DoD Enterprise DevSecOps Reference Design:

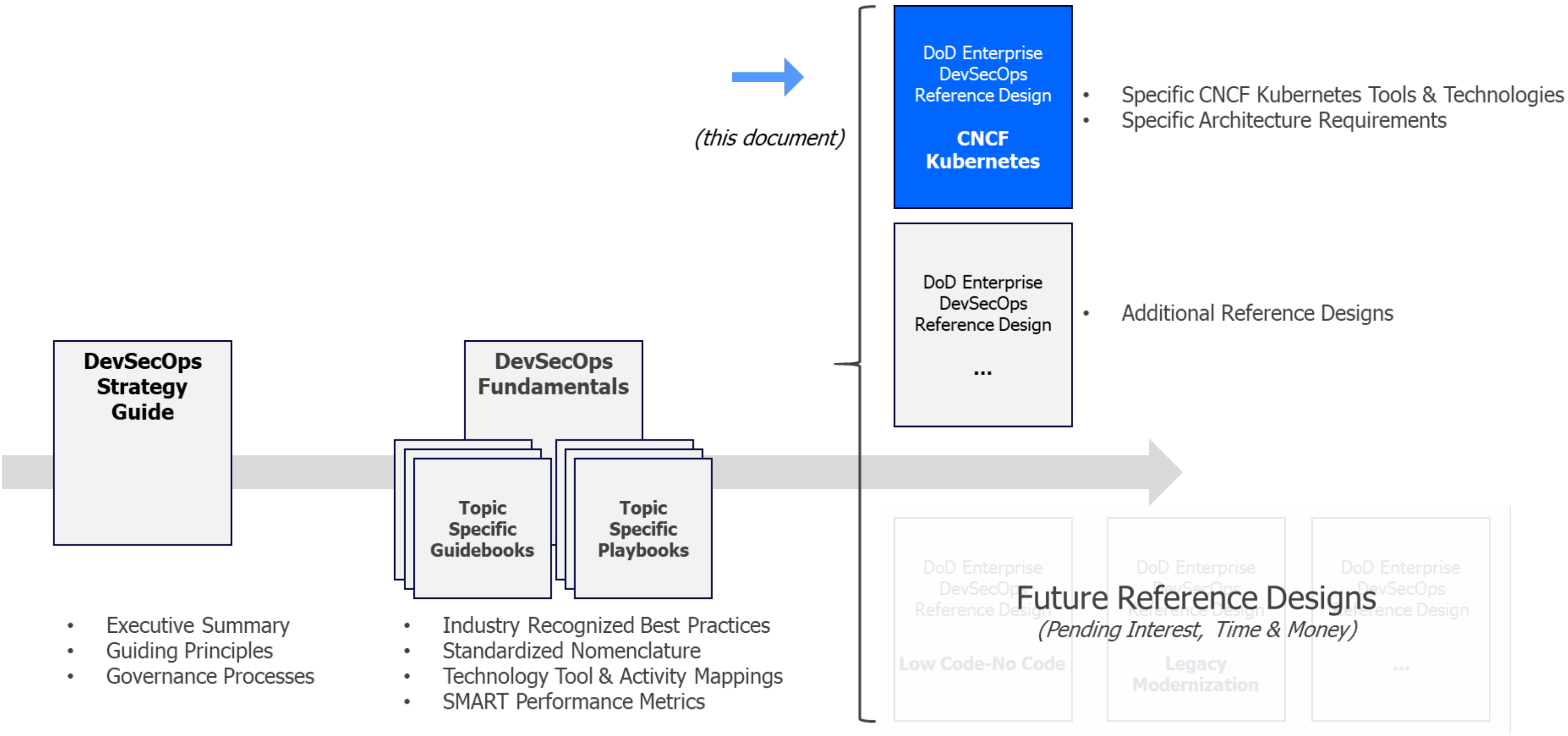
CNCF Kubernetes

September 2021

Version 2.1

This document automatically expires 1-year from publication date unless revised.

Document Set Reference



Document Approvals

Approved by:

____

Nicolas Chaillan

Chief Software Officer, Department of Defense, United States Air Force, SAF/AQ

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our readers, and do not constitute or imply endorsement by the Department of any non-Federal entity, event, product, service, or enterprise.

Contents

Figures

Tables

1 Introduction

1.1 Background

Modern information systems and weapons platforms are driven by software. As such, the DoD is working to modernize its software practices to provide the agility to *deliver resilient software at the speed of relevance*. DoD Enterprise DevSecOps Reference Designs are expected to provide clear guidance on how specific collections of technologies come together to form a secure and effective software factory.

1.2 Purpose

This DoD Enterprise DevSecOps Reference Design is specifically for Cloud Native Computing Foundation (CNCF) Certified Kubernetes implementations. This enables a Cloud agnostic, elastic instantiation of a DevSecOps software factory anywhere: Cloud, On Premise, Embedded System, Edge Computing.

In this reference design the software container ("container") is the standard unit of deployment. The software factory defined herein produces DoD applications and application artifacts as a product. Kubernetes must be part of the production environment.

For brevity, the use of the term 'Kubernetes' or 'K8s' throughout the remainder of this document must be interpreted as a Kubernetes implementation that properly submitted software conformance testing results to the CNCF for review and corresponding certification. The CNCF lists over 90 Certified Kubernetes offerings that meet software conformation expectations. [1]

It provides a formal description of the key design components and processes to provide a repeatable reference design that can be used to instantiate a DoD DevSecOps Software Factory powered by Kubernetes. This reference design is aligned to the DoD Enterprise DevSecOps Strategy, and aligns with the baseline nomenclature, tools, and activities defined in the DevSecOps Fundamentals document and its supporting guidebooks and playbooks.

The target audiences for this document include:

- DoD Enterprise DevSecOps capability providers who build DoD Enterprise DevSecOps hardened containers and provide a DevSecOps hardened container access service.
- DoD Enterprise DevSecOps capability providers who build DoD Enterprise DevSecOps platforms and platform baselines and provide a DevSecOps platform service.
- DoD organization DevSecOps teams who manage (instantiate and maintain) DevSecOps software factories and associated pipelines for its programs.
- DoD program application teams who use DevSecOps software factories to develop, secure, and operate mission applications.

[1] Cloud Native Computing Foundation, "Software conformance (Certified Kubernetes," [ONLINE] Available: https://www.cncf.io/certification/software-conformance/. [Accessed 8 February 2021].

- Authorizing Officials (AOs).

This reference design aligns with these reference documents:

- DoD Digital Modernization Strategy.[2]
- DoD Cloud Computing Strategy.[3]
- DISA Cloud Computing Security Requirements Guide.[4]
- DISA Secure Cloud Computing Architecture (SCCA).[5]
- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Executive Order (EO) 1380).[6]
- National Institute of Standards and Technology (NIST) Cybersecurity Framework.[7]
- NIST Application Container Security Guide.[8]
- Kubernetes (draft) STIG – Ver 1.[9]
- DISA Container Hardening Process Guide, V1R1.[10]

1.3 DevSecOps Compatibility

This reference design asserts version compatibility with these supporting DevSecOps documents:

- DoD Enterprise DevSecOps Strategy Guide, Version 2.1.
- DevSecOps Tools and Activities Guidebook, Version 2.1.

