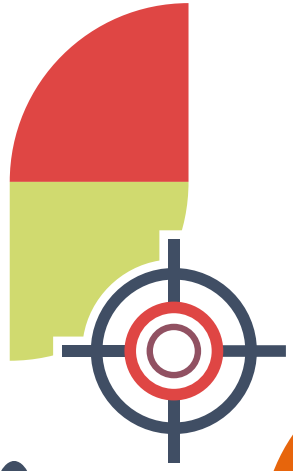
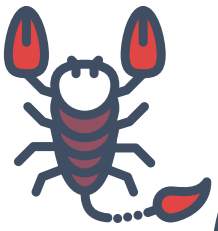
THE CYBER SCHEME

CSRTM

RED TEAM MANAGER ASSESSMENT



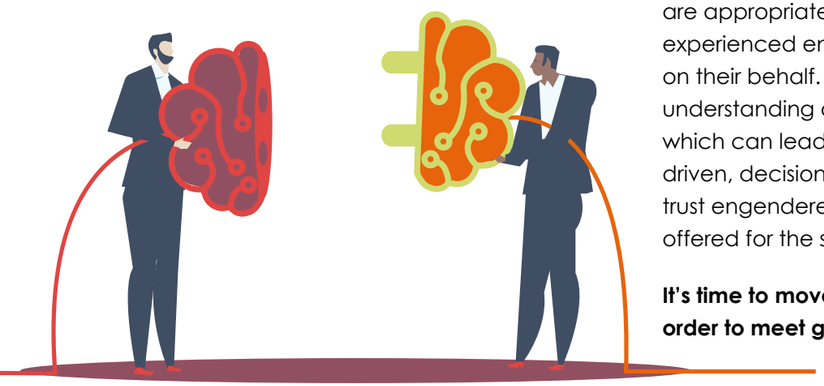


Red Team Manager

An innovative approach to a decades old challenge.

Scenario-based security testing is nothing new. When it was developed more than twenty years ago, the main threat was perceived as 'bedroom hackers' taking advantage of basic configuration errors or exploiting 1234 passwords. In response, technologies were tested, fixed, patched, rewritten and then tested again. However the security landscape has not moved in pace to reflect the growing threat - with a lack of funding, direction and appetite now being recognised at Government level.

In an article written for the Guardian newspaper Peter Kyle, the UK Science Secretary said the UK is 'desperately exposed' to cyber-threats and pandemics, claiming that national resilience has suffered "catastrophically", while too little has been done to address rising cyber security risks.
(July 2024 - Guardian Newspaper.)



Traditional penetration testing is no longer the 'gold standard' of offensive security it once was. In short, red teaming is a return to a more holistic security assessment, based on attack scenarios - just like those orchestrated by funded attackers.

What has evolved as a result of ever-more sophisticated and well-funded threat levels is a return to the 'scenario based testing' that existed before penetration testing became so universally accepted. Today it is described as Red Teaming.

Serious and organised crime groups operate at a level which is not limited in scope, budget, time or effort, so a scoped and budgeted penetration test is unlikely to provide a true view of an organisation's security posture. We need to move back to mimicking these types of attacker and their way of working, helping organisations – from CNI to SME – to understand their true security posture from every angle.

The cyber security industry needs to both assure commissioning organisations that engagements are appropriate, and recognise the individuals experienced enough to manage the engagements on their behalf. There remains a distinct lack of understanding of what a Red Team Engagement is, which can lead to price-driven, rather than security-driven, decisions being made, as well as a lack of trust engendered by wildly differing contracts being offered for the same scope.

It's time to move back to scenario-based testing in order to meet growing threat head on.

Competency is Key

Standardised definitions will engender trust.

A Red Team Manager (RTM) is responsible and accountable for the planning, team selection, tasking, risk analysis/management and overall quality assurance of engagement report(s).

The Cyber Scheme have undertaken extensive research into the assessment and procurement landscape around the role of a Red Team Manager, including consultations with principal organisations involved in the delivery of Red Team projects, as well as surveys carried out with Security Testing consultancies.

The result of this research led to the creation of a **standardised definition of the Red Team Manager role**: an objective description of the knowledge and skills required as core competencies.

> "A reputable Red Team is a chance to learn, remediate and improve security cultures enterprise-wide."

