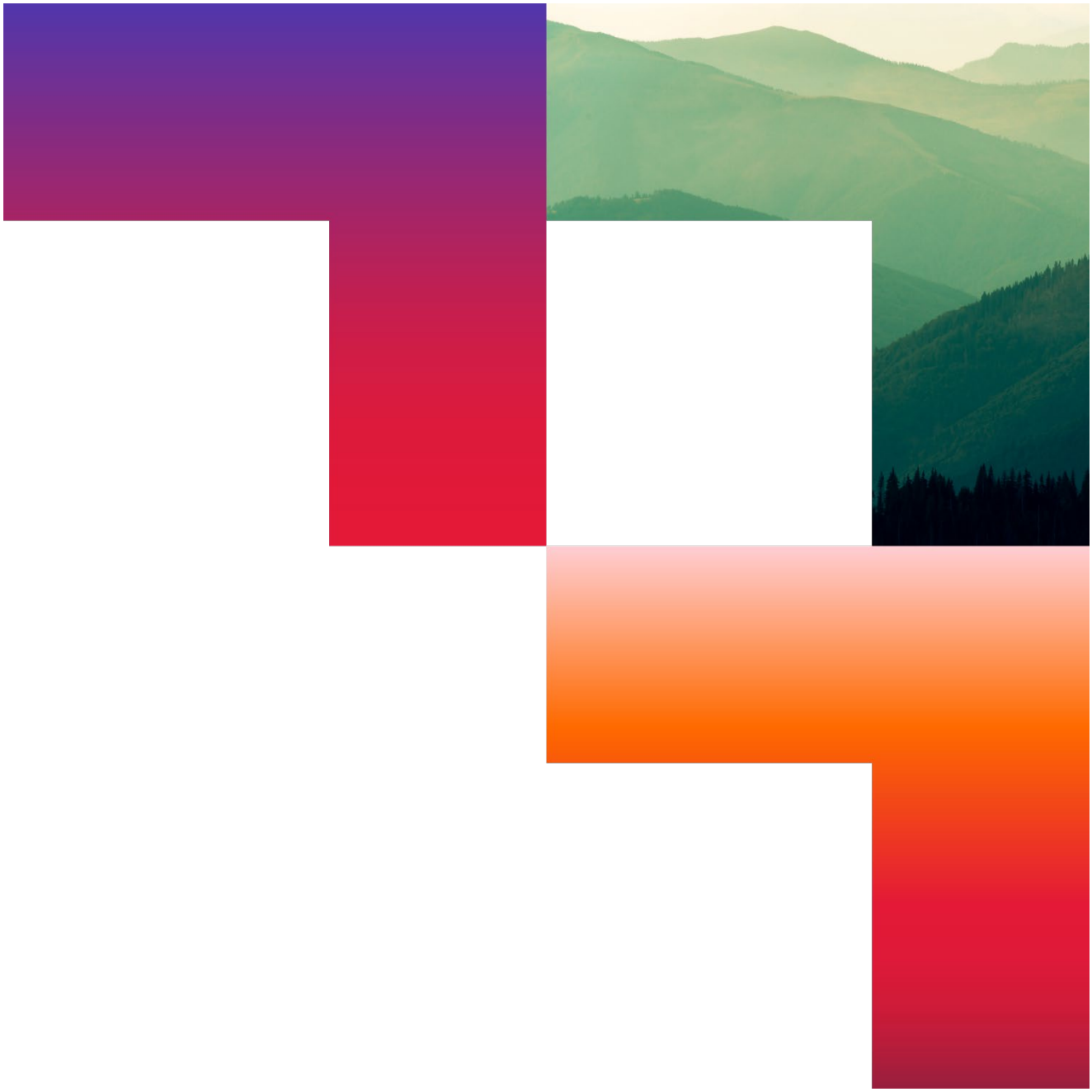


Situation Awareness Fusion Architecture (SAFA) as a Service

Contracting body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

Clients are increasingly confronted with a rapidly evolving cybersecurity threat landscape, characterised by more sophisticated and frequent attacks targeting IT infrastructure worldwide. Our capabilities are designed to enhance clients' ability to understand and respond effectively to these threats across various environments, regardless of their operational locations.

We provide a comprehensive service encompassing the design, build, and operation of a Cyber Detect & Respond (D&R) capability, known as Situational Awareness and Fusion Architecture (SAFA), specifically tailored for UK front-line commands. This service comprises three core components:

- Client Core Network System
- Mission Deployed (Configurable) System
- Incident Response Intervention System (IRIS).

Why CGI?

CGI has been delivering SAFA services since 2016, including the design, construction, and operation of D&R capabilities supported by a modern GitOps platform and a DevSecOps framework, all aligned with Secure by Design (SbD) principles. Our team of over 80 multidisciplinary professionals possesses extensive experience and the necessary skills to manage and operate SAFA capabilities effectively.

1. Service Description

SAFA integrates three advanced cyber detect and respond capabilities, developed through iterative and collaborative efforts within operational environments. These capabilities are considered to be at least third or fourth generation in terms of maturity.

