SecurityScorecard

Penetration Testing

Seek out exploitable issues before an attacker does

Breaches and ransomware attacks continue to be top headline news. The sophistication of adversaries combined with an increasing attack surface leaves security teams inundated with more cyber risks than ever before.

Understanding how your organization fares against skilled adversaries—and validating your security defenses against real world threats and risks that can lead to compromise—is a step toward achieving cyber resilience.

SecurityScorecard's Penetration Testing service tests the effectiveness of your security controls while achieving compliance and protecting your brand. Thinking offensively by using simulated cyber attack strategies and tools designed to access or exploit your computer systems, networks, websites, and applications is the approach to building stronger defenses.

Our team of elite ethical hackers with decades of real-world experience yields critical insight into potential exploits, identifying vulnerabilities that are often difficult or impossible to detect with traditional scanning software.

Three Benefits of Penetration Testing

VALIDATE SECURITY EFFECTIVENESS

A penetration test validates your security controls, including whether your people, processes, and technology are working as expected, showing ROI on your security investment.

STRONGER CYBER DEFENSES

Consistently performing regular penetration tests is a proactive approach to exposing real-world risks of compromise with a clearly defined remediation roadmap.

ACHIEVE COMPLIANCE

Satisfy compliance with regulatory standards including PCI DSS, HIPAA, FINRA, SOC 2, and FFIEC and requirements from some cyber insurance in order to secure coverage.

Custom Testing to Fit Your Business Needs

CLOUD TESTING

Our expert team excels at navigating the security assessment peculiarities of a shared provider tenant model. Whether you deploy to IaaS, PaaS, or SaaS, we will work with you and your provider to identify and assess relevant layers in scope.

APPLICATION TESTING

Tests are expertly designed to detect information security vulnerabilities within computer software— including web-based applications, bespoke software applications, Linux, Windows, and Mac software, databases, mobile operating systems and apps, and other programs.

WEBSITE TESTING

Our seasoned penetration testers can identify security flaws within your website or web application software by simulating an attack. As a result, we are able to thoroughly test your website for SQL injections, cross-site scripting vulnerabilities, server configuration problems, sensitive data leaks, and other weaknesses in your configuration.

HYBRID TESTING MODEL

We offer time- or subscription-based, cost-effective models. Our hybrid approach integrates automation with manual testing by SecurityScorecard's application security experts. We offer scalability, cost effectiveness, and very high quality.

Identify your weak spots before a hacker does, including:

1. Higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a customized sequence

2. Magnitude of potential business and operational impacts of a successful attack

3. Feasibility of a customized set of attack vectors

4. Ability of your network defenders to detect and respond to an attack

5. Leveraging penetration testing with Forensic Analysis post security incidents

SCALE YOUR CYBER DEFENSES

Speak to a Subject Matter Expert today to learn more about Penetration Testing.

Create your **FREE** account today, and enable your security teams to stay ahead of important security strategy questions.

GET STARTED

SecurityScorecard