Reflection Paper 2: Interview with Matt Thomas, ISA, ODU ITS

Matt Thomas is the Information Security Architect for Old Dominion Unviersity's (ODU) Internet Technology Services (ITS) department. A graduate of Radford University, Thomas joined ODU in June of 2021.

His background in IT extends as far back as high school, where he operated his school's computer repair shop. During this time, he acquired his Linux+ and A+ certifications, and took two years of programming classes. Encouraged by some of his teachers, he matriculated to Radford University as a Computer Science major, concentrating in Software Engineering and Database Management, as well as attaining an undergraduate Information Security certificate.

While attending Radford University, he interned in the web department as an associate web developer. Shortly before graduation, he was offered a full-time position in this department - "an interesting job, a very small shop," as he describes it. "The whole web department for the public website, the mobile app, all of it was just three people, and I was one of those three."

Additionally, Thomas assisted the Security department. "We had one Security engineer, and a [Chief Infomation Security Officer (CISO)] position, which was always unfilled. So I was always supporting and helping in Security matters. I got very interested in Systems, and started branching out a lot into System Administration, and then Networking on top of that."

Thomas felt he had gained all the experience he could from the position he was in, and so began looking for a new position as either a DevOps engineer or a Security Engineer, with a preference for Security. When the Security Engineer position at Radford became available, he took that position.

Eventually, he was made backup CISO, and after the CISO left that position, he was made acting CISO for Radford University. Through this position, he became involved in the Virginia Alliance for Secure Computing and Networking (VASCAN), where he was able to meet and collaborate with other CISO-level peers throughout the Commonwealth to gain insight on best practices and lessons learned. Through connections made at VASCAN, he learned of the ISA position at ODU.

I met with him over Zoom on November 4th, 2022, to get some of his insight as a working professional in the field of CyberSecurity.

Baty: What are the most important knowledge, skills, and abilities needed by someone in this field?

Thomas: Information Security is one of the few fields that has an incredibly wide background of people coming in. In a way, you getting a Cybersecurity degree makes you a minority in the field.

I would say that program should teach you a ton of theory of the why and how. Things like "principles of least privilege" and all these principles of Security. And those are great and good things to know.

But without a background in the actual core of IT, they can be hard to apply. So I have felt incredibly well-served from my background as a developer, for one. that's a skillset not a lot of people have in Security, so that's been invaluable in a lot of ways.

And the other: SysAdmin, and Help Desk, for that matter. You know, when you rise up out, especially out of Operations.... It's incredibly common for people to start in the field as a [Security Operations Center (SOC)] Analyst. You're sitting there, you're responding to alerts, you're following your procedures and your playbooks, you're escalating, and you rise up the ranks there. But as you get into Security engineering, now you're building all those tools and procedures, and helping inform the business on risk, and 'what should we do'. There is a cost to implemting two-factor authentication for an entire university, and not just a monetary cost, right? The politics, the getting buy-in, the supporting from a help desk standpoint, when it doesn't work, when they lose a phone.

It's one thing to read in a book 'hey, this is what you should do - you should block all outbound traffic'. Oh yeah, that sounds great! And now have fun writing forty thousand firewall rules to allow what's needed, granularly. So you've gotta take tradeoffs. There is a huge benefit of having other backgrounds than just running IT, and business, to help inform the Security. So I wouldn't trade my Systems background for the world. It's been invaluable on top of the Security skills.

Baty: Do you find the skills learned at CTFs useful in your job?

Thomas: If you want to be a penetration tester, CTFs are wondeful. You know, they're not always one hundred percent applicable, but they're far more applicable to that career path. And that is my recommendation for people who want to do pentesting. You should go do Hack The Box and Try Hack Me and compete in CTFs, because it's that sort of relentless 'try this, fail, try again, do this again' - that is what pentesting is at the end of the day. So it's a pretty applicable skillset, even if in the real world no one's using steganography and hiding flags like that.

But what CTFs really help show, especially to a potential employer, is some drive and curiosity, and that can be a very valuable thing to show, without a doubt.

Baty: What is your most favorite or most challenging event or project you've worked on?

Thomas: Small things can have huge impacts. Our SSO page at Radford got, I think it was forty thousand authentications a day. Which is not actually that big, in the grand scheme of tech - it's not Twitter, right? But, when you pulled up our SSO page, it didnt' have the auto-focus attribute on the username, so you'd actually have to go and click 'username' to put in your username. And I saw that one day and went and changed it, added autofocus. This is where your cursor should start, you know?

And I thought to myself, "over ten years, forty thousand logins a day, how many seconds of time did I save? Like, aggregate human time of not having to grab your mouse and click the username box". Admittedly, this was bad. Like, I didn't follow change management, I didn't get approval, I didn't go through any of the stuff we were supposed to. But the thing that just made me personally happy was just, "How much time did I save?"

Baty: The focus of the degree I'm doing is very technical: programming/CS type classes; electrical engineering type of classes; and then policy/cyber law type classes. I realize this is pretty broad, but I was interested to know what you might suggest as far as entry-level jobs, or what sort of jobs I should be looking at in the next eighteen months for when I graduate?

I don't know a ton about ODU's program, and it's a little heartening for me to hear that there is a bunch of technical stuff. I'm biased, I'm a computer science major, right? Like, I did software engineering. But I do think that it did help me a bunch. Did it teach me my day-to-day on the job skills? No, not at all. But it does inform that foundation of knowledge, without a doubt.

So, what do you like?

Baty: I really enjoy programming. I'm really attraced to the hands-on-keyboard, digging around in memory, researching, looking up man pages. That's what I'm interested in.

Thomas: Are you interested in consulting? Being billable? Working your own hours? Or would you rather be ingrained in an organization and be part of that team? Huge companies? Small companies?

Baty: What I'm looking for most is stability, ideally something fully remote. And maybe the flexibility to take some freelance work, but I don't love the idea of relying on freelance work. I would love a full-time position with benefits somewhere.

Thomas: Well, that's why I ask. Very few companies have an internal red team. They do, but they're the huge companies that can afford that, so you're gonna work at like Fortune 500 to do that sort of thing. I personally know that I don't like tracking hours, I don't like billing hours to clients. So even if you're not freelancing, most pentesting firms, that's what they're doing. If you work for the pentesting firm, you're a consultant for a client for a week or two, and you're billing and tracking your hours. I just happen to know that's something I'm not interested, so I just rule all that stuff out.

I'm also a little risk averse, like you said 'stability'. I ain't taking contract jobs - nope! I don't want a six-month contract and try to figure out where my next job is after. So that's why I ask, because it can change things a little bit.

I would say, obviously, most blue team jobs aren't so much the contract/consultant. You're usually ingrained in an organization and part of their IT program. So if that's something you're interested in, or if those sorts of things are important, there's more doors there than if you wanted to go red team side. Not to say you can't - you can have it both ways there too, it's just a little harder. It changes how you're applying to companies, I'd say, to an extent. Landing jobs at Silicon Valley and Fortune 500 -- they're just different and weirder.

SOC Analyst is the poster board entry-level job, and depending on how mature the organization, it can be fifteen dollars an hour, checking alerts, and following step one-two-three-four-five, and escalating higher up. Not super engaging work. Or it can be something more like what we do. Like our entry level SOC Analyst, sure, you're getting that operations experience, and doing that alert triage. But you're also probably doing incident response. You might get to do forensics on a compromised server or workstation, but we don't do a lot of that because time is scarce. If it came to the point where we need forensics done, we've probably engaged an external forensics firm at that point. We're gonna pay them to do it, just because those skills are so niche, you've got to do it to keep those skills sharp, and we don't have a business case to do it all the time.

So, you know, that's always the staple, if you can get a SOC Analyst job. The most important thing is getting some experience in the industry, to then go the direction you want to go. You almost can't go wrong there.

I wouldn't stray away from a SysAdmin job. I think that could be - you talk about hands-on-keyboard, wanting to program. SysAdmins who can program - people wil love you. You wanna script and automate stuff? People love you. And it's great experience. Computing in an advanced, corporate enterprise is completely different than your home lab.

If you like programming, I wouldn't be afraid of a developer job. Especially, there might be some jobs around application security. That's its own entire field. That was one of the things they were excited about hiring me for, because we didn't have a lot of people versed in

development and security. So DevSecOps, that's its own entire field, if you're more interested in being part of a development shop.