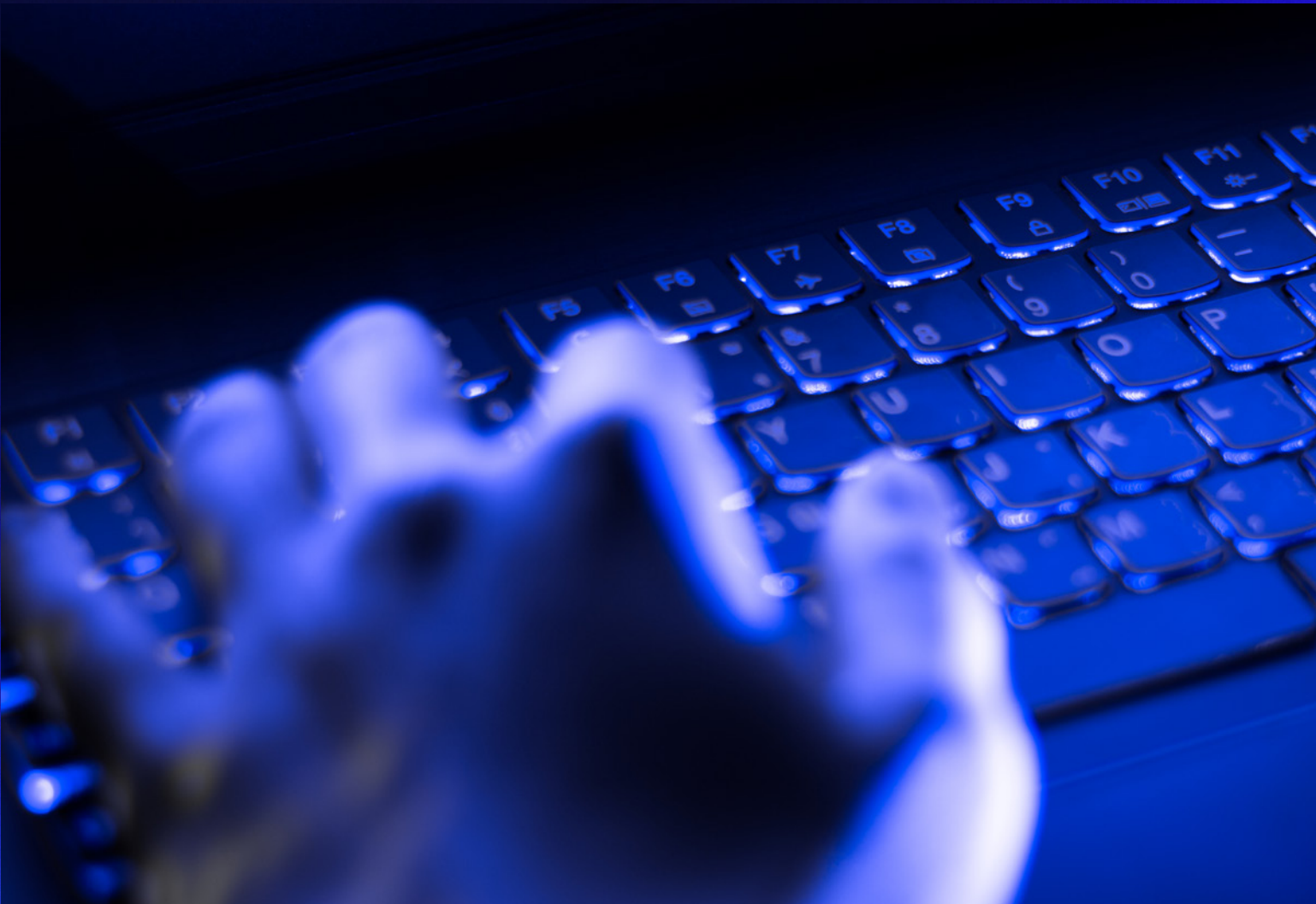


Secureworks®

WHITE PAPER

ADVERSARIAL SECURITY TESTING:

Which assessment is right for me?



Leveraging third-party security testing services can deliver the independent expertise, experience and perspective you need to enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency.