1.4 Scope

This reference design is product-agnostic and provides execution guidance for use by software teams. It is applicable to developing new capabilities and to sustaining existing capabilities in both business and weapons systems software, including business transactions, C3, embedded systems, big data, and Artificial Intelligence (AI).

---

[2] DoD CIO, *DoD Digital Modernization Strategy,* Pentagon: Department of Defense, 2019.

[3] Department of Defense, "DoD Cloud Computing Strategy," December 2018.

[4] DISA, "Department of Defense Cloud Computing Security Requirements Guide, v1r3," March 6, 2017

[5] DISA, "DoD Secure Cloud Computing Architecture (SCCA) Functional Requirements," January 31, 2017.

[6] White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (EO 1380)," May 11, 2017.

[7] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, 2018.

[8] NIST, "NIST Special Publication 800-190, Application Container Security Guide," September 2017.

[9] DoD Cyber Exchange, "Kubernetes Draft STIG – Ver 1, Rel 0.1," December 15, 2020.

[10] DISA, "Container Hardening Process Guide, V1R1," October 15, 2020

This document does not address strategy, policy, or acquisition.

1.5 Document Overview

The documentation is organized as follows:

- Section 1 describes the background, purpose and scope of this document.
- Section 2 identifies the assumptions relating to this design.
- Section 3 describes the DevSecOps software factory interconnects unique to a Kubernetes reference design.
- Section 4 describes the containerized software factory design.
- Section 5 captures the additional required and preferred tools and activities, building upon the DevSecOps Tools and Activities Guidebook as a baseline.

1.6 What's New in Version 2

- Refactored the document's overall structure to align with the shift to a DevSecOps Document Set approach.

2 Assumptions and Principles

This reference design makes the following assumptions:

- No specific Kubernetes implementation is assumed, but the selected Kubernetes implementation must have submitted conformance testing results for review and certification by the CNCF.
- Vendor lock-in is avoided by mandating a Certified Kubernetes implementation; however, product lock-in into the Kubernetes API and its overall ecosystem is openly recognized.

> **It is critically important to avoid the proprietary APIs that are sometimes added by vendors on top of the existing CNCF Kubernetes APIs. These APIs are not portable and may create vendor lock-in!**

- Adoption of hardened containers as a form of immutable infrastructure results in standardization of common infrastructure components that achieve consistent and predictable results.
- This reference design depends upon a number of DoD Enterprise Services, which will be named throughout this document.

3 Software Factory Interconnects

The DevSecOps Fundamentals describes a DevSecOps platform as a multi-tenet environment consisting of three distinct layers: *Infrastructure*, *Platform/Software Factory*, and *Application(s)*. Each reference design is expected to identify its unique set of tools and activities that exist within or between the discrete layers, known as *Reference Design Interconnects*. Well-defined interconnects in a reference design enable tailoring of the software factory design, while ensuring that core capabilities of the software factory remain intact.

> The value proposition of each **Reference Design Interconnect** block depicted in *Figure 1* is found in how each reference design explicitly defines specific tooling and explicitly stipulates additional controls or activities within *or* between any given layer. These interconnects are an acknowledgement of the need for *platform architectural designs* to support the primacy of security, stability, and quality. Each Reference Design must acknowledge and/or define its own set of unique interconnects.

Figure 1: Kubernetes Reference Design Interconnects identifies the specific Kubernetes interconnects that **must be present** in order to be compliant with this reference design. The specific interconnects include:

- Cloud Native Access Point (CNAP) at the Infrastructure layer manages all north-south network traffic.[11]
- Use of a conformant Kubernetes installation in each of the development environments.
- Clear identification of a locally centralized artifact repository to host hardened containers from Iron Bank, the DoD Centralized Artifact Repository (DCAR) of hardened and centrally accredited containers.
- Use of a service mesh within the K8s orchestrator to manage all east-west network traffic.
- Mandatory adoption of the Sidecar Container Security Stack (SCSS) to implement zero trust down to the container/function level, also providing behavior protection.

Each of these interconnects will be described fully next.

[11] DoD CIO, "Department of Defense Cloud native Access Point Reference Design," [ONLINE] Available: https://dodcio.defense.gov/Portals/0/Documents/Library/CNAP_RefDesign_v1.0.pdf. [Accessed 19 Aug 2021].

