Streamlining Compliance with NIST SSDF Cybersecurity Tasks

Global Electronics Contractor Leverages Wind River Security Services to Identify SDLC Gaps and Streamline the Path Toward Meeting SSDF Tasks

CUTS COST OF MEETING SSDF MANDATES WHILE ACCELERATING DEVELOPMENT PROJECTS

It's no secret that meeting the cybersecurity standards of the U.S. government and federal entities can be a daunting challenge for companies that develop systems and software. But what is the secret to optimizing the software development lifecycle (SDLC) in order to meet the tasks of the Secure Software Development Framework (SSDF) quickly, reliably, and at a lower cost?

For one Wind River® customer — an international provider of advanced, intelligent electronics systems for defense, homeland security, aviation, medical instrumentation, and more — the solution was **Wind River Security Services**.

Specifically, the company engaged with Wind River for a **Security Assessment** and **SSDF Gap Analysis**. The service provided a rigorous, expert assessment of the company's SDLC, identification of gaps in SSDF-related tasks that could impact self-attestation, and detailed recommendations for remediating those gaps.

These capabilities were extremely important to the customer and are also highly relevant to many other companies because, as directed by OMB Memorandum M-22-18, organizations providing critical software to any U.S. government agency are required to complete and submit the self-attestation common form from the Cybersecurity and Infrastructure Security Agency (CISA) between mid-2022 and early 2023.

Highlights

An international defense electronics company with substantial U.S. business needed to identify, prioritize, and remediate gaps between its SDLC and the tasks of the SSDF so it could reliably meet the cybersecurity requirements of Section 4e of Executive Order 14028, helping the company improve the nation's security and pursue more business opportunities with full confidence.

Challenges

- Enhance the SDLC to meet increasingly stringent government cybersecurity requirements, defined by EO 14028.
- Keep capital expenditure to a minimum as the company builds out the systems necessary to meet requirements.
- Meet compliance requirements reliably without overstaffing or overburdening cybersecurity staff.

As a longtime user of **VxWorks®** and **Wind River Linux**, the company had a history of success with Wind River and deep confidence in Wind River expertise and assessment capabilities.

The key recommendations focused on leveraging a centralized, automated DevSecOps pipeline, including necessary DevSecOps tasks and activities such as:

- Building out a generic base pipeline leveraging infrastructure-as-code and configuration-as-code automation, to allow a centralized team to generate pipelines via automation as needed
- Providing automated security gate capabilities in all pipelines
- Making available and requiring the use of application security testing tools in all pipelines (e.g., SAST, SCA, and DAST where applicable)
- Embedding security requirements into software configuration management

The analysis and recommendations gave the customer the ability to prioritize needed changes to the SDLC, quantify the staffing needs and costs associated with those changes, and implement them in a structured, cost-efficient way going forward.

Furthermore, the features and capabilities of Wind River Studio aligned extremely well with the requirements of implementing the recommendations. For example, the company has the ability to harness Pipeline Manager, workflow automation, digital feedback loop, third-party tool integration, and more to execute on the recommendations.

The net result: The company was able to quickly align its SDLC to address the stringent cybersecurity standards of the U.S. government and meet future self-attestation requirements at a lower cost, within a reduced time frame, with a high degree of reliability and confidence.

Learn more about the Wind River Security Assessment service:

www.windriver.com/resource/professional-services-security-assessment-datasheet

Wind River Solutions

- *Security Services: Security Assessment and SSDF Gap Analysis*
  - Expert analysis of the firm's SDLC
  - Identification of gaps between SDLC and SSDF
  - Remediation guidance on identified gaps
  - Collaboration with DevSecOps team to prioritize and strategize on remediation efforts
- *Future Migration to Wind River Studio Developer*
  - Multiple features and capabilities to facilitate remediations recommended in the SSDF gap analysis
  - Optimized for the customer's existing VxWorks and Wind River Linux platforms

Outcomes

- Identification of existing DevSecOps team capacity and capability to efficiently align to NIST SSDF practices
- Investment allocation insights that are based on tangible, objective data, helping to secure resources for high-return DevSecOps productivity
- Staffing recommendations to obtain the right number of people with the right mix of skills
- Unlocked ability to pursue new business opportunities that require NIST SSDF compliance

WNDRVR

Wind River is a global leader of software for mission-critical intelligent systems. For 40 years, the company has been an innovator and pioneer, powering billions of devices and systems that require the highest levels of security, safety, and reliability. Wind River offers a comprehensive portfolio of software and expertise that are accelerating digital transformation across industries.