November 2023

NAVY SBIR TRANSITION PROGRAM SPOTLIGHT

**Company:** G2 Ops
**Website:** https://g2-ops.com/

**POC:** Kevin Esser
**Phone:** 757-578-9091

**Address:** 2829 Guardian Lane, Suite 150
Virginia Beach, Virginia 23452

# Evaluating Cyber Risk: G2 Ops‘ Tools and Methodologies Enhance Navy Capabilities

By Jennifer Reisch

“Collaboration is essential for Phase III transitions,” said Kevin Esser, chief business officer at G2 Ops. “Collaboration spanning the program office that needs the technology, the contracting organization—whether that‘s NAVSEA, GSA, NAVAIR or another command, and the small business itself.” Esser has successfully transitioned two out of four Phase II SBIR technologies to the Navy. A third SBIR project, still in Phase II, has already transitioned portions of the technology. “A lot of companies don‘t think about that collaborative requirement. It might be that they don‘t have the resources or the know-how to collaborate with the Navy to construct a workable Phase III vehicle.”

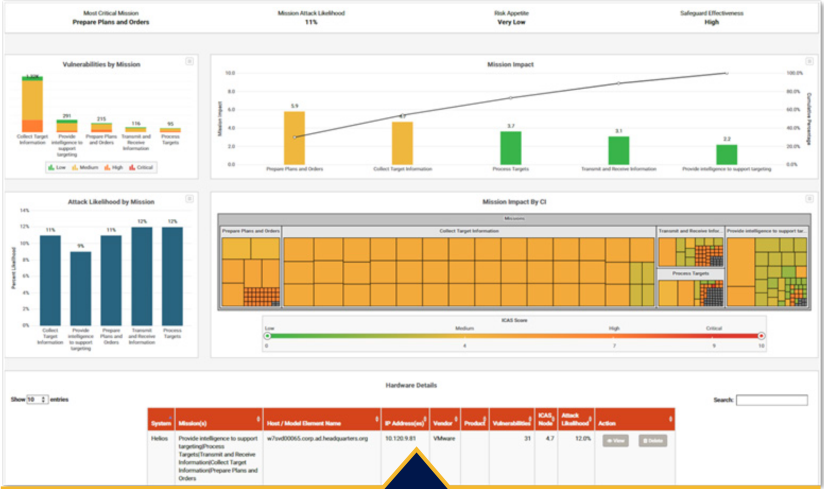
G2 Ops uses model-based systems engineering (MBSE) to address systems engineering and cybersecurity challenges. The company develops and applies modeling tools and analytics to improve systems engineering and uncover cyber strengths and weaknesses in tactical system design.

The first technology G2 Ops transitioned to the Navy was Strategic Optics for Intelligent Analytics (SOFIA), a mission-based cyber risk assessment tool, developed in collaboration with PEO Integrated Warfare Systems (IWS) 1.0, the developers of AEGIS Combat Systems. “What made this so special was that we were already working with the Navy in both model-based systems engineering and risk management, and the need spelled out in their SBIR program spanned the two areas that we were working on independently,” explained Corren McCoy, PhD, chief data strategist at G2 Ops. “It was an opportunity for us to bring two of our areas of expertise together into one solution. IWS 1.0 and NAVSEA are really trying to be forward leaners in digital engineering.”

G2 Ops’ ability to leverage existing work proved attractive to the Navy. “I think the fact that we had a structured and known approach that followed the Navy SOP for risk management gave them confidence that what we could deliver would be a sound solution,” McCoy said.

The name SOFIA is derived from the Greek word for wisdom. “That‘s what we‘re providing here: insight into the cyber posture of a tactical platform and the impact of cyber vulnerabilities on mission-based risk. Classical risk assessments focus on the component level, which does not give a true operational picture of where risk really resides. The beauty of this tool is that the systems modeling language models we create of the baseline architectures flow into a hierarchy that allocates components to the systems and missions they support. The digital engineering models give layered context to the way that a platform operates: not just its physical attributes, but its behavioral attributes—how they interrelate, downstream impact—and then risk-scored through an overlay against open-source intelligence data that we collect.”

