

Cybersecurity: An Information Assurance Challenge

| August 26, 2021



Cybersecurity: An Information Assurance Challenge

COMPANY PROFILE

Synergy Business Innovation & Solutions, Inc. (Synergy) is an Information Technology (IT) firm specializing in Agile Development, System Integration, Cyber Security, Business Process Reengineering, and Mobile Solutions. Synergy's leadership team consists of technical experts who began their careers providing enterprise solutions to large Fortune 500 companies. This commercial IT delivery experience drives Synergy's efficient delivery, ingenuity, and tangible return on investment for our customers.

Synergy leverages its Innovation Lab to build prototype solutions using emerging technologies such as RPA, AI, and ML to address unique business challenges.

With a focus on quality, Synergy has been rated at CMMI Maturity Level 3 for Development, CMMI Maturity Level 3 for Services, and is compliant with ISO 9001:2015, ISO 27001:2013, and ISO 20000-01:2011. Synergy has a DCAA/DCMA Approved Accounting System and has affiliations with the ITIL Foundation and the PMI Institute.

Problem

On a recent contract, our government customer was faced with a three-part information assurance challenge.

- » Their security baseline was either out of date, inaccurate, or altogether missing for many critical business systems.
- » They were faced with an overwhelming amount of technical debt due to years of de-emphasis on action around information assurance findings.
- » Due to lack of funding, the lower environments of the business systems were often missing critical functions found in production, resulting in an unacceptable level of risk in their release management process.

Solution

Team Synergy addressed these problems with a unique mix of proprietary techniques anchored on sound best practices such as the NIST (National Institute of Standards and Technology) Risk Management Framework (RMF), Agile techniques, automation, and the Systems Engineering Lifecycle (SELC).

CAPTURING A COMPLETE BASELINE

To address the out-of-date security baselines, we prioritized business systems, and—following Agile metrics—we separated the business systems into phases. During each phase, we used Kanban methodologies to conduct STIG (Security Technical Implementation Guide) assessments on the business systems, capturing a complete baseline of technical and documentation deficiencies.

Assessments were conducted using a combination of industry-leading and proprietary tools as well as a significant amount of manual analysis.

“Through successful remediation and compliance with Cyber Orders and security assessments, Synergy has reduced the number of outstanding vulnerabilities and open POA&Ms for USCG business systems. They have completed 1,300 POA&Ms for 34 business systems, improving the security posture for USCG Information Systems and reducing the security risk to the DoD Information Network.”

“ Synergy has been highly professional and responsive. They work collaboratively with the stakeholders to design and deliver a value-driven solution.

REMIEDIATING BUSINESS SYSTEM DEBT

The mountain of inherited technical debt was analyzed and prioritized based on risk metrics, criticality of the business system, and feedback from our government partner.

After completing the first STIG assessments, we compared the new findings to the previously known problems with each system. Remediation was conducted on each business system, with all documentation updated and technical changes implemented following SELC procedures. Tools were implemented and leveraged to maximize efficiency and eliminate human error on deployments where feasible.

FUNCTIONAL TESTING


Environment discrepancies were addressed by conducting functional testing on each business system to establish a known baseline of gaps and missing functions. When technical remediations were deemed too high-risk for implementation due to environment inconsistency, a complete technical Level of Effort (LOE) for remediation was delivered to the Government for future planning.

Benefits

- » The processes and policies created during the execution of the solution resulted in a dramatic drop in new findings.
- » Quarterly STIG assessments now build on the existing baseline and POA&Ms (Plan of Action & Milestones) are now being closed within established guidelines.
- » The tools implemented during remediation are now being utilized in the development pipeline for static code analysis and security impact assessments prior to releasing to Production.
- » The government partner is now able to target funding based on real, actionable data around the most critical systems.
- » Addressing the information assurance findings also had a significant impact on OMB (Office of Management and Budget) A-123 findings and ATO (Authority to Operate) schedules. The government partner is now positioned to better respond to new compliance audits, penetration tests, and malicious actors.

Start your own project with Team Synergy!

 www.synergybis.com

 571-375-7723