SecQuest Cyber Services Capabilities

2025

Version 1.0

Overview

SecQuest ('SQ') are Cyber Security Service specialists, with a trusted and experienced team that carry security clearance, skills and qualifications, to provide in depth expertise in Cyber Security.

We play an important role as a supplier to the United Kingdom Government and all private industry sectors, delivering Penetration Testing Services, Cloud & Mobile Risk assessments, Build Reviews; plus, Risk Management on all technologies.

SQ is approved by the National Cyber Security Centre ('NCSC') and employs NCSC Certified Professionals and UK Cyber Security Council Chartered cyber practitioners, ensuring that our clients receive knowledge, skills and experience.

Services and Capabilities

Assured Services

SQ has been assured by CREST and the NCSC since 2021. We are one of a select number of companies able to provide assured Penetration Testing Services, which permts SQ to conduct penetration testing across the country's Critical National Infrastructure.

There are stringent requirements for these schemes that involves annual client feedback and CREST / NCSC reviews of SQ services - to confirm we are operating in accordance with their professional standards, ethos and values.

Our Team

Our team is at the heart of our capability. We maintain robust and comprehensive continual professional development plans, with many being members of the UK Cyber Security Council ('UKCSC'), CISSP, The Cyber Scheme and SANS GIAC; plus, Cloud and Mobile certification bodies.

Our Services

Cyber Essentials and Cyber Essentials Plus

SQ can protect your business from a wide range of common cyber-attacks with our self-assessment option. By addressing basic vulnerabilities, you reduce the risk of becoming a target for more sophisticated cyber criminals.

Achieving certification provides peace of mind, confirming your cyber defences are robust against many common cyber threats. Cyber Essentials certification means your organisation has the necessary technical controls in place, making you a less attractive target for attackers.

Cyber Essentials Plus provides a higher level of assurance and involves completing the online assessment, followed by a technical audit of the systems that are in-scope for Cyber Essentials.

This includes a representative set of user devices, all internet gateways and all servers with services accessible to unauthenticated internet users.

Your assessor will test a suitable random sample of these systems (typically around 10 per cent) and then assess whether further testing is required. The cost of a Cyber Essentials PLUS assessment will depend on the size and complexity of your network.

Security Testing

Attack Simulation. A cyber-attack simulation is designed to emulate real-world cyber threats to test and improve your organisation's cybersecurity defences.

Cloud Services Security Testing. Cloud security testing is designed to evaluate the security of cloud-based infrastructure, applications, and services. This involves vulnerability scanning, configuration review, threat modelling, reporting and remediation.

Infrastructure Security Testing. Infrastructure Security testing focuses on the security of both the application environment and the supporting infrastructure, including third-party services and applications. The testing is performed with a combination of manual and automated techniques, tailored for the specific environment.

Website Security Testing. Website Security Testing is an authorised simulated cyber-attack against a public facing web application or website. SQ will assess privilege escalation, session management testing, configuration review, input validation testing and vulnerability scanning.

Pentest/IT Health Check CREST/CHECK. An IT Health Check (ITHC) is a comprehensive assessment of an organisation's IT systems and infrastructure. CREST Pen testing is predominately used in the Private Sector, whereas CHECK is a NCSC certified scheme used across the Public Sector. The primary goal is to identify vulnerabilities and weaknesses that could be exploited by cyber threats.

Social Engineering Test. A social engineering test is a simulated attack designed to assess how well individuals or organisations can recognise and respond to deceptive tactics used by cybercriminals. This test helps identify vulnerabilities in human behaviour and improve overall security awareness.

Open-Source Intelligence (OSINT) Assessment. An OSINT Assessment establishes the information publicly available that may aid an attacker in targeting and attacking your organisation.

Vulnerability Management. The vulnerability management service is a comprehensive approach to identifying, assessing, prioritising, and mitigating security vulnerabilities within an organisation's IT infrastructure and software.

Secure Firewall Configuration Scan. A secure firewall configuration scan service is designed to evaluate the security and effectiveness of a firewall's configuration.

Cloud Security Risk Assessment. A cloud security risk assessment involves evaluating an organisation's cloud infrastructure to identify potential vulnerabilities and threats, ensuring the confidentiality, integrity, and availability of data and services. This process includes threat modelling, vulnerability scanning, and analysing cloud service configurations for misconfigurations and compliance gaps.

Risk Management. Security risk management consultancy involves assessing and mitigating potential security threats to an organisation's assets, people, and operations. These consultants provide expert guidance on identifying vulnerabilities, implementing protective measures, and ensuring compliance with regulatory requirements.

