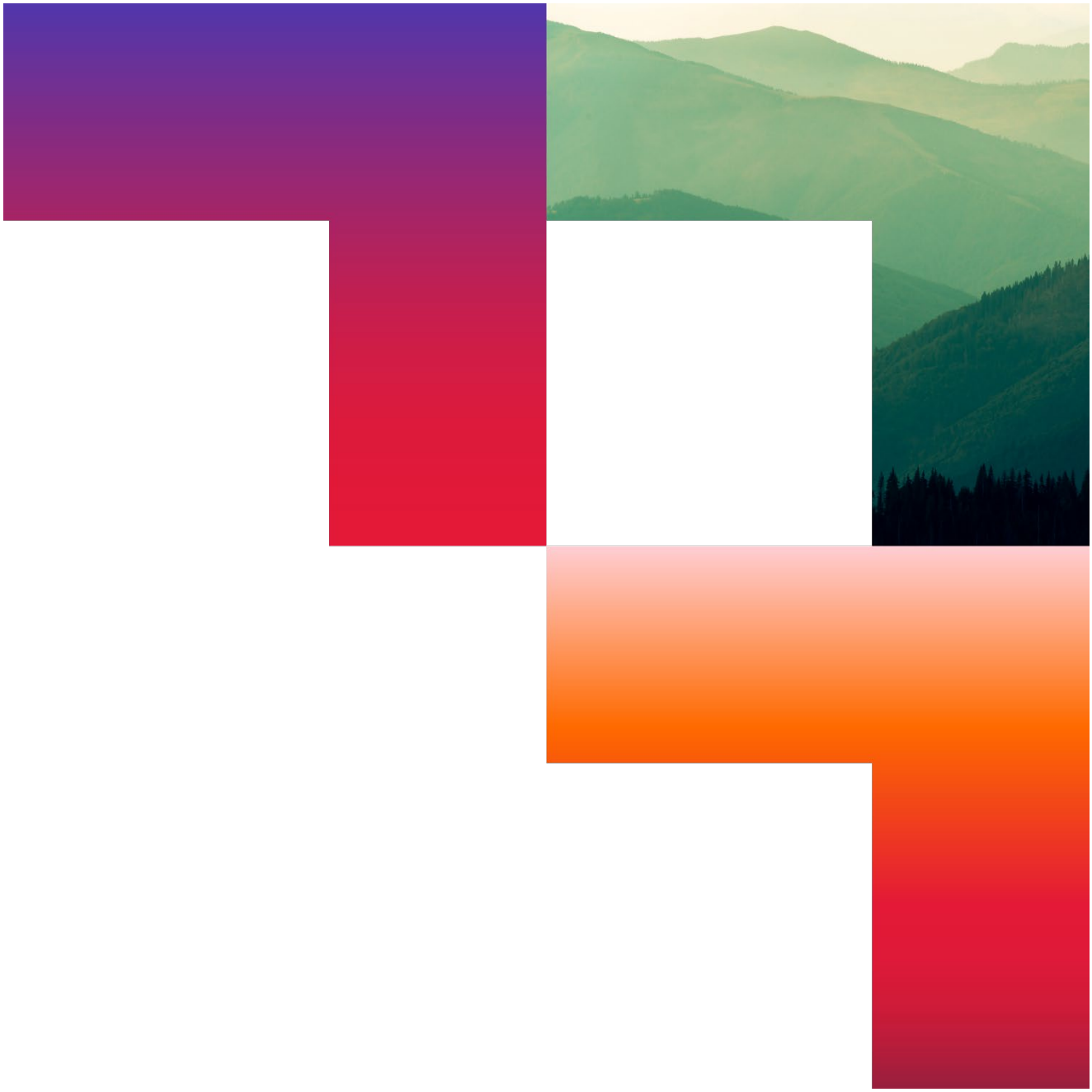


Blue Team Assessment Service

Contracting Body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

When was the last time your SOC detection capability was audited? Our qualified cyber auditors will independently review your SIEM detection rules to ensure that you can identify the most recent cyber threats to your organisation.

Choose from one of our most common assessments:

- Review of detection rules against the OWASP top 10
- Review against the top 10 malware variants in your industry
- Review against MITRE ATT&CK framework, understand the gaps
- Security log review, are you ingesting too much.

As part of this engagement, we will provide you with a comprehensive report that details what cyber threats you can and cannot detect.

Why CGI?

CGI is an established UK supplier of managed cyber security services our Analysts are experts in detecting threats and explaining to you where you have threat detection coverage gaps.

1. Service Description

What is Blue Teaming?

