InfoSight's Penetration Testing

InfoSight's Penetration Testing services reduce the risk of a successful attacks before they occur.With over two decades of experience in security, compliance and risk management, our experts work as ethical hackers to identify security issues beyond the capability of automated tools and cursory assessments.

Overview - The Challenge

Today all organizations have become targets of bad actors and cybercriminals. As a result, regular penetration testing is critical to ensure security in the Cloud and the Datacenter. We understand how difficult it can be to find a partner that understands your industry specific operating environments and compliance requirements, and as a result testing is not goal-oriented and lacks the outcome needed to ensure robust security. That's where we come in!

Key Service Features

- **Reduce your overall attack surface**
- **Evaluate specific environments for real-world readiness**
- **Identify security issues beyond the capability of automated tools**
- **Prioritize your risks and quickly take the right preventative measures**

How We Solve It

We mimic the tactics and techniques of a real-world attackers by:

1. Conducting an external attack surface evaluation and vulnerability scanning of any external facing attack vectors in the Cloud and Datacenter.
2. Conducting Email Phishing, Telephone pretexting and other social engineering tactics to gather user credentials.
3. Attempting to gain access remotely which may include any externally facing wi-fi
4. Attempting to use any credentials we may have acquired to gain system access then promoting credentials to admin levels.
5. If onsite we will try to gain entry into physical facilities using various tactics.
6. After all black-box covert attempts are conducted we use permitted and privileged access to perform comprehensive network testing.
7. After testing is complete, we deliver both an Executive Summary and detailed Technical Remediation Report during your Exit Interview.
8. We will also continue to support you throughout the remediation process by making our team available to answers questions, and provide additional context and insight.

InfoSight®
Bringing the Future into Focus®

305-828-1003
info@infosightinc.com
www.infosightinc.com

InfoSight's Goal Oriented Security Assessments

Service Descriptions

Vulnerability & Penetration Testing - Consists of a multi-disciplinary, multi-faceted review of the organization’s systems which identifies vulnerabilities outside and inside the network and attempts to exploit any vulnerabilities in the same way a malicious actor would.

Threat Hunting - Searching for indicators of compromise in an IT environment that the potential presence of malicious activity, usually before any alerts are generated by security devices or systems. To remain ahead of the next intrusion attempt, we use threat intelligence and custom tools to identify threats and thereby automate searches focused on thwarting a skilled human attacker.

Red Team/Blue Team Testing - ·Designed to test an organization’s readiness to detect, withstand and respond to a targeted attack. The red team’s goal is to find and exploit any identifiable weaknesses in the organization’s security as the blue team works to defend the organization by finding and patching vulnerabilities and responding to successful breaches.

Social Engineering - Encompasses a comprehensive set of security tests conducted to establish the current state of security awareness among the organization’s personnel. It identifies vulnerabilities within human resources as well as gaps in awareness training. Social engineering assessments are performed against electronic messaging, telephony, and other onsite and human vectors.

Web & Mobile Security & API - Involves the security testing of web, mobile and software application interfaces to identify privilege escalation, authorization creep, and security controls bypass. It includes a detailed report outlining discovered vulnerabilities and remediation steps.

Why InfoSight

- 24x7x365 US-Based SOC
- SOC 2 Certified
- 25+ years of proven outcomes
- Offering full threat lifecycle services from Detection and Response to Mitigation and Remediation
- Flexible pricing models that can be 24x7, 8x5, or off-peak 7pm to 7am only coverage
- Solutions are Regulatory Compliance driven (GLBA, PCI, HIPAA, NERC, AWWA, etc.)
- Offering Services for the Data Center, Cloud and Hybrid environments
- Certified Experts (CISSP, CISA, CEH, OSCP, AWS, AWWA, etc.)