Purple Teaming and Actionable Intelligence

A QinetiQ Cyber Security Service

Key Benefits

* Targeted threat actor emulation in a safe environment
* Exercising SOC capabilities in real time with attack methodologies
* Uses spear-phishing and OSINT
* Provides real, actionable intelligence against security posture OSINT
* Assess an organisations security from a human perspective

The best time to test a Blue Team and an organisation's resilience is before it is attacked. QinetiQ's Purple Team exercise is designed to team up our Red Team specialists with your Blue Team defenders to identify tools, signatures and techniques used by threat actors before they become a problem.

Understanding that people form the first and most important part of an organisation's defence, QinetiQ's Social Engineering service helps identify if your staff training and security culture have been embraced, understood and implemented. Social Engineering can be tested through spear phishing with emails, phone calls, text messages, or in person.

The QinetiQ Approach

QinetiQ's subject matter experts will undertake testing that aims to simulate attacks against a target application or network using the same tools and techniques as the most highly skilled adversary.

Throughout this process QinetiQ experts liaise with the customer to ensure they are kept informed of progress. All engagements are expertly managed from inception to delivery and include the generation of clear and concise reporting in a timely manner.

Our reports prioritise areas of technical risk and present them in an easily understandable and actionable format.

QinetiQ can offer security cleared staff with both industry standard CREST and CHECK qualifications.

QinetiQ's SHC team continues a strong heritage of innovation, leading the way in Red Team exercises by challenging the normal penetration testing paradigm. The Red Teaming service identifies those attack vectors which may be overlooked by more tightly scoped penetration testing exercises, culminating in highly focused technical reporting and leading to deeper insights for our customers.

CHECK
IT Health Check Service

CREST

TIGERSCHEME
Providing excellence in penetration testing

QinetiQ's Security Health Check (SHC) team has a strong heritage of innovation and continues to lead the way by challenging the normal penetration testing paradigm.

SHC understand that the most accurate way to prove if processes and defence systems are able to detect, identify and respond to incidents is to use them on real world cyber-attacks and that real incidents are not limited to a single application or system. By emulating real world threat actors SHC enable our customers to see the real effect of the tools and techniques, highlighting where to concentrate network defence measures and monitoring.

Expert simulation of real-world threat actors and methods

Over two decades of experience and Discretion

All Staff hold UK security clearances.

Service summary

The best time to test a Blue Team and an organisation's resilience is before it is attacked. QinetiQ's Purple Team exercise is designed to team up our Red Team specialists with your Blue Team defenders to identify tools, signatures and techniques used by threat actors before they become a problem.

Threat Intelligence
QinetiQ's own Threat Intelligence team produce a technical report to inform the security specialists of the tools and technologies utilised by threat actors specifically for the target organisation.

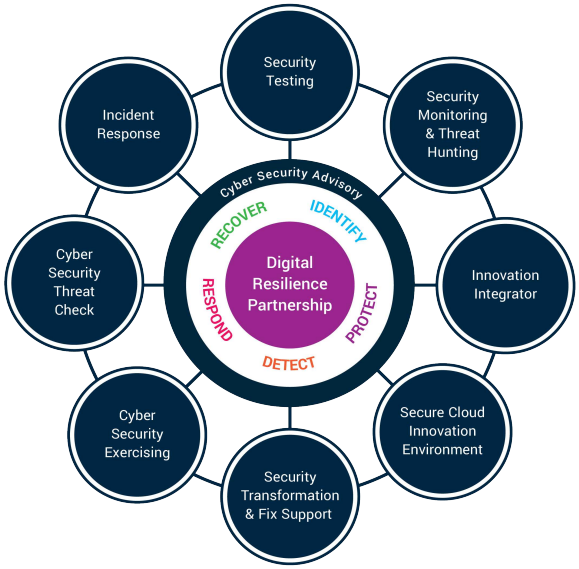
Open Source Intelligence OSINT
QinetiQ experts use the latest techniques to identify individual targets within our customer's business. By leveraging the information discovered from this phase it's possible to test whether social engineering, phishing and s pear phishing awareness campaigns are providing the desired effect. SHC never identifies individual employees or discloses which employees were successfully targeted.

Social Engineering
QinetiQ experts, backed by years of practical experience, will give an organisation a view of how easily its internal processes and staff can be manipulated to divulge sensitive information or to perform actions which might make further attacks possible.

Phishing
Blocking a cyber-attack within the first steps in the attack chain is key to cost effective network defence. When attempting to gain a foothold an attacker may attempt a targeted/sophisticated spear-phishing attack in an attempt to execute code on a workstation to establish a command and control channel within the target's estate. SHC will examine the organisation's security posture and readiness with regards to these initial infection/attack vectors.

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 Security Testing.



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

QINETIQ/SHC/20/0106

For further information please contact:

Malvern Technology Centre
St Andrews Road
Malvern
WR14 3PS
United Kingdom
+44 (0)1252 392000
SHC@QinetiQ.com
www.QinetiQ.com