For SOFIA, G2 Ops established a data pipeline encompassing over a dozen open-source intelligence databases. This pipeline provides cybersecurity engineers with ready access to data that is typically constrained due to concerns that open-source intelligence can resemble malware and trigger protection mechanisms on Navy networks. G2 Ops scrubs and associates the data with the attack surface, creating a clean repository for risk scoring at various levels using SOFIA’s algorithms and hardware and software descriptions in the system models. The resulting risk assessments can be applied to missions, offering a customizable approach to mission risk assessment and quantifiable reduction in known cyber vulnerabilities, McCoy explained.



| Most Critical Mission | Mission Attack Likelihood | Risk Appetite | Safeguard Effectiveness |
|---|---|---|---|
| Prepare Plans and Orders | 11% | Very Low | High |

Vulnerabilities by Mission
1.32K
291
215
116
95
Collect Target Information
Provide intelligence to support targeting
Prepare Plans and Orders
Transmit and Receive Information
Process Targets
Low
Medium
High
Critical
Mission Impact
10.0
8.0
6.0
4.0
2.0
0.0
Mission Impact
5.9
4.7
3.7
3.1
2.2
Prepare Plans and Orders
Collect Target Information
Process Targets
Transmit and Receive Information
Provide intelligence to support targeting
100.0%
80.0%
60.0%
40.0%
20.0%
0.0%
Cumulative Percentage
Attack Likelihood by Mission
14%
12%
10%
8%
6%
4%
2%
0%
Percent Likelihood
11%
9%
11%
12%
12%
Collect Target Information
Provide intelligence to support targeting
Prepare Plans and Orders
Transmit and Receive Information
Process Targets
Mission Impact By CI
Missions
Prepare Plans and Orders
Collect Target Information
Transmit and Receive Infor...
Provide intelligence to support tar...
Process Targets
ICAS Score
Low
Medium
High
Critical
0
4
7
9
10

Hardware Details

Show 10 entries

Search:

| System | Mission(s) | Host / Model Element Name | IP Address(es) | Vendor | Product | Vulnerabilities | ICAS Node | Attack Likelihood | Action |
|---|---|---|---|---|---|---|---|---|---|
| Helios | Provide intelligence to support targeting\|Process Targets\|Transmit and Receive Information\|Collect Target Information\|Prepare Plans and Orders | w7svd00065.corp.ad.headquarters.org | 10.120.9.81 | VMware | | 31 | 4.7 | 12.0% | View Delete |

G2 Ops’ SOFIA architecture shortens the timeline for identification and prioritization of mission critical vulnerabilities.

“The company was founded primarily as an engineering services provider,” Esser said. “But we started creating reusable tools to help our customers with applied digital engineering work and intensive kinds of cyber analytics projects. It was at that point that we started looking at the SBIR program as a way to bring to life some of the capabilities that we were building. I use the term ‘little I’ innovation for what we were doing internally, and turning it into ‘big I’ innovation: formally funded capabilities with a Navy sponsor.”

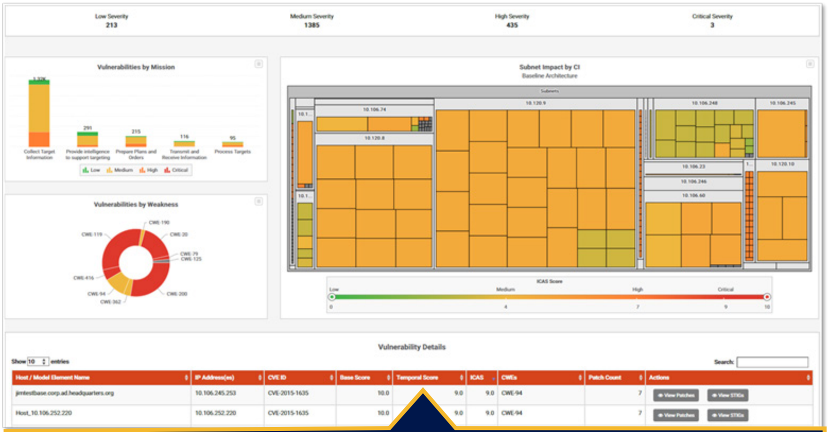
SOFIA was G2 Ops’ first SBIR contract award. “The experience we‘ve had with PEO IWS and the support we received allowed us to be innovative and bring the idea to life. We started to look at other opportunities as well and ended up winning a Phase II Air Force SBIR through a pitch day competition. The Commercial Derivative Aircraft Division, CDAD, was looking for a way to baseline their systems, the airframe, the interactions between them, and do creative cyber analytics to understand the cyber posture of the entire platform. There are so many different systems, each with different attributes and capabilities, and they needed to understand the impact of different threat factors/vectors on the platform as a whole,” Esser said.

