A New Approach to Software Development for the DoD

www.blackpearl.us

Revolutionizing DevSecOps with an Enterprise-wide Software Factory Ecosystem

In its **Software Modernization Strategy**, the Department of Defense (DoD) defines its vision to "deliver resilient software capability at the speed of relevance."

Developing and deploying at speed requires seamless coordination across multiple software factories. To this end, DoD has set clear directives for establishing a Department-wide software factory ecosystem that uses the military's existing investments. DoD instructs agencies to use these enterprise-level services as a first choice before creating unique services.

This will enable developers across services to share code, use a common set of tools, and significantly accelerate security approvals for all software developed within that ecosystem.

Black Pearl—an enterprise service authorized by the Department of the Navy—is enabling Defense agencies to meet these goals. As the foundation for a software factory ecosystem, Black Pearl provides reusable pipeline components to all developers operating within the ecosystem. It supports both classified and unclassified environments, providing turnkey compliance and security for all levels.

Black Pearl allows agencies to quickly create new applications and continuously modify code in response to changing needs and priorities. All this is done within a secure framework that breaks down silos and unifies software development, deployment, security and operations.

Currently, the U.S. Navy is using Black Pearl as its DevSecOps platform in an effort to develop multiple capabilities and applications through various existing and upcoming software factories. When fully operational, it will link to other enterprise services and deploy capabilities to other cloud and tactical edge platforms.

Pre-existing ATO, centralized development, and pipeline essentials

Authority to Operate

DevSecOps teams can spend months getting Authority to Operate (ATO) approval for software systems—time that could be better spent developing the software. Black Pearl has ATO from the Navy, which shortens development timelines and can easily be reciprocated with other Defense agencies.

While serving as a stable, reliable platform, Black Pearl will constantly evolve to support new tools as they become available. It also supports policies that advance DevSecOps within DoD. For this reason, Black Pearl is a driving force for continuous ATO (cATO) within DoD—providing the flexible tools and environment to enable cATO across services.

A Shared DevSecOps Environment

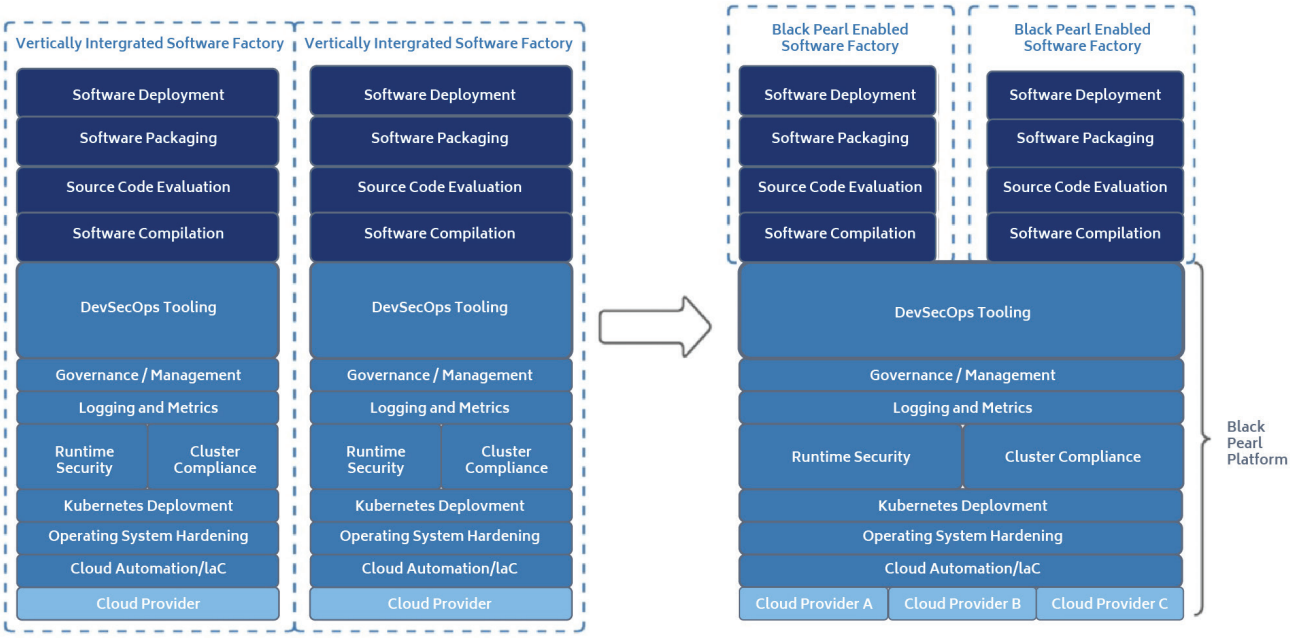
Black Pearl is a portfolio of DevSecOps products and services that support modern software development and delivery. The platform is anchored by a central development environment that provides all required building blocks for testing, delivery and deployment.

Black Pearl's common software environment provides commoditized DevSecOps tooling and pipeline component templates, integration infrastructure and compute. Together, these enable fast, cost-effective standup of software factories.

