The Cybersecurity Readiness Podcast Series

Episode Title	Reducing the Disconnect Between Security and Development Teams
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.dchatte.com/podcast/ https://the-cybersecurity-readi.captivate.fm/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Harshil Parikh, CEO and Co-Founder Tromzo,
Summary Pitch	How do you make security a first-class citizen of the software development process? According to an industry report, “many information security engineers don’t understand software development—and most software developers don’t understand security. Developers and their managers are focused on delivering features and meeting time-to-market expectations, rather than on making sure that software is secure.” Harshil Parikh, CEO and Co-Founder Tromzo, shares best practices for reducing the disconnect between software development and information security engineers. One such practice is the establishing and automation of security guardrails for application development.
Time Stamps	00:41 -- Talk a little bit about your background, and then we can proceed with the discussion. 02:15 -- According to an industry report, "many information security engineers don't understand software development, and most software developers don't understand security. Developers and their managers are focused on delivering features, and meeting time-to-market

	expectations, rather than on making sure that the software is secure." What are your thoughts and reactions? 04:10 -- Security personnel are incentivized to ensure the product is highly secure. Developers are incentivized to make sure the product has all the functionalities and gets to market on time. So, the incentive systems are often not aligned. That's one of the reasons why there exists a disconnect. What do you feel? 06:36 -- What practices, what structures, are in place to achieve the dual goal of quality software that is also very secure? 08:18 -- Why is it that these teams (software development and information security teams) must be separate? Why can't they be fused and work as one team towards the delivery of a particular product? 12:49 -- Share with the listeners some best practices for reducing the disconnect. What would be certain things that folks could do in their organization within their sphere and scope of influence? 17:14 -- What are some best practices for building and scaling a modern application security program? 24:55 -- How do you empower AppSec teams so they can focus their time on more high-level strategic work? 27:43 -- I'd like to give you the opportunity to put it all together and wrap it up for us. So, what are your final thoughts?
Memorable Harshil Parikh Quotes/Statements	"The unfortunate reality of our current world is that most engineering leadership does not measure developers or does not incentivize developers on building high-quality code that is also secure, to a reasonable extent." " I doubt if most companies are in the business of building the most secure software ever. That's just not the reality of the world. So, how

	do you find that balance of being agile, being fast, but also being able to incorporate security to a reasonable extent that works for the business." "Our world is nowhere close to being automated by bots because it is complex." "If development is continuous, deployment is continuous, then security should also be continuous."