FORTIS CYBER®

TECHNICAL SURVEILLANCE COUNTER MEASURE INSPECTIONS

FORTIS INFORMATION SECURITY & RISK MANAGEMENT

An Introduction to Fortis Cyber®

Fortis Cyber® is an ISO 9001 certified UK based Information Security and Risk Management consultancy

Fortis Cyber® has constructed an arsenal of information security and risk management services, allowing organisations of any size or industry to stay in control of their cyber security. By being able to identify security risks and detect vulnerabilities, companies will be armed with the knowledge required to more easily protect themselves and meet and respond to omnipresent and evolving cyber threats.

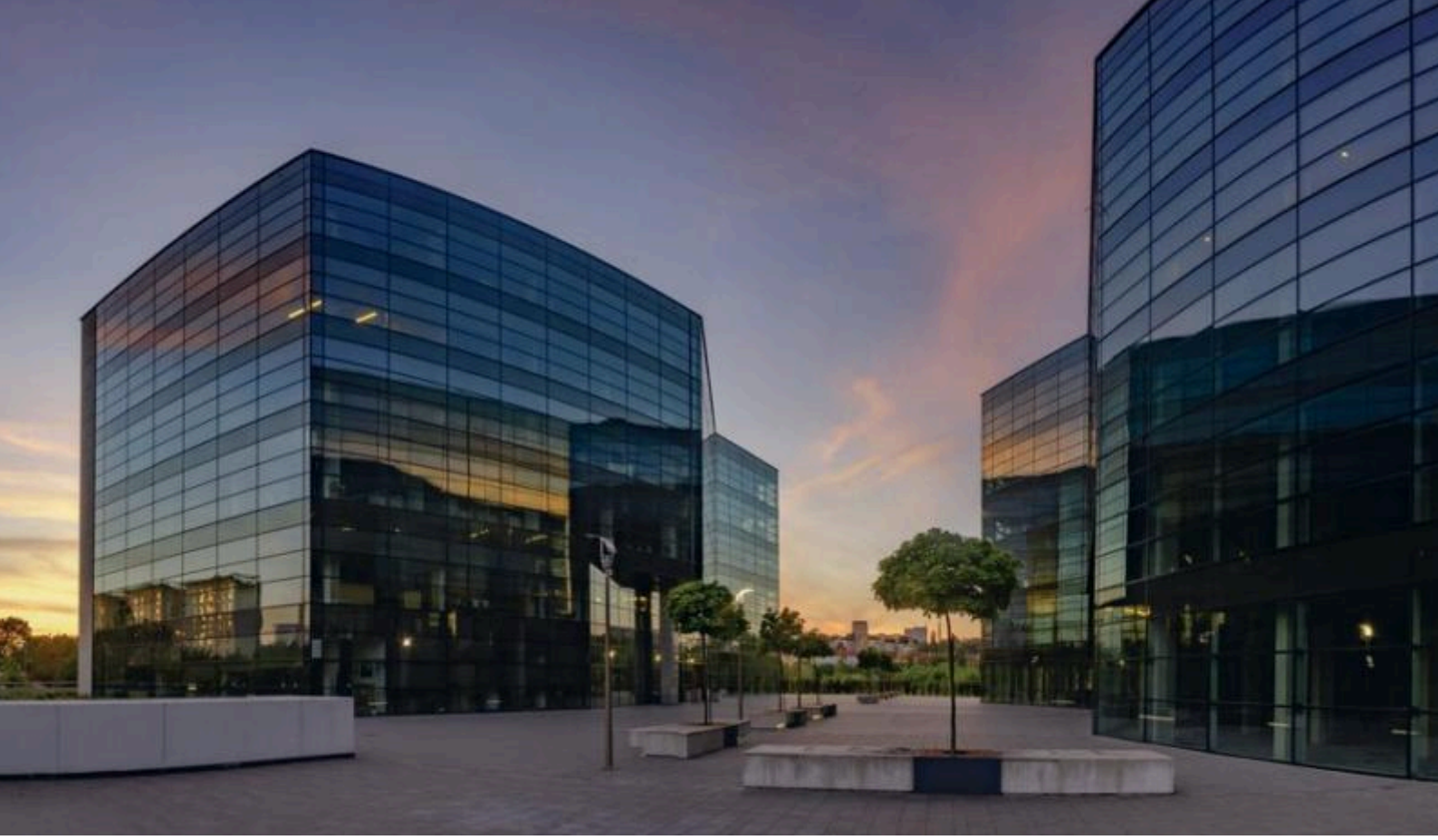
Core Values: Trust, Discretion, Delivery, and Privacy

