secarma®
CYBERSECURITY EXPERTS

A ADVISE

C CERTIFY

T TEST

CULTURE
EXPERTISE

ADVISE
CERTIFY
TEST

PARTNERSHIPS
CLIENTS

WHY SECARMA?

Independently owned and customer focused, Secarma exists to keep our clients safe and support their growth.

Our approach puts the needs of the client first and works through the security challenges you face, providing you with a set of tools to fortify your posture.

We work collaboratively, supporting you at the appropriate technical levels. We find that this approach bridges knowledge gaps and ensures that your security improvements are consistent and effective.

Our cyber consultants work as an extension of your core business to develop your security strategy, offering the level of advice you need as you need it. Our testers are all highly accredited, passionate and proficient, not just at hacking into your systems but also at communicating their findings with senior management and security teams.

We've been providing CREST & CHECK approved Penetration Testing and information security consultancy and advisory services for over 20 years, and our in-house experts deliver to a global client-base.

OUR TEAM + CULTURE

Headquartered in Manchester UK, we have security personnel operating out of key locations around the world. With multi-national banks through to software start-ups our client list is expansive because everyone's data is important and deserves to be protected.

Our employees are based in 10 different cities, with 8 distinct nationalities.

There is a diversity amongst our team that promotes innovation, creativity and knowledge transfer.

We thrive on challenge and progression and have an educational approach to company growth.

Our in-house academy ensures all team-mates have the chance to line up their professional ambitions with the needs of our clients.

A growth mindset is crucial in a developing industry and has allowed us to become more empowered as individuals and collaborative with customers in supporting your needs.

Passion.

Integrity.

Innovation.

In attracting new talent in this competitive industry, we value the skills that you cannot teach. We look for passionate people whose honesty, integrity and reliability makes them great at looking after clients and we place them in our in-house skills process. You can teach someone 'cross site scripting' but you can't teach them to care.

Ultimately, we are big enough to deliver and small enough to offer a truly personalised service. We recognise that our job is to look into your vulnerable space, so building a genuine sense of trust with clients is crucial to our success.

OUR EXPERTISE

Continuous investment in research, internal training, and technical development ensures that we provide our customers with the highest quality service.

Our ethos for growth and learning can be found at all levels within the business and results in our team holding, amongst others, the following qualifications.

Our consultative approach is how we stand out from the competition and in order to live our own standards we are proud holders of the following business accreditations.

ADVISE

We work with you to develop a better understanding of your organisation's security posture, meet security objectives and prepare for worst-case scenarios.

The aim is to build your organisation's resilience to real world attacks. With us, you can expect strong communication across your entire team as standard. We're here to advise you on how to maintain control, stay informed and reduce pressure.

Each of our services provides an independent view of your organisation's security, consulting with you on what's working, what isn't, and how to improve.

CYBER SECURITY MATURITY ASSESSMENT

This detailed evaluation of your organisation's current security status takes a holistic view looking beyond technical configuration, to the ability to protect, detect and respond to security threats. It's a fantastic starting point for a long-term relationship.

VIRTUAL INFORMATION SECURITY MANAGER

A dedicated expert, embedded within your organisation to provide an independent view of your security posture, manage large-scale projects, and communicate their findings with senior management.

INCIDENT RESPONSE SCENARIO TESTING (WARGAMING)

We'll use established methods to test the effectiveness of your incident response and business continuity plans before consulting with you on necessary changes and improvements.

PHISHING ASSESSMENTS

Targeted at emails and other online communication, the fraudulent theft of passwords and credit card information is sadly commonplace in society today.

To test your defences, we simulate deceptive email phishing, spear phishing and business email compromise (BEC) attacks and feedback on whether your business and team manage to survive the threat.

THREAT MODELLING

A risk management activity used to identify and mitigate potential threats to a system or application. It is an essential step in the software development process to ensure that security is built into the product from the outset.

