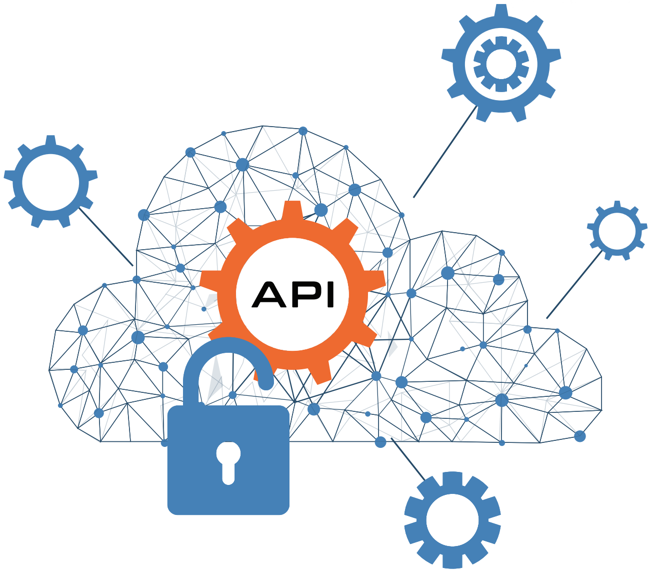
InfoSight®
www.infosightinc.com

API SECURITY ASSESSMENT

305-828-1003 info@infosightinc.com

Overview - The Challenge

APIs have become a prime target for bad actors because many applications are integrated, and utilize open-source code, so you're only as secure as the weakest link in your application supply chain. Weaknesses and flaws in an application's APIs can result in exploitation compromising confidential data. And with large amounts data being exchanged via APIs, it's no surprise they have become a large attack target, and it's gaining momentum.



How We Solve It

Our API Security Assessments assist in identifying underlying security issues with your application by providing a comprehensive review that meets the latest security best practice standards.

The Outcome

Actionable reporting and recommendations that enable your development team, or that of your partners', to secure APIs better!

Bringing the Future into Focus

www.infosightinc.com

Other Assessment Services

Vulnerability & Penetration Testing

Consists of a multi-disciplinary, multi-faceted review of your organization's systems to identify vulnerabilities and attempt 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.

The assessment will cover four main areas.

Injection

An injection code technique will be used to attack web applications, in which malicious statements are inserted into an entry field for execution. Injection is mostly known as an attack vector for websites and APIs but can be used to attack any type of applications.

Gathering

Information Gathering is the most critical step of an application security test. By using public tools (search engines), scanners, sending simple HTTP requests, or specially crafted requests, it is possible to force the application to leak information, e.g., disclosing error messages or revealing the versions and technologies used.

Server

Server security is the protection of information assets that can be accessed on and from a server. Server security is important for any organization that has a public or private API connected to the Internet. It requires a layered defense and is especially important for organizations with customer-facing APIs.

Usage

Usage of weak authentication methods makes it easy for an attacker to intercept credentials, replay them to other hosts, and trick users into providing the credentials to the wrong location.

Recommendations for remedial action will be made at the conclusion of the testing procedure, with the option of additional security testing following post-change.

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