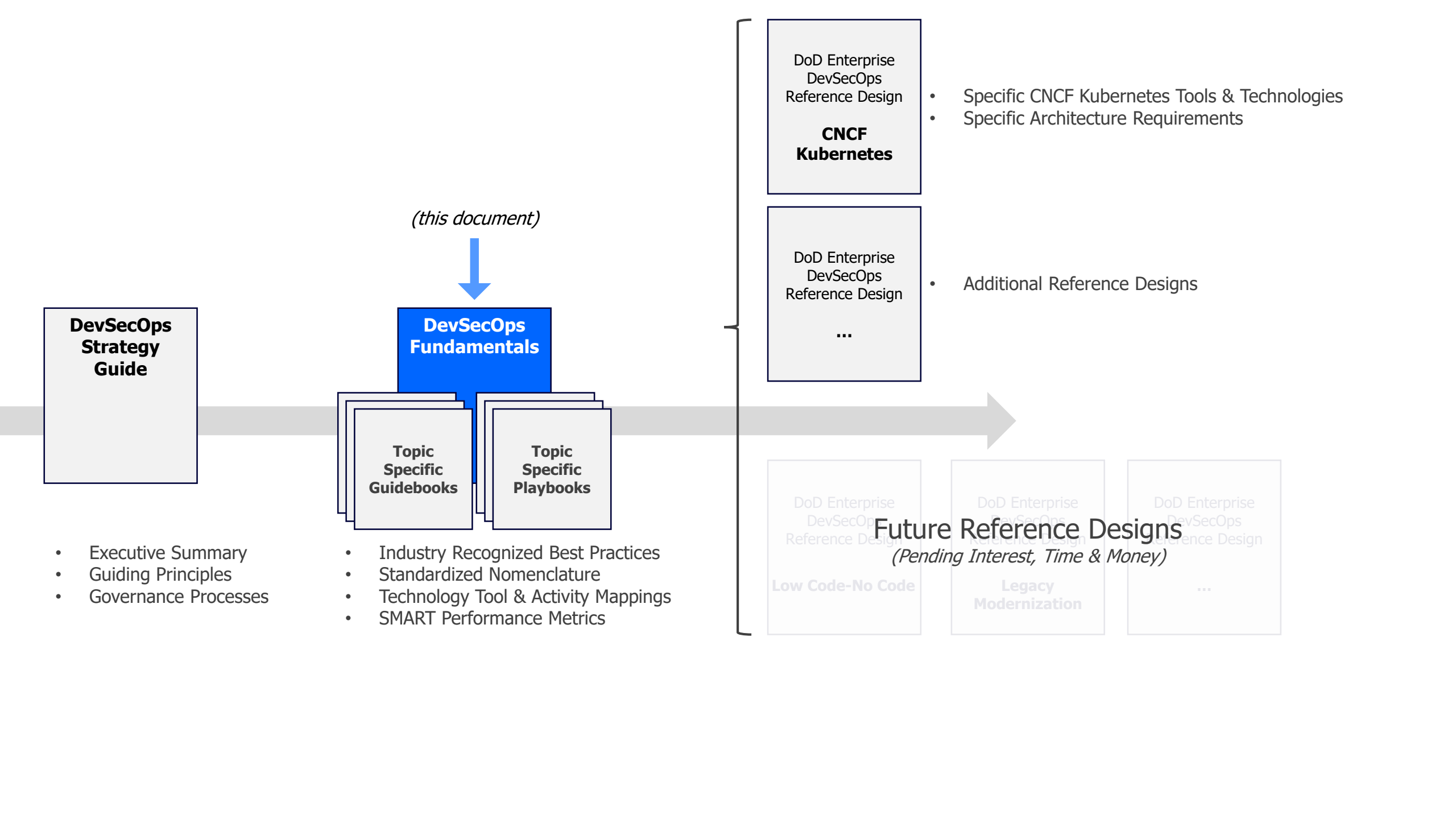
**Legacy
Modernization**

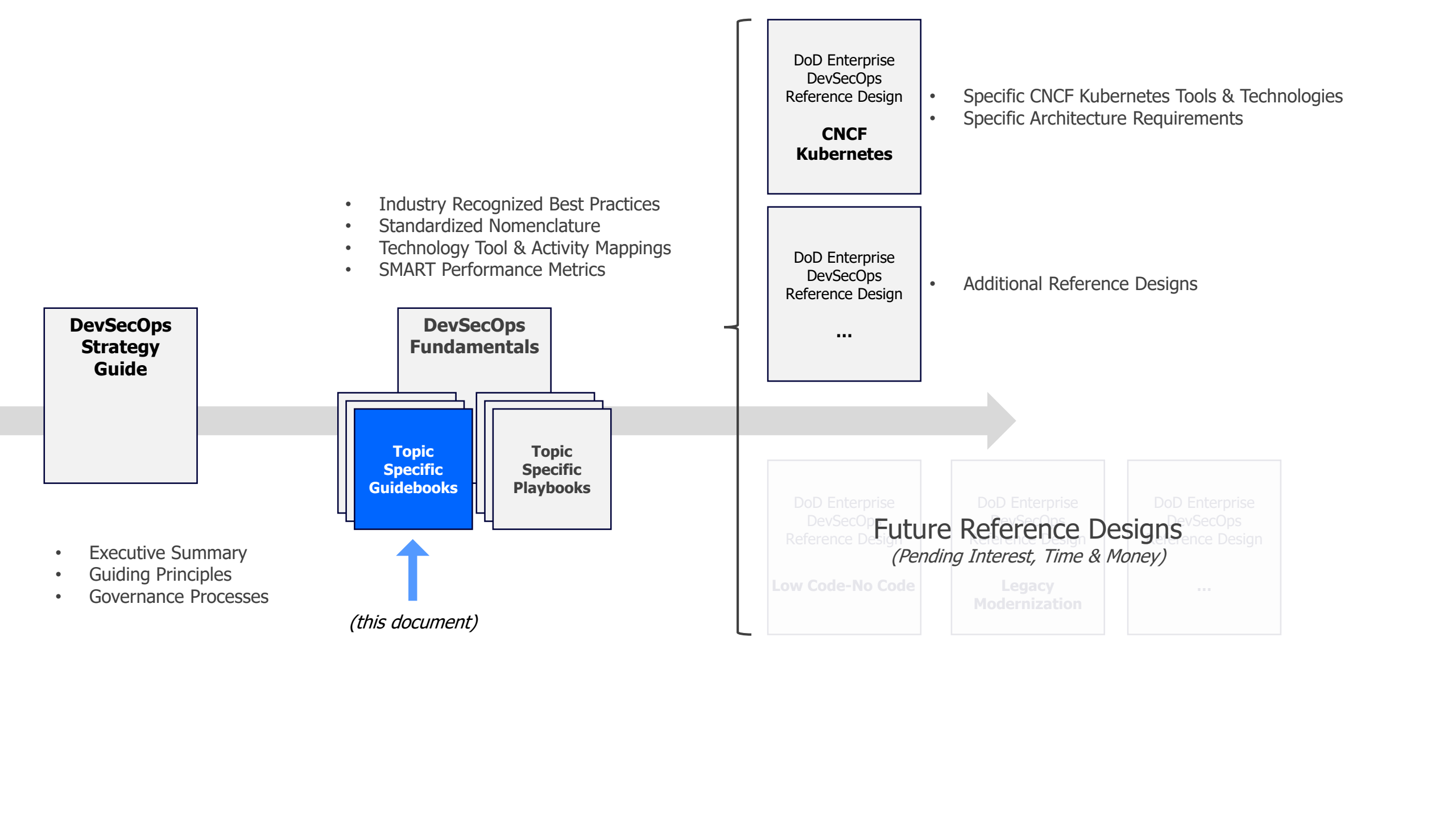
DoD Enterprise
DevSecOps
Reference Design

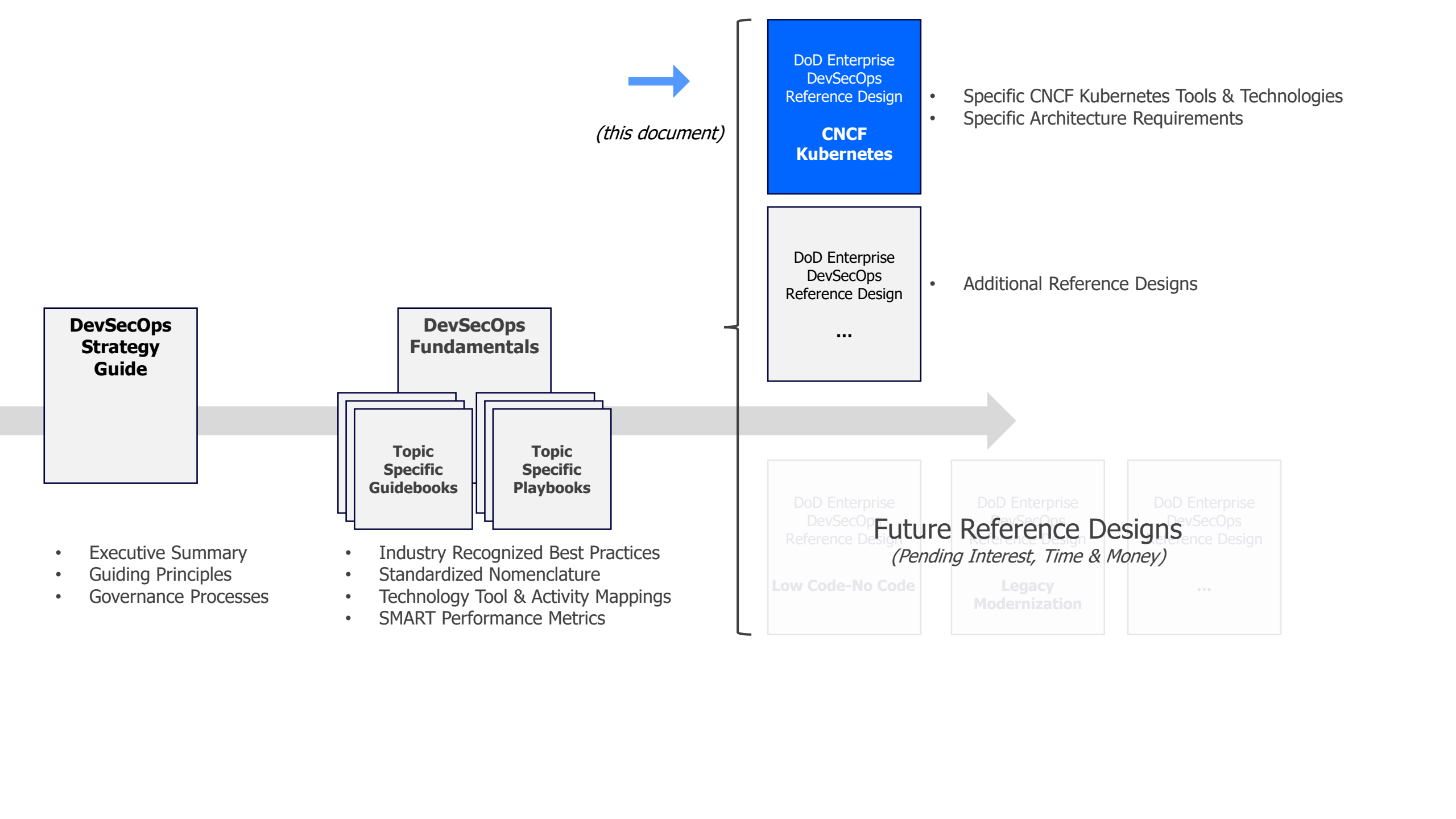
...