SECURITY REVIEWS

Cloud – assesses your cloud provider's management interfaces for security misconfigurations.

Firewall – our review provides system administrators with a comprehensive overview of your organisation's firewall configuration.

Tech Stack Build – in-depth assessment of server builds, end user device builds, or system deployment tools for vulnerabilities.

SECURITY TRAINING

Our security awareness training sessions analyse the security threats that modern businesses face, including an overview of hackers' motivations and methods.

By learning to identify potential attacks, your workforce can become your organisation's best defence. The hands-on security training courses can be run in-house or remotely and focus on application and infrastructure security vulnerabilities.

We take key members of your team through the process of a penetration test, while our labs training allows for practical experience of breaking security systems and building them in more resilient ways.

Information Security Management ISO 27001 Certified

Lead Auditor

Compliance

From producing company policies to managing ISO processes, our team can design a framework of compliance that keeps your business safe.

ISO27001 IMPLEMENTATION GUIDANCE

Certified as Lead Auditors against the latest version of ISO27001, our consultants are well placed to help your organisation achieve or maintain certification.

We offer everything from Gap Analysis to policy creation, third party reviews, strategic roadmaps and a full internal audit programme.

We can also train your internal team to carry out elements of the ISO27001 management system requirements, and even attend external audits alongside you.

INTERNAL AUDIT

Our regular Internal Audits assess an organisation against its own policies, whilst keeping a close eye on their relation to ISO27001. The process highlights any key changes or deviations from policy and selects specific areas for in- depth analysis.

SUPPLIER REVIEW

Supplier management is key to information security standards. Our review helps you manage these requirements and build a confidence around the sizeable risk surface of third-party security.

We also offer Policy Review and Implementation Services, Data Protection Impact Assessments and consultancy around PCI DSS and NHS frameworks (DSPT, DTAC and DCB1596).

C CERTIFY

As an IASME accredited certification body, we can support your business in achieving standards of cyber maturity.

CYBER ESSENTIALS & CYBER ESSENTIALS PLUS

The basic Cyber Essentials scheme is a self-assessment certification introduced to help organisations mitigate 80% of cyber threats.

The scheme assesses Firewalls, Secure Configuration, Security Update Management, User Access Controls, Password Based Authentication and Malware Protection. With this certification you can build more trust with customers and reduce the cost of cyber insurance.

Cyber Essentials Plus involves a manual assessment of the technical controls and protections put in place within your organisation. This provides a deeper assurance that your corporate data and vital systems are protected against common threats and shows commitment to a proactive and specialist approach.

IOT CYBER SCHEME

When manufacturing and selling IOT devices in the UK, you must comply with UK Legislation to prove a base level of security.

IASME's IoT scheme aligns with all 13 provisions of the worldwide standard.

Each individual device may need annual certification but our experts can help you design a structured and efficient approach before completing necessary assessments.

Compliance avoids legislative enforcement action, opens up your devices to regulated industries and reassures potential buyers.

IASME CONSORTIUM

IoT Security Foundation Corporate Member

CERTIFICATION BODY CYBER ESSENTIALS PLUS

IASME IoT CYBER SCHEME

T TEST

How do you know your systems are secure if you don't test them regularly?

In an ideal world for our customers, we wouldn't find any way to break their systems, but that's rarely the case. And it's certainly better that we find our way into your systems ethically, rather than a cybercriminal hacking in and causing havoc.

Our experienced consultants utilise similar tools and techniques to real-world threat actors, meaning we can simulate realistic exploits without harming your systems in any way.

With a diverse range of skills across the team, we are offer a vast array of testing services. Our most common services include:

WEB TESTING

As a doorway to client communication, web interfaces are designed with functionality and aesthetics rather than security in mind. This oversight leads to some of the most significant security risks on the internet. Our testing highlights all known vulnerabilities to your team.