James Mason, QinetiQ

With definition comes a new assessment landscape.

Once the definition was agreed upon by all stakeholders, The Cyber Scheme developed a new assessment, the **Cyber Scheme Red Team Manager (CSRTM)**. All the assessments conducted by The Cyber Scheme are developed and carried out using our principle of mimicking 'what do you do in your day job' and this is no different.

In essence, CSRTM is a measure of competence, capability and experience. Candidates are asked about specific situations, and what their decision making processes and their understanding of the risks is. What is being measured is whether or not somebody is capable of operating as a red team manager. It's not a technical exam, though a candidate may need to explain technical concepts and be able to translate them into language consumable to a stakeholder.

So if it's not a technical assessment, how do we ensure a CSRTM preserves their skill and knowledge, and maintains understanding of rapidly evolving industry-specific technology and regulations?
The answer lies in using the principles of the KSAT (Knowledge, Skills, and Abilities to conduct Tasks) model; we have created an assessment which measures true competency, not the ability to l earn on demand.

Standardised Definitions

The benchmarks this industry needs

A benchmarked standardisation of the term 'red team' is essential; not only for the buying and selling communities to understand the terms used and speak the same language, but also for the assessment of an individual to remain fair, impartial and acceptable to all stakeholders.

A confused commissioning landscape is driven by a lack of standardised definitions about what red teaming exercises actually involve, as well as a perceived belief that red teaming is 'better' than pen testing – with the result that a client can inadvertently follow unregulated advice or is driven by budget over actual need.

The Cyber Scheme have created the following standardised definitions, on behalf of and in conjunction with industry partners, allowing the prospective scope to be more reflective of actual need in contracts.

Red Teaming

Red teaming is the practice of mimicking an adversarial approach/attack designed to evade detection and to test an organisation's defence capabilities. By defining an organisation's likely threat actors*, attack vectors can be created using knowledge of real-world threat actor capabilities which would allow the red team to play out the scenario most likely to be used by an adversary.

A Red Team is a **stress test under control conditions**, designed to simulate an attacker scenario and test the defensive capabilities in a Blue Team. Playing out these scenarios rigorously challenges the commissioning client's assumptions of readiness to manage an attack and to enact defence strategies, security policies and procedures all tested against a live simulation of an attack.

The client may specify reporting requirements and any quantitative metrics. The report should include (but not be limited to) an executive summary which details the commercial implications of any critical findings, a technical report detailing discoveries and methodologies, tactics and techniques deployed and any tool output specific to successful attack vectors. These should be supported with actionable recommendations.

* There is a huge range of threat actors; the tactics, techniques and procedures deployed by each is different in maturity and capability.

Sponsors of The Cyber Scheme will each have their own defined methodology for performing a Red Team assessment, these methodologies may vary in approach and are sometimes tailored to a clients threat assessment, what is critical is the lead Red Team Manager must be skilled, proficient and highly capable across multiple cyber disciplines.

Vulnerability Assessment

VA – The process of finding vulnerabilities on a system, environment, or enterprise by running well established automated scanning tools, the output of which will be the standard vulnerability tool findings report. Usually repeated on a regular basis to identify vulnerabilities for internal remediation teams, it forms the basis for basic security hygiene.

VA+ Builds upon a VA exercise by requiring the testing team to remove false positive results.

No exploitation of the findings is conducted. Usually repeated on a regular basis to identify vulnerabilities for internal remediation teams and it is one of the initial activities in a penetration test.

In both cases the tests are automated with little skilled tester input, such input would come from an internal team or external consultant.

Penetration Testing

Internal (from within an organisation) and External (from outside an organisation) testing:

The process of finding vulnerabilities or chains of vulnerabilities, misconfigurations and data breach risks through enumeration and then exploitation (or proof of concepts where exploitation is considered unnecessary or too great a risk*) within a scope defined by the commissioning client.

Usually, such tests are performed on a subset or section of infrastructure, a defined target environment, application, API or product. Reasonable proof that the vulnerabilities exist through tool and manual review is expected (i.e. removal of false positives**) and remediation advice is expected to be presented.

The client may specify any reporting requirements and any quantitative metrics (i.e. CVSS). It is reasonable for the client to expect an executive summary to support a technical report detailing findings and tool output to prove the existence of issues discovered by the penetration test, these should be supported with actionable recommendations.

