## Framework in Focus: Maril Vernon
## Winter 2021 (publish date: January 2022)

Maril Vernon is an Offensive Security Engineer at Zoom. In this interview, Ms. Vernon discusses the variety of cybersecurity roles that exist, shares the importance and value of engaging with the cybersecurity community, and shares the joy she feels working in this field, among other topics.

---

## Interview Full Transcript:

**Karen Wetzel**: Hello, my name is Karen Wetzel. I am manager of the NICE Framework at the National Initiative for Cybersecurity Education at NIST. The NICE Cybersecurity Workforce Framework, published as NIST Special Publication 800-181, establishes a taxonomy and common lexicon used to describe cybersecurity work. The NICE Framework is intended to be applied in the private, public, and academic sectors. In this edition of the NICE eNewsletter series, *Framework in Focus*, it is my pleasure to speak with Maril Vernon, offensive security engineer. Maril, thank you for letting us learn more about your career pathway and understand the NICE Framework from the lens of someone like yourself, who is performing cybersecurity work.

**Maril Vernon**: Absolutely. It's awesome to be here.

**Karen**: Let's just jump into it and get started off with maybe an easy one. Can you explain more about what an offensive security engineer is?

**Maril**: Absolutely. Offensive security engineer is kind of a broad title, and they do that on purpose. For my org, specifically, that's very purposeful in how we title everybody. Typically when you work in offensive security, people mostly know you as being a penetration tester, or pen tester for short. However, within offensive security, you can do a number of things. You could be a pen tester; you could be a proper red team operator; you could be a purple team operator; you can be an exploit developer; you can be developing tools; you could be developing tools for exploits, reverse malware engineering.

Of all those flavors that are available, I specifically am a red team operator, which is nuancedly different from a pen tester. Pen testers, when they conduct an engagement against a target – so someone will contact them to say, hey, I think this product or my network is so secure, will you come in and test it to make sure I'm as secure as I think I am and I haven't missed anything? So pen testers want to get in there and kind of want to find everything they can possibly find. They want to throw the kitchen sink at you and see what sticks and try and find as many vulnerabilities as possible for you to remediate. If you're doing a proper red team engagement,

generally you have a much more specific goal. Like, my goal is to get you to provide me corporate credentials on a malicious website; or to get remote code execution on a compromised remote host; or to exfiltrate data from your environment without you knowing. Typically you have a very specific objective, and everything the red team is doing is to that end objective. We could get in and start messing with your SQL databases or deface websites, but we're not going to do that just because we can. We want to get in, be stealthy, stay low under the radar, accomplish our objective, and get out without you knowing we were there. That is actually the kind of team that I work on.

**Karen**: It sounds like it could be a lot of fun. As the red team lead, what other kinds of people are on your team? What other kinds of roles do you work with?

**Maril**: On a red team, it kind of depends on the size. You can be a one-woman red team, as I was at one of my previous organizations, where you're kind of doing the [gamut] of vulnerability testing firewalls and products and pen testing your website and helping the devs do DevSecOps and all these things. Or, if you're on a larger team, typically a red team will have someone doing exploit development, someone who's in charge of infrastructure, someone who's typically really good at pivot and lateral movement. You'll also possibly have a social engineer or someone who's good at the client side of your kill chain. That's what usually I specialize in. I am gregarious and outgoing. I came from a customer service marketing background. So I'll hop on and pretend to be someone else, or I'll write all the phishes and stuff. You'll work with a number of roles. As far as roles we work with in the organization, I think this is so important for a red teamer because a lot of red team operators seem to think they get to kind of hang out behind the curtain and they don't have to answer much or do a whole lot. As a red teamer, it's really important for you to build rapport with other departments. We work a lot directly with the CTI teams, which is cyber threat intel, DFIR teams, digital forensics and incident response, the SOC, which is the security operations center – those are all technically blue teams. We work a lot with the other departments because at the end of the day, our goal is to make our organization more secure. There can be a lot of animosity because blue teams just kind of see you as firing missiles and tearing down their product and telling them you found all these holes in their system, which makes them feel like they do a bad job. But we're not here to tell you that you do a bad job. We're here just to make sure that, for whatever reason that hole is there, it gets addressed before someone really bad tries it. So you want to do a lot of relationship building; you want to do a lot of interfacing; you do a lot of assuring managers in other departments who aren't technical that our goal isn't to come in and take down the company. We're not going to delete a bunch of things in production. We're not going to take the entire company offline. We're not here to boot users out of their computers and limit productivity. You want to do a lot of reassuring and explain to people what you do and how you do it and how everything has a learning objective; everything has a purpose; you're not just doing something because you can. Because being on a red team is really powerful, so you need to make sure you're not doing what you want – you're doing what you say in your test plan because that has a purpose for the org.

