ISSUE 72 | MARCH 2023

WWW.TAHAWULTECH.COM

Se ity ADVISOR

DLE EAST

* SPECIAL REPORT: PROTIVITI

* WOMEN IN TECH

BATTLE READY

ROSS BREWER, CHIEF REVENUE OFFICER AT SIMSPACE, TELLS ANITA JOSEPH HOW THE COMPANY HELPS WITH BUSINESSES WITH CONTINUOUS SECURITY IMPROVEMENTS AND DELIVERS QUANTITATIVE AND ACTIONABLE INSIGHTS INTO HOW ORGANISATIONS CAN PROTECT CRITICAL ASSETS AGAINST CYBER THREATS.

tahawultech.com

cnme
computer news middle east
SUPPLEMENT

CONTENTS

BATTLE READY

ROSS BREWER, CHIEF REVENUE OFFICER AT SIMSPACE, TELLS ANITA JOSEPH HOW THE COMPANY HELPS BUSINESSES WITH CONTINUOUS SECURITY IMPROVEMENTS AND DELIVERS QUANTITATIVE AND ACTIONABLE INSIGHTS INTO HOW ORGANISATIONS CAN PROTECT CRITICAL ASSETS AGAINST CYBER THREATS.

Tell us about SimSpace and your business and offerings.

SimSpace comes from our founder, Hutch, who was an F-15 fighter pilot. He then went into the Pentagon and later to one of the three-letter agencies and was asked by General Alexander, who was the 4-star general that set up Cyber Command to build out a training capability for the US Military. He was joined by Lee Rossey, who is our co-founder. Lee was with Lincoln Laboratory as part of MIT. He specialised in building simulation environments. So, they created SimSpace, the platform, which is our Cyber Force Platform, and it is broken down into three offerings. We provide military-grade cyber rangers, elite force training, and live fire exercises. And this is what we built for the US Cyber Command that we are now making available to allied organisations and countries, and critical national infrastructure throughout the region.

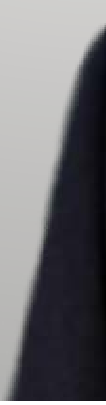
Tell us how you help organisations develop their cybersecurity teams to protect strategic assets and manage risk overall.

We help organisations move from several maturity aspects. If you take financial services as an example, they are looking to move beyond the classic Capture-the-Flag table topics or size to where they want to do live team sort of mission rehearsal, just like the military does.

HUMAN IS OUR BEST LINE OF DEFENCE, BUT IT'S ALSO OUR BIGGEST WEAKNESS.

So, we provide cyber ranges that help organisations, institutions, and critical national infrastructure, do exactly that. Last week, we were in the Gulf region, at a country level working with one of the big four auditors. We were supporting an event they held, which was a national war game exercise for you know for country-level Financial Services Group of the top bank. They were run through a two-day technical exercise and immersive technical exercise using SimSpace and then a business exercise for the executives for the following day. We are looking to sort of repeat this with leading financial services organisations throughout the Gulf now.

So, what we do is help organisations answer several sophisticated complex questions they can answer with



their teams and in their production environment today; they have all these highly skilled individuals, but how do they operate as a team? And how they operate under pressure.

For instance, in one of the biggest banks in the world, last October, we did a 24-hour event where we collapsed three years of attacks into a 24-hour window, and their organisation wanted to see how the shift pattern handover would work. There were three, eight-hour shift patterns within that 24-hour window. And we put the team through its paces. It helps organisations understand the communications, the delegation, the collaboration, that sort of human skills, if you will, on whether they are going to be up to the required sort of strength in time of need, i.e., when there's a serious attack.

Tell us about cyber ranges. How critical is it to an organisation's comprehensive security readiness program? And what are the different cyber ranges delivery models? And how does the simulation work for customers?

Cyber Ranges help organisations answer several questions about the people, processes, and technology that they are struggling to answer in their production environments today. There is testing that goes on to test controls. And I come from a background in that industry segment myself. However, with a range, it creates a sort of a consequence-free, safe environment that organisations can work in, and turn up the heat if you will.

So, in production, if you want to do some red teaming, or some penetration testing, or some activity in production, you might be able to turn the volume up too; but you don't want to break anything, you don't want to break the people and you don't want to create too much noise, that it blinds the security operations center to their normal activities.

So, by using a range, which is separate from production, you can turn the temperature up and test technologies and people and processes to that sort of much higher impact level. The range also has the additional benefit of being able to do all sorts of things within that range and answer all kinds of sophisticated questions for instance, they might be looking to rationalise the number of security controls they have. So how might they overlap? And obviously, a lot of security controls mean complexity. So how can they reduce that complexity, and know that they can swap some of the tools out to reduce the cost of them without losing protection, and without losing the overall effectiveness of their capability? So, there are many use cases for the range and the delivery models can be provided as software – as a hosted solution or can be provided with the hardware.

Now, a lot of the critical national infrastructure work, Ministry of Defence

CYBER RANGES HELP ORGANISATIONS ANSWER SEVERAL QUESTIONS ABOUT THE PEOPLE, PROCESSES, AND TECHNOLOGY THAT THEY ARE STRUGGLING TO ANSWER IN THEIR PRODUCTION ENVIRONMENTS TODAY.

work, and intelligence community work that we do, these organisations want to be in control of the data. And they want to be in control of the assets. So, these are typically close. They're not connected to their production network. They're not connected to the internet. And they're often you know, the old traditional on-prem-approach if you will.

