DEPARTMENT OF THE NAVY
SBIR/STTR TRANSITION PROGRAM

SUCCESS STORY

TOPIC NUMBER: AF192-001

SBIR INVESTMENT: $999,808

PHASE III FUNDING: $59,645,680

EMBEDDED CYBER RESILIENCY (ECR) TOOL SUITE

G2 Ops' methodology and tool suite support the design of a new cybersecurity system for surface Navy ships and will enable future development of NAVSEA cloud brokerage services.

G2 Ops, Inc.

POC: Kevin Esser
757-578-9091
Virginia Beach, Virginia 23452

www.g2-ops.com

THE CHALLENGE

The Naval Sea Systems Command (NAVSEA) Cyber Engineering & Digital Transformation directorate developed the Situational Awareness, Boundary Enforcement & Response (SABER) system to provide cybersecurity defenses on board Navy surface ships. SABER is a boundary defense and situational awareness system that performs continuous monitoring of Naval Control Systems. SABER is integrated within different platform enclaves to identify, protect, detect, respond to, and recover from cyber events. NAVSEA sought a comprehensive, innovative digital approach to managing the complex and dynamic SABER design, including automated approaches to supporting all of its engineering, cybersecurity and deployment requirements.

THE TECHNOLOGY

G2 Ops has developed a suite of tools and specialized methodologies to make the enumeration and analysis of complex system of systems more efficient and effective. The Embedded Cyber Resiliency (ECR) tool suite enables mission-based cybersecurity analytics, security control decomposition and mapping to capability, detailed architectural configuration management and automated generation of artifacts required by a wide spectrum of systems engineering activities. The tool suite includes digital model capture and manipulation, as well as niche data parsing capabilities that enable the ingest and mapping of numerous data sources that are used to enrich the model. The ECR solution integrates traditionally separate systems and security engineering activities, providing for the rapid and automated analysis of system designs, engineering baselines, cybersecurity and mission resiliency, and proposed system changes throughout the system lifecycle.

THE TRANSITION

G2 Ops created its ECR tool suite and associated methodologies through SBIR Phase I and Phase II awards sponsored by the Air Force under an Open Call topic (Innovative Defense-Related Dual-Purpose Technologies/Solutions).

The Air Force sought a new framework to evaluate the integrated systems that make up a commercial aircraft platform and determine the adaptations that would be required to make those systems resilient enough to meet DoD requirements. At the conclusion of the Phase II, the Air Force did not have an immediate path to transition the technology. The Navy awarded G2 Ops a Phase III to apply its methodology, the ECR tool suite, and its associated analytical framework to SABER.

THE NAVAL BENEFIT

By applying the ECR tool suite and associated methodologies to the SABER program, G2 Ops rapidly created a digital model that all groups involved in the SABER design process can use to manage data. This model replaces former tools that led to stovepiped processes in which the design, logistics, acquisition, and cybersecurity teams each used different product stacks to accomplish their work. The ECR analytical framework has been used to perform cyber resiliency analyses of SABER operations, to conduct granular evaluations of security controls application at the configuration item level, and to map SABER requirements to capabilities and standardized ontologies like MITRE's D3FEND to comprehensively evaluate the posture of the system and its development environment.

THE FUTURE

G2 Ops' ECR solution is currently supporting the development and deployment of SABER. NAVSEA plans to expand its application to assist in evaluating capability changes at the individual platform variant level and expanding the use of threat data mapping to various implementations to enable a more granular evaluation of system posture. These implementations move NAVSEA closer to creating an efficient and unified data environment to support large, rapid growth of Navy IT services while proactively addressing cyber threats.

Published 2024