Red Team Tradecraft

A QinetiQ Cyber Security Service

Key Benefits

- Realistically emulate real world threat actors in a safe environment
- Learn attack simulation methodologies
- Access to QinetiQ's challenging assault courses
- Take skills to the next level

QinetiQ's Red Team training service elevates a penetration tester to think like an offensive security specialist by teaching through lecture and practical experience, across multiple modules, how to plan, build, and execute a high assurance, offensive, cyber operation; the training culminates in a simulated operation against QinetiQ's challenging cyber lab.

This course is for pentesters who wish to break into at tack simulation or blue teamers who wish to further a ppreciate the methodologies of threat actors.

The QinetiQ Approach

This course provides the theoretical and practical experience required to realistically simulate advanced threat actors. This course provides pentesters with the techniques required to become red teamers, and provides blue teamers with the opportunity to practically understand the techniques that may be deployed against them.

The course practically teaches the atomic elements used in a red team attack, including but not limited to setting up the attack platforms, passive and active reconnaissance, phishing, command and control, lateral movement, privilege escalation and exfiltration of target resources. Then the course draws the lessons learnt together in a realistic stand-off electronic attack against a simulated organisation utilising enterprise technologies and mature defensive technologies which alert the "blue team hunt pack" which will try to push you back out of the network if you register on their alert dashboard.

The theoretical elements will also cover the often overlooked infrastructure fundamentals and secure handling of customer data and persistence to protect your access to your clients and to protect their data.

CREST

CHECK
IT Health Check Service

TigerScheme
Providing excellence in penetration testing

Service summary

This course aims to train a pentester or network defender about how to operate and simulate real-world threat actors, at various levels of sophistication. Candidates of the course will learn an in-depth methodology and approach, while operating at the standards required for a professional simulated attack specialist. The course is designed to introduce the latest tools, techniques and procedures (TTPs) being used by real-world attackers and allow students to try them out in simulated, but realistic, lab environments.

The theoretical elements will cover the registration of attack domains, building domain reputation and the other often overlooked infrastructure fundamentals required for successful exploitation without detection. Students will be subjected to the experience of the QinetiQ Advanced Intrusion Testing team which performs high-assurance red team testing for highly security-mature clients.

Expert simulation of real-world threat actors and methods

Over two decades of experience and discretion

All Staff hold UK security clearances

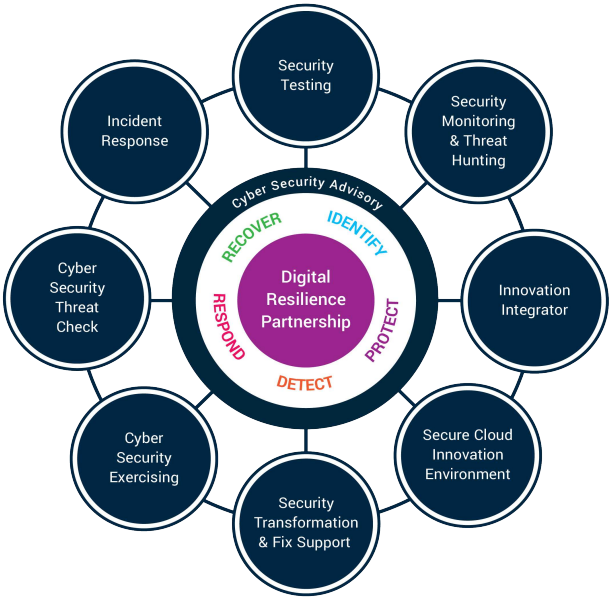
Activity description and skills, experience and knowledge gained in this training

- Introduction
- Cyber Kill Chain & MITRE Attack Framework
- Scoping & Pre-Engagement
- Law and Logging
- Red Team Overview
- Attribution & Operational security
- Active vs passive reconnaissance & OSINT
- Threat Intelligence
- Setting up C2 Infrastructure (Empire, PoshC2, Cobalt Strike)
- Setting up domains, reputation and proxies
- Phishing setup
- Weaponisation
- Phishing payloads
- Living off the land (LOLBAS)
- Persistence
- Lateral movement
- Privilege escalation
- Assault Course

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