The Cybersecurity Readiness Podcast Series

Episode Title	Best Practices for Overcoming Troublesome Vulnerability Management Trends
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	Ashley Leonard, CEO at Syxsense
Summary Pitch	A 2023 State of Vulnerability Management Report finds that only half of the surveyed organizations (51%) have, at best, a moderate level of visibility into vulnerabilities. Several other vulnerability management metrics, such as maturity levels, frequency of vulnerability scans, and patch deployment speed, reveal an alarming and troublesome trend. In this episode, Ashley Leonard, CEO at Syxsense, joins me in reviewing the research report findings and discussing vulnerability management challenges and best practices.
Time Stamps	00:02 -- Introduction 02:20 -- Ashley Leonard's Professional Highlights 04:00 -- Scope of Vulnerability Management 06:34 -- Human Vulnerability Factor 08:57 -- AI-enabled Phishing Attacks 09:32 -- Vulnerability Management Objectives

	15:50 -- Continuous Vulnerability Scanning and Remediation 18:24 -- Practicality of Continuous Vulnerability Scanning 22:37 -- Securing All Attack Surfaces, Especially IoT Devices and Cloud Assets 25:57 -- Vulnerability Management Maturity Levels 31:33 -- Apparent Disconnect Between Scanning and Visibility 36:15 -- Promptly Acting On Vulnerability Report Findings 41:49 -- Selecting Appropriate Vulnerability Management Tools and Solutions 43:55 -- Vulnerability Management Best Practices 46:30 -- Final Thoughts
Memorable Ashley Leonard Quotes/Statements	▪ *"We try and train most of our users not to log in an unknown USB device. But there have been cases where threat actors will take the USB devices and drop them in the parking lot of companies they're trying to breach. People will often pick up these USB sticks, wonder what's on it, walk into the office, and plug it in. It's shocking."* ▪ *"I would share that patching should not be a monthly process. Many companies do this kind of, "Oh, it's Patch Tuesday, so we're gonna go and deploy our patch Tuesday patches to our organization." It's not even a weekly process, this should be a continuous process."* ▪ *"New vulnerabilities are being published constantly, we have a whole threat research team that is constantly publishing new content. And if you're not scanning on a continuous basis, then your organization's exposed. So you really need to find technologies and*

	partners that can do this kind of continuous vulnerability management for you." ▪ *"In the past, after a vulnerability was publicly announced, it typically took three to seven days before you started to see attackers actually weaponizing these vulnerabilities and attacking, which meant you kind of had a week or so to get your act together, deploy the patches and make sure your organization was safe. It's now down to 24 hours. And that's a problem. That's a huge problem for most organizations, because, unless you are doing continuous vulnerability scanning and remediation, you're not going to be able to respond quickly enough, and your organization is going to be exposed. So you really need technology to step in here. And you need automation that you can use to deploy these patches to your most vulnerable assets as quickly as possible."* ▪ *"Patches don't get tested normally as much as a full release of a product; that's also a risk."* ▪ *"Automation can really help you respond quickly but also thoughtfully in the way that you go about remediating these patches."* ▪ *"Think carefully about the data, categorize how important it is, and think about where it's stored. And that's a really good starting place."* ▪ *"Threat actors are now using AI to analyze the exfiltrated data from the organization. And then using that data from the AI, for example, finding customer lists, and then contacting those customers, and getting those customers to apply pressure on the organization to pay the ransom."*

	▪ *"Research finds that the more tools you have, the more likely you are to have a breach."* ▪ *"The fewer agents that you actually have on your endpoints, in many cases, the safer you are."* ▪ *"You can't just mass deploy a patch, because the patch itself causes more problems than the vulnerability it's closing. So, it needs to be done very thoughtfully, using automation and processes."*