CISO MAG

beyond cybersecurity

Volume 3 | Issue 9 | OCTOBER 2019

CYBERSECURITY AWARENESS AND SKILLING IN THE ORGANIZATION

STAY TUNED FOR THE UPCOMING

ENDPOINT SECURITY

CISO MAG
beyond cybersecurity

POWER LIST

SHOWCASING THE POWERHOUSES IN CYBERSECURITY

ON NOVEMBER 2019

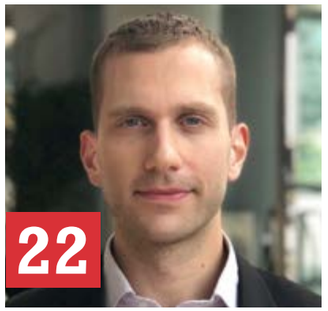
For more information contact:

Jyoti Punjabi
Deputy Business Head - CISO MAG
+91 9963654422
jyoti.punjabi@eccouncil.org

Taruna Bose
Publishing Sales Manager **- CISO MAG**
+91 7838483171
taruna.b@eccouncil.org

INDEX

VOLUME 3 ISSUE 9



EDITOR'S NOTE

Cybersecurity and the risk associated with cyber-attacks are frequent topics in the Boards of companies. News of cybersecurity threats and attacks is now common everyday news, so there is much more awareness.

The Board is not expecting an explanation of how malware or ransomware works. Instead, they want to know how an attack will impact the business. It needs to be quantified with business metrics.

The CISO needs to be an expert in communicating the impact of security to the Board. If he speaks the language of the business – in terms of the risks – he might win mindshare. That also makes it easier to convince the CFO for additional security investment.

Companies have for long used deceptive techniques like decoys and honeypots to trap hackers. But these techniques are evolving, writes Chris Roberts, the Chief Security Strategist at Attivo Networks. Chris is an advisory board member at EC-Council. Read his views in the BUZZ section.

These days CISOs have more career options and can pursue other executive roles, writes Charles L. (Chuck) McGann, Jr., in the INSIGHTS section. This is good news, and it should open the door for security professionals who are looking for alternative avenues of growth or responsibility, outside the CISO function. Chuck is a nationally recognized information security professional and the former Co-Chair of the (ISC)2 Government Advisory Board on Cyber Security. He is also engaged with the EC-Council to facilitate the Certified Chief Information Security Officer program.

Tell us what you think of this issue. If you have any suggestions, comments or queries, please reach us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief

CISO MAG
beyond cybersecurity

Volume 3 | Issue 9
October 2019

Editorial
International Editor
Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Principal Editor
Brian Pereira
brian.p@eccouncil.org

Senior Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Sr. Graphics Designer
Sameer Surve
sameer.s@eccouncil.org

UI/UX Designer
Rajashakher Intha
rajashakher.i@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Senior Director,
Compliance & Governance
Cherylann Vanderhide
cherylann@eccouncil.org

Deputy Business Head
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Marketing and Business Development Officer
Riddhi Chandra
riddhi.c@eccouncil.org

Digital Marketing Manager
Jiten Waghela
jiten.w@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

