ceocfointerviews.com

Issue: May 24, 2021

Tego Cyber Inc. – Using Threat Intelligence to Simplify Cybersecurity

Shannon Wilkinson
CEO

Tego Cyber Inc.
(OTCQB:TGCB)
www.tegocyber.com

Contact:
Tego Cyber Inc.
info@tegocyber.com
https://www.linkedin.com/company/tegocyber
https://twitter.com/tegocyber
https://www.facebook.com/tegocyber

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Ms. Wilkinson, what is the overall vision behind Tego Cyber?***
Ms. Wilkinson: Tego Cyber is a threat intelligence company which is a cybersecurity company. What we are doing is taking in all the data that is found there out there on the internet, out in the dark web, like bad IP addresses. We bring all that information into our platform and compile and analyze it and then we add additional context to it, so not just the basic information of the IP addresses. Then we are adding the information about certain IP addresses being associated with certain threat actors and their locations, and the type of activities they are known to do.

"In a world where we have so many disparate cybersecurity tools and services and solutions, I think it is vitally important that the tools work together and we try to simplify cybersecurity." Shannon Wilkinson

Our platform integrates into other cybersecurity tools, such as SIEM platforms which are log aggregation and data warehousing solutions typically used by security operations teams because all the information about an enterprise is found there but we layer our solution on top of that platform so that they have the threat intelligence integrated so that if an incident occurs and something pops up as bad, they have basically all the information at their fingertips that they need to know to make an important decision and how to respond.

CEOCFO: ***What are the challenges in getting all the in-depth data you have and how is it automated? How do you keep up with constant changes?***

Ms. Wilkinson: The challenge for security operations teams is that the threats are constantly evolving, IP addresses are constantly changing, so having relevant timely data is essential for a security operations team when they are responding to incidents. That is one of the challenges that we are looking to change with Tego by providing timely, relevant data integrated into existing cybersecurity tools, so that security operations teams do not have to spend time going out looking for information on the internet or dark web or wherever they would find information at their fingertips once an incident occurs. They can immediately see the information presented within the tools that they are using already. It is a little like the idea of using a single pane of glass but we are not asking all of our customers to use Tego's glass, we are asking them to use the tools they have already invested in.

CEOCFO: ***How important is that?***
Ms. Wilkinson: In a world where we have so many disparate cybersecurity tools and services and solutions, I think it is vitally important that the tools work together and we try to simplify cybersecurity. Cybersecurity has gotten very complicated with layers upon layers of protections that do not work with each other, do not play nicely with each other.

Overall, as an industry we need to think about changing that because it is in everybody's benefit that their enterprise is protected, protecting data, not just for the organization but for all the private individuals and consumers that do business with enterprises. It is not just the business's information that can be compromised, it is all the customers of the business and anybody that the business has data on.

CEOCFO: ***Is the industry ready for a solution like Tego or is there still a lot of noise and confusion?***
Ms. Wilkinson: Threat intelligence as a segment within cybersecurity is still very much an emerging technology. We are one of the few companies that are offering this kind of solution out there. I think now because of the evolving nature that threats evolve, it is definitely needed and it is becoming an integral part of enterprise cybersecurity strategy to have cyber intelligence.

CEOCFO: ***How are you reaching out?***
Ms. Wilkinson: We are doing a lot through customer advocacy. Cybersecurity I think is still very relationship based where CISOs (Chief Information Security Officers) who need some sort of solution will go to a friend or another CISO in the industry and say they are looking for intelligence, and ask who they are using. We are relying on that type of referral.

Our first integration of our threat platform is with the Splunk SIEM, and they have something much like the iTune store for your phone. They have something called Splunkbase, which is an app marketplace for add-ons that have been developed for their platform. They specialize in what they do which is log aggregation and data warehousing, so they encourage developers to build applications that compliment and give return on investment on their platform.

CEOCFO: ***What is involved in an implementation?***
Ms. Wilkinson: We have tried to make it as simple as possible. There is the Splunkbase which is the app marketplace for Splunk, our first integration. We do have plans to integrate to about nine or ten other platforms in the next coming years. With Splunk, what a customer would do is either know the name Tego Cyber or they would search for threat intelligence within Splunkbase. Our app would pop-up and just like you would install apps for your telephone you just click install within Splunkbase. It would then install and you would get a license key from Tego. Then they would plug-in that license key and their platform would start ingesting our threat data.

CEOCFO: ***Do the people using Tego define the parameters of what they want to know or do they have choices on the threats they wish to enquire about? What happens when you detect a threat?***
Ms. Wilkinson: We have created dashboards within our Splunk application that show detected threats for the enterprise. Let's say there are five computers within their enterprise talking to a certain bad IP address, we would say, "Hey we have identified this threat within your environment, you should go take a look based." The notification would be based on the severity of the threat and some other information about what kind of attacks that are happening. Within Splunk the customer is able to build their own dashboards but we provide some ready-made dashboards regarding threat intelligence and what we are detecting within the customer environment within our app.

CEOCFO: ***Who makes the decision on what to do next?***
Ms. Wilkinson: That would be up to the security operations team. What we are trying to do is give them the information that they need to make a quick and informed decision. How the enterprise responds is really up to them.

CEOCFO: ***What has changed in your approach over time and what have you learned as you have grown your customer base, either from your end or customer feedback?***
Ms. Wilkinson: We pride ourselves in listening to our customers and having them explain to us some of the features that they would like to see in the future, and of course if there are any shortcomings in our features that they would like to see us improve on. We welcome all of that feedback because if there is one thing I have learned in my experience in being a software developer and architecting solutions is that developers making decisions on what they think the customer needs, often leads to failure because developers do not understand the intricacies of the business. That is one of the reasons why we pride ourselves and make sure that we listen to our customers. We call it the Chick-fil-A style of customer service where the customer is king and we need to make the customer feel like they are valued and also take in their feedback.

One of the differentiators for Tego is that we pride ourselves in listening to our customers and we greatly value the feedback of our customers. As we have been going through the beta testing portion of our platform with customers, we have been doing walk-throughs and gaining

feedback from them such as "this is great but it would be better if…" type of scenarios. We have been taking that kind of feedback into account throughout our feedback cycle.

CEOCFO: ***What surprised you through the process of getting to where you are today?***
Ms. Wilkinson: One of the things that surprised me a little bit is that somebody has not done this already. We know how incidents can affect enterprises, so the fact that there was not really a threat intelligence solution that was out there delivering all the information that a security operations team needs in a very quick manner was surprising. They would have to go out to an external website and login to get information they needed and some providers were just saying that the IP address is bad and they are not giving any more information to the customers.

That surprised me because of just the value of information that can be presented to the enterprise is vital. It surprised me that nobody was really doing what Tego is doing right now. We easily have the information available to us that we have been able to automate through our platforms.

CEOCFO: ***COVID has affected just about everyone and every organization. There have been more security threats as companies were often not ready for remote working, but on the other hand, so many other fires to put out and not a lot of companies want to get involved in something new, like adding more security during a crisis. Where does Tego come in and how has this affected you?***
Ms. Wilkinson: Unfortunately for security operations teams, the pandemic has not slowed down or lessened the load in the work that they face on a daily basis, in fact it has increased. I believe the statistics from the FBI is that there is a 300% increase in cyberattacks during the pandemic. The security operations teams in addition to now contending with a remote workforce there is an increased level of attacks. Now is an ideal time for enterprises because they are facing so many threats and they do have to pivot so quickly from incident to incident. It is a perfect time to work with Tego and our solutions.

We have had a lot of excitement about our platform, so I do not think the pandemic has really affected us in a negative way. As a corporation we have felt some of the effects of COVID. I myself was knocked out for about a week in January when I contracted COVID. Some of our software developers also either had family members or they themselves contracted COVID. It has definitely had some impact on the corporation of just people being out for a week or so to care for their families or to get better themselves. There have been little impacts here and there for Tego.

CEOCFO: ***Tego Cyber is a public company. What has been the response from the investment community and are you seeking funding, investment, or partnerships right now?***
Ms. Wilkinson: We are a public company and we actually founded Tego to go public from the very start using our IPO and S1 process to help raise money through friends and family primarily, to fund the

research and development. We have run the organization about as lean and mean as we could through development.

