SOLUTION BRIEF

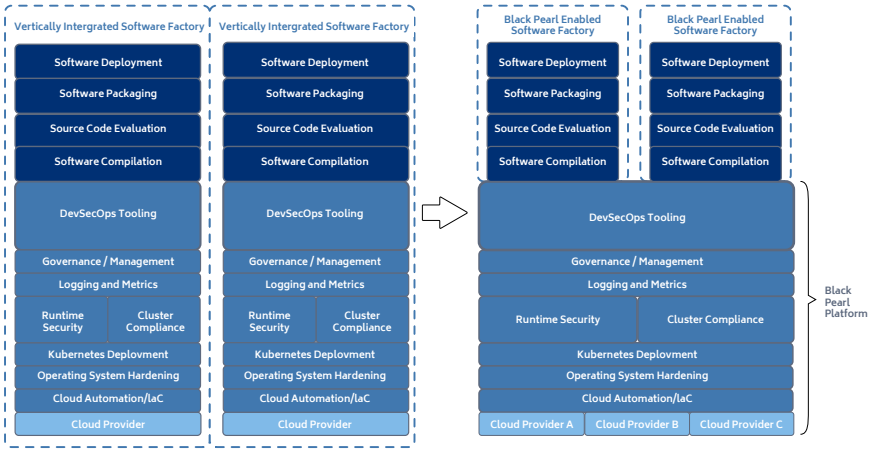
Sigma Defense DevSecOps Platform

Sigma Defense enables fast, secure stand-up of software factories with less cost and complexity than building from the ground up.

The U.S. military requires fast, reliable software delivery to maintain technological superiority—at home and at the tactical edge. Increasingly, DoD is relying on software factories to deliver those capabilities. By standardizing on a common platform, developers can take advantage of existing components and focus on parts of development that make a difference to the mission.

The **Sigma Defense DevSecOps platform** provides reusable pipeline components to all developers operating within the ecosystem. While stable and reliable, it can evolve to support new tools and lets teams **quickly create or iterate on capabilities** as needs change. It provides turnkey compliance and security for all levels—all within a **secure environment** that unifies software development, deployment, security and operations.

Sigma Defense is delivering these capabilities via **Black Pearl**—an enterprise-wide DevSecOps portfolio of people, processes, and technologies for modernizing the Naval software practice. **Party Barge**, a component of Black Pearl, is the common DevSecOps environment offered as a SaaS to the Naval enterprise. Together, they are the foundation for the Navy's software factories and provide the building blocks for tactically deploying new applications and configuration toolsets. Black Pearl's pre-existing **ATO from the Navy** speeds development, removes the need to authorize new factories one by one, and can be easily reciprocated by other DoD agencies.



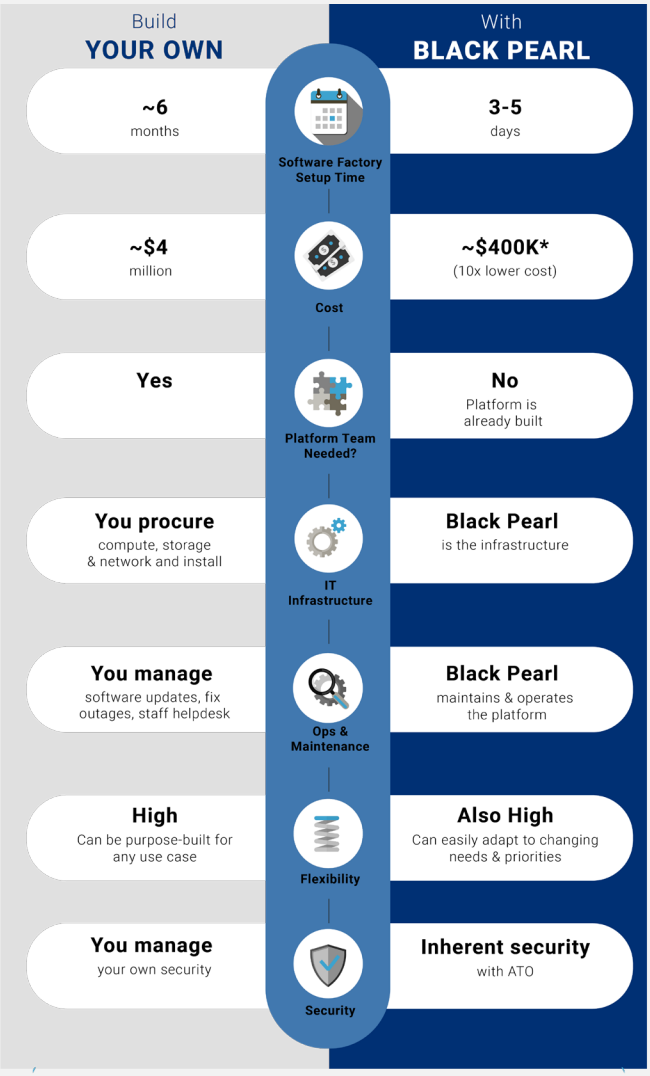
Black Pearl's horizontal integration challenges the traditional software factory model

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

- Turnkey 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
- The ability to stand up common environments at higher classification levels
- Expert guidance from seasoned DevSecOps practitioners

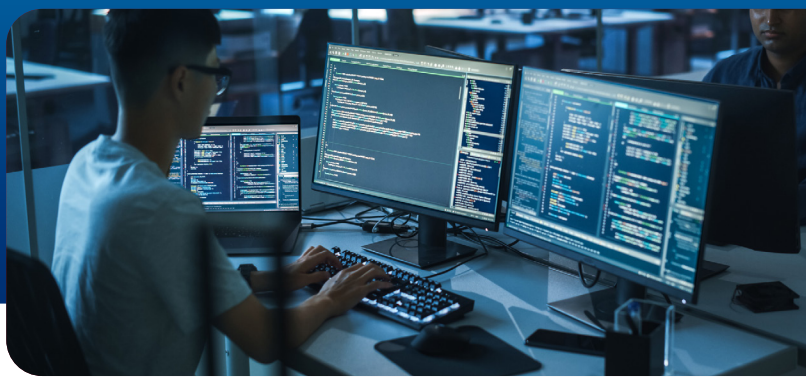
Benefits of a Centralized, Standardized Development Platform

- **Tool standardization.** Developers work with a shared set of curated tools for software analysis, collaboration, task management, and source code management.
- **Easy access from any location.** Internet-accessible platforms remove the need to connect to government networks or route through a VPN.
- **Easier collaboration.** With all developers on the same platform, multiple software factories can collaborate and share code easily.
- **Built-in security and compliance.** Instead of starting from scratch with security and accreditation, the platform satisfies these ahead of time.
- **No need for patching and upgrading.** A subscription-based platform assures all resources are current, secure, and available.
- **Saved time and money.** Preconfigured tools, inherent security and streamlined access help developers work faster and focus on outcomes.



Sigma Defense's DevSecOps Platform Delivers:

- **Authority to Operate (ATO).** Built-in accreditation simplifies onboarding and development, with reciprocity across DoD.
- **Host-level compliance.** Validates that resources requesting access to tools or code comply with DoD policy
- **Run-time security and enforcement.** Top-level security functions guard against diverse vulnerabilities; includes double encryption for higher impact levels
- **Standard interfaces.** Designed to cleanly interface with the rest of the DoD software ecosystem
- **High-fidelity integration testing.** Hosts mission-specific testing in real-world environments
- **A proven platform.** Demonstrated history of delivering measurable results to DoD



Sigma Defense