Secureworks®

WHITE PAPER

SELF-INFLICTED CYBER ESPIONAGE

The Power of Adversary Exercises

WHAT IS AN ADVERSARY EXERCISE

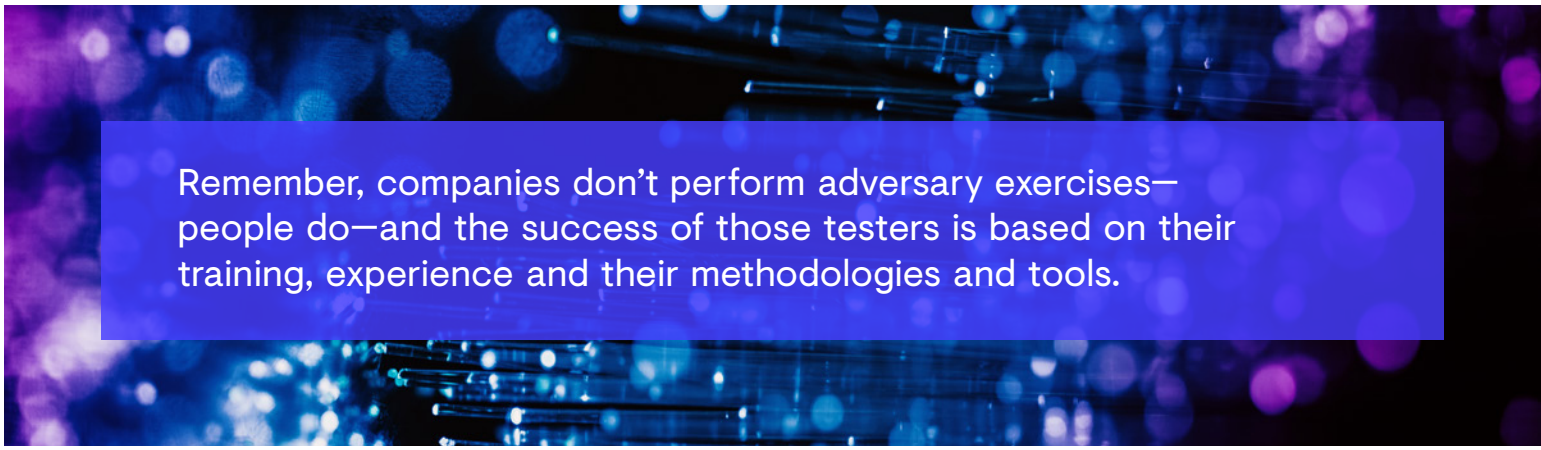
Adversary exercises are like training to be a professional boxer—you have your goal to be the best boxer in the world, you want to dominate your opponents and have world class defense to minimize risk from long term damage. First, you start eating healthy—a start similar to a vulnerability assessment. Then you want to dial in on your goals, so you begin hitting the punching bag—that's a penetration test (pentest). You want to eliminate further weaknesses, so you hire a trainer—that's a more advanced pentest blending wireless and phishing, for example. Finally, it's time to step into the ring and spar for a few rounds—that's an adversary exercise. These exercises leverage a Red Team who play the role of real-world adversaries mounting realistic attacks, with no holds barred, just as a targeted attacker would. These exercises challenge an organization's defense against electronic, physical, and social exploits. The objective

is to identify gaps in security practices and controls that standard technical tests are unable to find using a blend of attacks that combine various techniques to avoid detection and prevention.

HOW DO YOU KNOW WHEN YOU'RE READY FOR AN ADVERSARY EXERCISE?

Because exercises that leverage Red Teams seek to mimic a real-world attack, an adversary exercise provides information about your organization and security program that is otherwise difficult to collect. It also functions as an excellent tool for providing training for your Blue Team, assessing policies, programs and communications in a controlled way without the unfortunate aftermath of an actual breach. But, while an adversary exercise is a powerful tool and an important part of a security program, it's not something for which every organization is ready. It's not a silver bullet. You want to make sure you prepare to get the greatest possible benefit from the test.

For an organization interested in Red Team testing or adversary exercises, the first thing to look at is the type of testing you have already performed and the actions taken as a result of previous tests. Periodic vulnerability assessments, pentesting, social engineering, and the subsequent actions from the findings are important. Why? Because adversary exercises should be hard; it should be difficult for the Red Team to find and successfully exploit weaknesses. And it should also be difficult for the defender who has to attempt to detect. If you've built your program up to that point, then adversary exercises can provide you great value. If not, consider whether you could highlight gaps in your detection systems with a quality adversarial pentest before you invest in adversary exercises.