**Karen**: We introduced competencies in the NICE Framework with our latest revision that came out in November 2020. Included in there are those professional competencies or soft skills because we keep hearing from the community how important those are, in no matter what kind of role one plays. Just as you were saying before we hit record, I know you were talking about you do more work [ ] than people might think you might do. Having those communication skills, as you said right there, being able to have those interpersonal skills is key. You also mentioned you came from a customer service background. I think you began your career in marketing, is that right? What led you to cybersecurity in your current job?

**Maril**: I did begin my career in marketing. I actually used to be a copy editor and social media marketing manager for a hospitality brand. That was where I grew up, corporate-wise. I got into cybersecurity because one day in my marketing job I looked at the jobs ahead of me. I looked at my boss and her boss and his boss, and I was like, I don't want to be any of those people. They have no work-life balance. They're super stressed-out about certain things all the time. I'm pretty good at my job, but I've kind of hit the ceiling so I needed a new challenge. I was known for kind of industry hopping because I would find a new industry and get super excited to learn it and then I would master it and kind of get bored. So I was desperate to find an industry where I would never kick back one day and say, well I know it all now and I'm the all-knowing expert on everything and there's nothing new to learn. Cybersecurity was just that perfect match made in heaven. I don't know anyone who claims to know it all. Everyone is learning something new every day. We're all kind of perpetual students, and I think that makes us more effective security professionals because continuous education is a pillar of being a professional. It's just really reassuring because you can know that you're probably not the only one in the room who hasn't heard of a new term or a new tool or a new framework. Probably some people have, but probably some people haven't. It's reassuring to know that you're amongst other people who want to continuously learn, just like you.

**Karen**: This is definitely not one of those fields where nothing changes. One of the things that I heard in the last year or so is that we're not looking at career ladders anymore. It's a career lattice. There are always those lateral moves, and I think that's going to be much more common. Luckily, in cybersecurity there are tons of roles and lots of opportunities. Even if you're in one spot in cybersecurity, there are always places to continue to grow. You were talking about wanting to learn a lot. Now, with what you're doing, how do you keep your knowledge and skills sharp and current? What are your tricks to doing that?

**Maril**: Part of my recommendation such as like knowledge would be: If you know where want to be, if you know what your next role looks like to propel your career forward, then learn the things that will give you the most return on investment for that role. For me, when I came over here, there were certain things I wanted to learn but certain things that would benefit my org and benefit my team for me to learn. They're not always synced up. So while you want to learn everything, you have to target the things that are going to propel you forward in the role where you're at. Let's say you're in an all-Windows and AD environment and you're like, I'd really like

to attend this sector ops training on Mac OS opportunities. That's not going to serve you in your role although it would be cool to know. So I always say let your role define what you learn next. Always have a career plan in mind. As far as industry knowledge, I rely a lot as a fly on the wall in most of the hacker environments. Discord servers, Twitter conversations – that's where people are posting new bugs that they're finding, new breaches that are happening, new tactics that they're seeing. As I come across those things, I'm like, oh man does this apply to us, or have we already tested that? A lot of your industry knowledge is going to come from your peers, so if you want to be plugged into hacker things, then you need to hang out where hackers hang out.

**Karen**: Luckily, with cybersecurity, we do have such a nice, strong community and one that is really willing and open to work with each other and share knowledge. It's great that way. You know my perspective – I always am coming back to the NICE Cybersecurity Workforce Framework and how people use that. What are your thoughts on how you might use that for your career?