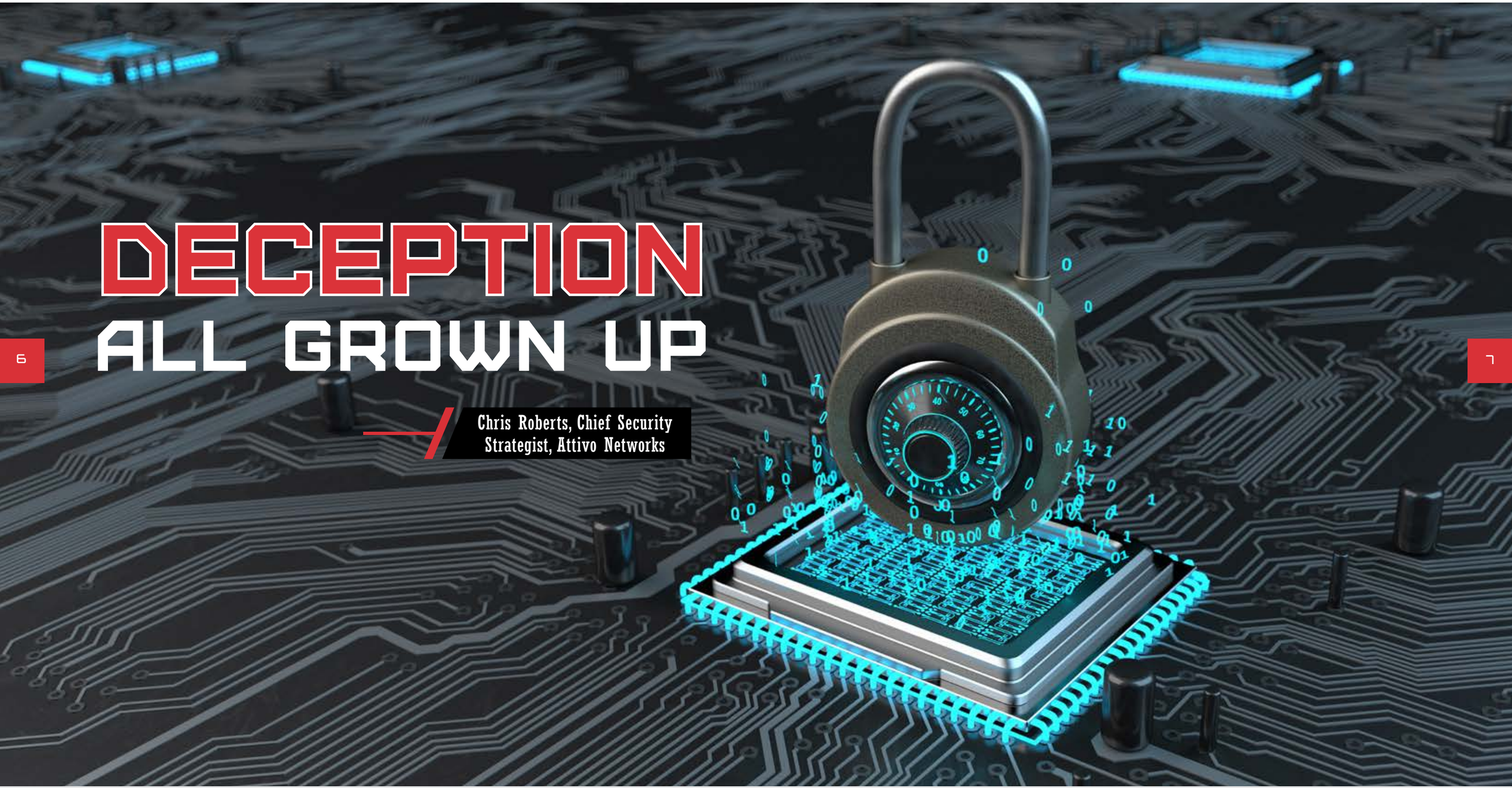
Technology
Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