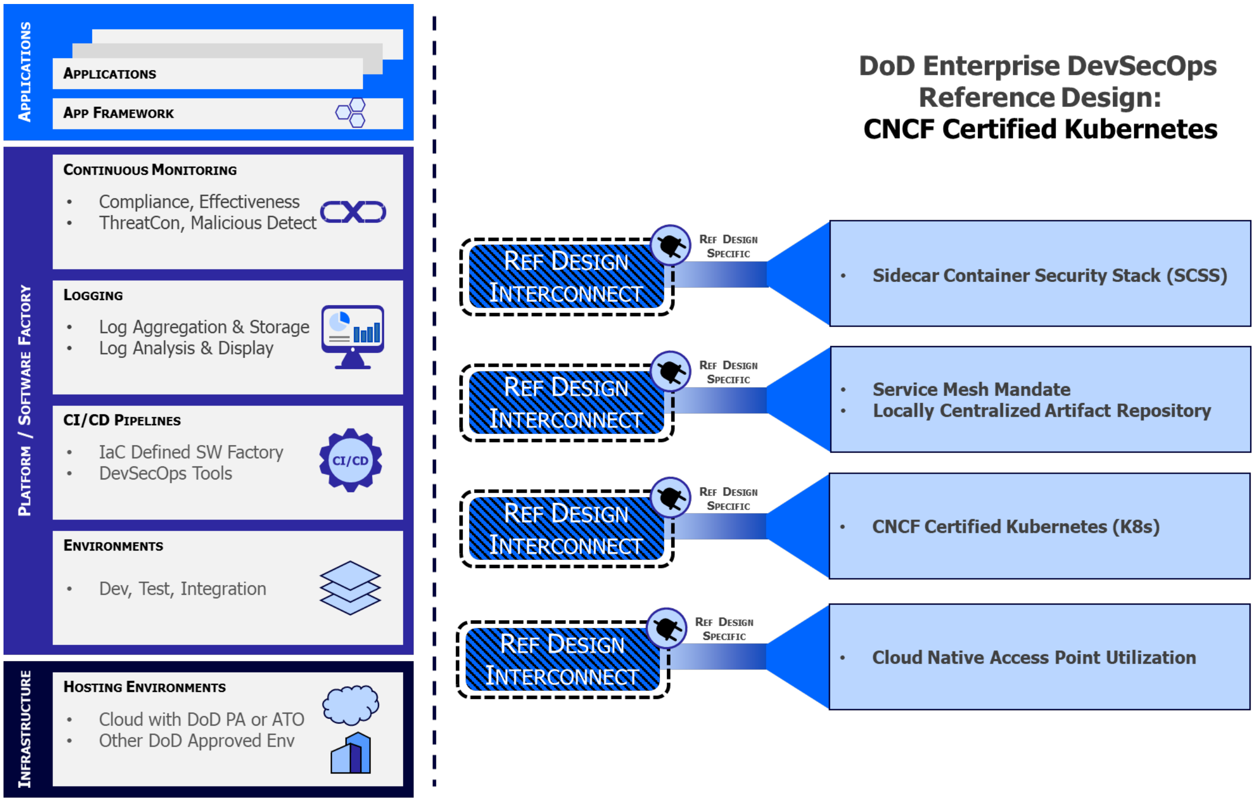


Figure 1: Kubernetes Reference Design Interconnects

3.1 Cloud Native Access Points

A Cloud Native Access Point (CNAP) provides a zero-trust architecture on Cloud One to provide access to development, testing, and production enclaves at Impact Level 2 (IL-2), Impact Level 4 (IL-4), and Impact Level 5 (IL-5).[12] CNAP provides access to Platform One DevSecOps environments by using an internet-facing Cloud-native zero trust environment. CNAP's zero trust architecture facilitates development team collaboration from disparate organizations.

3.2 CNCF Certified Kubernetes

Kubernetes is a *container orchestrator* that manages the scheduling and execution of Open Container Initiative (OCI) compliant containers across multiple nodes, depicted in *Figure 2*. OCI is an open governance structure for creating open industry standards around both container formats and runtimes.[13] The container is the standard unit of deployment in this reference design. Containers enable software production automation in this reference design, and they also allow operations and security process orchestration.[14]

---

[12] DISA, "Department of Defense Cloud Computing Security Requirements Guide, v1r3," Mar 6, 2017

[13] The Linux Foundation Projects, "Open Container Initiative," [Online] Available at: https://opencontainers.org.

[14] For more insight about the benefits of containers, visit https://cloud.google.com/containers

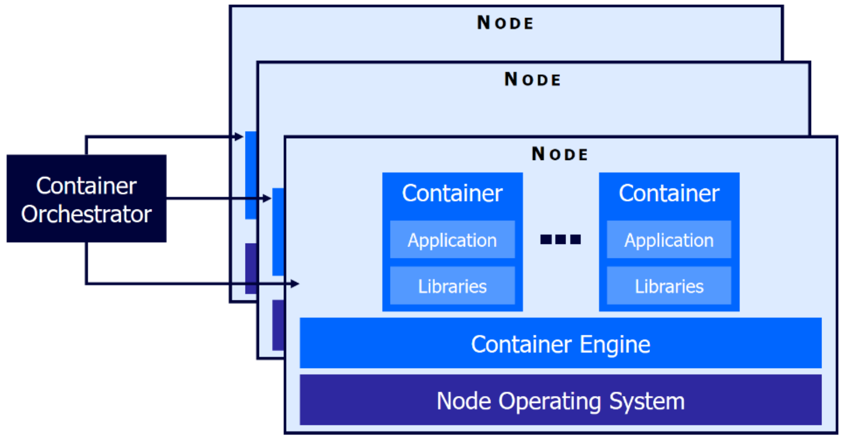


Figure 2: Container Orchestrator and Notional Nodes

Kubernetes provides an API that ensures total abstraction of orchestration, compute, storage, networking, and other core services that guarantees software can run in any environment, from the Cloud to being embedded inside platforms like jets or satellites.

The key benefits of adopting Kubernetes include:

- **Multimodal Environment**: Code runs equally well in a multitude of compute environments, benefitting from the K8s API abstraction.
- **Baked-In Security**: The Sidecar Container Security Stack is automatically injected into any K8s cluster with zero trust.
- **Resiliency:** Self-healing of unstable or crashed containers.
- **Adaptability:** Containerized microservices create highly-composable ecosystems.
- **Automation**: Fundamental support for a GitOps model and IaC speeds process and feedback loops.
- **Scalability**: Application elasticity to appropriately scale and match service demand.

The adoption of K8s and OCI compliant containers are concrete steps towards true microservice reuse, providing the Department with a compelling ability to pursue higher orders of code reuse across an array of programs.

3.3 Locally Centralized Artifact Repository

A Locally Centralized Artifact Repository is a local repository tied to the software factory. It stores artifacts pulled from Iron Bank, the DoD repository of digitally signed binary container images that have been hardened. The local artifact repository also stores locally developed artifacts used in the DevSecOps processes. Artifacts stored here include, but are not limited to, container images, binary executables, virtual machine (VM) images, archives, and documentation.

The Iron Bank artifact repository provides hardened, secure technical implementation guide (STIG) compliant, and centrally updated, scanned, and signed containers that increases the cyber survivability of these software artifacts. At time of writing this reference design, over 300 artifacts were in Iron Bank, with more being added continuously.

Programs may opt for a single artifact repository and rely on the use of tags to distinguish between the different content types. It is also permissible to have separate artifact repositories to store local artifacts and released artifacts.

3.4 Sidecar Container Security Stack (SCSS)

The cyber arena is an unforgiving hostile environment where even a minute exposure and compromise can lead to catastrophic failures and loss of human life. Industry norms now recognize that a modern holistic cybersecurity posture must include centralized logging and telemetry, zero trust ingress/egress/east-west network traffic, and behavior detection at a *minimum*. The sidecar container security stack provides baked-in, not bolt-on, security.

A cybersecurity stack is frequently updated as threat conditions evolve. A key benefit of a cybersecurity K8s sidecar container design is rapidly deployed updates without any recompilation or rebuild required of the microservice container itself. To support this approach, the SCSS is available from the Iron Bank repository as a hardened container that K8s automatically injects into each container group (pod). A pod is the smallest deployable units of computing that can be managed in Kubernetes. This decoupled architecture, shown in *Figure 3*, speeds deployment of an updated cyber stack without requiring any type of re-engineering by development teams.

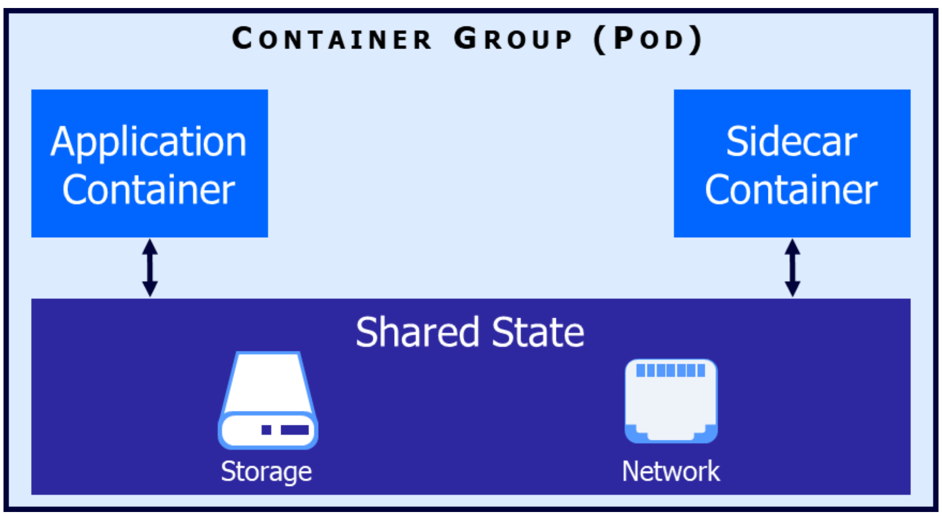


Figure 3: Sidecar Container Relationship to Application Container

As shown in *Figure 3*, the sidecar can share state with the application container. In particular, the two containers can share disk and network resources while their running components are fully isolated from one another.

