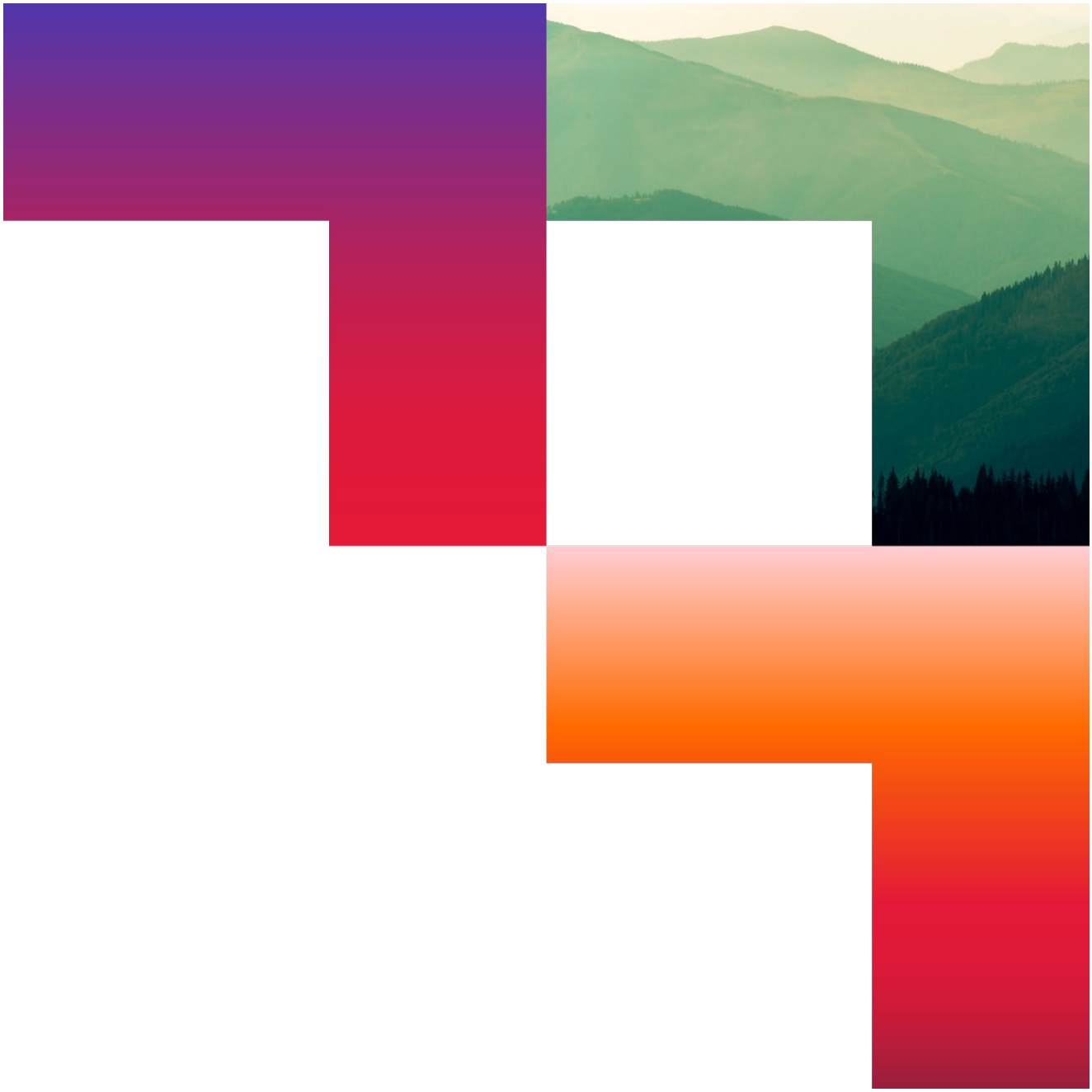


Purple Team Assessment

Contracting body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

Our purple team testing puts our NCSC CHECK accredited penetration testers and SOC Analysts together to perform an attack on your environment whilst watching in real-time to understand if and where attacks would be stopped. During a Purple Team engagement, CGI's highly skilled red team consultants will attempt to infiltrate your network, compromising sensitive data and employing the latest adversarial Tactics, Techniques and Procedures (TTPs). Concurrently, your blue team will actively monitor and respond to the simulated intrusion, leveraging your existing security controls, detection capabilities and incident response processes to identify and stop the attack in real-time.

The Purple Teaming service replicates the end-to-end attack lifecycle, from initial reconnaissance and exploitation, through to lateral movement, data exfiltration and persistent Command & Control (C&C). This full-spectrum approach provides unprecedented visibility into how your organisation would perform against a real world, multi-pronged attack, conducted by a persistent and highly skilled threat actor. By spanning the entirety of the cyber kill chain, a Purple Teaming exercise transcends limited penetration tests and vulnerability assessments, delivering a holistic evaluation of your prevention, detection, and response capabilities

1. Service Description

During a Purple Team engagement, CGI's highly skilled red team consultants will attempt to infiltrate your network, compromising sensitive data and employing the latest adversarial Tactics, Techniques and Procedures (TTPs). Concurrently, your blue team will actively monitor and respond to the simulated intrusion, leveraging your existing security controls, detection capabilities and incident response processes to identify and stop the attack in real-time.