VOLUME 3 ISSUE 9

BUZZ

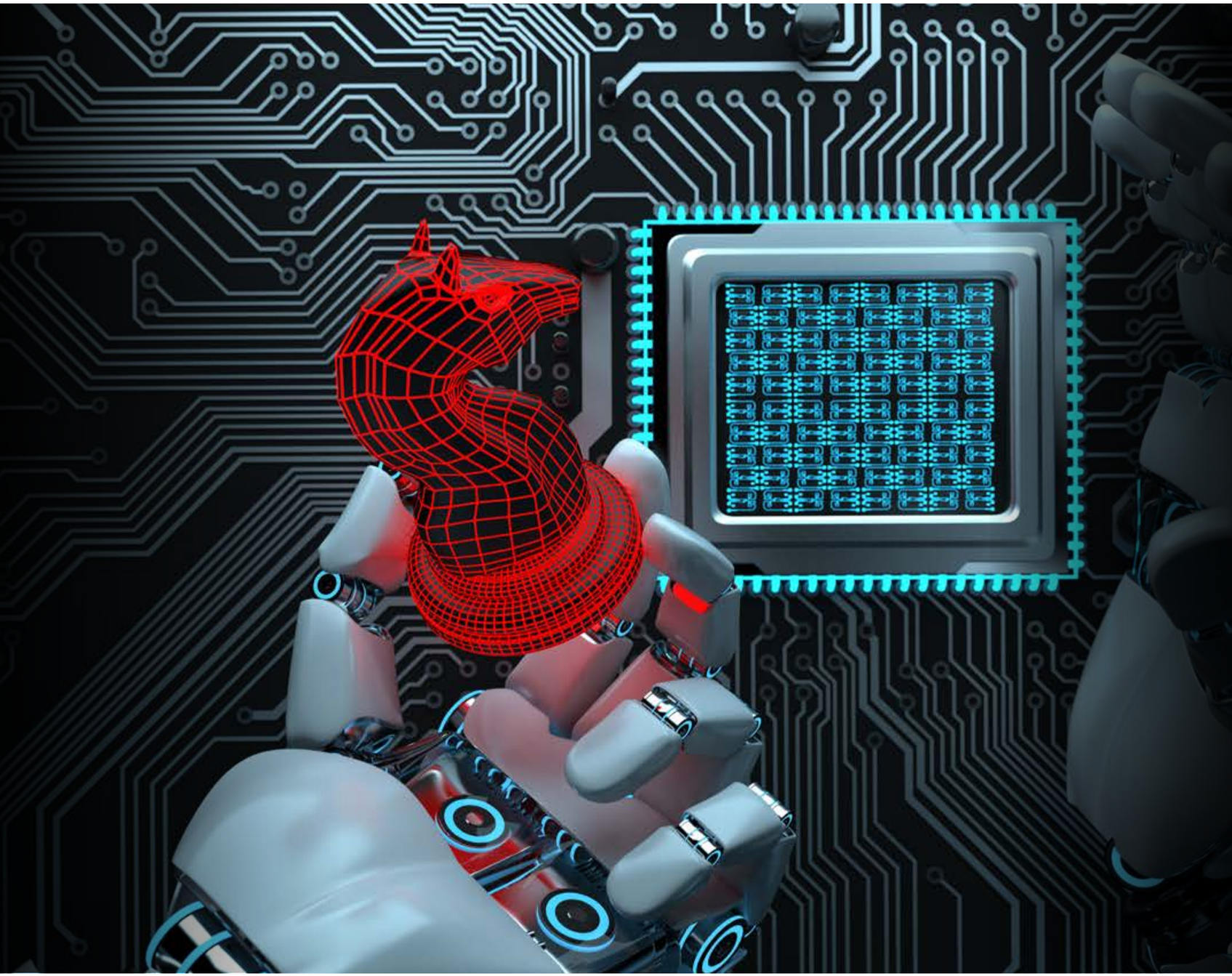
DECEPTION
ALL GROWN UP

Chris Roberts, Chief Security Strategist, Attivo Networks



VOLUME 3 ISSUE 9

BUZZ



I remember the days when we built our honeypots on CDs and dropped them onto machines without hard drives. The days when (let's face it) the idea was to research what the heck the attackers were doing. If we were lucky, we caught one and they hung out for a while, then realized they were being taken for a fool and moved on. Meanwhile, we got some intelligence and carried on regardless.

Oh, how the times have changed!

For the last couple of years, a number of companies have been working to build better and better mousetraps. Some have focused on the endpoint, some on the SMB market, and others have worked to drop decoy machines, systems, and all manner of enticing morsels of cheese scattered across the enterprise in the hope of catching attackers as they freely traverse around your networks (spoiler alert, I work for one of those companies).

One of the challenges has been engagement, and, like the art of fishing, it can involve long periods of boredom wondering if you've gotten it right, punctuated by short bursts of frenzied activity as you realize you've either hooked Jaws or just another sunken tree root.

