Securing your IoT systems

Ready?

vodafone business

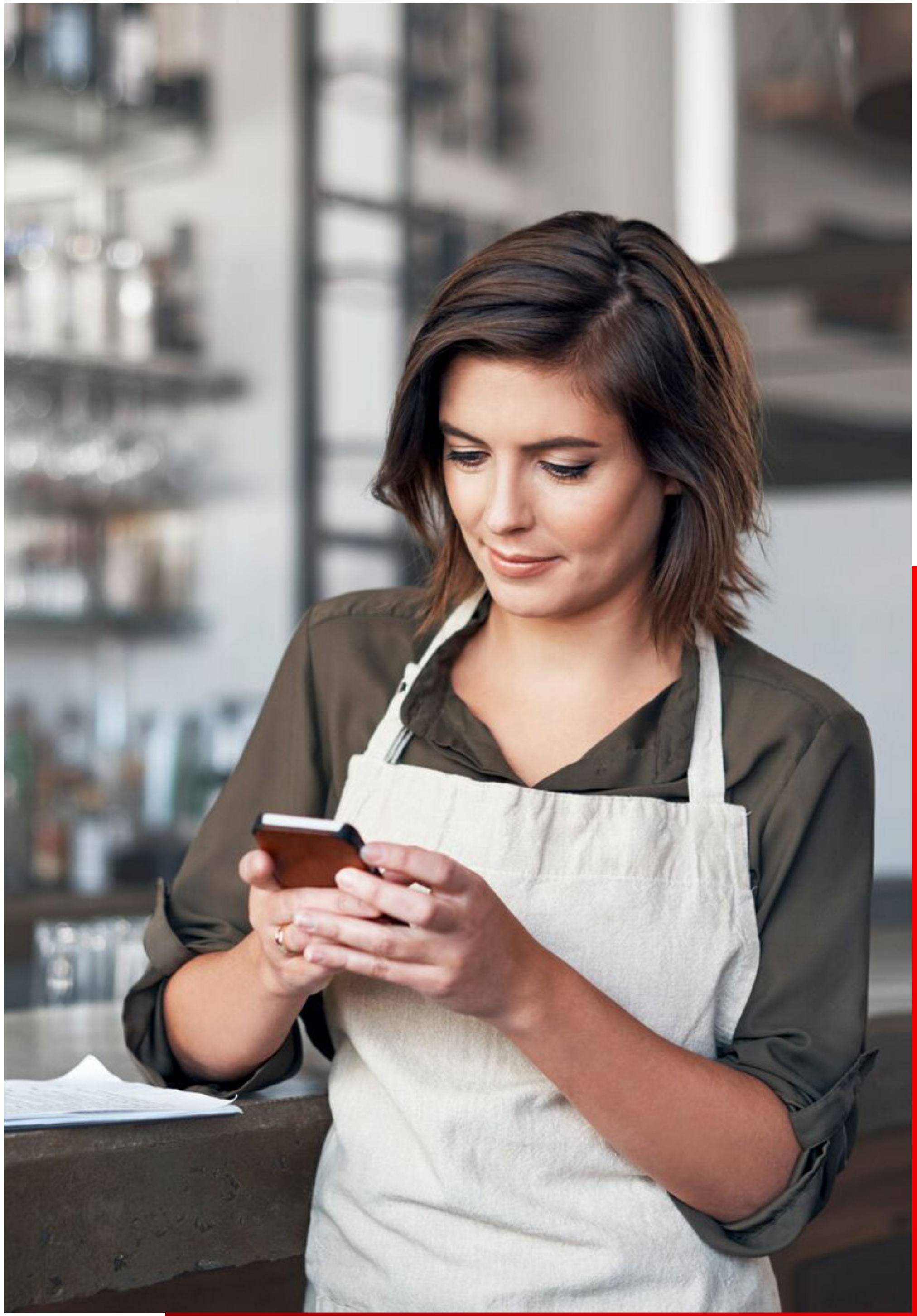
IoT Security Assessment

From public buildings to healthcare facilities and smart cities to connected vehicles, all are increasingly reliant on networks of sensors and actuators known as the Internet of Things (IoT). As IoT systems become ubiquitous in our homes and daily lives, it is imperative that IoT solutions, applications, infrastructure and associated data remain secure. Vodafone works closely with its independent security partner to provide a security assessment service. We can help you identify, understand and manage security risks against all aspects of IoT systems alongside the physical environment and the people that configure, manage and operate them.

What do we offer?

IoT Security Assessment gives you the essential knowledge you need to understand the security posture of your IoT systems and plan appropriate countermeasures and mitigating actions.

Security Assessment will help you secure your organisation and operation from those who seek to damage your organisation and its operations.



Experience at your service

Our industry-leading consultants have extensive experience of securing IoT and related technologies. By assessing the threats to your IoT deployment against the consequences of a breach of security, we can provide you with a comprehensive profile of the IoT risks to help prioritise security resources.

