ceocfointerviews.com

Issue: September 8, 2014
The Most Powerful Name in Corporate News

Products that Accelerate Cyber Security Incident Response

Scott Hartz, *CEO*

"The world of cyber defense is about to undergo a paradigm shift from perimeter defenses that rely on threat information that is in constant flux, to a behavior based risk intelligence that is resilient to evasion. TaaSera is at the forefront of the technology that will revolutionize the IT infection detection and response process."
- Scott Hartz

TaaSera Inc
1751 Pinnacle Drive
Suite 600
McClean, VA 22102
855-822-7372
www.taasera.com

About TaaSera, Inc:
TaaSera is revolutionizing cyber security incident response by helping identify, resolve and restore business operations more quickly. TaaSera's patent-protected NetTrust solution allows IT security professionals worldwide to gain invaluable minutes when responding to coordinated attacks and infections.

Unlike traditional security tools that require highly trained professionals to analyze millions of events to identify a potential breach, NetTrust instantly "connects the dots" to visualize which systems may already be compromised, and to prioritize them by risk. With NetTrust, for the first time incident response teams know where to focus their efforts, and how urgently they need to act.

TaaSera has offices in Cupertino, California and McLean, VA.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

CEOCFO: ***Mr. Hartz, what is the concept of TaaSera?***
Mr. Hartz: TaaSera NetTrust is a suite of products used to accelerate cyber security incident response. Unlike tools that focus on individual events or intrusions, NetTrust watches for patterns of malicious behavior in systems and prioritizes them according to their risk to assist security analysts resulting in a more timely, targeted response.

CEOCFO: ***What do you understand fundamentally about this area that perhaps other companies do not?***
Mr. Hartz: I think in the existing paradigm, virtually all of the products in this arena rely on what we call perimeter defense. The concept being

that if we protect the edge (or perimeter) of the enterprise and keep malware out, then by definition, everything inside will be great, which is a good concept. Unfortunately, it is not working very well as the recent attacks would attest. The adversaries are smart enough to penetrate the perimeter defenses and no one is really watching what is going on inside the system, and that is where we come in. We monitor traffic inside the enterprise system, looking for malicious activities that have gotten through the perimeter. We identify the breach and help target the security team to where they need respond.

CEOCFO: ***How are you able to do that?***
Mr. Hartz: Our product is based on years of research at SRI International (formerly Stanford Research Institute). Most solutions on the market today depend on well-known signatures, file hashes, and published blacklists to identify the malware in flight or at rest. So, they block input based on a static pattern match, and not based on dynamic behavior recognition that does not rely on information that is in constant flux. These other products depend on a blacklist of "bad" IP signatures harvested daily from multiple sources with limited or no attribution. The blacklist is in the order of hundreds of millions of signatures, and they are always out of date because of constant IP and domain flux, and evasion techniques used by cyber criminals. Therefore, such approaches will not scale and identify an emerging and well-orchestrated first time attack. Rather than using such run of the mill approaches, what the SRI team figured out was that when they looked at behaviors of malware inside a network, they found that all malware exhibit a common set of behaviors. They found that combinations of those behaviors inside a network can be used to identify malware that evaded other detection systems. That was break through patented research. We are adding our own innovations, to this behavior analysis technology, some of which are also patented or patent pending.

CEOCFO: ***What would be one or two of the behaviors?***
Mr. Hartz: Think about when you get something suspicious on an email coming in and you click on it. The resulting first step is generally an egg download. That is one behavior. A second would be that the malware comes alive and starts sniffing around your network to see where it is. The third would be that it communicates out with its command and control server to get further instructions and further code to tell it what to do. That is a sequence of three behaviors.

CEOCFO: ***What are you are providing to an organization that will enable preventive detection?***
Mr. Hartz: We are continually monitoring traffic, looking for this combination of behaviors and then flagging them. We are keeping an ongoing track of suspicious activity and building up a case as we see one behavior, two behaviors, three behaviors, four behaviors and the case gets stronger. As it gets stronger, it bubbles up on a reporting and alerts dashboard and our system highlights to the customer that this is a rising concern. Maybe another way to describe it is we operate in a post intrusion mode when the malware is already inside, but pre-breach -- before they have actually grabbed your key data and sent it back out. We are operating at a different timeframe, not before it has gotten in but after it has gotten in and before it has done harm.

CEOCFO: ***What is involved in implementation?***
Mr. Hartz: That is somewhat amazing. We implemented one of our clients yesterday and it took about an hour. We have it loaded on a small device. It is a software tool we are supplying, but in many cases, we are loading it on a small appliance as a plug-and-play set up, which is easy to deploy and quickly shows results.

CEOCFO: ***When a potential problem is identified so that you can look at it, are you doing that at your end and is the customer being notified where?***
Mr. Hartz: No, the client has a control tool. In a typical enterprise, there are staff assigned to security response. We are providing a tool and a dashboard to them that is highlighting an array of risky behaviors they are facing, and identifying the most serious problems. You touched on another problem that those security analysts face today. Many of the other tools identify potential problems, what are called false positives in the statistics world. If you take the example of Neiman Marcus, the story there was that there were sixty six thousand alerts that could have pointed to a problem in the several weeks before the actual breach occurred. The real problem is that the vast majority of those alerts were ignored or considered false positives. That is one of the big problems security analysts face today. TaaSera screens out that type of noise to amplify the signal.

CEOCFO: ***What types of companies are using your service today?***
Mr. Hartz: We are fairly early into the market. We have just come to market this year, we have several insurance companies, and some banks, technology companies and universities using it. We are trying to cover a variety of industries and use-cases because each of these is a learning experience for us as we gather more customers.

