MACHINE LEARNING & AUTOMATION: TRUST BUT VERIFY

07/02/2019

Brian Contos: Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Lisa Huff. Welcome to the podcast, Lisa.

Lisa Huff: Thank you, Brian. Glad to be here.

Brian Contos: Lisa, we first started working together at ArcSight back in 2002, early 2003, and you've had quite a distinguished career in security throughout that time and following. Can you give our listeners a bit of a background on you and maybe some of the highlights?

Lisa Huff: Absolutely. I started off as a security consultant, networking and a security consultant. I realized that early on when I got my CISSP that the pivot from networking to security was an important one, and I made that pivot early on in my career. ArcSight, which is my first official sales engineering role – thank you for that, Brian – was my first go at sales engineering, and I spent 10 years at ArcSight. My career pivoted multiple times while [there].

Lisa Huff: I started off as a sales engineer and did very well. Then I realized that a lot of our customers were struggling with the implementation of our product, but because of the time I was able to spend with the customers, being very consultative during the selling process in many cases, a lot of those customers were following up with me on the back end, asking me more questions during post-sales engagements. I recognize that there was a gap with regards to the time that pre-sales moved something to post-sales and then what happens to the customer after that.

Lisa Huff: So, I started really focusing heavily on customer success. I wrote up my little, if you want to call it, my business plan, and I presented it to senior leadership at the time, and this was prior to our acquisition from HP, and they allowed me to build a team. We called it the Customer Success Organization and ArcSight Enterprise Specialists. Basically, what we focused on was ensuring the customers were happy, ensuring the customers were fully enabled with our solution, extending use cases, and driving value and up-selling opportunities. I did that for about four years. At that point, HP had acquired ArcSight once we

went public, then I pivoted into a consulting role, and I was running post-sales for the central region for HP for another four years after that acquisition.

Lisa Huff: From there, I moved onto an organization called Solera Networks, and again, one of the reasons why I went over to an organization like Solera was it was a different type of technology. I'd spent a lot of time with SIEM. I learned the space very well from a pre-sales and a post-sales perspective. I wanted to really dip my toes into something that was completely outside of my realm of what I'd learned in the past. I spent a lot of time getting to know the Solera solution.

Lisa Huff: Fortunately or unfortunately, we were acquired shortly thereafter by a company called Blue Coat. I spent a couple additional years at Blue Coat, and basically, focusing on the packet capture solution and doing deep packing solution, and basically going back to a lot of the customers that I had engaged with before during my SIEM days and basically learning a new product and positioning a brand new product to a customer, which was nice because it was my way of dipping my toe back into the pond and really understanding how all these different types of solutions that customers had made an investment in are being leveraged outside of SIEM.

Lisa Huff: After Solera, I pivoted over to a company called Exabeam. That's where I am today. I am the VP of North America Pre-Sales at Exabeam. The reason why I went over to Exabeam and what attracted me to Exabeam was that, at the core of what the product does, is that same thing with SIEM. The product collects logs. It's something that I know at the core of my experience, and it just seemed like the next logical step. The big difference between what we do at Exabeam versus what I was doing with traditional SIEM is what we do with the logs.

Lisa Huff: Instead of collecting logs and building correlation rules around that, we are collecting logs and leveraging machine learning, letting the machines do the heavy lifting, instead of having the humans be involved in it. We're building up models and building up a baseline of what's normal for a user and asset within a company's organization, and then what we basically do, it's very elegant and very simple, but there's a lot going on in the back end. We're basically bubbling up when someone does something different that's outside of what's normal, and that's what I'm focusing on right now at Exabeam.

Brian Contos: Wow. Very cool. A couple things I took out of that. I always find people that work in pre-sales are benefited from spending time in post, and people that work in post- are benefited from spending time in pre- as well. Those two are usually very, very different, those roles, but I think it really makes you so much better at whatever role you're in if you have exposure to the other side, and of course, you've done that for so much of your career, which I think has made you so successful and you've had a number of great wins. ArcSight, Solera Networks, now Exabeam, all amazing names in our industry.

Brian Contos: Lisa, let's get down to some of the topics I want to discuss. You spend a lot of time working with security teams, both inside and outside of the security operation centers, the SOC. Let's start by talking about the people. What's top of mind for security teams and SOC analysts today?

Lisa Huff: It's an interesting question, Brian, because it comes down to people, process, and technology. It's something that you taught me a long, long time ago when I first started at ArcSight, and it's still very, very prevalent as it stands today. Customers are really still struggling with all facets of that. Dealing with a lot of legacy technologies, underutilized technologies. In many cases, the legacy technologies are basically not being leveraged properly. They're not fully integrated into their current workflow processes. In many cases, it's either lack of or inefficient processes. Again, a lot of that gets down to underutilized teams or understaffed teams. In many cases, it starts to spread out so you also have problems with outdated systems and applications that create a lot of false positives and a lot of white noise, and it builds up to alert fatigue.

Lisa Huff: You know, you have a lot of these security analysts or SOC analysts having to deal with all of these challenges and, in some cases, you have inexperienced staff, and that's a huge pain point and especially when you have a lack of process and automation that causes a lot of times an infective response in automation from a customer perspective.

Brian Contos: Yeah, you know, we see that all the time. People have these legacy security controls and really what's legacy in our industry, a few years old maybe? They have these security tools in place, and maybe the person that was the champion they've left or they've moved into a different organization or they've just become bored with it, but people are still paying maintenance and support and they still have these products running. Maybe during the POC they just got all this value, and it was really awesome, and it was this new shiny thing and everybody loved it. Over time, it starts getting less love, so it's providing less value and now you're left with millions of dollars in security gear of which maybe you're getting 10%, 15%, 20% or 30% value from them because they just haven't been optimized.

Brian Contos: Or, more so, you have now people working in your SOC for example that haven't been trained on these or these older solutions that could provide a lot of value, simply aren't integrated with some of your newer workflow and your newer processes. I think organizations are wasting just a mountain of money and certainly time and resources on solutions that if they were a little bit less focused I think on the next new buzzword and a little bit more focused on actually getting results out of their security controls that they have, I think we'd be at a much better spot today.

Lisa Huff: I agree 100%.

Brian Contos: So, building on that, what are some of the emerging technologies that you see defining today's SOC, if you will?

Lisa Huff: It's funny, there's so many different products and solutions that customers are attempting to make investments in. Again, as I mentioned previous, customers are still struggling with getting value out of their existing investments, but they're also getting inundated on a regular basis by all these new solutions that are out there that are talking AI and deep learning and machine learning, and customers are struggling right now to understand what's the difference. When you ask someone about data science, and you have all these different products that are out there that are focusing, and they're just throwing around these buzzwords, many organizations have no idea what any of these things are tied to from a data science perspective.

Lisa Huff: From my perspective, and, again, this is based on my own experience and one of the reasons why I decided to move to an organization like Exabeam is the focus on machine learning. From my perspective, it's letting the machines do a lot of the heavy lifting, and as I mentioned before creating those baselines, and we've attempted in the SIEM days to do that artificially with static rules, and it was very difficult to build rules that are going to predict what's going to happen next.

Lisa Huff: Correlation was great for those things that were known entities, but what about the 0-day attacks, the new types of attacks that happen? The cool thing about machine learning and one of the things that I'm focusing on right now with my new organization is that it takes a lot of that heavy lifting and the hard work out of the human's hands, and it does a lot of the heavy lifting, and it bubbles up anything that's outside of what's normal from a baseline perspective. I think that any products that are going to be leveraging machine learning, I think are going to add a lot of value to the SOC because of the fact that you still have understaffed resources or inexperienced resources. In many cases these types of solutions can do a lot of the heavy lifting and present the results where you can get more impact from your level one and level twos.

Brian Contos: Yeah. I remember, and you were in the same role, we were out in the field with customers writing rules and developing strategies to get value out of their SIEMS, and the solutions that fed into those SIEMS. You'd write correlation rules, and you'd try to write it to the best of your ability based on best practices and this and that, but oftentimes you never really knew if they were actually going to fire a real-life case depending on what systems were actually able to report up at that time, and if the time stamps and the parsing were correct. There [are] just so many variables.

Brian Contos: Then you started getting into temporal based and volumetric analysis and anomaly detection pattern discovery, but it was still very manual. It was kind of

white knuckles if you will in terms of the approach, so any way to augment that with some back-end processes such as you mentioned machine learning I think it can really augment – probably not replace entirely – but certainly augment. I know there are some companies out there that claim, "Oh, we do everything with AI." One of the best statements I think I've ever heard about artificial intelligence is that in security there is a lot of artificial intelligence.

Lisa Huff: Exactly.

Brian Contos: Right?

Lisa Huff: Exactly right. That's one of the reasons why from my perspective at the end of the day when you see every single day a headline of someone being compromised, at the core of it, it doesn't matter what the attack method was used in order to get into someone's environment, whether it was someone that's rogue inside or someone is breaking through the perimeter and they're making their way inside through a phishing campaign or what have you. At the end of the day, it's all about credentials until there's a technology that is introduced that takes away the burden of an organization from maintaining credentials because that's at the core of everything.

Lisa Huff: Someone is looking for a set of credentials to compromise and they can move laterally to get to some type of whatever assets that have, the customer's crown jewels, and that typically will lead to some form of exfiltration. Until something is introduced to solve that problem with credentials and maintenance and upkeep of those credentials, it's going to be an ongoing problem.

Brian Contos: Yeah, certainly. I think it's well said. Identity sort of permeates everything that we do these days and it used to be network access control and you were tying things to devices, but now with IOT and Cloud and just the pervasiveness of systems that people are accessing and number of accounts, identity just becomes so critical in that overarching role.

Brian Contos: So, let's kind of pivot on that now. We've talked a little bit about the tech. Let's talk a little bit about roles. How are SOC roles evolving today?

Lisa Huff: Yeah, I'm starting to see a lot more as I spend time with a lot of different customers in the field. You're starting to see different types of jobs popping up when you go into LinkedIn. There are different types of roles that are starting to come out where you didn't see them before because obviously you have traditional security analysts, and you always have those incident responders, but now you start to see people that are looking specifically for cyber hunters. Those folks are going to proactively hunt and understand the methods used for the attack, and you're also starting to see folks that are triage specialists because, again, when you have a compromise, in many cases senior leadership

wants to understand what's the damage, how many systems and/or user credentials were involved, is it still going on?

Lisa Huff: Having specific resources that are focused on not only just understanding what happened from an attack perspective but also understanding the damage that was done.

Brian Contos: Yeah. How much of do you think business DNA is being injected into that? You mentioned senior leadership and there's attack ABC, and it's hit us. Did we prevent it? Did we detect it? How quickly did we respond to it? How much of an onus of responsibility is putting on security leadership to really tie what's happening in that security world to what's the real impact on the business side in terms of brand and operations and maybe finances, etc.? Is that sort of a maturation of the space you think of the SOC or is that outside of the SOC, and it's at the CISO or Chief Risk Officer or something like that?

Lisa Huff: Oh, no, no. I absolutely think that it's still a huge concern from this aptitude all the way up to the C-suite. Understanding what happened and the damage is one thing, but getting an understanding of how quickly you're going to be able to remediate. That's why I think that when we talk about things that are top of mind, my original answer was more from the aspect of someone who's on the front line or running the SOC team, like a SOC manager. When you talk about the C-suite, their concerns are going to be about automation. How much efficiency do I have in my SOC? We're going to be bubbling up all these metrics, but at the end of the day, how can I mitigate this risk? Yes, that's important, but I also want to have some type of automation in play today so that I have a good level of understanding that if something did happen, at least maybe I've cut it off at the knees before the worst thing that can happen, i.e., exfiltration.

Lisa Huff: I think that a lot of the C-suite are concerned with automation in the direction of their SOC team to move towards entrusting automation.

Brian Contos: Yeah. Now, you hear the term automation thrown around quite a bit, and I absolutely agree it's a big part of it, but you also followed it up with the fact that I need to trust it. I need to validate that if this thing says it's going to do this other thing, I need to know it's actually happening, and I need proof of that. I can't guess. I love this comparison of financial services and security. Your CFO versus your CISO. The CEO says, "Hey, CFO, how much money do we have in our checking account?"

Brian Contos: "I don't know, like a million, two million, fifty thousand something. I don't know." It's kind of how we approach things in security but without basing it on real evidence. Okay, automation without metrics is just kind of this false sense of security that I think makes people a little complacent. "Yeah, we've

automated it." Yeah, but have you automated it [and] is it actually doing what you want? That's the question, right?

Lisa Huff: Exactly. In many cases, if the SOC teams or the security analysts would really focus on those things they already consider to be high fidelity alerts, the things that they already triage and look into every single day, start there. Because, again, it has to be something that's in phases because as we both mentioned you have to be able to trust the automated processes. In many cases, if you start with the things that you know, and in many cases focus on those high fidelity alerts that the teams already trust. Start there and see what some of those results come back to because I think that if you start at that point, I think that the adoption rate will be a lot easier than to try to just push automation on a team that's not really ready to move in that direction.

Brian Contos: Well stated. So, Lisa, as we wrap up here, the final and arguably most important question of this podcast. Who's your favorite superhero or super villain, and why?

Lisa Huff: For sure, Deadpool. The reason being is that my personality, I'm a bit snarky, and in many cases I'm not necessarily the most politically correct person on the planet. I just love the character. The first time that I saw the movie... I didn't get introduced to the character until I saw the movie, and I backtracked and then started reading more about Deadpool and getting more into reading some of the stories behind the character. I'm really obsessed at this point with Deadpool.

Brian Contos: Yeah, it's such a great character. I actually heard something about Deadpool just the other week that in Deadpool 2, there was the character The Vanisher, which is an invisible character. It was actually played by Brad Pitt.

Lisa Huff: No way.

Brian Contos: He's in there, I think they said eight frames of the movie he's actually in there. He did the movie. He was paid with a cup of coffee. Ryan Reynolds bought him a cup of coffee, and that was it.

Lisa Huff: Oh, that's fantastic. You know what? I saw the movie, and you're right. That's absolutely right. It was Brad Pitt, that's funny.

Brian Contos: Yeah, I guess Ryan Reynolds was sitting around, "Hey, what A level celebrity can I get to play a role where you don't even see them in the movie?" That was it. It was Brad Pitt. So awesome. All right. Well, Lisa, thanks so much. It's been great having you on the program, and for all of our listeners, please check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.