Multi Scenario Advanced Attack Simulation (MSAAS)

A QinetiQ Cyber Security Service

Key Benefits

* Emulates real world threat actors and vectors in controlled environments
* Engagement run over extended period, mimicking a true threat actor
* Provides real, actionable intelligence against security posture
* Highly-experienced, SC and DV-cleared CHECK specialists

QinetiQ will design and execute multiple attack scenarios, supported by an open source intelligence gathering exercise, tailored to an organisation, while emulating the capabilities and techniques of threat actors. The Multi-Scenario, Advanced Attack Simulation service provides an organisation the opportunity to evaluate its ability to defend against real world threats.

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.

CHECK
IT Health Check Service

CREST

The QinetiQ Approach

QinetiQ deliver four phases of testing. Each phase concentrates on a particular part of the Cyber Kill Chain and performed from a blackbox perspective. QinetiQ draw on the skills of QinetiQ's own Threat Intelligence service to identify threat actors and their tools, techniques and procedures. This helps us craft a custom campaign designed to emulate our customer's real-world adversaries with the highest degree of authenticity.

QinetiQ have developed the Multi-Scenario, Advanced Attack Simulation to avoid the usual drawbacks of traditional penetration testing, namely that the response teams are aware of upcoming tests and will be more vigilant than under normal circumstances. This creates a false sense of security and is generally accepted to diminish the value of test results. By marrying this testing with the Cyber Kill Chain, QinetiQ provide a thorough examination of our customer's current defensive and monitoring capabilities. QinetiQ understand that the most accurate way to test processes and systems designed to detect, identify and respond to incidents is to use them on real world cyber attacks. QinetiQ also understand that real attacks aren't normally confined to the week or two of a conventional penetration test. By extending the overall testing window, QinetiQ's Multi-Scenario, Advanced Attack Simulation provides the best levels of assurance.

TIGERSCHEME
Providing excellence in penetration testing

QINETIQ

QinetiQ ensure that the testing provides real-world feedback by delivering reports after each phase, and by aligning each phase to the Cyber Kill Chain, QinetiQ identify specific areas of concern for the target organisation.

At the completion of the final phase of testing, each of the separate phase reports are collated into a single technical report, producing a consolidated overview of the entire operation. The final report can be accompanied by a board-level presentation from our technical delivery team providing another opportunity to understand the techniques used and effects at each phase.

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.

Expert simulation of real-world threat actors and methods

Over two decades of experience and Discretion

All Staff hold UK security clearances.

Service summary – Four Phases

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 organization.

Phase One
Can we identify targets for a spear-phishing attack?

Phase One aligns with the early elements of the Initial Foothold stage of the Cyber Kill Chain. Using social media and other open-source investigation techniques to identify potential targets to be used in Phase Two (a spearphishing campaign). SHC will only disclose the targets if explicitly requested, to ensure that our customer operates under the same 'black box' conditions as our technical team.

Phase Two
Can we establish a foothold via spearphishing?

Phase Two aligns with the Initial Foothold stage of the Cyber Kill Chain. Using information discovered during Phase One to launch a Spear Phishing campaign against the chosen targets within the target organisation. SHC use multiple payload and delivery techniques, identified within the Threat Intelligence findings. The QinetiQ technical team crafts custom payloads, to circumvent any protection or detection systems.

Phase Three
Can we infiltrate the wider network?

Phase Three aligns with the Network propagation stage of the Cyber Kill Chain. QinetiQ HC leverage network persistence and attempt lateral movement through the target estate. Using 'Living Off The Land' techniques to subvert existing operating system tools as a means of enumerating the network and identifying other targets for exploitation and compromise. SHC employ persistence methods to ensure that implants survive a reboot.

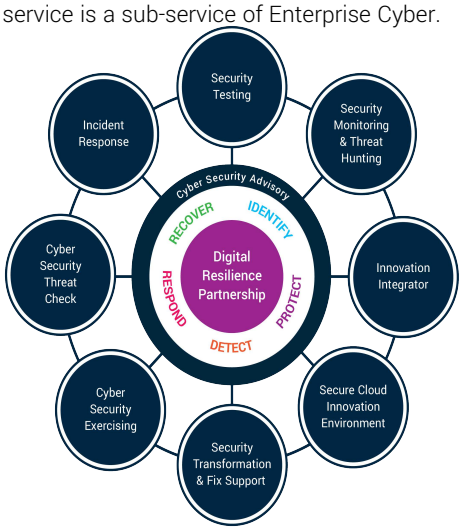
Phase Four
Can we get data out?

Phase Four aligns with the Action on Objectives stage of the Cyber Kill Chain. SHC use the information and implants from all of the previous stages to attempt exfiltration of customer data from the estate.

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 Enterprise Cyber.



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
(0)1252 392000
SHC@QinetiQ.com
www.QinetiQ.com