The complete set of sidecar container security monitoring components are captured in Table 1 on the next page. Capability highlights include:

- Centralized logging and telemetry that includes extract, transform, and load (ETL) capabilities to normalize log data.
- Robust east/west network traffic management (whitelisting).
- Zero Trust security model.
- Role-Based Access Control.
- Continuous Monitoring.
- Signature-based continuous scanning using Common Vulnerabilities and Exposures (CVEs).
- Runtime behavior analysis.
- Container policy enforcement.

Table 1 Sidecar Security Monitoring Components

Tool	Features	Benefits	Baseline
Logging agent	Send logs to a logging service	Standardize log collection to a central location. This can also be used to send notifications when there is anomalous behavior.	REQUIRED
Logging Storage and Retrieval Service	Stores logs and allows searching logs	Place to store logs	REQUIRED
Log visualization and analysis	Ability to visualize log data in various ways and perform basic log analysis.	Helps to find anomalous patterns	PREFERRED
Container policy enforcement	Support for automated policy testing. The data format for the policies must be a structured machine-readable format, e.g. JSON or YAML. These policies can be defined as needed.	Automated policy enforcement	REQUIRED
Runtime Defense	Creates runtime behavior models, including whitelist and least privilege	Dynamic, adaptive cybersecurity	REQUIRED
Service Mesh proxy	Ties to the Service Mesh. Only required if the application uses microservices.	Enables use of the service mesh.	REQUIRED
Service Mesh	Used for a microservices architecture, and only required if the application uses microservices.	Better microservice management.	REQUIRED
Vulnerability Management	Provides vulnerability management	Makes sure everything is properly patched to avoid known vulnerabilities	REQUIRED
CVE Service / Host Based Security	Provides CVEs. Used by the vulnerability management agent in the security sidecar container.	Makes sure the system is aware of known vulnerabilities in components.	REQUIRED
Zero Trust model down to the container level	Provides strong identities per Pod with certificates, mTLS tunneling and whitelisting of East-West traffic down to the Pod level.	Reduces attack surface and improves baked-in security	REQUIRED

3.5 Service Mesh

A service mesh enhances cybersecurity by controlling how different parts of an application interact. Some of the specific capabilities of a service mesh in K8s include monitoring east-west network traffic, routing traffic based on a declarative network traffic model that can deny all network traffic by default, and dynamically injecting strong certificate-based identities without requiring access to the underlying code that built the software container. A service mesh also typically takes over ownership of the `iptables` in order to inject an mTLS tunnel with FIPS compliant cryptographic algorithms to further protect all data in motion.

Service mesh integration into the K8s cluster reduces the cyber-attack surface, and when coupled with behavior detection, it can proactively kill any container that is drifting outside of its expected operational norms. These capabilities restrict the ability of a bad actor to laterally move around within the K8s cluster and fully eliminate the ability of the bad actor to achieve escalated privileges. For these reasons, service mesh integration is a powerful component in ensuring the cyber survivability of the software factory and the containerized applications produced by the factory's pipelines.

4 Software Factory K8s Reference Design

This section will discuss the software factory design required for this reference design. It creates a software factory using DevSecOps tools from hardened containers stored in Iron Bank.

All software factory implementations follow the DevSecOps philosophy and go through four unique phases: Design, Instantiate, Verify, Operate & Monitor. *Figure 4* illustrates the phases, activities, and the relationships with the application lifecycle. Security is applied across all software factory phases. The SCSS must be used for cybersecurity monitoring of the application in this reference design.

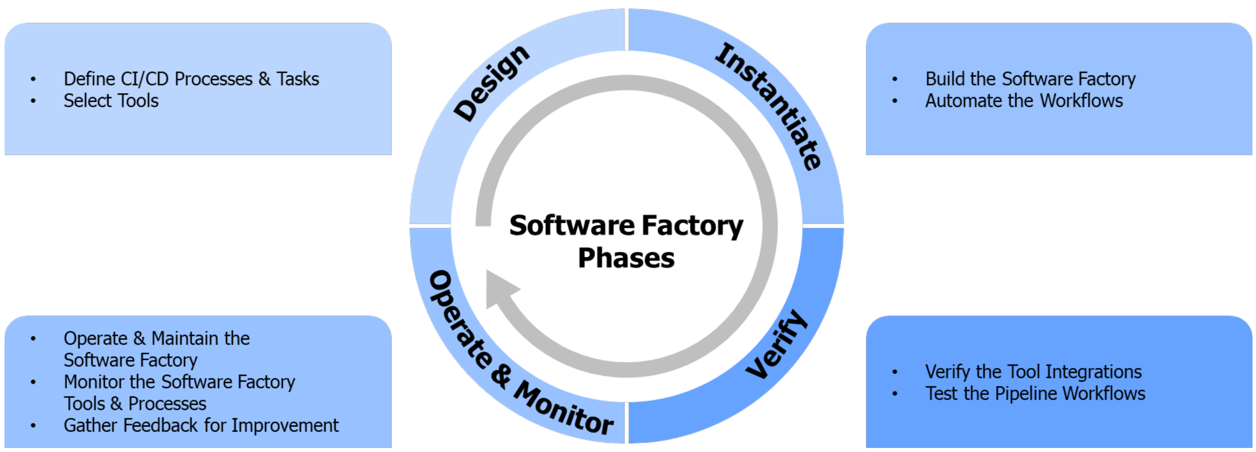


Figure 4: Software Factory Implementation Phases

The components of this reference design's software factory must be instantiated as follows: A CSP-agnostic solution running a CNCF Certified K8s using hardened containers from Iron Bank. This design recognizes that K8s is well-suited to act as the engine powering a container defined software factory.

The software factory leverages technologies and tools to automate the CI/CD pipeline processes defined in the DevSecOps lifecycle plan phase. There are no "one size fits all" or hard rules about what CI/CD processes should look like and what tools must be used. Each software team needs to embrace the DevSecOps culture and define processes that suit its software system architectural choices. The tool chain selection is specific to the software programming language choices, application type, tasks in each software lifecycle phase, and the system deployment platform.

The CI/CD orchestrator automates a build pipeline workflow by validating security control gates. DevSecOps teams create a pipeline workflow in the CI/CD orchestrator by specifying a set of stages, stage conditions, stage entrance and exit control rules, and stage activities. If all the entrance rules of a stage are met, the orchestrator will transition the software artifact into that stage and perform the defined activities by coordinating the tools via plugins and scripts. If all the exit rules of the current stage are met, the software artifact exits the current stage and the pipeline starts to validate the entrance rules of the next stage. *Table 2* shows the features, benefits, and inputs and outputs of the CI/CD orchestrator.

Table 2: CI/CD Orchestrator Inputs/Outputs

Features	Benefits	Inputs	Outputs	Baseline
Create pipeline workflow	Customizable pipeline solution	Human input about: • A set of stages • A set of event triggers • Each stage entrance and exit control gate • Activities in each stage	Pipeline workflow configuration	REQUIRED
Orchestrate pipeline workflow execution by coordinating other plugin tools or scripts.	Automate the CI/CD tasks; Auditable trail of activities	Event triggers (such as code commit, test results, human input, etc.); Artifacts from the artifact repository	Pipeline workflow execution results (such as control gate validation, stage transition, activity execution, etc.); Event and activity audit logs	

4.1 Containerized Software Factory

Software factory tools include a CI/CD orchestrator, a set of development tools, and a group of tools that operate in different DevSecOps lifecycle phases. These tools are pluggable and must integrate into the CI/CD orchestrator. **In this reference design, instantiations must rely on a containerized software factory instantiated from a set of DevSecOps hardened containers from Iron Bank.** Iron Bank containers are preconfigured and secured to reduce the certification and accreditation burden and are often available as a predetermined pattern or pipeline that will need limited or no configuration.

Running a CI/CD pipeline is a complex activity. Containerization of the entire CI/CD stack ensures there is no drift possible between different K8s cluster environments (development, test, staging, production). It further ensures there is no drift between different K8s cluster environments spanning multiple classification levels. Containerization also streamlines the update/accreditation process associated with the introduction and adoption of new DevSecOps tooling.

Figure 5, illustrates a containerized software factory reference design. The software factory is built on an underlying container orchestration layer powered by K8s in a host environment. Applications typically use different sets of hardened containers from the Iron Bank than the ones used to create the software factory.

The software factory reference design captured in *Figure 5* illustrates how cybersecurity is woven into the fabric of each factory pipeline. All of the tooling within the factory is based on hardened containers pulled from Iron Bank.

Moving from left to right, as code is checked into a branch it triggers the CI/CD pipeline workflow and resulting automated build, SAST, DAST, unit, and other relevant tests are executed. The CI/CD orchestrator coordinates the different tools required to perform all the various tasks defined by the pipeline via plugins. If the build is successful and a container image is defined, the pipeline must also trigger a container security scan. Some tests and security tasks may require human involvement or consent before being considered complete and passed. If all of these relevant tests are successful, then the artifact is deployed into the test environment. If all the entrance rules of the next stage are met, the CI/CD orchestrator will transition the software artifact into that stage and perform the defined activities there by coordinating the tools via plugins. When all stages are complete, a significant number of security activities have completed and the artifact is eligible for deployment into production. Deployment into production should be fully automated, but may be gated by a human actually pressing a button to trigger the deployment. Once deployed, there is another control gate to decide to turn it on; this typically requires an Authorization to Connect (ATC).

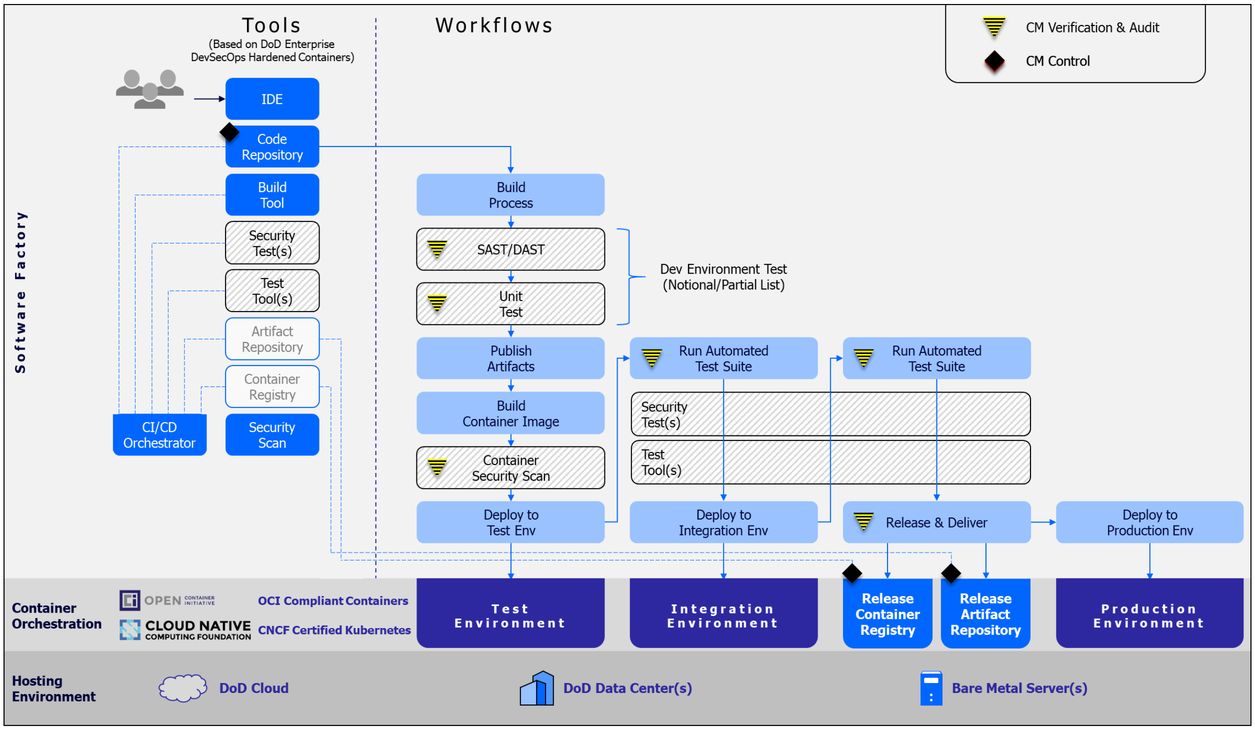


Figure 5: Containerized Software Factory Reference Design

Operating a custom DevSecOps platform is an expensive endeavor because software factories require the same level of continuous investment as a software application. There are financial benefits for programs to plan a migration to a containerized software factory, reaping the benefits of centrally managed and hardened containers that have been fully vetted. In situations where a containerized software factory is impractical, or the factory requires extensive policy customizations, the program should consult with DoD CIO and (if applicable) its own DevSecOps program office to explore options and collaborate to create, sustain, and deliver program-specific hardened containers to Iron Bank.

Platform One is the first DoD-wide approved DevSecOps Managed Service.
For more information: https://p1.dso.mil

4.2 Hosting Environment

The reference design does not constrain the software factory hosting environment, which could be a Cloud Service Provider with a DoD provisional authorization or ATO, DoD data centers or even on-premises servers. The hosting environment provides compute, storage, and network resources in either physical or virtual form.