**Maril**: For me specifically, I'm not really in a management or a hiring role. I think a lot of managers and hiring people could use it to better understand the skills that are demanded by a cybersecurity role and not just the acronyms they hear associated with a cybersecurity role. For me, who's someone who's really big in the mentoring space and kind of informally involved in that give-back community that we have, my biggest thing I want people to know is that pen testing is really fun and really attractive and pays a lot, of course, but it' s not the end all be all. A lot of people are like, I want to be in cybersecurity so how do I be a pen tester. I'm like, well why do you want to be a pen tester? Pen testing is fun, but it's also more than people think it is. I maybe spend 20% of my time actually hacking something and the other 80% writing and defending reports and test plans and attending meetings. I always ask people why, and I want people to know that pen testing is not the end all in cybersecurity. You can learn about so many cool roles. I always say find a capability or responsibility and find a role that relates to that. Don't necessarily get attached to a job title. That's really what I want people to know. There are so many cool places to go in architecting and DevSecOps and Cloud architecture. There's purple team. There are tons of opportunities as a security engineer on the blue side or an offensive security engineer on the red side. Just because you're on the red team doesn't mean you're stuck in the pen testing box either. Again, you could be a reverse malware engineer; you could be a binary expert; your could be a source code expert. There are so many niches in this field, no shortage of things to do, so don't limit yourself by thinking, if I want to contribute in this field I have to be in offensive testing and I have to be in pen testing. I myself really pride myself on being the type of red teamer who doesn't just leave a smoking pile when I'm done with an engagement, like that was so fun, thank you for letting me break all your systems. Your value comes from providing effective recommendations to those defensive teams, who are going to take the things that you found and try and mitigate around them. I am one of the few people who understands a lot of the blue side, a lot of the threat hunting side, a lot of the detection side, as well as the red side. That's what makes me a really effective purple teamer. There's no shortage of places to go. Use this Framework to see where people were and where they ended

up and the skills they relied on to get there. Find an alignment and maybe you can target a trajectory that's the same. Or you can pull enough from their career path but change it up a little bit and add in a few extra skills they didn't have and create a niche of your own.

**Karen**: One of my favorite ways that people use the NICE Framework is that career pathing. You mentioned earlier that it is an important thing to do, to plan your career and always think maybe a step or two ahead. We have over 50 work roles identified. We're looking at adding others. If there's ever interest in expanding, that's something we're always open to, as well, because this isn't a static field. We've just, as I said before, introduced competencies, and there are 50 or so of those. We're cConstantly looking at the different kinds of things that someone might be able to focus in on. What skills are in those areas, or if I'm looking to collaborate with people in different spaces and be able to identify what they are focused on – it can be great that way. There are so many jobs out there, but what are your thoughts on the ones that might be the most difficult to fill today.

**Maril**: I would say anything where you have cross-responsibilities. You might be a network architect but someone needs someone with Cloud specialties. They need you to be somewhat network architect but somewhat Cloud also. Or someone who's a red teamer even. You might know how to operate really well, but the second you get an AWS key you don't know what to do with it because you don't have Cloud knowledge or you don't have some piece of something that's not just your lane. There are so many multiple lanes involved with just about any job that it really behooves you to become not an in-depth expert but at least a service-level expert in as many lanes that apply to your role as possible. Being someone in offensive security, I understand red teaming really well, blue teaming decently well, and I understand risk really well. Business risk – that's a business function, not an IT function, but it serves me to know it because when I'm trying to explain to a business manager why something I did is bad and make the impact statement, I can tie it to dollars; I can tie to revenue; I can tie it to productivity lost and make it in terms they understand. That really helps drive my program forward because I get more buy-in from those managers versus in a language they don't speak. I just think the roles that are hardest to fill are the ones where we don't need someone to just be an expert 10 layers deep in one thing. We really need people to be three layers deep expert in three different things. That's where I think your time is going to be better spent. See what companies are doing. See what other red teams are doing, and see if you can give yourself one or two capabilities that will fill a hole because that's how I got onto my team. I was lighter on the red team than everyone else. But given that we had a bunch of people with super heavy red team experience and I brought Cloud, client side, social, and purple team, that's not something that anyone else had. So that was value that I was immediately able to contribute that was a niche that was mine. Those are made up of capabilities you don't typically see go together. It's like, why would you pick those things. That's just how my career evolved.

**Karen**: Do you think then that these are maybe the more the emerging kinds of jobs that are out there too, or perhaps even the more crucial ones, just because they are not as common?