- Founded by a senior cyber expert with 30 years' first-hand experience in the UK Military and Global Enterprise.
- Fortis Cyber® is a trusted partner of the UK Home Office and Police Forces – Cyber Resilience Centre.
- Fortis Cyber® can provide you with access to cross industry skilled, experienced, and certified information security subject matter experts.

The Core Team Members:

- Trusted - All our Consultants are skilled, experienced, and certified professionals, who have an invaluable depth of knowledge in their respective security fields.
- Enterprise Experience - held senior information security architecture and leadership positions for Juniper Networks, Thomson Reuters, Airbus, WorldPay and Atomic Weapons Agency.
- Government Experience - Information Security at government levels, gained from within the UK Defence, UK Home Office, and UK FCO.
- Insight - Security specialists drawn from leading security organisations: HM Forces, global enterprise, and UK intelligence services.

Industry Accreditations and Certifications



Technical Surveillance Counter Measures

Our TSCM inspection (TSCMI) team specialises in servicing clients who wish to safeguard and protect their privacy and / or intellectual property. Typically, this applies to sizeable corporations, boardrooms, banks and high net worth individuals with valuable assets and invaluable information. However, this service is available for anyone who wishes to safeguard their privacy.

Fortis Cyber® provides a professional service with over 20 years of experience in sweep operations and information protection, and we equip our team with the finest specialist equipment, augmented by leading edge tools.

Bugs are now much smaller, more technologically advanced and more prevalent than ever. Modern eavesdropping devices are easily capable of fully capturing conversations, video footage and / or data remotely, and can even be activated via silent drones. This can leaves businesses and individuals extremely exposed and vulnerable to being covertly monitored, and the victim of technical surveillance.

Eavesdropping can be achieved via a plethora of methods: the establishment of radio frequency (RF) audio microphone transmitters (aka 'bugs'), the established technique of wire tapping, IT network cables, telephones, 'drop-in' recording boxes to electricity lines (AC & DC) and out of area laser microphones etc. This is also true for wireless communication types, such as mobile phones, and more frequently internet Wi-Fi and Bluetooth.

Fortis Cyber® provides an executive level of assurance for our clients, suited to any environment on the planet, providing you with sky-high protection.

Complete Coverage Capability

The Fortis Cyber® TSCMI team manages a detailed inventory of the latest technical equipment for use by the trained and experienced inspectors.

Whilst not an exhaustive list, this includes:

Purpose built spectrum processers, 2G, UMTS, 3G, LTE & 4G detection, identification & location finding of cellular systems, telephone and line analyzer with built in Frequency Domain Reflectometers, RF, infrared, visible light & carrier current receivers, non-linear junction detectors, stimulated microphone detection systems, cable testers, UV and forensic lighting systems, covert camera detectors including wireless camera's, WiFi sensors and thermal imaging systems.

The Fortis Cyber® Approach

Effective TSCM based defence is not a single product or a short-term response; it is a constantly adapting process, in the face of the rapid evolution of technical surveillance and information attacks. Fortis Cyber® partner our clients through every aspect of this journey, building long term relationships based on trust, value and assured results.

