Topic: N181-051

G2 Ops, Inc.

Unified Cybersecurity System Modeling of Naval Control Systems

Strategic Optics for Intelligent Analytics (SOFIA) is a mission-based cyber risk management tool that allows evidence-based assessments of a system's cybersecurity posture. SOFIA's centralized repository integrates vulnerability data – attack vectors – compatible with the NIST Risk Management Framework (RMF). G2 Ops, Inc. utilizes advanced Model-Based Systems Engineering (MBSE) methodologies to capture the architectural and functional characteristics of complex system interfaces in a high-fidelity model – digital twin. Dashboards and interactive reports allow threat analysts to implement dynamic configuration changes, isolate known vulnerabilities, identify undiscovered attack vectors through simulation and historical trend analysis, autogenerate RMF compliance artifacts, and monitor the impact of emerging threats on mission-critical operations and assets. Any organization (Program Office, SYSCOM) with a need for cybersecurity analysis and automated RMF compliance analysis can use SOFIA.

Technology Category Alignment:

Cyber
Modeling and Simulation Technology
Command, Control, Communications, Computers, & Intelligence (C4I)

Contact:
Kevin Esser
kevine@g2-ops.com
(757) 578-9091
https://g2-ops.com/
SYSCOM: NAVSEA
Contract: N68335-19-C-0550

Corporate Brochure: https://navystp.com/vtm/open_file?type=brochure&id=N68335-19-C-0550

Tech Talk: https://www.youtube.com/watch?v=y3K3wzWITBA

Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

NAVSEA #

Topic # N181-051

Unified Cybersecurity System Modeling of Naval Control Systems

G2 Ops, Inc.

WHO

SYSCOM: NAVSEA

Sponsoring Program: PEO IWS 1.0

Transition Target: AEGIS and Ship Self Defense System (SSDS)

TPOC:

Other transition opportunities: Cooperative Engagement Capability (CEC), Submarine Warfare Federated Tactical System (SWFTS), Submarine Operations Authority WAN (SWAN), Common Submarine Radio Room (CSRR), Consolidated Afloat Network Enterprise Services (CANES), Navy Tactical Grid (NTG), COLUMBIA Class SSBN, USAF Ground Based Strategic Deterrent, USAF Future Carrier Aviation (FCA).

Notes: SOFIA utilized the Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM) framework for software security during development. SOFIA is Section 508 compliant.

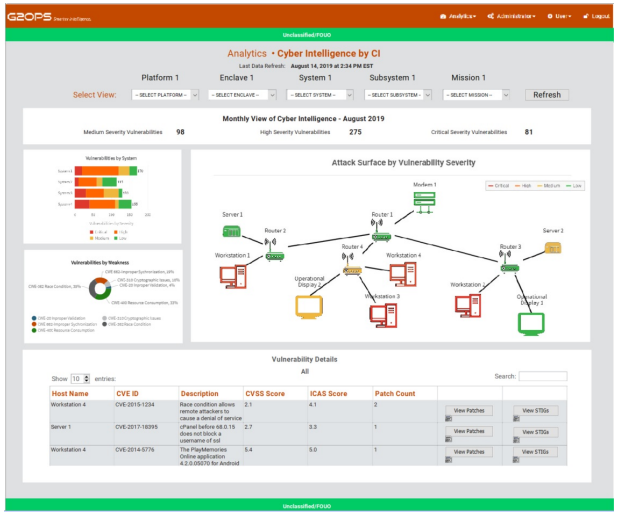

Image Courtesy of G2 Ops, 2020-07-14

WHAT

Operational Need and Improvement: Conducting traditional systems of systems analysis across stove-piped models and artifacts impedes the cybersecurity analysis conduct. A unified model facilitating the cybersecurity analysis of Naval Control Systems (NCSs) is necessary for system engineers, and no software tools providing this analysis currently exist. Understanding how cybersecurity vulnerabilities can impact Navy missions, if exploited, results in better system architectures and designs. Cultivating efficient cyber functionality and cyber-resilient designs through optimizing cybersecurity postures within mission context reduces cyber-related acquisition and maintenance costs.