We are now looking for investment partners, so we would like to uplift to a more senior exchange probably in the fall this year. We are looking for somebody not necessarily just to give us money but truly be a partner to help Tego through that process. We have an S1 offering that we have extended through the beginning of August. We will be filing a subsequent S1 after that expires.

CEOCFO: ***Your website features articles about the gender diversity gap in cybersecurity, about STEM (Science, Technology, Engineering and Mathematics) education for women. What is your take on women in cyber and what are you doing personally in this area?***

Ms. Wilkinson: I am a huge proponent of encouraging women not only in cybersecurity but technology because we still makeup a minority in the industry. A couple years ago women were only making up about 11% of cybersecurity professionals and now the number is more around 20%. When you get into the executive levels such as CEO and executive leadership the numbers drop back down because while we have more women a lot of them are down in the entry-level SOC analyst type junior cybersecurity positions. It would be great to uplift more women to the leadership. Personally, being an advocate, I go to career days locally. I wrote a book called "Ripping off the Hoodie: Encouraging the Next Generation of STEM Girls." It deals with not only with what women face in our careers like discrimination and harassment, but all the factors that lead up to less women in cybersecurity starting at a young age.

We push girls to go play with Barbies and dolls and go play house, whereas for boys we tell them to pretend to be an astronaut and be a doctor and be interested in technology and video games. We push girls into what I would say are societal norms of Susie Homemaker and that stereotypical thing. However, when we get into middle-school, we find that girls and young women are looking at technology and STEM careers less and less and going more towards other career paths and that is having an impact when they go to college and enter the workforce. I am just trying to bring awareness. I talk at a lot of conferences about being a woman in a male-dominated industry and what that means. I have to say through my experiences and my career, I have been fortunate in not experiencing any harassment and very little discrimination just because I have had the opportunity to work with really fantastic people, but I know that there is that problem out there that discourages women from looking at cybersecurity.

CEOCFO: ***It seems hard to believe that it is like that today; do you find that it is still prevalent but maybe more under the surface?***

Ms. Wilkinson: It is still under the surface. I am actually the mother of three girls who are very into technology and video games. As a parent I had difficulty buying clothing that matches my daughter's interest. When they were young and very into technology, we would go to the store and everything for little girls was pink princesses or something like drama queen and all those catchy little slogans, where it is almost trying to

sexualize 7-year-olds. It has been upsetting to my daughters. They love Minecraft and I would have to go into the boys section to buy them a T-shirt that had Minecraft on it. It is 2021 but still it is like they do not make things that encourage those kinds of activities for girls. I still have to go to the boys clothing section to buy them clothes. For toys it is still very much the girls with Barbies and the boys with dinosaurs and astronauts.

CEOCFO: ***With so many companies to look at in cyber, why pay attention to Tego Cyber?***

Ms. Wilkinson: We are in the threat intelligence market of cybersecurity which is the emerging segment and there are not a lot of players in that segment. It is also one of the fastest growing segments within cybersecurity and growing and twice the rate of the overall cybersecurity market. The Threat Intelligence segment itself is estimated at somewhere around $5.1 billion annually and growing at a rate of 20% per year. It is definitely a great market segment. Some of the things that also make us unique are just basically the highly scalable nature of our platform and as we add more customers, it does not exponentially increase our cost to the organization to add more staff for add servers and a bunch of equipment. We built platform with scale in mind.

The third thing that sets Tego apart is our world-class management team. We have myself who comes from a background with United Nations, doing software development, leading software development teams. My husband Troy Wilkinson, a former law enforcement officer and a cybersecurity rock star in his own right is currently the global head of cybersecurity operations for a Fortune 300, so he is in cybersecurity security operations on a day-to-day basis and provides a great deal of feedback about our solution. We also have Michael De Valera, he is a 20-year technologist in New York and comes with a great deal of knowledge about technology and platforms. Lastly, we have Chris White, he was a former technologist with the US Air Force and he worked for General Dynamics and built the managed cybersecurity practice for EY. Now he is the deputy CISO for Fortune 300 an advertising and media agencies. Chris also brings a tremendous amount of security knowledge and experience to our management team. Just that combination of people, our skills and experience in the industry as well as our relationships that we have developed really make a difference, in addition to the technology.