Interview with Kate Rhodes - CISO for ODU Security
Interviewed by: Aiden West
Feb. 13 2026
CYSE 368 - Teresa Duvall - Vincent Mitchel

Kate Rhodes was an interesting person to interview because she has a high valued position as the CISO for ODU. Kate started her career in the army as a nodal network systems operator. She joined the army because she wanted to have a job where it felt like she had purpose in her work. In her job, she deployed networks and switches and got most of her background in networking. This first role is what led Kate into realizing that she was interested in cybersecurity. She was able to advance in her career due to taking opportunity where she saw it and not being afraid to try new things. Her first job out of the army was a linux administrator. She did not enjoy the role as much, and ended up moving onward to being an information assurance engineer for the Navy, then NASA. After that, she took a role at ODU working with the GRC team. In her free time, she would volunteer as a SecOps analyst for the on-call rotations. While volunteering, she got the chance to work with the current CISO at the time. When the CISO left, she stepped in as the interim CISO and eventually was hired to be the permanent CISO.

While advancing through her career, Kate noted that she was thankful that she had always had someone with her to encourage her. There was not one specific person that pushed her to where she was, but multiple people found their way to her to encourage and support her. She always had the willingness to try new things and was aggressive to learn everything she could. It was interesting to hear that she got her Bachelors degree in a non-technical role. When she left the army, all she had for certifications was her Security+. A lot of students now try to build their foundation on certifications, but experience and asking questions to learn are the most important when trying to land a job role. If she could have gone back in time, Kate would have pursued a degree in cybersecurity to set her foundation in the field in stone. Even now, Kate wants to get her masters degree in cybersecurity, but as a CISO, she does not have nearly enough time. She also would have gotten her CISSP certification with her Security+.

Knowledge is key in the cybersecurity industry. The roles and responsibilities of cyber positions are always demanding more of people and as the CISO, Kate recognizes that. One important area of knowledge that Kate noted was to understand all the facets of cybersecurity. There are so many teams that Kate has to work with to secure ODU. Every team has to keep in mind security when they are working. It is Kate's job to make sure everyone stays that way and also that she stays caught up in the mindset. Some ways that Kate stays personally updated on new threats, technology, and best practices include newsletters, blogs, threat feeds, and following multiple communities. Some specific examples of tools that she uses include HackerNews, Krebs, and SANS. Kate also works with technical tools such as phishing alert software, ticketing software, and her GRC analysis tool. The most important tools she uses are Teams and Outlook, because communication is so important in this field.

I asked Kate a few questions about what her day to day activities look like as the CISO of ODU. One interesting fact I found out was that Kate never really had much coding and scripting experience. She stated that she had some knowledge in PowerShell in her past, but never really got into the scripting and coding side of cybersecurity. Her background in networks

really started her career. Since she also did not have a foundation with a degree in cybersecurity, it makes sense as to why she never learned those kinds of skills. Kate works with all kinds of teams at ODU. She meets with her security architect the most to talk strategy about gaps in security and how they can improve their defense. Minimizing the scope of attacks is essential. Kate also stated that she talked with Luke Watson, Deputy CISO, and Matt Thomas, a security architect, the most. When an important security incident occurs, the most important thing to do is collect as much info as you can and understand what is going on. It is always important to understand the scope of the situation before responding so that there is nothing to overreact to. Overreacting to a scenario could potentially cause more problems.

Some of the biggest challenges a cybersecurity team can face are keeping up with new threats and expectations, while also performing day to day activities. It is important to know how to navigate what the buzzword is at the time. For example, the buzzword now is AI, whether it is AI security or AI governance. Teams have to be able to expand as new technology comes out and respond to everything that comes in the news. For Kate's role as CISO specifically, she has to be a business leader during all of this. The auditing and documentation process during all of these challenges is of the utmost importance. This role gives Kate the purposeful job she was searching for in the army. She gets the opportunity to defend people and data, and her work is very meaningful to her.

Last, I asked Kate if she had any advice for newcomers in the field. Some advice she gave was that nobody will love you like yourself, do not be afraid to negotiate roles, and you do not have to be the smartest person in the room. Kate stated that she did not realize her worth going into the cyber industry, and that she just wanted a job. Realizing your worth is extremely important and it is good to let employers know that you know you are worth something. Overall, speaking with Kate made me excited for my future career. I got lots of valuable advice, and it is always fun to learn about how people made their way into their current cyber role. The end.