DoD Enterprise DevSecOps

Pathway to a Reference Design

September 2021

Document Set Version 2.1

Pathway to a Reference Design

There is no singularity in software architecture. There are many different ways to construct productive, resilient, and secure software factories. Further, the ebb and flow of software architecture and innovative tooling creates an ever-changing landscape that makes today's best practice a risk to be mitigated tomorrow. This document captures the *Pathway to a Reference Design*. It solicits best practices, innovative and differentiating software factory architectures, and captures the requisite steps necessary to produce a vetted software factory reference design.

Every developer, cybersecurity, and operations (DevSecOps) reference design (Ref Design) begins with a community proposal or demand signal and travels a specific journey before becoming an approved design. That pathway is depicted in Figure 1.

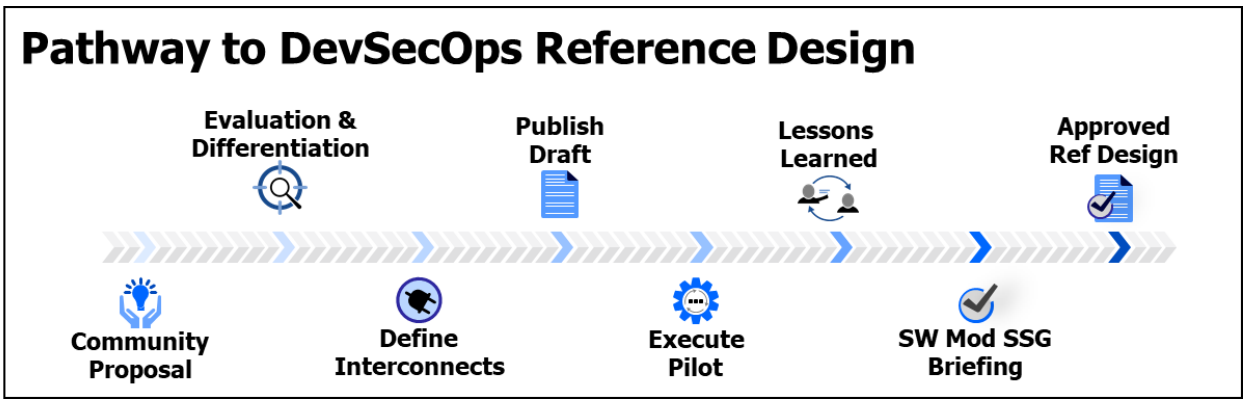

Figure 1: Eight step journey from Community Proposal to Approved DevSecOps Reference Design

Community Proposal

Ideas and demand generation for new DevSecOps software factory reference designs originate from the DOD software community. A good proposal can start with simply asking "What if…" in conversation, email, Teams, etc. There is no expectation for formal proposals, but every proposal should clearly articulate how it differs from existing published draft and approved reference designs.

Evaluation and Differentiation

Every reference design proposal will be evaluated against zero trust architectural principles, software supply chain assumptions and interactions, how it defines configuration management, how it manages environmental drift, software assurance topics, etc. The fundamental question that must be answered: *Does this community proposal present enough differentiation from existing published draft and approved reference designs to begin drafting a new set of interconnects?*

Define Interconnects

Each reference design must present a set of opinionated interconnects that uniquely define a platform architectural design that intrinsically supports the primacy of security, stability, and quality. This step starts to establish how an implementation of this reference design would undergo a compliance check and concretely capture zero trust architectural principals, its philosophy of meeting various cybersecurity controls, etc.

Publish Draft

Each reference design must build from the 'REQUIRED' items captured in the DevSecOps Tools and Activities Guidebook. It may introduce additional 'REQUIRED' or 'PREFERRED' tools and activities, and it must include suitable narrative and figures that explain its philosophy, merits, differentiation, and interconnects. The draft is then published as part of the DevSecOps document set to begin an open and transparent discussion across both government and industry.

Execute Pilot

Every draft reference design must be piloted in an operationally relevant environment and cannot proceed towards becoming an approved reference design without this step. The definition of pilot is preferably aligned to completion of a minimum viable product, but this alignment is not a rigid expectation and thus intentionally left a bit vague.
No one takes a paper design of a tank to war; they want the actual tank!

Lessons Learned

The execution of the pilot tests the hypotheses and cybersecurity mettle of the overall reference design generally, and its opinionated set of interconnects specifically. Zero trust principles evaluated and confirmed. Cybersecurity controls are evaluated and confirmed. Lessons learned and reference design improvement opportunities are aggregated during sprint retrospectives across the developers, cybersecurity professionals, and operational team members, and the reference design is refined.

Software Modernization Senior Steering Group Briefing

At the conclusion of a successful pilot, the refined reference design will be presented to the Software Modernization Senior Steering Group for an approval vote. This presentation covers the differentiation, the opinionated set of interconnects, and key highlights from the pilot. If the tri-chairs concur with the recommendation, a new approved reference design is added to the DevSecOps document set.

Approved Reference Design

Every approved reference design is a living document that will continue to be updated at the speed of relevance. The specific update cadence is not rigidly defined, but must be revised no less than once per year. Each design is publicly releasable (Distro A), and to mitigate the distribution and consumption of stale reference designs, a banner will be included on the front page with a clear expiration date.