DM22-0309

Script: DevSecOps for AI Engineering
SME(s): Hasan Yasar and Jay Palat
Moderator: Jay Palat
Interview Conducted: *04/04/2022 at 2:15 p.m. ET (Remote)*

[PRE-Recorded Intro.]

Jay: Hi and welcome to the SEI Podcast Series. My name is Jay Palat, and I am the Interim Technical Director for AI for Mission in the SEI's Artificial Intelligence Division.

Today I am joined by Hasan Yasar, who is the director of Continuous Deployment of Capability at the SEI. Today we are going to discuss the engineering of AI systems with DevSecOps, what that means, the challenges, and strategies for organizations who want to learn more. Welcome, Hasan.

Hasan: Responds.

1. Hasan, we have both been guests on the podcast series before. Let's tell our guests a little bit about who we are and the work that we do here. Hasan, you can start. What does it mean to be director of Continuous Deployment of Capability?

2. First let's talk about the *why*. Why bring DevSecOps into creating AI systems? What's the benefit?

3. Hasan, you were featured in our 2020 Year in Review for your work with the Department of Defense using DevSecOps to harness the power of artificial intelligence and machine learning. The story noted that you worked with Air Force Missions, which rely on capturing and processing real-time data streams, a task well suited to AI/ML

systems. Is this an early experience of using DevSecOps in an AI Engineering effort? Tell us about it.

4. Let's talk about data. In an SEI paper outlining 11 foundational practices of AI Engineering, the authors noted that the output of an AI system is intrinsically tied to the data used to train the system and how well the training data correlates to the problem and the current world. There are a lot of things that can wrong with the data, ranging from changes in format that can break an ingest function, to malicious injection of data into a training set that causes an incorrect model or a data leak, to data lacking diversity or sufficient examples of classes of interest.

   What role does DevSecOps play in securing these types of data issues?

5. As the SEI advances the discipline of AI Engineering, we're always adding to the body of knowledge around how to build AI as well as AI can be built. With DevSecOps as a leading practice for engineering AI systems, what overarching principles should teams be aware of?

6. What other problems can crop up when engineering an AI system and how can DevSecOps address these issues?

7. One thing we like to emphasize in our podcasts is transition. If I want to incorporate DevSecOps principles into my AI efforts, where do I start? What resources are available?

8. Let's talk about next steps and where we see this area headed.

Jay: Thank you for talking with us today. We will include links in the transcript to resources mentioned during this podcast.

Finally, a reminder to our audience that our podcasts are available on Soundcloud, Stitcher, Apple Podcasts, and Google Podcasts as well as the SEI's YouTube Channel. If you like what you see and hear today, give us a thumbs up.

Thanks again for joining us.

<Canned Outro>