Interview with Edmond C. Cook, Security Engineer for University Information Security Office, Dec 5, 2025, Interviewed by: Nehemia Araia

I chose to interview Edmond, a Security Engineer at Old Dominion University, because his career path mirrors the direction I want to move in. As a Student SOC Analyst, I see security work from one angle, but I wanted to understand how someone grows into the engineering side and what the day-to-day looks like. People in the student SOC talk about how knowledgeable and helpful he is, so I knew he would give me some great insight. His experience helped me understand not only what his role looks like but also what mindset and skill set I should be developing as I start my own career.

For the first question, I asked him to explain his career path and how he transitioned from earlier roles into becoming a Security Engineer. He told me that after graduating in 2016 with a bachelor's degree in Information Technology, he did not immediately land an IT job. His first job was at a payroll call center where he handled customer service and helped with technical issues. He explained that even though it was not a traditional IT position, it helped him develop communication skills and patience with people who may not understand technical concepts. Later on he applied to Old Dominion University and interviewed multiple times before being hired as a Desktop Support Technician. He worked in that role for three to four years and said it gave him a strong understanding of the systems across campus. He told me Vince eventually encouraged him to apply for the Security Engineer position. He interviewed with the previous CISO and received the job. His path from Desktop Support to Analyst to Engineer showed me that growing into security engineering is more about building a solid foundation and taking opportunities when they appear.

I also asked him what a typical day looks like for a Security Engineer. He explained that most of his day involves working on projects and helping the university stay aligned with security requirements. He uses the Monday platform to track tasks and organize ongoing work. Part of his role involves managing the vulnerability service and helping different departments learn how to use Nexpose for scanning. He spends time creating documentation so people have clear steps to follow. He also attends three scheduled meetings every two weeks to report what the team has accomplished and what challenges still remain. Along with project work, he supports operational tools. He is the secondary administrator for CrowdStrike and a tertiary researcher for Everfox case management. Those responsibilities involve investigating alerts, researching activity, and making sure the environment stays secure.

I then asked him how his role as a Security Engineer has changed over time with the development of AI and the cloud. He told me that the biggest change has been the amount of training and skills that cloud work demands. He told me that they are pushing everyone to learn more about AWS and other CSPs like Azure and GCP. They are also working toward integrating all three cloud service providers into the security environment. Cloud automation has become

more important and tools like Amazon Lambda now replace tasks that used to be manual. When it came to AI, he said it makes certain tasks much faster. AI helps him work through small roadblocks and speeds up the research process. He mentioned that AI does not replace the need for technical knowledge but it removes friction and gives him more time to focus on harder problems.

I asked him what technical skills or tools he believes are essential for someone entering security engineering in the future. He said that learning the specific tools used by the companies you want to work for is extremely helpful. Whether a company uses AWS, Azure, CrowdStrike, Palo Alto, or other platforms, being familiar with those tools can give you leverage. He stressed the importance of automation and said that PowerShell, Python, and Git are three skills that every future engineer should learn. He also recommended spending time practicing on HackTheBox and LeetCode for hands-on experience.

I asked him about the biggest incident or security challenge he has handled and what it taught him. He explained that one of the hardest tasks he worked on was rebuilding the entire vulnerability management system for the university. He had to rebuild Nexpose and reconstruct one of the servers from the ground up. During this process he also had to lead meetings and coordinate with several different teams. He said the experience taught him a lot about leadership and communication. It also showed him how large and connected the university environment is. He said that challenge gave him a clearer sense of where he wanted to grow technically and professionally.

I also asked him what separates a good security engineer from a great one. He said that a good engineer knows how to use tools, but a great engineer understands them deeply and can think ahead. He emphasized communication and said that great engineers know how to explain things clearly and create an environment where people feel supported. They know when to take calculated risks and how to help guide team members. He also said that attention to detail is one of the most important traits an engineer can have because small mistakes can lead to major issues.

Next, I asked him what entry level roles build the strongest foundation for becoming a security engineer. He said that SOC Analyst, Help Desk, and Desktop Support roles all provide strong starts. Help Desk teaches communication and how to support users. SOC work introduces you to real incident response and threat analysis. Once someone gets into a technical entry level role, they can start taking on projects and move around the organization. He said this is exactly how he built his foundation before becoming a Security Engineer.

For the last question, I asked him what long term career advice he would give someone entering the field. He said that the most important thing is to keep growing your skill set and not let the pace of the field overwhelm you. He explained that companies pay high salaries because expectations are high, and staying stagnant can hold you back. He also stressed the importance of

building a strong network. He said that the people around you can open doors you did not expect and can push you forward when opportunities come up. His main point was to stay consistent, keep learning, and surround yourself with people who want to see you grow.