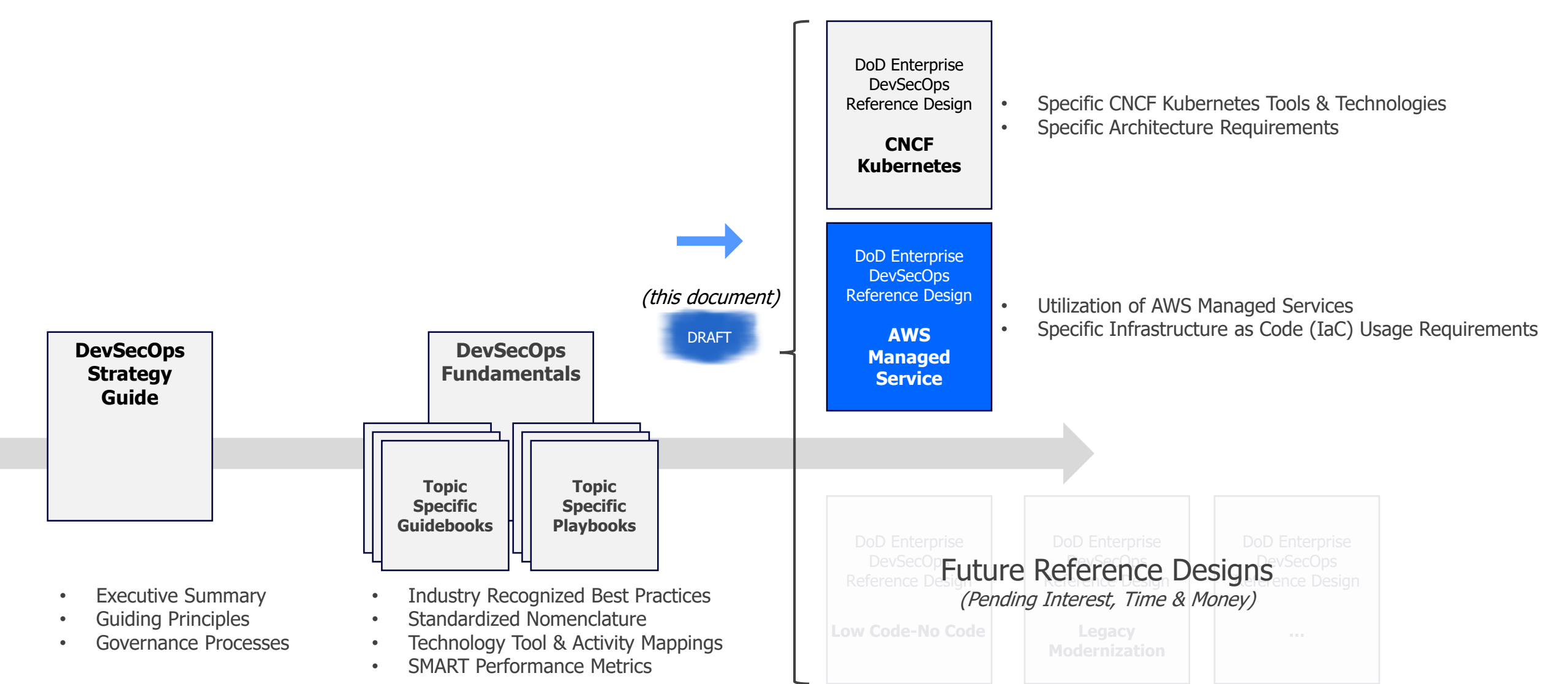
Future Reference Designs

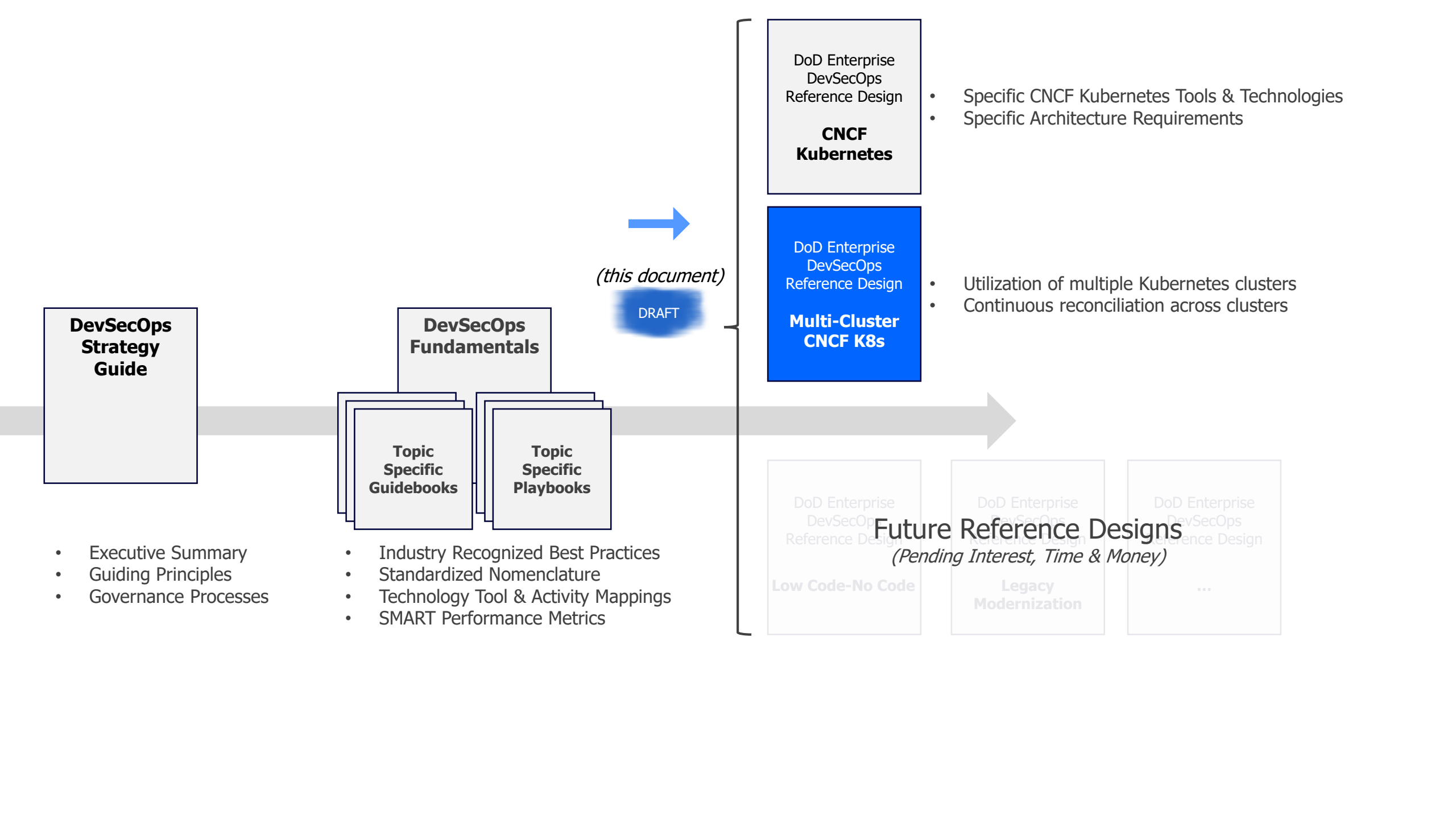
(Pending Interest, Time & Money)







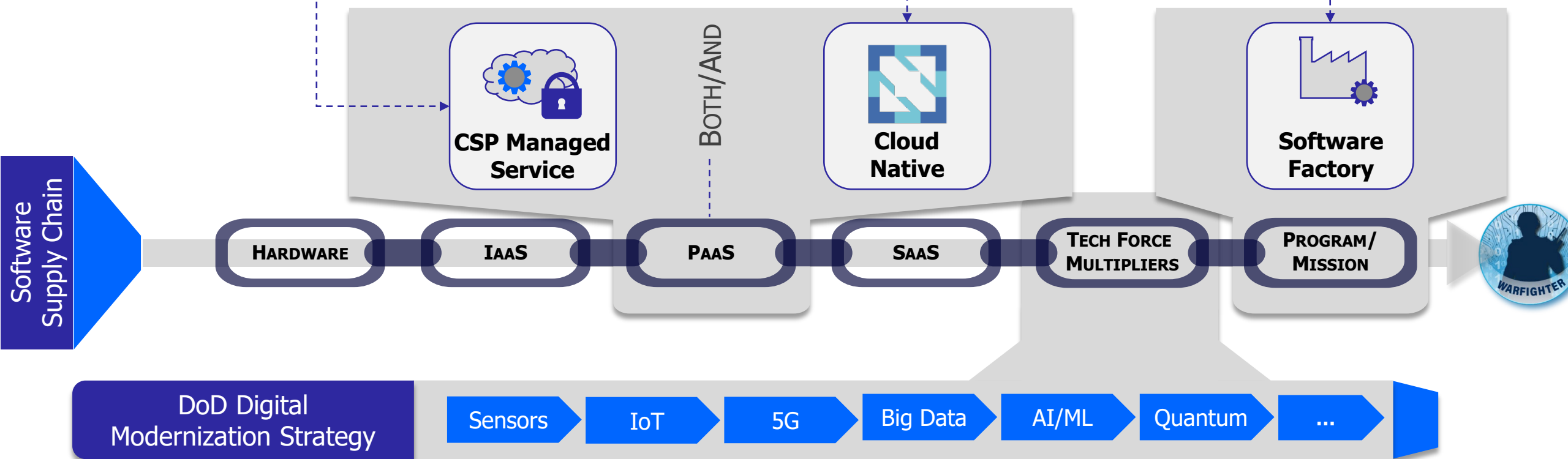


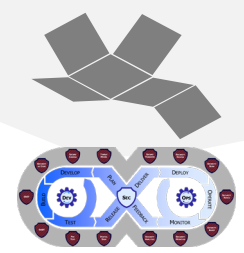
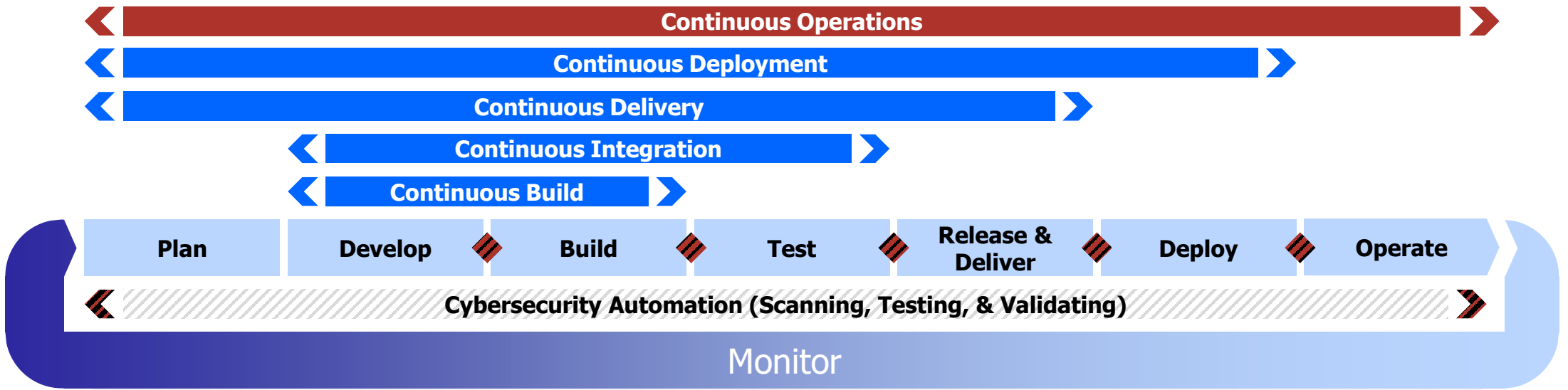


An architectural approach that attempts to **exploit the advantages of cloud architecture**, on bare metal or in a Cloud agnostic manner; a conscious focus on *how* the architecture is designed and deployed, over where it is deployed.





An architectural approach that accepts CSP lock-in to **exploit CSP managed services and technologies** to create cybersecurity hardened raw ingredients where further value-add activities occur further down the software supply chain.

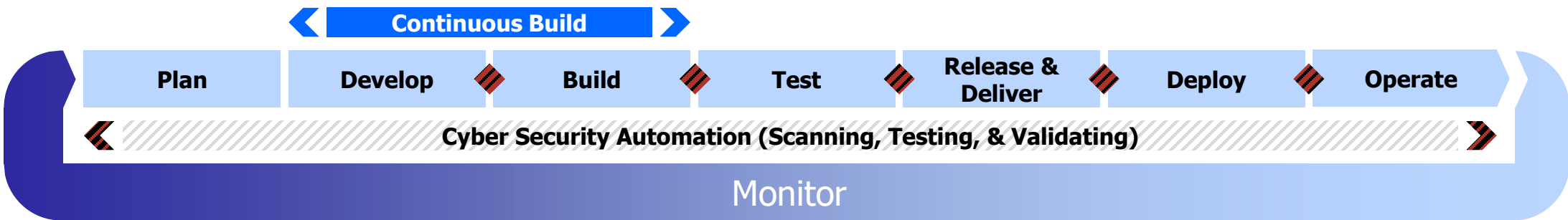
Collection of DevSecOps CI/CD pipelines, where each pipeline is dedicated to unifying people, automated processes, and relevant tools to create artifacts in support of a specific program(s) and/or mission set(s).

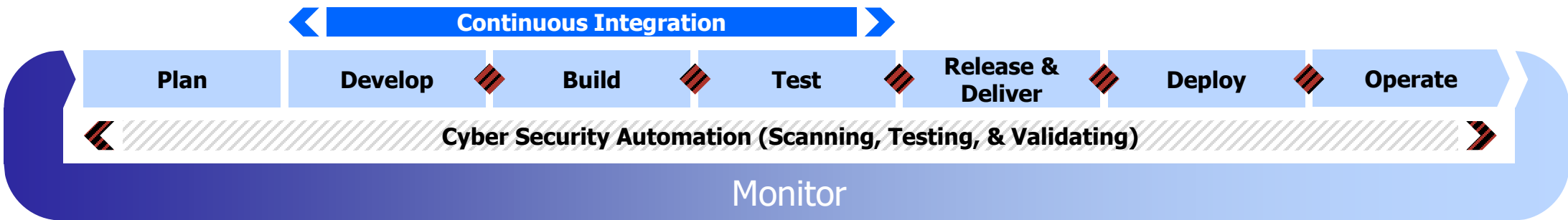


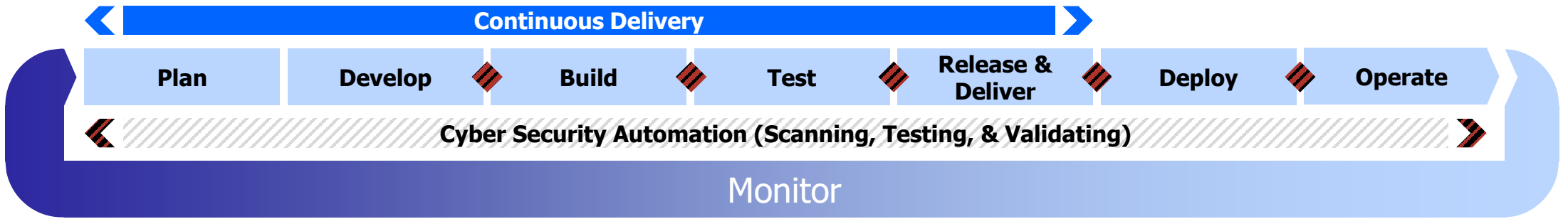


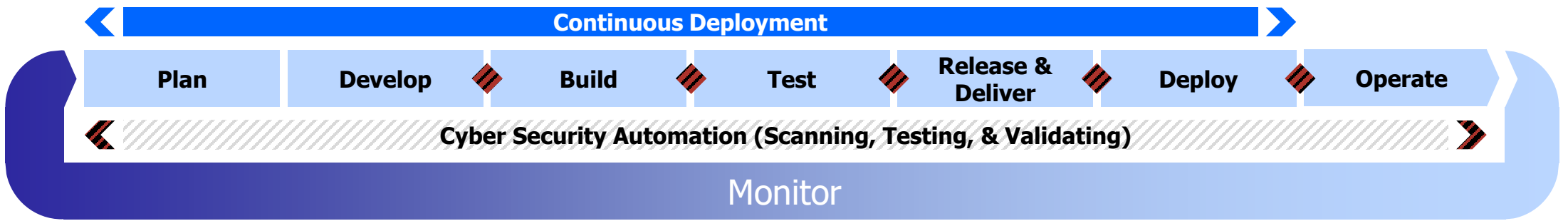
Legend

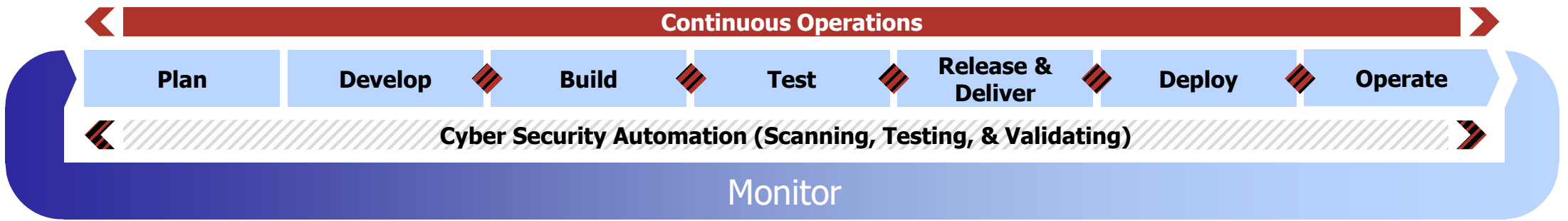
-  Control Gate
-  Risk Determination
-  Feedback Loop
-  Compliance, Effectiveness, ThreatCon, Malicious Detection

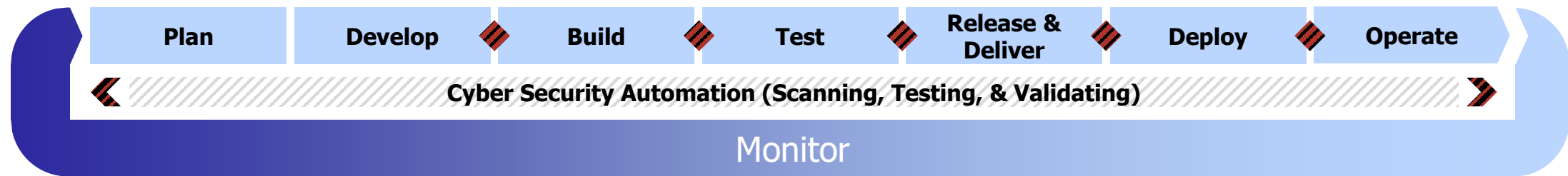


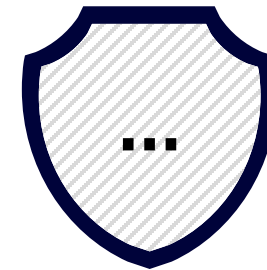
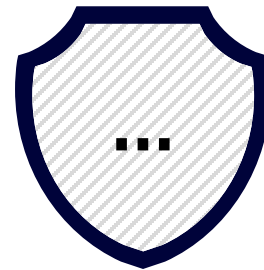
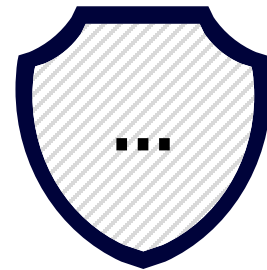


