Penetration Testing

K logix stands out with our Penetration Testing offerings. We understand your business and technical needs to determine which test is appropriate for your security program. We then customize each test using our thorough methodology and process.

Our expert testers have conducted K logix Penetration Tests for over twelve years. They provide results that address your specific needs and provide insight into a clear overview. Our recommendations are actionable and help move your program maturity and preparedness forward.

K logix Penetration Testing includes:

- External Penetration Test
- Internal Penetration Test
- Application Penetration Test
- Web Application Penetration Test
- Red Team Exercises
- Phishing

12+ years conducting Penetration Tests using the same testers

Highly qualified pen testers using repeatable and thorough methodology

Each test is customized based on the specific business and technical needs of the customer

Testers go above and beyond typical methods – i.e. utilizing dark web, social media, fake phone calls, breach data, etc.

Results tell a clear and concise business-minded story

Recommendations help improve overall security strategy and guide tactical initiatives

	EXTERNAL	INTERNAL	APPLICATION	WEB APPLICATION	WIRELESS
Purpose?	Shows whether people who shouldn't enter your systems can be kept out	Determines whether people already inside your network can access anything they shouldn't be able to	Evaluates vulnerabilities within internally-facing applications or client-side dependency applications	Evaluates vulnerabilities with publicly facing applications	Evaluates publicly accessible wireless infrastructure for configuration oversights and easily exploitable conditions
What is Evaluated?	Externally-facing perimeter security posture	Internal technical security posture	Thick client applications, internal databases, source code, configuration files	SaaS environments, cloud-based deployments, public facing interfaces and APIs	Wirelss infrastructure
Results?	Understanding of how access was gained Understanding of who can get data out once they get inside Improvements on people, process and technology to better secure perimeter security	Weaknesses and vulnerabilities Understanding of how close someone can get to your 'crown jewels' Understanding who can use escalation to get admin access	List of vulnerabilities (typically more serious than web application test)	List of vulnerabilities that are exploitable by unknowable unauthenticated general public	Verification of appropriately secure configurations and identification of exploitable security oversights Understanding how an outsider connected to your wireless can access internal resources

	RED TEAM	PHISHING
Purpose?	Red team simulates scenarios targeting the highest risks to your company to see how your team responds (typically 'no holds barred' using any resources) Done through customized, complex campaigns utilizing all available reconnaissance efforts – phone, dark web, social media	Measures effectiveness of security awareness training program, identifies opportunities for additional training, and measures effectiveness of security protocols Done through customized, complex campaigns utilizing all available reconnaissance efforts – phone, dark web, social media
What is Evaluated?	How readily organization's internal team can respond to 'red team'	Internal technical security posture
Results?	What was expected to happen? What actually happened? What areas of people, process, and technology need to be improved based on the blue team's response to the simulated attack?	Who responded to phishing and in what manner? What additional training is needed to improve in the future? What additional technical mechanisms and preventative controls are needed?