DATA SHEET

iQ3 Cyber Security Advisory Services

Network Penetration Testing Services (External or Internal)

iQ3 Penetration Testing Services enables our team to stimulate both internal and external real-world attacks on your environment, utilising recognised methods including black box, white box and grey box testing. The purpose of external testing is to compromise the target network, identifying any vulnerabilities and exploits in order to streamline the remediation process. In many cases, external systems when compromised become well known public knowledge which in many cases can lead to reputational damage.

Web Application Penetration Testing

iQ3's team of highly-skilled testers utilise industry-standard proven processes to achieve Web Application Penetration Testing providing consistency, certainty and confidence in your applications. Our service combines automated tools to scan applications in addition to manual web application penetration testing, to maximise accuracy and identify potential gaps which automation may overlook. iQ3's highly comprehensive security services deliver in-depth analysis, identifying open source vulnerabilities which are not compliant to OWASP Top 10.

Social Engineering Penetration Testing

Threat actors are often more successful at infiltrating a network through social engineering. To help you prepare for this kind of exploitation, iQ3 uses a combination of human and electronic methods to simulate an attack. Human-based attacks consist of impersonating a trusted individual in an attempt to access specific information, compromising the client infrastructure. Electronic-based attacks utilise complex phishing attacks which passively source organisational public resources, creating a profile of your business in order to inform hackers of your most sensitive vulnerabilities.

Vulnerability and Security Assessment

iQ3 security methodology follows international best practices and a structured framework of assessment to provide detailed reports and improvement recommendations to businesses. We will work closely with your management and technical teams to align the focus of the security work with business priorities and produce highly relevant reports to organisations. iQ3 will complete a thorough assessment of your organisation's infrastructure to identify vulnerabilities within your organisation.

Key Deliverables:

- Detailed summary of results and description of all key findings
- Classified report weighting vulnerabilities according to ease of exploitation and risk-level
- Actionable recommendations to eliminate revealed security gaps

Email sales@iq3.com.au to receive a copy of our iQ3 *Sample Penetration Testing Report*