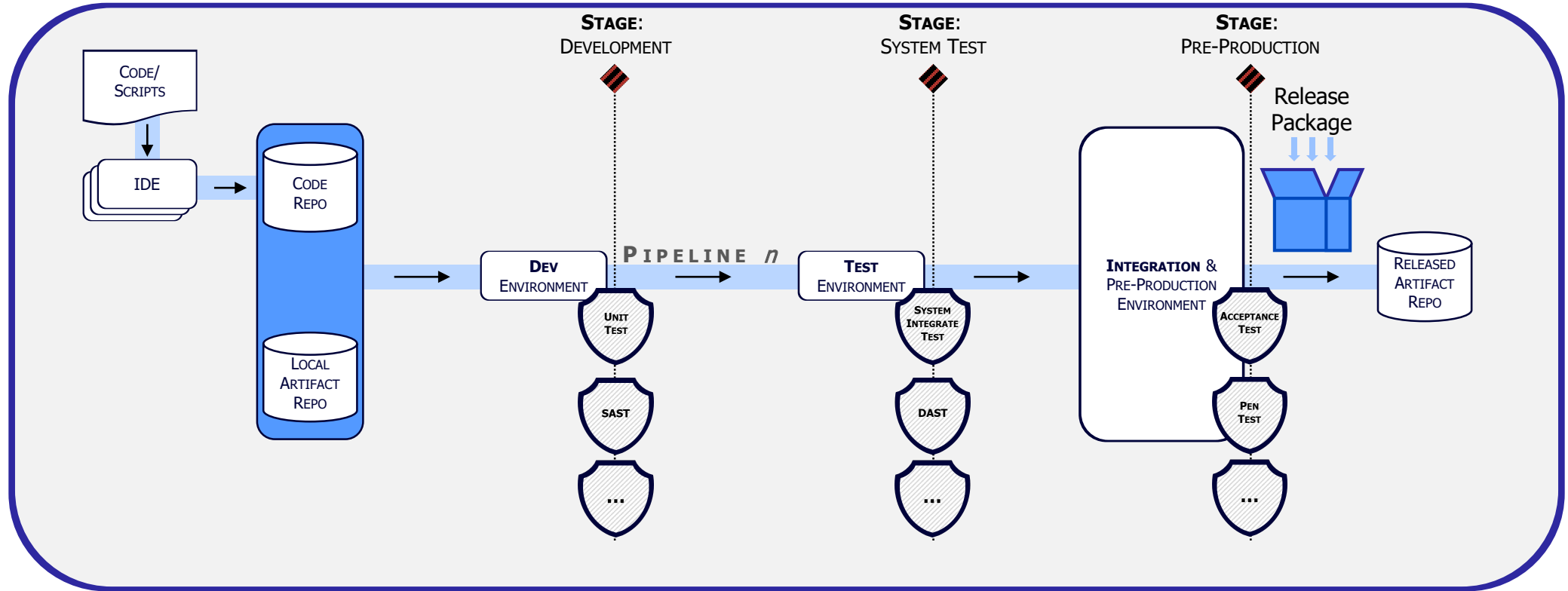


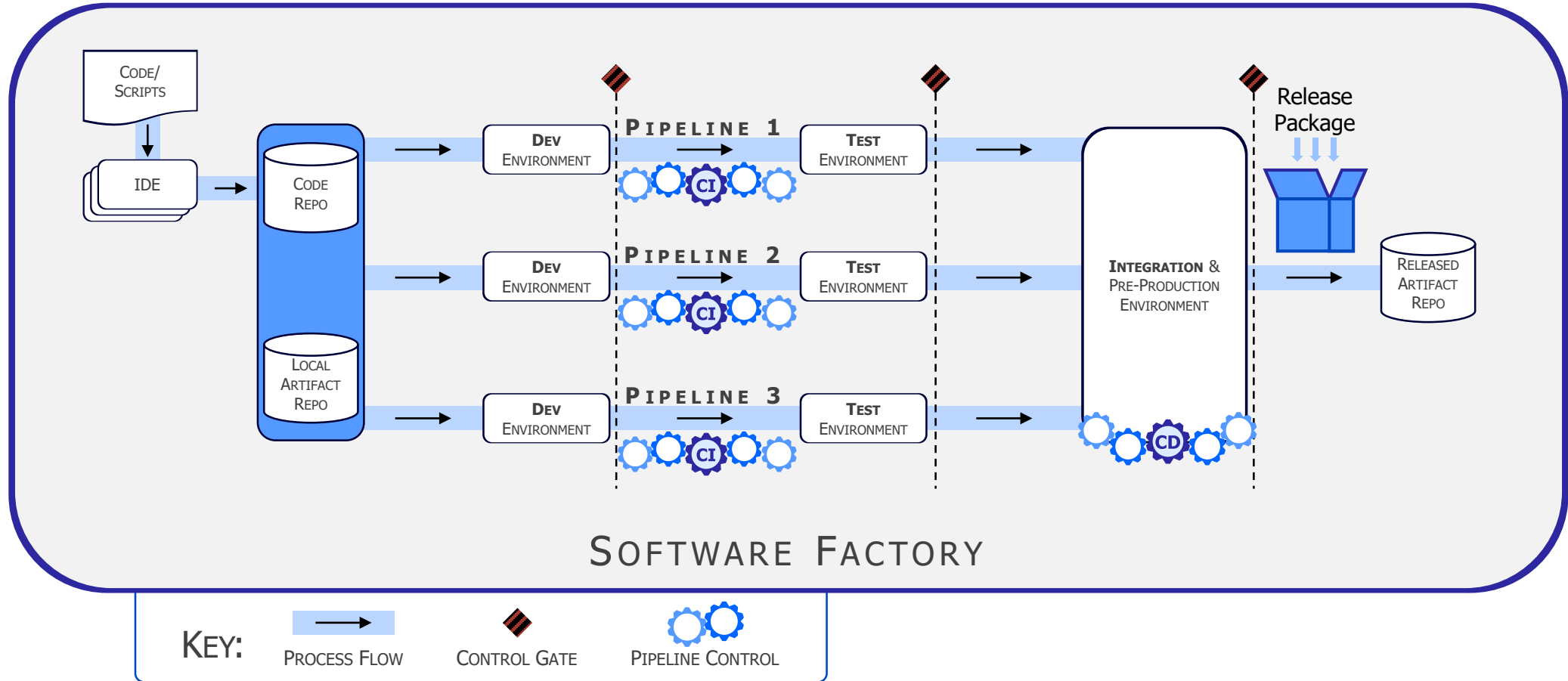


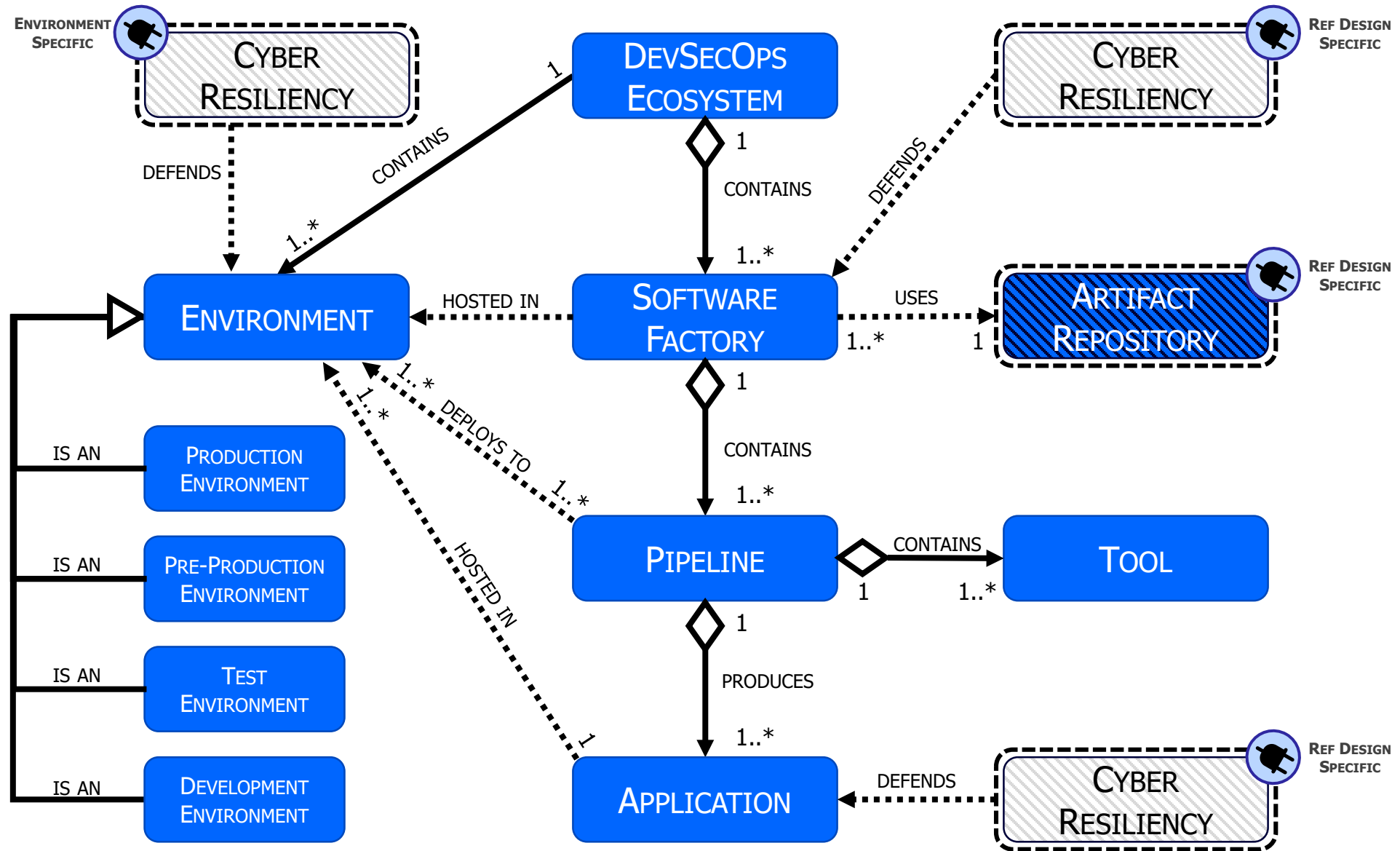












APPLICATIONS

APPLICATIONS

APP FRAMEWORK

PLATFORM / SOFTWARE FACTORY

CONTINUOUS MONITORING

- Compliance, Effectiveness
- ThreatCon, Malicious Detect

LOGGING

- Log Aggregation & Storage
- Log Analysis & Display

CI/CD PIPELINES

- IaC Defined SW Factory
- DevSecOps Tools

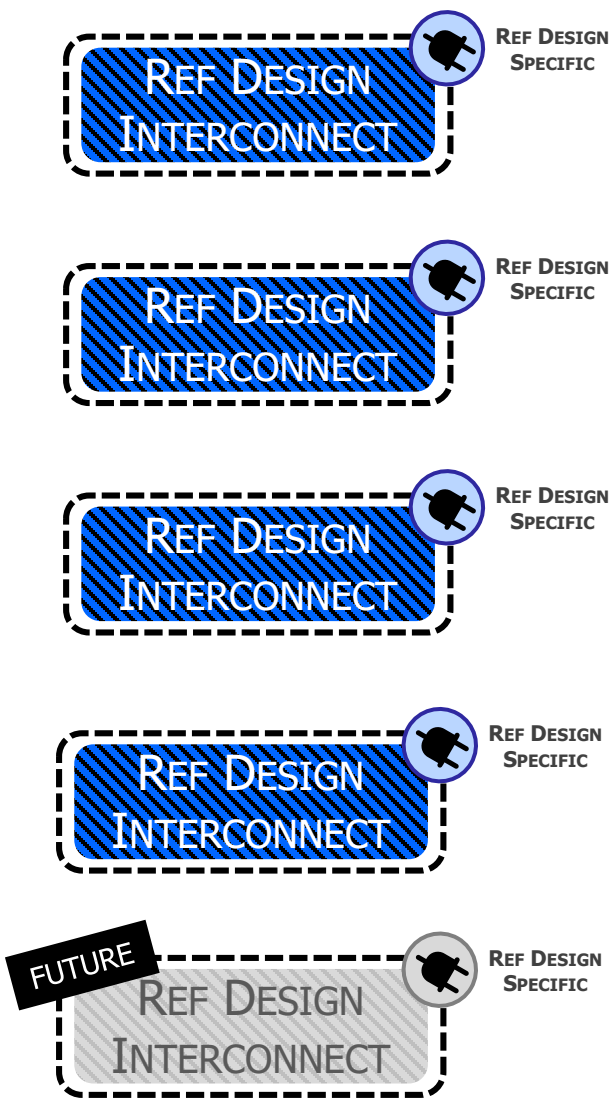
ENVIRONMENTS

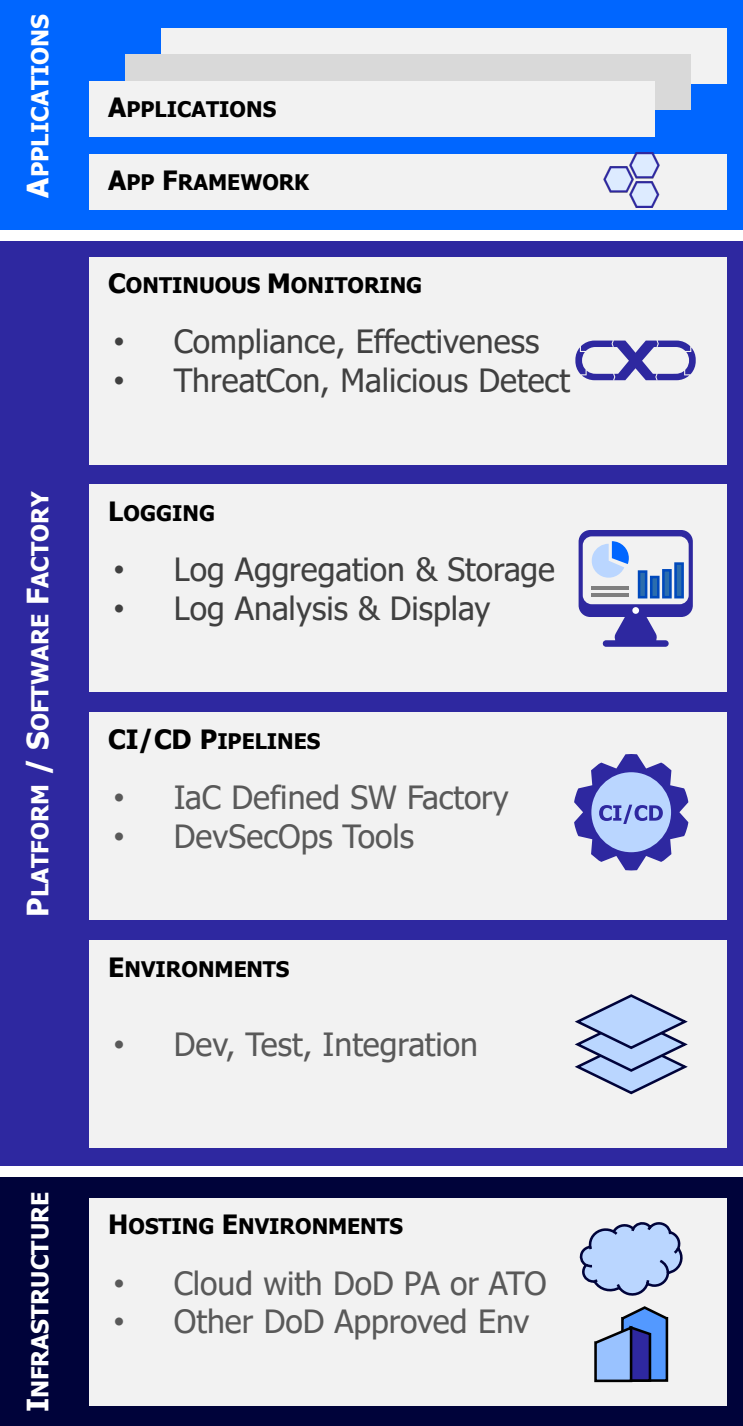
- Dev, Test, Integration

INFRASTRUCTURE