THE VALUE OF ADVERSARY EXERCISES

Once you've validated that working with a Red Team is what you need, you have to determine what it is you are trying to protect. What's important to your business? Often, it's a fairly easy decision because you've already given it a lot of thought. Common areas to protect include critical systems and assets you don't want anyone gaining unauthorized access to due to potential business impact.

Why is setting specific targets important? By setting goals, adversary exercises provide a more realistic simulation of an actual attack and an opportunity to assess those defenses protecting critical assets. The purpose isn't to assess security just for the sake of security. Instead, adversary exercises move you further from the theoretical and closer to the practical.

Think about the realism of the blended attack approach—by combining an external pentest, phishing and physical tests, for example. If you have a developer uploading internal code to a public hub, an executive who will open any email attachment they receive, or if someone forgets to lock the side door of a building, criminals are going to use every advantage they can. Red Teams are no different. Red Teams step through processes, collect information, identify weaknesses, and combine them to gain some level of access that moves them closer to the target. It's not linear, it's not predictable, and it allows for the development of a planned attack. It attempts to bypass the fences while efficiently achieving the goal. Many times, it involves a combination of social engineering, wireless, physical and network attacks. Because a Red Team is not limited to one particular area, these types of attacks can highlight the potential impact of what might otherwise be considered a lower severity issue.

TYPES OF ADVERSARY EXERCISES

In addition to identifying gaps in security that wouldn't otherwise have been found or considered, data from adversary exercises can be used to create and tune detections to close visibility gaps and harden defenses even further. Also, leveraging a Red Team provides Blue Teams with a perfect chance to gain and build game-time experience. The more an organization can practice and learn about techniques that they may be faced with, the more prepared they will be and the more confident they will feel in their ability to respond. Going from pentests to Red Team tests can be daunting, so it's important to consider your maturity and objectives when moving to this next stage. Becoming comfortable with exercises and operational flows for detecting and responding to activity can be built up through a deliberate approach to building an advanced testing program. There are different types of exercises to consider: collaborative, adversary emulation or adversary simulation.

	Collaborative	Adversary Emulation	Adversary Simulation
Scoping	Defined scenarios that cover different aspects of the kill chain	Highly customized engagement goals	Highly customized engagement goals
Ongoing communication between Red and Blue	Yes – open channel of communication to understand each action	No – covert	No – covert
Skill level required	Medium	Medium	High
Objective	Measure detection, prevention, and response capabilities for common TTPs.	Measure detection, prevention, and response capabilities for **common and attributable TTPs**.	Measure detection, prevention, and response capabilities for **attack primitives and unattributable TTPs**.
Adversarial Input	Pre-defined playbook scenarios	Customized attack scenario mimicking a real-life threat actor's TTPs	Red Team simulates a unique adversary, custom tool and exploit development
Port scanning, exploitation, post- exploitation, escalation, pivoting	Playbook scenario dependent	✓	✓
Can be performed remotely	✓	✓	✓
Phishing		✓	✓
OSINT to Gather Additional Targets		✓	✓
Perimeter Breach: Wireless			✓ (available as add-on)
Perimeter Breach: Physical Testing and Drop Box Placement			✓ (available as add-on)
Targets users		✓	✓

WHY ADVERSARY EXERCISES OVER OTHER TESTS?

Why can't you just run vulnerability scans and keep up with patching? Different tests focus on assessing different levels of security in different areas. The value of these build as the complexity increases—provided of course that some action is taken as a result of the testing.

Adversary exercises will break down the artificial barriers imposed on other testing and mimic the motivations and actions of criminals attacking your organization. Testing will focus on finding the weak points, network security, application security, and physical security and the way users respond to social engineering. Not only will the specific findings raise questions on mitigation and prevention, but the entire attack can be analyzed from a divisive point of view. Which attacks were detected? Which ones were not? Why? Were the indicators of compromise correlated to uncover the larger attacks? What kind of time frame are we looking at for detection? How can we stop these guys next time we have a test? Because the next time you see similar activity it might not be a test.

CONCLUSION

Getting your organization ready for an adversary exercise is on par with getting ready for the worst the world might throw at you. You can plan and prepare, but testing can tell you how the fight might go down. Maybe you're ready to be exercised by a Red Team. If so, great. Maybe you're at the point of still working towards it. That's great, too. There are plenty of organizations out there that can help get you to that point. We hope you choose to do your testing with Secureworks, as we can work with you on all areas of information security.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

CORPORATE HEADQUARTERS

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MIDDLE EAST

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

ASIA PACIFIC

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Otemachi One Tower 17F
2-1 Otemachi 1-chome, Chiyoda-ku
Tokyo 100-8159, Japan
81-3-4400-9373
www.secureworks.jp