**Maril**: Yes. Anything where you see on a job description two or three responsibilities where you're like, that shouldn't typically be the same person. Typically, you need one employee for each of those – they might, but they might not have that bandwidth. So in the interim, they need someone who can, even at a very beginner level, do those three things. And then as your workload becomes too much and you're seeing now all three of these things are demanding too much time for one person, now they can justify the additional resource. And you can say, hey, this is what I've put in place, this is where we want to go, and I can't get there by myself. Now you are in charge of kind of knowing what that workload looks like and that process flow and you become even more crucial. So a lot of pen testers are not just pen testers. They're project managers, and they're also consultants, and they're also like hey, evaluate this product or we want to use this DLP and what do you think? That's a defensive tool, but as a red teamer I'm going to say that tool sucks because I've been in an environment with that tool and they didn't see a thing I was doing. I know exactly how I would get around that. But *this* tool is really great. So you're going to serve in multiple hats no matter what role you're working in. That's why security people are so hard to find. It's like, I don't just need a security person. I need a security person with a little bit of project management, with a little bit of this, with a little bit of that, and that's why they are so hard to find. What skills do we focus on, and what are the auxiliary skills that that person might need to have.

**Karen**: And yet it's why it's such a great field to go into, for both upskilling and reskilling as well as just straight out of skill. It has a lot opportunity.

**Maril**: Absolutely. There's a path you can carve for yourself just about anywhere you point.

**Karen**: Exactly. So switching perspective here. We know that workplaces that value that diversity, equity, and inclusion have rates of return, make for smarter teams, have improved outcomes. Can you share about how DEI has played a role in your career and, in some ways, maybe you're trying to see how you can make your own workplace more diverse?

**Maril**: Absolutely. I'm a walking diversity case study. I came from a non-technical background, from a non-technical family. When I started, I didn't even know what IP addresses were and how those worked. Someone took a chance on me, took a chance on my academic aptitude, took a chance on my drive and my ethic. I told them I might not know that thing today, but if you give me a week I will know that thing and I won't just know it a little bit. I'll know it backwards, forwards, and upside down. I will know it really well. I was given a chance, and I brought a level of diversity to my team because they had been working in tech for 50 years combined among them at the time. They were all kind of used to looking at this stuff, and they don't bring the fresh perspective that I do. So they'd be like, nah this is normal, and I'd be like, well why is it necessarily normal? Couldn't that indicate this, this, this, and that? And they were like, oh my gosh she's right – we didn't even consider that. So everyone has a unique perspective to bring. I always say if you're working in sales, audit, customer service, marketing, a different function of IT – anywhere that you can come from, you can bring something to this field. I think the more perspectives we gain, the more differing opinions we have, and the more

different learning paths people took – because some will be self-taught, some will rely totally on classrooms, some will have brought the biggest, baddest bootcamps out there – all these people will bring something different, and I think the more differing opinions you have, the more value-added and driving discussions you have, the better your security program will be. We've seen that time and time again. As you give people from lower income backgrounds, people from different socio-economic backgrounds, people of different nationality backgrounds even have a different outlook on cybersecurity than us. I think the more the better. I don't want to have an idea and everyone in the room goes, yes that is the best idea that we've ever heard. I want people to say, why? Have you considered this? What if you tried this? I will take that feedback every time and say yes, thank you for making my product better. We could have just launched it, minimum viable product, but now it's going to be even better because you contributed something I didn't see.

**Karen**: It's that whole idea of not wanting to be the smartest person in the room. You do better when you've got other people around who can actually question the work that you're doing and make sure you're heading on the right path. I was just reading a report earlier today abut people who are successful at recruiting for cybersecurity positions, and one of the things about the people who were most successful is that they were interested in and more likely to hire less-experienced candidates as well as having some re-skilling in programs in place. Looking for that maybe non-traditional person to come in to bring that different perspective can actually be a really good approach.

**Maril**: My old CISO – he was a pretty smart guy and he's been working in this industry a long time – he used to say, I don't want to be smarter than my team. I hire people smarter than me on purpose. I want them to outthink me. That was a great philosophy to have.

**Karen**: Exactly. I've heard a lot of joy in your voice when you talk about your work. Maybe you can be a little more explicit and tell me, what do you enjoy most about the work that you do?

