Secure by Design

A QinetiQ Cyber Security Service

Key Benefits

- Understand your assets and actively track them
- Establish centralised security governance
- Avoid needless complexity in already complex systems
- Anticipate failure.

Secure by Design is a principles based approach to Cyber Security assurance that has been adopted by the MOD and promoted by the NCSC. Instead of rigid rules, this approach relies on a set of principles to guide decision-making. These principles serve as general guidelines, allowing flexibility in adapting to diverse situations. The MOD principles are broadly arranged around: understanding, planning, risk management, security controls, supply chain security, test and evaluation, and through life management. These can easily be adapted for different scenarios and the driver is to reduce, checklist type security activity and improve cyber risk ownership and management.

QinetiQ's Secure by Design approach can help you to hasten delivery, improve user experience and product resilience. Security can be seen as a separate & disruptive activity to capability delivery, and is consequently often delivered as a bolt-on task post-production that might require redesign, increasing cost, and potentially resulting in disruption or delay to delivery.

.

We will enable you to understand your assets and actively track them, mapping organisational networks, how components interact with each other, and information flow, along with the business impact of loss events.
Establish centralised security governance, with clearly defined roles, responsibilities and accountability.
Structure security governance, process and controls around business and capability objectives.

Elevate the importance of user experience in defining approaches to security. Design capability to actively enhance rather than impede operational delivery. And in doing so, improve user experience and avoid workarounds.

We'll use pre-built and replicated secure images and infrastructure to deploy capability at scale.
Breaches and disruption are inevitable and uncontrollable, but you can control how you respond, including contingency planning, disaster recovery and rigorous testing of failover and resilience.

Incident response plans, contingency measures and disaster recovery mechanisms mean little if you do not test them ensure that your business continuity mechanisms actually work by engaging through our Cyber Exercising offering.
Embedded security testing throughout the capability delivery process.
Automation to remove the likelihood of human error as much as possible and reduce mental fatigue.

CHECK
IT Health Check Service

CREST

THE CYBER SCHEME

The QinetiQ Approach

Our approach embeds within your development cycle whether that is an engineering lifecycle approach or agile delivery. We remove duplication of effort by avoiding a separate security track and support existing platform engineering and reliability teams through:

- Secure by default. Secure platform configuration is the default baseline, reducing workload in manually configuring.
- Planning to respond to failure scenarios.
- Framing security controls through the lens of a Business Impact Analysis (BIA).
- Supporting Agile delivery environments, embedding resilience statements into user stories.
- Mapping mission critical functions, and designing in mitigations against failure scenarios.
- In cloud environments, re-use template design patterns and hardened images that allow patches and fixes to be consistently deployed.
- Reduce complexity.
- Make replication and redundancy easier to implement.
- Apply the same mindset to processes as well as technology, deliberately designing process to make the secure way the easy way for user and operators, and reduce cognitive fatigue.

Our test, exercise and verification offerings complement the Secure by Design philosophy, and range from scenario-based penetration testing through full spectrum read teaming and to organisation-wide cyber exercising.

Effective security governance brings it all together. QinetiQ's Secure by Design strategy enables capability delivery teams by:

- Supporting senior leadership teams, at board-level, understanding the mission focus of the organisation, and how Secure by Design embeds in their risk management strategy.
- Define what legal and regulatory requirements that organisational systems are required to meet.
- Clarify risk and incident management, with clearly defined roles, responsibilities, and escalation paths.

Service Summary

QinetiQ is a market leader in the provision of cyber security services. Our secure by design service will work with you to maximise your ability to respond to a cyber-incident We understand the challenges of due diligence and meeting regulatory requirements; helping you to navigate these issues and have in place the capability you need.

Additional Support 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.

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
Worcestershire, WR14 3PS

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