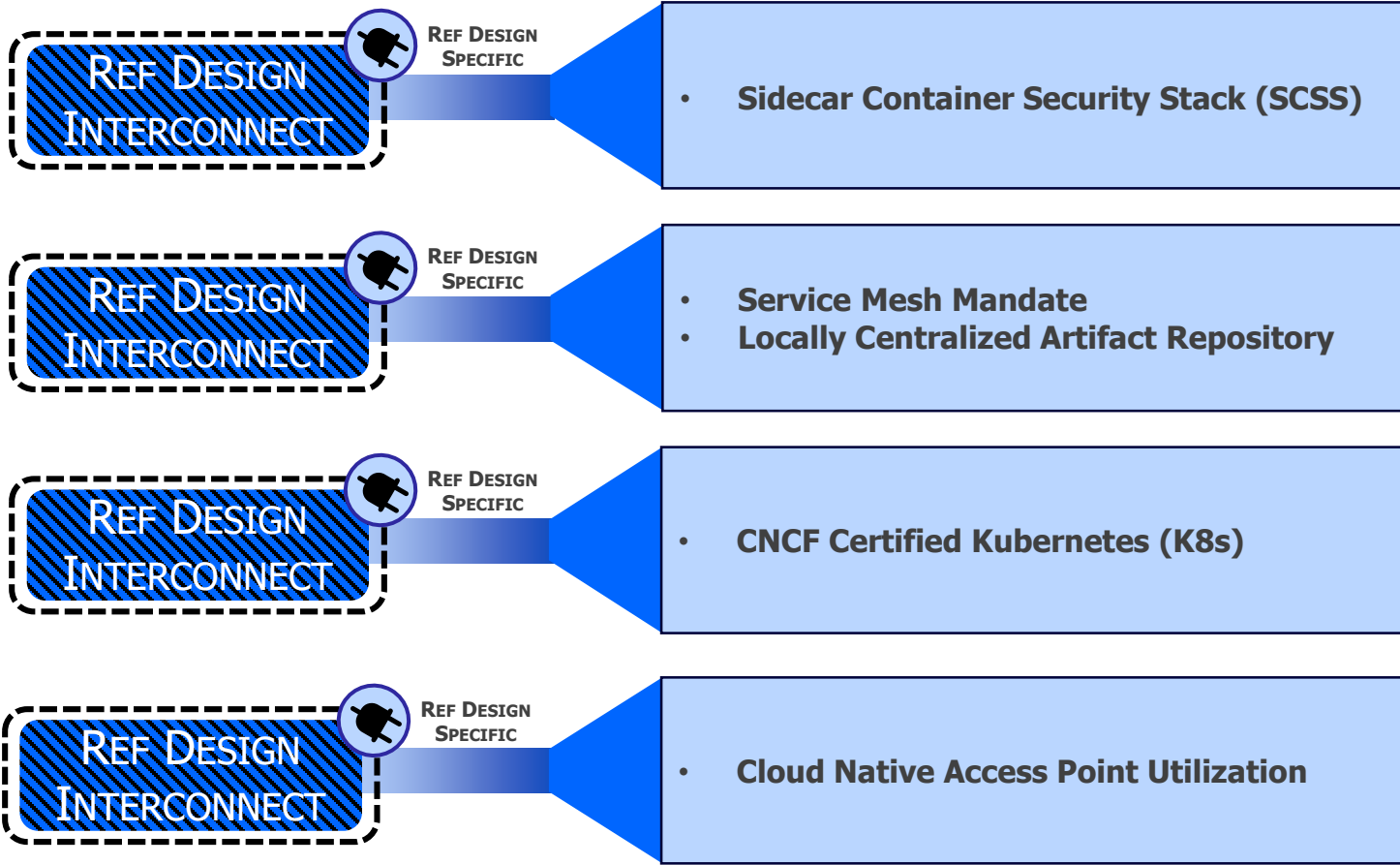
HOSTING ENVIRONMENTS

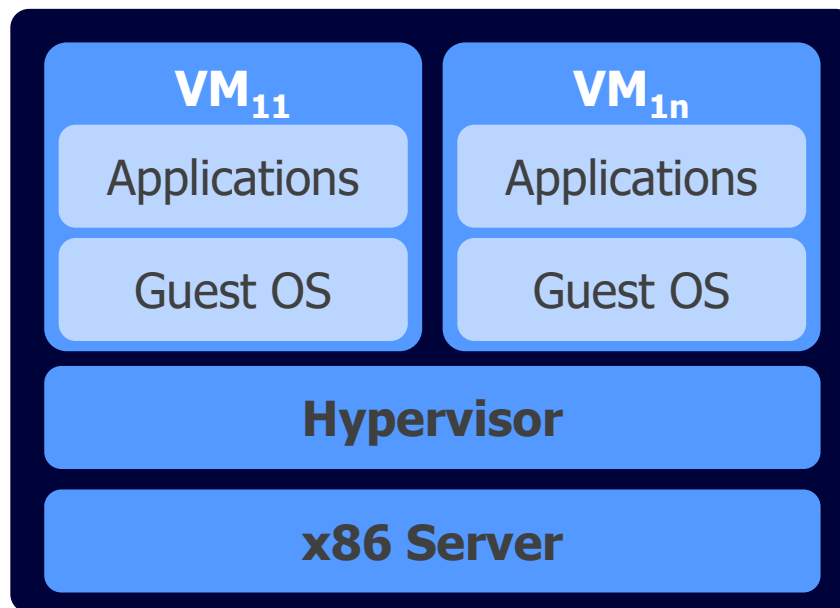
- Cloud with DoD PA or ATO
- Other DoD Approved Env

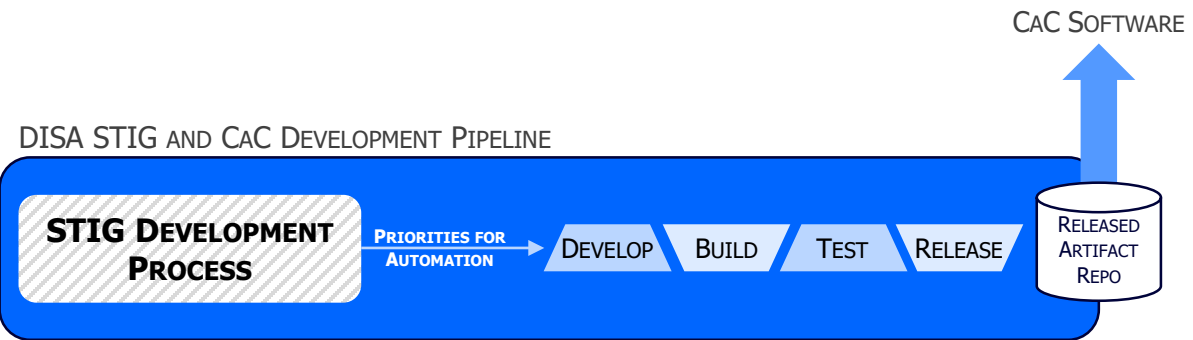


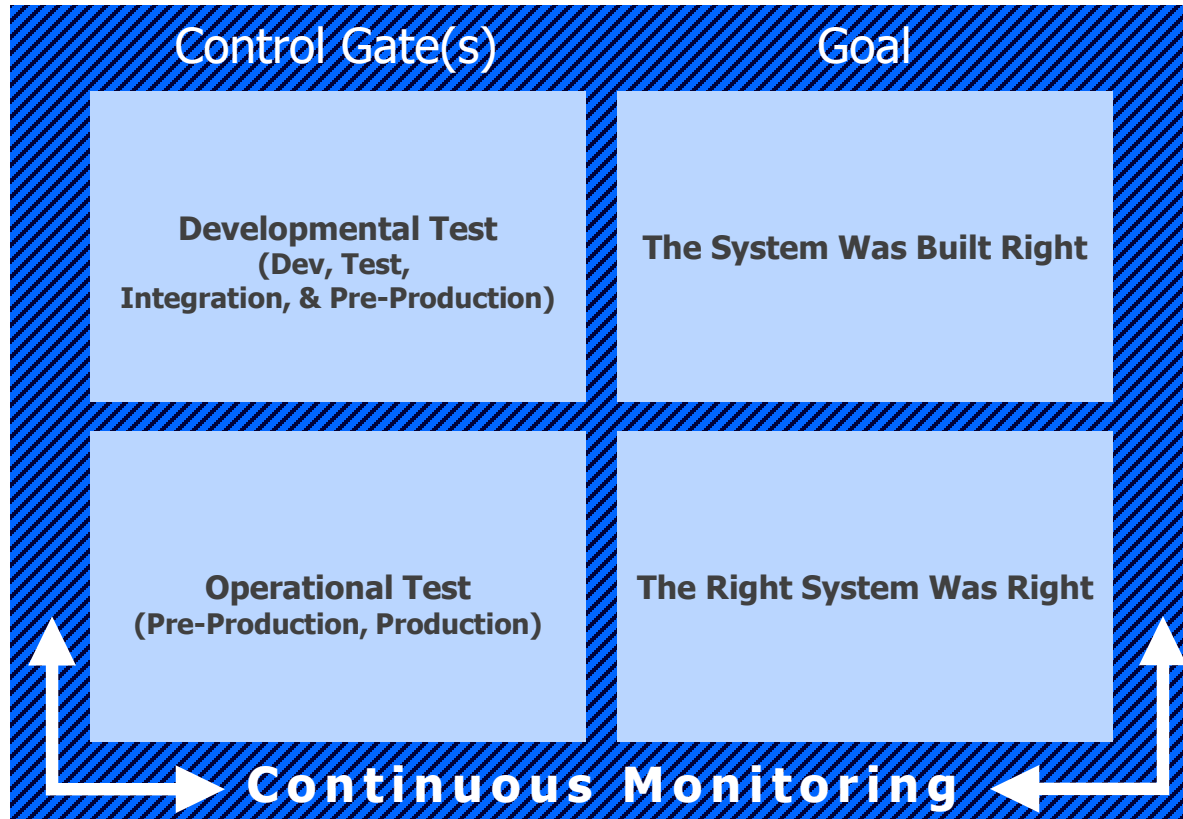


DoD Enterprise DevSecOps Reference Design: CNCF Certified Kubernetes

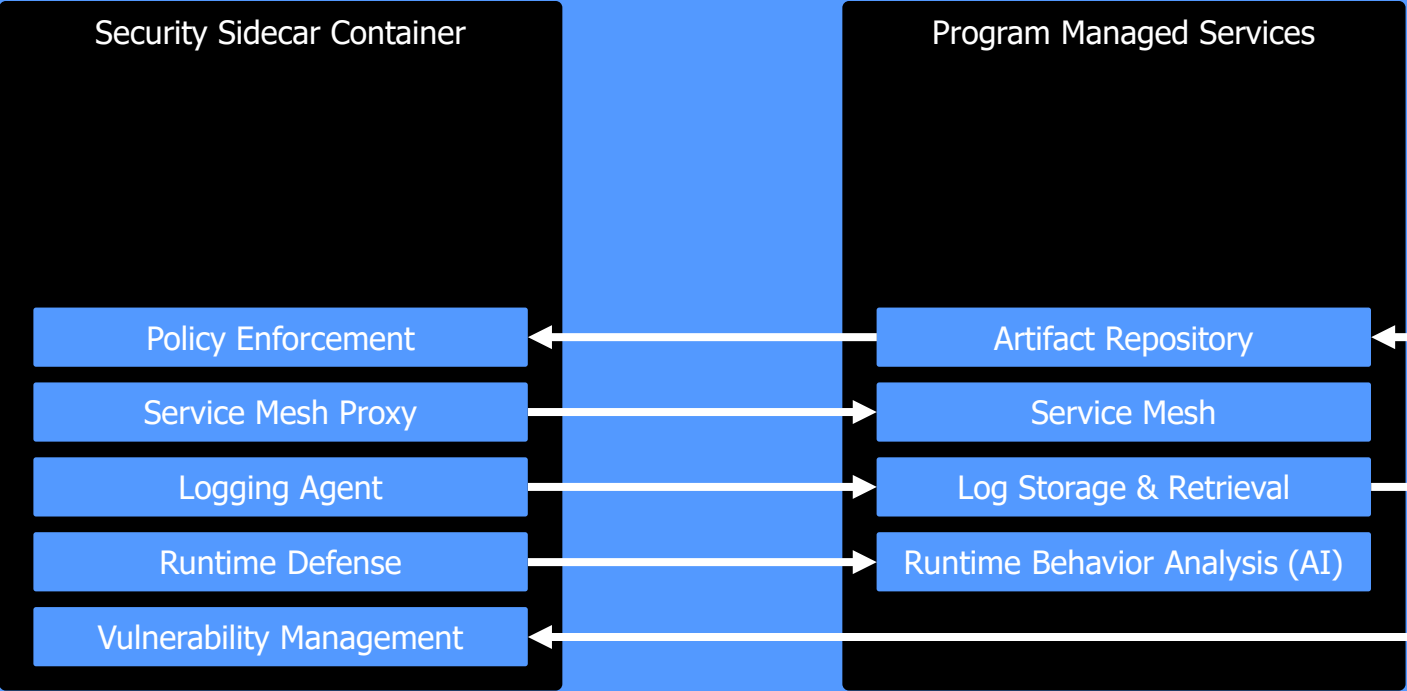




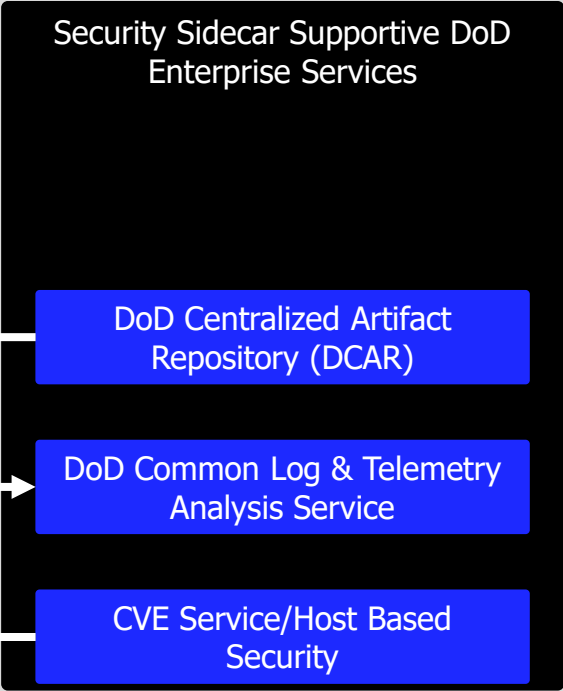




Sidecar Container Security Stack (SCSS)



DoD Enterprise Cloud



Hosting Environment



DoD Cloud



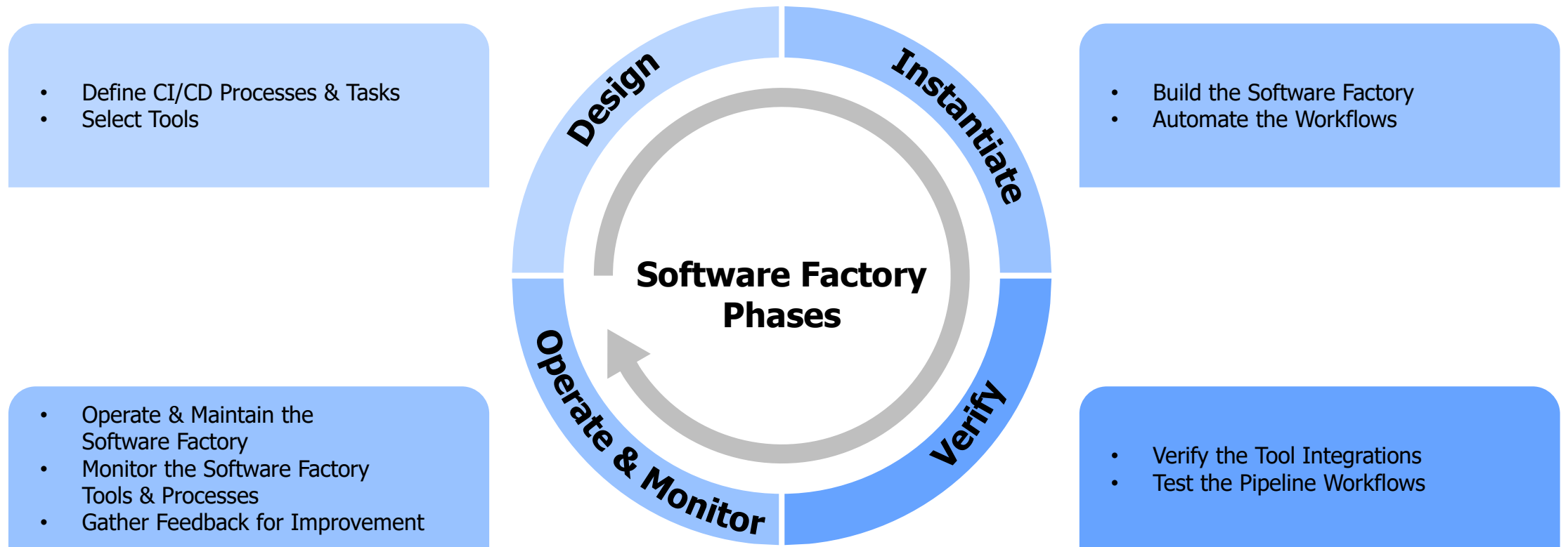
DoD Data Center(s)

