The Cybersecurity Readiness Podcast Series

Episode Title	Skilling Up for Security Operations Center Roles
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	James Risler, Senior Manager, Cisco Learning and Certifications
Summary Pitch	The Security Operations Center (SOC) is at the heart of an organization's cyber defense system. Highly skilled and motivated personnel must work in these centers. James Risler, Senior Manager, Cisco Learning and Certifications, discussed the roles of the security engineer and the security analyst and the hard and soft skills needed to be effective in those functions. While the ability to code, learn computer forensics techniques, and know how to operationalize MITRE attacks are top skills, the ability to communicate effectively is equally important. Jim strongly recommends that academic institutions partner up with industry to provide hands-on training opportunities and also engage in security solutions-focused research.
Time Stamps	01:24 -- Please share with listeners some highlights of your professional journey. 03:27 -- So Jim, for the benefit of our listeners, many of whom may not have a good insight on SOC (Security Operations Center), let's give

	them a bit of an overview of SOC. Why don't you start, and if I want to plug anything in, I will. 05:09 -- Jim, when we were having our planning meeting, we kind of agreed that we wanted to focus this discussion on the skill sets that need to be in place for effective SOC operations. So why don't you talk a little bit about that? 09:21 -- I'd like your thoughts on how threat intelligence should be managed and governed, from logging it to acting on it. What are some best practices out there? 12:29 -- People who are strong technically often are not the greatest communicator, and vice versa. What are your thoughts? 15:33 -- How should someone decide whether they would like to follow the track of an engineer or the track of an analyst? 19:24 -- Let me share another interesting finding from the Voice of the SOC Analyst report. The top three skills needed to succeed as an analyst came out to be: 1) learning to code, 2) learning computer forensics techniques, and 3) knowing how to operationalize MITRE attacks Jim, your reactions and thoughts, you'd like to add to that? 24:01 -- What advice do you have for the directors of these cyber security programs, whether they are housed in the business school or the engineering school? 30:44 -- So I'd like to give you the remaining time to sum it up for us, maybe share some key messages, and some final thoughts with the listeners. 35:27 -- Jim, I said you would have the last word; you still get to have the last word. And after that, we'll pack it up.

Memorable James Risler Quotes/Statements	The people that work in SOC, I call them the gatekeepers of this castle that the security engineers have built. They got to protect the castle against threats, both internal and external. Some companies just want a SOC to check off the box. Oh, we have a SOC; ensure we follow HIPAA compliance and all other compliance requirements. And then there's some SOC out there that literally go on the offensive following leading threat hunters out there, finding the latest threats, and then taking those threats and going back and seeing if they've been successful in their organization or not. If you look back at one of the most successful attacks that impacted many people with their credit cards, that retail organization was getting alerts about the intrusion on their network, but somebody went in to investigate it and said it was a false positive. You have to get down and find out what to your organization is a false positive and what's not a false positive, but what's a true positive indicator, and what's critical to communicate. Playbooks inside SOCs are critical because they tell you the quality assurance of your process. My number one recommendation is to partner with corporate America, find companies that want to give back, that want to partner with you, that want to create a communication pipeline and work with them to understand and see the problem you've got. The future of IoT security is a risk to all of us. Using the escape room analogy, one person coming into that room may have a philosophy background or may have been an accountant or a lawyer coming in and looking at the problem very differently,

	which might be the key to solving that puzzle that gets you out of that escape room.