Specifications Required: A unified cybersecurity system model creation tool incorporating the key system attributes required for cybersecurity analysis of any NCS; portable to any NCS (tuned to correlate cyber posture to mission performance). Attributes include the physical architecture, data flows, and performance requirements; and deployed software components and operating environments. Other attributes include mission threads executed by the system and system component dependencies, system component partitioning, system states and modes, system cybersecurity protections, vulnerabilities, posture, threats, and penetration pathways. The tool will enable attribute alteration, allowing the exploration of "what-if" scenarios in near real-time.

Technology Developed: Our software tool, Strategic Optics for Intelligent Analytics (SOFIA), provides vulnerability assessments of a system's cybersecurity posture in a centralized repository. Using Model-Based Systems Engineering (MBSE), SOFIA captures the sophisticated characteristics of NCSs and their external interfaces in a digital twin model—at any phase of its acquisition lifecycle, then maps the associated model's cyber assets attack vector space. The unified platform allows dynamic configuration changes, known vulnerability isolation, attack vector discovery through simulation and historical trend analysis. It continuously evaluates the impact of the evolving mission-critical cyber threat landscape.

Warfighter Value: Fielding more cyber-resilient systems reduce operational impacts due to cyber-attack and improve system and warfighter effectiveness. SOFIA's models enable optimization of cybersecurity architectures, driving up critical system operational resiliency while lowering maintenance and sustainment costs. SOFIA's MBSE-based architectural models also speed the process execution and artifact generation for Risk Management Framework (RMF).

WHEN

Contract Number: N68335-19-C-0550 **Ending on:** June 12, 2021

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Phase I	Low	Near real-time data ingestion of public vulnerability sources	3	August 2019
Phase II	Low	Integration with data feeds that assist in preparing the FY budget using product de-support dates	4	June 2020
Phase II	Med	On-demand, dynamic threat simulation capability to provide candidate remediation strategies	5	October 2020
Phase II	Med	Analysis of network connectivity and pathways between hosts to define multiple levels of mission criticality	5	March 2021
Phase II	Med	Prototype Operational Demonstration	6	March 2021

HOW

Projected Business Model: G2 Ops will license SOFIA processes and tools directly to prospective customers on an annual per-seat basis and will provide technical assistance for setup. Separate MBSE consulting services can be procured to build an end-to-end architecture model of a given system to capture and map hardware, software, interfaces with associated mission threads (or business processes) to enable a comprehensive evaluation of cybersecurity posture and system operational readiness.

Company Objectives: G2 Ops, Inc. provides innovative solutions to address complex challenges in the cybersecurity and systems engineering spheres. Utilizing MBSE methodologies and tool suites, we offer a pathway forward for digital transformation, identifying cyber risks, and optimizing system resiliency. G2 Ops is a recognized MBSE innovator responsible for developing integrated modeling environments that reduce the costs and risks associated with complex design evolution, integration, modernization, cyber vulnerability, and sustainment operations.

Potential Commercial Applications: Any organization (Program Office, SYSCOM) with a need for cybersecurity analysis conducted within an operational/mission context will benefit from SOFIA. Organizations with RMF process execution requirements will benefit from SOFIA's efficiencies and associated MBSE models in conducting vulnerability analyses and auto-generating required RMF artifacts. Partnerships are possible with organizations with complementary products, tools, or processes that allow rapid expansion of SOFIA's core capabilities. An example would be an IT Service Management (ITSM) tool that allows the rapid consumption of hardware, software, and services. Another example would be a message trafficking tool enabling real-time analysis and pattern detection for anomalies.

Contact: Kevin Esser, Chief Business Officer
kevine@g2-ops.com 757-578-9091