InfoSight®
www.infosightinc.com

VULNERABILITY & CYBERSECURITY ASSESSMENTS

InfoSight's Vulnerability & Cybersecurity Assessments reduce the risk of successful cyberattacks before they occur.

305-828-1003 info@infosightinc.com

With over two decades of experience in security, compliance and risk management, our security assessors work hard to identify security issues beyond the capability of automated tools. Our goal-oriented approach enables us to provide an accurate assessment of your current security posture.

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

Overview - 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 expert security assessors test your network to identify vulnerabilities that could be exploited by a bad actor. 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, as well as your organization's ability to respond to security incidents. 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

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 your organization's systems to identify vulnerabilities and attempting to exploit them in the same way a malicious actor would.

Red Team/ Blue Team Testing

Designed to test an organization's ability to detect, and respond to a targeted attack. The red team's goal is to find and exploit any identifiable weaknesses in the organization's security. The blue team works to defend the organization by defending attacks and remediating vulnerabilities.

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, SMS, and other attack vectors.

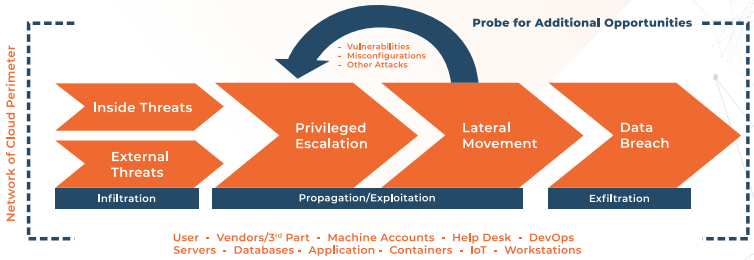
Our Approach & Methodology

Our assessments a are goal-oriented and designed for your specific environment. We will simulate the actions of an actual bad actor by using the same tools, tactics, and techniques.

During the initial Kickoff you can choose from Black, Gray and White box testing. Then, as we move into white-box testing, both credentialed and non-credentialed testing is available.

Our experienced security assessors use both off-the-shelf and custom scripted toolsets to perform reconnaissance and infiltration, and to move laterally with your environment and attempt exploits.

We leverage AI toolsets to create a real-world attack simulation.



Our Deliverables

Mitigator Vulnerability & Threat Manager – Report deliverables are accessed through our proprietary Mitigator platform. Reports and vulnerability data are stored digitally and available for download.

Analyst-prepared Custom Reporting – Our reports are designed with both a Technical and Executive Audience in mind. Our graphical Executive Report contains Critical, High, and Medium findings with a composite risk score.This report is made to share upstream to board, executives, or any 3rd parties – written in language they can understand. The Detailed Technical Report contains all your findings with criticality (CVSS), asset and remediation instructions.

Exit Interview – We'll conduct a formal exit interview to review findings and discuss your remediation plan.

Post Exit Support – that's not where our service stops. We make ourselves available to you should you have any questions regarding remediation.

Rescans & Retests– If you've elected to do a rescan or retesting of findings post remediation, we'll do exactly that and issue an amended final report.