KARTHIK CONSULTING
Beyond the expected

3120 Fairview Park Drive
Suite 800
Falls Church, VA 22042
www.karthikconsulting.com

AT A GLANCE

# SDLC-Wide Security via a Software Factory with Continuous ATO

## KEY SCOPE AREAS

- Design, develop, and implement Coast Guard's DevSecOps Platform capabilities and processes for building software - including cloud services
- Provide continuous compliance with security requirements and continuous software deployment
- Enhance and simplify security-related reporting and remediation, including historical results of code scans and runtime assessments of common vulnerabilities and exposures (CVEs) and threats
- Facilitate secure application operations, covering deployment and runtime
- Meet DoD/DHS requirements for continuous Authorization to Operate (cATO) designation

## KEY STATS

- Authorized to run in up to DISA-certified Impact Level (IL)-5 environments
- First system across all DHS components to be designated for cATO
- cATO-designated Software Factory permits the creation of reusable agency-wide DevSecOps CI/CD pipelines
- Support for rapid Certificate to Field (CTF) issuance baked into CI/CD pipelines, for all applications built by the Software Factory
- Replaces the need for traditional time-consuming ATO with repeatable CTF, allowing continuous deployment of software… saving time, money, and effort

### KC CUSTOMER IN FOCUS

The US Coast Guard's (USCG's) Command, Control, Communications, Computers, Cyber and Intelligence Service Center (C5ISC) contracted with Karthik Consulting (KC) to collaboratively develop, test, implement, and sustain a Software Factory (SF) solution. USCG dubbed their solution the High Efficiency Rapid Modernization Network (HERMN), which embodies methods for translating commercial practices and DoD requirements into repeatable self-sustaining processes for establishing, growing, operating, and adapting scalable, high-quality, and secure in-house agile software operations.

### SIGNIFICANCE OF REQUIREMENTS

In addition to the quality and productivity gains realized by automating DevSecOps practices via the USCG SF, KC developed the solution within AWS GovCloud at IL-5 to meet the federal government's new cATO requirements. This provides USCG with an agency-wide solution that significantly reduces the time and costs to deploy new software releases for any application processed through the SF. Furthermore, to improve security and support multi-cloud capabilities plus cloud agnosticism, the SF complies with the DoD DevSecOps Reference Architecture and the Secure Cloud Computing Architecture (SCCA) – and is built on Cloud Native Computing Foundation (CNCF) and Zero Trust (ZT) principles.

The KC-built solution leverages various automated security processes to continuously maintain and improve the security posture of both the SF and the applications built through it – thereby streamlining CTF issuance. This includes: a library of baselined container images, auto-refreshed from DoD-approved container repositories; threshold-configurable security gates integrated into code builds; code signing; SBOM generation and tracking; storage and trend analysis of build artifacts.

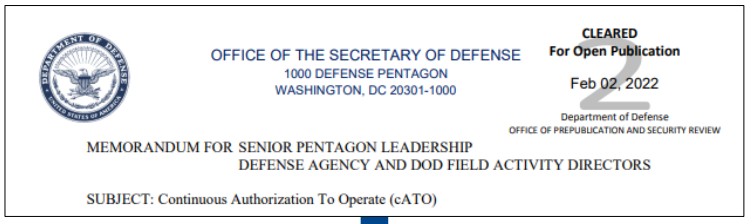
*Continued on next page*

## DELIVERED RESULTS

KC's solution aligns with and demonstrates the three competencies required per the DOD's cATO memo:

**(1) Continuous Monitoring (CONMON)**

- The USCG SF conducts various types of scans of each application as it proceeds through the CI/CD pipelines, such as supply chain (SBOM), static and dynamic vulnerability analysis, code quality, code coverage, 508 compliance, container scans, OpenSCAP scans for STIGs, AWS WAF and NIST SP 800-53 scans.
- The solution automatically generates, analyzes, and stores the required artifacts from each step/gate in the pipeline for each build of each branch of each application.
- The SF collects, analyzes, and presents the generated artifacts to Security Teams so they can make the determination to issue the CTF for each application, thereby eliminating the need for a laborious RMF-based ATO.
- By storing data related to each build's scans, the AO can view the historical progression of the application over the course of all branches of code and versions.
- The SF employs native AWS and other tools to detect drift between approved baselines and any runtime environment.


OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

CLEARED
For Open Publication
Feb 02, 2022
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Continuous Authorization To Operate (cATO)

### Competencies to Demonstrate

1. **CONMON:** On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls
2. **Active Cyber Defense:** The ability to conduct active cyber defense to respond to cyber threats in real time
3. **Secure Software Supply Chain:** The adoption and use of an approved DevSecOps reference design

**(2) Active Cyber Defense**

- The solution has built-in configurable security gates and thresholds throughout the progressive stages of each CI/CD Pipeline (DEV, TEST, STAGE, and others as configured by the user for each application). Hence, through the execution of these pipelines, the applications proceed through an automatic risk determination based on the AO's prescribed risk tolerance – resulting in an application being automatically authorized for deployment once it meets the AO's specified criteria. This ensures that only adequately secure applications are deployed to Production. Additionally, an AO can configure progressively restrictive pipeline gate thresholds as the code is promoted from lower to higher stages (e.g., DEV to TEST).
- CI/CD pipelines leverage tools to ensure application compliance with FISMA/RMF standards, CNCF, and DISA STIGs.
- Upon drift detection, post deployment, the solution can alert individuals to the potential threats and can also be configured to automatically apply remediation actions.

**(3) Secure Software Supply Chain**

- Implements DoD DevSecOps Reference Design best practices such as: CNCF based multi-cloud support, service mesh, baseline image management using hardened containers from DoD's DCAR (Iron Bank), SAST/DAST scanning, and two or more vulnerability scanners.
- The SF automatically generates a Software Bill of Materials (SBOM) during build. Consequently, the Software Factory ensures the accuracy of any generated SBOM and the integrity of the corresponding app's build. The solution tracks the SBOM for each build, and thus institutes a rigorous and historical Configuration Management (CM) process. This also allows the SF to quickly determine the attack surface or impact of any newly-surfaced vulnerability on any application in the factory's purview.
- Leveraging the contents of each deployed app's SBOM, the SF continues to scan deployed code and dependencies to ensure the detection and subsequent remediation of vulnerabilities in deployed applications.

### SOFTWARE FACTORY STANDARDS, BEST PRACTICES, AND TOOLCHAIN

kubernetes · DISA · SCCA · GitLab · Selenium · JMeter · JSDoc · sonarqube · grype · trivy · CORESTACK · OpenSCAP

*Sample tools are noted. The SF's flexible design is tool agnostic.*

*Continued on next page*

# KEY AREAS OF KC IMPACT

## Better Security

By integrating the appropriate tools into the CI/CD Pipelines, the KC Software Factory improves the security of deployed applications.

- Factory tools provide feedback to developers to correct the most important security threats in their code, thus turning data (generated from various scanners) into actionable information.
- Beyond improved security, customers realize cost and time savings since the SF focuses development efforts on the most important security issues.
- With drift detection tools and continuous scanning of deployed applications, the solution can proactively detect and remediate security issues in runtime environments.

## Cost Savings

The SF provides automation throughout the DevSecOps process

- In development (Dev) with CI/CD pipeline tools
- In security (Sec) with tailored security gates and thresholds providing continuous metrics and refreshed dashboards
- In operations (Ops) with application upgrades and patches to address newly surfaced security concerns, application enhancements, and remediations for detected issues

With earlier detection and greater automation comes reduced labor costs, allowing customers to allocate budgets to other applications and enhancements, thus improving customer satisfaction.

## Time Savings / Improved Customer Satisfaction

The solution is a secure foundation which continuously generates security-related metrics that provide visibility into each application's security posture.

- This visibility, combined with the robustness of the CI/CD processes, give an Authorizing Official (AO) the confidence they need to permit Continuous Deployment.
- Thus, the SF enables the continuous deployment of new applications versions, bypassing the labor-, cost-, and time-intensive traditional RMF-based ATO process.
- Importantly, with faster deployments of new secure versions of applications, organizations can better meet their mission.

## Quality Improvements

- A robust CI/CD toolset facilitates improvements in application quality and better security risk management.
- By providing developers with a single pane of glass (dashboard) which ingests, processes, and displays the appropriate data from the CI/CD lifecycle and toolset, the SF identifies security issues much earlier in the SDLC – thereby helping developers address those issues more efficiently with higher quality, including design changes.

**ABOUT US**

Karthik Consulting was founded in 2008 to be a reliable and trusted advisor for our customers, providing independent, unbiased, and proven solutions that mitigate risk and help solve enterprise-wide IT challenges.

Our Cyber Security, Software Development and Program Management focus areas (and work methodology) ensure that we can deliver not just solutions, but architecture that scales and grows with the customer's needs over time. We are able to assist in projects ranging from short advisory engagements to assembling a full team to deliver a solution from concept through implementation and on-going management. KC has access to industry experts in various technologies and teaming partners to meet any of your IT challenges. The vision of KC is to bring the innovation, passion and agility of the commercial IT industry to meet the unique challenges of the federal government. We are a DOD Cleared Facility with a DCAA-approved accounting system.

**CONTACT**
Felix Martin, 571 435 7632
fmartin@karthikconsulting.com

**CAGE: 56GH3**
**DUNS: 828199880**
**UEI: FGNNM7KNUPF6**

**PRIME CONTRACT VEHICLES:**
GSA STARS III 8(a)
GSA MAS
GSA OASIS Pool 1 and 3
NIH CIO-SP3 8(a) & SB
Air Force SBEAS
Army RS3
Navy Seaport-NexGen
FAA eFAST