TESTING YOUR SECURITY DEFENSES

Organizations often lack the internal resources and expertise to keep up with the ever-changing security and regulatory landscape, let alone test and assess their networks, applications and overall security programs. They need help elevating their security profile, reducing risk and achieving compliance with applicable laws and industry mandates. Third-party security testing services can provide organizations with the knowledge, expertise and efficiency needed to conduct thorough security and risk evaluations of their environment. Consider utilizing the expertise of a credible third party for testing and assessments that address logical, physical, technical and non-technical threats to your environment. Many times, third parties can expose gaps that create risk, help you construct a stronger security posture and help you confidently meet your compliance mandates.

ADVERSARIAL SECURITY TESTING

Highly certified security consultants will test your networks, systems, facilities and employees. Through use of “real-world” strategies and tactics used by threat actors, you can learn where your security is strong and where gaps exist that could lead to a compromise.

Traditional security testing delivers a comprehensive review of all vulnerabilities and technical risks. For a more complete, hands-on test, a mock cyber attack should provide a collaborative test with you to establish testing objectives (sometimes called trophies). These are specific, high-value systems or data that are the same business-impacting goals that advanced threat actors aim to achieve.

Network Security Testing

Network Security Testing helps organizations identify and demonstrate vulnerabilities and determine actual risk, validate security defences and meet compliance mandates. Make sure you choose a provider that takes a security-centric approach, instead of one driven by compliance. Expert testers should work with you and your organization to determine the right cybersecurity tests that will provide the insights you need to develop a stronger security posture. Testing services include vulnerability assessment, penetration testing (pentesting), and wireless network penetration tests.

Vulnerability Assessment

Vulnerability assessments are "light-touch" evaluations that use automated tools to scan and find known issues and vulnerabilities. These types of assessments should be used during a low-security posture period or when you are seeking to baseline a new network.

What Does It Help You Answer?

- Are there gaps and vulnerabilities present in our network?
- Do we have proper configuration and patch management?
- Are there any low-hanging fruit present in the environment that an attacker could easily exploit?
- How can we establish a security baseline?

Penetration Testing

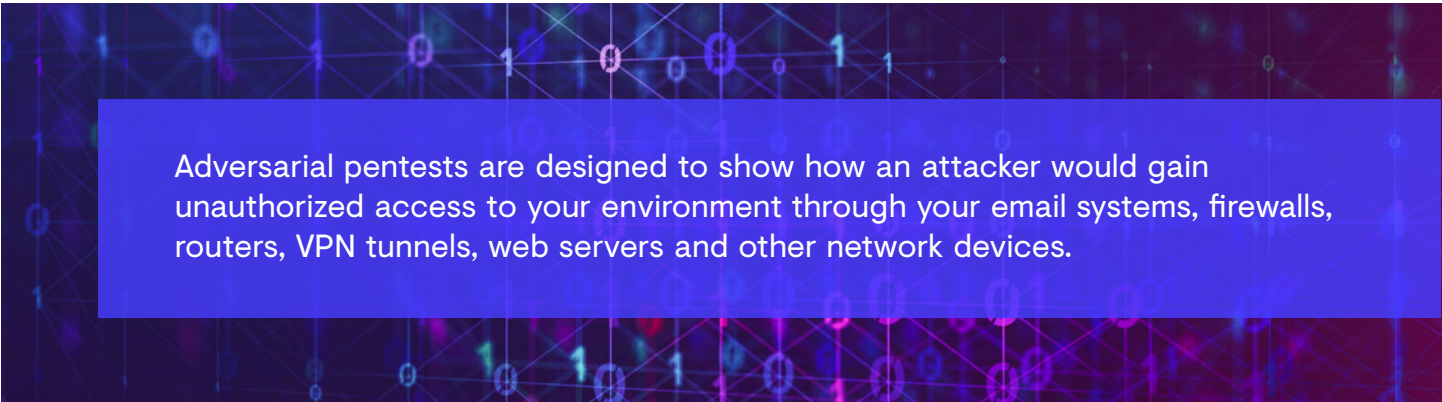
Pentesting helps organizations meet compliance requirements and validate specific security risks that may exist.

A pentest is a form of assurance testing. Pentesting can be performed from the perspective of threats attacking the network edge facing the internet (external pentest) and from inside the network environment (internal pentest).

Choose a provider with industry recognized expertise and mature consulting processes to deliver real business value to your organization.

