The Cybersecurity Readiness Podcast Series

Episode Title	Comprehensive Asset Discovery
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	Huxley Barbee, Security Evangelist at runZero and former Cybersecurity Practice Lead at Cisco
Summary Pitch	Comprehensive asset discovery is foundational to robust and proactive cybersecurity governance. The Cybersecurity and Infrastructure Security Agency recently issued a directive (BOD 23-01) requiring federal enterprises (civilian executive branch) to perform automated asset discovery every 7 days. Among other things, the directive also requires federal enterprises to initiate vulnerability enumeration across all discovered assets, including all discovered nomadic/roaming devices (e.g., laptops), every 14 days. Huxley Barbee, Security Evangelist at runZero and former Cybersecurity Practice Lead at Cisco, discusses the various methods of comprehensive asset discovery and provides guidance in selecting an appropriate asset discovery tool.
Time Stamps	01:33 -- Please share with the listeners some highlights of your professional journey. 03:13 -- Share some stories and anecdotes of the consequences of poorly managed asset inventory. 09:37 -- Why didn't organizations engage in comprehensive asset discovery? What were the hurdles, if any? Now that there is a CISA

	directive, what's the guarantee that organizations will be in a position to follow through with the orders? 13:12 -- Let's discuss some solutions, recommendations, and approaches to better managing asset discovery. 22:00 -- It seems that the unauthenticated scan is the best approach. Can you please clarify? 26:16 -- It is equally important for organizations to report on the actions taken in response to the discoveries. Is there a CISA directive to that effect? Can you shed some light on that, please? 33:32 -- Please summarize some of the key takeaways from our chat this morning 35:42 -- How about providing listeners with some selection criteria when they're evaluating different products in the market, asset discovery products? What should they be aware of? What are the kinds of questions they should be asking? So it helps them make good selections.
Memorable Huxley Barbee Quotes/Statements	"The unfortunate reality is that asset inventory is still an unsolved problem for so many organizations. They might have some tooling for dealing with asset discovery, but usually, they end up with spreadsheets." "There is greater recognition, especially from government agencies, of the need for asset discovery." "Asset Inventory isn't just a list of devices that you have on your network. It's also what is on those devices, what services are on those devices, what ports are those devices listening to, and who owns those devices." "There are many hurdles associated with asset inventory management. The one that looms the largest is unmanaged devices, unmanaged assets, that is the achilles heel of any asset inventory program."

	"Why would the adversary go for a well-managed up to date patched machine when they can just go ahead and attack something that's out of date and unpatched, with numerous exploits that they might be able to download from the Internet." "Unmanaged devices are why customers end up using spreadsheets where the existing tooling just isn't performing as they want. And so they have to end up using spreadsheets instead." "With unauthenticated scanning, you have the best of many worlds, right, you have the ability to go out and find all the assets on the network, even if they're unmanaged. But you don't have the problems of credential spraying. And depending on how the unauthenticated scanner is implemented, you can even talk to OT devices without the fear of crashing, some sort of mission-critical function. "Effectively, BOD 2301 is suggesting the use of unauthenticated scans for the asset discovery portion of this particular directive." "A customer told me that having a comprehensive asset discovery allowed his organization to move from a reactive security program to a proactive security program." "Oftentimes, the adversary knows more about your network than you do. And, of course, to combat that, you need a comprehensive asset inventory." "Oftentimes, asset inventory is not called out as a specific line item in security budgets."