The other core challenge has been "where." In essence, your entire environment is a target, and (as we are all well aware) the adversaries have had an easy time of coming and going through most enterprises with little concern for how they initially breach and pivot. We all know that one of the main components of most enterprises is the human, so it stands to reason that humans continue to be the core focus (after all we're easily fooled, ready to click on anything at a moment's notice, and rarely ask for help). However, as times change and technology progresses, we have to consider the other attack vectors: cloud, IoT, mobile, ICS (industrial controls/building controls), wearable technology, embedded technology (human healthcare as well as augmentation), transportation, and a myriad of other avenues. All of these require an engagement fabric that deception and detection technologies have to be ready for, and many of them still require human participation. In many cases, this unfortunately means that we are protecting our systems from the very humans that use them.

Watch, learn, and engage

So, how do you engage? How do you actually lay out bait that's good enough, yet not too good? How do you build a mousetrap that blends in but also isn't going to be glossed over as "just another machine in the mix"? You actively engage. You don't sit there like a frog on a log, waiting for the princess to come by. You actually watch, learn, and engage. You watch for "tells" and for actions. You are the Social Engineer of the deception world. Sitting there, actively looking at everything around you, saying hello to everyone, and

VOLUME 3 ISSUE 9

BUZZ

when necessary engaging. This is where it gets sneaky.

Up to this point, the red blinking light meaning "there's an attacker in our system" has only gone off when someone pokes a decoy or uses a set of credentials, or pivots a system, switch, etc. Now, with the way we've helped deception grow up, the simplest question or observation of anything is going to set off all the alarm bells.

The art of deception

Here's the logic: as an attacker/adversary, I'm going to land on your computer or in your network somewhere. Sorry, but you can't stop me. None of your EDR, FW, IDR/IPS, or SIEM/SP is going to stop me from getting in. My next task is to know what's around me. I might ask you if there are computers close to you (to which you'll answer yes). I might ask you (nicely) to give me your login credentials and all the other ones you have stored in the registry, browser, and 101 other places that applications seem to put data these days (which you'll willingly hand over). I might even check out the other systems/services you have running (obviously making sure to stop all the antivirus, host detection elements, and other things that can ruin my day), as well as other applications, systems, virtual drives, connected devices, etc. (which you'll also hand over). In fact, the upside of being the adversary is I have always had the luxury of asking the computer for almost anything, and, up to this point, it's handed everything over (which has always been rather handy).

In the past, you had to hope at each of those points that somewhere in that list of demands were deception credentials, systems, or accounts. Not anymore. Today, we're able to work out that you are up to no good, and the grown-up deception we've nurtured starts handing out credentials that look/feel/smell real and seem to work, and we cover all the computers around you (even ones that don't exist). We build responses and engagements on the fly, and we do it well enough to camouflage into the enterprise we're protecting while all the while recording and alerting the blue teams. Now, the nice thing here is, we can also do this across the enterprise, as if an adversary/attacker is moving laterally to other hosts on an IoT system, a switch, a cloud (which is, after all, just someone else's computer), your building controls, or virtually anywhere else in the network, we have the capabilities to engage effectively. We will welcome the attacker in with a bandshake, a hug, and a nice set of credentials that'll keep them busy while we alert all those around us.

The act of observing

The key to much of this thinking is to change the symmetry, place it firmly back in the hands of the blue team, and move from a reactive realm of security to something much more proactive. It's not waiting for someone to make a move, for an attack to begin, for a pivot to happen, or choices to be made. It's based on the logic behind observer effect: simply put, the act of observing will influence (or change) the phenomenon being observed (in this case your computer or anything on it). Think of this new breed of deception as the hypothetical experiment with Schrödinger's cat. The attacker is the one that cracks the lid on the box, and simply by observing whether the cat is alive or dead they trigger the change in state that alerts our intrepid band of quantum blue teamers.

This is deception grown up. This is proactive detection, deception, and something other than a pretty face in the crowd. This one goes looking for trouble rather than waiting for it to come to the doorstep. This is deception done right.

Chris Roberts is Chief Security Strategist at Attivo Networks. He is also an advisory board member at CISO MAG

CISO MAG | OCTOBER 2019