Red Team Cyber Attack Simulation

A QinetiQ Cyber Security Service

Key Benefits

- Emulates real world threat actors and vectors in controlled environments
- Uses network implants, spear-phishing and OSINT
- Provides real, actionable intelligence against security posture
- Gains a foothold on internal and external networks

Safely emulating the cyber elements of a targeted attack, network implants, spear-phishing, and Internet-based attacks can be the starting point, with the goal being lateral movement through the network towards key assets, and ultimately exfiltration. Examining the effectiveness of security controls, accuracy of alerting, and efficacy of incident response playbooks.

The challenge for organisations is to facilitate the sharing of information in a controlled and resilient manner for legitimate business purposes; whilst at the same time protecting information that should not be shared, altered or disrupted.

The QinetiQ Approach

QinetiQ's Red Team exercises are designed to deliver a fast paced and intensive cyber adversary simulation over a set period. For this offering, the SHC adopts the attributes of an adversary that is less concerned about stealth and attribution than about the ability to complete their exercise objectives and withdraw before the organisation can detect and mitigate the threat.

QinetiQ's Red Teaming service consolidates over two decades of experience delivering infrastructure and web application testing, open source intelligence gathering, and classical penetration testing. The Red Team service provides the highest levels of assurance by challenging our customer's assumptions of security by adopting the real world adversarial methodologies, tools and techniques used by highly skilled, highly motivated attackers.

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.

CREST

CHECK
IT Health Check Service

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

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 spear 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.

Infrastructure Testing

Testing can simulate external attack, giving an organisation a view of its exposure to multiple attack groups, and allowing customers to gauge whether their current security architecture gives them sufficient

Defence in Depth.

Application Testing

Application tests assess the threat from both authenticated and unauthenticated attackers to published applications. Testing will look at many areas of potential concern including user and role separation, session management, input validation and logic errors.

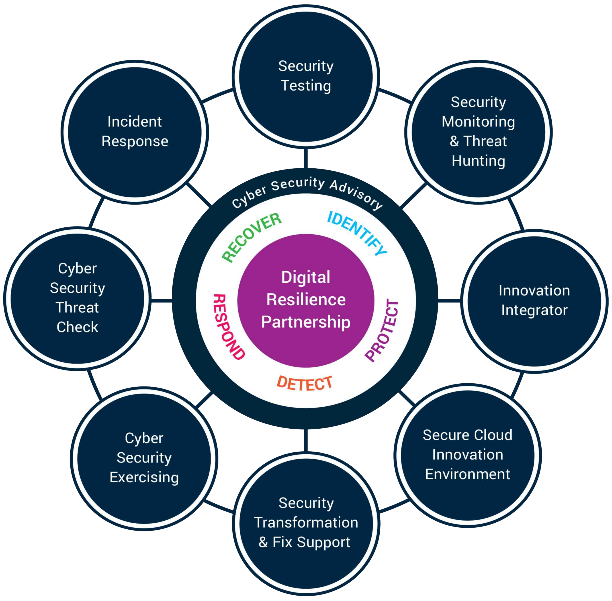
Phishing

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.


Security Testing
Incident Response
Security Monitoring & Threat Hunting
Cyber Security Advisory
RECOVER
IDENTIFY
Digital Resilience Partnership
RESPOND
PROTECT
DETECT
Cyber Security Threat Check
Innovation Integrator
Cyber Security Exercising
Secure Cloud Innovation Environment
Security Transformation & Fix Support

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 Worcestersh
ire, WR14 3PS
United Kingdom
+44 (0)1252 392000
SHC@QinetiQ.com
www.QinetiQ.com