Offensive security service

Tailored engagements, white glove service

Comprehensive service

One size does not fit all. Focus your attention on the areas that matter most to you.
Our extensive offerings reflect our expert capabilities with a personal touch. Services include:

Service	Category	Explanation
Expert reconnaissance	Common	Our reconnaissance leverages both proprietary and OSINT tools to understand perimeter security methods and potential vulnerabilities
Attack vector ID	Common	After reconnaissance, targets are selected due to identified or likely vulnerabilities
Targeted exploits	Common	Exploit attempts are deployed in a targeted manner at individual targets based on their attributes
Prioritized remediation	Common	Penetration tests include prioritized vulnerabilities with remediation recommendations
Web app testing	Common	Manual creative testing in conjunction with automatic testing methods are used to test the security of a web application against simulated real world attack methods
Network testing	Common	Manual creative testing in conjunction with automatic testing methods are used to test the security of a network against simulated real world attack methods
0-day hunting	Advanced	Testing for novel (never before uncovered or patched) vulnerabilities to exploit
Fuzzing	Advanced	Automatic bug finding using malformed data injection can be performed against proprietary or 3rd party targets for 0-day discovery. Note: we do not need source code to conduct fuzzing.

Reverse engineering	Advanced	Analysis of either a custom executable built by your organization to understand it and find vulnerabilities in it or an RE-based 0-day analysis on commonly used tools within your environment to ensure they are free of vulnerabilities
Distributed denial of service	Advanced	Attack that is launched to overwhelm the targeted server, service, or network with an influx of traffic
Custom malware	Advanced	Custom targeted malware built to simulate a real-world attack
Antivirus stress testing	Advanced	Custom assessment of antivirus ability to detect and prevent attacks
Internet of things	Specialized	Connected device attack simulation (e.g. wireless-enabled printers, coffee pots, etc.)
Social engineering	Specialized	Human-based attack simulation, leveraging holes in security of human infrastructure to gain system access (e.g. requests to IT helpdesk, etc.)
Phishing	Specialized	Email attack simulation with the intention to have users click on a “malicious” link
Mobile device	Specialized	We can analyze an entire device or specific applications, whether custom-built, native, or 3rd party.
Compliance penetration	Specialized	Attack simulation for companies in need of industry-specific compliance testing
Physical penetration	Specialized	Attack simulation where company building access is acquired
Priority fix order recommendation	Action Output	Remediation is categorized in a comprehensive matrix output to prioritize the most urgent and important remediations
Vulnerability severity scoring	Action Output	Vulnerabilities are scored based on the ease of exploitation to an attacker

Vulnerability impact scoring	Action Output	Vulnerabilities are scored based on business impact if an exploitation of an individual vulnerability were to occur
Remediation cost scoring	Action Output	Additional time is given for help with remediation activities, as there would be little point to a test without them. Budgets are limited and a blanket “fix everything” statement is often not realistic. We work with you to understand the costs and benefits of each remediation that we carefully recommend.
Remediation complexity scoring	Action Output	Remediation for found vulnerabilities is scored from a complexity standpoint to guide the remediation scheduling

Ready to learn more about *QOMPLX’s Offensive Security Service*? Contact us today.

+1 (703) 995-4199 | info@QOMPLX.com | www.QOMPLX.com

Why QOMPLX®

QOMPLX is the cloud-native leader in risk analytics. We help organizations make intelligent business decisions and better manage risk through our advanced, proprietary analytics platform. We are the leaders at rapidly ingesting, transforming, and contextualizing la rge, complex, and disparate data sources through our data factory, in order to help organizations better quantify, model, and predict risk in areas like cyber security, insurance, and finance. QOMPLX is headquartered in Tysons, VA with offices in New York, Denver, London, Cambridge, Oxford, and Montevideo. More information about QOMPLX can be found at www.qomplx.com.