HMGCC Co-Creation

Challenge: AI / Novel Technology Red Agent Penetration Testing

Summary of the challenge

Organisations and solution providers can apply for funding to: 1) undertake paper-based landscape mapping to evaluate the market maturity of AI or other novel technologies to operate as a 'Red Agent' penetration tester, and 2) provide a test environment and to subsequently undertake practical testing to evaluate the feasibility of AI or other novel technologies to operate as a 'Red Agent' penetration tester.

HMGCC Co-Creation will provide funding for time, material, overheads and other indirect expenses.

Key information

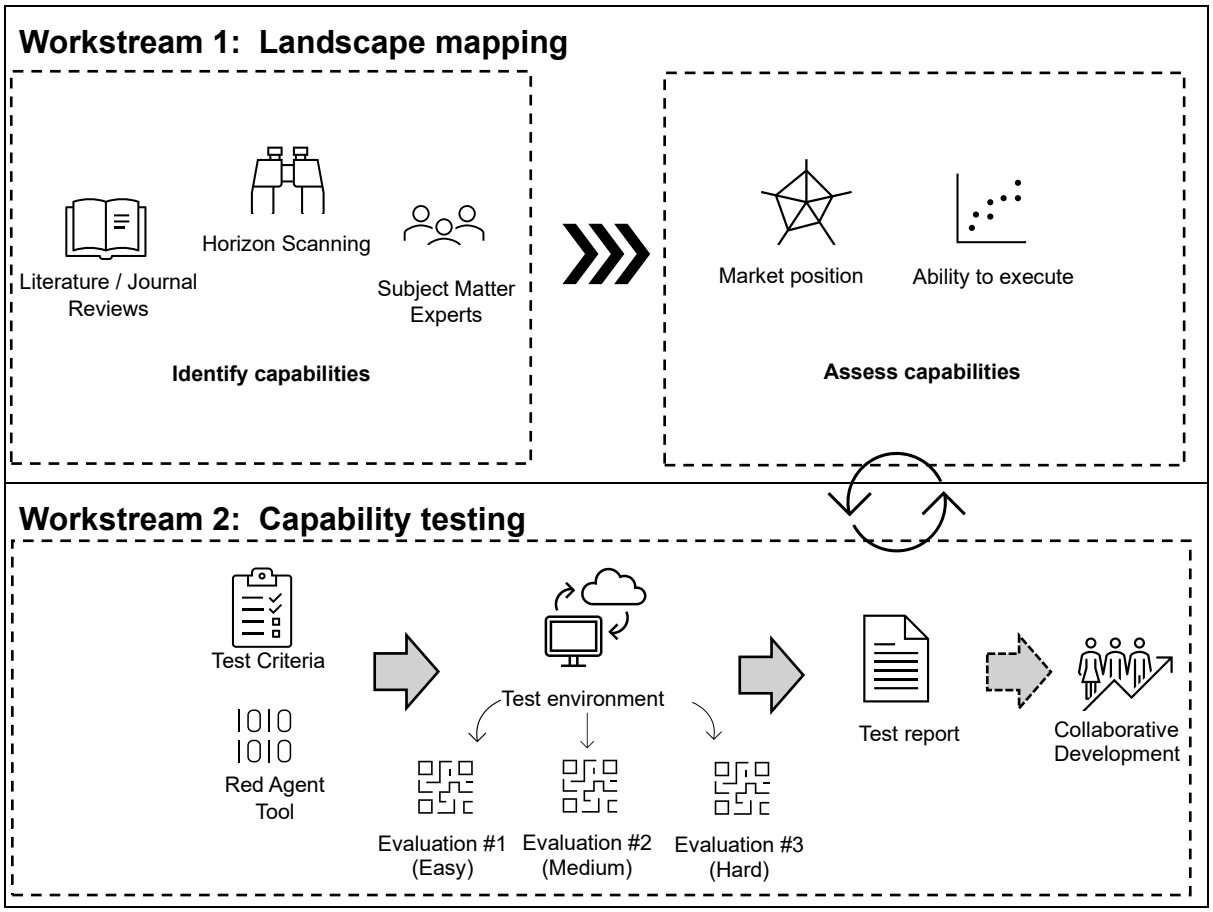
Budget per single organisation, up to	**£60,000 per workstream (plus call-off)**
Project duration	**12 weeks**
Competition opens	**Thursday 17 October 2024**
Competition closes	**Thursday 21 November 2024 at 5:00pm**

Context of the challenge

HMGCC is co-ordinating a Co-Creation challenge to further the security community's understanding of AI or any novel technologies that have the capacity to penetration test secure IT environments. Scripting based technologies are **excluded** as these are mature and available as commercial products.

