

Red Team Engagements

QinetiQ will design and execute multiple attack scenarios, support by an open-source intelligence gathering exercise, tailored to an organisation, while emulating the capabilities and techniques of threat actors. Our Red Team service provides an organisation the opportunity to evaluate its ability to defend against real world threats.

Features

- Emulates real world threat actors in a controlled environment
- Engagement run over extended period to mimic true threat actors
- Acquire physical access to sensitive and restricted areas
- Reconnaissance and surveillance of targeted sites
- Utilises network implants, spear-phishing and OSINT
- Provides real, actionable intelligence against security posture
- Highly experienced, SC and DV-cleared specialists
- Team in operation for over 28 years
- Full reports, delivered securely, detailing vulnerabilities prioritised critical to low

Benefits

- A real-world security assessment, not a check box exercise
- Understand the security culture of your organisation
- Identifies attack vectors that tightly scoped penetration test may miss
- Provides clear strategic understanding of exploitable vulnerabilities

- Actionable intelligence reporting to support organisational priority actions or remediation
- Identifies weakness in cyber security and preventative controls and policies
- Provides real, actionable intelligence against security posture
- Exercises SOC capabilities in real time with attack methodologies
- Assures effectiveness of technical controls and third-party investments