Advanced Intrusion Exercising (AIE)

A QinetiQ Cyber Security Service

Key Benefits

- Emulates real world threat actors and vectors in controlled environments
- Assess the effectiveness of physical controls and human practices
- Provides real, actionable intelligence against security posture
- Exercise SOC capabilities in real time with attack methodologies

Pro-actively examining the real-world threat posed by targeted attackers by combining social engineering, physical breach and traditional cyber-attack methodologies, the AIE provides the most comprehensive practical exploration of breach simulation. Performed by highly qualified and trusted security specialists, the AIT can safely emulate nearly any potential threat actor.

The AIE service can also be performed alongside and with the full interaction of a customer's SOC analysts and security teams so that they can see, in real-time, what different types of advanced attacks against the organisation look like as they happen, and to identify what footprints that even a highly skilled and covert attacker will leave in system logs. This helps the Blue Team network defenders to "train like they fight".

The QinetiQ Approach

QinetiQ's AIE service brings to bear the vast experience of over two decades of vulnerability assessment, classical penetration testing and responsibly conducted red-team cyber-attacks. It practically assesses the effectiveness of physical controls and human practices, as they are actually used within a customer's organisation, comparing them to the prescribed authorised behaviours for staff and visitors to an organisation. This allows our customers to understand the real impact of identified vulnerabilities and measure the skill level that might be required by an attacker in order to exploit them.

QinetiQ's SHC team has a strong heritage of performing such exercises, discreetly and ethically, identifying gaps in physical and technical controls while highlighting the areas within the organisation which could most benefit from additional staff training and education, without exposing the individual staff members who may have been targeted during the testing.

The AIE service not only identifies the attack vectors which may be overlooked by more tightly scoped penetration testing exercises, but can also be performed to ensure Security Operations Centre (SOC) monitoring and detection controls are functioning as intended, ensuring incident response and incident reporting procedures would be effective during a real cyber-attack.

CHECK
IT Health Check Service

CREST

TIGERSCHEME
Providing excellence in penetration testing

QINETIQ

Each assessment conducted by QinetiQ's SHC is expertly scoped to ensure the exercise answers our customer's requirements, optimising time and effort and delivering the best return on investment. SHC's AIE services are based on core building blocks and can be completely customised to meet our client's requirements, bringing the very best of QinetiQ SHC's comprehensive skill set to the exercise.

Expert simulation of real-world threat actors and methods

Over two decades of experience and Discretion

All Staff hold UK security clearances.

Service summary

Red Teaming

'Red Teaming' is the ultimate, practical, real world, assessment of an organisation's security position. Using a holistic approach, we draw on all of the specialisms outlined above, to provide an organisation with a highly accurate assessment of the threat to either a specific location or to the organisation as a whole.

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 either internal or 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 organisations security posture and readiness with regards to these initial infection/attack vectors.

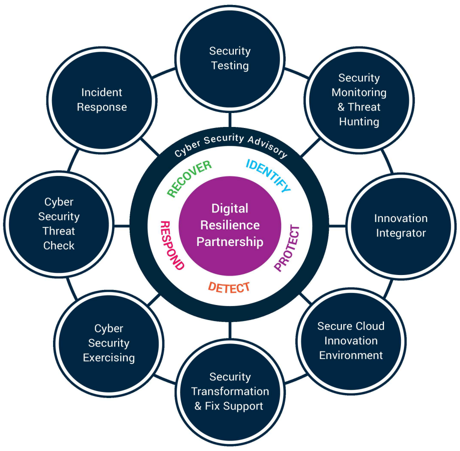
Physical Access Testing

QinetiQ SHC have proven experience of gaining physical access to secured sites, using social engineering techniques, card cloning, lock picking, or even by jumping a fence, if needed.

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