Pentests go further than vulnerability assessments to identify security gaps and vulnerabilities in your network. Tests are designed to show how an attacker would gain unauthorized access to your environment by compromising your email systems, firewalls, routers, VPN tunnels, web servers and other devices.

Prefer third-party testers who can use blended approaches and mimic a network-based attack to test your network security defenses, policies and practices, and provide the prioritized, risk-based steps and recommendations you can take to improve your security. Complete tests will continue beyond penetrating the network to identify methods that



Adversarial pentests are designed to show how an attacker would gain unauthorized access to your environment through your email systems, firewalls, routers, VPN tunnels, web servers and other network devices.

a hacker could use to gain full, persistent control of your systems and use that as a base for attacks deeper into your network. Learn what vulnerabilities exist in your systems but also how they can be exploited and the impact they can have on your organisation to be better protected against a persistent attack.

What Does It Help You Answer?

- Where are we vulnerable if a determined hacker were to attack?
- How is our current security posture across the network?
- What would be the impact of an attacker intrusion?

Wireless Networks Security Testing

Wireless Security Testing service evaluates the security of your wireless networks infrastructure and assesses their compliance with appropriate mandates. These risks will be exposed through configuration reviews, technical testing and scanning for rogue access point detection.

What Does It Help You Answer?

- What wireless devices are accessing our network?
- Are there any rogue access points?
- How secure is our Wi-Fi infrastructure?

PHISHING

The goal of phishing is to obtain user credentials or compromise a user's workstation. This can be accomplished using a variety of standard scenarios or custom-tailored situations. Manipulations generally involve the impersonation of customers, internal staff or third-party contractors.

Consider including phishing to your testing program or to complement a pentest to gain an understanding of user security awareness and how defenses measure up against simulated attacks.

What Does It Help You Answer?

- How can we increase user awareness for social engineering?
- How well can our users recognize malicious emails?
- How do our security controls perform against typical phishing campaigns?

Application Security Testing

Application security assessments provide assurance that your mobile applications, web applications and APIs are secure. A third party should leverage deep knowledge of the tactics, techniques and procedures (TTPs) threat actors use to assess and test the state of your applications and provide actionable recommendations to enhance security.

Some types of Application Testing services you may want to consider include:

Web Application Security Assessment

Get assurance that your web applications are secure. Where a pentest will bring light to the vulnerabilities on the application infrastructure, a web application security assessment will provide a thorough inspection on the application itself. Choose a security consultant that goes above and beyond the OWASP Top 10 to assess and test the state of your web-facing applications. This evaluation thoroughly evaluates the underlying operating system, web server and database for vulnerabilities.

What Does It Help You Answer?

- How can we thoroughly test a critical web application we have?
- How can we test changes we have made to our web application?
- How susceptible are we to SQL Injection and Cross-Site Scripting (XSS) attacks?
- Can someone get login credentials and inflict damage?

Mobile Application Security Assessment

Whether you develop mobile applications for use by customers, employees or business partners, testing is critical. Gain confidence that the application and the supporting backend infrastructure and data flows are secure and compliant.

What Does It Help You Answer?

- Can an adversary gain access to the network behind our mobile application?
- Are there any vulnerabilities present in our mobile application that can affect our company's image?
- Are the users of our mobile application protected?

Web Service Testing

Test internet-facing systems that support applications. These systems are often the ones that store or provide access to the most critical information or systems.

What Does It Help You Answer?

- Is our API authorization and authentication properly enforced?
- Can a threat actor modify or retrieve confidential information?
- Are our API tokens or keys scoped appropriately? Does our web service conform to best security practices?

Adversary Attack Exercises

Adversary attack exercises help organizations practice, cultivate and enrich their Blue Team capabilities, while identifying gaps in security practices and controls that standard, narrower-scoped penetration tests are unable to find. Adversary attack exercises leverage a Red Team, a team of “attackers” who mount attacks against an organization’s “Blue Team” (the defenders) using a blend of electronic, physical and social exploits to mimic real-world, persistent adversaries and their tactics, techniques and procedures.

The objective is to exercise and practice an organization’s detection and response capabilities in their own network with their own tools against a live threat actor, with organizational improvement at the core. Since detection and response is key, some maturity in these areas is recommended, including an established security monitoring capability (in-house or third party), and an internal team of defenders.

