

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.
- Gains a foothold on internal and external networks.
- Provides real, actionable intelligence against security posture.

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 Red Team is able to independently and objectively examine the effectiveness of your security controls, the accuracy of your alerting, and the efficacy of your incident response playbooks.

The Red Team does this by safely emulating the cyber elements of a targeted attack, including network implants and spear-phishing. Internet-based attacks can be their starting point, with the Red Team goal being lateral movement through the network towards key assets and ultimately making data/asset exfiltration.

The QinetiQ Approach

QinetiQ's Red Team exercises are designed to deliver a fast paced, realistic and intensive cyber adversary simulation over a set period.
For this offering, the Security Health Check (SHC) team 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 more than two decades of experience in 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 customers' security assumptions through 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.

QINETIQ IN CONFIDENCE

QinetiQ's 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 whether processes and defensive systems can detect, identity and respond to incidents is emulate real world cyber-attacks using real-world informed incidents that 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 attack tools and techniques, highlighting where the customer needs to concentrate their network defence measures and monitoring.

Expert simulation of real-world threat actors and methods.

More than two decades of experience and innovation.

Client confidentiality and discretion.

All staff hold UK security clearances.

Service summary

Threat Intelligence

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

Open Source Intelligence OSINT

QinetiQ SHC experts use the latest techniques to identify individual targets within our customer's business. By leveraging the information discovered from this phase it is 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. This enables a positive learning experience for customer staff without the fear of attribution.

Social Engineering

QinetiQ SHC experts, backed by years of practical experience, will give an organisation an evidence-based 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.

Application Testing

Application tests assess the threat to published applications from both authenticated and unauthenticated attackers. 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 during the first steps in the attack chain is key to cost-effective network defence. When trying to gain a foothold an attacker may attempt a targeted/sophisticated spear-phishing attack in an effort 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 security 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.
- Cyber Scheme assessed professionals, registered with the UK Cyber Security Council and NCSC.

Copyright QinetiQ Ltd 2024 | Red Team Cyber Attack Simulation QINETIQ/SHC/20/0106

For further information please contact:

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