Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVSEA #2022-0335

Topic # N191-030
Risk Reduction and Resiliency Modeling Software for Industrial Control Systems
G2 Ops, Inc.

WHO

SYSCOM: NAVSEA

Sponsoring Program: NAVSEA

Transition Target: NAVSEA

Other Transition Opportunities: Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems across National Security Systems (NSS),Critical Infrastructure such as manufacturing, water, electric, power industries, international maritime industry, and Hull, Mechanical, and Electrical (HM&E) integrated systems

Notes: IRIS utilized the Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM) framework for software security during development

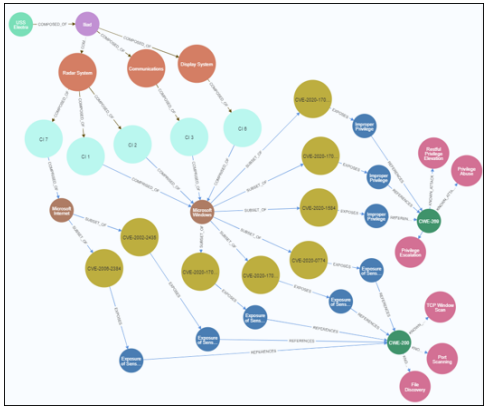

Image Courtesy of G2 Ops, 2022-08-12

WHAT

Operational Need and Improvement: The landscape between operational technology (OT) infrastructures and traditional informational technology (IT) presents challenges to cyber vulnerability analysis, especially for government-off-the-shelf (GOTS) and proprietary devices. Atypical IT environments and the complexity of control system design can limit an organization's ability to measure cyber resilience across integrated systems. Understanding how vulnerabilities, if exploited, can impact the resiliency of business operations, results in better system architectures and designs thereby reducing cyber-related acquisition and maintenance costs.

Specifications Required: A unified cybersecurity system model creation tool incorporating the key system attributes required for cybersecurity resiliency 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 operational threads executed by the system and system component dependencies, system component partitioning, system cybersecurity protections, vulnerabilities, threats, and penetration pathways. The tool will allow graph-based exploration of resiliency scenarios in near real-time.

Technology Developed: Our graph analytics tool, Industrial Control System (ICS) Resiliency Information System (IRIS), evaluates the resiliency of an ICS in conjunction with processes and operations in a centralized repository. Using Model-Based Systems Engineering (MBSE), IRIS captures the sophisticated characteristics of complex systems 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. Customized resiliency metrics allow the user to easily perform connectivity analysis of their system and understand cyber assets shared across their architecture. More than a dozen open-source cyber threat intelligence sources are curated and housed in IRIS's data repositories. Reusable libraries and classification schemas relate the system's architectural components to globally identified cyber intelligence to reduce the amount of time required to perform vulnerability and resiliency analysis.

Warfighter Value: Fielding more cyber-resilient systems reduces operational impacts due to cyber-attacks and improves system and warfighter effectiveness. IRIS's models enable optimization of cybersecurity architectures, driving up critical system operational resiliency while lowering maintenance and sustainment costs. IRIS's MBSE-based architectural models also speed the process execution and enhance the traditional Risk Management Framework (RMF). Customizable metrics and device classification schemes allow for broader measurements of the potential vulnerability of atypical IT environments that include ICS devices.

WHEN

Contract Number: N68335-21-C-0171 **Ending on:** May 25, 2022

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Phase I	Low	Near real-time data ingestion of public vulnerability sources	3	2nd QTR FY20
Phase II	Low	Measure impact of vendor and STIG support & obsolescence notices	4	3rd QTR FY21
Phase II	Low	On demand, dynamic threat simulation capability to provide candidate remediation strategies	4	1st QTR FY22
Phase II	Medium	Analyze network connectivity and pathways between hosts to define resiliency metrics	5	3rd QTR FY22
Phase II	Medium	Prototype Operational Demonstration	6	2nd QTR FY23

HOW

Projected Business Model: G2 Ops will provide customers direct access to IRIS processes and tools as well as provide technical assistance for setup.

Company Objectives: Utilizing our G2 Ops proprietary MBSE based Gold Standard Methodology (GSM) and developmental ecosystem, we identify cyber risks and provide system optimization resiliency. Our GSM practices reduce costs and risks associated with complex design evolution, integration, automation, cyber vulnerabilities, and sustainment operations.

Potential Commercial Applications: Any industry that relies on a complex network architecture can take advantage of the graph analytics envisioned for IRIS. This technology also has potential commercial transition to ICS/SCADA systems throughout National critical infrastructure. ITAR restrictions may be a factor if this technology is integrated into international maritime applications. The resiliency of ICSs is a cross-cutting, critical capability need. The insight provided by IRIS to aid in risk reduction and resiliency analysis is agnostic of military or commercial domains. Possible other uses include large industrial plants in the manufacturing, water, electric, and power industries.

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