ceocfointerviews.com
© All rights reserved
Issue: May 7, 2018

CEOCFO Magazine

Managed Security Provider onShore Security is using a Panoptic Approach to revolutionize Cyberdefence, Governance, Risk and Compliance

Stel Valavanis
CEO

onShore Security
www.onShore.com

Contact:
Stelios Valavanis
312-850-5200
info@onShore.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Valavanis, according to the onShore Security website, your mission is to protect the freedom of information by revolutionizing cyber defense and governance. How are you doing that?***
Mr. Valavanis: We have been developing our own security detection and event management platform since about 2004. We have been doing cyber security since 1998 or 1999. In 2004, we started building a tool set that we continue to develop today and our approach is what stands out in the industry and that is the panoptic approach as we call it, which is about seeing as many different points on the network and lots and lots of disparate data. Most of our competition just looks at the edge, just look at network traffic going through a firewall. We take a much more holistic approach. We are not alone but it is definitely at the cutting-edge of the industry and that is what we mean when we say we are revolutionizing it. This is an ongoing effort so tomorrow what revolutionizing means is different from what it means today and different from what it meant yesterday.

CEOCFO: ***It makes perfect sense to me that you would want to look at it holistically. Why is that not a standard approach, is it hard to do?***
Mr. Valavanis: It is hard to do. Part of the forces to blame are market forces but there is some industry forces on the investment side. The investment community has traditionally been mostly interested in product, for intellectual property that they can own and capitalize on. The IT buyers both on the enterprise side and the small businesses have preferred to spend on product rather than on services. You get more and more of "here is a tool that does this or does that or does a piece of it or automates," especially automates. They like that. IT departments feel threatened and they definitely feel like they would rather buy a tool that automates and there is a lot of pressure for them not to hire. If they bring in a service provider, they feel like that is stepping on their toes. Security is a process, not a product and people are just beginning to understand this. It is an ongoing effort rather than a box you put in and forget about. Most people out there are not even looking at their firewall logs let alone any kind of advanced data like intrusion data. One other important aspect of the forces that limit this holistic approach or that resistant holistic approach, are that the commercial world is more of a late entrant into the cyber security world. The commercial world likes to be monopolistic, they like to be full-stack, they like to say that their solution is everything you need and there are no openings for competitors. As a result, they have been less inter-operable than the free and open-source world. The cyber security tools and methods today come from the internet world which is an open-source world. That is our background. Our background is internet service providers and open-source developers. You bring those two together and you get to our approach today which is about visibility. When you are running an internet service provider company, you are managing a very large network and you are managing a network that you do not have control over because they are all your clients in there and you cannot tell them to block things or do this or do that or follow some policy or procedures. You get good at watching, good at monitoring. Along with

all of our peers in the internet service provider world and the open-source world, we started developing tools not only that give you that visibility, with the panoptic approach, but we also since this is mostly open-source and non-commercial software we developed on, we made it inter-operable and continue to do so. You can create full-stack this way and fill in the gaps without hindrance. Now the commercial world is starting to catch up on that but if you take note of the open offerings in the commercial world, notably the two most popular SIEMs (Security Incident and Event Manager). The two most popular ones which are Splunk and AlientVault both started from open-source projects and their key to success is that they are very open unlike most in the commercial world. There are forces that have opposed this panoptic approach in that commercial software tends to be less inter-operable, they are coming more from a server and host model rather than a network model and they have traditionally been closed. People like us that have foundations in open-source software and on the network with ISPs, we have been understanding this for a long time and we have been building our own tool sets for a while. The fact that onShore applies it to an enterprise is narrower. There are fewer people doing that but we have been doing it since 2004 when we started building this platform.

CEOCFO: ***Would you tell us about the range of services?***
Mr. Valavanis: There are two core services. One is a managed security service that has four components. It has a detection component, it has a security and event management component, it has a firewall management component. Then it has an analysis component which is the security operations centerpiece with monthly or weekly security briefings. Together they create what we call Panoptic Cyberdefense. The other offering is what we call Cybersecurity Leadership which is a governance, risk and compliance program that we put clients through. It is typically sold on a flat-fee monthly basis but we walk people through a security maturity program to develop improvements in the cyber security process and controls including developing policy sets. We have tools to map different kinds of security policy sets and risk management policy sets.

"The vast majority of people out there are still in a box, plugging it in, maybe putting some thought into getting something configured well like a firewall, and then walking away. This is true in the mid-market and this is true even in some enterprises."- Stel Valavanis

CEOCFO: ***Who is using your services today?***
Mr. Valavanis: For the most part it is a mid-market offering. Let's say starting at five or six-hundred users up to several thousand. That is the core and our main client base, which are some mid-sized banks. Now we do have one enterprise client so we have some enterprise business as well, one large bank in particular. We are our clients' security operations centers.

CEOCFO: ***How do you reach out to new customers and how would someone find onShore Security?***
Mr. Valavanis: Other than searching for the services or kind of providers, we market a lot with the Illinois Bankers Association. We are very visible in that community. We just starting gaining some visibility in the construction space because we have a large client there and there was a convention we were invited to and there is some interest there. We do have some health care business too; we were just recently present at the HIMSS conference. We hope to gain more visibility in the security information sharing organizations where we have only been participants but not sponsors. We do sponsor local security events in Chicago with the ISSA and the ISACA. Those are probably the two most prominent security professional organizations nationally.

CEOCFO: ***Is business ready for a new approach?***
Mr. Valavanis: I think we are a little ahead of it. The vast majority of people out there are still in a box, plugging it in, maybe putting some thought into getting something configured well like a firewall, and then walking away. This is true in the mid-market and this is true even in some enterprises. At the enterprise level, there is definitely a lot more advanced work being done. The mid-market is still way behind and I think it is poised for an absolute explosion though it is going to take more events to happen, big public and scary events I hate to say. Then it is also going to take increased external pressure and we are already seeing this in the banking space with regulations in particular like the New York Department of Financial Services regulations that just start getting enacted this month. I think there is going to be a lot more pressure from insurance companies because they are way behind in the maturity of their cyber liability policies. More and more they are starting to ask questions and ask for validation on requirements. It is one thing to ask somebody "do you have intruder detection on your network," and they will say "yes they do," versus asking "is somebody looking at the data from their intrusion detection and analyzing that on an ongoing basis." They are starting to get wiser in asking the right things. Again, the two things are events, breaches and what-not, and the other is external pressures from regulatory bodies, industry associations, and insurance companies. Maybe one company is regulated and they push on their own vendors to

follow the same regulation. That is happening with the Department of Defense, NIST-171 requirement. They told their vendors that they had to have a NIST-171 security policy network mapped out. Then those vendors would go to their supplier vendors and say I am not NIST-171 unless you are.

CEOCFO: ***Would you give us an example of what onShore Security would pick up or does pick up because of your approach?***
Mr. Valavanis: There are three things that we are detecting. One is threats, two is anomalies, three is that we are detecting for compliance. Now the majority of the industries such as service providers as well as the tool they use completely ignore compliance detection. That is really notable because compliance is something you can demonstrate whereas I cannot prove a negative and I cannot say you have not been hacked and nobody owns yours systems and there is no threat actor inside your network. I cannot really prove that and the truth of the matter is it is probably not the case. The majority of networks out there are probably compromised and they are probably not aware that is the case. It is to the point where it is almost unlikely that your network is not compromised and I am talking about companies big and small. A good example is Sony, where the threat actor was acting for four months inside their network before it was detected. The first kind of thing that is notable is that people are not necessarily attuned to looking for compliance and compliance matters in a lot of ways because compliance is enforcing behavior that you trust and can prove that a network is compliant in some way and measure to what degree they are. We have seen that many work stations are pushing out traffic in violation, even if we are blocking it we want to measure it and say that is something they should not be doing according to our rules. Compliance is not only about regulation; compliance is about the rule sets they put in place and the data to prove enforcement. The second thing is anomaly detection, there are definitely people doing anomaly detection but one of the problems with anomaly detection is that even with machine learning it is difficult to get value out of it without human beings and that is definitely more time consuming. We have focused our development efforts on empowering our analysts with tools rather than just purely trying to automate. When we automate, we automate in some way to empower the analyst to correlate some disparate set of data. We use tools such as Elastic Search and Kibana, which are very advanced tools for creating complex searches and rules. Our analysts, when they see something that does not look quite right, can create a more complex rule to mine for that kind of data elsewhere in the network. This also brings to mind another very significant difference between our detection systems and most of what is deployed out there. Most systems especially the ones that are at the edge only, do not store packet captures. What we do is store packet captures as a buffer, which is typically tuned to be about a day's work of a network data. As a result, when our analysts are looking for any kind of anomalies, they can track a session back in time in about a day and the analysts are doing this around the clock so they typically do not have to go further. Anytime anything that does not look right and that they want to even note for informational purposes, they set a flag that automatically locks that whole session of data and packet captures across the network and saves those packet captures for 12 months, back in our data center along with even un-tagged logs and other meta-data. We burn disks for clients that want a longer archival time for a fee and we may be the only ones in the business doing this for clients. Threat detection is a lot more established and a lot of people are doing threat detection and it is typically signature and rule-based sets that we share with a wide set of community peers. We are very similar in the industry with threat detection and very strong in anomaly detection because we focus on empowering the analyst rather than automation. We buffer, tag and store full packet captures. The third piece is compliance detection. We are just unusual there and most people are not interested in compliance detection but rather in regular vulnerability scans which don't capture behavior.

CEOCFO: ***Why choose onShore Security?***
Mr. Valavanis: We are the best. We have been doing this longer than most of our competitors have even been in business. We have cut our teeth in the complex ISP world and in software development which we turned back towards the enterprise. We are one of the most mature companies out there doing this kind of work. We understand the tool set better than anybody. We are continuously developing our own tool set. We primarily work with banks and therefore have high-level experience. We understand the regulatory space very well. While the rest of the world out there is catching up on what they should or should not do, we are already know how to work within the regulatory framework and even have a program specifically that addresses the security maturity through the heavy work of developing policy sets and complying with regulation. We are just simply among the most mature and developed and advanced companies in cyber security in the country.