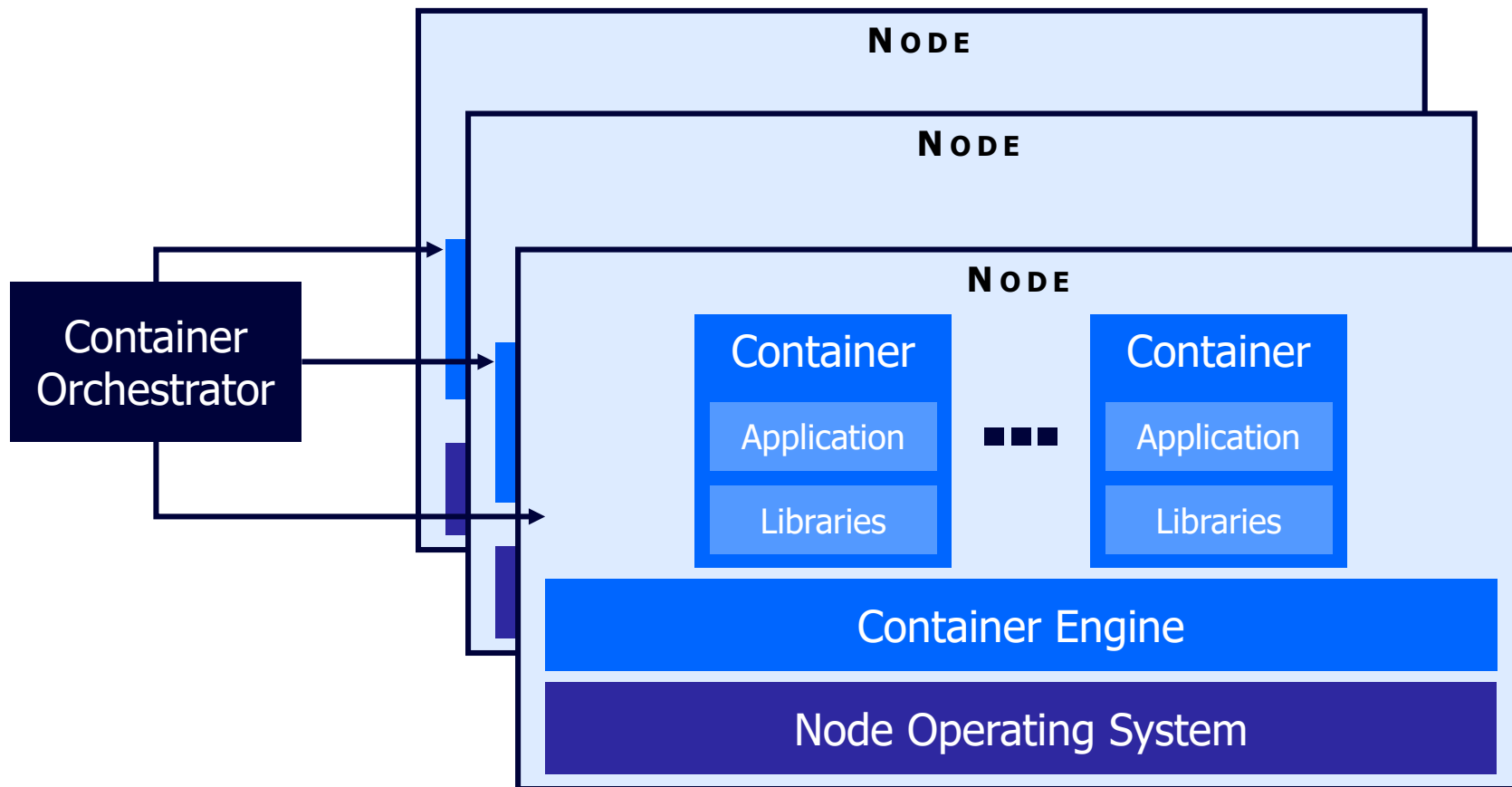


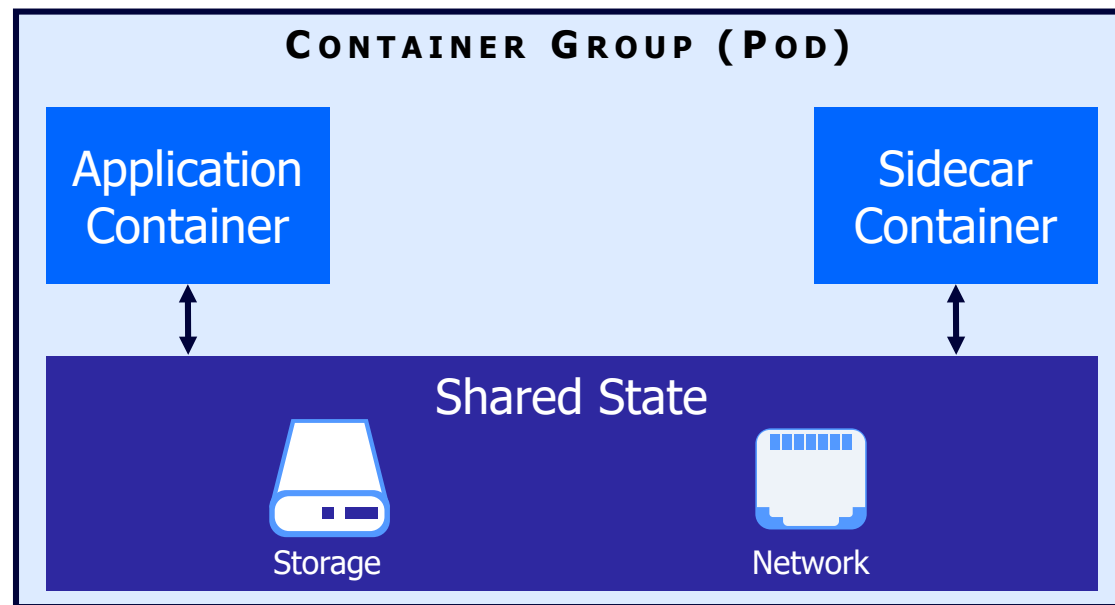
Bare Metal Server(s)

Legend

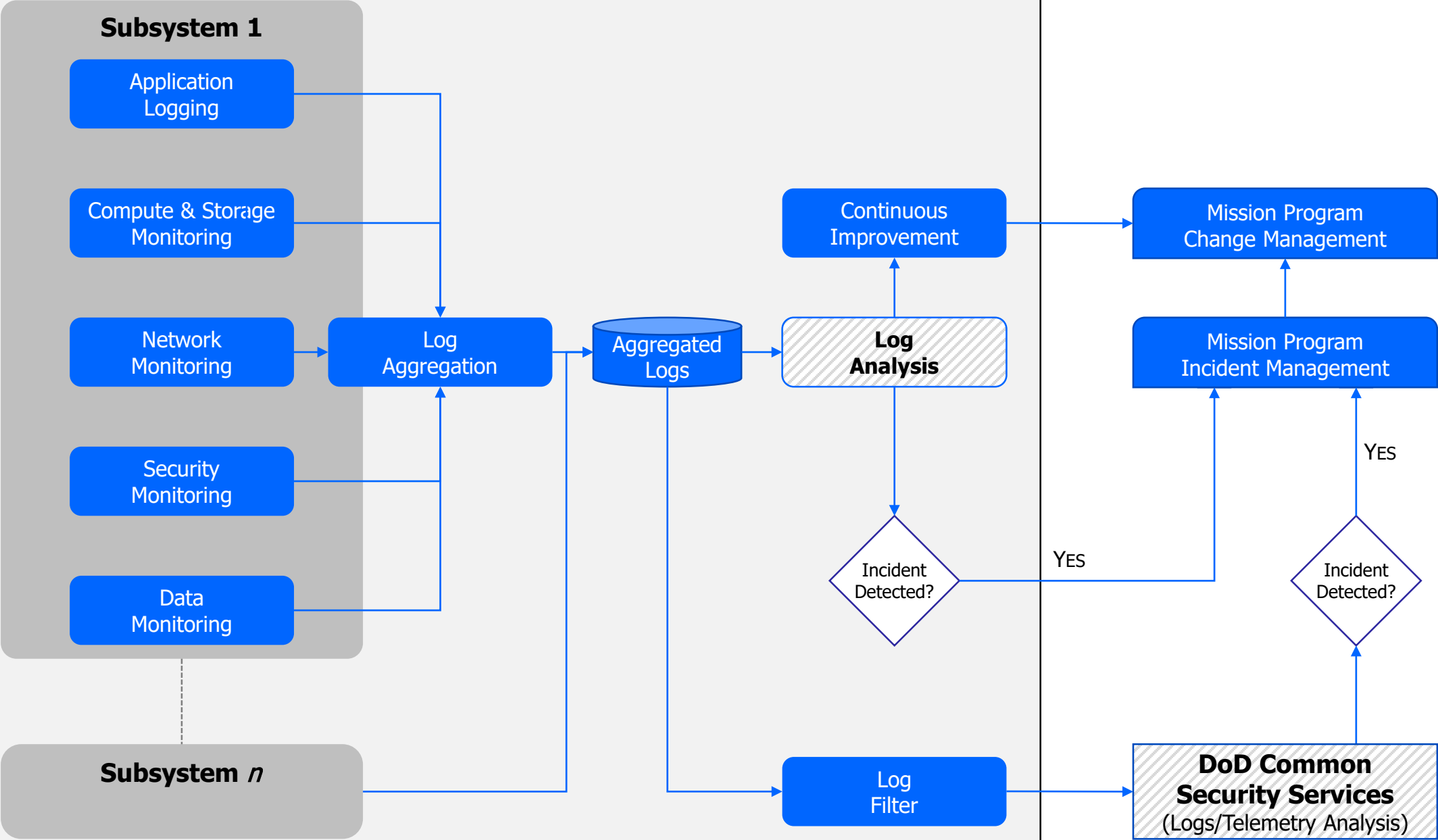
- DoD Provided Enterprise Service
- DoD Provided, Program Instantiated