1.1. Detect & Respond Capabilities.

1.1.1. Client Core Network Connected

The Defensive Cyber Capability (DCC) Core platform safeguards the Clients Digital Backbone, which supports over 400,000 users and more than 200 mission-critical systems. It is utilised by Front Line Commands and Defence Digital Security Operating Centres to monitor and defend against cyber threats. Many clients operate extensive IT estates supporting over 100,000 personnel across numerous locations, facing daily cyber-attacks ranging from low-level criminal activities to sophisticated state-sponsored threats.

The DCC Core is engineered to aggregate vast amounts of cyber-related digital data, enabling analysis, visualization, and intelligence extraction. This facilitates prediction, prevention, defence, and recovery from complex cyber compromises. Key features include:

- Processing of 6TB of data daily from over 200 systems.
- Storage of over 3PB of Big Data at UK Government Protective Marking OFFICIAL and SECRET levels.
- Security Information and Event Management (SIEM) powered by Elastic.
- Packet Capture analysis via Endace.
- Endpoint Detect & Respond supported by Tanium.
- Incident and case management through Atlassian.
- Security Orchestration, Automation, and Response (SOAR).
- Data science tools utilising Kafka, Spark, and Superset.

1.1.2. Mission Configurable System (Not Connected)

The DCC Configurable system provides cyber protection for Client systems that cannot be connected to the Clients Core Network. Many mission-critical systems require portable, deployable cyber detect and respond capabilities to support military operations. These systems are designed to scale incrementally to meet operational demands and are easy to maintain, based on feedback from Cyber Protection Teams. Key features include:

- Auto-scaling capabilities for increased data storage.
- Remote operation and maintenance functionalities, subject to wide-area network connectivity.
- Streamlined maintenance through an advanced patching system.

Hardware and software specifications include:

Software	
Data Store	RedHat OpenShift, Elastic
Packet Capture	Endace
Intrusion Detection and Network Analysis	Zeek (Corelight)
Operating System	RedHat OpenShift Kubernetes

Hardware	
Processor	Intel Xeon Gold 24/48 threads
Memory	256 GB

Storage	26TB (16TB usable)
Dimensions	1U
Weight	74 kg
Transit Case	Peli-Case
Physical Interfaces	X710-T4L Quad Port 10Gbe, X710-T2L Dual Port 10Gbe, Cisco Switch, Juniper SRX 340 firewall

1.1.3. Incident Response Intervention System (IRIS)

IRIS is a portable system designed to assist incident response teams in rapidly recovering from cyber incidents. It addresses challenges such as limited visibility into attacks and the complexity of IT environments, enabling swift root cause analysis and system restoration. Key features include:

- Data ingestion and storage
- Packet capture capabilities
- Endpoint detection and response
- Forensic analysis tools.

IRIS operates securely and can interact with infected systems or malware for investigation purposes. It is designed to be wiped and rebuilt between operations to ensure safety and security. Hardware specifications include:

Software	
Data Store	Elastic
Endpoint Detect & Respond	Tanium/Elastic
Packet Capture	Endace v-Probe
Intrusion Detection and Network Analysis	Zeek (Corelight)
Forensics	Kape

Hardware				
Operating System	Windows Server 2022			
Processor (Cores)	64	96	144	Up to 144 Cores Intel Xeon 6 6500/6700 series
Memory	256 GB	512 GB	1 TB	Up to 2 TB DDR5 RDIMM
Storage (TB)	36 (32+4)	64 (60+4)	128 (120+8)	Up to 491+ TB removable NVMe SSD
Dimensions	13.55" x 15.35" x 6.36"			
Weight	13-18 lbs			
Transit Case	Custom designed MIL-STD-810H and other options			
Physical Interfaces	Multiple USB ports, 10G SPF+, 10GbE ports, VGA, IPMI, PCI slots, NVIDIA GPUs, integrated touch display			

2. Onboarding and Offboarding

2.1. Onboarding

Prospective clients should contact CGI to express their interest in subscribing to our Cloud-based services. Following contractual agreement, CGI will prepare the Cloud-based instance according to the Client's specifications. If data migration and/or other services are required, these will be scoped and priced accordingly.

The time taken to provision the service from the point of order will be determined by the client's requirements, in regard to data migration, client-specific configurations (for example, user accounts) and other services. Should data migration and client-specific configuration not be required, the service can be provisioned within four to six weeks, based on a standard configuration. This allows for the client to upload data, test the system and conduct the necessary training activities.

2.2. Off-boarding

CGI will provide clients with a simple and quick exit process, including the retrieval of their data.

Our solution for off-boarding will build upon our standard commercial practices for transition and exit management services, using the framework agreed during contract negotiations. We will take responsibility for managing our exit and, where appropriate, the transfer of that service to a new supplier.

CGI will discuss the requirements for the format and content of the off-boarded data with Contracting Bodies when setting up each contract. We will include this within the contract price that is agreed.

The off-boarding process will include the phases and their associated activities described below.

