InfoSight®
Bringing the Future into Focus®

877-577-9703
info@infosightinc.com
www.infosightinc.com

Vulnerability & Cybersecurity Assessments

InfoSight's Vulnerability & Cybersecurity Assessments reduce the risk of 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 assessments/tests. As cyberattacks continue to rise everyday it is important to perform penetration tests regularly.

Key Features

- **Reduce the risk of a successful attack before it occurs**
- **Identify security issues beyond the capability of automated tools & assessments/tests**
- **Go beyond typical penetration testing and target mission critical applications and operations**
- **Prioritize your risk and quickly take the right remedial and preventative measures**

Overview - The Challenge

Today all organizations across every industry face the risks of cybercriminals and breached networks. Often times organizations lack the cybersecurity budget and internal expertise required to analyze all security events while doing day to day activities. We understand it is difficult to find a trustworthy third party that understands your industry specific compliance as well as your overall security system. That's where we come in.

How We Solve It

InfoSight's experienced engineers test your network manually to identify the extent your system could currently be compromised by a real-life attacker. Our vulnerability and security assessments can be used to test your security policy compliance, the effectiveness of your employee security awareness training and your organization's ability to identify and respond to security incidents.

InfoSight provides remediation reports going in-depth on steps to take your overall security to the next level. Our team can act as an extension of your team to assist in the remediation process to ensure cybersecurity right away.

The Outcome

InfoSight's security engineers conduct **comprehensive vulnerability assessments** with extensive knowledge of the most current attack vectors, no matter the network types which includes On-Premise Data Centers, Cloud or Hybrid environments. Following our security assessments, we will help you understand and prioritize the most critical threats on your network along with managing the appropriate response to lower your overall threat level.

InfoSight®
Bringing the Future into Focus®

877-577-9703
info@infosightinc.com
www.infosightinc.com

Vulnerability & Cybersecurity Assessments

A Deeper Dive into InfoSight's Vulnerability & Cybersecurity Assessment Services

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.

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.

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.

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.

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.

Why InfoSight

- 24x7x365 US-Based SOC/NOC
- SOC 2 Certified
- Complete MSSP Services that include Monitoring, Real-Time Threat Analysis, Mitigation/Remediation, Alerting, Reporting and Device Management
- Flexible pricing models that can be 24x7, 8x5, or off-peak 7pm to 7am only coverage
- 22+ years Regulatory Compliance experience (GLBA, PCI, HIPAA, NERC, AWWA, etc.)
- Certified Experts (CISSP, CISA, CEH, OSCP, AWS, AWWA, etc.)
- Managed Services for On-premise Data center, Cloud and Hybrid environments