* Where a client scope highlights no exploitation to be undertaken, this would be considered a vulnerability assessment.

* * Where vulnerability detection consists of running a set of automated tools and interpreting the results the activity should be considered vulnerability assessment.

Assessment methodology: The KSAT Model

What good looks like...

One of the challenges when considering new assessments is making sure it reflects as near real world a measure of the skills and competencies individual professionals need to undertake specific roles. There are many approaches to assessments; the model that best fits the way The Cyber Scheme presents its assessment methodology is the US NICE Framework. It establishes a common lexicon that describes cyber security work and workers regardless of where or for whom the work is performed.

Work roles and tasks are defined using KSATs, which fit our vision of making assessments and certifications as near 'real world' as possible.

What are KSATs?

KSATs are the Knowledge, Skills, Abilities & Tasks associated with a given role. We have used these to build the Red Team Manager Role, making use of existing published core KSATs in the NICE framework, as well as generating new ones as required to better reflect UK work roles compared to those that may exist in the US.

Sample KSATs for CSRTM

Knowledge

- Knowledge of crisis action planning and time sensitive planning procedures.
- Knowledge of cyber laws and legal considerations and their effect on cyber planning.
- Stakeholder Management.
- Understanding and defining a testing methodology.
- Sound Technical knowledge (to what level).

Skills

- Skill in preparing and presenting briefings.
- Skill in preparing plans and related correspondence.
- Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.
- Skill in utilizing feedback in order to improve processes, products, and services.

Abilities

- Ability to apply critical reading/thinking skills.
- Ability to collaborate effectively with others.
- Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
- Ability to tailor technical and planning information to a customer's level of understanding.

Tasks

- Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.
- Assess target vulnerabilities and/or operational capabilities to determine course of action.
- Report on tactics, techniques and procedures used by the cyber attack team, aligned with agreed frameworks and nomenclatures.
- Work with business risk owners, threat intelligence providers and relevant stakeholders to establish the scope, boundaries and assessment/learning objectives of a cyber attack simulation.

> "Under the CSRTM, we have defined the Knowledge, Skills, Abilities and Tasks necessary for the role, and designed an assessment that assesses whether candidates can operate effectively and safely when managing red team operations.
>
> A candidate who has passed the CSRTM assessment will have demonstrated their competency across the defined KSATs – including the ability to meet the objectives of an attack simulation safely and ethically."