Incident Management. Incident management consultancy involves providing expert guidance and support to organisations in preparing for, responding to, and recovering from security incidents and emergencies. These consultants help develop and implement incident management plans, conduct training and exercises, and ensure compliance with relevant standards and regulations.

Security Education and Awareness. Security education and awareness involves training and informing employees about best practices and policies to protect an organisation's information technology assets. These programs aim to change behaviour and foster a culture of security by ensuring that everyone understands their role in maintaining cybersecurity.

Vendor and Supply Chain Security. Secure vendor management involves overseeing and controlling third-party vendor relationships to ensure they meet security and performance requirements. This process includes assessing vendors' security practices, defining access requirements, monitoring activities, and regularly reviewing and updating access permissions to mitigate risks.

Physical Security Testing. Physical security testing involves simulating real-world attacks on an organisation's physical assets, such as buildings and infrastructure, to evaluate the effectiveness of existing security measures. This testing identifies vulnerabilities and provides recommendations to enhance physical security and protect against unauthorised access.

Facility Security Clearance (FSC) Review and Implementation. Previously known as List X, a FSC is required to store and manage Government or Ministry of Defence sensitive assets. A FSC review can determine what is needed to meet the National Protective Security Authority's (NPSA) requirements and we will then work with you to design and implement the physical facility.

Incident Response. Incident response involves an organisation's processes and technologies for detecting and responding to cyber threats, security breaches, or cyberattacks. It includes a formal plan to limit damage, contain the threat, and restore normal operations while minimising the impact on business continuity.

Incident Management. Incident management is the process of identifying, analysing, and resolving incidents that disrupt or reduce the quality of services to restore normal operations as quickly as possible. It involves a structured approach to detect, respond to, and mitigate the impact of incidents, ensuring minimal disruption to business activities.

Social Engineering Training. Social engineering training educates employees on recognising and defending against manipulation tactics used by attackers to gain confidential information. This training includes understanding common social engineering techniques, such as phishing and pretexting, and implementing best practices to prevent falling victim to these schemes.

Audit and Compliance Services

ISO 27001 Management. Implementing ISO 27001 involves establishing, implementing, maintaining, and continually improving an information security management system (ISMS) to manage sensitive company information systematically and securely. This process includes risk assessment, defining security policies, and ensuring compliance with legal and regulatory requirements.

ISO 27001 Gap Analysis. An ISO 27001 gap analysis evaluates an organisation's current information security measures against the ISO 27001 standard to identify discrepancies and areas needing improvement. This analysis results in a detailed report outlining gaps and providing recommendations to achieve compliance and enhance security practices.

Data Protection Support and Gap Analysis. Data Protection Support involves assisting organisations in implementing and maintaining data protection measures to ensure compliance with relevant regulations, such as GDPR. This support includes providing guidance on data handling practices, conducting audits, and offering recommendations to safeguard personal and sensitive information.

A Data Protection Act Gap Analysis assesses an organisation's current data protection practices against the requirements of the Data Protection Act to identify areas of non-compliance and potential risks. This analysis results in a detailed report highlighting gaps and providing recommendations to achieve full compliance and enhance data protection measures.

About SecQuest

Our Company

Established in 2012, SecQuest Information Security Ltd provides Cyber Security Services and is authorised by CREST and the NCSC to test against Government and Critical National Infrastructure (CNI) environments under the CHECK Scheme. We look forward to working with you and assisting you in achieving your security objectives.

Our Clients

SQ is well recognised for its consultancy services, with current clients including the UK Ministry of Defence and other clients in a variety of industries that include Financial, Energy, Charity and Health.

Why Us?

Above all else, we are passionate about security and share our clients' desire to develop and deliver bespoke penetration testing in a way that gets the buy-in from the Board to Operations – to ensure holistic effective risk management.

We learn from you what is at stake – to help shape how we can work effectively with you, as we understand that cost and value are paramount to our clients. Therefore, through our cost-effective operations, we can help you deliver the right quality of service whilst ensuring we deliver exceptional value. All our staff hold UK government security clearances and are experienced professionals ready to support you.

Security Assured

As a cyber security consultancy, SQ takes its own security very seriously. We hold (UKAS) ISO 27001 accreditation, as well as certifications for Cyber Essentials and Cyber Essentials Plus. We also hold (UKAS) ISO 9001 accreditation for quality management.

Quality Assurance

Throughout the contract, we will do our utmost to confirm you are totally satisfied with the service you receive. At the end of the service, we will always request feedback, and in fact it is a requirement under our ISO / consultancy scheme.

We aim to build a great relationship that is lasting and rewarding for both parties but if any concerns arise, we have an established escalation pathway to the SQ Security Director, for resolution.