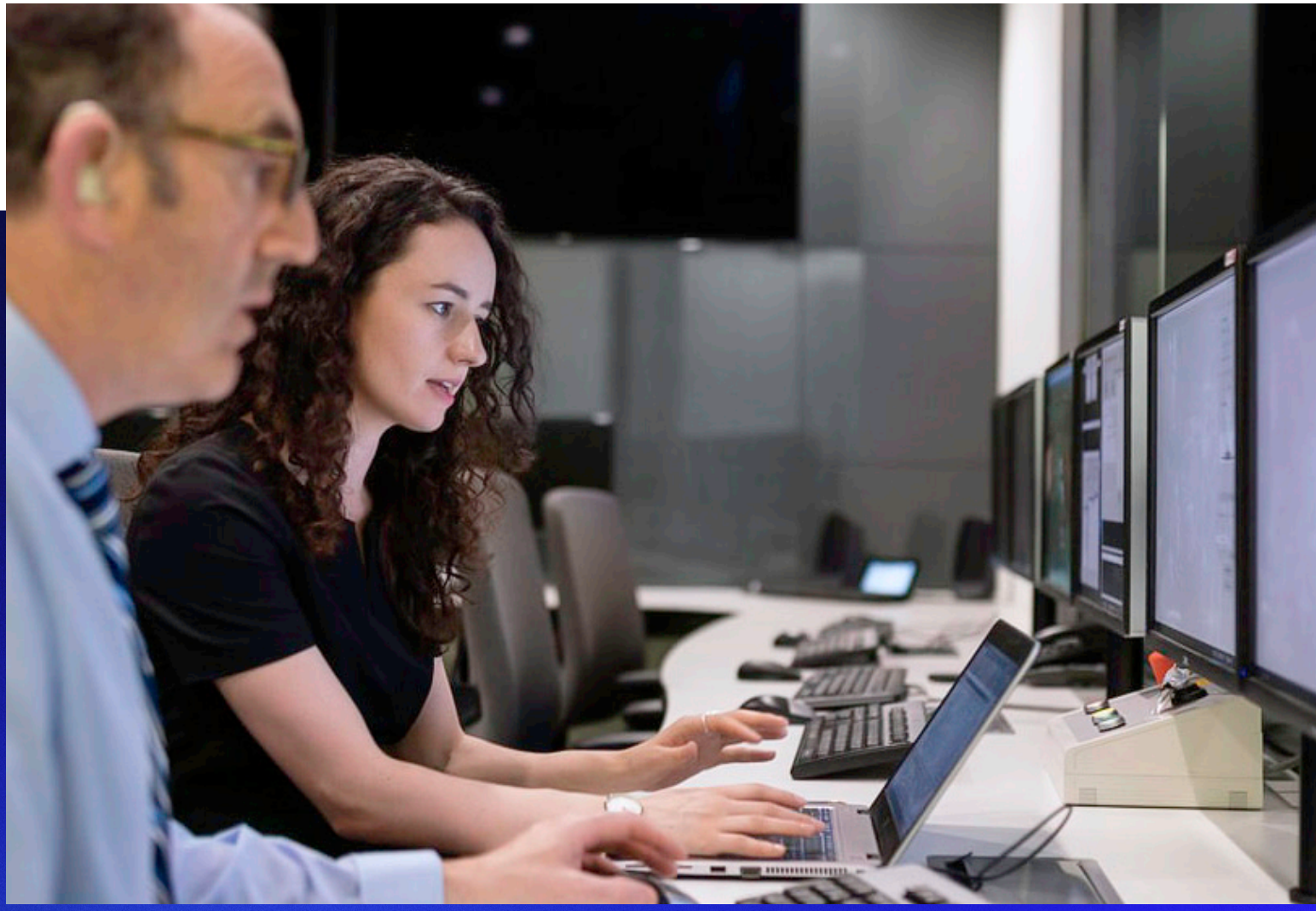
Secureworks®

WHITE PAPER

Self-Inflicted Cyber Espionage

The Power of Red Team Testing



What is Red Team Testing

Red Team testing is 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 start getting more specific, so you begin hitting the punching bag — that's a penetration test. You want to eliminate further weaknesses so you hire a trainer — that's a more advanced penetration test blending wireless and phishing, for example. Finally, it's time to step into the ring and spar for a few rounds — that's a Red Team test. Red Team tests simulate the real world with no holds barred, just as a targeted attacker would. These tests 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 combination of attacks that combine various techniques to avoid detection and prevention.

Remember, companies don't perform Red Team tests — people do — and the success of those testers is based on their training, past experience and their methodologies and tools.

How Do You Know When You're Ready for a Red Team Test?

Because Red Team testing seeks to simulate a real world attack, it provides information about your organization and security program that is difficult to collect in any other fashion. It also functions as an excellent tool for providing training for your Blue Team; assessing policies, programs and communications in a controlled fashion without the unfortunate aftermath of an actual breach. But, while the Red Team engagement 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 in order to get the greatest possible benefit from the test.

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

The Value of Red Team Testing

Once you've validated that a Red Team Test 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, the Red Team engagement provides 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, Red Team moves you further from the theoretical and closer to the practical.

By setting goals, the Red Team engagement provides a more realistic simulation of an actual attack and an opportunity to assess the defenses protecting those critical assets.

Think about the realism of the blended attack approach – by combining an external penetration test and phishing, for example. If you have a developer uploading internal code to a public hub, an executive who will open up 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 Team is no different. Red Team testing involves stepping through processes, collecting information, identify weaknesses, and combining 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. And because the 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.

	Vulnerability Assessment	Penetration Test	Red Team
Scoping	Reports on all systems and vulnerabilities found on in-scope systems.	Threat Modeling (includes suitable testing scenario)	Highly customized engagement goals
Skill level required	Low	High	High
Targets users			✓
Objective	Broad Scan	Limited Scope Adversary Simulation	Broadscope Adversary Simulation
Can be performed remotely	✓	✓	✓
Vulnerability scanning	✓	✓ (as necessary)	
Port scanning, exploitation, post-exploitation, escalation, pivoting		✓	✓
Manual testing to simulate attacker methods and techniques		✓	✓

	Vulnerability Assessment	Penetration Test	Red Team
Phishing		Can be added for a more advanced test	✓
Attack planning & preparation		✓ not covert/limited scope	✓ covert/stealthy
OSINT to gather additional targets			✓
Wireless Networks			✓ (as necessary)
Physical testing and drop box placement			✓ (as necessary)

Why Red Team Over Other Testing?

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. Take a quick look at some of these tests, vulnerability assessments, penetration tests and Red Team testing. The value of these build as the complexity increases — provided of course that some action is taken as a result of the testing.

Red Team tests 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 a 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 we see the stuff it might not be a test.

Conclusion

Getting your organization ready for a Red Team engagement 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 for a Red Team test. 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. If you are interested in exploring your readiness for a Red Team testing engagement or other forms of security testing, please visit our webpage to learn more or contact your local Secureworks security specialist.

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
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp