Penetration Testing Services and Solutions

Let Telos discover your vulnerabilities before someone else does.

- Discover and document hidden vulnerabilities
- High success rates ensure we uncover the problems you need to know about
- Experience and results for a firm fixed price
- 25 years' service to sensitive government and commercial customers

This is one test you may *want* to fail.

You know your systems and applications are vulnerable. What you don't know – and what you *need* to know – is where those vulnerabilities are and how much risk they pose to your organization.

End the mystery and relieve the anxiety by calling Telos® Corporation.

Telos offers the full range of penetration testing services and solutions that can give you the insights you need. We can help protect you from security breaches that will cost you time and money, bring sanctions and embarrassment down on your organization, and even threaten national security.

Telos has offered cybersecurity and information assurance services for more than two decades. We've conducted cost-effective penetration tests for high-profile federal and commercial customers for more than 10 years. Many of our customers contract with us for annual testing *precisely* because they can count on us to uncover the critical yet hidden issues they need to know about.

You might want or need a penetration test if...

- *You realize that being "patched" or "compliant" no longer means "secure" and you want to uncover any hidden or undiscovered threats to your IT environment*
- *You suspect (or know) that you've been hacked and want to test for any further vulnerabilities to avoid future breaches*
- *You're in a federal agency or regulated industry (for example, financial services or healthcare) in which a regulatory body or governing standards require a penetration test for compliance*
- *You're a software developer or cloud service provider that needs to verify the security of your application (or you have a regulated client that requires it)*

The Telos Difference: Experience and Results for a Firm Fixed Price.

Telos offers the skills, capabilities, and background that combine to make a formidable "enemy" when it comes to testing your systems. With Telos, you benefit from:

High success rates. Telos personnel go to extra lengths to uncover gaps in your security, often revealing obscure vulnerabilities that even the developers of your applications aren't aware of. Since the point of a penetration test is to uncover these kinds of problems in order to help protect your company, it only makes sense to turn to the company that can find more of them faster.

Ongoing relationships with high-assurance, high-security customers. Our customers are among the most security-conscious government and commercial organizations in the world. They return to us year after year – in many cases, for more than a decade – to get the in-depth penetration testing they know they need to stay vigilant in the face of increasing and ongoing threats.

Personnel who are trustworthy, cleared, credentialed, and trained. Because you're asking us to break into the inner-most recesses of your IT systems, you need the assurance that our personnel can be trusted and won't make mistakes. Many of our personnel are certified ethical hackers (CEHs) or have other certification such as Offensive Security Certified Professional (OSCP) or CISSPs. We have a strong commitment to cross-training our personnel so they can handle the full scope of cyber-related tasks including white-hat hacking, vulnerability analysis, assessment and authorization (A&A), and others.

A firm fixed price (FFP) with a guaranteed level of effort. We establish up-front the level of effort involved in your penetration test, including the level of analysis that will be expended. This gives you a clear understanding of the costs involved going into the testing process. You'll be pleasantly surprised how cost-effective a Telos penetration test can be.

The Telos Methodology

Our experts don't just run a few automated scans and hand you a canned report. Each Telos penetration test is a hand-crafted and thoroughly executed assault on your systems and applications. Our goal: to reveal any hidden threats and vulnerabilities so you can take action to address them. Our methodology includes:

Planning and execution by highly skilled cybersecurity experts. Telos penetration testers run a full series of hand-crafted simulated attacks against your systems and applications. We view your systems the way an intruder would – anything from a teen thrill-hacker to malicious assaults by highly skilled adversaries. Our personnel can quickly identify the most likely vectors for attacks.

A firmly established level of effort. Our methodology includes a clear understanding of which assets are within the evaluation boundary. This level of effort can be correlated to the importance of the systems, the system owner's risk aversion, or the anticipated motivation of adversaries.

Strict rules of engagement. We establish a strong, concise document signed by both parties that establishes the ground rules for your engagement, including when and where we will be testing, which systems we're attacking, start and stop rules, and other guidelines for our mutual protection and security.

Emergency notifications. Prior to the onset of testing, we determine when a customer should be immediately notified of an issue. For instance, if a critical asset has been compromised through our efforts, we can immediately notify you so that a remediation can be put into place now, as opposed to waiting for our report findings.

The right tools for the job. Our tests always have humans behind them, but the right tools can uncover common problems and expedite the entire process. Using a full complement of commercial and open-systems tools to map and gather information about the intended targets, we collect information regarding open ports and services, versioning, routing, and other parameters.

Think you're too small to be hacked? Think again.

A common myth is that "we're too small for anyone to be interested in hacking us." Actually, small and medium-sized enterprises make the most enticing targets for cyber attacks. Why?

Because the bad guys assume these organizations pay less attention to cybersecurity and have fewer resources to put toward the problem. Grabbing relatively modest assets from dozens of small businesses can be easier and more rewarding than the effort involved in making a major haul from a large enterprise.

More importantly, small and medium organizations are often integrated with the systems and networks of larger partners and customers. Bad actors can take advantage of smaller targets in order to breach those more enticing targets. Protect yourself and your partners and customers by letting Telos discover those vulnerabilities first.

Thoroughly researching your systems. Just as burglars and con artists do, we begin by "casing the joint" – researching your systems and applications for known and unknown vulnerabilities as a starting point for our investigations. (A lot of this information is posted and shared in unsavory digital neighborhoods; places we'll go so you won't have to.)

Tool usage and development has been a part of our assessment and authorization practice for over 20 years. Tools that we are proficient in and have successfully used during our penetration test efforts include:

- AppDetective™
- AppScan®
- Burp Suite
- CORE Impact®
- Metasploit® Framework
- Nessus®
- Nikto
- Nmap
- Retina
- w3af
- WebInspect
- WebScarab (or similar proxy technology)

Thoroughly researching your users. We also research your users through publicly available sources such as social networking sites, online trade journals, and others. There we can gather clues about potential usernames, passwords, roles-based privileges, and other information that's useful for "breaking and entering." (Sounds scary, right? It is. But that's what the bad guys do. And you *want* us thinking and acting like bad guys.)

Hand-crafted penetration attempts. Utilizing the results of the tools and the research, Telos analysts conduct hand-crafted penetration attempts to determine areas of weakness. These often focus on Web-based applications, as they are the leading area of weakness within systems. We check for issues such as cross-site scripting, database injection, or other possible compromise vectors.

Thoroughly documented results. Documenting the results of all major penetration attempt vectors, Telos prepares and delivers a report detailing the types of tests that were attempted, the status of their success or failure, any discovered issues and the resultant risks (sorted by priority), and suggested remediation efforts. In order to address your comments and feedback, we may provide draft and final versions of the report.

Our methodology is also consistent with guidance from external organizations such as OWASP (Open Web Applications Security Project) and federal guidelines such as those found in *GSA IT Security Procedural Guide: Conducting Penetration Test Exercises.*

When the Testing Is Done.

Software assurance to address application problems before they begin. A powerful complement to our penetration-testing services is our application software assurance (SwA) services. The most common vulnerabilities that allow unauthorized access to your systems are application design flaws, configuration errors, and software bugs that appear during development and implementation. Telos SwA personnel can provide the consulting services and solutions to help you avoid such problems in the systems you develop in-house or acquire from a commercial source.

Cybersecurity services for ongoing IT security. Another complement is our cybersecurity services, which we provide on a consulting and a managed on-site basis. We offer security policy and operational procedure development, cybersecurity engineering and operations, incident management and response, and assessment and authorization (A&A) services to ensure the ongoing security posture of your IT environment.

Get Started Now Discovering and Fixing the Threats to Your IT Environment.

There's an old saying: "The best time to plant a tree is 20 years ago. The second-best time is today." There's no better time than now to start uncovering and addressing the vulnerabilities that can cause no end of expense, embarrassment, and litigation for your organization.

It's easy to get started and costs less than you probably think.

So please contact us. *Today.*

800.70.TELOS (800.708.3567)

info@telos.com

www.telos.com/learn-more/