4.3 Container Orchestration

K8s software factory responsibilities include container orchestration, interacting with the underlying hosting environment resources (compute, storage, etc.), and coordination of clusters of nodes at scale in development, testing and pre-production in an efficient manner. As described in the opening paragraphs of this section, this reference design mandates a container orchestration layer as illustrated in *Figure 6*.

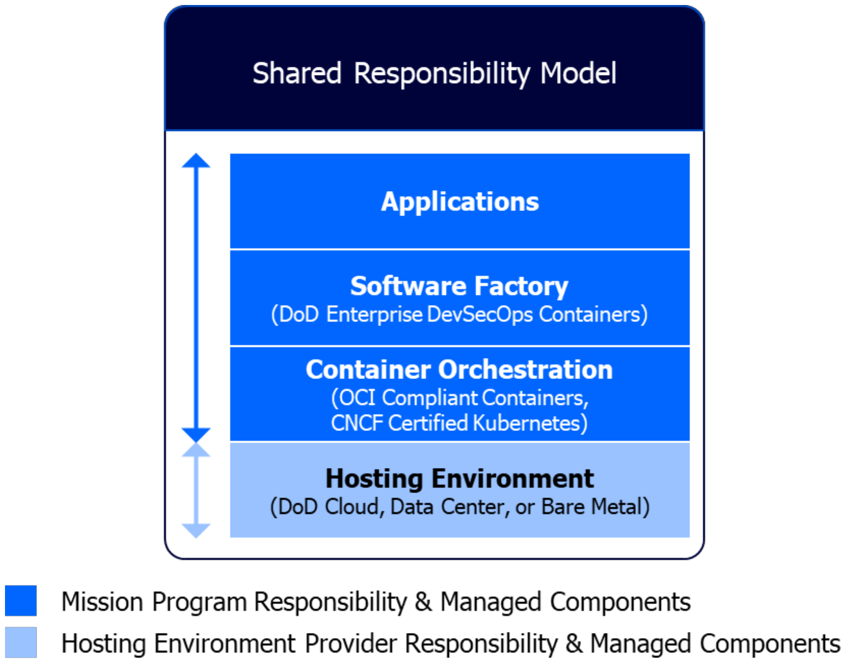


Figure 6: DevSecOps Platform Options

It is the mission program's responsibility (or that of a DoD software factory platform like Platform One), to build and maintain K8s using COTS solutions from Iron Bank. K8s can be deployed on top of a DoD authorized Cloud environment, a DoD data center, or on bare metal servers. K8s is subject to monitoring and security control under the DoD policy in that hosting environment, such as the DoD Cloud Computing Security Requirements Guide (SRG) and DISA's Secure Cloud Computing Architecture (SCCA) for the Cloud environment.

A notional set of DevSecOps services, an abbreviated representation of the DevSecOps workflow, and various cybersecurity mechanisms are depicted in *Figure 7.* The diagram should be interpreted as the basis of the software factory and not a normative reference. For example, the complete set of tests that should be defined to assure a specific software artifact meets mission objectives should be collaboratively defined with DOT&E.

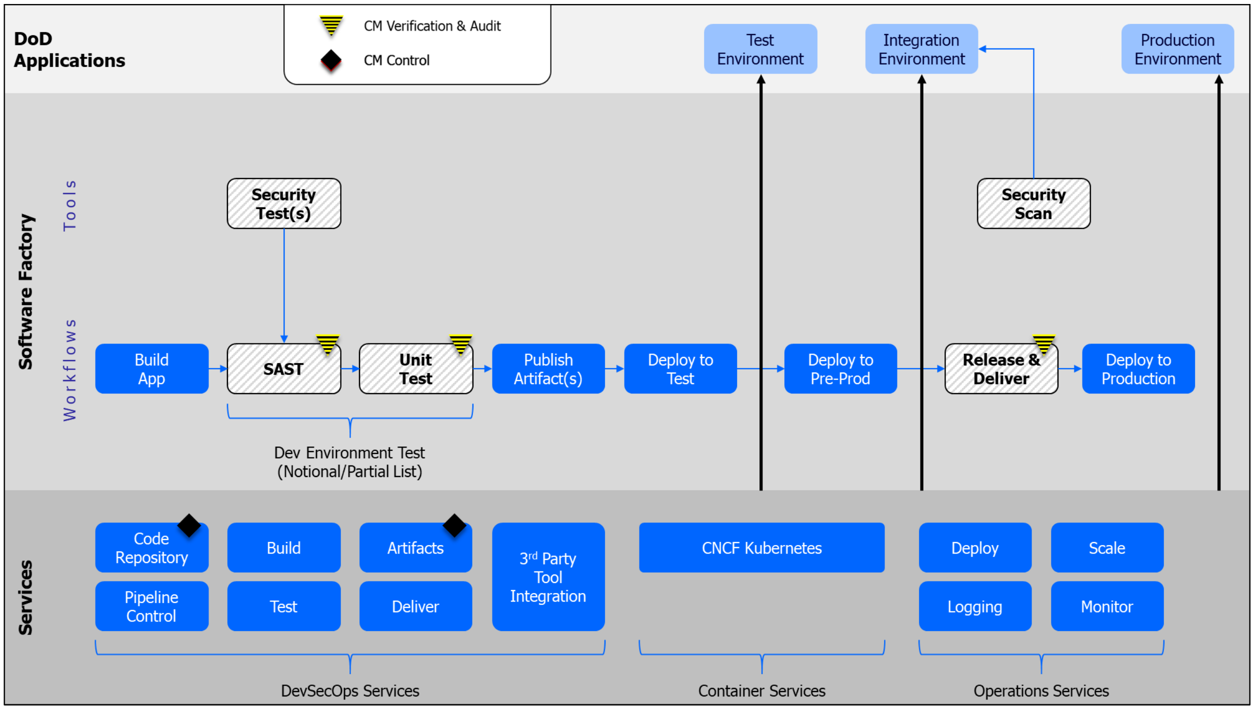


Figure 7: Software Factory - DevSecOps Services

5 K8s Reference Design Tools and Activities

The **DevSecOps Tools and Activities Guidebook**, along with the **DevSecOps Fundamentals** document, establishes common DevSecOps tools and activities. The guidebook recognizes that specific reference designs may elevate a specific tool from PREFERRED to REQUIRED, as well as add additional tools and/or activities that specifically support the nuances of a given reference design. The following sections identify those tools and activities unique to this reference design across the *Deploy* and *Monitor* phases of the DevSecOps lifecycle.

