InfoSight®
www.infosightinc.com

PENETRATION TESTING

InfoSight's Penetration Testing services reduce the risk of successful cyberattacks significantly.

305-828-1003 info@infosightinc.com

A Penetration Test is the process of using a number of technology tools attempting to exploit any vulnerabilities identified during the vulnerability assessment. The goal of this test is to mimic a potential attacker attempting to gain access to your organization's confidential systems and data.

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

The Challenge

Today all organizations face the risks of ransomware attacks and AI-powered cyberattacks. Staying ahead of bad actors often seems like a losing battle. Many organizations lack the cybersecurity budget and internal resources required to assess all vulnerabilities at a pace that keeps up with new threats. That's where we come in!

How We Solve It

Our assessments are goal-oriented and designed to test not just your Network, but also your Applications, APIs, Mobile Apps, Web Apps and SCADA/ICS Networks .We mimic the tactics and techniques of a real-world attackers by leveraging AI-driven toolsets to simulate sophisticated attack vectors. Our reports are comprehensive, providing both in-depth technical reports that include videos of successful exploits, and remediation instructions. Additionally, executive-level reporting. Is provided to suit your C-Suite, BOD, and 3rd party audit audiences.

The Outcome

Our comprehensive assessments leverage over 2 decades of experience and knowledge of the most current attack vectors including AI, to deliver the most actionable data. Our personalized approach will help quantify your cyber risk, prioritize the most critical threats, and create a continuous threat exposure management roadmap.

InfoSight®
www.infosightinc.com

PENETRATION TESTING

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.

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.

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.

Our Approach

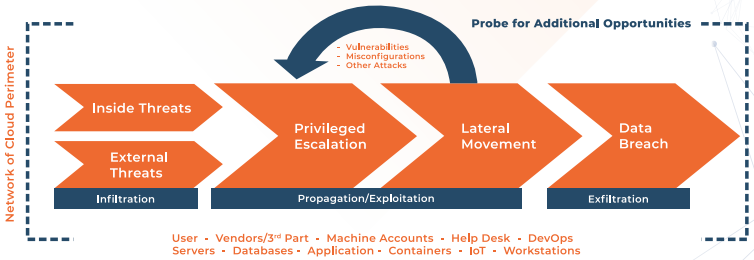
We first determine the feasibility of a particular set of attack vectors which can include logical, social and physical.

Next, we identify vulnerabilities that result from a combination of lower-effort vulnerabilities exploited in a particular sequence.

Then, we search for vulnerabilities that may be difficult to detect with automated tools.

Thereafter, we attempt exploits to gain access which will then allow us to move laterally.

Finally, we prove written and video evidence to support your investment in security personnel and technology.



Our Methodology

Our methodology is built on real world hacking strategies resulting in practical recommendations to strengthen your security posture.

Attack Surfaces – Targets are identified and prioritized within the scope of the assessment.

Vulnerability Assessment – Based on the data collected, security weakness in the target system can be identified.

Detection Testing – Testing of your organization's ability to detect and mitigate real threats from the perimeter to the endpoint.

Obtain Access – Obtain a foothold to initiate a connection and expand access to obtain credentials and strengthen hold.

Infiltrate & Collect – Utilize obtained credentials to collect confidential data while remaining undetected.

Exploitation & Execution – This being the crucial step, it requires special skills and techniques to launch attack on target system.

Digital reports are delivered via our proprietary **Mitigator Vulnerability and Threat Management Platform.** Reports can be exported in multiple formats and printed.

MITIGATOR™
VULNERABILITY & THREAT MANAGER