The Cybersecurity Readiness Podcast Series

Episode Title	From Reactive to Proactive: How behavioral psychology is transforming enterprise security
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Lynsey Wolf, Team Lead and Insider Threat Analyst at DTEX Systems
Summary Pitch	IBM recently reported a 71% year-over-year increase in attacks using valid credentials. This continued use of stolen credentials is also evident through ongoing public incidents like the string of attacks targeting Snowflake's customers that resulted in breaches at AT&T and Advanced Auto Parts. Lynsey Wolf, Team Lead and Insider Threat Analyst at DTEX Systems believes that users' psychological and behavioral traits are being overlooked when it comes to defending against credential misuse. In this episode, we discuss how best to mitigate such threats using a proactive approach to insider risk management by focusing on user behavior and indicators rather than just incident response. **Action Items and Discussion Highlights** • Establish specific use cases and indicators for identifying potential insider threat incidents. • Monitor for suspicious activities like outside of scheduled hours logins and unusual login locations. • Take a proactive approach to insider risk management, focusing on user behavior and indicators rather than just incident response. • Consider incorporating the expertise of behavioral psychologists and researchers into the organization's insider threat program.

Time Stamps	00:02 -- Introduction 02:16 -- Guest's professional highlights 05:41 -- Based on everything you have learned about human behavior over the years, is there anything that got your attention and surprised you? 10:12 -- What does "insider threat" mean, and what does it encompass? 12:54 -- Why do organizations tend to ignore behavioral factors? Is this something that you have noticed, or did I misinterpret? 16:10 -- Please shed light on insider threat monitoring and detection through an incident you dealt with. 19:07 -- When you said escalating their privileges, how is it possible if the controls are in place to not allow that to happen? 24:26 -- To discourage specific behavior, you must disable it technologically. 27:38 -- Taking a holistic approach to mitigating insider threat. 30:23 -- How do you define a holistic approach to mitigating insider risks? What do you recommend companies do? 32:42 -- Creating a culture of empathy. 34:59 -- How proactive is the organization? How proactively is the organization trying to create that high-performance Information security culture? 39:08 -- Finding that balance between using technology and humans to prevent insider attacks. 41:36 -- Best practices for respecting privacy without compromising the risks associated with insider threats.

	44:40 -- Building emotional capital 47:20 -- What are your thoughts on organizations employing psychologists and seeking their expertise when developing different solutions and processes to mitigate insider threats? How common is that? 50:02 -- Key Takeaways
Memorable Lynsey Wolf Quotes/Statements	"If a human is determined to do something, they're going to do it." "Convenience is a huge motivator. If it's more convenient for me to do it this way, even though it's not allowed, I might do it." "I'll classify insider threats into three main categories -- malicious, non-malicious, and negligent." "One of the biggest challenges we see now is that we're educating super sophisticated users. Higher degree programs are built to teach you how to become a cybersecurity expert. Many people are using that knowledge to circumvent the controls we put in place. So, in reality, it's a great opportunity, but we're also, again, educating these sophisticated users that can circumvent these controls." "One of the biggest things we come across is the insecure usage of credentials or insecure storage of credentials. We often see people storing their credentials on a spreadsheet or accessing a document on a corporate share where they have all their plain text credentials just sitting there. This is not credential misuse, but it's a precursor to a larger concern, where you're giving various individuals access to your credentials. So at the end of the day, it's not credential misuse, but then you're allowing that misuse to occur." "Not everyone is going to remember the do's and don'ts of the organization. I mean, it's just not possible to understand every security

	control that will be in place. However, ensuring users understand why different controls are in place is important. It does not necessarily prohibit them but explains to users that they're not just there to make their lives harder. They're not there to make your work difficult. There are reasons why these controls are in place, and getting that understanding from your workforce is more important than reprimanding those users." "I believe culture and awareness are two aspects that are often overlooked. I think it's important to create an environment where trust and respect are emphasized, and this, again, is accomplished by educating your workforce and providing regular training and awareness programs for your employees." "Having access to some sort of continuous trail telemetry data from machines, applications, and people gives you the insight and ability to surface dynamic indicators of intent." "I think the most successful people in the insider risk space are those behavioral psychologists because when you come from that mindset, you truly understand what it means to be human." "Machines, applications, and people give you the insight and ability to surface dynamic indicators of intent. Then, we combine all that information to deliver what we discussed earlier: a holistic and contextual awareness of our workforce activities." "We're not collecting all of your keystrokes. We're not even collecting the content of your files. Because, in reality, I don't need that. I don't need to know what's in your file to potentially understand that maybe you shouldn't have access to it; it's more about understanding the high-level behaviors and metadata."