Cyber Intrusion Exercise (CIE)

A QinetiQ Cyber Security Service

Key Benefits

* CIE's use the latest real-world simulated attack delivery methods, to determine how attractive your organisation would look to a motivated and determined adversary.

* CIE's can regularly exercise and provide visibility of the robustness of your organisation's internal technical controls and assure the impact and effectiveness of your third-party investments.

* Helps to fast track your organisational resilience by benchmarking and providing recommended remedial improvements clearly and concisely, from critical to low.

* CIE's provide a much higher level of organisational coverage and assurance by complementing conventional annual, compliance-driven testing, and therefore delivers more value for money to your business.

Optional on-site physical security/perimeter assessment, within the same exercise.

A Cyber Intrusion Exercise (CIE) provides a cyber litmus test of an organisation's security posture and business risks.
QinetiQ's Security Health Check (SHC) team is the longest established dedicated penetration testing team in the world. Drawing on extensive experience, QinetiQ SHC has developed a world-class Cyber Intrusion Exercise (CIE) service, finally providing our clients a unique, affordable, smaller and agile red-team exercise, delivering the highest levels of assurance.

The QinetiQ Approach

SHC's Cyber Intrusion Exercises are delivered highly collaboratively with our clients, in a controlled manner and for this reason are less fearful than a full-spectrum red-team exercise, while saving costs on time and improving efficiencies.

Cyber Intrusion Exercises are delivered in three main phases:

- Internet-based assessment
- Stand-off attacks
- Onsite testing and egress assessment

QinetiQ's Cyber Intrusion Exercise service consolidates SHC's over 25 years of operation and experience of delivering infrastructure and web application testing, open source intelligence gathering and classical penetration testing.

The Cyber Intrusion Exercise service regularly 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.

CHECK
IT Health Check Service

CREST

TIGERSCHEME
Providing excellence in penetration testing

Output
Securely-delivered technical report of identified security issues with relevant supporting information, vulnerabilities prioritised from critical to low and a management summary to make it easy for the business to understand and respond.

Optional on-site key stakeholders presentation of findings, recommendations, key observations and lessons learned

QinetiQ's SHC team continues a strong heritage of innovation, leading the way with Cyber Intrusion Exercises by challenging the normal penetration testing paradigm. The Cyber Intrusion Exercising 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.

Cyber Intrusion Exercise - Key Elements

Internet-Facing Security Posture Assessment
Examine your organisation's Internet-facing security posture from the perspective of a remote threat actor getting ready to perform a stand-off electronic targeted attack. These exercises are used by QinetiQ's clients to proactively examine the attack surface of the organisation, to exercise data loss protection controls, and test Intrusion detection effectiveness.

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.

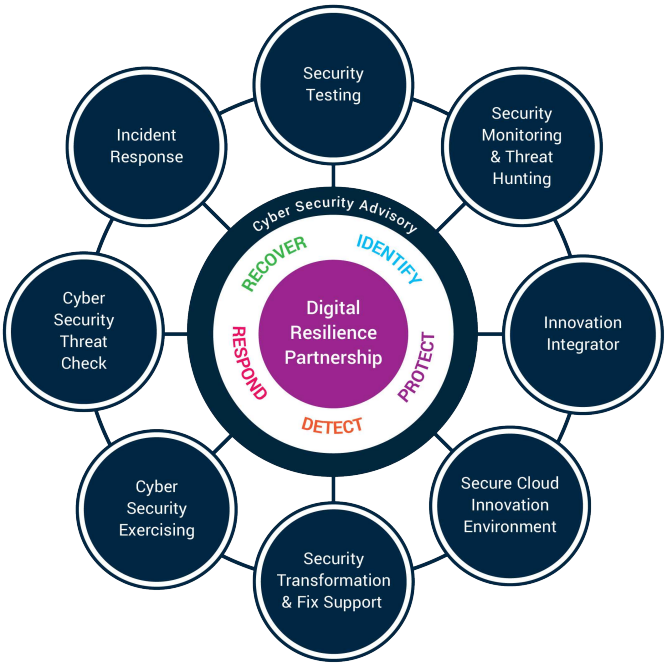
Phishing
This is delivered collaboratively through CIE's to ensure maximum organisational value for money, over traditional phishing exercises. Blocking a cyber attack within the first steps in the attack chain is key to cost effective network defence. When attempting to gain a foothold an attacker may 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.

Egress Assessment
Quantifies the avenues available to an attacker attempting to exfiltrate data from your networks.

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

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