ceocfointerviews.com

Issue: August 15, 2022

AgileBlue-Helping Organizations Detect Cyber Threats Before a Breach Occurs

Tony Pietrocola
President

AgileBlue
Advanced Cybersecurity | AgileBlue

Contact:
Gillian Sweny
814-490-5964
gsweny@agileblue.com

Follow us on:

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Pietrocola, what is the overall concept behind AgileBlue?***
Mr. Pietrocola: AgileBlue is a Security Operations Center-as-a-Service. What that means is we detect potential cyber threats for our customers 24/7 before they are actually breached.

CEOCFO: ***At a fundamental level, what do you understand at AgileBlue about how to detect potential threats?***
Mr. Pietrocola: I think there are lots of answers. The one thing we do really well is we are able to detect anomalous activity. It is not just rules or trends or potential patterns. It is really understanding how people, devices, networks, and the cloud is worked on a normal basis and identifying those anomalous trends that tell us that something probably is not working correctly.

If you can get out in front of those, if you can get there before they do, you have a chance to either stop it or at least mitigate the risk, and that is the key in cybersecurity. Can you stop everything? I think history has shown absolutely not. Can you mitigate your risk? Absolutely.

CEOFO: ***Would you give us an example of what you might be able to detect and why you are able to detect it or what you are able to understand when seeing a particular pattern to indicate a potential problem?***
Mr. Pietrocola: I think when you think about things like multiple users logging-in at the same time and what happens to be a geographic area not realistic to where the other person is, that is probably a good sense. The wrong people accessing the wrong data or attempting to access the wrong types of data, that anomalous activity, a regular server or work station, a person doing things that they do not normally do, or more tactics and techniques that hackers use that are more avert like brute force or credential stuffing. We use a very unique algorithm in our machine learning that helps identify those things.

There are literally hundreds of those things. It is those types of things that we are looking for. There are things called indicators of an attack that tell us something could go wrong, not just when somebody has been attacked.

CEOCFO: ***Do you have several different solutions; does a company help set guidelines or information about how they operate so that you can provide the best solution? What is a typical engagement for AgileBlue?***
Mr. Pietrocola: We are working with that midmarket client, so they have an IT team, they probably do not have the most experienced cyber team. Those two things are very different, just because you know IT does not mean you know cyber. They are very different and nuanced. We have a very specific process and technology, so our technology is built for that. It is built to be their outsourced Security Operations Center.

We have not only the technology, which I mentioned, SOC and the XDR technology, we have a 24/7 team, cyber analysts, that are not only looking for alerts but they are also hunting for threats within our customers' ecosystems. All those people are here in the USA. We run them all from the Ohio, and that is the product and service we are able to bring to our clients to give them that cybersecurity team that most likely they do not have.

CEOCFO: ***Are companies appreciative of USA customer service these days?***
Mr. Pietrocola: I think so. I think at the end of the day people know they can probably get good service from other areas as well. We have customers all over the world. I think people do look at the United States as having very deep experience, as well as, a very solid skill set. I think when you add those together, people do appreciate doing business with US resources.

"I think you will choose AgileBlue because it is a company that literally detects cyber threats before our you are breached. If somebody wants to put together a program and bring in a trusted advisor, not even the technology but also the people, we are going to help our customers stay ahead of the hackers and that is going to give them the ability to sleep better at night, knowing we are there 24/7 to help protect and monitor their most critical digital networks." Tony Pietrocola

I understand there is a cost to it, you are going to pay more. However, there are ways to work on the expense side of things where you can still have tremendous people who use a lot of technology in terms of automation to help reduce some of those costs.

CEOCFO: ***Do you work directly with your end-customer or through resellers? What is the business model?***
Mr. Pietrocola: A little bit of both. We have a direct business that we do go directly into customers who have higher regulatory frameworks that they need to understand, but we also have a tremendous partner program. We are in the United States, we do not have office or sales reps in South America or the Middle East or Canada but we do have partners in those geographic regions that are trusted tech advisors to their clients. Even that trusted tech advisor does not have the security platform of skill set needed, so they partner with us to bring that to their customers.

CEOCFO: ***When you are bringing somebody onboard, how do you know they have that extra level of skill in security threat detection?***
Mr. Pietrocola: It is hard. Any time you interview people they are going to tell you all the great things, so you have to do a few things. You have to put them through some paces, you have to have engineers ask engineering questions and not just the recruiting or HR side of things. You have to be able to give them a little quiz and bring them along slowly and make sure they understand.

There is a practical application to seeing them do their work, and how they are able to work with in both environments, which are cyber skills and customer skills. We need to work with our customers' hand-in-hand. At the end of the day, we are literally an offshoot and a compliment to their team, so we are part of their team.

CEOCFO: ***Would you tell us about the acquisition of Crowe LLP's MDR Platform, and are acquisitions part of the growth pattern?***
Mr. Pietrocola: They are typical in our industry. When it comes to AgileBlue, this is the first acquisition we have done. We are not walking the ends of the earth to look for every acquisition possible. If something it is something that looks like

a one plus one equals three, we are going to look at it. This was brought to us and we looked at it and when you look at the common technology backbone, smart solid people and excellent organization that they are coming out of and a client base that was in regions where we are not only physically located, but also have a lot of customer concentration, this was a really good opportunity for us. When you think about a good acquisition, there is always going to be a valuation component to it.

There is talent you want to acquire and of course there is the revenue and customers you want to acquire, but if it is built on that common tech backbone and we can make a very quick migration for our customers where they do not have to do a lot of work, and be migrated into our platform, that is a huge win-win and one we know we will mitigate our risk of that transaction. We are thrilled about Crowe LLP selling us their MDR business. We are excited and it just happened over the last week and a half. We are working hard now to migrate.

CEOCFO: ***How do you reach out to potential customers and how do you stand out from the crowd?***
Mr. Pietrocola: We are pretty aggressive. We have a great sales team and a tremendous marketing team led By Gillian Sweny who is doing everything she can to make sure AgileBlue is at the tip of the tongue when CIOs are looking for what we do through Google or programmatic marketing and all these great things. We are pretty aggressive. We host lots of webinars and thought-leadership pieces on what we do because people want consume content, so we try to write a lot of content.

CEOCFO: ***How do customers find you?***
Mr. Pietrocola: A lot of customers still look at word-of-mouth and talk to people they know in the industry. I do think when they see an ad or something that catches their eye on LinkedIn or Google or some other site that they come from, if it catches their eye, they visit the website and see that these people know what they are talking about, they will engage in a call or at least a demo. Do they all buy? Of course they do not all buy, but the point is we love showing our technology because we know the wheels are spinning for our potential customers and more often than not we are able to get that customer and bring them onboard.

CEOCFO: ***When you start an engagement what do you need to look at and how do you integrate with a company; what is involved?***
Mr. Pietrocola: It is a simple process. Whatever their digital infrastructure looks like, their servers, their networks, their end-points and their cloud, we do a complete digital inventory of everything. We are then able to install our technology, agents to the endpoints, things called APIs that collect data from the cloud and other resources that the client was using. It is generally a couple-day install that our team does jointly with the customer. The key is to start streaming that data back so that we can build those benchmarks.

Our customers are live within two to three weeks. I mean fully live, and by the way, we are not asking them to do much. We are asking them to so some joint things with us to give us approvals, we are doing the testing and then we are live. It is a very streamlined process. If you think about it, people have been burned in IT in cyber with lengthy installs that just never end. We get our customers done extremely quickly.

CEOCFO: ***What have you learned over time and what has changed in your approach either from new technology, new threats, or perhaps from customer feedback?***
Mr. Pietrocola: Cyber changes quick, so we are constantly adding new things to our algorithms and machine-learning models for our clients. That is just from being in the industry. We also subscribe to lots of third-party threat intelligence, so we are seeing what the world is seeing, and we are able to move fast.

We also have an advisory board made up of clients and partners that we meet with quarterly, and nobody knows better than the client because it is them that has to make sure their business is secure. We meet with our clients all the time, monthly with client meetings, advisory boards quarterly, to just get feedback and help us craft our rolling 12-month roadmap.

Our clients have great ideas and we bring great ideas to the table ourselves. We are supposed to be the security experts too so you match those things together and we have a roadmap that is growing and a roadmap that is literally putting us out in the forefront of where we need to be with our technology.

CEOCFO: ***What if anything might a potential customer miss when they first look at AgileBlue, which they should understand?***
Mr. Pietrocola: It is hard to stop cybersecurity threats and hackers. If they are determined, all the odds favor, we are in a defensive position and we are going to help our customers play defense, but AgileBlue adds a little bit of offense to the equation, things like auto response, proactive threat hunting, combined correlated third-party threat intelligence. Us bringing that to the table also helps us become a little bit offensive for our customers, not only potentially stop but at least mitigate these threats and that is a big key when a customers is thinking through these things.

CEOCFO: ***With so many companies in your industry, why choose AgileBlue?***
Mr. Pietrocola: I think you will choose AgileBlue because it is a company that literally detects cyber threats before our you are breached. If somebody wants to put together a program and bring in a trusted advisor, not even the technology but also the people, we are going to help our customers stay ahead of the hackers and that is going to give them the ability to sleep better at night, knowing we are there 24/7 to help protect and monitor their most critical digital networks.