After the scoping phase, the Fortis Cyber® TSCMI team will deploy to customer locations worldwide, wherever our client's electronic privacy is required and data is to be protected from the omnipresent threat of eavesdroppers.

The TSCMI team inspectors will work on the client site with minimal supervision and noise so as not to alert nefarious monitoring teams, and so not to disturb the established work environment which our client enjoys.

Fortis Cyber® Credentials

At Fortis Cyber®, the TSCM inspection team is drafted from world-class and prestigious security and intelligence organisations and have experience of, and insight into, a vast myriad of complex surveillance issues. The TSCM inspection team fully understand and comprehend how businesses operate and the nature of the latest risks posed by any threat: from insiders, to a criminal network or a state sponsored attack.

The TSCM team comprises a founding member of the Technical Surveillance Counter Measures Institute (TSCMi), the premier authority on the subject.

Alongside this outstanding understanding of the TSCM space, our inspectors also keenly engage with the growing physical and electrical security community, being present at specialist TSCM conferences and actively leading the thinking within the TSCMi.

To ensure we adapt in the wake of new threats, our inspectors attend many tradeshows to identify what new threat has emerged to plague the marketplace, alongside their individual study and research. For every surveillance evolution, our team are observing how the TSCM operators and technology evolve, as we watch and learn from the leading figures on information security, to maintain the integrity of the Fortis Cyber® TSCM inspections.

Through this investment, Fortis Cyber® forms a bridge between the latest thinking and capabilities in the military, the intelligence community and the commercial world. This ensures our clients receive the right advice, comprehensive support, and access to innovative, state-of-the-art capabilities unseen prior in both private and public sector Enterprise domains.

TSCM Methodology

The Fortis Cyber® TSCM team leader is a founding member of the TSCM Institute, alongside our vast experience we have engaged with both industry peers and clients over many years. With this outstanding pedigree, Fortis Cyber® has engineered a methodology which is both effective to counter-measures and efficient to the business or personal needs of the client. After the initial engagement with the customer to identify areas of concern the engagement moves on to the actual sweep itself.

Phase 1 – A comprehensive and detailed radio spectrum search. This detects active radios such as GSM, video transmitters, Wi-Fi and general RF.

Phase 2 – An electronically enhanced search employing non-linear junction detectors. This ensures eavesdropping devices are located when they are in both an active and passive state.