“As a part of that Phase II effort for the Air Force, we created the Embedded Cyber Resiliency (ECR) tool suite. This included novel digital engineering modeling as well as new scripting capabilities that make it easier to ingest and output data. Then we came up with different ways to look at cyber vulnerability and a framework to evaluate vulnerability at the platform level. When we completed that Phase II, the Air Force didn’t have an immediate path to Phase III. We got permission to take the technologies to NAVSEA, which had just established a new directorate to manage digital engineering and cybersecurity. They awarded us a Phase III and now we‘re applying the tool suite and methodologies to NAVSEA’s new cloud brokerage and a cybersecurity system they‘re building called SABER.”

Esser continued, “The ECR suite was created with an airframe in mind, but it can be used to evaluate the cyber posture of any system, whether an enterprise network, a cloud environment or even a single component. And because ECR is comprised of digital engineering tools and capabilities, the attack simulation can be an iterative process. As they make design decisions, we can help them understand, ‘Yes, that was a good change, or no, it wasn‘t. You should consider this instead.’”

G2 Ops was founded a decade ago. “The founders all had Navy-related backgrounds and wanted to build a company that was going to be fun to work at. It may sound silly, but among the three founders, we‘d all worked at 20 different organizations and we had an idea what the culture of a dynamic place to work would look like. We wanted to do important work for the Navy, to offer services that other companies were not providing, and to create a workplace people wanted to be a part of, where they could grow and develop their technical expertise. That’s really what G2 Ops is,” Esser explained.

“When we started in 2013, the Navy was embarking on a digital engineering transformation. We saw that organizations across all the SYSCOMs were having a hard time making the transition; they didn‘t understand the benefits, or how to get started. We wanted to help the Navy understand why digital transformation is important, and how it would benefit both the acquisition community and the warfighter—the end user. That‘s been a big part of our success: We have picked up the hard problems and helped find solutions to them.”



Vulnerability Details

| Host / Model Element Name | IP Address(es) | CVE ID | Base Score | Temporal Score | ICAS | CWEs | Patch Count | Actions |
|---|---|---|---|---|---|---|---|---|
| jimtestbase.corp.ad.headquarters.org | 10.106.245.253 | CVE-2015-1635 | 10.0 | 9.0 | 9.0 | CWE-94 | 7 | View Patches View STIGs |
| Host_10.106.252.220 | 10.106.252.220 | CVE-2015-1635 | 10.0 | 9.0 | 9.0 | CWE-94 | 7 | View Patches View STIGs |

G2 Op’s mission-based cybersecurity risk management tool allows threat analysts to identify assets critical to mission essential functions and assets impacted by emerging attack vectors, to prioritize remediation strategies, and to gain new insights about the system.

The company has experienced remarkable growth, reaching 170 employees, and has been recognized as one of the fastest-growing companies in the United States by Inc. 5000 for six consecutive years.

“It‘s a business truism that if you‘re not growing, you‘re dying,” said Esser. “As soon as you win a contract, it‘s expiring. You have one, two, maybe five years, and then you have to either go win it again, or win something else. That being said, growth is not a singular purpose. Growth shows that you‘re expanding; you’re providing more capability. We also think of it as building the foundation underneath the feet of our employees. That growth pace is indicative of how hard we have worked to build a foundation for our employees. Bringing in the absolute best possible people we can, and making them want to stay, is really important. Dr. McCoy is a great example. You need to surround yourself with fantastic people and you need to build an environment where people want to stay. That is a benefit to the Navy, to our customer base. When people want to stay, that institutional knowledge continues to grow and it makes us better. And then we can help make the Navy better.”

Understanding the cyber posture of platforms is crucial, and the company‘s tools and methodologies provide a quantifiable and repeatable process for evaluating and reporting on cyber risk, McCoy explained.

“A lot of Navy technology consists of physical things that are fabricated. They‘re easier to understand because you can touch them. Since evaluating cyber risk is something you can‘t touch, we strive to give the Navy tools for repeatable quantifiable processes that give them confidence in how they are reporting, either up vertically, or laterally. I think that‘s the importance of having solutions like SOFIA and our ECR suite, because without them, you‘re just looking at a lot of data and you can‘t make any sense of it. We‘re trying to make sense of the information in a way that can be understood at every level, so everyone gets the same picture of where the risk lies.”

For more information on G2 Ops, visit the company website at https://g2-ops.com/. For information on Industrial Control System (ICS) Resiliency Information System (IRIS) A Model-Based Cyber Resiliency Suite, G2 Op’s current Phase II project with the Navy, visit the Navy STP VTM at https://vtm.navyfst.com/.