Security Testing

QinetiQ Digital Resilience

As the reliance on digital systems increases and the sophistication of cyber-attacks continues to grow, it is important that organisations regularly test their ability to defend themselves from digital compromise. Many organisations invest heavily in digital security controls and have spent time and effort developing procedures and processes to counteract cyber-attack, but many have never tested these to see if they are fit for purpose in this ever evolving digital world.

It takes regular and repeatable testing cycles to ensure that an organisation is ready to protect and respond to comprise of digital platforms and it often requires sophisticated approaches to replicate and simulate the types of attacks an organisation may face. In many cases testing needs to go far beyond simple exercising of digital systems to identify potential vulnerabilities and move more towards actually testing the resilience of a company's digital estate and associated operations.

QinetiQ has a well-established pedigree in providing testing mission critical services and capabilities for the UK public sector and defence communities, and has built on this to develop the longest established dedicated security and penetration testing team in the world.

QinetiQ's experts can work with organisations to simulate real-world scenarios and test the digital systems of an enterprise in a way that emulates the attack methods threat actors in order to practically, but safely and ethically, test an organisation's digital resilience posture.

The service follows three key principles to personalise the service and deliver exceptional security value. They are:

Advanced Intrusion Testing
Bringing to bear the vast experience of over two decades of vulnerability assessment, classical penetration testing, responsibly conducted red-team cyber-attacks and real world attack simulation, including social engineering. This element of the services assesses the robustness of the digital and physical controls, and human practices as they are actually used within customer's organisation, comparing them to prescribed authorised and expected behaviours, helping to identify attack vectors which may be overlooked by more tightly scoped penetration testing. This allows our customers to understand the real impact of identified vulnerabilities and measure the skill level that might be required by an attacker in order to exploit them.

Penetration Testing
QinetiQ's subject matter experts undertake testing which aims to simulate attacks against a target application or network systems, using the same tools and techniques as the most highly skilled adversary. The aim is to identify areas of technical risk and present them in an easily understandable, prioritised and actionable format, which allows customers to take appropriate steps to rectify digital controls. The service can also offer security cleared staff with both industry standard CREST and CHECK qualifications, providing a level of assurance to customers that penetration testing activity is carried out to the highest standards.

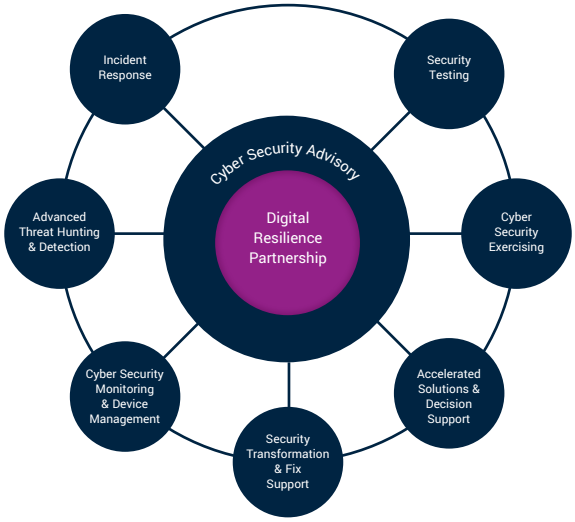
Communication Testing
Building on QinetiQ heritage in radio frequency, satellite and wider communication technology research and development, and with the growing dependency of digital systems on communication, QinetiQ's experts can work with organisations to test these platforms from end to end. Encompassing network configuration, wireless propagation, network jamming and local interference, the service enables customers to build resilience into their communication systems and prevent them from becoming an attack vector or point of comprise.

QINETIQ

Digital Resilience

This service forms part of a wider service portfolio, which seeks to helps organisations mature their digital resilience and to help build confidence in their ability to deal with cyber-attacks, through a holistic approach. The main integration points for this particular service are:

- **Cyber Security Monitoring & Device Management** - Is informed by this service to ensure that Security Operations Centre (SOC) monitoring and detection controls are functioning as intended
- **Advanced Threat hunting** - Is informed by this service to improve detection capabilities in relation to new methods of attacks identified through testing
- **Incident Response** - To help safely drill incident response and incident reporting procedures to ensure that they would be effective during a real cyber-attack



Key Features & Benefits

Vulnerability Identification - Helps organisations identify critical vulnerabilities in their digital systems and operations, which may expose them to risk of compromise

Better Decision Planning - Allows organisations to take a systematic approach to risk mitigation, provides a prioritised view of system vulnerabilities on which action can be taken

Building Confidence - Gives organisations a level of confidence in their digital and physical controls, thus allowing a board to assess their level of digital resilience

Improved Defensive Capabilities - Testing helps organisations better understand their defensive capabilities and to test security operations across the enterprise.

Intelligence-led QinetiQ's extensive exposure to a variety of targeted industries provides us with an excellent insight across the cyber threat landscape. Leveraging this breadth and depth of knowledge enables QinetiQ to tailor testing to match real-world attack scenarios and build a realistic picture of the risks an organisation faces.

Collaborating with QinetiQ

At QinetiQ we bring organisations and people together to provide innovative solutions to real world problems, creating customer advantage.

Working with our partners and customers, we collaborate widely, working in partnership, listening hard and thinking through what customers need. Building trusted partnerships, we are helping customers anticipate and shape future requirements, adding value and future advantage.

www.QinetiQ.com

QinetiQ/19/01784

For further information please contact:

Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX
United Kingdom

+44 (0)1252 392000
customercontact@QinetiQ.com
www.QinetiQ.com