ceocfointerviews.com

Issue: April 4, 2016
The Most Powerful Name in Corporate News

An advanced 'Offensive Deception' Platform using Decoys and Mini-Traps to Smoke Out Malicious Cyber Attackers

Doron Kolton
Founder & CEO
TopSpin Security, Ltd.

CEOCFO: ***Mr. Kolton, according to your website, TopSpin Security is a leader in offensive deception and rapid detection. Would you tell us about your offering?***
Mr. Kolton: TopSpin Security offers a unified network-based detection platform that uses intelligent offensive deception technology in a new way. Our solution, DECOYnet, reduces the critical time between malware infection (a.k.a. cyberattack) and its detection. When we say "deception" we mean that we lure the attackers into so called 'traps' by setting up decoys that mirror the network and its assets (endpoints, servers, file repositories etc.). The attackers are tricked into believing they're seeing real assets, but in fact, they enter a trap.
We are combining intelligent deception with in-depth analysis and visibility of the Internet traffic of the organization. This allows our customers to quickly detect threats that are otherwise missed by peripheral defenses and to produce highly accurate threat analysis with very little effort or investment.

CEOCFO: ***How does it work?***
Mr. Kolton: Our DECOYnet platform lures the attackers into the decoy systems by using a variety of deception attributes that are automatically distributed in the organization. It is an endless process that "breathes" the organization's network, understands what assets are installed and identifies subnets, systems and applications. Then, DECOYnet automatically sets up decoys that resemble real network assets, and seeds mini-traps across the organizational network. "Regular" users and employees will not access the decoys – but an attacker from the outside will be lured and deceived to believe they are real. Once a decoy is tapped, for example access into a decoy web page, the platform immediately signals this out as malicious activity and triggers the alert.
It's important to note that when an attacker lands on a machine, it doesn't know which exact machine has been hit – so in fact, the *attacker* is the one who is vulnerable. We're using different kinds of mechanisms to lure attackers into our decoys. For example, we can seed fake data on endpoints to make it look like an engineer's PC, like that of a sales rep or even the CEO's. We seed the mini-traps (and make them as noticeable and as attractive as possible) so the attacker uses them and lands on our decoy systems. At the same time, using our egress traffic analysis capabilities, we track the activities and the communication of the attacker with the command and control servers. This allows us to combine all the attackers' activities and cover the different stages of the attack. DECOYnet covers everything the attacker does from right after the initial infection. We use multiple security engines to correlate the different events into significant incidents. The fact that we are able to base our solution on the real context of the events allows us to display very accurate incidents that include only the relevant information for the analysts. That way they can address threats accurately without having to bother with false positives.

CEOCFO: ***How do you implement the system? Is there much customization involved?***
Mr. Kolton: DECOYnet was designed to assist rather than intrude – so the efforts that are required to implement it are minimal. The deployment is typically completed within one to two hours. That's followed by a training session for the IT staff. From then onwards, the analyst can start using the platform with zero hassle. Much of the feedback we get from customers is that the detection is very accurate, the forensic information provided is detailed, the visibility into the activities in the organization reveals a lot of unknowns and the UI is very intuitive and simple to use. The solution presents the information to the analyst in a streamlined way, so it is very easy to analyze and understand attacks. Even a level 1 engineer can analyze the data and understand the type of incident that he or she need to deal with. In general, there's very limited customization required if at all, and that can be addressed in specific cases.

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

CEOCFO: ***How do you garner attention for TopSpin and DECOYnet™?***
Mr. Kolton: The main challenge here is to remain above the "white noise" created by so many solutions and technologies that all promise to solve cybersecurity once and for all.
The offensive deception market is quite new but companies are starting to pay attention to this category and want to use our technology. They see our intelligent deception platform as a key, fundamental element of their security arsenal - and this helps us to open doors. We have a great sales team that really understands the needs of the customers, which leads to POCs and pilots that are then converted into sales. We are also fortunate to be backed by well-known investors including: Shlomo Kramer, who was one of the cofounders of Check Point and Imperva; Mickey Boodaei, who was the cofounder of Imperva and Trusteer; Zohar Zisapel who leads the Israeli Rad/Bynet group and Rakesh Loonkar who was the cofounder of Trusteer. They are all private investors with years of experience in cybersecurity. They believe in the technology and they believe in our company.

CEOCFO: ***Are most people aware of the deception approach to security, or is that fairly new?***
Mr. Kolton: People typically understand the deception approach and recognize the real value it provides. In fact, we're seeing deception gaining more and more momentum in the market. The shift from traditional honeypot technology to what we call "offensive deception" really strikes a chord with customers. They love the way we actively engage with the attackers because we don't only deflect attacks from the real sensitive information, we also gather intelligence about the attacker and feed it back to other security platforms that the organization uses. So our added value is doubled and tripled. Plus, the integration of our intelligent deception with our analysis and visibility tools, is a game changer in that it provides several protection layers in one, easy to implement and easy to use solution.

"We are combining intelligent deception with in-depth analysis and visibility of the Internet traffic of the organization. This allows our customers to quickly detect threats that are otherwise missed by peripheral defenses and to produce highly accurate threat analysis with very little effort or investment."- Doron Kolton

CEOCFO: ***How will you be using the funding that you recently received?***
Mr. Kolton: We've recently launched the second generation of our DECOYnet solution so our current focus is to push this advanced platform into the market. Following the recent funding round, we've doubled our sales and customer support teams in the US as well as strengthened our management with seasoned Sales and Marketing VPs. We have paying customers in the US from the financial, healthcare, and technology sectors. They are extremely satisfied with DECOYnet. The recent investment will allow us to increase sales and marketing efforts and gain an even stronger foothold in the rapidly expanding security market.

CEOCFO: ***Put it together for our readers. Why choose TopSpin Security DECOYnet?***
Mr. Kolton: DECOYnet is a great product. It's very mature and the management console is so intuitive, that you don't have to be a security expert to understand where your threats are and what you need to do in order to deal with them. But it's not just technology. We have a wonderful team behind the product. We care about our customers and we care about their needs. DECOYnet gives an added value to our customers because it helps them detect cyberattacks quickly and provides them with the information they need - without drowning them in unnecessary data. As one of our customers simply put it: "DECOYnet finds threats that other software simply misses." I think that sums it all.

For more information visit: www.topspinsec.com

Contact: Yoel Knoll 708.310.4025 yoel@topspinsec.com

TOPSPIN SECURITY

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