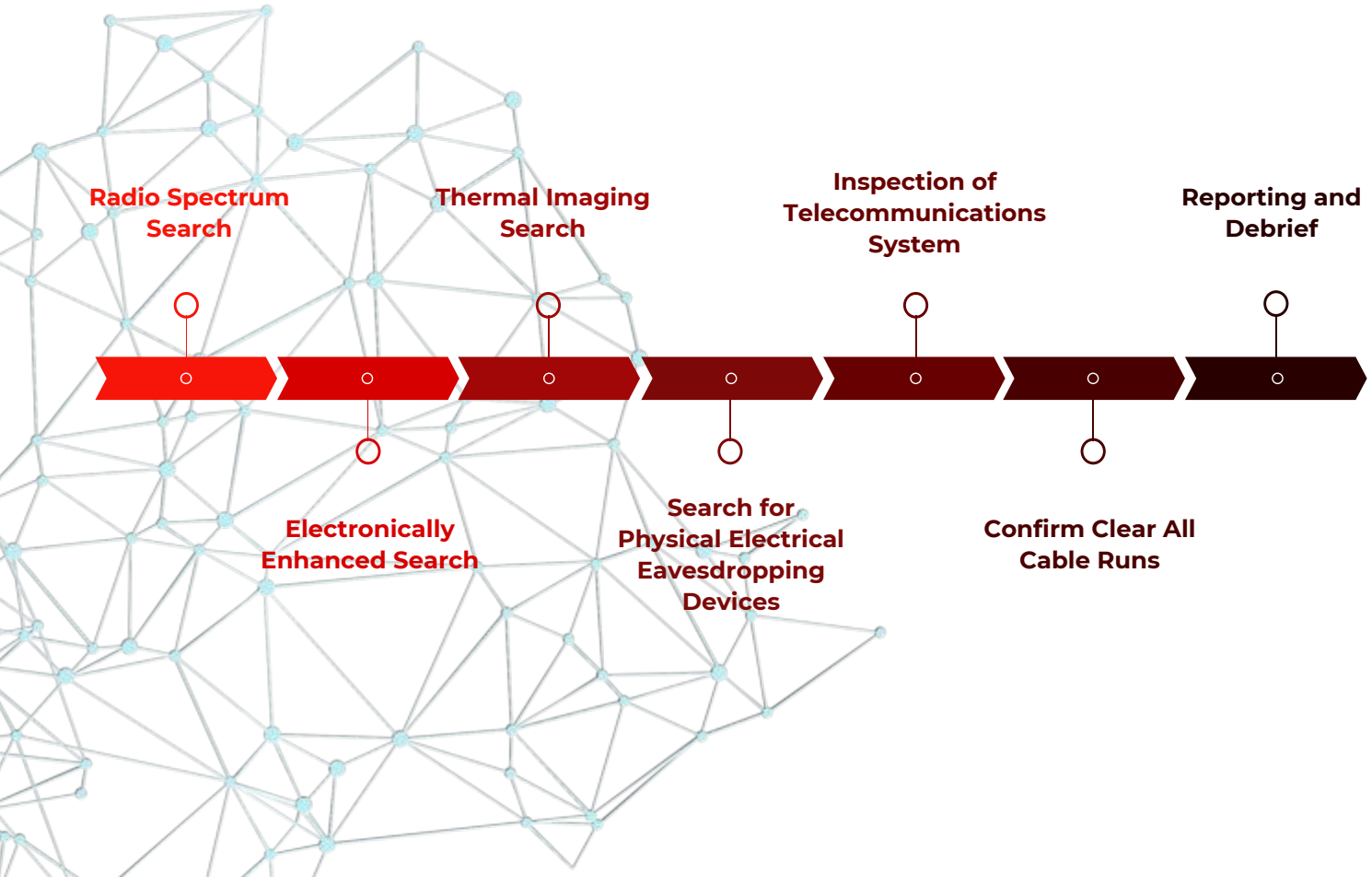
Phase 3 –Thermal imaging search with forensic light equipment. Inspects the structure of office furniture for integrated surveillance devices.

Phase 4 – Searching for the presence of computer input devices in the absence of physical electrical eavesdropping devices, preventing the threat of man-in-the-middle attacks (aka an inside threat).

Phase 5 – Physical and electronic structural inspection of telecommunications systems, their distribution points and sockets. This includes frame rooms and the main telephone intake room, which are key targets that enable attackers to scale the surveillance footprint and avoid simple counter surveillance measures.

Phase 6 – Confirm clear all cable runs using a time-domain reflectometer and BT approved test equipment. Deploying discreet and auditable tamper evidence labels.

Phase 7 – Reporting and debrief. A detailed technical threat assessment report that includes the results of both the technical and physical inspection, complete with our qualified recommendations to improve your security posture, is delivered and presented back to the client, ensuring future security upon completion of the job .



TSCM Clients

Our clients are government agencies, NGOs, banks and financial institutions, major corporations and mid-tier small to medium enterprises. The Fortis Cyber® TSCM professionals also advise individual private clients and families.

Delivering TSCM inspections of enterprise offices, exhibition spaces, hotels, vehicles, airplanes and superyachts.

Delivering TSCM inspections of:

- Enterprise offices
- Boardrooms
- Exhibition spaces
- Hotels
- Vehicles
- Airplanes
- Superyachts

Other Fortis Cyber® Services

Fortis Cyber® has built a suite of Information Security and Risk Management Services to enable organisations of any size or industry stay in control of their cyber security. By being able to identify security risks and detect vulnerabilities, companies are armed with the knowledge to more easily protect themselves, meet and respond to ongoing and changing cyber threats.

