K logix
Be confident.

K logix Security Testing Services

K logix's Security Testing Services offerings empower organizations to gain a clear understanding of posture to proactively reduce risk and improve their programs, services and products. Our outcomes focus on both tactical findings and strategic advancement opportunities.

Our Testing team believes in meeting customers where they are with our flexible, white glove approach. We spend time understanding your organization's business direction and vision, your unique organizational structure, technologies and key information security risks to determine the appropriate testing for your needs.

K logix Testing Offerings

Application and Product Penetration Testing

- Web Application and Web Services API
- Product and Native Applications
- Mobile Applications
- IoT Devices

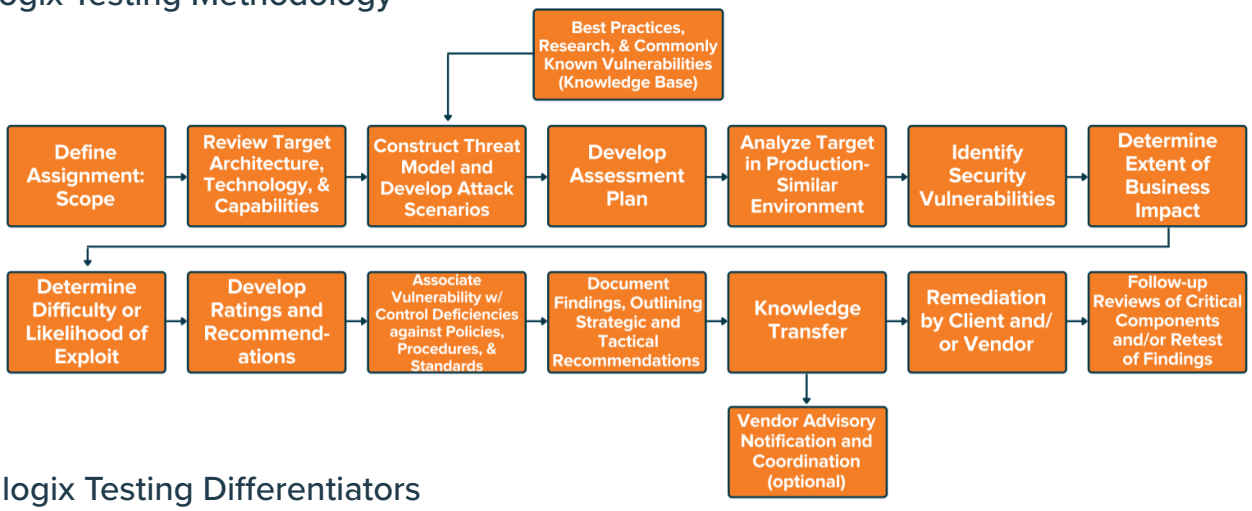
Configuration Review

- Cloud Infrastructure and Services Review

Infrastructure Penetration Testing

- Internal Network
- External Network
- Wireless Network

K logix Testing Methodology



K logix Testing Differentiators

- Deep expertise and threat modeling to craft test plans based on specific customer needs
- Partner with customers to provide long-term value with adaptive testing
- Go beyond a deliverable with actionable recommendations to improve the overall security strategy and guide tactical initiatives
- Coordinate responsible disclosure of vulnerabilities identified in third-party systems or software

K logix
Be confident.

Application and Product Testing

Web Application and Web Services API

- Highlights common web application service vulnerabilities including OWASP Top 10 and beyond
- Identifies vulnerabilities stemming from design, implementation, or deployment weaknesses
- Emphasizes authentication, authorization, and session management
- Evaluates data access layers for potential injection vulnerabilities
- Identifies presentation layer vulnerabilities such as Cross-Site Scripting in application code as well as reliance on 3rd party libraries
- Evaluates code behavior in a production-similar environment to determine effectiveness of web application, web server, and supporting infrastructure security controls
- Evaluates APIs sometimes used by backend components or otherwise not exposed to end-users for consistent authentication, authorization, and data protection practices

Product and Native Applications

- Evaluates consumer, enterprise, and B2B software and hardware for potential risks based on design, implementation, or integration specific threats
- Identifies potential threats from components implemented using unmanaged code (C/C++), with specific focus on memory corruption vulnerabilities which could lead to remote code execution, privilege escalation, or information disclosure
- Analyzes custom protocols as a means of identifying flaws which could lead to compromise of application or system components, or unauthorized access to data
- Evaluates cryptographic implementations for transport layer security and authentication handling

Mobile Application

- Testing focuses on coverage for common application security vulnerabilities which face all application types and other unique aspects associated with mobile applications and mobile device security, including:
  - Lost/stolen device: evaluates risk of credentials, shared secrets, and data stored on mobile device by application
  - Server-side vulnerabilities: performs testing of mobile application supporting APIs for protection associated with authentication and authorization of access to data, and protection of server-side infrastructure based upon implementation
  - Client-side vulnerabilities:
    - Evaluates potential risks associated with custom URL handlers and intents
    - Data protection of application assets
    - Data presentation layer vulnerabilities including Cross-Site Scripting
    - Evaluates mobile device user privacy and permissions associated with custom applications

K logix
Be confident.

Infrastructure Penetration Testing

Internal Network

- Testing focused on internal infrastructure from perspective of compromised system or malicious insider
- Identifies vulnerabilities in internal services with a prioritization on remote code execution, privilege escalation, or unauthorized data access
- Discovers services using default or weak credentials
- Maps internal infrastructure and finds interesting services to evaluate using manual testing techniques
- Analyzes Active Directory groups, trusts, access control lists, and other elements to identify high value systems and users
- Uncovers misconfigurations that may be used to gain pivot points to gain deeper access into client environment

Wireless

- Identifies wireless networks, including hidden or cloaked networks
- Discovers authentication and encryption standards (WPA/WPA2, WEP) in use
- Attempts to intercept communications to recover pre-shared keys
- Conducts “Evil Twin” attacks against wireless clients
- Evaluates access controls between guest networks and corporate networks
- Attempts to bypass Network Access Control (NAC) and MAC based filtering

External Network

- Testing focused on infrastructure accessible to the Internet
- Identifies vulnerabilities in public services
- Leverages Open Source Intelligence (OSINT) techniques to better understand the target
- Uncovers misconfigurations that may be used to gain footholds into client environment
- Fingerprints exposed systems and services
- Develops threat models of exposed IP enabled services
- Exploits identified vulnerabilities

K logix

Be confident.

Configuration Review

Cloud Infrastructure and Services Review- Amazon Web Services

- Identifies and exploits application and services running on EC2 instances
- Discovers and compromises AWS IAM keys
- Attempts privilege escalation through misconfigured IAM policies
- Exploits S3 bucket configuration and permissions flaws
- Obtains private-cloud access through exploiting Lambda functions
- Gap analysis of cloud configurations and security best practices

Cloud Infrastructure and Services Review- Microsoft Azure

- Attempts privilege escalation through misconfigured IAM policies
- Identifies Azure AD-Connect workflow issues
- Exploits S3 bucket/Azure blob configuration and permissions flaws
- Finds compromising AWS/Azure IAM keys
- Gap analysis of AWS and Azure cloud configurations and security best practices
- Identification and exploitation of application and services running on EC2/Azure VM instances
- Obtains private-cloud access through exploiting AWS

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.