The platform centralizes the following capabilities—taking them out of their traditional silos and provisioning them across multiple factories:

- Turn-key and accredited tooling
- Host-level and runtime security, monitoring, and compliance
- Logging and metrics
- Zero-trust security
- Cluster-level and infrastructure-level compliance
- Standard interface formats for inter-software factory communications
- Infrastructure as code (IaC) and Configuration as code (CAC)
- The ability to stand up high-fidelity testing infrastructure in development environments
- The ability to stand up common environments at higher classification levels
- Expert guidance from seasoned DevSecOps practitioners

Figure 1. Black Pearl Removes DevSecOps Platform Silos Across Software Factories



Black Pearl's horizontal integration challenges the traditional software factory model

How it works

When a critical piece of software is developed to advance the mission, time is often short. DevSecOps has revolutionized the way the DoD approaches software development, but even that requires access to the right tools and infrastructure. By relying on a centralized DevSecOps environment, many of those challenges are mitigated and even eliminated.

After developers log into the web-based environment, accessible via Internet, they are presented with a set of tools for collaboration and task management, source code management and software analysis. In the case of Party Barge—a shared

development environment popular with Navy developers—those tools include Jira, Confluence and Gitlab. While there are plenty of other tools developers could use, Black Pearl strategically chooses tools that provide the optimal mix of functions and are likely to be well-known by a large community of developers.

Once inside the environment, developers have access to a rich set of resources, including templates for how to use the provided tools and reference implementations for creating a unique pipeline. These are recommendations to guide developers, but developers have the flexibility to integrate their own pipeline tooling.

Depending on the sensitivity of the development effort, developers can choose from two different approaches. For unclassified up to secret systems, developers can choose a public cloud-based common development environment. Effectively, this is a shared DevSecOps environment provided using a Software-as-a-Service (SaaS) model. Teams that do not have their own DevSecOps environments can rapidly onboard into the environment and start developing immediately.

For classified, sensitive or top secret projects, mission owners can choose to leverage the baseline, which Black Pearl calls Lighthouse, to deploy their own development environment. This environment can operate in a private cloud, a dedicated data center or at the tactical edge. The Lighthouse platform is the same baseline and technology used to deploy the Black Pearl common environment, but it can be tailored to mission-specific needs. The Lighthouse platform is also used as the foundation for the production runtime environment where applications will eventually be deployed. Mission owners can use Lighthouse to stand up their own DevSecOps environment or as the baseline platform for a mission application hosting environment. Additionally, the platform's core is a resilient, compliant, secure Platform as a Service (PaaS) that can speed the development of tactical and edge runtime platforms for difficult, cyber-hostile environments.

No matter which development environment is best suited for a given project, security and compliance are critical. Client host-level compliance enforcement, for example, ensures that anyone connecting to the environment is compliant with DoD policy. For example, Personally Identifiable Information (PII) requires encryption of data at rest on client devices. These policies are enforced in real-time by the Black Pearl system prior to accessing this type of information.

In addition to compliance, real-world security monitoring and enforcement is a primary goal within Black Pearl. To support this, Black Pearl's platforms are built to protect against many types of security breaches. For example, instead of relying on simple anti-malware scans, these platforms include a layer of behavioral analysis and runtime policy enforcement. Should an advanced adversary actively exploit a zero-day vulnerability and try to escalate permissions to control the system, the platform's built-in security tools will examine the request and compare it to the ways privileged users usually request permissions. If it is flagged as a problem, the request will be quarantined, and the Black Pearl team will be notified immediately.

What to look for in a DevSecOps platform:

- Options for classified and unclassified environments: No platform is one-size-fits-all, especially with the relative sensitivity of applications and data.
- ATO: Don't waste time waiting for an ATO. Instead, choose a platform that has already been approved.
- Host-level compliance: The platform should be able to automatically validate that resources requesting access to tools or code comply with DoD policy.
- Run-time security and enforcement: Look for top-level security functions that guard against a range of vulnerabilities, including double encryption at higher impact levels. If a vulnerability is suspected, the platform should immediately quarantine it and notify the platform owner.
- Standard interfaces: Choose a platform that is designed to cleanly interface with the rest of the DoD Software Ecosystem.
- High-fidelity integration testing: Look for a platform that has built-in integration testing environments and can host high-fidelity, mission-specific integration environments.
- A proven platform with a good pedigree: Platforms with real successes and experienced engineers demonstrate reliability and create less risk.

Benefits of a Centralized, Standardized Development Platform

Most agencies choose the platform approach to develop software at speed. Other use cases include:

- Quickly responding to cyber vulnerabilities in software
- Efficiently deploying software on vehicles or in the field
- Refactoring legacy systems into microservices
- Migrating applications to the cloud
- Rewriting legacy tactical applications to be more resilient and scalable
- Hosting applications in a secure cloud environment

Use Cases: Faster development, better collaboration, rapid innovation

One example of a successful software factory built on Black Pearl's capabilities is The Forge, a Program Executive Office Integrated Warfare System (PEO IWS) prototype and the Navy's first weapons system software factory. With 60 developers needing to collaborate, this type of software factory option was the clear solution. Built on Black Pearl infrastructure, it provides a physical and virtual space where developers can collaborate on developing, testing and distributing software for combat systems used by AEGIS surface combatants. Black Pearl's platform will enable developers to quickly write, test and deliver code to ships at sea, rapidly improving the warfighting capability and the ability to respond to emerging threats.