CEOCFO: ***Do you find that you are able to reach the correct person or people, and do people understand immediately?***
Mr. Hartz: We find that during the first fifteen minutes at a prospective account, they seem a little skeptical. Then we light up a few screens and find they have a very high level of interest after that.

CEOCFO: ***Skeptical because you cannot do it or that it even exists?***
Mr. Hartz: Skeptical as in what we broadly say does not sound possible, knowing what they know from other tools.

CEOCFO: ***How do you get your foot in the door?***
Mr. Hartz: The product really speaks for itself, and much of our early business has come from word-of-mouth and referrals. Word is beginning to spread about TaaSera and we're now being invited into more and more accounts.

CEOCFO: ***Have there been changes or tweaks since you started to develop the product and since it has been available? What have you learned along the way to make it better?***
Mr. Hartz: We have had to provide access for the user to a broader set of underlying information from our system. One of the things we have learned is that the user does not just want to know that there is something bad happening; they want conclusive evidence to understand why they need to be concerned. We provide forensic evidence over a period of time that gives them enough actionable intelligence to take to their boss and say "we have to take that server offline," even it is generating revenue, because the risk of breach or exfiltration is too high.

CEOCFO: ***How do you really get the attention and follow through that it really proves its worth?***
Mr. Hartz: I come back to my earlier point that the security teams now come in every morning, and turn on a screen showing millions of alerts and thousands of problems they need to deal with, but they cannot deal with thousands of potential problems. TaaSera narrows it down to individual systems and shows the top five or ten that are most critically in need of attention. So we give them a highly focused set of intelligence that really directs them to the most serious problems. Therefore, I

envision no real difficulty in our customers quickly seeing the value from TaaSera. We are being very helpful in filtering out the noise and pointing out the real problems.

CEOCFO: ***Would you be implementing your system in addition to others or would this replace current systems that people might be using?***
Mr. Hartz: We think of our system largely as a compliment. You certainly still want to maintain a perimeter defense with a network firewall and an event management system together with antivirus software. We are picking up what they miss. You do not take down the perimeter defense of the fort just because you are watching the middle, so we compliment what is there.

CEOCFO: ***What do you bring to the table from previous experience that has been helpful at TaaSera?***
Mr. Hartz: I spent the bulk of my career at PricewaterhouseCoopers consulting and I spent my last seven years there as CEO of that business. I was running a six billion dollar business on five continents with thirty thousand people. I dealt with a large array of large corporate enterprises and managed a large number of people. I think I have learned the importance of teaming technology solutions with service providers who can actually implement them. One of the things that we are spending more time on now is establishing partnering relationships with expert services organizations who will help us extend our reach, but also be able to hand-hold customers and make us part of a larger solutions set.

CEOCFO: ***What about at Wharton?***
Mr. Hartz: There, the focus was on the financial issues of an enterprise and one of the things I am doing in our organization right now is focusing a great deal of attention on the fund raising and capital structure that supports all the things we are trying to do, so that was a helpful background.

CEOCFO: ***Are you finding interest from investors?***
Mr. Hartz: We have taken a very different approach from many start-ups. Many organizations in this phase of their development would have been going out and chasing venture capital firms. Instead we have relied on private investors. The net result is I think we have a very friendly and supportive investor base. I am rather pleased with the outcome of that.

CEOCFO: ***Is it one standard offering or are there bells and whistles that companies might utilize?***
Mr. Hartz: There is a core product right now but we have a pipeline of other complimentary product offerings that will be coming on down the line.

CEOCFO: ***Are smaller businesses an area that you are addressing or will be in the future?***
Mr. Hartz: I think it will be through these partnering relationships that I talk about. This will enable us to extend our reach through IT services organizations that are already dealing with smaller enterprises.

CEOCFO: ***The bad guys constantly come up with new ways. What gives you the confidence that you will be able to identify those as time goes on?***
Mr. Hartz: They have done a good job of disguising their presence (IP addresses and such), which are fooling other detection tools, and they have learned to stay asleep in sandbox type situations and come out on the other side undetected. However, we do not think they can change the

core fundamental behaviors of malware and I think that is our great defense. They have to communicate with command and control, perform reconnaissance, and communicate in and out of the enterprise they have penetrated to exfiltrate information. As long as we are watching the life cycle episodes of malware and identifying risky behaviors, I think we can do a good job of detecting it.

CEOCFO: ***Put it all together. Why pay attention to TaaSera today?***
Mr. Hartz: Because the world is facing an increasing level of cyber risks. These come from both criminal enterprise and state sponsored groups. Virtually every enterprise at some level has already been penetrated by malware. No prudent organization can ignore it and the existing tools do some things well -- but they are not providing complete protection.

In short, the world of cyber defense is about to undergo a paradigm shift from perimeter defenses that rely on threat information that is in constant flux, to a behavior based risk intelligence that is resilient to evasion. TaaSera is at the forefront of the technology that will revolutionize the IT security incident response process.

BIO: Scott Hartz
Mr. Hartz is recognized as a pioneer in leading transformational business solutions for Fortune 500 global enterprises. His career in management consulting and systems integration at Price Waterhouse and PricewaterhouseCoopers brings experience with managing an enterprise serving more than half of the companies in the Fortune 500 as well as numerous smaller business organizations and governmental units throughout the world. From 1995 to 2002, while Global CEO of PwC Consulting, Hartz led the company's growth to a $6.0 billion enterprise with a global leadership position serving multi-national companies in corporate transformation and systems integration. He serves on the Boards of the Erie Insurance Group, Satmetrix, and Alien Technology. Hartz also served on The Wharton School Graduate Board and Lehigh University Business School Advisory Board and on the Board of Directors of Siebel Systems until its acquisition by Oracle in 2006.

He holds a B.S. degree in Economics from Lehigh University and an MBA degree from The Wharton School at the University of Pennsylvania.