Table 3: Security Activities Summary and Cross-Reference

Activities	Phase	Activities Table Reference	Tool Dependencies
Container or VM hardening	Develop	Table 4	Container security tool; Security compliance tool
Container policy enforcement	Test	Table 6	Container policy enforcement

Table 4: Develop Phase Activities

Activities	Description	Inputs	Outputs	Tool Dependencies
Container image selection	Must leverage approved and hardened container images strictly from the Iron Bank repository	N/A	N/A	Artifact repo
Container hardening	Harden the deliverable for production deployment. Containers must follow the DISA Container Hardening Guide.[10]	Container	-Vulnerability report and recommended mitigation -Hardened Container & Build File	Container security tool

Table 5: Build Phase Tools

Tool	Features	Benefits	Inputs	Outputs	Baseline
Container builder	Build a container image based on a build instruction file. Must use a hardened container image from Iron Bank as the base image in all cases.	Container image build automation	Container base image; Container build file	OCI compliant container image	REQUIRED
Artifact Repository	Container Registry	Better quality software by using centrally managed, hardened containers.	Artifacts	Version controlled container	REQUIRED

Table 6: Build Phase Activities

Activities	Description	Inputs	Outputs	Tool Dependencies
Containerize	Packages all required OS components, developed code, runtime libraries, etc. into a hardened container	Container base image; Container build file	Container Image	Container Builder
Store artifacts	Store artifacts to the artifact repository	Container Image	Version controlled container image	Artifact Repository

Table 7: Test Phase Tools

Tool	Features	Benefits	Inputs	Outputs	Baseline
TWO DIFFERENT Container security tool	Container image scan OS check. Two are required because scan results are too disparate.	Ease the container hardening process	Container images or running containers	Vulnerability report and recommended mitigation.	REQUIRED
Container policy enforcement	Support for automated policy testing. The data format for the policies must be a structured machine-readable format, e.g. JSON or YAML. These policies can be defined as needed.	Automated policy enforcement	Policies in a structured machine-readable format.	Compliance report	REQUIRED
Security compliance tool	Scan and report for compliance regulations, such as DISA Security Technical Implementation Guides (STIGs), NIST 800-53.	Speed up ATO process.	Container images.	Vulnerability report and recommended mitigation.	PREFERRED

Table 8: Test Phase Activities

Activities	Description	Inputs	Outputs	Tool Dependencies
Container policy enforcement	Check developed containers to be sure they meet container policies	Container policies in a structured machine-readable format.	Container compliance report	Container policy enforcement

Table 9: Release and Deliver Phase Tools

Tool	Features	Benefits	Inputs	Outputs	Baseline
IaC / CaC	Automated “push button” instantiation of the applications running on K8s in addition to the software factory itself (including the SCSS stack on top)	Eliminate drift between environments; ensure desired state is always accurately captured in git.			REQUIRED
GitOps Kubernetes Capability	Pull source code from git repositories instead of requiring the CI/CD pipeline to push artifacts to the next environment	Eliminates the need to open ports and/or require keys to be shared with CI/CD tooling. Eliminates environment drifts. Ensures desired state is always accurately captured in git.			PREFERRED

Table 10: Release and Deliver Phase Activities

Activities	Description	Inputs	Outputs	Tool Dependency
Release go / no-go decision	This is part of configuration audit; Decision on whether to release artifacts to the artifact repository for the production environment.	Design documentation; Version controlled artifacts; Version controlled test reports; Security test and scan reports	go / no-go decision; Artifacts are tagged with release tag if go decision is made	CI/CD Orchestrator

Table 11: Deploy Phase Tools

Tool	Features	Benefits	Inputs	Outputs	Baseline
CNCF-certified Kubernetes	Container grouping using pods; Health checks and self-healing Horizontal infrastructure scaling Container auto-scalability Domain Name Service (DNS) management Load balancing Rolling update or rollback; Resource monitoring and logging	Simplify operations by deployment and update automation Scale resources and applications in real time Cost savings by optimizing infrastructure resources	Container instance specification and monitoring policy	Running container	REQUIRED
Service mesh	Ability to create a network of deployed microservices with load balancing, service-to-service authentication, and monitoring. Ability to enforce Zero trust mTLS traffic for east/west traffic	Support for microservice interactions.	Control plane: service communication routing policies, authentication certificates. Data plane: service communication data	Control plane: service status reports Data plane: routed service communication data	REQUIRED

Table 12: Deploy Phase Activities

Activities	Description	Inputs	Outputs	Tool Dependency
Deliver container to container registry	Upload the hardened container and associated artifacts to the container registry	Hardened container	New container instance	CNCF-certified Kubernetes; Artifact repository container registry

Table 13: Operate Phase Activities

Activities	Description	Inputs	Outputs	Tool Dependency
Scale	Scale manages containers as a group. The number of containers in the group can be dynamically changed based on the demand and policy.	Real-time demand and container performance measures Scale policy (demand or Key Performance Indicator (KPI)threshold; minimum, desired, and maximum number of containers)	Optimized resource allocation	Container management on the hosting environment
Load balancing	Load balancing equalizes the resource utilization	Load balance policy Real time traffic load and container performance measures	Balanced resource utilization	Container management on the hosting environment

Table 14: Monitor Phase Tools

Tool	Features	Benefits	Baseline
Resource, Service, Container policy enforcement	Support for automated policy testing. The data format for the policies must be a structured machine-readable format, e.g. JSON or YAML. These policies can be defined as needed.	Automated policy enforcement	REQUIRED
Vulnerability Management	Provides vulnerability management	Makes sure everything is properly patched to avoid known vulnerabilities	REQUIRED
CVE Service / Host Based Security	Provides CVEs. Used by the vulnerability management agent in the security sidecar container.	Makes sure the system is aware of known vulnerabilities in components.	REQUIRED

Table 15: CSP Managed Service Monitoring Tools

Tool	Features	Benefits	Baseline
Netflow Analysis	Logs network traffic within as enclave Network troubleshooting	Helps to find anomalous patterns across environments	REQUIRED
Centralized Logging	Stores logs from the entire environment. Used by the SEIM/SOAR for log analysis and incident detection	Place to store logs across environment and Platform	REQUIRED
Centralized Analysis	SEIM/SOAR for log analysis and incident detection Tier 3 CSSP tools	Helps to find anomalous patterns across environment and Platform	PREFERRED

5.1 Continuous Monitoring in K8s

Continuous monitoring of a K8s cluster must include behavior and signature-based detection in the runtime environment. These and other container specific controls are captured in NIST Special Publication 800-190, *Application Container Security Guide*. CSP services also routinely monitor and scan CSP resources and services for misconfiguration, incorrect access control, and security events. These CSP specific capabilities should be integrated into every continuous monitoring strategy.

Figure 8 illustrates a notional process of monitoring, logging, and log analysis and alerting. The process starts with application logging, compute resource monitoring, storage monitoring, network monitoring, security monitoring, and data monitoring at the Kubernetes pod.

Each application team must determine how the application is decomposed into containers and the specific monitoring mechanisms within those. The security tools within each will aggregate and forward the event logs gathered from monitoring to a locally centralized aggregated logs database on the mission program platform. The aggregated logs will be further forwarded to the Logs/Telemetry Analysis in the Defensive Cyber Operations / Tier 2 CSSP after passing the program application configured log filter. The program's local log SIEM/SOAR analysis capability will analyze the aggregated logs and generate incident alerts and reports.

