PREMIER®
Contracted Supplier

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS

Advanced Penetration Testing Services

for Premier Member Organizations

Premier Healthcare recently awarded DynTek a Group Purchasing Agreement for Hardware, Software and Services in the inaugural Cybersecurity Category – Contract Number PP-IT-232

Testing in a Real-World Environment Requires Real-World Hackers

Put your security through a real-world test.

As part of compliance measures and security best practices, healthcare organizations should conduct trusted penetration testing of the effectiveness of security controls in place.

To enable healthcare organizations to uncover all potential threats they may be exposed to, there is a need to inspect further than common scans, surveys and assessments. Using state-of-the-art technologies and tools and military-grade hackers, DynTek simulates and demonstrates the tactics, techniques, and procedures (TTPs) used by real-world adversaries. Our multi-layer attacks include targeted social engineering campaigns, beaconing mechanisms, advanced privilege escalation and exploitation techniques, and much more. And, since we are working with real-world attack scenarios, each campaign and project is customized specifically to each and every customer.

Through our ADVANCED PENETRATION TESTING, we help you:

- Evaluate the current security posture maturity of your organization
- Comply with regulatory standards requirements (such as HIPAA and HITRUST)
- Examine the potential risks you might experience in case of a security breach and a successful external infiltration attempt
- Test the current protection chain integrated with your infrastructure
- Get a realistic overview on how your company will respond to a real-world attack

EXTERNAL

External Penetration Testing

Our External Penetration Test demonstrates the cyber threats an organization is facing by an external offensive factor, as a part of the organizational risk management process.

During this test, our top-notch experts will try to infiltrate in the internal organization infrastructure from the publicly accessed internet while being remote, unauthenticated, unauthorized (IT-wise) and undetected.

This test offers precise insights about the external exposure of the organization's confidential information and internal data via the IT infrastructure, exposed systems and data files while demonstrating which security breach could eventually be used by a malicious source.

INTERNAL

Internal Penetration Testing

The Internal Penetration test will target the organization's infrastructure; the entire Information Technology (IT) environment — the domain controllers, databases, mailing systems, network equipment, and more.

Our test intensifies common passive activities and exploits vulnerabilities to prove (or disprove) real-world attack vectors and scenarios.

AN ACTION PLAN

At the conclusion of our engagement, DynTek will provide written documentation of the approach, findings and recommendations associated with the project to include:

- A detailed listing of the intelligence gathered, and the reconnaissance issued on each of the services
- A comprehensive documentation of the path that led the security expert to exhibit the findings
- Solid evidences supporting the stated findings

In addition, we provide an effective, efficient, and clear remediation plan divided to Tactical (immediate/short-term) and Strategic (long-term) phases, to assist the CISO prioritizing the process.

About DynTek

DynTek helps design a healthcare security system using an “assumed breach” approach focused on identity and access — the pillars of a dynamic, effective threat defense. This type of security architecture is built around the key elements of the network — endpoints, systems, and data. The DynTek security offering includes legal and regulatory guidance, risk management, data security, security solutions, threat management, and managed service offerings.

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS