

Xtremax Cyber Security Services Catalogue



DELIVERING SIMPLICITY

SCALING YOUR BUSINESS

Document Confidentiality Statement

The information in this document is confidential to the company to whom it is addressed and should be used for that purpose only. It may not be reproduced in whole, or in part, nor may any of the information contained therein be disclosed for any purpose outside the addressee's company without the prior written consent of Xtremax Pte. Ltd. The addressee's company shall have the right to duplicate and use the data for its own internal evaluation. A recipient may not solicit, directly or indirectly (whether through an agent or otherwise) the participation of another institution or person without the prior approval of the directors of Xtremax Pte. Ltd.

Table of Contents

About Xtremax	4
Overview	4
Our Services	4
SentryPage – Your Digital Watchdog	5
Our Principles	7
Why Choose Xtremax	8
Quality and Security Standards	8
Quality Management System (QMS)	8
Information Security Management System (ISMS)	8
Government Security Standard (IM8)	9
Personnel Security Certifications	9
Solid Success Track Records	10
Our Unique Value Proposition	11
Annex A: ISO 9001:2015 Certificate	12
Annex B: ISO/IEC 27001:2013 Certificate	13
Annex C: CSA STAR Certificate	14
Annex D: Data Protection Trustmark (DPTM)	15
DPTM Certificate	15
Xtremax DPTM Policies	16

About Xtremax

Overview

Xtremax has more than 21 years of history. Since 2003, we have grown into a strong strategic business partner with various Singaporean Government agencies, MNCs, local SMEs, and educational institutions. We see challenges as opportunities for innovation to give our clients the digital edge they deserve.

With an **extensive portfolio of developing top-notch cloud solutions** and **digital applications**, we are committed to empowering our clients and reshaping their digital presence, leveraging the latest technology. However, our cloud solutions and digital applications will only be effective if supported by robust security measures. Therefore, we always **test the security** of every detailed part of the system, to search and take action for every vulnerability that we find.



Our Services



Xtremax is a digital agency that specialise in providing the following cyber security services and product:

- **Application Vulnerability Assessment**
- **Network Vulnerability Assessment**
- **Penetration Testing**
- **Source Code Review**
- **Configuration Review**
- **Defacement Monitoring SaaS - SentryPage**

SentryPage – Your Digital Watchdog



With a commitment to design, technology, strategy, and innovation, Xtremax Pte Ltd has launched a defacement monitoring software-as-a-solution (SaaS) product known as SentryPage, an innovative and intelligent monitoring tool designed to protect the corporate image of organizations and help them guard against web defacement with precision, speed, and reliability.

Defacement is unintended and harmful changes that happen on our web pages. SentryPage was built to monitor and prevent such defacement. SentryPage works like CCTV, our digital watchdog that continuously **monitors and sends email alerts** to the user whenever captured anomaly activity.

Four (4) advantages of monitoring defacement using SentryPage are:

- Fastest Capture Rate in the Industry
- Up-to-date Attack Signature Engine
- Simple yet Manageable Alerts
- Archived Change History

For its quality and innovation, SentryPage also won the Cybersecurity award at the **SBR's Business and Technology Excellence Awards 2022**.



We understand that using a website defacement monitoring system that often notifies with **false positives** can be frustrating and time-consuming, with significant effort for the team to respond to these false positives. This is why **SentryPage is designed to reduce the number of false positives**.

Our monitoring solution uses an evaluation engine that utilizes real data from defaced websites to analyze and identify potential defacements on your website. This engine ensures that the monitoring system is up-to-date with the latest defacement techniques and trends, providing you with reliable and accurate monitoring.

Besides cyber security services and product, Xtremax also provides the following digital solutions:

Figure 1: Our Services



- **Cloud Managed Services**

For years, our certified cloud experts have partnered with the major cloud service providers - AWS, Microsoft Azure and Google Cloud - to deliver cutting-edge solutions to over 100 businesses and government organisations. Our success lies in our in-depth knowledge of the entire cloud journey, a customer-obsessed mindset, and a continuous desire to deliver solutions that address the business requirements of the end users.

- **Application Modernisation**

With our roots in application development, coupled with deep expertise in cloud infrastructure projects, Xtremax is well-positioned to advise, develop and manage your application modernisation journey. We have been helping clients make the shift from monolithic applications that are difficult to update and expensive to scale, to a microservices architecture that's easier to build, update, deploy, and advance.

- **Data and Machine Learning Implementation**

Data and machine learning can help organisation to achieve intelligent, sustainable, and efficient transformation. Whether it is to simply speed up and improve the accuracy of tedious, repetitive processes, or to streamline inventory management across multiple locations - our team of technical experts and consultants are able to craft a solutioning based on business and IT requirements.

- **Digital Workspace Implementation**

Digital workspace technology is the solution to the radical workplace transformation that lead to the ever-increasing threat of data privacy and cybersecurity risks. With our expertise, we are capable of empowering organisations with the ability to work from anywhere, anytime, on any device. It gives the employees easier collaboration among colleagues, clients and vendors, while facilitates seamless sharing of information in a secure environment.

- **Digital Consultancy**

In a digital era of mobile, modern and cloud-native applications, the importance of User Experience (UX) and User Interface (UI) design can no longer be ignored. Done well, it will improves the user experience and touchpoints across the entire customer journey, deepens engagement, and builds customer loyalty. With our in-house team of digital consultants and UI designers, we craft and deliver the solutions with the most important audience in mind – client customers.

With our vision of becoming the best in our line of business in the long term, we aim to attain the highest possible standard in all of our services. We do not just strive to meet our clients' requirements; we strive to exceed them.

Our Principles

We strive to be the strategic partner for our customers with our key principles:

Trust, **I**nterest, **C**ommitment



- Trusted – to build win-win relationships.
- Interested – to acquire a deep understanding of our customer's domain.
- Committed – to delivering success for our customers.

In short, we make our customers **TIC**.

Why Choose Xtremax

Quality and Security Standards

Xtremax is committed to quality and security standards and are familiar or has been certified for the following:

- Quality Management System (QMS),
- Information Security Management System (ISMS), and
- Government IM8.

Quality Management System (QMS)

Following the implementation of ISO 9001:2015, we paid careful attention to several factors to meet this new benchmark in quality. We perceive design, implementation, standards, and procedures as essential to achieve excellence. Guaranteeing the desired level of quality is maintained throughout the process also plays a key role in our QMS. Additionally, we make sure that our quality control (QC) focuses on the product, as the end result of the process, by identifying the defects in existing versions of the product.



Quality planning, quality assurance, and quality control encapsulate our QMS.

Information Security Management System (ISMS)

Xtremax is committed to running our operations defined by international security standards. Xtremax has been audited and certified for ISO 27001:2013. This means that Xtremax has implemented the Information Security Management System and certified to meet ISO 27001:2013 standards.



So, Xtremax already:

- Systematically examine the client organisation's information security risks, taking account of the threats, vulnerabilities, and impacts.
- Design and implement a coherent and comprehensive suite of information security controls or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and

- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Note that ISO27001 is designed to cover security much more than just IT.

Government Security Standard (IM8)

Xtremax has extensive familiarity with Govtech's stringent security standard, IM8, which stands for Instruction Manual 8. This familiarity stems from our ongoing operation of their cloud platforms and our successful completion of numerous application development projects in collaboration with them. Our team's deep understanding of IM8 and our proven track record in adhering to its requirements underscores our commitment to maintaining the highest levels of security and compliance in all our endeavors.

Personnel Security Certifications

Our dedication to security extends beyond the organizational level; it permeates through every member of our team. We take pride in the fact that our personnel are not just experienced but also certified in various security disciplines, such as:

- Certified Information Systems Security Professional (CISSP),
- Certified Information Systems Auditor (CISA),
- CREST (Certified Security Tester), and
- Certified Ethical Hacker (CEH).

Figure 2: Personnel Security Certifications



These certifications reflect our team's unwavering commitment to staying at the forefront of industry best practices and ensuring that our clients' data and systems are safeguarded against evolving threats.

Solid Success Track Records

Xtremax has strong track records in the successful development and security testing of Singapore government projects. Xtremax has the know-how and experience in helping government clients build strong cybersecurity solutions and achieve successful project outcomes. Our past security testing projects include:

Table 1: Solid Success Track Records

Customer	Security Testing Scope
Singapore Institute of Management (SIM)	<ul style="list-style-type: none"> Website vulnerability assessment Website penetration testing Source code review
GovTech Singapore	<ul style="list-style-type: none"> Application vulnerability assessment Network vulnerability assessment Penetration testing.
Ministry of Education (MOE)	<ul style="list-style-type: none"> Source code review Website vulnerability assessment Website penetration testing
Temasek Polytechnic (TP)	<ul style="list-style-type: none"> Vulnerability scanning Penetration Testing Risk analysis of the identified vulnerabilities Recommendations to address identified vulnerabilities
Institute of Technical Education (ITE)	<ul style="list-style-type: none"> Application vulnerability scanning Penetration testing
Commzgate	<ul style="list-style-type: none"> Sharepoint vulnerability assessment Sharepoint penetration testing Website vulnerability assessment Website penetration testing Network vulnerability assessment
Singapore Grand Prix (SGP)	<ul style="list-style-type: none"> Website vulnerability assessment Website penetration testing
MBK Healthcare Management (MHM)	<ul style="list-style-type: none"> Network consultancy and implementation Network security assessment Access control and management assessment Third-party applications review Network and application penetration testing Vulnerability assessment and penetration testing (VAPT) Configuration review

Our Unique Value Proposition

Xtremax has the combination of strong security expertise and strong government projects know-how. Furthermore, Xtremax is a homegrown company owned by Singaporeans. For us, it is not just business -- we take pride and nationalism in helping the Singapore Government achieve strong cybersecurity.

Our unique value proposition is:

We don't just deliver strong cyber security; we deliver successful project outcomes.

Annex A: ISO 9001:2015 Certificate

Figure 3: ISO 9001:2015 Certificate



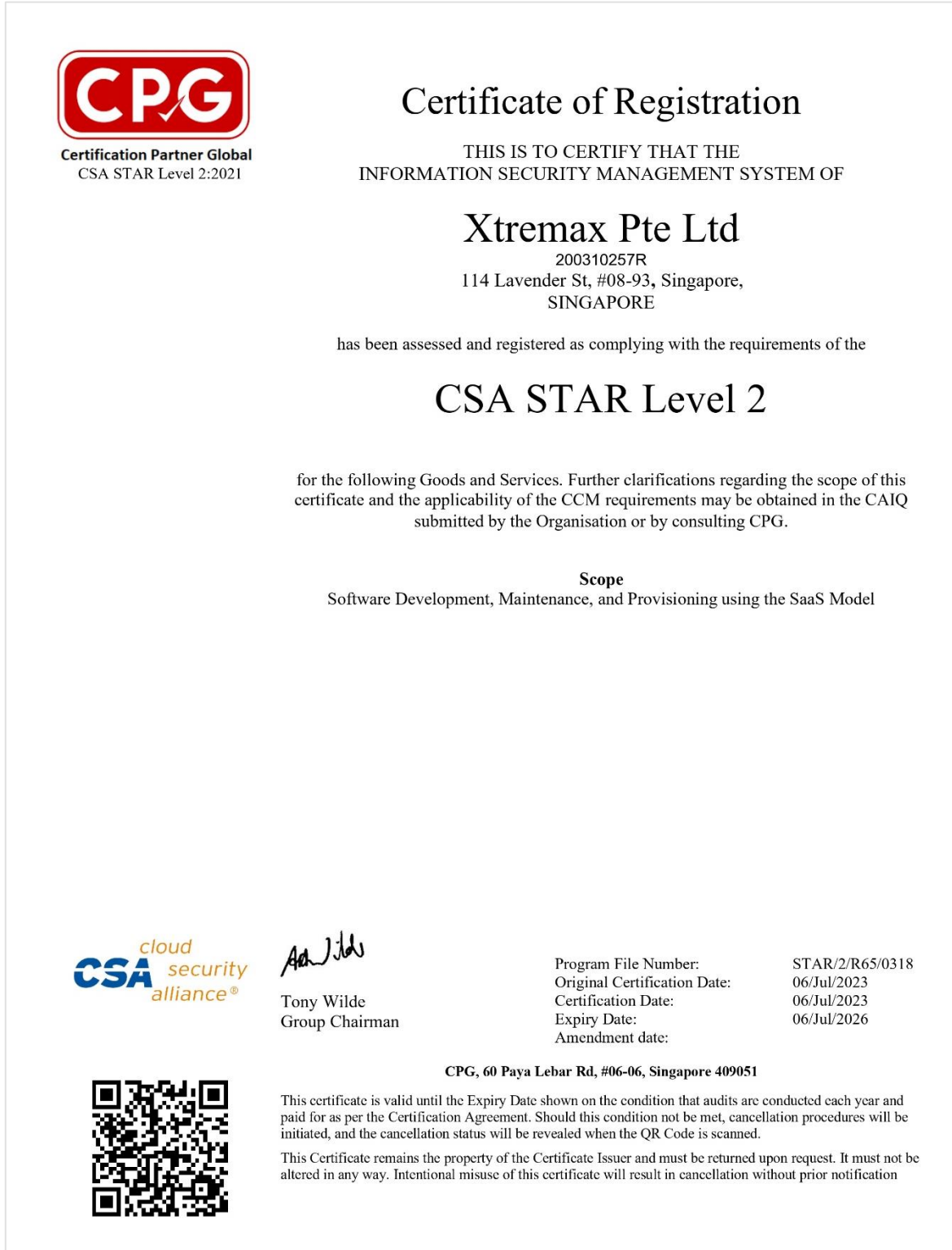
Annex B: ISO/IEC 27001:2013 Certificate

Figure 4: ISO/IEC 27001:2013 Certificate



Annex C: CSA STAR Certificate

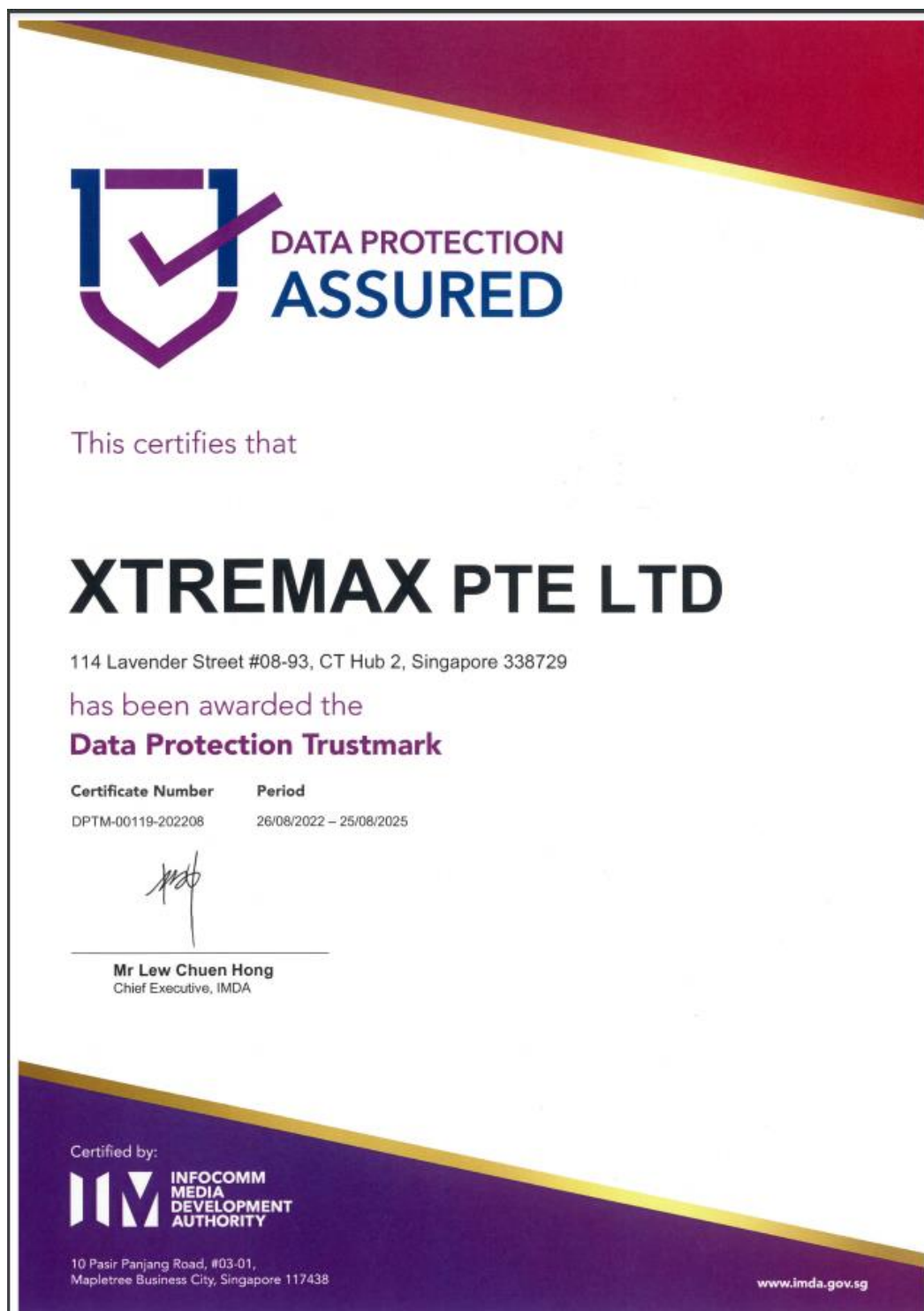
Figure 5: CSA STAR Certificate



Annex D: Data Protection Trustmark (DPTM)

DPTM Certificate

Figure 6: DPTM Certificate



Xtremax DPTM Policies

Xtremax created DPTM policies and action items to adhere to DPTM requirements. These practices included (but not limited to):

1. **Access Control**

All personal data should only be shared on a need-to-know basis, and in a secure manner.

Example:

- a. A manager interviewing a candidate should not keep physical copies of CVs and if required to download on to personal computer, should be disposed immediately after required use.
- b. Personal data stored on an online platform should only be given access on a need-to-know basis and if possible, password protected.

2. **Owner Consent**

Xtremax should ensure that all personal data held is with the owner's consent. This includes employees and external 3rd party personal data. The owner should also have the right to recede consent and have access to personal data.

Example:

- a. All Xtremax staff must have given consent (or implied consent) to Xtremax to hold personal data, which may be used for business use. Xtremax staff have the right to recede consent.
- b. When receiving personal data from 3rd parties such as job portals, Xtremax must ensure that consent (or implied consent) is received by the owner.

3. **Storage and Management of Personal Data**

Xtremax's improved processes to manage and store personal data in a manner that is compliant with DPTM requirements. These include:

- a. Regular review of personal data held e.g., Xtremax should not hold CV of ex-staff.
- b. Proper security measures should be set up to ensure prevention of hacking. Regular security testing should be carried out.

DPTM policies and practices are shared through the company:

1. Documents are acknowledged through HRMS.
2. Policies are easily accessible through the company wiki.
3. Regular reminders through monthly newsletters and announcements.