CYBERSAFE SOLUTIONS

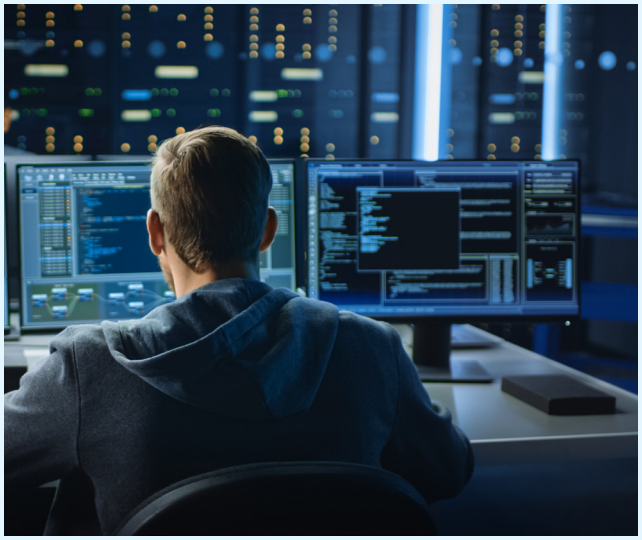
Penetration Testing

Identify risks in your systems Before attackers do

A penetration test simulates the exploitive techniques used by attackers.

This is done to identify security gaps that exist inside your network, information systems, personnel practices, and business processes. From vulnerability assessments to penetration tests to red team engagements, Cybersafe Solutions' technical team has the expertise to customize an assessment plan to fit your needs.

Regardless of which testing level is right for your organization, the value of intelligence cannot be disregarded. Every business operates differently, and not all threats are created equal. An intelligence-driven approach prioritizes what puts your assets most at risk, not what is most at risk for everyone else.



Methodology

The term "penetration test," or pentest for short, has come to cover a wide variety of security testing engagements. At the most basic end of the testing spectrum is an engagement Cybersafe commonly refers to as a "vulnerability scan." Vulnerability scans are quick, simple, and highly automated assessments that use commercial scanning tools against defined targets to check for any known vulnerabilities.

However, vulnerability scans will not find unique security gaps in a particular environment or gaps that require a combination of vulnerabilities to be successful. Penetration tests add the expertise of a seasoned security consultant to find security gaps that a vulnerability scan cannot.

Cybersafe employs an intelligence-driven penetration testing methodology to identify and exploit vulnerabilities in target environments. Cybersafe's security consultants attempt to exploit weaknesses in security controls and combine attacks to penetrate deeper into a target.

Finally, organizations wishing to test their defenses as well as their detection and response capabilities would look for a red team assessment. Red team assessments do anything and everything necessary to achieve the defined objective. They may include additional methodologies such as social engineering or even attempts to bypass physical controls.

Rationale For A Penetration Test

In a "pentest," Cybersafe assumes the role of adversary and attempts to hack into your computer system in order to determine attack vectors, exploitable vulnerabilities, and whether attacks are detectable. A pentest can also be used to test organizations' security policy compliance, their employees' security awareness, and their ability to identify and respond to security incidents. Depending on the scope, the process can include a single web server or a wider overview. The latter features a proactive, in-depth analysis of your aggregate network to find any potential vulnerabilities, including inadequate system and application configurations, hardware and software flaws, and operational weaknesses in the process or technical countermeasures.

Benefits Of Pen Testing

Risk Awareness

The results of your penetration test will arm you with the information and insight to understand where your organization's weaknesses are in order to create a program to minimize those vulnerabilities.

Assurance

Ensure that personnel practices, business processes, deployment of new systems, and changes to your critical applications maintain the level of security that you require.

Compliance

Penetration testing, in some instances, is required by law to maintain compliance with standards such as SOC 2 and PCI DSS.

Be Informed

A penetration test will help you forecast budgetary spending on future plans and create a plan to improve your security program.

Access Cybersafe's senior-level security experts with 20+ years of experience and a state-of-the-art Security Operations Center.

For more information, call
1-800-897-CYBER (2923)

CYBERSAFE SOLUTIONS®