



# Security Transformation and Fix Support

## QinetiQ Digital Resilience

As organisations continue to invest in digital systems and conduct digital transformation programmes, they run the risk of failing to adequately address cyber security to ensure digital resilience, often leading to systems that are fundamentally vulnerable. This means that organisations are exposed to increased levels of threat from cyber-attacks, through their continued adoption of digital tools and technologies.

QinetiQ's team of seasoned industry experts bring together best practices from across industry and defence along with cutting-edge technology to deliver leading assurance services to our customers.

Our Security Transformation and Fix Support Service engages with customers across a broad range of digital transformation programmes. We advise on the best approaches to security architecture, as well as providing hands-on expertise to help customers configure and extract value for money from security products and technologies.

This service provides guidance on security approaches and design principles. It is relevant to both those planning or entering transformation programmes and those who are within or completing programmes as a retrospective activity.

The key objective of the service is to understand the customer's cyber risk profile, how it relates to the business and organisation and to ensure that digital systems are appropriately designed and delivered to mitigate the risks.

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

### **Security Architecture**

Designing systems with cyber security as a key cornerstone and fundamental principle is a significant step towards achieving a high level of digital resilience. Our experts have years of experience in helping organisations build and deploy digital systems using well developed security architectures and approaches.

We work closely with transformation and technical teams to ensure at all stages digital resilience is considered and that appropriate security controls are effectively deployed. QinetiQ's approach takes into account current thinking of industry leaders, such as the NCSC, follows industry standards such as NIST and SANS and is capable of integration with wider solution and enterprise architecture standards, such as TOGAF.

### **Security Engineering**

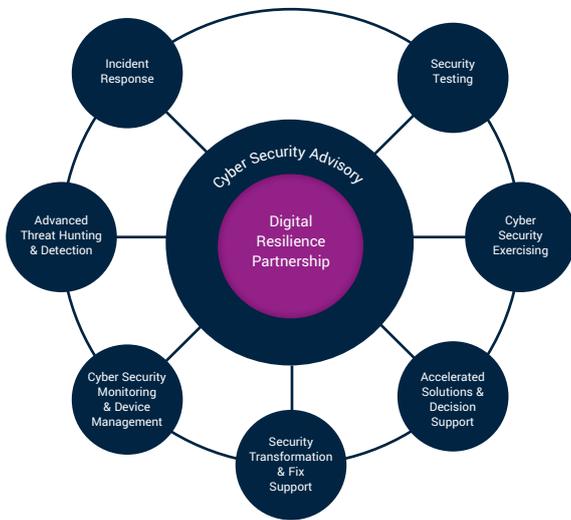
We recognise that organisations may have already invested in security technologies as part of their digital transformation, and that getting the most from this investment is important. Our team of highly trained and experienced security engineers can work with a wide range of security technologies to ensure that they are appropriately deployed and configured to address threats to the organisation.

We can support the initial deployment of these technologies, as well as retrospectively reviewing existing deployments, to help align configuration and policy to address relevant threats.

## Digital Resilience

This service forms part of a wider service portfolio, which seeks to help 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** - will be more effective on a better architected and configured digital system
- **Cyber Security Exercising** - can provide greater value by focussing on non-technology aspects in the confidence that these have been addressed
- **Cyber Security Advisory** - shared insight of risks and digital systems enhance the value delivered by both services to address customer threats



## Key Features & Benefits

---

**Threat Mitigation** - The service helps to ensure that digital systems are configured in a way that helps to minimise risk exposure across an organisation

---

**Maximise Investment** - Help organisations extract value from previous investments in security technology and help show at board level the return on investment

---

**Security by Design** - By working with transformation teams we help place security at the heart of our customers' digital strategy and help implement this as a cornerstone of digital transformation activity

---

**Inform Investment** - By supporting decision processes and helping inform security investment strategies, value for money is optimised against customer objectives

---

**Professional Advice** - Access to a wide range of cyber security professionals in both the architecture and engineering domains to help guide and deliver resilient digital systems

---

**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 employ defensive capabilities throughout the cyber kill-chain, helping to ensure digital systems are deployed and managed commensurate to the threat landscape.

---

## 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](http://www.QinetiQ.com)

Copyright QinetiQ Ltd 2019 | SECURITY TRANSFORMATION AND FIX SUPPORT

### 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

QinetiQ/19/01808