CISO MAG

beyond cybersecurity

Volume 4 | Issue 03 | March 2020

CISO MAG EXCLUSIVE

PAGE 18

INTERVIEW

BRIAN M. HARELL

ASSISTANT DIRECTOR FOR INFRASTRUCTURE SECURITY

CISA, DEPARTMENT OF HOMELAND SECURITY, USA

RED TEAMING

SIMULATING TARGETED CYBERATTACKS

CISO MAG
beyond cybersecurity

Volume 4 | Issue 3
February 2020

Image credits: Shutterstock
Cover design: Rajashakher Intha

EDITOR'S NOTE

Think like the Enemy!

There is a game called Ambush that is designed for young adults to play for team building and confidence building purposes. The rules of this wargame are simple: the group splits up into two teams. One team hides in the forest, choosing their places strategically to minimize their chances of being found or ambushed. The other side then sets out to find them, and when they do, they yell "ambush!" I reckon it is the militarized version of the popular "hide and seek" game. Of course, there are other aspects of this game that make it truly engaging and enjoyable—like exploring nature, navigation, and teamwork. One also needs to have a good sense of the terrain, the foliage, and the surroundings to seek out the best hiding places—and the "enemy."

There is a connection between the game of Ambush and Red Teaming. In his book titled "Red Teaming," author Bryce G. Hoffman writes that business leaders can transform their businesses by thinking like the enemy. Past and current war generals are trained to do just that, pre-empting the enemy's next move.

Our Senior Feature Editor, **Augustin Kurian**, came up with the idea of producing an issue dedicated to Red Teaming. And the editorial team curated a set of Red Teaming articles from contributors.

In our BUZZ section, **Dick Wilkinson**, IT Security Officer, New Mexico Judicial Information Division, tells us how to plan and prepare for a Red Teaming exercise.

Be sure to read our interview with **Tom Van de Wiele**, Principal Security Consultant at F-Secure in TABLE TALK. Van de Wiele specializes in red team operations and targeted penetration testing for the financial, gaming and service industries.

The COVER STORY has been written by **David Balaban**, a computer security researcher with over 15 years of experience in malware analysis and antivirus software evaluation. Balaban runs the Privacy-PC.com project.
We believe the tips, advice and best practices shared by our esteemed contributors will help you plan your next red teaming exercise.

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

Jay Bavisi
Editor-in-Chief

INDEX

SAUDI CYBERSEC SUMMIT 2020

APRIL 21, 2020 | RIYADH

SAFEGUARDING THE KINGDOM'S DIGITAL ECOSYSTEM

events.cisomag.com

#ksacybersec

Block your calendar

APRIL 21, 2020
RIYADH, SAUDI ARABIA

Meet and Connect with:

- 150+ Senior Infosec Leaders from Public and Private Sector
- 20+ Thought Leaders and Influencers
- 100+ Top Companies