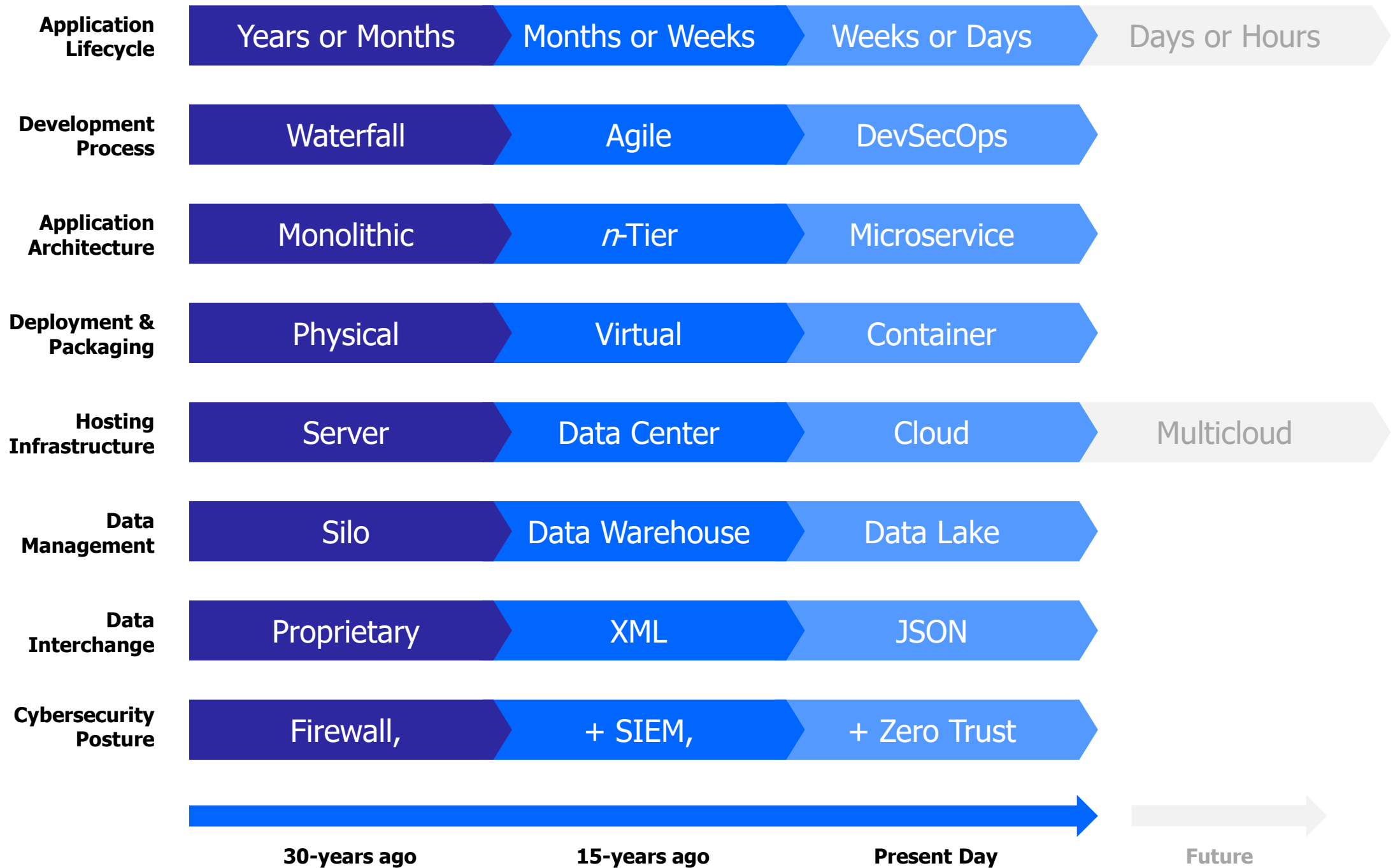


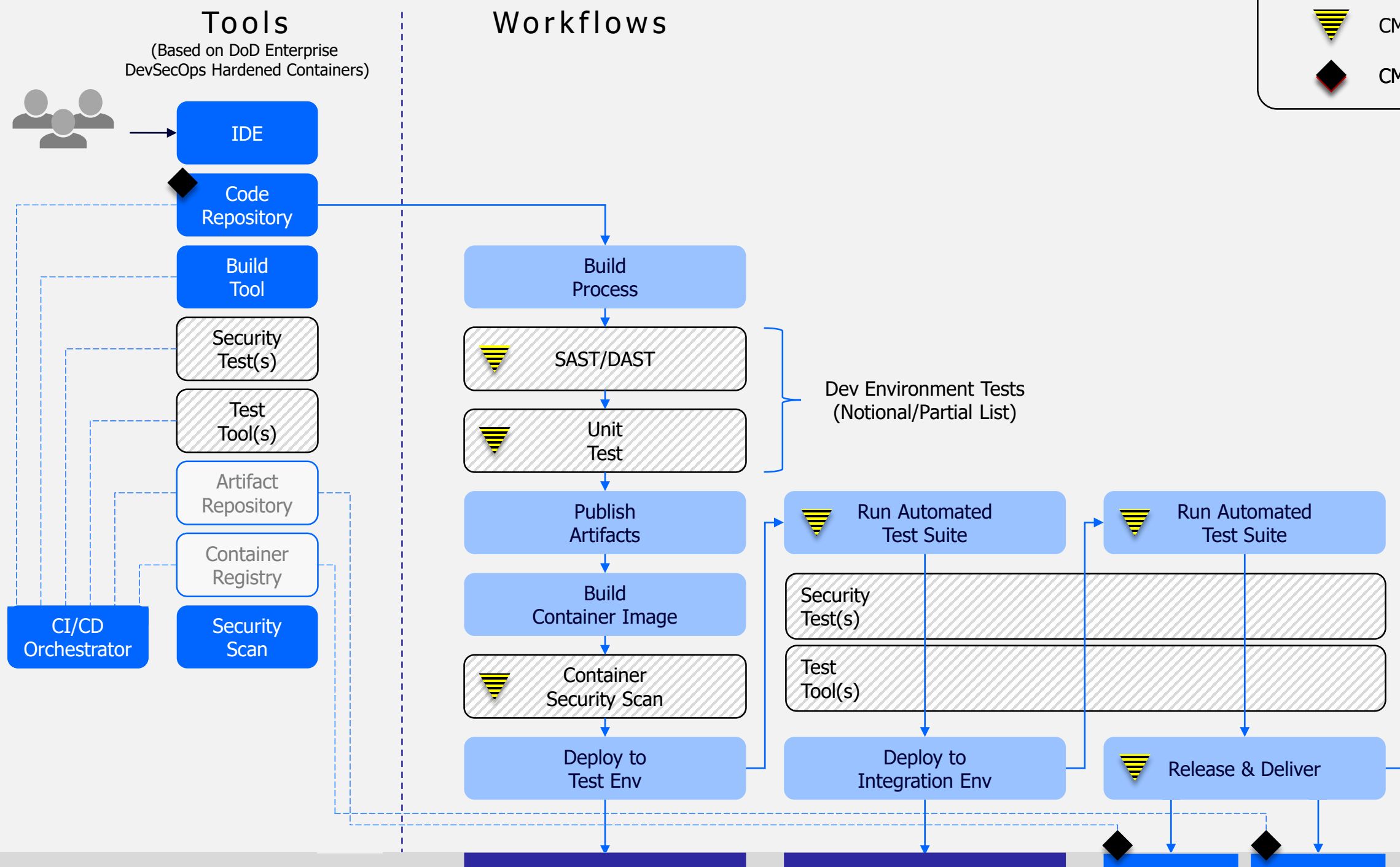


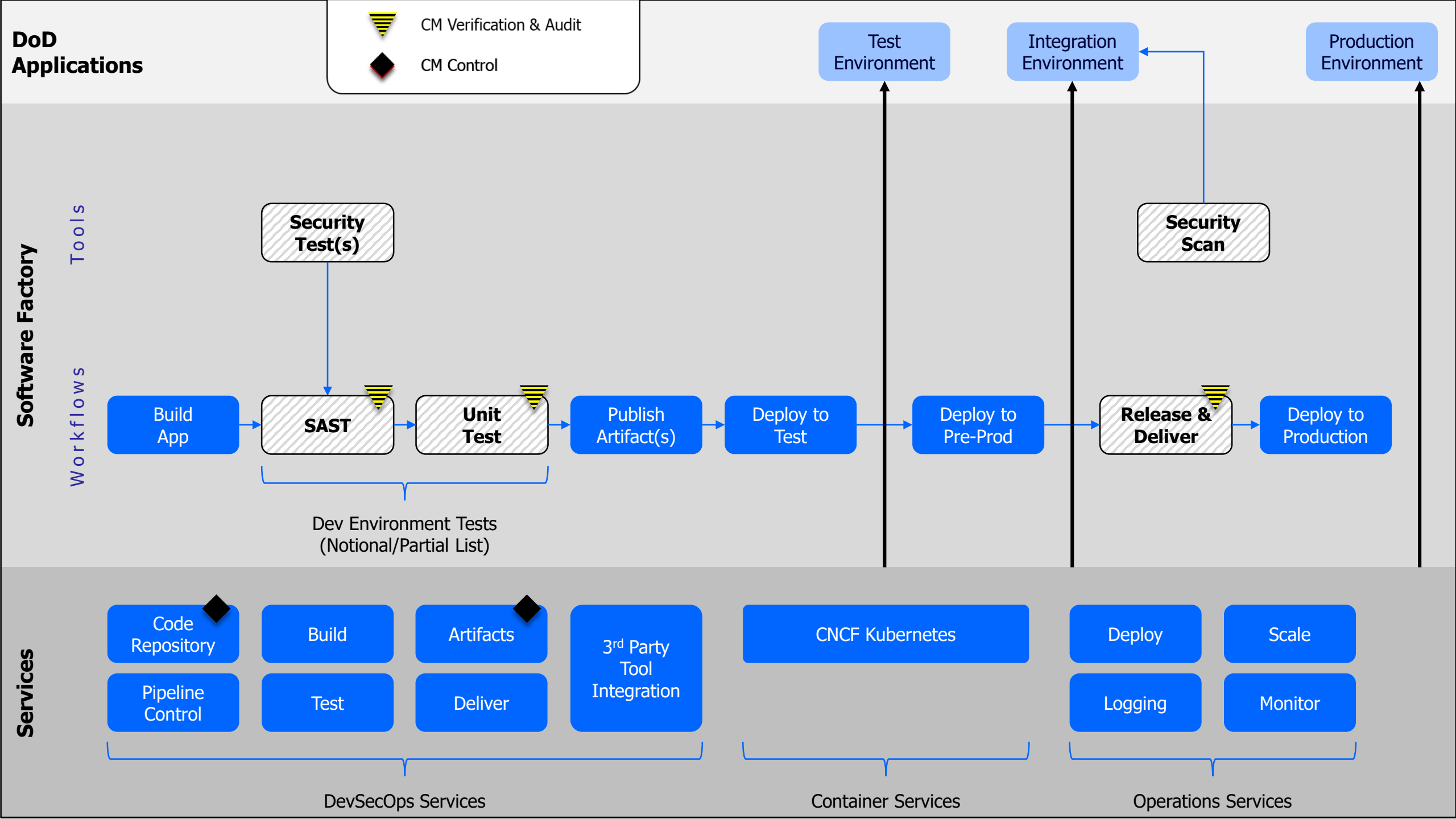


Mission Program Application Platform









Continuous Delivery

- Use a source code repo for all production artifacts
- Use trunk-based development methods
- Shift left on security
- Implement test automation
- Implement continuous integration
- Support test data management
- Implement continuous delivery
- Automate the deployment process

Architecture

- Use loosely coupled architecture
- Architect for empowered teams

Cultural

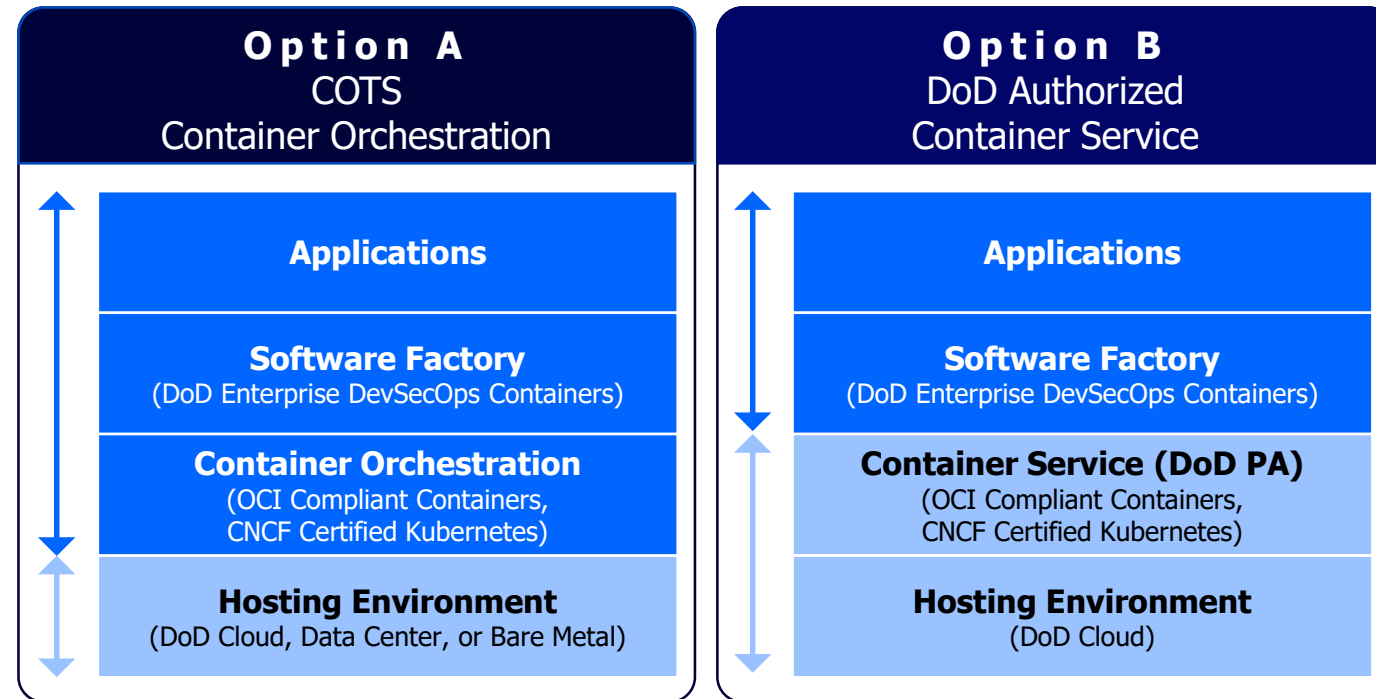
- Adopt a Likert scale survey to measure cultural change progress
- Encourage and support continuous learning initiatives
- Support and facilitate collaboration among and between teams
- Provide resources and tools that make work meaningful
- Support or embody transformational leadership

Product & Process

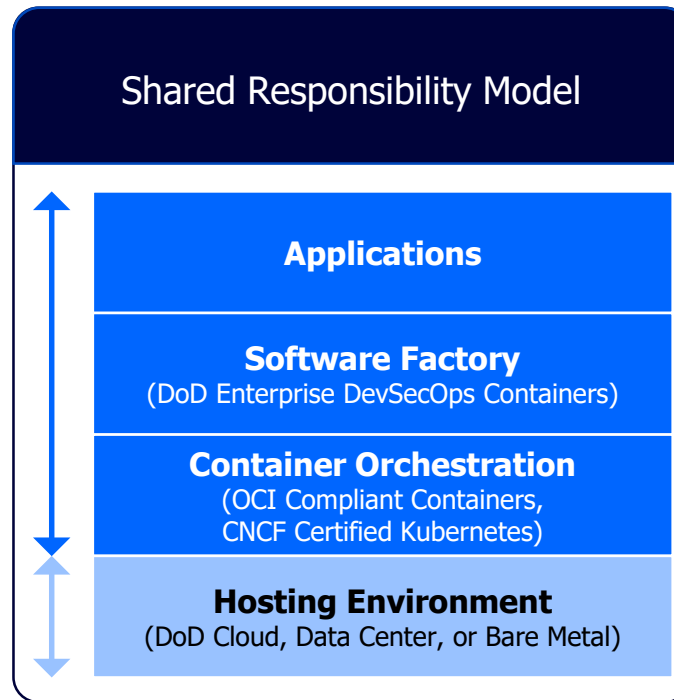
- Gather and implement customer feedback
- Make the flow of work visible through the value stream
- Work in small batches
- Foster and enable team experimentation

Deployment

- Have a lightweight change approval process



- Mission Program Responsibility & Managed Components
- Hosting Environment Provider Responsibility & Managed Components



Mission Program Responsibility & Managed Components



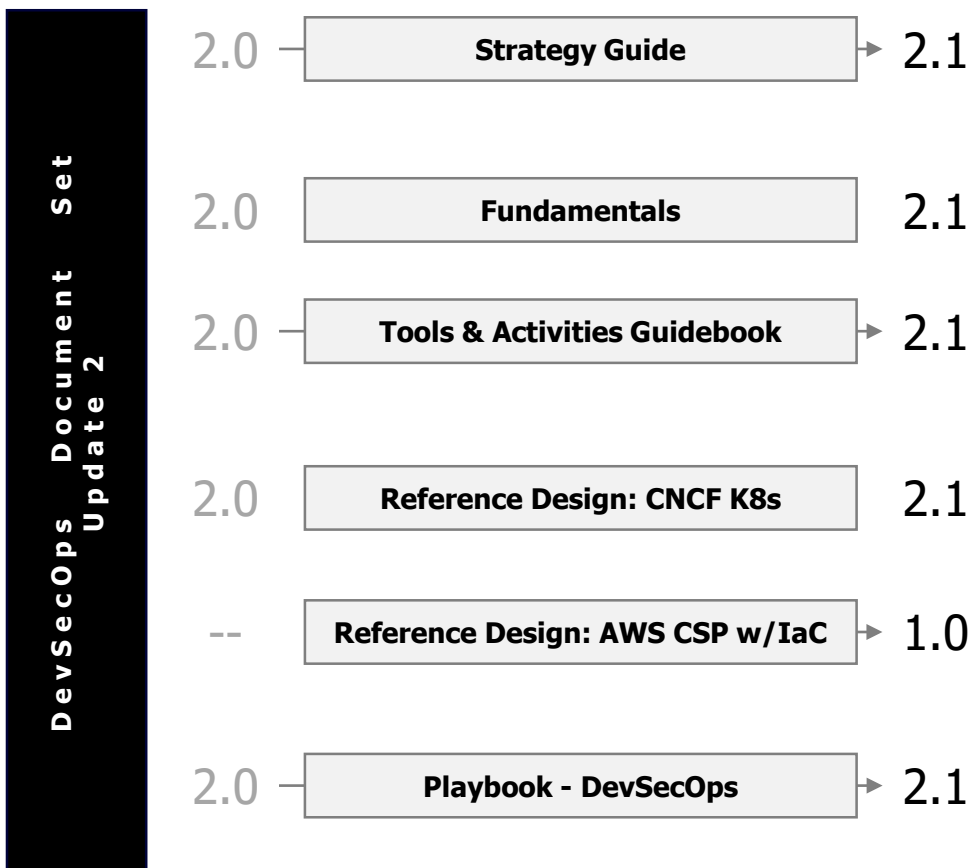
Hosting Environment Provider Responsibility & Managed Components

SECURE SOFTWARE DETECTS AND RESISTS
CYBERATTACKS, OFFERING THE
WARFIGHTER A QUANTIFIED DEGREE OF
CYBER SURVIVABILITY



STABLE SOFTWARE PERFORMS WELL
WITHOUT BREAKING OR CRASHING, &
DYNAMICALLY SCALES TO MATCH
DEMAND

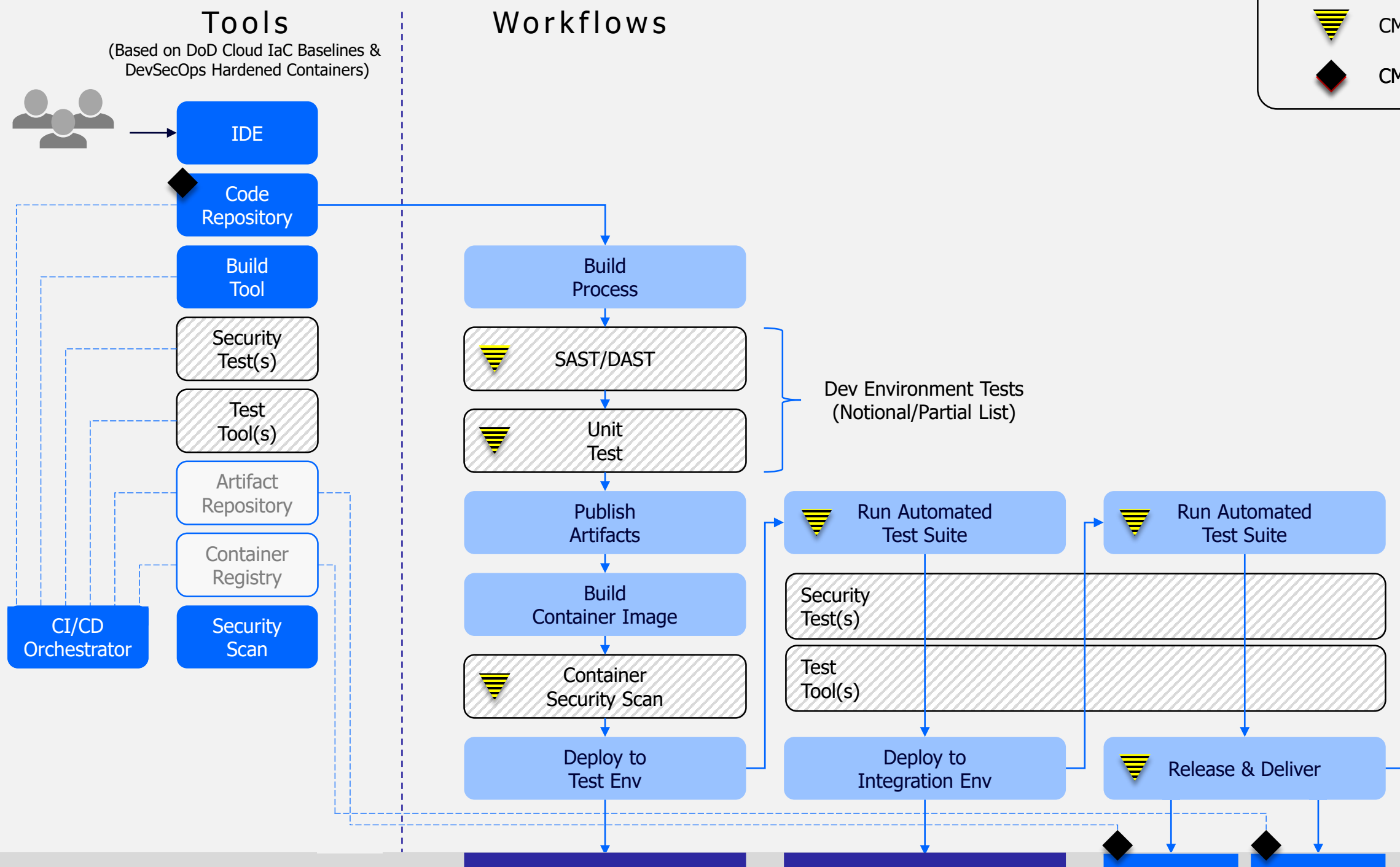
QUALITY SOFTWARE MAXIMIZES USER
REQUESTED FEATURE SETS AND
MINIMIZES FUNCTIONAL DEFECTS

