Company Description

About Crowe Singapore
As a member of Crowe Global, a top-10 accounting network, Crowe Horwath First Trust ("Crowe Singapore") is an award-winning firm that leverages its core strengths in Audit, Advisory, Tax, Transfer Pricing, Risk Advisory, Corporate Services, Outsourcing, Fund Administration, Corporate Finance, Valuation and IT Consulting and Assurance Services to bring smart decisions that create lasting value for its clients. With a global reach, and a local expertise, Crowe Singapore is well positioned as a one-stop, integrated solutions provider of a full suite of professional services to a diverse and international clientele, including public-listed entities, multinational corporations, and financial institutions.

- Led by 24 Partners and Directors
- More than 100 Experienced Professional Staff
- Winner of the Best Practice Award 2016 and the Growth Award 2018
- More than 20 Years in Service
- Over 15 Professional Services and Counting

Crowe Singapore is an Accredited Cybersecurity Consultant

- **Licensed Penetration Testing Service Provider**
  In June 2022, Crowe was among the first in Singapore to receive a Penetration Testing Service Licence from the Cybersecurity Services Regulation Office of the Singapore Government.
- **Cyber Essentials Mark-Certified Organisation**
  Crowe Singapore is a Cyber Essentials Mark certified organisation, by the Cybersecurity Agency of Singapore. The Cyber Essentials mark recognises that organisations have implemented robust cybersecurity practices to safeguard their operations and customers from common cybersecurity threats.
- **Appointed and Onboarded Chief Information Security Officer as a Service (CISOaaS) Consultant – Cyber Essentials**
  Crowe Singapore is among only a handful of cybersecurity consultants appointed and onboarded by the Cybersecurity Agency of Singapore to provide CISOaaS solutions to assist enterprises achieve their Cyber Essentials Mark.

Product Description

Cybersecurity Consulting

- **Baseline Health Check**
  Our baseline health check services provide a baseline gap analysis for our clients to have a bird's eye view of their current cybersecurity posture. This covers IT Security Governance, Risk and Compliance. With this baseline health check report, you will be able to define and plan a cost-effective strategy to meet your compliance and cybersecurity objectives.
  - Quick and accurate report under a week
  - Cost-effective health check on current environment
  - Identify maturity level of current information security posture

- **Cybersecurity Assessment**
  With evolving cybersecurity threats, it is critical for businesses to perform cybersecurity assessments periodically. A Cybersecurity assessment will help to identify potential vulnerabilities and threats that may exist in your current network. This activity also helps to identify weaknesses, so that we can work together with you to build a more resilient environment against threats.
  - Evaluate current business process and policy
  - Identify vulnerabilities and risks
  - Review cybersecurity compliance according to your industry requirements
  - Providing a risk matrix on current environment according to various international frameworks
  - Aligning the organisation with cybersecurity industry standards
  - Comprehensive report including recommendation and remediations

- **Penetration Test**
  A holistic cybersecurity approach is multi-faceted, integrating various components together to deal with current threats. Penetration testing is one of the keys to the puzzle, which completes the cybersecurity total defense. A penetration test is a simulated attack done by qualified expert to exploit your network in a controlled manner, under noble intentions. By investing in a regular penetration testing regimen, an organisation is able to reap many benefits such as:
  - Evaluating how your current defense mechanism fares against simulated cyber attacks
  - Quantifying, evaluating, and prioritising your cybersecurity investments
  - Discovering hidden vulnerabilities and exploits
  - Providing insightful reports on strength and weaknesses of the current infrastructure
  - Vulnerability Assessment and Penetration Testing to get your TrustMark certification which can be used for your website and promotional materials

- **Red Teaming**
  As cyber threat actors are getting more creative, penetration testing alone at times is not enough to cater for large-scale sophisticated, targeted attacks. While the main objective of penetration testing is to identify as many vulnerabilities and exploits as possible of the targeted environment, the main focus of Red teaming is to sneak into the environment stealthily, bypassing detection, with a precise target. As an organisation matures in their cybersecurity posture, this service is the next step forward upon conducting penetration testing.

  - An adversarial approach which helps to identify and attack the organisation's security posture via technical, physical, and process-based means
  - Access the organisation's cyber mechanism to detect such attacks
  - Providing the organisation insights on the modus operandi that bad actors may deploy
  - Giving the organisation confidence in addressing such attacks

- **Incident Response Services**
  Preparedness is identified as one of the critical assets in a holistic cybersecurity defense mechanism. To effectively combat against any cyber threats, incident response plan and guidelines must be in place to contain, eradicate and recover during a cybersecurity incident. IT cybersecurity resources are scarce.

  Therefore, our incident response service comes in to fill this critical gap due to the lack of available resources.

  - Identify critical stakeholders during a cyber incident
  - Define the roles and responsibilities in the organisation during a cyber breach
  - Assessment of our client's current critical business assets
  - Provide a well-defined response plan during an incident
  - Have an Incident Response team on contract for your Incident Response needs

- **Security Awareness and Training**
  Our comprehensive IT security awareness training programme helps to maintain high levels of awareness for your staff/members, contractors, and service providers. It includes the individual's responsibility to safeguard information assets, the current cyber threat landscape, and their implications.

  We have standard and tailored programmes catered for organisations, and these will be conducted on a periodic basis, such as yearly or every six (6) months. Our programmes are reviewed and updated regularly.

  Our programmes are conducted online at the convenience of the individuals, and reports will be generated based on their awareness. Further tests such as email phishing and USB drops, can also be arranged to validate the level of awareness on top of the tests, during the training programme.

- **Chief Information Security Officer (CISOaaS) Consulting**

  As a sanctioned CISOaaS provider, we offer comprehensive cybersecurity solutions to help SMEs meet the Cyber Essentials Certification benchmark

  1. **Assets**
     - People: Equipping your staff in cyber-preparedness
     - Hardware & Software: Understanding the range of hardware and software in use by your organisation and safeguarding them
     - Data: Be informed of the kinds of data that your organisation stores, where they are stored and to secure them
  2. **Secure/Protect**
     - Virus/Malware Protection: Protection against malevolent software like viruses and malware
     - Access Control: Gatekeeping access to critical data and services
     - Secure Configuration: Put in place secure settings for your enterprise's hardware and software
  3. **Updates**
     - Software Updates: Ensuring software on your devices and systems are updated in a timely manner
  4. **Backup**
     - Backup: Ensure that essential data have been backed up and stored offline
  5. **Respond**
     - Incident Response: Be prepared to detect, respond to, and recover from cyber incidents