The Cybersecurity Readiness Podcast Series

Episode Title	Actionable Threat Intelligence and the Dark Web
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	Victoria Kivilevich, Director of Threat Research at KELA Group
Summary Pitch	In a recent news release, Reuters reported that "United States has offered a $15 million reward for information on Conti ransomware group. The FBI estimates that more than 1,000 victims of the Conti group have paid a total in excess of $150 million in ransomware payments." Victoria Kivilevich, Director of Threat Research at KELA Group, describes the cybercrime ecosystem and provides guidance on how to gain and leverage actionable intelligence from dark and deep web resources.
Time Stamps	00:41 -- Let's begin by providing listeners an overview of the Dark Web. So Victoria, what is the Dark Web? 04:09 -- What are some good practices for organizations to leverage intelligence from Dark Web type resources to proactively prevent potential attacks? What are your thoughts? What are your recommendations? 07:02 -- Let's say, I am representing the security team of my organization. Obviously, I would not want my organization to be a top

	target. But I would like to know if it is. Shed some light on what makes for a top target? 11:13 -- From an organization's standpoint, how is the relationship between the Initial Access Brokers and say the ransomware attackers significant? 13:27 -- What is the profile of an ideal ransomware target? Is it different from the top targets of Initial Access Brokers? 17:29 -- What advice do you have for organizations from the standpoint of avoiding becoming double victims? 22:54 -- Now, let me present you with a scenario. An attacker approaches an organization and says that they have the organization's data. Obviously, they're asking for money. How should the organization evaluate the genuineness of the threat? 26:53 -- It almost seems that an organization needs to have a team that solely focuses on monitoring the cybercrime ecosystem. What are your thoughts and advice? 30:42 -- What are your final thoughts?
Memorable Victoria Kivilevich Quotes/Statements	"I believe one of the important steps is to evaluate the genuineness of the information that you see on the Dark Web and other cybercrime sources, connect the dots, and also have in place an established process of passing on the intelligence to people who make decisions." "An ideal ransomware victim is based in the US, has more than $60 million in revenue, and most likely is not from education, government, or the nonprofit sector, because it's just not valuable for the ransomware attackers." "From the moment the access credentials are listed for sale, it takes on average one month to attack the company, try and have negotiations,

	and then publish the company name on the ransomware blog if the negotiations fail." "So unluckily for us, the cybercrime ecosystem will unlikely disappear. But luckily for us, we can have almost the same visibility into the attack surfaces as potential attackers."