**NICE Framework in Focus – Miguel Ramirez**

**Mr. Petersen**: Hello, this is Rodney Petersen, the Director of the National Initiative for Cybersecurity Education. Thank you for joining us today for our Framework in Focus interview where we're joined by Miguel Ramirez, who recently completed an apprenticeship program with the Information Technology Department in the State of North Carolina. Miguel, thank you for participating in this interview.

**Mr. Ramirez**: You're welcome, Rodney.

**Mr. Petersen**: Miguel, please explain your role and responsibilities as an IT security and compliance apprentice.

**Mr. Ramirez**: My role as an IT security and compliance apprentice consisted of vulnerability management and assisting with compliance regarding state regulations and also PCI TSS framework. The State of North Carolina has PCI networks, PI networks, and also other networks. We have to be compliant with the state's laws and regulations, and also industry standards such as PCI TSS. I also was part of an in-house SOC team. We monitor incidents and events using SIMs and IPS alerts and my role was to track them down, find the system in play, and determine whether there was a false positive or an actual threat that needed to be escalated or resolved, if possible on-site. That sums it up.

**Mr. Petersen**: What does it mean to be an apprentice? Were you an employee, were you a student, were you doing this as an internship? Describe what the apprenticeship experience was like for you.

**Mr. Ramirez**: The apprentice experience was a little of both school, I worked for Innovative Systems group, they were my sponsor. They provided schooling on Fridays. It was a work day sitting in a lab with an instructor going over materials. We focused on pen testing, vulnerability assessment, and different tools we might use in the state. Then, Monday through Thursday was a regular week as an analyst. When I first started it was more shoulder surfing, learning the tools. The state sent me to different classes to learn the different tools that we use, and also online resources so I could be a little bit productive. Within six months or so, I would say I was very comfortable with the tools and the processes, but I was still learning the environment. One of the hardest things in government is learning the environment. It is so complex and so vast that in order for you to put your skills to work you have to know who to contact. You don't play by yourself. It's a team of layers of people you work in sync with to resolve issues and get things done. That was my role.

**Mr. Petersen**: You were part of the Information Security office team. Can you talk a little bit about that team? What were some other roles played? Maybe start by letting us know who you reported to in this position.

**Mr. Ramirez**: Let's start by talking about the most previous role. The two-year apprenticeship position was in two locations. The most recent - let's say the team was a ten-man team, we have a recon lead, a disaster recovery analyst, an ability management analyst, policy, and an, almost like an integrator analyst and team, and a threat management analyst. Those were two-man teams and we alternated. The primary role might be vulnerability management and an assistant you trained up. Everyone on that team had assisted or had other duties, but they could rely on when they were on vacation or when they weren't there. Then I reported directly to the Department of Transportation CISO. The second year as an IT employee, our team was located at the Department of Transportation and the CISO that was there, Al Rothsenburger, our team directly reported to the CISO.

**Mr. Petersen**: Talk a little bit more about your career path toward becoming an apprentice in the Department of Technology for the State of North Carolina. What was your career path to get into that role?

**Mr. Ramirez**: My career path getting into the apprenticeship role started when I was injured. I had a Humvee roll over and I was recovering, and I decided instead of just sleeping my life away, I sat with this program called WayTech. It was a community college in Raleigh that was offering refreshers on some of the courses I had already taken in the Army, like Net+, Security+, CH, A+. I was going to school Tuesday and Thursday nights and Saturday mornings. During that time, once I completed my CCNA course, a gentleman by the name of Tony Marshall, the CEO and President of Innovative Systems Group approached some of us. He asked the professor who were the top-notch students – at least that's what he told me. He interviewed me and told me that he might have a position as an apprentice with the State of North Carolina, and he wanted to hear more from me and about me. That was our first conversation. After that there were a few more interviews with him. Then within a month or so I was interviewing with the state chief security officer which was Maria Thompson, and some of the other directors in North Carolina. I was chosen as one of five candidates. That was October 2016. The rest is history.

**Mr. Petersen:** Thanks so much for your service, and I'm so sorry to hear about your injury. But thank you for your perseverance and pursuing a cybersecurity career. This column is about the NICE Cybersecurity Workforce Framework and I wonder if you could talk about how you would use the NICE Framework to further guide your career.

**Mr. Ramirez**: I've actually used the NICE Framework for education purposes. The role I'm currently in, if I'm not mistaken, falls under 101 category, because we do have to investigate. It falls under that piece of the pie, protect and defend, and operate and maintain. But also, as developers build web pages or stand up systems, we kind of oversee that process as well. I see security falls across all the realms. We oversaw the majority of what IT did. Now the NICE Framework, if I'm not mistaken, also provides the guidance to the NIST Framework as well, is that correct, Rodney?

**Mr. Petersen**: There are some cross-maps to the NIST Framework that talk about the "what" and "how" of cybersecurity for critical infrastructure protection and the NICE Framework is more the "who is going to do it?", and what knowledge and skills they need.