A Blue Team in a Cyber context is all about defending your organisation, whereas a Red Team is engaged in attacking it and probing for vulnerabilities. (Red Team assessments help you to understand existing risks and how a malicious user could exploit them. However, they are not a direct substitute for regular penetration testing or an IT Health Check). A Purple Team is a mixture of both blue and red, simultaneously attacking and defending an organisation and its assets. CGI has Security Analysts with specialisms in all types of Teaming and can offer them either as a one-off activity, or as part of our Managed Detection and Response service.

A Blue Team Assessment will provide confidence that your SOC is able to detect the latest emerging threats, such as Ransomware.

Why you need to act.

A Blue Team Assessment checks to see if a client is capable of detecting the latest emerging threats. If the assessment finds that a client is unable to do so, then they are vulnerable, and action needs to be taken. As an example, imagine a new piece of ransomware appears called ‘PayMeNow99’ that has been around for several months and is well known in the industry. Our Blue Team Assessment would check to see if this was detectable or not; if not then there is a coverage gap which exposes a client to this particular risk.

What is a Blue Teaming assessment?

CGI's Blue Team Assessment is a short engagement whereby our Security Analysts review a client's SIEM configuration to ensure that it:

- Can detect threats and alert on them.
- Is cost effective, only ingesting security logs that are required and nothing else.

A Blue Team assessment will evaluate your SIEM detection capabilities against real-world cyber-attacks enabling you to determine the effectiveness of your investment. Our assessment will leverage current tools, tactics and procedures used by bad actors such as penetration testing, vulnerability scanning, social engineering, and deployment of payloads.

The Blue Team assessment will allow you to proactively identify and then address security detection coverage gaps before they are exploited by a bad actor.

Assessment duration and outputs

At the end of the Blue Team assessment, we will produce a report containing a set of recommendations. The report would include advice on the above two points, but some content will vary depending on the Blue Team's findings. For example:

- An assessment as to whether an organisation's current SIEM solution can detect all identified threats.
- Identifying any gaps and risks in the current solution e.g. How easy is it for malware to propagate?
- Tuning recommendations.

CGI's Global Threat Intelligence platform

We will leverage our global threat intelligence platform to assess your ability to detect threats associated with your organisation, taking intelligence feeds from a wide variety of sources, including:

- CGI's Global Threat Intelligence Platform.
- The National Cyber Security Centre (NCSC) which includes CISP.
- Microsoft Intelligent Security Association (MISA).

All of which provide unique, combined intelligence data on emerging threats relevant to your organisation and knowledge of defences against those threats. Many of the tools we use contain machine learning and AI elements to help keep up with continually evolving threat actors.

Benefits Include:

- Confidence that your SIEM can detect current threats.
- Cost effective, only ingesting security logs that are required and nothing else.

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:

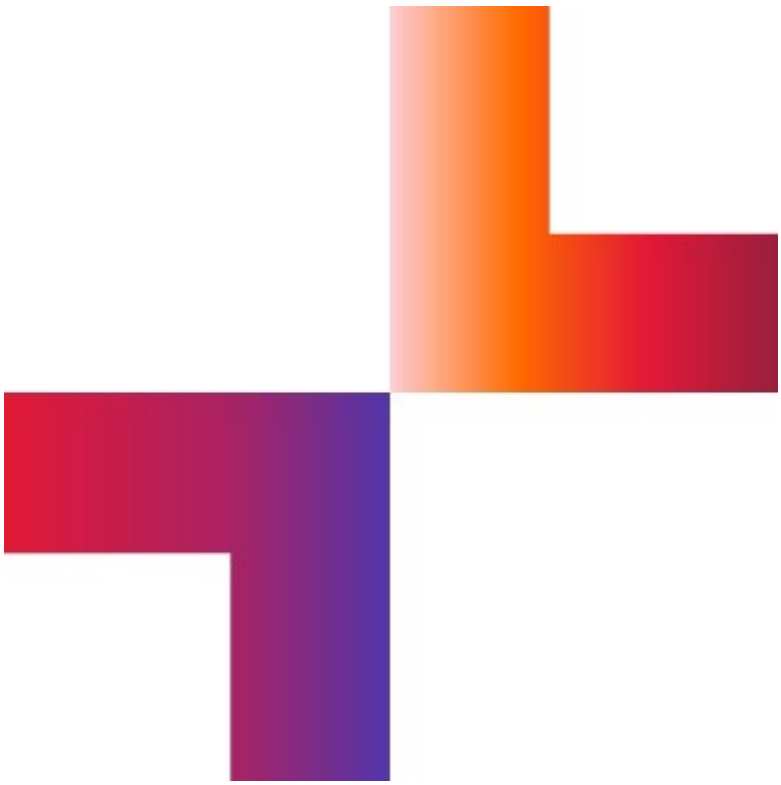
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk