ceocfointerviews.com

Issue: October 2, 2017

CEOCFO Magazine

Q&A with Chris Freedman, Co-Founder – Business Operations & Development and Ben Finke, Co-Founder - Information Security Operations & Management for OnDefend providing Cyber Security, Network and Application Penetration Testing and Tools

Chris Freedman
Co-Founder - Business Operations & Development

Ben Finke
Co-Founder - Information Security Operations & Management

OnDefend
www.ondefend.com

Contact:
Jennie Mazur
860-604-2101
jennie@tailoredcampaigns.com

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

CEOCFO: ***Mr. Freedman, big and bold on your OnDefend website, is "We help prevent cyber-attacks before they happen." How are you able to do that?***
Mr. Freedman: OnDefend helps protect our clients from successful cyber-attacks by providing the cyber security testing and tools they need to decrease their vulnerable IT surface area thereby improving their overall security posture.
We also give our clients an opportunity to understand how well their security defenses work when being tested by a potential adversary. It is as if you were going to go compete in the Olympics, you want to make sure you get plenty of chances to work out before you show up for the actual event. Therefore, that is what we do. We give the clients the opportunity to see, based on scenarios that they are concerned about, how their environment will react and what blind spots they might have or what additional controls they need to put in place to prevent the worst-case scenarios from happening. One of the things our clients like about us a lot is that often our solutions to problems that we find do not require them to buy more equipment or buy more licenses or software, when simply a change in process or a change in the way something is set up is enough to make a big difference in the way that their network is able to be defended.

CEOCFO: ***What might you find in your evaluation that other companies miss? What do you understand?***
Mr. Finke: One of the things that we do that separates us from a lot of folks who do this kind of work is that we rely heavily on, not just using common knowledge of tactics and techniques, but also we have really talented testers on our team who use their imaginations to come up with new ways and new techniques to get around security controls and to understand how what might be a small problem otherwise, can be used in conjunction with other findings to create the way in that the attackers would look for to take advantage of in a customer network.

CEOCFO: ***Who is using your services? Is there a typical client?***
Mr. Freedman: Yes. We have worked with clients in just about every industry. Most of our success has been with enterprise level clients in the financial, healthcare and insurance industries. Those companies tend to understand the risks, appreciate the services that we can provide and have the budget/board approval to engage such testing. Other common clients are those who are required to complete annual testing due to their PCI-DSS requirements, which are companies in the food service, retail and hospitality industries.

CEOCFO: ***What is your geographic reach today?***
Mr. Finke: One of the great things about what we set up at OnDefend is our ability to test pretty much anywhere. We cover the entire United States by utilizing our national remote testing team. We have built a platform that lets us distribute testing systems to customers on site that allows our testers to work remotely in a secure environment that gives the tester the access that they need without having to have a bunch of people on site a customer location. Therefore, we can deploy very rapidly. Also, if our device shows up on site and the customer is not ready it is not like we have a consultant sitting on site, not doing anything and waiting around. Therefore, if a customer needs to move a timeline it is easy for us to accommodate that. Additionally, if we have a customer who suddenly has an urgent timeline and we need to bring multiple testers there we can do that in a same day type of a scenario. Lastly, this setup allows us to save money and pass those savings on to our customers in the form of affordable services.

"OnDefend helps protect our clients from successful cyber-attacks by providing the cyber security testing and tools they need to decrease their vulnerable IT surface area thereby improving their overall security posture."- Chris Freedman

CEOCFO: ***Would you help us understand why OnDefend can really be a cut above other cyber security companies? What one hears is that it is virtually impossible to be "ahead of the bad guys." Where can you provide an edge?***
Mr. Finke: That was a great question! Let me answer your second question. In terms of staying in front of the bad guys, it is certainly true that there are certain types of threats out there that it would be very difficult for anyone, even entire nations to stay in front of. if a bad actor decides they are going to target your business related to data theft, denial of service or other malicious intents, they are going to have many talented people with lots of resources at their disposal to find a way to get that done. What is important is that when you look at the actual statistics of cybercrime as we know it, which is when there are breaches of information; whether it is credit card data or information about people's health and medical records, what is almost always true is that the way that the bad guys got in was advantageously taking advantage of missing patches in a system that is on that faces the internet that has been missing for over a year. Most of these things have been out for a really long time. We know they are bad. They just have not been fixed because the customer has got so much stuff going on, their IT staff is overwhelmed and they can't keep up with all of the day to day activities as well as watching for things like this. Therefore, the attackers just take advantage and waltz right in and take what they are looking for. The numbers on this are staggering and there are something like ninety percent of cases where a company's IT vulnerability was at least a year old and was used to get in. That is certainly what we find in many places that we provide our services. Many times there will be a system that for some reason gets overlooked and as it goes on and on more and more things accumulate it becomes a much easier target for attackers. While we might not be able to come up with attacks like a state or a nation state actor would before they come up with them, we certainly can help prevent 90% of the attacks that occur in the world. Now this might circle around to your first question about what is the difference between OnDefend and similar companies to ourselves. Outside of our national availability and pricing noted in the last question, we spend a great deal of time working with our clients, not just on how you prevent these types of attacks but how to move their company up the security maturity curve. We help our clients better manage and "tune" their current systems, platforms, tools, networks and overall infrastructure as well as to find security blind spots. Therefore, when we deliver our results; this is especially true for any successful incursions where we were able to reach the objective, whatever the target is, it is that we will actually demonstrate, using a classification system, all of the steps that were necessary for us to get there. Everything from doing reconnaissance and mapping of the target, to understanding the initial identifying of the

