Test Your Cybersecurity Defenses and Determine Your Cyber Attack Vulnerabilities

ADVISORY SERVICES: PENETRATION TESTING

You've taken some security measures to safeguard your healthcare environment; you've likely purchased several IT tools, deployed some software, installed firewall protection, and possibly implemented MFA. The next step is to test everything you've done to see if it will stop a cyber attacker from launching a successful attack against you.

To truly test the security of your environment, you need someone who understands the attacker's perspective, has had success breaching even the most secure networks and environments, and will provide you with actionable results to improve the security of your hospital and, ultimately, your patients.

TYPES OF PENETRATION TESTING

Internal Network Infrastructure Penetration Test:
The testing aims to identify potential gaps in cybersecurity and possible avenues that an attacker could use to breach the overall security of the internal network. The penetration test will employ black-box testing approaches based on the Open-Source Penetration Testing Framework.

External Network Infrastructure Penetration Test:
The testing will attempt to identify vulnerabilities associated with the underlying operating system and applications and identify security misconfigurations or other opportunities which could be used to exploit the system and allow an attacker to gain control of the system and gain access to the internal healthcare infrastructure and networks.

Wireless Security Assessment:
The testing will include an assessment of the wireless network architecture. This will analyze a representative sample of Wireless Access Point (WAP) cybersecurity configurations and patch levels. CloudWave's Sensato team will perform a wireless network survey and assess the overall wireless network associated with your organization.

CloudWave's Sensato Penetration Testing Services

You'll Achieve these Outcomes:

- Identify potential vulnerabilities and security risks
- Identify avenues of exploitation
- Provide remediation and best practices recommendations related to specific findings
- Parties involved will mutually agree on Rules of Engagement specific to each type of test

100 Crowley Drive, Marlborough, MA 01752 877-991-1991 | **gocloudwave.com**

CloudWave

Social Engineering Testing:
CloudWave's Sensato team will work with you to develop a social engineering test combining phishing and direct voice intrusion. The Phishing component of the testing will target a random sample population of end-users and utilize multiple attacks, including highly targeted e-mails considering the current threat landscape.

Our Penetration Testing teams comprise individuals with solid backgrounds in advanced offensive computing and a rich understanding of healthcare information technology. Our penetration testing programs are designed to help identify opportunities for improvement and are intended as a collaborative experience to help evolve our clients' overall cybersecurity knowledge and capabilities.

Our programs can adjust testing severity and are always based on the current threat landscape and the latest attacker Tactics, Techniques, and Procedures (TTP). Each engagement is tailored to your specific requirements and objectives and always respectful of the mutually agreed upon Rules of Engagement (ROE). The Penetration Testing program provides deep insights into findings through custom-written reports and real-time technical debriefings.

PENETRATION TESTING FINDINGS REPORTING

Executive Briefing Report - a high-level overview of completed activities, identified risks and vulnerabilities, and recommended actions.

Detailed Findings Report - includes additional technical details regarding the approaches utilized, vulnerability findings, and remediation recommendations. The report uses a risk stratification scale to quantify the possible threats and vulnerabilities that have been identified.

Findings Remediation Plan - The Findings Remediation Plan is a suggested action plan to address the threats and vulnerabilities in the Detailed Findings report.

Findings Debrief - CloudWave will provide a formal debrief for your organization's management to review the findings. This debriefing allows your management or others to ask questions, clarify the following steps, and gain a deeper understanding of the findings.

Findings Workshop - This planning workshop is meant for technical team members responsible for implementing remediation recommendations. During the session, CloudWave will assist your organization in customizing the Remediation Plan as best as possible to support your organizational abilities and priorities.

To discuss your organization's penetration testing needs, contact us at customersfirst@gocloudwave.com

LEARN MORE AT

gocloudwave.com

CloudWave's Sensato Cybersecurity division is an Information Sharing & Analysis Organization (ISAO) working with government agencies (like CISA, DHS, FDA) to share threat intelligence, evaluate threats, and provide recommendations for action. We have a Memorandum of Understanding (MOU) with the FDA. This means that as a client, you have access to these organizations and threat intelligence.