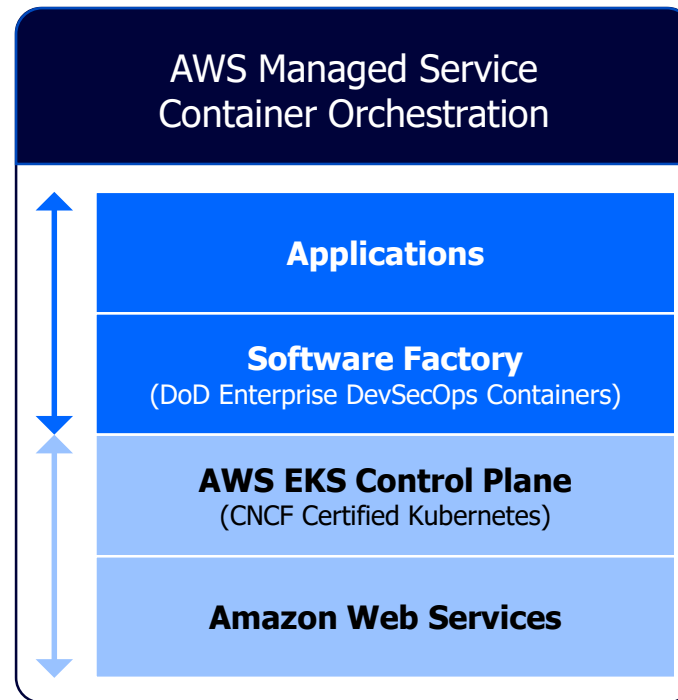




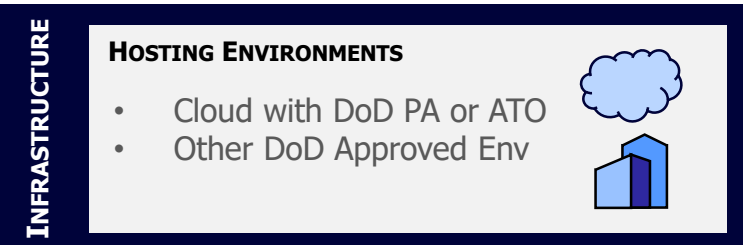
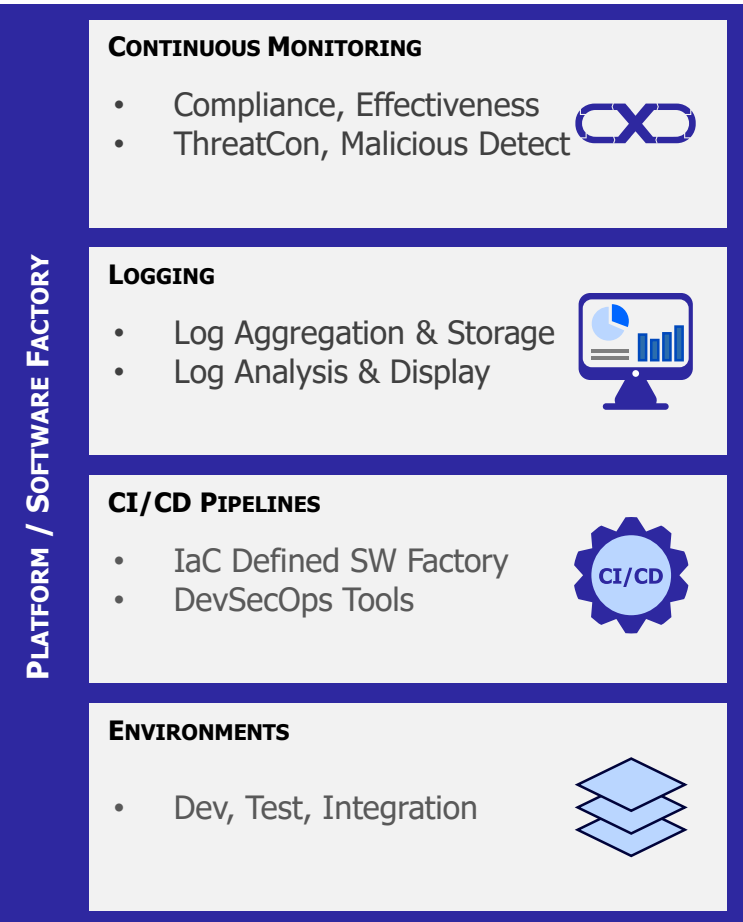
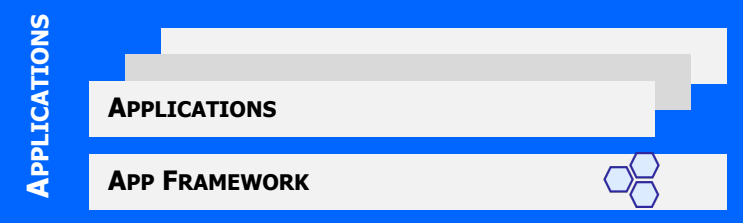
"DoD should modify its processes to mimic industry's best practices rather than try to contract for and maintain customized software."

(Defense Innovation Board, *Software is Never Done*, May 2019)

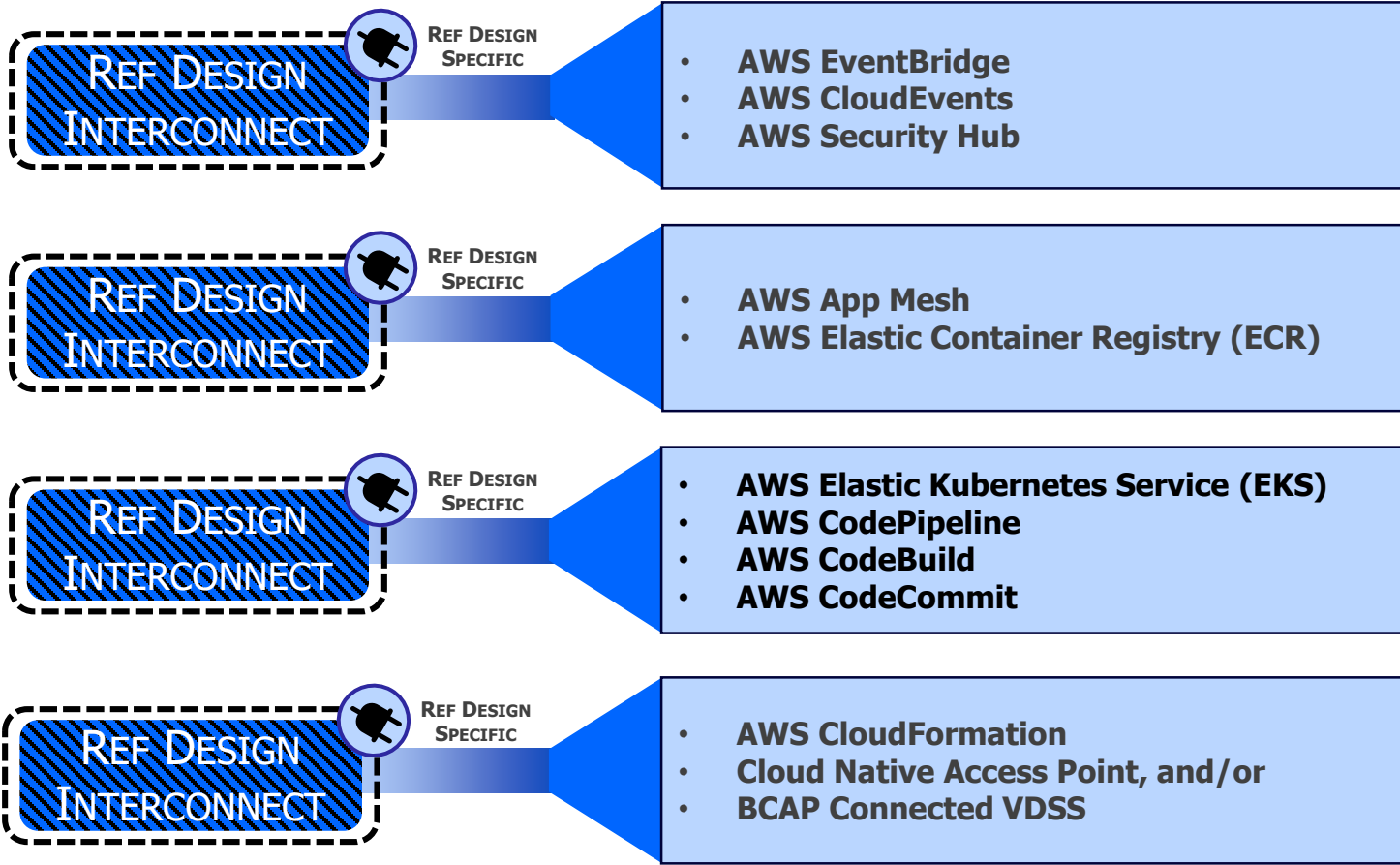


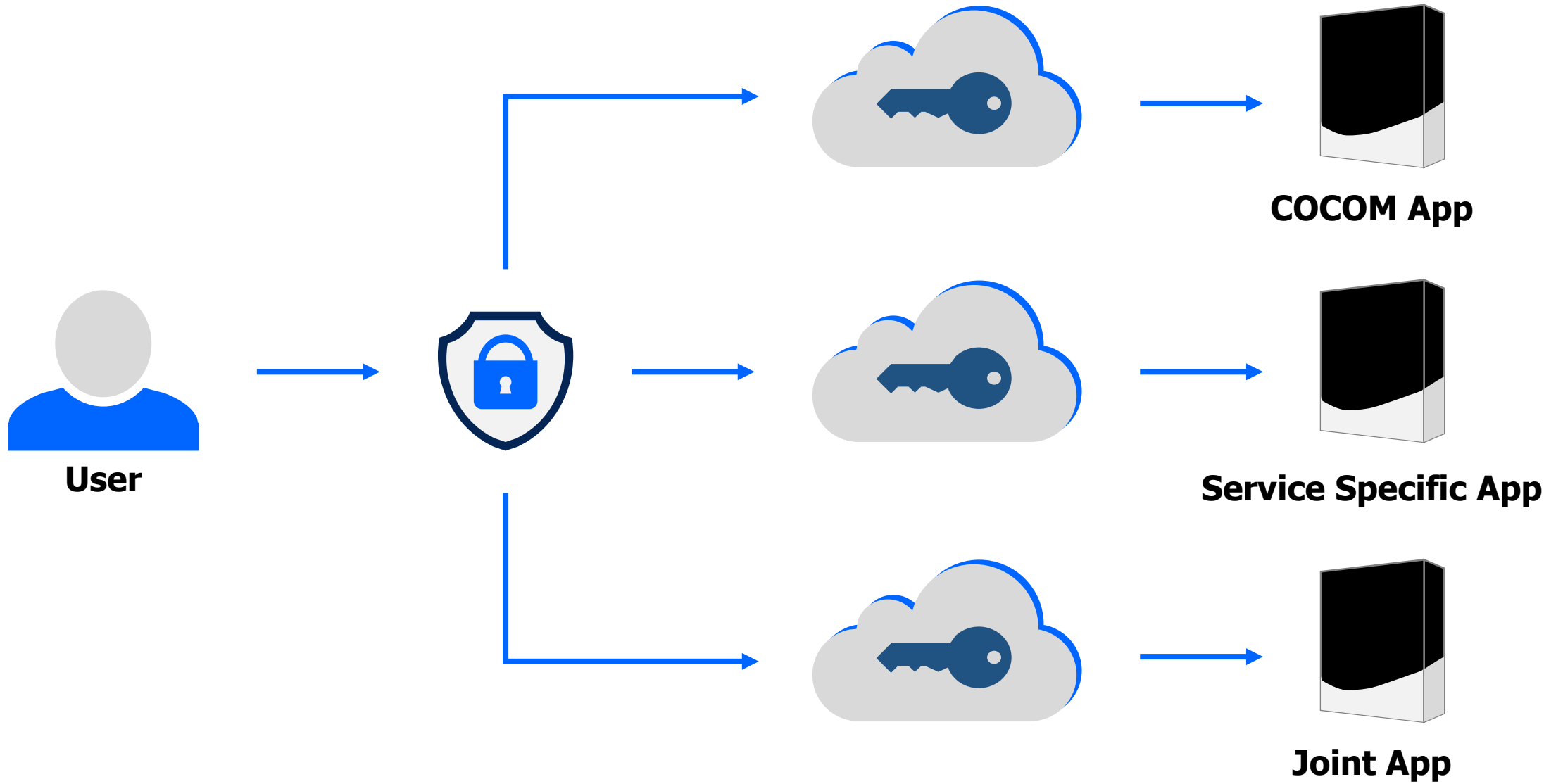


- Mission Program Responsibility & Managed Components
- Hosting Environment Provider Responsibility & IaC Provisioned Managed Components

