Interview with Edward E. Scott

Sr. Cloud Security Engineer for Old Dominion University Information Security Office

Date: February 18, 2026

Interviewed by: Nehemia Araia

Student SOC Internship

Spring 2026

Professor Teresa Duvall, Mr Luke Watson

For this semester's staff interview, I chose to speak with Edward, the Sr. Cloud Security Engineer here at Old Dominion University, because his career path and role closely align with where I hope to grow professionally. As a Student SOC Analyst, I spend most of my time looking at alerts, investigating phishing emails, and learning how security operations function in a real environment. However, I wanted to understand what comes after that stage and how someone progresses into the engineering and cloud side of security. Edward's experience working across multiple technical roles before fully focusing on cloud security made him someone I could learn a lot from. Another reason I wanted to interview Edward is because cloud security is continuing to grow fast, and it is an area I'm really interested in exploring further. Hearing directly from someone who has transitioned through roles from system administration to now cloud security provided insight into what skills actually matter over time, not just what is listed in job descriptions. His perspective helped me better understand both the technical expectations and the mindset needed to succeed long term in this field.

One of the first questions I asked Edward was about his career journey and how he transitioned into becoming a Cloud Security Engineer. He explained that his path was not a

single jump into cloud security but rather a progression through several foundational roles. He started as a systems administrator, which helped him understand how systems are built and maintained. From there, he moved into a network engineering role, where he developed deeper knowledge of infrastructure and how environments communicate. After building those foundations, he transitioned into a Cloud Engineering position. That role introduced him to cloud platforms and infrastructure. He then said he later advanced into a Cloud Architecture role, followed by a combined Cloud and Security Architect position. Eventually, his responsibilities evolved into his current role as a Cloud Security Engineer at ODU. What stood out to me the most was how each role built on the previous one. It reinforced the idea that strong fundamentals in systems and networking are extremely valuable before specializing.

I also asked him what a typical day looks like in his role. He explained his day to day is typically not the same, but most of his work focuses on hardening cloud systems, reviewing logs, and preparing infrastructure. From what he told me, hardening mainly consists of ensuring systems are configured securely, reducing attack surfaces, and applying best practices across environments. Log review is another important part of his responsibilities because monitoring activity helps detect potential threats or misconfigurations early. Preparing infrastructure includes planning and implementing changes that support both security and operational needs. Hearing this helped me understand that cloud security is not only about responding to threats but also about building environments correctly from the beginning.

I asked Edward how his role has changed over time with the development of AI and cloud. Interestingly, he explained that cloud itself has not really changed his responsibilities, since cloud security has always required strong foundational skills. However, he did mention that AI is contributing to an increase in the rate of simpler attacks and automated hacking attempts,

including more agentic threats. This perspective was helpful because it highlighted that while technology evolves, the core principles of security remain consistent. AI may accelerate certain activities, but strong security fundamentals still matter the most.

When discussing technical skills, Edward emphasized the importance of understanding security fundamentals, networking, and cloud platforms such as AWS and Azure specifically, with some familiarity in GCP as well. He also stressed the importance of infrastructure as code and understanding the DevOps lifecycle. He mentioned that knowing formats like JSON and YAML is also important because cloud environments rely heavily on configuration files. His recommendations made it clear that cloud security engineering is not just about learning one tool but understanding how systems integrate and operate together.

I then asked him about the biggest incident or security challenge he had handled. He described an outage related to remote management systems, which highlighted the importance of having strong disaster recovery planning in place. He explained that situations like this reinforce the need to be proactive instead of reactive. This answer stood out to me because it connected directly to his repeated emphasis on proactive thinking. Rather than only responding to problems after they occur, strong engineers anticipate risks and prepare for failures before they happen. That mindset is something I realized I need to continue developing as I grow in my career.

One of the most interesting parts of the interview was when I asked what distinguishes a good Cloud Security Engineer from a great one. He explained that many people in security are naturally reactive because the field involves responding to threats and incidents. However, what separates stronger professionals is being proactive. He described proactive behavior as identifying weaknesses and fixing problems before they break. This perspective helped me realize that technical skill alone is not enough.

When I asked about entry-level roles that build the strongest foundation for becoming a Cloud Security Engineer, Edward explained that his own early roles in systems administration and networking were extremely beneficial. Those experiences provided the building blocks that allowed him to transition into cloud and security later. He also mentioned that what we're currently doing in the SOC is a strong starting point. He suggested that beginning as a junior analyst after graduation would be a great next step while continuing to build cloud experience through projects or internships if possible. Hearing this was encouraging because it confirmed that the experience I am gaining now is directly relevant to future opportunities.

For the final question, I asked him what long-term career advice he would give someone entering the field after graduation. His main advice was simple but repeated multiple times, which is to be proactive. He explained that the technology landscape will always change, including developments related to large language models and data centers, so people need to stay adaptable. He also emphasized the importance of communication and working well with others. Technical knowledge alone is not enough to succeed long term. Being able to collaborate effectively and explain ideas clearly can open opportunities and help advance a career.

## Conclusion

Overall, interviewing Edward provided valuable insight into the responsibilities and career progression associated with cloud security engineering. His emphasis on proactive thinking and strong technical foundations skills helped me better understand what it takes to succeed in this field. The interview also reinforced how rapidly evolving technologies like AI and cloud continue to change cybersecurity careers.