PSB Singapore

Add value.
Inspire trust.

SMEs Go Digital – Pre-Approved Cyber Security Solutions

Receive up to 80% grant support till Dec 2020

VISIT OUR WEBSITE

Your challenges

As cyber criminals continue to evolve their attacks with more sophisticated tactics, every organisation, regardless of size, are prone to cyber-attacks if they are unprepared. However, not all organisations are affected by malicious attacks in the same extent. Small and medium enterprises (SMEs) face greater threats due to the lack of resources, including expertise, personnel and budget for conducting standard enterprise security practices such as penetrating tests and cyber security assessments, to mitigate risks.

What is the SMEs Go Digital Programme?

Launched in April 2017, the SMEs Go Digital programme by the Infocomm Media Development Authority (IMDA) aims to help SMEs in Singapore use digital technologies and build stronger digital capabilities to seize growth opportunities in the digital economy.

Under the programme, SMEs can apply for proven SME-friendly cyber security solutions pre-approved by IMDA to meet your business needs. Government grants such as Productivity Solutions Grant (PSG) are available to enable your business for the digital future and to help lower the barrier of cost for the adoption of Attack Surface Assessments & Penetration Testing and Cyber Security Assessment services.

Why are Cyber Security Solutions important for your organisation?

Attack Surface Assessments & Penetration Testing and Cyber Security Assessments provide an excellent view of the current security status of an organisation. Based on the results, business owners will gain a better understanding of their levels of exposure, identify weaknesses in their IT systems and provide details for rectifying vulnerabilities. This will allow the organisation to implement the necessary measures to be less vulnerable to cyber-attacks which could cripple the business and cause costly downtime.

TÜV SÜD PSB

TÜV®

How can we help you?

With highly skilled Vulnerability Assessment and Penetration Testing (VAPT) and Cyber Security assessment experts, TÜV SÜD can support SMEs in identifying cyber security flaws within their solutions and infrastructure to minimise the cyber-attack surface.

SMEs can now enhance the security posture of your solutions with access to our cyber security experts. Starting off with a 'health check' of your solution, your company will be able to determine how secure your solutions are and whether there is an urgent need to go for further testing.

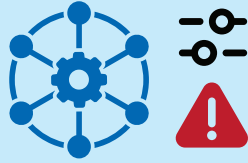| ATTACK SURFACE ASSESSMENTS AND PENETRATION TESTING			
Security Configuration Review	**Web Application Grey-Box Penetration Testing (Limited Scope)**	**Web Application Grey-Box Penetration Testing (Full Scope)**	**Endpoint Black-Box Penetration Testing**
Service Overview: - Reviews the configuration settings of operating systems, databases, devices etc against cyber security hardening industry benchmarks; - Ensure that systems are hardened to the best within your business needs to prevent vulnerabilities from being exploited; - Assure your customers that their user accounts are unlikely to be breached by attackers and their personal data in the applications are kept secure.	**Service Overview:** - A lightweight service as compared to a full-scope penetration test, a faster turnaround period; - Tests the login mechanism and session management of the web application; - Ensure that the first line of defence of the web application will not be easily compromised by malicious attackers; - Assure your customers that their user accounts are unlikely to be breached by attackers and their personal data in the application can be kept secure.	**Service Overview:** - Includes all the assessments in the limited scope and also test cases based on OWASP and MITRE which are not covered in the limited scope; - Covers test cases from OWASP Top 10 2013-2017, injection-based attacks as well as privilege escalation; - Assurance to customers that the web application is not affected by the common vulnerabilities that web applications are commonly subjected to; - Your customers can feel confident that their Personal Identifiable Information (PII) will be handled securely while using the web application.	**Service Overview:** - Targets the vulnerabilities of an endpoint from an attacker's point of view; - The objective is to mimic real-life hacking scenarios an attacker uses to gain access to the endpoint from an outside in approach; - Assure your customers that the endpoint is unlikely to be subjected to an external attack.