This Co-Creation challenge aims to evaluate the readiness of the technologies, their capabilities and integration needs. This will be achieved by evaluating ease of adaption and integration.

The challenge is being delivered across two workstreams delivered in parallel over 12-weeks, as illustrated below:



One workstream will identify the capabilities of autonomous Red Agent tools, measuring them up in a paper-based assessment against the major factors involved in how they would be used.

The second workstream will involve taking a small group of these tools forward (if they passed the initial workstream test) into an assessment of how they work in practice. We anticipate testing between 3 to 6 Red Agent tools. The results from both workstream tests will then be assessed together. Collaborative development might then be undertaken to help further test and improve the most promising tools where appropriate.

The gap

Workstream 1: Landscape mapping

We are looking for a Solution Provider (SP) with knowledge of AI and novel technology in the penetration testing domain. We would like this solution provider to identify current and future 'Red Agent' solutions and to develop an assessment framework – which will be used by the SP to evaluate these capabilities on paper. This would be an iterative agile process between Co-Creation and the SP, where the joint team would provide insight into the evaluation criteria, process and findings on a sprint-by-sprint basis. Red agent tools of interest from the paper-based assessment (Workstream 1) would be highlighted to the capability testing team (Workstream 2), where practical experimentation would take place. The results from this testing would be fed-back into the horizon scanning team so that the horizon scanning process could be enhanced if needed.

Workstream 2: Capability testing

We are looking for a Solution Provider (SP) with knowledge of AI and novel technology in the penetration testing domain. We would like this solution provider to provide a test capability in which we will undertake practical experimentation with between 3-6 Red Agent tools. The SP would provide the IT test environment (potentially in the cloud), team and processes/procedures to test and report on the effectiveness of each capability. The Authority would instruct the SP which 3-6 Red Agent tools to install in the test environment as these are identified during the project. All work would be undertaken at a classification of OFFICIAL.

We envisage three test scenarios within the technical test environment – each one increasing in difficulty (easy/medium/hard). For example, the 'easy' environment could have a low level of IT security and could include 2 easily identifiable vulnerabilities that the SP would 'plant' in the environment for the Red Agent tool to find.

This would be an iterative agile process between Co-Creation and the SP, where the joint team would provide insight into the evaluation process and findings on a sprint-by-sprint basis.

Example use case of a 'Red Agent' capability

Secure standalone networks may be monitored and managed by a security team. This team needs to be tested in their response to potential network attacks and identify any vulnerabilities introduced via changes in configuration or equipment being added.

Currently the security team's response to security incidents is tested by a red penetration test team. The cost and availability of this team can sometimes limit the frequency and depth of testing of the network. To address this, the workstreams are

evaluating the potential of AI and novel technologies to supplement the 'red' penetration test team.

To minimise human resource, the technologies need to operate with no knowledge of the network and disconnected from the internet.

The AI / Novel Technology Red Agent Pen Tester (Red Agent, for short) is connected to the standalone network and will work independently of human interaction. The Red Agent has no knowledge of the network and starts a scanning process to obtain some initial information. From this initial information the Red Agent is able to decide on the next actions to take to pivot about the network, taking advantage of a discovered vulnerability. The security team (Blue team, for short) are monitoring the network. They detect the abnormal activity and take corrective action to prevent the Red Agent continuing to pivot about the network. The Red Agent is able to report on the information gathered, confirmed vulnerabilities, action take and the 'reasons' for taking the actions during the exercise.

Project scope

We are seeking applications to deliver one or both of the workstreams in this challenge. Please make it clear in your application which workstream(s) you are bidding for.