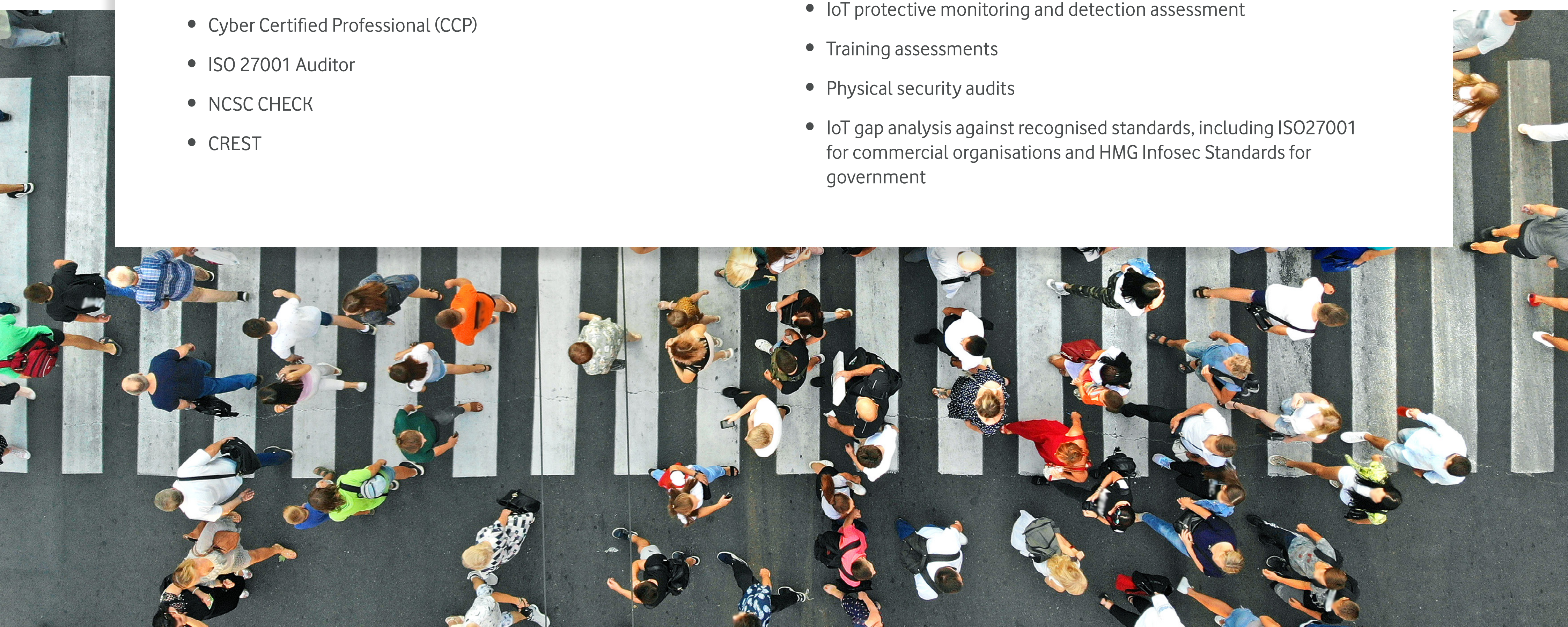
We have access to consultants who have a wide range of industry-recognised qualifications and certifications including:

- Certified Information Systems Security Professional (CISSP)
- Cyber Certified Professional (CCP)
- ISO 27001 Auditor
- NCSC CHECK
- CREST

Benefits from Security Assessment

With our consultancy, you will benefit from:

- IoT risk assessment, using multiple tools tailored to the organisation, including Cyber ADVANTAGE, STREAM, C2M2 and CNI Cyber Assessment Framework (CAF)
- End-to-end and infrastructure security assessment including 5G platforms
- IoT criticality, continuity and recovery planning assessments to ensure that operations can continue in the face of malicious activity
- IoT protective monitoring and detection assessment
- Training assessments
- Physical security audits
- IoT gap analysis against recognised standards, including ISO27001 for commercial organisations and HMG Infosec Standards for government



Security Assessment approach

Due to the large attack surface and range of hardware, software, firmware and communication protocols involved in IoT compared to web or mobile applications, IoT security assessments can be much more challenging. A successful IoT security assessment requires the consideration of the end-to-end architecture – this would typically require all IoT endpoint devices, communications infrastructure, and hardware and software components to be assessed. Individual IoT devices and interactions with the wider estate will need to be considered to understand vulnerabilities or the potential for vulnerabilities. We will consider your IoT critical business processes, information flows and the technology you use to support your operation. Once the architecture and component interactions are understood, then a comprehensive assessment plan can be developed. This may range from a simple desktop study to the involvement of ethical hackers and red team specialists who can try and attack the IoT system, using a number of attack vectors developed from the initial assessment phases. The final stage will be to consider the profiles of threat agents against the profile of your organisation and to see where any overlap occurs. We will consider the capability of the threat agent and your IoT vulnerabilities and weaknesses. IoT is expected to grow to over 29 billion devices by 2022. It is almost certain that attackers will target vulnerable IoT installations using similar tactics to those seen today on desktop and mobile devices. It is important therefore that security assessments are undertaken as early as possible in the IoT deployment and regularly, especially when changes are undertaken. Our consultants are regularly asked by the media for commentary on IoT; an extract from one such article can be seen below:

> "We have seen plenty of ransomware attacks where computers are encrypted by hackers and only decrypted if the company pays money; it is very easy to see a scenario of such an attack on a building management system, where a factory or hospital is disabled and hackers request payment."

From BBC News: Tomorrow's Buildings: Help! My building has been hacked

Why Vodafone?

Vodafone has more than 20 years' experience in the IoT arena with more than 1,300 dedicated IoT experts. We bring unrivalled capabilities together as one of the world's largest mobile networks with outstanding customer experience and a long track record of success with more than 100 million IoT connections deployed.

Our customers are confidently connected, receiving unmatched services, experience and benefit from proven expertise. Vodafone will enable you to harness the full potential of IoT technology with a range of professional services and keep your organisation ahead of the game.

Next steps

To discover more about how IoT Security Assessment from Vodafone can help your organisation optimise your IoT solution effectively and affordably, contact **IoT@vodafone.com** or visit **vodafone.com/business/iot.**

www.vodafone.com/business

Ready?

vodafone
business