REGISTRATIONS OPEN

For more details write to
marketing@cisomag.com

CISO MAG
beyond cybersecurity

EVENTS
An EC-Council initiative

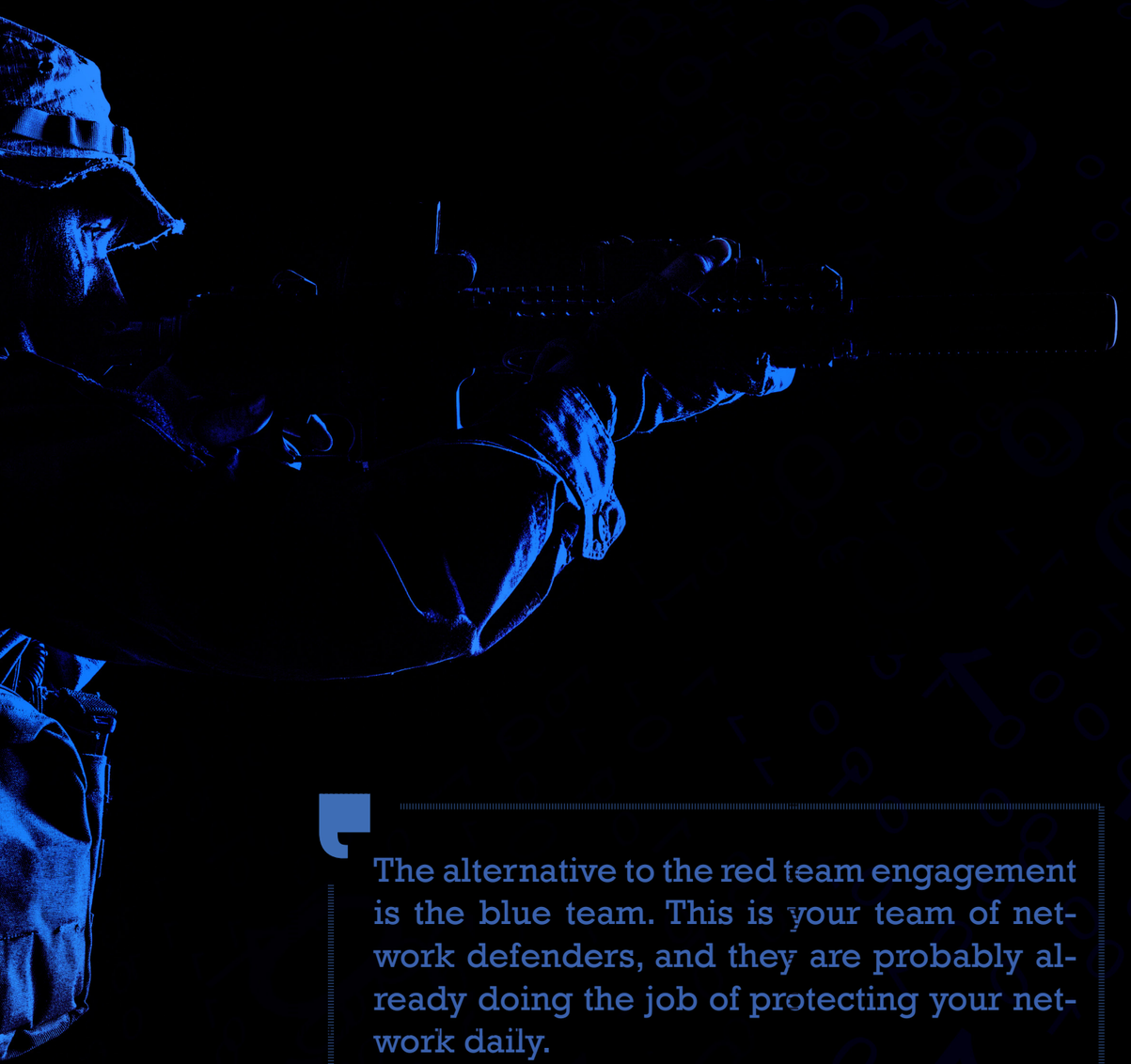
ENTER THE RED TEAM

Dick Wilkinson, IT Security Officer
New Mexico Judicial Information Division

You are an IT leader in your company whether CIO or CISO, and you have determined that you have a very mature security program. You have a list of technical and administrative security controls and know why they are in place. You have stopped a variety of dangerous events in the past 12 months and you can see things are going well overall. Some leaders would say that you have achieved the best defensive posture you could possibly create. Security professionals know there is always room for improvement. The threats we can't see and can't plan for are still lurking. To have a true check on maturity, it is time to test out your fortress and see if a worthy adversary can cause any harm—enter the **Red Team**.

Red Team engagements are a series of simulated attempts to breach your security perimeter. The concept can include physical attempts to enter secure spaces, social engineering on the phone and in person, technical attacks against your computer network or even a spear-phishing attempt at senior board and executive members. The team of people executing these attacks will be given some amount of limited knowledge about your organization and some clear boundaries on acceptable behavior. Rules may include: no breaking windows to gain entry or physically damaging computer equipment to disrupt the network. You must capture these boundaries in your contract's statement of work. The hope is to create a realistic dress rehearsal of attacks your organization may face. Understanding your business market, the security practices of industry peers and the threats that face your industry as a whole are crucial to creating a realistic set of scenarios your security plan can defend against. The previous experience of the red team will likely determine what techniques they find most useful. Be open to suggestions from the team and listen to how they have helped previous clients. This event can be a learning experience for your organization, even during the planning stages, before any offensive actions have taken place.

BUZZ...



> The alternative to the red team engagement is the blue team. This is your team of network defenders, and they are probably already doing the job of protecting your network daily.

> From the beginning of planning the event, the IT staff needs to create clear objectives to cover that help you learn the most about your gaps in the security plan. Create a list of known threats and what controls you have in place to protect against those threats; refer to your risk registry to get you started.

The Blue Team Defends

The alternative to the red team engagement is the blue team. This is your team of network defenders, and they are probably already doing the job of protecting your network daily. These employees are crucial to help you define what the outcome of this special event should be. They should have the best insight to understand what the weakest parts of your security plan may be. Advice from this group could range from very technical input to general anecdotes about previous security incidents. The historical knowledge from these employees should be built into your requirements for your red team actions. That knowledge may not define the entire plan but it will give you very clear starting points. The everyday network defenders will be your blue team during the engagement as well. To maintain some realism to the penetration events, keep this team out of the meetings where you go over the plan with the red team. You will want the defenders to use their real world tools and sensors and execute real responses to the red team's offensive actions. They need to have some element of surprise to act the way they would in real scenarios. Details to share with the blue team should be the rules of the engagement, what is and is not allowed, the start and end date of the event, the way to call a stop to the exercise if a real world incident begins to impact business operations. The blue team does need to be informed but they should not know the script the red team may follow.

Planning

Several factors

team engage

quite some t

security plan

have heard

waste to try

could be ad

know it is tr

your ideas

the red tea

to learn ho

planning t

objectives

your gape