vulnerability, to how we actually exploited that and then everything that we had to do after that to be able to get to where the objective was. We line that all up and then we give the opportunity to every single one of these places; “Here is how you could have prevented this, here is how you could have detected this, here is how you could have made our job harder.” Really, the goal is that if you could make the job of the attacker harder and longer you get the better chance to detect it and be able to intercede before damage happens.

CEOCFO: ***Do clients look at the details or do they just want to know you are keeping them safe?***
Mr. Finke: Yes! That is a great question! I think most of the customers that we deal with absolutely want to know. They want to be better. They are not looking for just a rubber stamp of saying, “Yes, security is good.” The reason a customer would bring us in is because they understand our goal is to work with them to create that type of awareness of where they can get better and also where they are doing a good job. A big thing that we do in our reports is that we spend a lot of time calling out good practices! That is because we want to reinforce the things that are working well as well as pointing out the things that are not. That is because we want them to know, “This particular thing you have done is doing a great job.” What is funny is that most of the things that do a great job for them are not things that they really spend a lot of money on. It is typically the way they just set up processes or the way they have configured systems to work that are typically the biggest barrier. However, if we do see a particularly effective security control, some piece of software or hardware that they bought; we call that out and say, “That particular thing really slowed us down. We had a bunch of vectors we thought were going to work and they did not because of this. That was really good.” We operate in two modes when we do the attack simulation. There is one we call the Black Box method, where the only person who knows we are coming is our sponsor at the company. The goal is to test, not just the network defense, but how well is the security team monitoring to detect and identify and contain someone who has got actual intention to go after a target of value inside their network. That can be very valuable. We also do what is called White Box testing, where we come in and work with the security team and we can train the security team up to do a little bit of their own testing and to teach them to understand how the mindset of an attacker works and how some of the tools work. In my career, I have been very fortunate to work on both sides of both sides, one being offensive security going after and testing like this as well as defending networks day to day. I think it is very important that people do that, because I think it makes you better at both. Therefore, our goal is to work with the team. We get access to networks maps. We get access to system information. We can really accelerate the testing schedule, so where as in a Black Box test we are going to do whatever we need to do just to get to the objective, we can be very broad in a White Box test and go after many more different avenues of attack, because we are working with them. Therefore, rather than us having to figure it out they can give us that information and we can use that to make some very quick determinations and show them how we are testing things, so that they can understand in the future how to do that themselves. There is a tremendous amount of value to both. Some of our customers will have us do both types of engagements in a year just because of the value that we get from testing, not just their systems, but their people, as well as being able to train them up while we are doing it.

CEOCFO: ***How do your people maintain the attention span needed to monitor so many different aspects?***
Mr. Finke: One of our primary assets is the people who do testing work for us. They spend a lot of time doing this because they are inspired by it. This is a hobby and a passion for them as it has been for me for years. It is amazing that people pay me for this! I am super glad that they do, because I would probably do it for free even if they did not. It is just something they enjoy doing! You can tell because it is what they do in their spare time, whether they want to work on it as a hobby or think of things to do. Many of us have this as a hobby. Many will go to security conferences to learn about all of the other things that people in the industry are doing. They are always reading about this. They are frequently participating in national hacking competitions and other events to stay ahead of the bad guys. When you are on a test there is a lot of information to go through. I think that part of what is at the core is that people who are good at doing this type of testing really are good puzzle solvers and good detectives and the idea for them is that there is going to be an enormous amount of information. However, somewhere in there is three or four clues, that if they can stitch them together the right way, gives them the answer that they are looking for. I think that really drives people. We have a lot of cross disciplines, not just for network penetration testing, but for other specialties, such as web application testing. Many people spend a lot of time and money developing applications that service their customers, their employees or their partners directly, that have access to a lot of critical information that is very sensitive. Therefore, we do the same type testing for web applications. What makes us complete is that we have people who are very talented in all these different spaces. We will bring a different team to there, based on the type of technologies that are involved in that test to make sure of a good cross section of people and they are always teaching and learning. My personal formula has been to always be learning; to never assume that I know everything about a particular thing and to recognize that I have got a lot of people around me who can teach me things and that I can also share things with them that I know that they might now. Therefore, we spend a lot of time sending that kind of information around. If someone has a particularly successful outcome on a test, something new that they tried of came up with on their own. We have places in our internal documentation where we write

up how that works so other people can use it. We develop a lot of our own tools and scripts and things that our testers use, either on engagements or while they are working some research on their own. That is extremely valuable place for us to be able to keep moving the knowledge of all the testers forward.

CEOCFO: ***What is the business model? Do you engage directly with your clients, do you work though partners or both?***
Mr. Freedman: We have a couple of models. One is that we definitely work directly with customers. They typically approach us when they have pretty mature vulnerability management processes in place and they are of the maturity of where they can take a report of a bunch of findings that we deliver to them and turn those into actions. Those clients typically already know how some of this type of testing works. We also provide our services through strategic partners, such as IT service providers; whether they are full outsource managed service providers or others, to both augment their current capabilities. We provide these services either as a trusted third-party partner or via private-label. We also work as a third party verification to some of our MSP clients or our partners bring us in to show their client that, "Not only do we give you these reports about everything we are doing, but we are going to bring you this third party provider who is going to do a server review that is going to prove a lot of the things we have shown you, but your systems are staying up to date and were are configuring things so all these things happen." Therefore, we have been very fortunate to be able to work with some really great service providers, either with their clients directly or with some of their clients that they are bringing in. One thing that we have done for these customers who typically work for MSPs is that they might not have a mature process for fixing some of these things as others do, so we have created a very simple to use vulnerability management work flow. Therefore, when we create our report you get the standard long form report like you would from any other tester. We also put the information into this dashboard that they can then assign work to people in the organization. They can see what things have been fixed and what things have not. When they are ready for us to come back and retest it is easy for us, because our testers know exactly what things they believe are fixed, so we can go right back and retest those things. It also gives them some really good information about how long did it take them to go from knowing they have a problem to fixing the problem. We often get asked by customers, "What is a good metric that I should show my boss or the board or whomever." I think a really useful metric for a security organization or an IT organization is to say, "It takes us X amount of days or hours or whatever the right number is to find a problem and fix it." I think it has been proven pretty reliably that, getting back to the ninety percent number I referenced earlier about breaches that happen based on vulnerabilities that are at least a year old; if you can have a situation where you know within, maybe it is fourteen days or maybe it is thirty days, that you go from having problem to having it fixed, that is pretty good! I think that is a really useful metric, not just for understanding the current capabilities of the organization, but to be able to put in very clear terms if you want that number to go down. Let us say the board decides that five days is the right number. Here are the resources that I need to make that five instead of thirty. I think that that is a very compelling thing, not just for making organizations safer, but for selling the need for additional resources at senior level management. We are also working on a holistic, game changing security product for the mid to smaller markets that will likely be used as a tool by these MSP partners across the US to keep their clients secure in an affordable way.

CEOCFO: ***You are developing a cyber defense product for mid to small markets. Would you tell us about that?***
Mr. Freedman: As previously noted, the majority of our clients are larger companies with budgets to engage live cyber security tests. What we have found is that typical live cyber security testing, which requires manhours of cyber security professionals, is too expensive for the small to mid-market clientele. Therefore, these companies are left unsecure. A recent study showed that 60% of small businesses who are breached are out of business within 12 months. The reality for these businesses is anti-virus and firewalls are no longer enough to keep the bad actors out and they need an affordable solution to maintain data and business IT continuity safety. To solve this problem, we are building a product that will fill this security void which will not only be affordable, but also easy to understand and interact with in a "Turbo Taxy" kind of way. This product will include an automated version of our vulnerability management with additional cyber security features such as email phishing, policy building, incident response and an industry specific compliance manager. This product is being made to be a one-stop-shop for managing a company's cyber security risk. We feel that our incoming solution is going to be a game changer and we will be providing additional public information soon as we head toward our Beta launch.