In a second instance, a DevSecOps team supporting F/A-18F/EA-18G chose to build its software factory on Black Pearl's platform—and achieved a better outcome than expected. During the software development process, it became clear that the F/A-18F group would need support for its Microsoft Windows-based software build, which the Black Pearl platform did not offer at the time. Together, the F/A-18F and Black Pearl teams partnered to develop and integrate the capability. With Windows capabilities now available, the F/A-18F team is now working to integrate Amazon Workspaces, which will enable it to provision virtual, cloud-based Windows desktops for users, eliminating concerns about lost or stolen devices.

A third use case is the Navy's Rapid Autonomy Integration Lab (RAIL). In this upcoming partnership, Black Pearl will support a development environment where the Navy can test and deliver autonomous capabilities for unmanned undersea vehicles. Using the Black Pearl platform, the RAIL development team will have the compute power and connected environment to perform loop testing against real hardware as part of the pipeline. RAIL is an important prototype for the Navy, which expects to increase its use of unmanned systems in the air, on the surface and underwater over the next several years.

To develop these projects within their own silo software factories would cost the Navy significantly more time, effort and personnel. But because all three are part of the same Black Pearl software factory ecosystem, they will be able to share code, test capabilities and learn from each other quickly to achieve optimal outcomes.

Embracing the software factory ecosystem for fast, effective software delivery

The U.S. military relies on fast, reliable delivery of software when and where it's needed, and is banking on software factories to deliver those capabilities. But while DoD has stood up dozens of software factories in the past few years, many of them stand alone—needlessly re-inventing processes and technologies that result in unacceptably slow software delivery. By standardizing on a platform, developers can take advantage of existing components and focus on parts of the development that make a difference to the mission.

With multiple divisions on the same platform, a centralized environment will grow over time, creating a common systems integration and testing infrastructure. Each will benefit from the efforts of the other, and the pace of development will only accelerate. This is exactly the type

of ecosystem DoD has in mind—one that enables efficient software development and more effective collaboration. And by standardizing on a solution that already complies with all security and compliance requirements, has ATO approval and is backed by an experienced DevSecOps team, Defense agencies can get to the business of developing cutting-edge software.

Black Pearl is also working to develop software factory interfaces to facilitate the interchange of artifacts between the various software factories within DoD. This will enable the integration of Software Factories, both within and outside of Black Pearl. In turn, this will create software pipelines that can truly take software from source code to tactical platform.

DoD Guidance on Software Factories

DoD Software Modernization Strategy sets goals for creating a software factory ecosystem where agencies can share tools from one repository, speed development and deliver to warfighters faster.

DoD Enterprise DevSecOps Strategy Guide promotes use of software factories, urging agencies to seek existing platforms and leverage the cATO that comes with them.

DevSecOps Playbook states all custom software development should be driven through software factories. Agencies should leverage enterprise-level services before creating unique services.

About Black Pearl
Black Pearl is a group of military, civilian and contractor personnel with experience solving software delivery issues across the Defense environment. Our team understands the problems and needs of Defense programs seeking to accelerate delivery of capability to the warfighter.

Uses for a Centralized, Standardized Development Platform

- Tool standardization. With one environment of carefully curated tools for software analysis, source code management and collaboration and task management, everyone is working with the same finite number of tools.
- Easy access by developers, regardless of location. Internet-accessible development platforms eliminate the need to connect to a government network or route through a VPN during development.
- Easier collaboration. With everybody on the same platform, multiple software factories using the same tools can collaborate and share code easily.
- Built-in security and compliance. Instead of starting from scratch with security and accreditation, platforms like Black Pearl have done the work ahead of time.
- No need for patching and upgrading. Using a subscription-based development platform means that all available resources will be current, secure and available.
- Built-In Accreditation. Black Pearl's common environment has a Navy-wide, blanket authorization to simplify customer onboarding and remove the burden of authorizing new factories one by one.
- Saved time and money. With a preconfigured suite of tools, inherent security and streamlined access, a standardized platform like Black Pearl allows developers to work faster and focus on outcomes.

Black Pearl serves as the foundation for software factories and provides building blocks for tactical deployment. Black Pearl offers two different platforms for developing software factories: the common environment for rapid standup of software factories, and Lighthouse for deployment of software factories for sensitive workloads.

Our experts can also help Defense agencies with agile development, IT modernization, digital transformation, prototype development, and lean management. When needed, Black Pearl can also help programs deploy their tools into target environments, from the cloud to a vessel or aircraft, and function as adjunct software developers for projects as necessary.