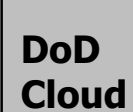


DoD Enterprise DevSecOps Reference Design: AWS Managed Services

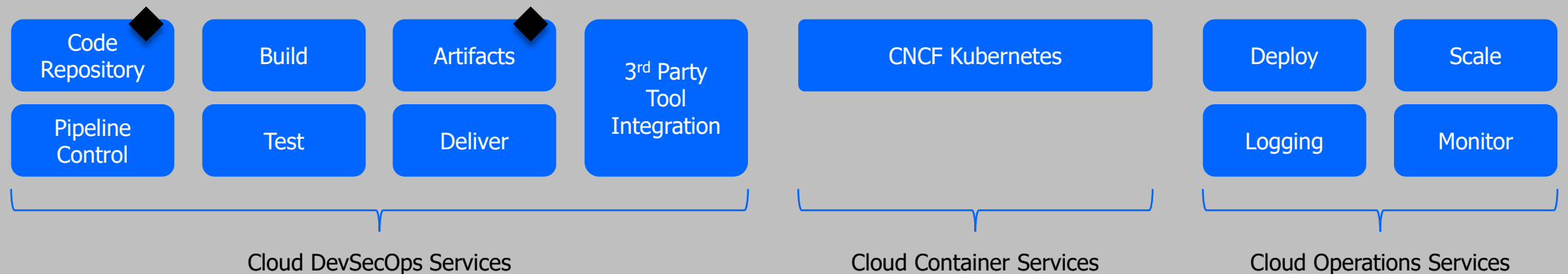


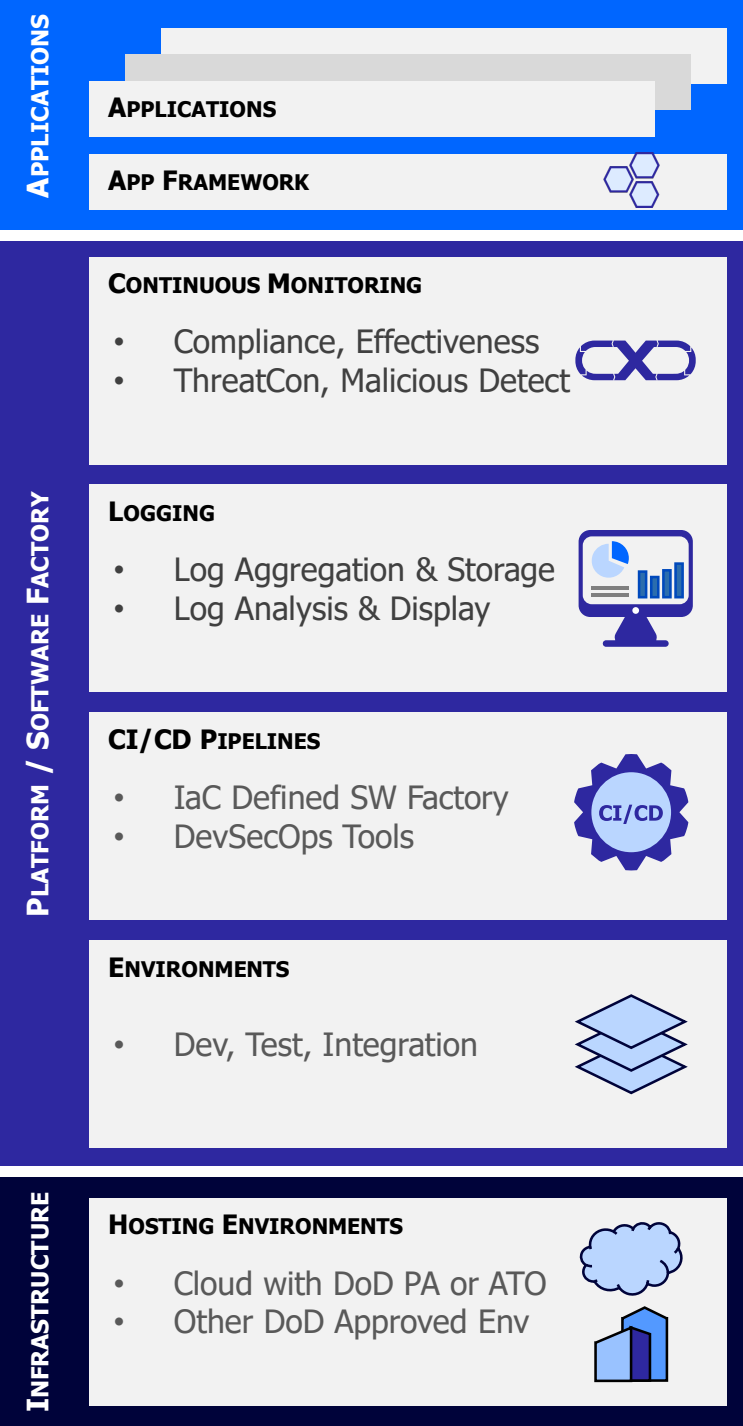


Software Factory

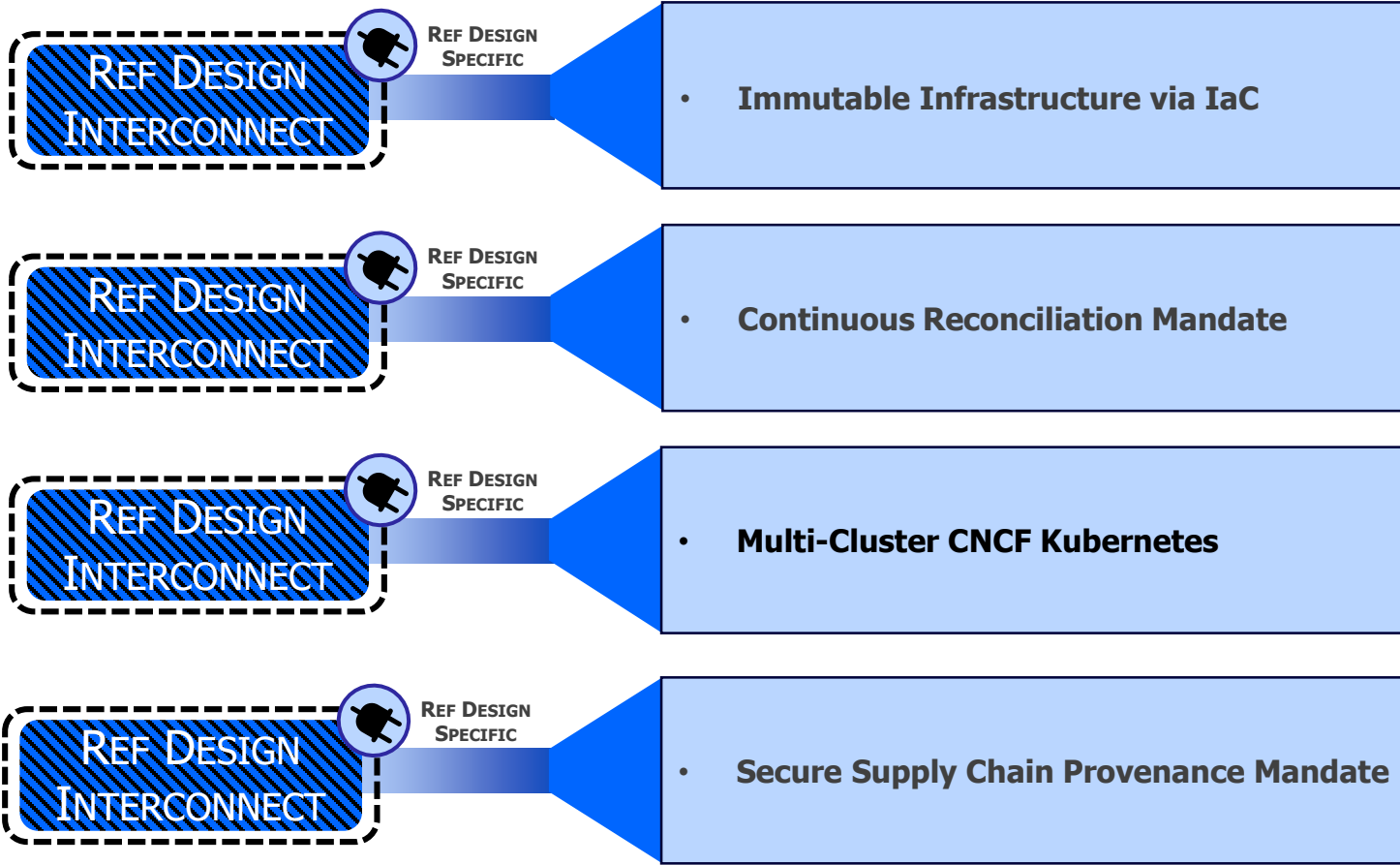


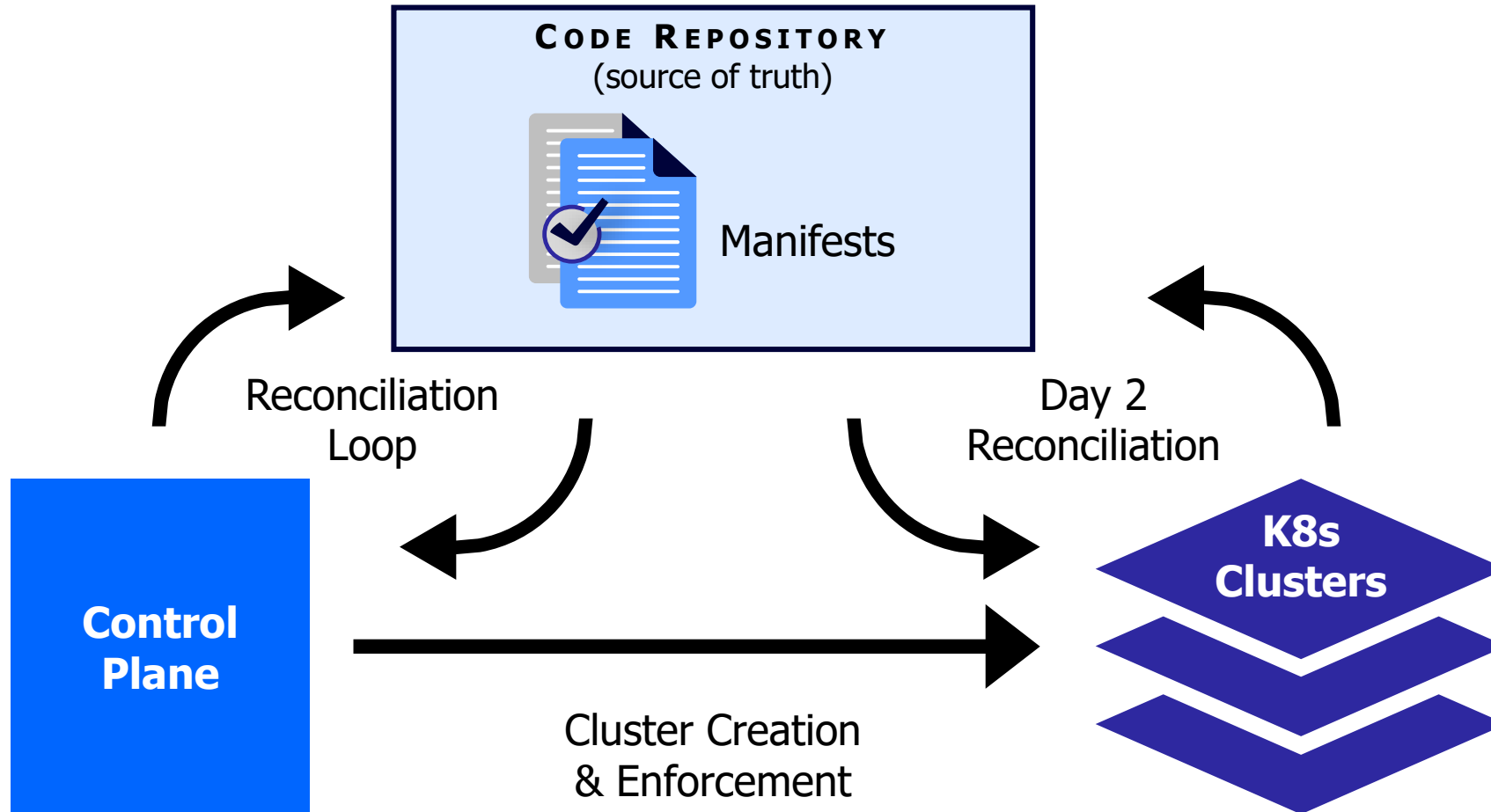
**CSP
w/PA**

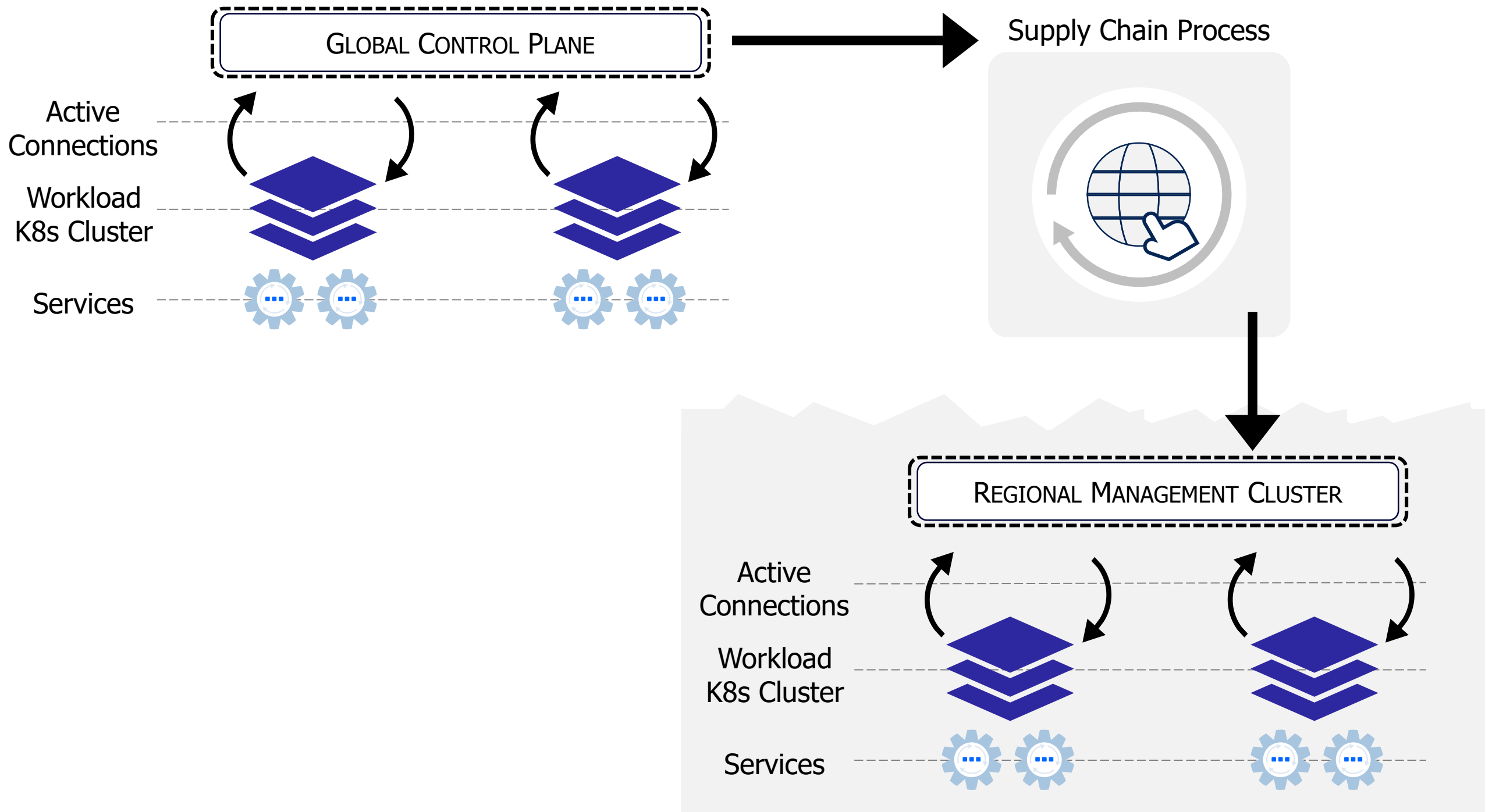




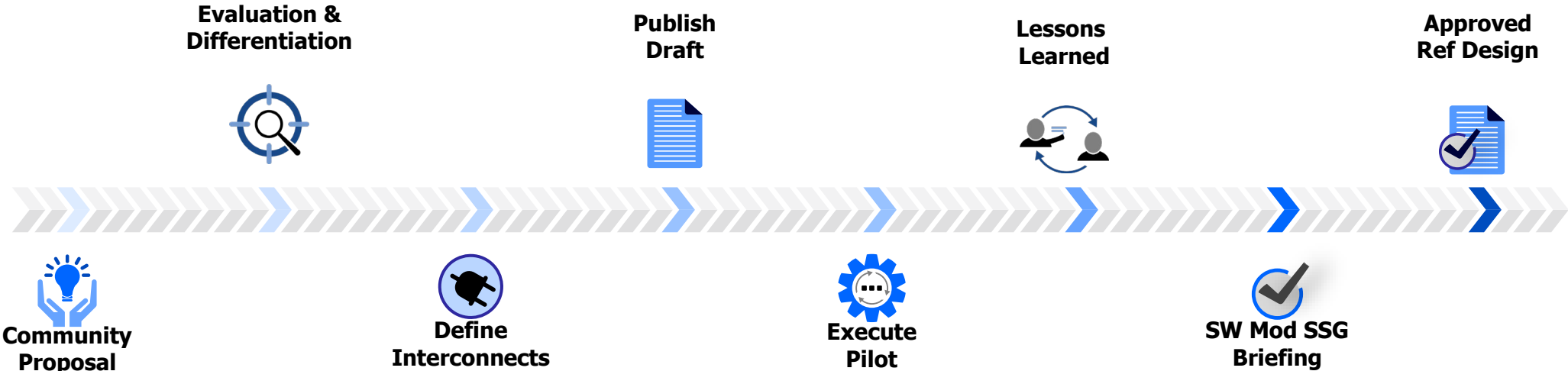
DoD Enterprise DevSecOps Reference Design: Multi-Cluster CNCF Kubernetes







Pathway to DevSecOps Reference Design



Pathway to DevSecOps Reference Design

