DM21-1127

<Canned Intro>

Katie Stewart: Welcome to the SEI Podcast Series. My name is Katie Stewart, and I am the technical manager of the Cyber Assurance Team in the SEI's CERT Division.

Today I am pleased to welcome to our podcast Gavin Jurecko, team lead of Resilience Diagnostics in the SEI's CERT Division. We are here to talk about supply chain risk in the Defense Industrial Base.

Welcome.

Gavin: Responds.

1. **Katie**: Before we delve into that topic, tell us about yourself, your background, and the work that you do here at the SEI. What is the best part of your job?

2. **Katie:** Thank you Gavin. Now, to turn our attention to today's topic. In late September, it was reported that, in an attempt to head off single-point failures in the Defense Supply Chain, the Biden Administration is seeking industry feedback to inform policy development in this area. Let's begin by talking about the Defense Supply Chain and the role the Defense Industrial Base plays in securing our country.

   Gavin:
   - Worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

   - Estimated between 300-500,000 companies
   - Considered critical infrastructure

3. **Katie:** Why is it so important to secure the Defense Industrial Base software supply chain? How many different vendors might have a piece in a given software-enabled product?

   Gavin: Some of the most vulnerable in the supply chain are small and mid-size businesses.

4. **Katie**: Why is that?

Gavin:

- Limited resources, expertise, and often times they have sensitive data that has been pushed to them by default
- Without the resources to protect themselves, they are often the weakest link in the supply chain.

Katie: What are the challenges in securing the software supply chain.

Gavin: There are a set of Key Challenges we are working with DoD to help solve.

5. **Katie**: Let's talk through those. I know the first challenge is the current checklist approach to compliance. It's been known to be applied unevenly by our DIB companies with self-attestation and really doesn't give DoD a good idea of how secure the supply chain really is.

Gavin. That's right. What we are helping DoD develop is a repeatable methodology that allows an independent party to quickly baseline DoD contractors against requirements. By providing this framework, DIB companies can identify gaps before an official assessment occurs, take their results from the assessment, and manage their improvement efforts.

6. **Katie**: Yes. I think moving from a checklist approach to something that is more enduring is critical. We can no longer just ask for a snapshot in time.

   How about tackling inconsistent capabilities? The DIB is a complex ecosystem of organizations of significantly diverse sizes, capabilities, and resources.

   Gavin: Certainly. We see this in all of our assessments. The key is to provide DIB contractors with tools that can meet them where they are. These tools should help focus DIB contractors on the capabilities they should implement. Our measurement frameworks offer DIB contractors a way to measure capabilities, prioritize improvements, and then manage those improvement efforts.

7. **Katie**: Good. Being able to manage improvement efforts to a framework or roadmap is key. This is extremely valuable, I'm sure, to our small and mid-size businesses who maybe don't know where to start.

   Gavin: Yes, exactly.

8. **Katie**: So, what about driving DoD decision making around the security posture of the DIB. I think DoD leaders would

want to have a good picture of the current security posture of the DIB. This seems like a challenge.

Gavin: Yes. What's needed is a more data-driven approach.

9. **Katie**: Can you say a little more about that?

   Gavin: Sure. Our approaches our grounded in the CERT Resilience Management Model, or the CERT RMM, capability maturity model and assessment method for the DIB that is data-driven and underpinned by rigorous measurement. And the linkage between controls and risk reduction has often been difficult to quantify. Our methodologies produce metrics and measures that facilitate data driven, risk decisions. (Whatever else you want to say here.)

10. **Katie**: With that said, we talked about it at the beginning, the DIB supply chain is huge. And assessing the cybersecurity posture of the DIB at this scale must require the automation of analysis.

    Gavin: Absolutely. CERT is developing automated tools to aggregate and visualize DIB cybersecurity posture data allowing for increased scalability.

11. **Katie**: Sounds like you and your team are busy.

Gavin: Haha, yes, we have a lot of challenges that we are trying to solve.

12. **Katie**: So, looking ahead, what is on the horizon?

    Gavin:

- Continue to enable DIB partners to make data-driven decisions around supply chain risk informed by our assessment methodologies.
- Continue to refine and improve our assessment methodologies to keep up with current threats and technologies.
- Develop a data collection strategy to continue to leverage assessment insights.
- Develop robust training program for our assessments to increase assessment reach.
- Continue to add visualizations to support data analysis as the data set expands.
- Develop a Social Media Risk Assessment to augment our capabilities.

13. **Katie**: Sounds like a good path forward.

14. \

Katie: Gavin, thank you for talking with us today about this work. For our audience, we will include links in the transcript to resources mentioned during this podcast. Thanks again for joining us.

<Canned Outro>