SECURITY ASSESSMENT EXPERTISE

SECURITY INNOVATION

Each language and platform has unique idiosyncrasies, built-in defenses, attack vectors and threats that require a level of customized testing. Matching the tooling and skillset of our engineers to the nature of each software application yields the most accurate results possible. This is of particular importance when it comes to our ability to provide expert remediation recommendations.

Over the years, we've developed expertise in the following areas:

- .NET, J2EE, C/C++, C#, PHP, Python, Ruby on Rails, Scala, objectiveC, HTML5, Web 2.0, Ajax
- Web, mobile, IoT, embedded, thick client, cloud, automotive, database, desktop, native applications
- Linux, Windows, and real-time operating systems
- Amazon AWS and Microsoft Azure

Web Application & Web Services

Web application testing uncovers threats from internal and external users as well as vulnerabilities in web clients, servers, and back-end databases. Making use of proxies, commercial scanners, internally developed tools and scripts, and manual efforts, our team uncovers threats from internal and external users.

We have tested Web applications for technology, e-commerce, marketing, banking, and other business purposes for clients like Discover, Akamai, Credit-Suisse and others.

Mobile

This assessment identifies and mitigates vulnerabilities in mobile applications, devices, and back-end systems. Our experts masquerade as a rogue client a rogue server and routinely bypass client protections.

We have tested mobile banking, e-commerce, and payment systems for organizations like Kronos, HP, Reuters, SAP, Digital Insight, Microsoft and others; as well as major mobile Operating Systems including iOS (iPad/iPhone), Blackberry, Android, Windows Mobile, Symbian, and Windows Phone 7.

Thick Client

Our protocol and binary reverse engineering skills uncover vulnerabilities that elude automation. Leveraging fault-simulation and proprietary technologies, we force thick clients into hostile environments while testing error-handling and boundary condition behavior.

We have tested thick client applications for healthcare, retail, software and more for industry leaders such as Philips Medical, Microsoft, and Sony.

Cloud

Lost control of data is the biggest threat in the cloud. To ensure data is secured both at rest and in transit, we validate that encryption and data security components are implemented properly. We also look for misconfigurations of services that allow authentication and authorization components to be bypassed, and ways to attack bandwidth and storage moles.

We have conducted multiple assessments directly on Amazon Web Service (AWS) and Windows Azure. Additionally, we've tested dozens of applications that run on these infrastructures as well as HP CloudPrint and Teradata's Active Data Warehouse Private Cloud.

IoT & Embedded Devices

Our strong crypto, embedded architecture, and software analysis skills are put to the test on set-top boxes, personal entertainment devices, automotive communication systems and transactional kiosks.

Our clients in the embedded space include iRobot, Kronos, TIVO, Massachusetts District Attorney's Office, US DoT and US Courts.

Automotive

Our security experts analyze security features, identify weaknesses, and enable effective implementation of automotive software applications. Specialties include code review, penetration testing, and design review for both embedded and OTA (over-the-air) software systems.

Automotive industry clients include Harley Davidson, SiriusXM, Harmon, GM, and more.