The Purple Teaming service replicates the end-to-end attack lifecycle, from initial reconnaissance and exploitation, through to lateral movement, data exfiltration and persistent Command & Control (C&C). This full-spectrum approach provides unprecedented visibility into how your organisation would perform against a real world, multi-pronged attack, conducted by a persistent and highly skilled threat actor. By spanning the entirety of the cyber kill chain, a Purple Teaming exercise transcends limited penetration tests and vulnerability assessments, delivering a holistic evaluation of your prevention, detection, and response capabilities.

Below are some testing methods that we regularly employ. These are identified and applied based on our initial evaluation and proposal.

Delivering outcomes through purple team testing

Immediate visibility of the vulnerabilities in your detection capability against real-world attacks by our NCSC CHECK Penetration test team

- Actionable reporting, against the exercise type selected
- Caters for Information Technology and Operational Technology
- CGI’s service is certified to help you meet your compliance obligations.

Select an exercise that’s right for you

- OWASP top 10 web application security risks
- Ransomware top 10 variants
- Payment gateways and e-commerce platforms

- Traditional Methodologies (e.g. Internal / External Infrastructure Assessment; Build Reviews;
- Configuration Reviews; Network Devices / Firewall Reviews; Web Application / Services
- Testing; Wireless Testing; Vulnerability Assessment)
- Mobile Application Testing
- Red Team Exercises
- Cloud Assessment
- Industrial Control System (ICS) Testing
- Active Directory Review
- Phishing Exercises
- Network Segregation Testing
- Firewall Exposure Testing
- Static Source Code Analysis.

The engagement culminates in a comprehensive report detailing your performance across the full attack lifecycle and outlining recommendations for improvement. With extensive expertise in assessing both cyber offence and defence and delivered by our CHECK and CREST accredited penetration testing team; this service enables you to enhance your cyber resilience against emerging threats.

2. Service Pricing and Terms and Conditions

2.1. Pricing

Please refer to the G-Cloud 15 portal for the rates available.

2.2. Terms and Conditions

Please refer to the associated Terms and Conditions Document relevant for this Service including termination by the Buyer or Supplier.

3. Further information

For more information about this or any of our G-Cloud services, please contact us:

Phone: +44 0845 070 7765. Ask to speak to the G-Cloud team.

Email: uk.gen.ccsframeworks@cgi.com, including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

We will prepare a quotation for you. Once the quotation is agreed upon, we will issue you the necessary documentation (as required by the G-Cloud Framework) and ask you to provide us with a purchase order.

Once we have received your purchase order, the services will be configured to the requirements agreed with invoices issued to you for the services procured. On a monthly basis, we will also complete the mandated management information reports to Government Procurement.

PROPRIETARY AND CONFIDENTIAL

The information in this proposal is submitted on 30 Jan 2026 - Issue 1.0 on behalf of CGI by the following authorised representative:

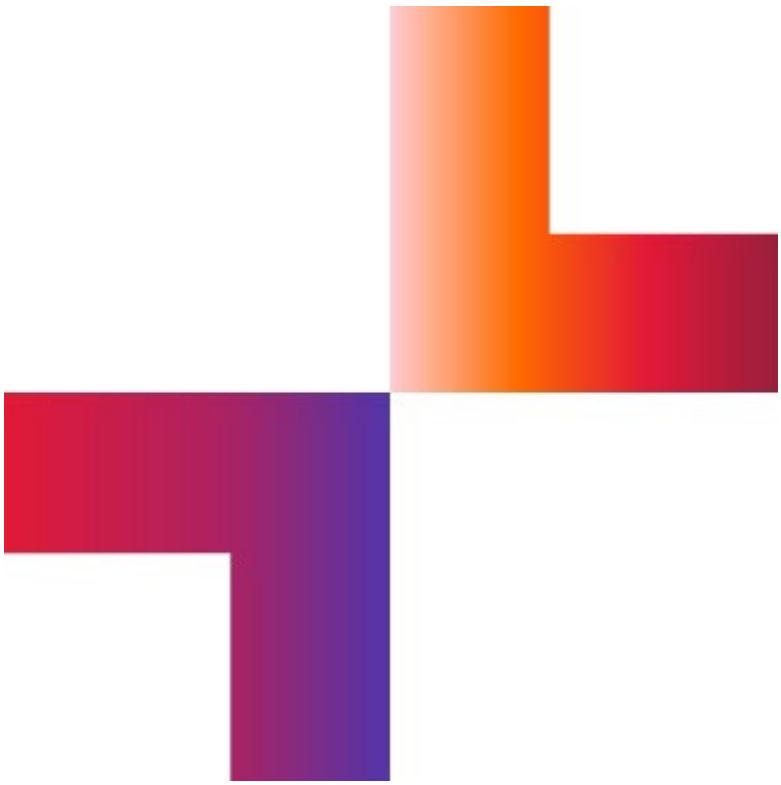
Simon Figg

Frameworks Manager

CGI IT UK Ltd

14th Floor, 20 Fenchurch Street, London, EC3M 3BY

Tel: +44 0845 070 7765



cgi.com/uk