The Cybersecurity Readiness Podcast Series

Episode Title	The State of Attack Surface Management
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	David Monnier, Team Cymru Fellow
Summary Pitch	With increasing digitization and the use of cloud-hosted assets, managing attack surfaces continues to be a major challenge. A recent survey report on the state of attack surface management (ASM) finds security teams drowning in a flood of legacy and ineffective tools with limited discovery capabilities. The need for ASM platforms with advanced digital asset detection capabilities is revealed in the survey findings. David Monnier, Team Cymru Fellow, sheds light on the latest ASM platform capabilities and discusses the implementation challenges and success factors.
Time Stamps	00:50 -- I'd like to take this opportunity to welcome David and have him share with all of us some highlights of his professional journey. 03:14 -- What was the motivation? What led to this very important study that y'all conducted? 07:41 -- David, would you like to add anything to that from a methodology and participant demographic standpoint? 09:52 -- The first finding that I'd like to talk about is "the biggest reason organizations implemented ASM is to increase the visibility of Shadow

	IT in the enterprise." I think this is a very significant finding. If you would expand on this and also describe what Shadow IT means? 14:50 -- Over the years have ASM platform capabilities been enhanced to better monitor cloud-hosted assets? What's been the trend? 19:17 -- Moving along to another interesting finding, which states that "23% of the respondents said that identification of rogue or unclassified assets is the most valuable capability that ASM has provided their organization." I guess my question here is, shouldn't this be obvious? Shouldn't that be what an ASM is supposed to be doing? 20:56 -- What steps should an organization take, should the security analysts, the security professionals take, to ensure that their ASM platform is performing at a satisfactory level? 24:30 -- To what extent is AI being used to enhance the functionality, the capabilities, of these ASM platforms? 27:48 -- So talking about the human component, and in this discussion, we have been talking about attack surfaces, more from a physical standpoint, devices, and so on, so forth. How about humans as attack surfaces, as very vulnerable attack surfaces? Are we doing better in terms of securing this very vulnerable attack surface? Can tools help us secure that attack surface? What are your thoughts? 31:23 -- Is there anything that you'd like to address that you found interesting, or something that surprised you all? 34:22 -- Is there a way of notifying multiple personnel just to make sure that the alerts don't go unheard? 36:43 -- So if you had to make recommendations to potential buyers, or investors of this ASM platform, what does it take to prepare the organization, so they can effectively use such a platform? 40:33 -- I'd like you to share some final thoughts.

David Monnier Memorable Quotes/Statements	"You have to approach the tool sets as, am I going to have a tool that's going to show me things I didn't know to know. And that, in my opinion, is the killer feature, way more important, in my opinion, is discovery, than the vulnerability management component." "If your tool can't tell you that your DNS hosting provider has a poor reputation, or that the IPs around your IP services are bad, if it's not able to show you these kinds of things, then it suggests that you are probably working with an antiquated tool. But frankly, let's use the word static. And if it is static, I think in the information age, that should be a huge red flag to you." "The number one compromised source is still stolen credentials. And the number one method for that is still some type of phishing, or some type of social engineering, so nothing seems to really be changing there." "We still work and live in a world where everything is kind of magic. And the majority of people who are relying on technology, still have absolutely no idea how it works, and therefore can't really spot things when they aren't correct, right." Frankly, there's only so much time in the day. And if you have to pick between defending the mothership or defending a rowboat out in the dock, you know, you're going to defend the mothership, hopefully. So your tool, if it's not aware of that, that's going to be a problem." "There are entities and organizations that carry adequate insurance to pay the fines for non-compliance because they wholly expect to be out of compliance because they consider the compliance component, a burden." "So my number one advice to anybody considering to go down the path of implementation of ASM is, one, be willing to do something that you find, but number two, be willing to actually use it because it's going to make your job easier, it's going to make your life easier."