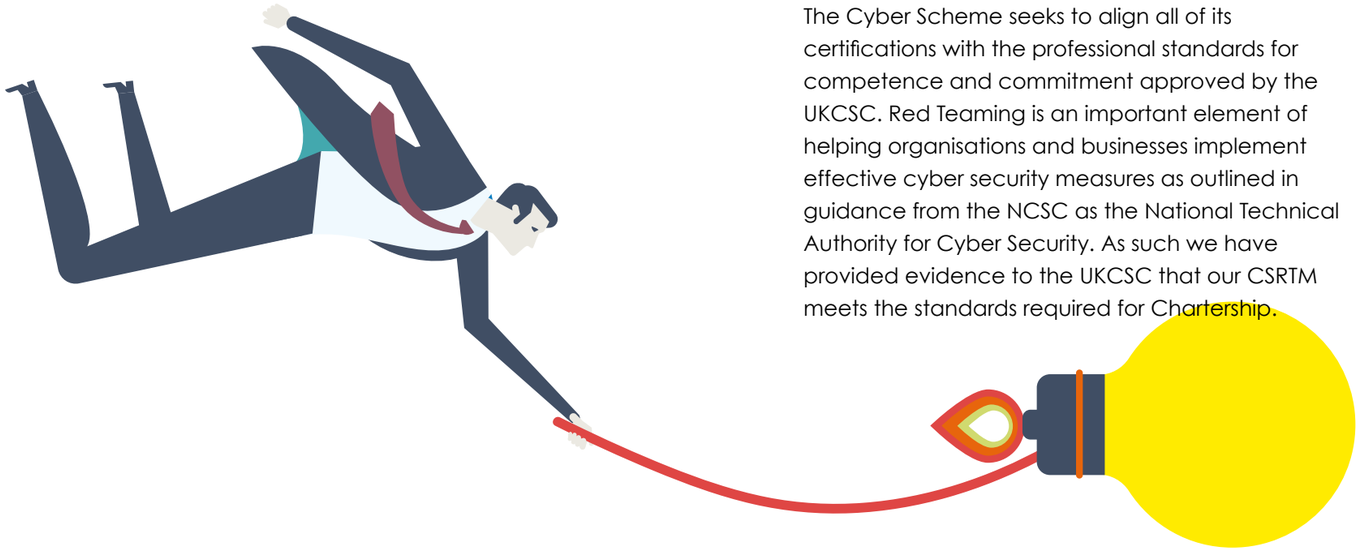
Gemma Moore, Cyberis

Assessing Experts

Proof of Competency

A seasoned Red Team specialist should easily be able to demonstrate knowledge in the following areas:

- Show you understand the principles of managing a red team
- Articulate the differences between management and technical work
- Evidence management of a complex political environment with a customer
- Manage the risk around some of the technical elements of red teaming
- Deal with clients under duress and communicate clearly
- Demonstrate definitive, immediate decision making
- Prove you are focused on getting value-for-money outcomes that actually help with resilience
- Manage any sort of hostile control group situation
- Demonstrated understanding of operational complex organisations with lots of competing parties
- Anticipate adversarial actions that may require control group intervention
- Show knowledge of legislation and the difference between ethical and non-ethical processes
- Articulate different types of leg ups, and how they would impact the quality of the evidential assessment on detection and response
- Show consideration of staff welfare, including the likelihood of physical attack
- Show how to work with a Blue Team to get best transfer of knowledge
- Demonstrate good evidence collection, good reporting, and good planning/briefing.



Licensed Body

UK CYBER SECURITY COUNCIL®

Security Testing

The Cyber Scheme are committed to ensuring that its certifications align with the objectives set out in the National Cyber Strategy and the Government Cyber Security Strategy (GCSS). The UK Cyber Security Council has been established to develop a higher quality, more established, recognised and structured cyber security profession for the UK.

The Cyber Scheme seeks to align all of its certifications with the professional standards for competence and commitment approved by the UKCSC. Red Teaming is an important element of helping organisations and businesses implement effective cyber security measures as outlined in guidance from the NCSC as the National Technical Authority for Cyber Security. As such we have provided evidence to the UKCSC that our CSRTM meets the standards required for Chartership.

The creation of these definitions, the KSATs and the Cyber Scheme Red Team Manager assessment have been made possible by the extensive involvement of industry experts who are experienced Red Team practitioners.

This has ensured industry objectivity, impartiality and the creation of 'what good looks like'.

Thank you to everyone who has been involved:

- **Accenture**
- **Cyberis**
- **KPMG**
- **NCC Group**
- **Pen Test Partners**
- **PwC**
- **QinetiQ**
- **WithSecure**
- **UK Cyber Council Technical Advisory Board**
- **Sponsors of The Cyber Scheme.**

The Cyber Scheme work closely with the National Technical Authorities and have fully taken into account all the advice and guidance from them when creating this brochure.

"It was a privilege to contribute and collaborate with experienced and esteemed peers on the CSRTM. The professional collective, which has an impressive pedigree in the field of adversary simulation and emulation, brought essential creativity and innovation to the design process.

The result is a progressive approach to capability assessment that fits with the perpetual evolution of the specialism, recognises the diversity of today's candidates, and is borne from real-world practitioner-lived experiences."
Dave Hartley, NCC Group

Assessing Competence - Training Excellence

Established in 2013, The Cyber Scheme is a leading assessment body and an NCSC Certified Delivery Partner for technical training and exams. Consultants who are evaluated by us are expected to demonstrate competence and skill at the highest level defined by the UK's National Technical Authority for Cyber Security (NCSC). Our assessments cover IoT/ICS, Red Team Manager, Cyber Advisor (Cyber Essentials) and Team Member and Team Leader technical exams.

We are a Licensed Body for the UK Cyber Security Council, able to assess and recommend individuals for Chartered Professional Recognition for relevant specialisms including Security Testing and Incident Response.

We offer training and mentoring to complement our assessments, from entry to expert level, meeting the growing needs of our industry as threats evolve. We are also committed to increasing the talent pool of prospective offensive security specialists, encouraging people from a diverse range of backgrounds to train with our Cyber Scheme Academy.