MOBILE TESTING

Attacks against mobile apps are on the increase and can have a devastating effect on your business. We commonly test mobile applications that handle sensitive data and/or interact with backend systems to assess the risk exposure for your core systems and client data.

INFRASTRUCTURE TESTING

Our onsite or remote services exploit vulnerabilities in your company's networks and servers to improve your resilience to attacks. We provide context around the vulnerability, threat and impact and tailor advice on protecting your critical operating systems and networks.

Wireless network testing will often be part of an infrastructure test. We'll look at the risks to your wireless access points, production applications, and data repositories, testing encryption protocols, authentication and segmentation.

CREST PEN TEST

OBJECTIVE DRIVEN, RED TEAMING & PURPLE TEAMING

A key strength of the Secarma senior testing team is their objective led project work for clients. A significant step up from basic penetration testing work, objective led and red teaming engagements are usually conducted with the knowledge of only a small group of people. They are carefully scoped to ensure specific objectives are addressed.

During a red team operation, our consultants will mimic the Tactics, Techniques and Procedures (TTPs) that a genuine cyber criminal might adopt to your defences.

To guarantee our integrity we work to the Mitre ATT&CK Framework.

Often involving the creation of test infrastructure, domains, personal identities, and malware payloads these engagements are designed to breach the client's infrastructure. Techniques adopted include social engineering, physical security, and third-party interrogation.

Most engagements of this type include a timebound and multi-phased approach where for instance reconnaissance leads to access attempts and assisted foothold testing before a detailed report and analysis wraps up the assignment.

VULNERABILITY SCANNING

We offer a 24/7 intelligent scanning service that gives you a full overview of your current security posture, allowing you to track remediation, spot vulnerabilities, and identify your areas of risk.

Other more bespoke assessments include: PCI DSS, VPN/remote desktop, wireless network testing/segmentation, defanged ransomware, physical access and of course, Phishing, Vishing and SMShing!

PARTNERSHIPS

WHO WE PARTNER WITH

As we have a consultative approach, our partnership services tailor to your specific needs. We work collaboratively to expand your potential reach offering expert guidance and assurance.

Whether you're looking to protect data, meet industry standards, or fortify cybersecurity strategies, we're dedicated to helping you achieve information security goals.

Naturally, you get access to experienced Penetration Testers and Information Security Consultants. We'll assign you a dedicated Technical Account Manager who can ensure agile scoping and service delivery processes for the projects we work together on. We also recognise the need to provide services for a fair price, on time and within budget.

We work in two different ways. Our referral partnerships allow you to identify projects and delegate the process to our team, Our specialists will manage the engagement and you can choose to be as involved or as hands off as you wish.

Alternatively, our Strategic Partnerships present a more collaborative approach, allowing you to re-sell Secarma's offerings directly to customers. You retain the management of a customer directly and position our team as independent agnostic security specialists and trusted partners.

CLIENTS

Working in collaboration.

We're proud of the diversity of our client base. From multinational financial institutions through to micro-businesses, we work with clients who care deeply about keeping their data safe.

With a 20-year history, we have gained extensive experience across most industries but there are some that we tend to work in regularly, including technology, education, financial, media, retail and legal.

Some clients use our expertise for very specific services, while others employ us across their security estate to improve their general posture. Some work in testing cycles, allowing us to return periodically onto their supplier lists, others use us consistently and consider our consultants an extension of their own team.

As an assessor for IASME's cyber secure schemes, we see the early stage security of a very broad spread of businesses. This gives us a privileged view on security across industries and business size. We are passionate about taking what we learn from our largest clients and sharing it with those who need as much security but have far less experience.

Some of the industries our regular customers operate in

EDUCATION

SOFTWARE & TECH

RETAIL

MEDIA

FINANCIAL SERVICES

MANUFACTURING

HEALTHCARE

LOCAL GOVERNMENT

LEGAL

CONTACT OUR TEAM

☎ 0161 513 0960

secarma.com

✉ enquiries@secarma.com