HMGCC will provide the supplier of Workstream 2 with additional reasonable call-off costs of up-to £65k (exc. VAT) during the project to support third-party charges for selected Red Agent tools in the test environment.

HMGCC may also provide additional costs for collaborative development of selected tools where appropriate after initial testing has been completed.

Characteristics of the assessment for each Red Agent capability could include:

1. Number of factors are considered in decision making, i.e. does not work through a simple ordered list of actions in a scripted behaviour.
2. The capability is adaptable, and is able to adapt to different networks with no specific reconfiguration.
3. Function with no knowledge of the network being tested.
4. Operates disconnected from the internet.
5. Easy to add new exploits.
6. Quick to train.
7. Quick to make decisions.
8. Ability to integrate with existing (commercially available and bespoke) tool sets, for example, to perform bespoke actions.
9. Ability to integrate with commercially available and bespoke tool sets to provide two-way control where appropriate, for example, using APIs.

10. Logging / justification of actions that support security team with relevant outputs.
11. Allow for human decision making at key points to support more sensitive testing.
12. Able to operate in different ways, e.g. a) as fast as possible, b) slow and least disruptive, c) easily detectable, and d) difficult to detect.
13. The technology will run on a normal commercially available laptop, i.e. there is no need for any specialist compute.

The following capabilities would be out of scope for the assessment:

1. Scripting-based technologies are excluded as these are mature and available as commercial products.
2. Solutions at or below Technology Readiness Level (TRL) 2.
3. Security research tools.
4. Academic research papers.

Dates

Competition opens	Thursday 17 October 2024
Briefing Call	Wednesday 30 October 2024 @ 10:00am Link for Briefing Call: https://events.teams.microsoft.com/event/c810e732-4297-4841-aa46-1b4910d6e954@fad42abb-dfda-43f0-9120-b18e6e86169d
Deadline for clarifying questions	Wednesday 30 October 2024 at 17:00pm
Clarifying questions published	Wednesday 6 November 2024
Competition closes	Thursday 21 November 2024
Applicant notified	Friday 29 November 2024
Pitch day in Milton Keynes	Thursday 5 December 2024
	& Friday 6 December 2024
Target project kick-off	Monday 06 Jan 2025

Eligibility

This challenge is open to sole innovators, industry, academic and research organisations of all types and sizes, including those not traditionally associated with the defence and security sector. There is no requirement for security clearances.

Solution providers or direct collaboration from countries listed by the UK government under trade sanctions and/or arms embargoes, are not eligible for HMGCC Co-Creation challenges.

How we evaluate

All proposals, regardless of the application route, will be assessed by the HMGCC Co-Creation team. Proposals will be scored 1–5 on the following criteria:

Scope	Does the proposal fit within the challenge scope, taking into consideration cost and benefit?
Innovation	Is the technical solution credible, will it create new knowledge and IP, or use existing IP?
Deliverables	Will the proposal deliver a full or partial solution, if a partial solution, are there collaborations identified?
Timescale	Will the proposal deliver a minimum viable product within the project duration?
Budget	Are the project finances within the competition scope?
Team	Are the organisation / delivery team credible in this technical area?

Invitation to present

Successful applicants will be invited to a pitch day, giving them a chance to meet the HMGCC Co-Creation team and pitch the proposal during a 20 minute presentation, followed by questions.

After the pitch day, a final funding decision will be made. For unsuccessful applicants, feedback will be given in a timely manner.

Clarifying questions

Clarifying questions or general requests for assistance can be submitted directly to cocreation@hmgcc.gov.uk prior to the cut-off date. These clarifying questions may be technical, procedural, or commercial in subject, or anything else where assistance is required. Please note that answered questions will be published to facilitate a fair and open competition.

Routes to apply

HMGCC Co-Creation are working with a multiple and diverse set of community collaborators to broadcast and host our challenges. Please follow this link for the full list of community collaborators.

If possible, please submit applications via a community collaborator.

If the community collaborator does not host an application route, please send applications directly to cocreation@hmgcc.gov.uk, including the challenge title with a note of the community collaborator where this challenge was first viewed.

All information you provide to us as part of your proposal, whether submitted directly or via a collaborator platform, will be handled in confidence.