**Maril**: I do love my work. I love my work more than anyone should reasonably love what they do for work. My favorite part of what I do is how creatively I have to think. Nothing in my field is a straight cut a to b, we're going to get in here, hop here, get in here, and now we're done. There is constant pivoting. There is constant in the middle of the operation, oh man, this isn't working, what else can we try? You have to get really creative with what's in front of you, and I love that because I want to solve the puzzle. I want to find every teeny, tiny little piece of information that's 8 years old and hidden in an image somewhere that you totally forgot about it and I find it and now I have a backdoor. I love that about my job. It's like a little treasure hunt every time. I really enjoy trying to be as crafty and sneaky and legit-looking as possible to trick people and to worm my way around an environment. That's my favorite.

**Karen**: It sounds like a lot of fun the way you describe.

**Maril**: I only get to do it 20% of the time, but when I do I really love that part of my job.

**Karen**: And that it's fresh. It's not the same thing each time. That, I think, makes a big difference too. My last question to you is, for someone who's considering a career in cybersecurity, what bit of advice would you give them? We've heard a few things from you already, but is there one that you would really want to make sure they hear?

**Maril**: I would say be open to the foot-in-the door position. So people are like, I'm not going to accept anything unless it's a pen tester position. You know that's good, I guess, to have that drive, but I got in as a risk analyst and I went from risk analyst to pen testing because it's much easier to pivot yourself into a security role at an org when you can speak to their security goals, program, and outcomes already because you have that knowledge having worked with security in a different capacity. So be open to those off-the-beaten path positions. They're a place where you can learn a lot without the pressure of having to perform in a security capacity right away, and they're a place where you can get a lot of information about how security relates to the business as a whole.

Additionally, I would say get a mentor. Literally, if you think you want to be in cybersecurity, explore some different jobs, Google some different job descriptions – put security engineer in, put architect in. See what the things are that people look for in these jobs. Then go find someone on LinkedIn with that job title and see where did they start. How did they get here? What places did they work? What roles did they have? What projects did they work on? That will tell you the best experience that's going to get you the most ROI to get you where you want to go. And it will tell you what organizations take chances on people who need to gain that experience on the job, as an added benefit. I would say have a plan, and get a mentor. If you know you want to be a CISO one day, and you know what role steps you would take to get there – what your stepping stone are – get a mentor in that space because they will help you do it more efficiently than they did it. Even if they did it in 3 years, they will teach you how to do it in 1 year if you take the proper steps because you need not repeat the mistakes that they made. I had six mentors when I first started and I still have four to this day, so mentors are awesome.

Additionally, I would say start showing up where we show up. We have a very small world, and the more you're known in it the more people will think of you. I know almost no people who can just coldly apply for a job and get it. It's a very hard club to get into, unfortunately. But I know people who are like, I said I wanted to work in this field and someone I know recommended me to their boss and now I have an interview. We're all technicians, and technicians hate being social, and they hate networking, and they hate talking about themselves and how cool they are. But you need to network yourself and tell people how cool you are or they won't know. So start showing up in our communities, in our Discords, in our Twitter. Start commenting. Interact with people, and then say, hey we seem to interact on the same stuff a lot. We seem to have a lot of the same views about security or MITRE or red teaming or purple teaming, and I would love to discuss that with you sometime. Now you have a security buddy. And now, when that buddy sees you're looking for work, they're like, I know this person. I know this person has great ideas, understands the field, understands the methodology. I would

believe this person could do a good job, and we will recommend you to jobs for you. So those are my key pieces of observation.

**Karen**: That's great advice, and I even maybe say that a lot of that advice even works when you're at a large, even internal to the organization. Say if you're not in the cybersecurity area right now, maybe reach out and shadow someone for a little bit. A lot of times people are hiring from within. Like you said, if you already have that organizational knowledge, that's a leg up. An organization's not going to want to lose good staff if there's a better fit for them or a place for them to grow, that's in their best interest too. All good advice. I really appreciate this conversation. I'm sure we could talk for longer, but I don't want to keep you all day. Maril, thank you so much for your time today, thank you for sharing all of your insights and for letting us learn more about the kind of work you do.

**Maril**: Absolutely. Thank you so much for giving me a platform on which to continually talk, which I will do all day.

**Karen**: Well, we'll have you again another time. Thanks so much.