THE GREAT THING ABOUT THE REGION IS THAT MOST OF THE ORGANISATIONS WANT THE BEST AND THEY WANT TO MOVE TO THE HIGHEST LEVEL OF CAPABILITY THAT THEY CAN.

SimSpace recently announced its expansion in the MEA APJ markets. What opportunity do you see in the Middle East market and in which segments specifically?

Well, as I said, in February, I was in the region in Saudi, UAE, and other countries, and we were looking to appoint our distributor in the region. The announcement will come from that in the coming period here. And there's a huge opportunity because if you look at the LEAP conference, as an example, I managed to attend that on the first day. By four o'clock, there was a notification, and as I was leaving to go from the conference to the airport, I saw hundreds of people milling around the doorways and I thought, this is interesting; there must be some dignitaries here and the crowd is here to see the dignitaries. But it turned out that there was a notification to say that they closed the doors because they had too many people at the event at four o'clock on the first day! So, if you look at the amount of activity and volume of cybersecurity work that's going on in the region, especially in the Kingdom of Saudi Arabia, we have a huge opportunity.

The great thing about the region is that most of the organisations want the best and they want to move to the highest level of capability that they can. And that fits nicely with what we're doing around helping organisations sort of move to this sort of continuous security improvement model that we can do by not only providing training for the individuals but training for their teams. These exercises measure and show progression and maturity over time as we continue to do this.

WHAT WE DO IS HELP ORGANISATIONS ANSWER SEVERAL SOPHISTICATED COMPLEX QUESTIONS THEY CAN ANSWER WITH THEIR TEAMS AND IN THEIR PRODUCTION ENVIRONMENT TODAY.

The Middle East cybersecurity market size is projected to grow from USD 20.3 billion in 2022 & to USD 44.7 billion by 2027. So how do you see SimSpace planning to utilise this huge opportunity? And what are your plans for the region, anything that we should look forward to?

Well, we've got a huge history in the region. We've been very successful there with previous organisations and previous teams. And then with that growth, I've always made it very clear to my colleagues around the world that in terms of the Gulf region, it's a little unique, and as much that it's still in sort of infrastructure, sort of creation and infrastructure-build mode; where I would see some of the other countries, maybe in Europe, maybe even in the US, to a certain extent, where it's more in maintenance mode, you know. All the highways were built in the US in the 50s. And they're all there. So, if you're driving a concrete truck, and in the 50s, you were a very wealthy person, and you had a lot of work to do well, whereas you look at cybersecurity in the Gulf, it's at that stage of, it's a huge market already. And it's going to double in size. And it's the sort of a hidden gem, if you will, for cybersecurity companies that understand that and know how to operate through partners and know how to support the market culturally and locally in a way that you need to be successful.

If you can, sort of unlock that lock with the right key, it can be a phenomenally successful market. And so, you know, hiring local teams, knowing the local culture, local talent, is critical. And watch the space as we develop and expand and do all the things that we've done in the past to make the region so successful. And in my previous roles, we've even got to the point where the Gulf region produced as much as 50% of the global revenues for a company, which given the size of the market, that's a huge outcome.

Cyber threats are a constant concern, so how do you prepare for the future? As far as threats, which may not be existent now, what are the unique threat trends or trends specific to this region that you intend to focus on? And how do you ensure that the talent acquired for the same remains versatile and equipped to face new challenges?

I think that's an important question and AI is going to be a huge factor in what's going on. And we've heard a lot about chatGPT, or whatever AI technology you want to talk about. I think there are some risks around that, that people may be getting a little bit lazy and programming and using these kinds of tools to provide code for them.

Potentially, there's a MEL training aspect to those technologies where you could create a world where you sort of MEL-train the AI so that it's producing code that's got embedded vulnerabilities in it. There's a risk there these technologies are not designed to check the code. They're just designed to produce what they've heard about and what they think they've been told is good, right?

So, I think AI quantum computing is going to make a big difference, but that's not going to be in the short term that's going to be in the medium term, but people need to think about that because that's going to have a big impact on the algorithms. And that's going to fundamentally change all the security. I'm not sure that's in the next one to three years, it's probably more than the three-to-five-year range.

But I think AI in the next one to three years, can bring in what I call the Wuhan of cybersecurity. Before you know it, you've got the snowball effect of slowing down the internet and chewing up a whole lot of resources, because this thing gets out of control. And, as you know, is propagating around the internet. But I think we need to come back to just the reality here, of the big digital hygiene problem in the industry. And people need to focus on the basics.

AI QUANTUM COMPUTING WILL MAKE A BIG DIFFERENCE.

This is making sure that the teams are trained on the technologies that they have. If you look at the data breach investigation report of Verizon, two years ago, they said that 85% of breaches stemmed from a human failure. So, human is our best line of defence, but it's also our biggest weakness. So, I think the shift must happen, where we put increasingly more effort into our resources, training them as individuals, training them as teams, testing them under pressure, identifying their weaknesses, and then filling those weaknesses with people processes or additional training.