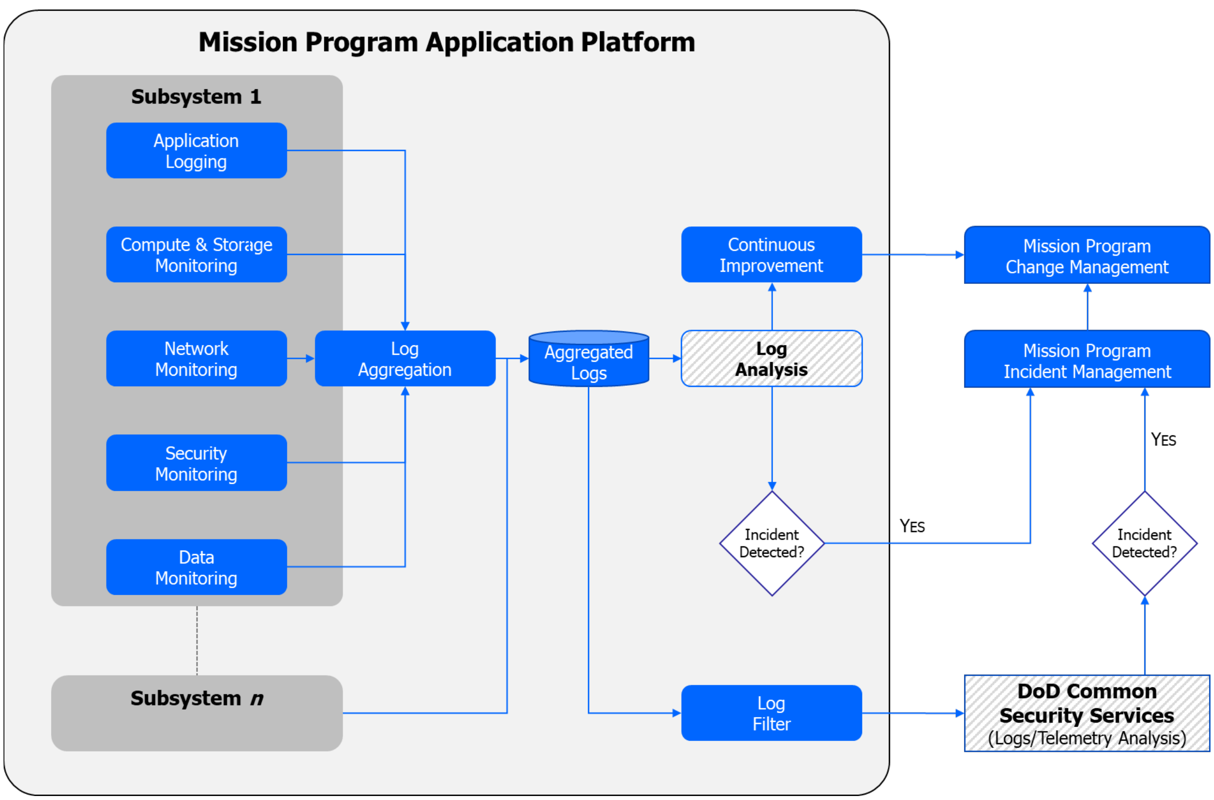


Figure 8: Logging and Log Analysis Process

Incidents will be forwarded to the relevant cybersecurity service provider(s) (CSSPs) to facilitate change request generation for incident resolution. The mission program incident management should alert or notify the responsible personnel about the incidents. The change request may be created to address the incident. These actions make the DevSecOps pipeline a full closed loop from secure operations to planning.

5.1.1 CSP Managed Services for Continuous Monitoring

The use of CSP managed services for monitoring alongside 3rd party security tools should always be viewed through a “both/and” lens instead of an “either/or” lens. CSP managed services can be utilized to monitor CSP resources & services, netflow, and entity behavior analysis at a deeper level than with 3rd party tools alone. It may also be possible to employ CSP managed services to perform log analysis (SEIM/SOAR). The monitoring ecosystem should rely on curated IaC to instantiate the monitored environment to the maximum extent possible, ensuring completeness and accelerating the A&A process.

CLEARANCE REQUEST FOR PUBLIC RELEASE OF DEPARTMENT OF DEFENSE INFORMATION

(See Instructions on back.)

(This form is to be used in requesting review and clearance of DoD information proposed for public release in accordance with DoDD 5230.09.)

TO: *(See Note)* **Chief, Defense Office of Prepublication and Security Review, 1155 Defense Pentagon, Washington, DC 20301-1155**

Note: Regular mail address shown above. For drop-off/next day delivery, use:
Room 2A534, 1155 Defense Pentagon, Washington, DC 20301-1155

1. DOCUMENT DESCRIPTION

a. TYPE: Document	b. TITLE: DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes
c. PAGE COUNT: 31	d. SUBJECT AREA: Software Modernization

2. AUTHOR/SPEAKER

a. NAME *(Last, First, Middle Initial)*: Lamb, George W.	b. RANK: GS15	c. TITLE: DevSecOps Lead
d. OFFICE: DCIO IE Cloud and Software Modernization		e. AGENCY: DoD CIO

3. PRESENTATION/PUBLICATION DATA *(Date, Place, Event)*

When approved, this will be posted to the DoD CIO Public Library. The changes to this document from v2.0 to v2.1 were captured in the DoD Enterprise DevSecOps Change Log which is also going through the public release process.

CLEARED
For Open Publication

Oct 22, 2021

2

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

4. POINT OF CONTACT

a. NAME *(Last, First, Middle Initial)*: Lamb, George W.	b. TELEPHONE NO. *(Include Area Code)*: (703) 629-6389

5. PRIOR COORDINATION

a. NAME *(Last, First, Middle Initial)*	b. OFFICE/AGENCY	c. TELEPHONE NO. *(Include Area Code)*

6. REMARKS

Version 2.0 was approved and posted to the DoD CIO Public Library Site. Some content has been updated and we are resubmitting for approval to publish Version 2.1.

7. RECOMMENDATION OF SUBMITTING OFFICE/AGENCY

a. THE ATTACHED MATERIAL HAS DEPARTMENT/OFFICE/AGENCY APPROVAL FOR PUBLIC RELEASE *(qualifications, if any, are indicated in Remarks section)* AND CLEARANCE FOR OPEN PUBLICATION IS RECOMMENDED UNDER PROVISIONS OF DODD 5230.09. I AM A GOVERNMENT EMPLOYEE *(civilian or military)*, AND NOT A CONTRACTOR, AUTHORIZED TO MAKE THIS RECOMMENDATION FOR RELEASE ON BEHALF OF:

DoD CIO and DCIO-IE

b. CLEARANCE IS REQUESTED BY 20211029 *(YYYYMMDD)*.

c. NAME *(Last, First, Middle Initial)*: Wolfkill, Timothy J.	d. TITLE: CSI Chief of Policy and Oversight/DOPSR Lead
e. OFFICE: DoD CIO	f. AGENCY: OSD/DoD
g. SIGNATURE: WOLFKILL.TIMOTHY.JAMES.1050511657 — Digitally signed by WOLFKILL.TIMOTHY.JAMES.1050511657 Date: 2021.10.20 14:54:58 -04'00'	h. DATE SIGNED *(YYYYMMDD)*: 20211020