

Cyber Secure by Design and Security Architecture

A QinetiQ Cyber Security Service

Key Benefits

- Visualise and understand cyber risk across all domains at an enterprise level
- Integration of cyber security into standard delivery processes
- Security risk management embedded throughout the whole lifecycle of system development
- Creation of resilient business operations
- Reduced complexity and increased operational pace through the delivery of standard outputs
- Regulatory frameworks used to improve security rather than just compliance

The culture and approach to how cyber security is being addressed in organisations needs to change. Cyber security is often viewed in a silo, or added in retrospectively and not part of the organisations standard delivery processes. This does not give organisations the best chance to keep their business operations secure.

At QinetiQ, we are helping organisations to advance their digital resilience towards a business systems level view, integrating cyber security into standard delivery processes, enabling a context aware security culture to become secure by design. A central concept of Secure by Design is that security risk management needs to be embedded throughout the whole lifecycle of system development from inception to design, implementation and service. Our Secure by Design approach will lead to the delivery of more secure business operations through better integration, simplified and consistent processes, clearer guidance, more flexibility and empowered decision making.

The QinetiQ Approach

We have a large team of in-house Cyber specialists, supported by an extensive supplier network of Subject Matter Experts to provide specialist expertise on projects and programs beyond security architecture where required. Between our in-house staff and partners, we have access to an extensive partner network with access to Security Information Risk Advisors and Security Architects cleared to SC or higher.

- Best Expert' approach using partner ecosystem enabling agility & sustainability
- In house SQEP resources, with experience of technology domains including monitoring and IT and OT knowledge and expertise
- Proven delivery model for MOD, Government and Industry
- Familiarity with Traditional and Agile approaches to project delivery
- Core team consistent throughout project life, with supporting resource as required
- Understanding of working to constraints, no two systems are the same especially when dealing with specialised environments with high security needs.
- Cutting edge security tools and methods

Resilience engagement model

We use a standard engagement model, which has proven successful across a number of projects and clients in both Government and industry. The security engagement model is illustrated in the figure below

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing
CREST PEN TEST
THE CYBER SCHEME



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.

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
- NCSC Certified Cyber Professionals and Services

For further information, please contact:

Malvern Technology Centre
St Andrews Road
Malvern
WR14 3PS
+44 (0)1252 392000

Cyberenquiries@QinetiQ.com

www.QinetiQ.com

Copyright QinetiQ Ltd 2024