The Cybersecurity Readiness Podcast Series

Episode Title	Implementing Secure and Fast Authentication Processes
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	Slavik Markovich, Co-founder and CEO, Descope
Summary Pitch	Traditional authentication methods are outdated and need many layers of code, which can take time and resources away from developer teams. If developments like FIDO2, WebAuthn, and passkeys are to be cornerstones of a passwordless future, then every application (not just Apple, Google, and Microsoft) needs an easy way to adopt these methods and weave them into current user authentication flows. Slavik Markovich, Co-founder and CEO, Descope, discusses current and future authentication trends and the importance of building a low-code/no-code passwordless authentication solution for app developers.
Time Stamps	02:52 -- Slavic, share with us some background information, some highlights of your professional journey. 04:19 -- What are the pain points when it comes to authentication? 09:58 -- So Slavik, where are we headed in terms of the next stage or the next phase of evolution when it comes to more sophisticated authentication systems?

	16:04 -- What is that low code, no code, passwordless authentication solution that would make it feasible for developers to focus on developing solutions and functionalities? 25:02 -- There are products in the market, open source or proprietary, that can help take away that additional pain or challenge of developing the authentication part of the solution. The developers can then focus on what they are good at, developing the product functionalities. Is that a fair, high-level representation of what you said? 26:20 -- So where are we with biometric authentication? Have we made more progress? 33:56 -- Are we further along in getting to that ideal goal where just compromising an account doesn't mean the end of the world or doesn't mean a major problem? 36:58 -- Please share some final thoughts.
Memorable Slavik Markovich Quotes/Statements	**“**If you have a token that you use to authenticate, that's pretty secure, it's very hard to phish it, and it's very hard to steal it." "A lot of effort is being made in creating authentication around who you are versus what you know. So using biometrics-based authentication is a big step in that direction." "Use of passkeys, which allow a secure and somewhat frictionless way of authenticating, without having to remember anything." [Note: "With passkeys, users can sign in to apps and websites with a biometric sensor (such as a fingerprint or facial recognition), PIN, or pattern, freeing them from having to remember and manage passwords"] (https://developers.google.com/identity/passkeys#) "Like everything in security, the devil is in the details."

	"There is an inherent tension between the security teams and the developers. You kind of try to solve it by bringing security into the development teams." "Security shouldn't become a bolt-on process but should be part of the architecture, design, review, and implementation." "Security doesn't sell your product. Eventually, features will sell your product." "Most developers are not security experts. So, if they implement authentication, there might be big holes that they cannot catch. Then, you end up with account compromises and stolen data from the application." "The biggest obstacle to biometric authentication is actually education." "The best password is no password."