Penetration Testing & Red Team Ethical Hacking

“Taking the vantage point of an attacker and attempting to gain access”

Penetration Testing service enable clients to identify, assess and prioritise vulnerabilities and security flaws across their applications & API’s, platforms and infrastructure.

Penetration testing will help to identify security vulnerabilities which might otherwise leave your company open to compromise. Fortis Cyber® has a proven track record in finding such vulnerabilities in some of the most complex, and sophisticated IT environments. The majority of the testers Fortis Cyber® employ work on red teaming engagements as well as penetration testing. This ensures clients receive the highest level of quality, with testers often recognising scenarios that a normal penetration tester wouldn’t have the experience to detect.

The Fortis Cyber® penetration testing and red teaming group are extremely well certified, holding multiple certifications awarded by bodies such as CREST, Offensive Security and the Tiger Scheme. Fortis Cyber® also complements this focused knowledge with its National Cyber Security Centre (NCSC) CHECK & Certified Cyber Professionals to provide a valuable wider viewpoint to penetration testing assurance.

Threat & Vulnerability Management With Virtual Shield

“See the attacker’s view of your company”

Vulnerability Assessment scans will map your threat landscape, by identifying vulnerabilities and configuration issues that hackers can use to attack and gain a foothold within your infrastructure. We will prioritise vulnerabilities against your business critical services and report on when those threats are actively exploitable.

This service pairs automated tools with human interaction, providing understanding and analysis on an ongoing basis. Delivered monthly to ensure a constant reduction on a company’s risk profile; threats change daily, and systems need to be changed continuously to combat them.

This should be implemented in addition to any existing penetration testing countermeasures you have in place. This external vulnerability scanning will provide additional assurance that your risks are detected, identified and classified across your estate.

Cyber Vulnerability Risk Assessment

“Where is your security risk in the context of business operations”

CVRA is a style of information security risk assessment which includes socio-technical elements. This recognises and measures the interaction between people and technology in workplaces. Traditionally risk assessments haven’t included the people working on tech, which is a blind spot for any organisation not assessing the socio-technical component.

In order to effectively target security activities, it is important to understand the holistic risks to businesses. A cyber maturity model should include a modern risk assessment, called a cyber vulnerability risk assessment (CVRA). This offers an enterprise-wide risk assessment of the cyber security posture and awareness of your organisation and highlights key risk areas.

ISO Certification Services

“Win and retain business, stand out from competitors”

The breadth of our service portfolio enables us to offer a variety of risk management & consultancy support solutions: from a simple one-off gap analysis against a specific standard such as ISO/IEC 27001 or NIST’s Cybersecurity Framework, through to complex multi standard integrated management systems projects.

Fortis Cyber® prides itself in achieving a 100% success rate with its clients achieving UKAS Accredited Certification to ISO 27001, 9001, 14001 and many other management systems standards ‘first time, every time’.

Fortis Cyber® will continue to work with your organisation beyond certification to support it with the ongoing maintenance of system. Fortis Cyber® does this by providing an innovative and pragmatic risk-based approach across the organisation, helping maintain legal obligations, drive down cost and increase profit.

Digital Forensics

“Identify what really happened”

Fortis Cyber® offers a complete, digital forensic investigations package to establish and identify the cause and source of cyber incidents. These events are instigated by internal or external threat actors. These services are carried out by experienced and certified investigators who will utilise versatile and powerful software and technology solutions to undertake digital forensic investigations & data restoration services.

Please get in touch

https://www.fortiscyber.co.uk/contact

enquiries@fortiscyber.co.uk

+44 (0) 207 898 3971

Fortis Cyber Security Limited is a limited company registered in England and Wales.

Company Registration Number: 11162256

VAT Registration Number: 291874659