Goal Oriented Security Assessments

What You Need To Know

For any organization to achieve the level of protection it needs for its critical networks, security needs to grow from a collection of disparate technologies, policies and practices into an effective business process.

Every organization, from banking, to healthcare and public utilities, utilizes different systems with different functionalities. Securing information, systems and networks is a complex task that can be achieved by understanding of business requirements, employing the right technologies and people, and most importantly, creating a cybersecurity plan.

Today, every business needs to implement an in-depth cybersecurity plan to help protect its systems and data against threats. Successful cybersecurity plans start with a goal-oriented security assessment tailored to their unique environments.

Key Differentiators

With 22 years of experience and certifications in CEH, CISSP, CHFI, CISA, CGEIT, and more, we specialize in Security, Compliance and Risk Management. We deliver analyst prepared reports, NOT stock canned output from scan tools. We provide:

- **Two reports –** An Executive Level Summary Report with graphs of priority findings, a composite security risk score, and a summary of the findings; and a Detailed Technical Remediation Report that outlines vulnerability severity, host affected, remediation required and sources for remediation.

- **Post-assessment,** we are available to answer any questions regarding remediation or network hardening to ensure maximum benefits.

Key Benefits

- ✓ 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

Service Description

Our goal-oriented penetration testing, vulnerability assessment, and threat hunting services provide a complete evaluation and detailed view of your organization's security posture. The goal is to proactively identify existing IT vulnerabilities and threats, test how far a potential exploit can compromise the network and allow you to remediate the vulnerabilities before a malicious actor exploits them.

We can also test the organization's security policy compliance, the effectiveness of its employee security awareness training program, as well as the organization's ability to identify and respond to cybersecurity incidents.

Available services include:

- **Vulnerability & Penetration Testing**
- **Red Team/Blue Team**
- **Threat Hunting**
- **Web, Mobile & API**
- **Social Engineering**
- **Physical Security**
- **Industrial Security and IoT**

14100 Palmetto Frontage Rd
Suite 310
Miami Lakes FL 33016

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

Goal Oriented Security Assessments

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 Exercises are 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 amounts to 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.

Physical Security involves a far-reaching assortment of security tests conducted against the organization's physical plant to determine the efficacy of physical security design within the company's offices, buildings, and other properties. It may include Clean Desktop evaluations, dumpster diving and document destruction testing.

Industrial Security & IoT Security Services include an expansive group of technical tests that inspect the security controls of industrial installations, resources, utilities, materials, information and IoT applications that are essential to safeguarding it from unauthorized access, service interruption or damage.

Cyber Security & Compliance Reviews are designed to help reduce the compliance burden and improve an organization's overall information security posture. The program covers most industries and requirements including NERC, GLBA, HIPAA, PCI, etc. Compliance can be a legal obstacle course that requires a professional to navigate safely, which is why many enlist the help of an experienced and knowledgeable third party like InfoSight.

14100 Palmetto Frontage Rd
Suite 310
Miami Lakes FL 33016

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