How to apply

Applications must be no more than six pages or six slides in length. The page/slide limit excludes personnel CVs and organisational profiles.

There is no prescribed application format, however, please ensure your application includes the following:

Applicant details	Contact name, organisation details and registration number.
Scope	Describe how the project aligns to the challenge scope.
Innovation	Describe the innovation and technology intended to be delivered in the project, along with new IP that will be generated or existing IP that can be used.
Deliverables	Describe the project outcomes and their impacts.
Timescale	Detail how a minimum viable product will be achieved within the project duration.

Budget	Provide project finances against deliverables within the project duration.
Team	Key personnel CVs and expertise, organisational profile if applicable.

HMGCC Co-Creation terms and conditions

Proposals must be compliant with the HMGCC Co-Creation terms and conditions. By submitting your proposal you are confirming your organisation's unqualified acceptance of HMGCC Co-Creation terms and conditions.

Commercial contracts and funding of successful applications will be engaged via our commercial collaborator, Cranfield University.

HMGCC Co-Creation supporting information

HMGCC works with the national security community, UK government, academia, private sector partners and international allies to bring engineering ingenuity to the national security mission, creating tools and technologies that drive us ahead and help to protect the nation.

HMGCC Co-Creation is a partnership between HMGCC and Dstl (Defence Science and Technology Laboratory), created to deliver a new, bold and innovative way of working with the wider UK science and technology community. We bring together the best in class across industry, academia, and government, to work collaboratively on national security engineering challenges and accelerate innovation.

HMGCC Co-Creation is part of the NSTIx Co-Creation network, which enables the UK government national security community to collaborate on science, technology and innovation activities and to deliver these in partnership with a more diverse set of contributors for greater shared impact and pace.

HMGCC Co-Creation aims to work collaboratively with the successful solution providers by utilising in-house delivery managers working Agile by default. This process will involve access to HMGCC Co-Creation's technical expertise and facilities to bring a product to market more effectively than traditional customer/supplier relationships.

FAQs

1. **Who owns the intellectual property?**

As per the HMGCC Co-Creation terms and conditions, project IP shall belong exclusively to the solution provider, granting the Authority a non-exclusive, royalty free licence.

2. **Who are the end customers?**

National security users include a wide range of different UK government departments which varies from challenge to challenge. This is a modest market and so we would encourage solution providers to consider dual use and commercial exploitation.

3. **What funding is eligible?**

This is not grant funding, so HMGCC Co-Creation funds all time, materials, overheads and indirect costs.

4. **How many projects are funded for each challenge?**

On average we fund two solution providers per challenge, but it does come down to the merit and strength of the received proposals.

5. **Do you expect to get a full product by the end of the funding?**

It changes from challenge to challenge, but it's unlikely. We typically see this initial funding as a feasibility or prototyping activity.

6. **Is there the possibility for follow-on funding beyond project timescale?**

Yes, if the solution delivered by the end of the project is judged by the HMGCC Co-Creation team as feasible, viable and desirable, then phase 2 funding will be made available.

7. **Can we collaborate with other organisations to form a consortium?**

Yes, and additional funding may be made available as per the outlined budget.

8. **Do we need security clearances to work with HMGCC Co-Creation?**

Our preference is work to be conducted at OFFICIAL, we may however, request the project team undertake BPSS checks or equivalent.

9. **We think we have already solved this challenge, can we still apply?**

That would be welcomed. If your product fits our needs, then we would like to hear about it.

10. Can you explain the Technology Readiness Level (TRL)?

Please see the UKRI definition for further detail.

11. Can I source components from the list of restricted countries, e.g. electronic components?

Yes, that is acceptable under phase 1 - feasibility, as long as it doesn't break UK government trade restrictions and/or arms embargoes.

Further considerations

Solution providers should also consider their business development and supply chains are in-line with the National Security and Investment Act and the National Protective Security Authority's (NPSA) and National Cyber Security Centre's (NCSC) Trusted Research and Secure Innovation advice. NPSA and NCSC's Secure Innovation Action Plan provides businesses with bespoke guidance on how to protect their business from security threats.

Further advice and guidance on how to keep your organisation secure online can also be found on the NCSC's website.