Passion For Learning

Matt Thomas

Security Architect

2/17/2026

Jonathan Morales

CYSE 368

Spring 2026

Teresa Duval

Introduction:

Rolling into the second semester of this year at the student SOC (security operations center) internship we have been tasked with interviewing a staff member. For this interview I choose to question and learn more about Matt Thomas, who is currently the security architect here at Old Dominion University. I had chosen Matt due to him being in a slightly different department but still having close ties with the SOC, allowing me to get not only the perspectives of individuals in the SOC but also externally. However, learning about Matt's journey I found he was on the same SOC team after being approached by Kate and eventually the department expanded to the position, he's in now.

Journey:

Going down memory lane, Matt's IT journey began in high school. Matt attended a vocational school based on computer repair along the lines of the CompTIA A+ which he got a 15 or 16. As well while still in this same program in high school when he was a senior he got his Linux +. After graduating from high school Matt attended Radford for undergraduate software engineering and database management as well as obtaining an undergraduate information security certificate. While at Radford he had built an app that let students keep track of when their finals were and notified them. He also attended an internship at Radford for web development. Nearing the end of his time at Radford as a student six months before graduation he took a full-time position at the university to fill the spot of someone who quit. This position was in devops engineering and infrastructure building. Around this time, he also worked with a company called Black Hills information security. While in this position after five years he became the security engineer and then a few months later Matt also became the backup ISO. During his time in this position, he focused a lot on infrastructure and how to automate it.

Eventually through hard work and determination Matt became the CISO but realized it stepped away from the work he was passionate about. Through his work at Radford Matt had the opportunity to brush shoulders with many people through things like VASCAN, one of these places being Old Dominion University. The first attempt to get Matt to ODU by Mark had failed but later Kate had reached out to Matt, and they had settled on him becoming the security architect here at Old Dominion University allowing him to be more in tune with the side of IT he desired. During his career he has also picked up certs in SANS and GCIH.

Responsibilities:

Matt's current responsibilities as a security architect at Old Dominion University are almost like a multipurpose role. This is since he must do both groundwork and manage projects. An interesting analytic he had was that per week he spends about 26 hours in meetings while also maintaining his day-to-day tasks. Matt also is involved with most projects providing security guidance. His job also entails identifying risk, effective strategic planning to meet security goals, and cloud strategy.

Advice:

During the interview I asked Matt several different questions on what would be good practices, skills, techniques, or general advice to an up and coming IT professional. Matt suggested that someone in the security architect field should have a mindset of innovation and development as well as being able to see both the technical side of things and the business side. With one of the biggest qualities being communication. Especially when it comes to trying to find the most important problems to work on, being able to communicate with your team and others is invaluable and allows for one to have better prioritization. When asking for his opinion

on soft skills that are essential for his job he responded with finding what your organization deems as security and convincing people why cybersecurity is important and why in non-technical terms. Furthermore, I had asked Matt what technical skills would be important for his job, and he suggested coding/scripting language but in a sense said all IT information is valuable. The more exposure you can get to it the better, this is because being able to understand how something works allows you to better understand risks and weaknesses and give you a better idea of how attackers are breaking in.

When asked what he would recommend as an entry job, Matt recommended help desk and security analyst. Essentially any role that can get your foot in the door and working in the IT field. However, the most important thing he said was experience. Experience being so important that when he looks to hire someone, he specifically notes their real-world experience. Tied with their passion and drive in security as well as being technically minded and malleable. Another key aspect of someone who would excel is having the ability to prioritize. Matt explained how many of the challenges he faces relate to having too many problems with too little time. Making it more important to prioritize which problems pose the biggest risk to security. Additionally, I had asked Matt if he had participated in any organizations to help further his career and he mentioned Black Hills Information Security which is a pen testing company and the honors society for computer science. But mainly expressed the importance of finding an organization that allows for collaboration and the exchanging of information.

Lastly, I had asked Matt, “If you could leave a lasting message to an entry level IT/Cyber person, what would it be”? Matt said, “You must have fun, it is a stressful field that can be challenging, tons of work, and requires the constant need to stay up to date with technology. But

you must find joy in it to prevent yourself from burning out. Making fun of it goes further than anything especially when your able to keep joy in tech, people, and learning".