DATA SHEET

Technical Testing

Application, Network and Red Team Testing

The SecureWorks Technical Testing services deliver the independent expertise, experience and perspective you need to enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency.

Test Your Security Defenses

Organizations often lack the internal resources and expertise to keep up on an 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.

SecureWorks Technical Testing Services provide organizations with the knowledge, expertise and efficiency needed to conduct thorough security and risk evaluations of their environment. We offer testing and assessments that address logical, physical, technical and non-technical threats to your environment. We can help you identify gaps that create risk, help you construct a stronger security posture, and help you confidently meet your compliance mandates.

Determining which assessment is right for you depends on what you are trying to accomplish.

What is your goal?

- Mitigate risk
- Improve your security posture
- Evaluate your team's response capabilities
- Meet compliance

Security Risk and Consulting

The SecureWorks Technical Testing experts are part of the Security and Risk Consulting practice which provides expertise and analysis to help you enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency. Before you determine which technology and policies you need to improve the strength of your security program, work with a trusted partner who will assess and/or develop the right policies and procedures for your organization.

Expert Testing, Analysis and Assessments

- Highly Credentialed Experts passionate about security
- Focused on security Best Practices for your industry
- Deep understanding of Compliance, Regulations and Security Frameworks
- Latest threat intelligence from the Counter Threat Unit™ research team
- Risk-based approach

Test Your Security Defenses

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

Technical Testing

Technical Tests are hands-on tests by consultants that evaluate your application or network security. Traditional technical testing delivers a comprehensive review of all vulnerabilities and technical risks. For a more complete test, a simulated cyber attack or Red Team Engagement will provide a collaborative test with you to establish testing objectives (sometimes called trophies): specific, high-value systems or data that are the same business-impacting goals that advanced threat actors aim to achieve.

Application Security Testing

Testing Application Security Assessments provide assurance that your mobile applications, web applications and APIs are secure. Leveraging our deep knowledge of the Tactics, Techniques and Procedures (TTP) threat actors use, our security consultants assess and test the state of your applications and provide actionable recommendations to enhance their security.

Application Testing services available include:

Web Application Security Assessment

Get assurance that your web applications are secure. Where a Penetration Test will bring light to the vulnerabilities on the application infrastructure, a Web Application Assessment will provide a thorough inspection on the application itself. Our security consultants go 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. In addition, we provide actionable recommendations to enhance their security.

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?

Application Security Assessment: Mobile

Whether you develop mobile applications for use by customers, employees or business partners, testing is critical. Gain confidence that the not only the application, but the supporting backend infrastructure and data flows are secure and compliant.

What Does it Help You Answer?

Get a thorough review of not just the application but whether a hacker could gain access to the network or data behind it. Protect your company's image, maintain client, employee and business partner confidence while gaining peace of mind.

Web API Testing

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

What Does it Help You Answer?

API Testing will make sure that your data and backend systems are secure from a threat actor adding inappropriate content or stealing confidential information.

Network Security Testing

Network Security Testing helps organizations identify and demonstrate vulnerabilities and determine actual risk, validate security defenses and meet compliance mandates. SecureWorks takes a security-centric approach, instead of one driven by compliance. Our expert testers work with you and your organization to determine the right cybersecurity tests and assessments to develop an overall stronger security posture. Testing services include Penetration Testing, Social Engineering Tests and Specific Network Tests

Penetration Testing

Penetration Testing helps organizations meet compliance requirements and validate specific security risks that may exist. A Penetration Test is a form of assurance testing. It is 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.

Penetration Testing can be performed from the perspective of threats attacking the network edge facing the Internet (external) and from inside the network environment (internal).

Vulnerability Assessment is a "light-touch" evaluation to identify gaps and vulnerabilities in your network, help you validate your configuration and patch management, and identify steps you can take to improve your security. The assessment helps you meet your minimum compliance mandates and security assessment needs.

Penetration Tests are also known as "ethical hacking" and go further than vulnerability tests 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.

Advanced Penetration Tests simulate a networkbased attack to test your network security defenses, policies and practices, and provides the steps you can take to improve your security. It is a more complete test that continues beyond a Penetration Test to identify methods that 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 to they can be better protected against an attack.

