

Identify | Protect | Detect | Respond | Recover

Cyber Transformation and Remediation Support Services

A QinetiQ Cyber Security Service

Key Benefits

- Enhance collaboration with customers and partners
- Enable a secure single global identity
- Foundation for secure information exploitation
- Targeted cyber remediation services fulfilling business security requirements.
- Cost effective approach to deliver business improvements based on identified risks.
- Controlled to ensure minimal business impact and cost.
- Provides additional resources to support cyber assurance requirements within the business.

Digital transformation enabled by good security engineering has obvious security benefits, enabling hardware and software to receive security patches and embedding the latest security features.

Digital Transformation offers the opportunity to retain key information within the organisatonal boundary, while giving controlled access to customers and partners. A range of Use Cases can be met out of the box with functionality provided by Cloud services, while other techniques such as Virtualised Infrastructure can be used to provide secure access to parties whose ecosystems aren't directly compatible. We can help you to understand your Use Cases and how best to extend collaboration functionality to your different groups of customers/partners.

Over time, as organisations grow organically, their users accrue numerous different identities and credentials. This gets expensive and difficult to manage and increases the risk of accounts remaining live long after their owners have moved on. Cyber Transformation offers the opportunity to unify a user identify into a single "Identity Provider", with Single Sign-On allowing for secure token passing between applications. This simplification enables the Joiners, Movers & Leavers (JML) process to be managed from a single place, dramatically improving an organisation's security posture. Account provision and revocation can be achieved almost instantaneously, and account changes can cascade throughout the applications estate as part of a single process.

Large and well-established organisations have amassed huge quantities of valuable information over their lifetime. But all too often, it's spread across a multitude of different repositories and hidden behind different access controls. It is difficult to re-purpose valuable information in the long term, and over time people forget it exists. Information is expensive to keep yet might pay for itself many times over if only its value could be leveraged. Cyber Transformation offers the opportunity to apply metadata enrichment to your information estate. Sophisticated tooling such as A.I. can be configured to work securely across your internal boundaries, recognising patterns and surfacing business intelligence to inform more efficient ways of working.

Following an incident, in depth penetration test or extensive audit, your business may have numerous vulnerabilities to prioritise and fix. It is difficult to evaluate what actions need to be taken and to prioritise remediation in a way that maximises efficiency whilst minimising business disruption.

Coordinating remediation with a variety of suppliers takes your staff away from their front-line duties causing an adverse impact to your core business functions.

Typical remediation activities can include excessive technical jargon and you need subject matter experts to translate it into business impact so you can decide on actions to take.

Our team will work with you to understand your business, map the interconnections and agree a suitable remediation approach to rapidly reduce operational risk whilst minimising disruption to business operations.

Why QinetiQ

Our teams have vast experience with a range of Defence, Government and Critical National Infrastructure clients who operate in complex environments with multiple supply chain connections. We help those clients to build greater resilience to attack within their complex environments by supporting them to design secure solutions from the outset, undertake secure digital transformation or remediate identified gaps in existing solutions.

We are part of the NCSC Assured Cyber Security Consultancy (ACSC) scheme and Cyber Resilience Audit (CRA) scheme offering security audit, risk management and security architecture support to clients.

Our security expertise has been used to support complex multi-year IT transformation initiatives with a need to make sound security judgements to reduce attack paths, promote secure infrastructure and remediate issues and technical debt whilst ensuring an effective end user experience.

We work closely with stakeholders to identify and understand the areas of greatest business impact by undertaking a discovery and modelling phase. This is key to identifying and categorising potential security risks in a system and producing transformation and remediation roadmaps focused on the key areas so as to achieve outcomes in a timely and least disruptive manner.

Service Description Model

Our staff will partner with you in a phased approach to review and prioritise transformation and/or remediation. Our approach seeks to minimise disruption to your business activities by working to achieve your desired outcomes which we will agree at the start.

Discovery and Modelling Phase

Our discovery will define the systems in scope, their interconnections and the areas of greatest impact. We will produce business -focused cyber security models to clearly communicate the system and structure our modelling approach at different levels which abstract to more detailed system models.

Secure Design and Engineering Phase

Based on the defined model and areas of greatest concern, we will produce an action plan to implement a more effective secure solution. These could be isolated fixes, or consider key security improvements such as segmentation, information flow controls or applying zero trust controls to secure your key assets.

The engagement plan we produce will agree and prioritise transformation, remediation and improvements with identified stakeholders including external suppliers. This is crucial to confirm responsibilities and to agree a workable plan to achieve the outcome. The plan will be a living and iterative document to show overall progress,

Our expertise across a range of information systems means we are well placed to discuss technical matters with suppliers and focus their efforts on effective transformation or remediation. We can manage change requests in consultation with affected stakeholders.

Detailed Security Analysis

We will support you to validate that remediation has been successfully applied through testing of controls and will produce evidence packs in order that you can communicate and assert progress for any reporting or regulatory requirements. Success is achieving this with minimal disruption to you and your business by aligning our reporting to your standard operational reporting procedures.

We will produce attack path reports showing how the remediation of issues has reduced the viable attack paths over time and what the remediation has done to alter the risk profiles.

QINETIQ

Other QinetiQ Cyber Services

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.

This service is a sub-service of Cyber Security Advisory.

Why QinetiQ Cyber

- Unmatched team of vetted, expert cyber consultants, architects, engineers and human performance scientists
- Unique experience and patented intellectual property in securing the world's most complex, safety critical environments
- UKCSC registered cyber professionals, NCSC Assured Services

For further information please contact:

Malvern Technology Centre
St Andrews Road,
Malvern
Worcestershire, WR14 3PS
United Kingdom

+44 (0)1252 392000
cyberenquiries@QinetiQ.com

Copyright QinetiQ Ltd 2026 | CYBER REMEDIATION SUPPORT SERVICES

QINETIQ IN CONFIDENCE