KPMG Enterprise

Technical Security Assessments

At **High Growth Ventures**, we support people with world changing ideas. Our products, tools and programs are designed to help founders achieve sustained high performance.

Data breaches and cybercrime are at all-time highs with most businesses facing the inevitability of a cyber-attack. We believe cyber security should be at the core of every tech process within your business.

Together with our cyber team, you can take proactive action to ensure your business is continuously enforcing security into your product and services and gain an understanding of where you are most at risk.

Key benefits

- ✓ An objective and independent technical assessment of your technology product and services. Measure your risk and evaluate consequences and impact of an attack on your systems and business operations.
- ✓ Discover and guide remediation of cyber risks before they adversely impact your systems and data and helping you mitigate potential financial and reputation damage to your business
- ✓ Improved understanding of the effectiveness of the security controls designed and deployed to protect your digital product and services and identifying vulnerabilities that may impact operations.
- ✓ Give confidence to founder/business owners, management, investors and other stakeholders through validation of security posture of your product.
- ✓ Clear recommendations to address identified critical security issues in your product and business.
- ✓ Guidance on the appropriate industry best practice mitigating controls for your business.

Why it's important?

Our research shows that 68% of CEOs viewed customer data protection as one of their most important personal responsibilities. Data breaches bring huge reputational damage and often have a lasting negative impact on a business.

KPMG's Penetration Testing service uncovers technical security issues, reduces uncertainty in your business, increases agility and helps to turn risk into your advantage.

Our Penetration Testing service is a controlled simulated real world assessment that technically evaluate the security posture of your systems, infrastructure and applications for both on premise or in the cloud. Through this service, we will help you identify and assess the technical risks of security vulnerabilities that may will negatively impact your startup financially and reputationally. We help you understand the impact of these vulnerabilities and allow you to prioritize the remediation effort base on a combination of technical and business risk.

Our tailored testing can incorporate black, white or grey box penetration testing across key pillars of:

Cloud security

Network security

Web and mobile application security

Mobile security

Methodology

A methodical approach is taken to identify information, systems and services which may facilitate a threat agent in executing a successful attack.

Our end to end process (excluding remediation testing) typically can be completed within 2-3 weeks.

Intelligence gathering

Utilising a variety of techniques we probe and collate information from various sources to build a detailed picture of your business and system profile and the operating environment.

Vulnerability analysis

We review relevant web or infrastructure application or services to identify weaknesses which can be exploited.

Technical Testing

In the event potential weaknesses are identified during the vulnerability analysis, we attempt to conduct further technical testing to validate their potential impact.

Report & recommendations

Our report outlines detailed findings for non-authorised and authorised user perspective & a detailed technical summary of remedial, tactical and strategic recommendations.

Remediation testing

Included in our package is one session of remediation testing following delivery of our report.

Pricing

Our Penetration Testing service is tailored to your business needs and requirements with complete packages starting from $25,000 depending on the complexity and scope of the engagement.

Your team

Gordon Archibald

Gordon leads KPMG's national cyber security practice and has over 15 years' experience in cyber security global executive and leadership roles. Gordon specialises in building enterprise security governance and strategies, information risk management and application security frameworks, solution designing, building and deploying managed security services and security risk assessment, consulting & policy development.

Robert Tang

Robert brings over 15 years' experience in cyber security covering a number of domains and markets across Australia and Singapore. Robert has extensive experience in strategic governance, security architecture, and technical risk assessment and security operations.

Chatnura Abeydeera

Chatura is your tier 1 CREST certified tester with over 14 years hands-on industry experience in the field of cyber security. Chatura has worked with clients across all industries from State & Federal Government through to technology, retail, telecommunications and financial services, specialising in red teaming and objective based penetration testing.

For more information contact the High Growth Ventures team at highgrowthventures@kpmg.com.au

KPMG.com/au/highgrowthventures

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.

March 2019. 314552186HGV.