Adversary attack exercises are a great way to build incident readiness and resilience, but it’s recommended that you select exercises based on your specific organization’s objectives and maturity to get the most value from them. The industry often refers to Red Team Testing, Red/Blue Team Testing or Purple Team Testing, but those definitions can remain broad and vendor specific. Instead, determine what you are trying to achieve by using the principles of Red Team Testing. There are different ways to perform adversary attack exercises, including collaborative, emulated or simulated exercises.

Collaborative Exercises

Most akin to what is sometimes known as a Purple Teaming, collaborative exercises are a great starting point for organizations seeking to step up their testing program. These exercises enable organizations to experience live-fire information security attacks designed to mimic real-world threat scenarios. Often shorter than other exercises, these focus on specific threat scenarios often drawn from the third party’s experience breaching targets, insights from incident response engagements, and threat intelligence based on both defensive and offensive research.

Unlike a traditional Red Team exercise, the collaborative nature and the use of defined scenario playbooks that cover several aspects of the cyber kill chain allow for a controlled hunting exercise prior to executing more advanced exercises.

INDUSTRY DEFINITIONS

RED TEAM

Under the Red Team testing model, your *faux* attackers will operate without advance knowledge of your defenders (aka the Blue Team).



PURPLE TEAM

Under the Purple Team testing model, attackers and defenders—the Red and Blue Teams—work together continuously throughout the exercise to pinpoint issues and implement fixes.



What Does It Help You Answer?

- How is our incident readiness and are appropriate response processes in place?
- How well do existing security controls detect activity and do they need to be tuned?
- Do security controls need tuning?
- Is our team ready for other adversary exercises?

Emulate Adversary Exercises

Moving beyond playbooks that target specific scenarios and aspects of the kill chain, adversary emulation exercises are customized and driven by threat intelligence based on defined threat actors known to target your industry. By emulating the TTPs of a specific threat actor, the exercise identifies gaps in security that could allow threat actors to act on their goals unimpeded. The exercises aim to train defenders to spot indicators of compromise from known threats. This type of exercise aligns itself with CBEST and TIBER-type testing methodologies.

What Does It Help You Answer?

- Are there gaps in security controls that real-world attackers could exploit?
- Can our team and processes respond to and ward off common attacks?
- Are our security controls and hunting playbooks properly tuned?

Simulated Adversary Exercises

The threat landscape is continuously evolving with newer techniques and derivatives of techniques that aim to find small gaps in your security to exploit and bypass detection. Simulated exercises challenge your Blue Team with a realistic attack by a unique adversary with non-attributable TTPs to identify gaps and further strengthen your security posture in a continuously changing environment.

What Does It Help You Answer?

- How does my security stand up to an unknown, sophisticated and persistent threat actor?
- How is my team's incident readiness?
- Are our team and processes sufficient to withstand a combination of advanced techniques and blended threats?

KEY DEFINITIONS

EMULATION

Emulation places an emphasis on mimicking “**known bad**,” known threat actors and attributable TTPs that have been analysed and in many cases signed.

SIMULATION

Simulation places an emphasis on “**unknown bad**” and avoids imitation to be a unique threat actor in the wild. They tend to utilize customized sets of advanced TTPs and are persistent in their attempts to reach their goals or objectives.

SUMMARY

Each security test has its own objectives and acceptable levels of risk, while maturity of your security program can also help drive where you should start. There is not an individual technique that provides a comprehensive picture of an organization's security when executed alone. A qualified third party can work with you to determine what combination of techniques you should use to evaluate your security posture and controls to begin to determine where you may be vulnerable.

ABOUT SECUREWORKS® ADVERSARY GROUP

Secureworks Adversary Group tests provide organizations with the knowledge, expertise and efficiency needed to conduct thorough security and risk evaluations of their environment. We offer testing, assessments and exercises that address logical, physical, technical and non-technical threats to your environment. Our dedicated team of testers leverage their experience, expertise and the latest threat intelligence from the Secureworks Counter Threat Unit™ (CTU™) Research Team. We can help you identify gaps that create risk, construct a stronger security posture, strengthen incident readiness, and meet and exceed your compliance mandates.

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