Deliverables:

Report indicates the findings, steps to replicate the findings, risk rating and recommended solution(s) for each finding.
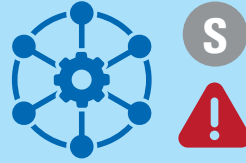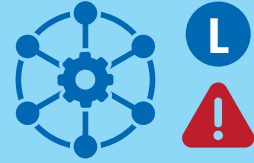
CYBER SECURITY ASSESSMENTS

Security Architecture Review (Small System)	Security Architecture Review with TRA and Control Review	Security Architecture Review with Threat & Risk Assessment (TRA) (Small System)	Security Architecture Review with TRA (Large System)

Service Overview:
- Security Architecture Review focuses on the architecture of the IT system (<6 hosts);
- Asset details and system architectural information are consolidated and high-level system vulnerabilities potentially exploitable by hackers can be identified;
- The outcome of this exercise feeds into other deliverables in this advisory service.

Service Overview:
- Security Architecture Review focuses on the architecture of the IT system (<16 hosts);
- Asset details and system architectural information are consolidated and high-level system vulnerabilities potentially exploitable by hackers can be identified;
- The outcome of this exercise feeds into other deliverables in this assessment service.

Service Overview:
- Security Architecture Review focuses on the architecture of the IT system (<6 hosts);
- Asset details and system architectural information are consolidated and high-level system vulnerabilities potentially exploitable by hackers can be identified;
- A threat and risk assessment is a systematic process of identifying various threats and vulnerabilities to the IT system, based on the likelihood and impact of potential cyber-attacks;
- Business processes change over time and the cyber security landscape is constantly evolving, hence there is a need to perform regular risk assessments and keep the risk register updated.

Service Overview:
- Security Architecture Review focuses on the architecture of the IT system (<16 Hosts);
- Asset details and system architectural information are consolidated and high-level system vulnerabilities potentially exploitable by hackers can be identified;
- A threat and risk assessment is a systematic process of identifying various threats and vulnerabilities to the IT system, based on the likelihood and impact of potential cyber attacks;
- Business processes change over time and the cyber security landscape is constantly evolving, hence there is a need to perform regular risk assessments and keep the risk register updated.

Deliverables:
- A report of the asset details and system architectural information which are consolidated;
- Identifies high-level system vulnerabilities potentially exploitable by hackers.

Deliverables:
- A report of the asset details and system architectural information which are consolidated;
- Identifies high-level system vulnerabilities potentially exploitable by hackers;
- A risk register aligned to CSA's Cybersecurity Risk Assessment Framework will be tailored to the company's needs for future tracking purposes.

Optional:
- Security Control Review and / or Gap Analysis

Your business benefits

- **Detailed report** – Our experienced cyber security experts will provide detailed documentation of the outcome of the tests.
- **Suggestions for network security improvements** – By performing penetration tests, TÜV SÜD's experts not only expose security gaps, we also provide recommended solution(s) on how to close them.
- **In-depth assessment** – TÜV SÜD can tailor a unique programme to suit your organisation's needs. We can provide penetration tests on a regular basis spanning different areas with differing requirements to ensure the overall security of your business.
- **Build customer trust and confidence** – By demonstrating that the security of your customers' data and records is one of your company's top priorities.

Why choose TÜV SÜD?

As experts in IT security and data protection, TÜV SÜD can carry out Attack Surface Assessments & Penetration Testing and Cyber Security assessments to the very highest standards. Our teams of cyber security experts stay up to date with all the latest cybersecurity breaches and hacking techniques and can therefore help you keep your systems future-proof. Our expertise covers all business IT systems from major technology providers.

Add value. Inspire trust.

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specialises in testing, certification, auditing and advisory services. Since 1866, the company has remained committed to its purpose of enabling progress by protecting people, the environment and assets from technology-related risks. Through more than 24,000 employees across over 1,000 locations, it adds value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in a physical and digital world to create a safer and more sustainable future.

Visit IMDA & Tech Depot for more details

IMDA GoSecure
https://www.imda.gov.sg/programme-listing/gosecure

Attack Surface Assessments
and Penetration Testing
https://www.smeportal.sg/content/tech-depot/en/psg/specific-it-solution-category/security-assessment-services-for-solutions.html

Cyber Security Assessments
https://www.smeportal.sg/content/tech-depot/en/psg/specific-it-solution-category/security-controls-and-operations-advisory-services-for-solutions.html

Follow us on social media

- @tuvsud
- linkedin.com/company/tuvsud
- twitter.com/tuvsud
- youtube.com/tuvsud
- fb.me/tuvsudASEAN

An initiative of:

SG:D | SMEs GO DIGITAL
PRE-APPROVED

INFOCOMM MEDIA DEVELOPMENT AUTHORITY