What Does it Help You Answer?

Learn where you are vulnerable if a determined hacker were to attack your organization. Are you looking to assess your security posture? Use these tests to assess networks, systems and applications for security gaps and risk to improve the overall security posture and controls of your organization.

Social Engineering

Employees need to be vigilant against attackers who will prey on their tendencies to be helpful and cooperative. Social Engineering your employees using "true-to-life" tactics is the most effective way to test workers against non-technical threats posed by social engineers.

Whether performed standalone or as part of an integrated Red Team testing engagement, SecureWorks' Social Engineering experts evaluate the effectiveness of your employees against softer, non-technical break-in attempts. Based on the latest intelligence on social engineering tradecraft, these services evaluate your employees' vigilance against creative and often personalized threats that work to exploit their trust and lack of security awareness.

Phishing: Click and Log

A remote social engineering assessment, Phishing Click and Log is designed to identify gaps in user security awareness that an attacker can exploit. Receive a log and report showing who clicked on the various links.

Testing is designed to deliberately attempt to trick users by mimicking common websites, impersonating internal staff, third-party service providers or customers.

Phishing: Endpoint Attack

The goal of Phishing Endpoint Attack is to obtain either 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.

Vishing

The telephone equivalent of phishing, Vishing is an attempt to verbally steer the user into surrendering sensitive information like passwords, or to execute malicious software that gives attackers remote control of their workstation.

Our experts work with you to identify appropriate scenarios to test your employees to prevent attackers from thwarting common phishing security controls.

What Does it Help You Answer?
These point-in-time tests help to get a benchmark on how well your employees respond to phishing and other social engineering attempts. They test whether employees unknowingly represent a significant risk to the organization and help justify creation of Security Awareness Programs.

Network Equipment Testing

Our security consultants can test your networks, systems, facilities and employees. Through use of "real-world" strategies and tactics used by threat actors, we determine where your security is strong and where gaps exist that could lead to a compromise.

Wireless Network Penetration

Evaluates the security of your wireless network infrastructure and assesses your compliance. Risks can come from improperly secured infrastructure, rogue access points and wireless clients themselves.

What Does it Help You Answer?
Wireless Network Testing will help identify what wireless devices are accessing your network, if there are any rogue access points and how secure your Wi-Fi infrastructure is.

Wardialing

Wardialing probes the simplest of network devices — your faxes and modems — which are accessible through traditional telephone carrier connections and vulnerable to phone auto-dialer attacks. Mimicking real-world auto-dialer threats, wardialing seeks to identify, gather information and test vulnerabilities of your modem and fax devices.

What Does it Help You Answer?
Learn where an attacker might gain access privileges to the modem-enabled systems of your organization.

Red Team

Red Team Tests simulate cyber attacks against your organization to clearly understand vulnerabilities across all security areas. 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.

Red Team testing differs from standard Technical Testing by using a combination of attacks that combine various techniques to avoid detection and prevention. They include real-world attack goals customized to simulate the business impact this type of attack would have on your organization. Red Team Tests are covert attack methods that try to defeat existing security devices.

What Does it Help You Answer?
Simulated cyber attacks are goal based and aim to find small gaps in security that real-world attackers could exploit. Test the capabilities of your organization against physical, social, email, phone and other network and application cyber attacks to learn the response to an attack. Examples of advanced techniques and blended threats that will increase security awareness and help improve your readiness for a cyber attack.

Summary

Technical Tests are designed to cover specific services. Each security test has its own objectives and acceptable levels of risk. There is not an individual technique that provides a comprehensive picture of an organization's security when executed alone. SecureWorks 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

SecureWorks provides an early warning system for evolving cyber threats, enabling organizations to prevent, detect, rapidly respond to and predict cyber attacks. Combining unparalleled visibility into the global threat landscape and powered by the Counter Threat Platform – our advanced data analytics and insights engine – SecureWorks minimizes risk and delivers actionable, intelligence-driven security solutions for clients around the world.

より詳細な内容に関しては下記のメールアドレスにご連絡ください
SWRX_PreSales@Dell.com
代表03-6893-2317
www.secureworks.jp/
SecureWorks Japan株式会社