**Mr. Ramirez**: That is my experience with the NICE Framework, but I've noticed with certain aspects of security, there were certain roles and based on those roles and skills I also used it for my education to see what I needed to focus on as an analyst or as a security officer. It gave me guidance on where to continue my studies or where to continue my training. Does that answer your question, Rodney?

**Mr. Petersen**: It does, that's great. On that last point, when you described the NICE Framework to identify either knowledge or skills that you need to develop to move up in your career, or maybe knowledge and skills you need for your current job, how do you keep your skills sharp and current both now and in the future?

**Mr. Ramirez**: It's an everyday thing. I read a lot of security blogs. I read a lot of internet pages, like dark reading. I use Cybrary, which is an online free, open source, educational video log. It's like a training portal. I also use FedVTE, which is accessible to veterans, to take classes online and for free. Mainly I'm staying current with what's new in technology. What tools, what technologies are being degregated, what security protocols are changing or degregated, or what's changing with the web. I read a lot about technology. There's a lot of forms out there. I specifically follow dark reading, which is a form. It gives me the next trends, the next reports in cybersecurity and I go on and do a little bit more research on my own.

**Mr. Petersen**: That sounds great. What do you see as the role of diversity in the cybersecurity workforce?

**Mr. Ramirez**: I think it's changing. The diversity, at least in North Carolina, I've noticed coming in from different fields even in the Army. In my work, contracting in the last year or so, females are starting to come up the ladder. For example, our chief information security officer is a female, Maria Thompson, whom I greatly respect. It brings a little balance to what used to be an all-male institution. Some of the directors in the State of North Carolina are females. There is a balance that's being changed right now, where it's becoming more balanced. For example, in both teams where I work for the State of North Carolina, I was the only Latino person there. But I also saw different ethnicities within the groups but with me being the first, it also speaks to the diversity of the state that things are changing and being a bit more diverse. I think everybody brings something to the table, especially going back to the female thing, it's a good thing. Females balance us and have a different perspective on how to handle things and it keeps us in check. The State of North Carolina is headed the right way. It's achieved diversity.

**Mr. Petersen**: That's great Miguel. As a Latino, if I could ask a follow up question. If we were to want to increase the diversity, particularly ethnic diversity in hiring Latinos, what would you say to hiring managers and directors about how to get more Latinos into the cybersecurity workforce?

**Mr. Ramirez**: One of the reasons I think we're not more represented is because there may not be that many Latinos in the cybersecurity realm. I know that North Carolina has a large population of them. Maybe to advertise to different groups and ethnicities to pursue a cybersecurity degree or technical skills and then you create a pool of candidates. As you know, Latinos are known to be hard workers. We're grateful we’ve been accepted into this great land, the USA; the ones that want to do the right thing and better themselves and be an asset to an institution. Does that answer your question, Rodney?

**Mr. Petersen**: It does. Thank you so much for that perspective and experience. I want to go back to your role in the Department of Information Technology in North Carolina. What did you enjoy most about the work that you did?

**Mr. Ramirez**: What I enjoy most about the work that I did in IT was the work constantly changing. It was one thing one day, assigned another task or fire to put out while I was doing that. It was very fast paced. I had access to some of the best training in enterprise tools and very seasoned analysts and people, all the way down to the analysts and all the way up to the CISO, they were very eager to point me in the right direction. Pointers included what to study, what to do, to include one of our CISOs, Chip Moore, at the IT. From day one of your theoretical studies you should be aware we use Cisco's IPS; you learn that tool. When you leave out of here you'll be a candidate for a high paying job. They pointed me to some of the tools and gave me access to those tools. At first it was read access. They gave me a vast knowledge of how to guide myself in my path to becoming a security analyst and the resources, support and guidance overall. That's what intrigued me about working there. That those people were so eager to help me achieve greatness.

**Mr. Petersen**: I'm glad you had a good experience there and thanks for sharing that. The final question, Miguel, is if you could give advice to a young person considering a career in cybersecurity, or maybe somebody who is an older adult considering changing careers, what would you tell them?

**Mr. Ramirez**: First, if you're passionate about technology, and you like learning new things every day, after mastering a trade and thinking you're not ever going to go back to school and you're never going to refresh those courses, it's not for you. First you have to identify you have the passion for it. If you have the passion and you like learning new things every day, and you like staying current, then the cybersecurity realm is for you. Also, I think it all starts with self-motivation and finding a mentor, someone in the field to guide you and provide you the resources, or at least point you in the right direction so you're not zig-zagging through coursework that doesn't relate to one another. Then you have a linear path toward becoming an analyst or technician or whatever role you're seeking. There are different fields like policy, which is more management, or threat hunting. They can describe those things from the get-go and give you a better description of operations in those fields, and therefore, you can better assess which of those fields you want to go into within cybersecurity.

**Mr. Petersen**: That's great advice, Miguel. Thank you so much. We've been speaking with Miguel Ramirez, who is an apprentice in IT Security and Compliance with the Department of Information Technology in the State of North Carolina. Miguel, thanks so much for participating in the NICE Framework in Focus interview.

**Mr. Ramirez**: Thank you Rodney, it's been a pleasure.