2.3. Pre-exit

This is the period in which the Contracting Body will have identified the need to off-board CGI or be negotiating the exit of CGI. CGI's Service Delivery Manager (SDM) will support the client in defining and agreeing:

- The business impact statements.
- Communications plan both into the Contracting Body and the Supply Chain.
- Client obligations and dependencies.
- CGI responsibilities, obligations and dependencies.
- Governance and progress meetings for handover to the new supplier.
- Exit related milestones.
- Completion and acceptance criteria.
- The overall risk management plan for the Off-boarding phase.

The outcome of this phase will be a distinct off-boarding plan, delivered by the SDM, with clearly defined and documented accountabilities and responsibilities for the implementation phase. It will include clear financial and commercial plans and clear completion criteria.

2.3.1. Exit Management

The Off-boarding SDM will manage the risks (identify, mitigate and manage those under our control), those risks identified in the pre-implementation phase and any others as they arise, using our standard risk and issue management processes defined and agreed for all project activities.

When necessary, the Off-boarding Project Manager will escalate non-conformances, changes to risk status or issues arising from the new supplier's actions, or indeed from those of yourselves or CGI.

The specific areas of activity for which the Off-boarding Project Manager will be held accountable are:

- Ensuring that the access rights to both CGI and your systems, processes and tools are terminated.
- Remove and clean up all related documentation, removing references to CGI where appropriate, to ensure that documentation and process integrity is maintained. This will be in accordance with any necessary requirements appropriate to the removal and deletion of classified material.

- Ensure that any requirement to return information, data and material provided or generated by representatives of the Contracting Body in the appropriate format (as requested by yourselves, and as defined in the Operations Manual), is met.

2.3.2. Post Implementation

This phase deals with closing the Off-boarding project after its successful conclusion. In addition to the standard post-implementation review processes, the CGI Transition Manager will also support you in verifying that exit obligations have been met by all parties.

3. Security

CGI uses our Management Foundation including our Integrated Management System (IMS) for information assurance. These IMS processes are independently certified to BS/EN/ISO 9001:2008.

CGI is committed to retaining our current range of UK-based certifications and will extend these to meet client expectations as required.

The CGI Management Foundation design allows incorporation of best practice from across all our Public Sector and Commercial engagements.

Our accreditations include:

- ISO9001, ISO27001 and ISO20000
- ISO/IEC 27001:2005 Audit and Certification SSAE 16/ISAE 3402 Attestation
- E.U. Data Protection Directive - (95/46/EC).

All information is held at the appropriate security level for the service. CGI hosted services can be provided at any level defined in the new Government Security Classification (GSC) policy with the appropriate assurance.

Information Principles for the UK Public Sector supported and documented?

CGI recognises the UK Public Sector information principles which are fundamental to the efficient and effective delivery of public services. Where we store and manage government information in our G-Cloud services we aim to ensure that it is appropriately protected and available to exploit. Through this we would aim to maintain and, depending on the particular service purchased, enhance the quality of the information stored in a standard manner that enables its re-use. Where the selected services require it, we would engage positively both to support the buyer in the publication of public information and to support them in the access of information by citizens and business.

Government ICT Strategy and Greening Government ICT Strategy supported and documented?

The design and delivery of our Cloud-based SaaS offerings is consistent with the principles of the Greening Government ICT Strategy. Scalable, Cloud-based services allow pooling of capacity across multiple clients, reducing overall hardware requirements. These are further reduced through virtualisation, which has delivered up to a 90% reduction in server numbers and power consumption for some of our services. We select modern, energy efficient servers, storage and network hardware and have also invested heavily in improving the energy efficiency of our data centres. This includes initiatives such as free air cooling, aisle containment, power supply upgrades, lighting controls and power management and monitoring software. In the UK, electricity for our data centres is sourced from renewables, which is also the case for many of our third-party hosting providers. We closely manage the impact of IT hardware throughout its lifecycle, aiming to optimise refresh cycles to balance in-use carbon savings of newer, more efficient hardware against the carbon impact of its manufacture. At end of life, we also ensure responsible disposal through resale or recycling of old hardware wherever possible. Our sustainability performance has won widespread recognition, including our listing on the Carbon Disclosure Leadership Index for four consecutive years and our certification under the Carbon Trust Standard.

4. Service Pricing and Terms and Conditions

4.1. Pricing

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

4.2. Terms and Conditions

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

5. 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 contained in this document is confidential to CGI and/or CGI group companies. This document shall not be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, or submitted to a generative AI tool without the prior written approval of CGI. The receiving party may use this document and the information contained in it for the purpose of evaluating CGI's proposal only. Any personal data included in this document must not be replicated, stored or distributed beyond the immediate recipient or used for any purpose other than evaluating the document.

This proposal is subject to contract and shall not be binding unless and until execution by CGI and Contracting body of a final agreement to the proposal, containing the terms and conditions that will govern the relationship between the parties. Any final agreement is conditional (inter alia) upon due diligence and customary business investigations by CGI. The results of such due diligence and/or investigations may impact upon content of this proposal, including the business structure, business terms and financial arrangements.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at +44 0845 070 7765 and to return this document by special delivery marked for the attention of Simon Figg.

Except where indicated otherwise, all names, trademarks, logos and brands (registered or not) referred to in this document are the property of a company in the CGI group or its licensors.

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

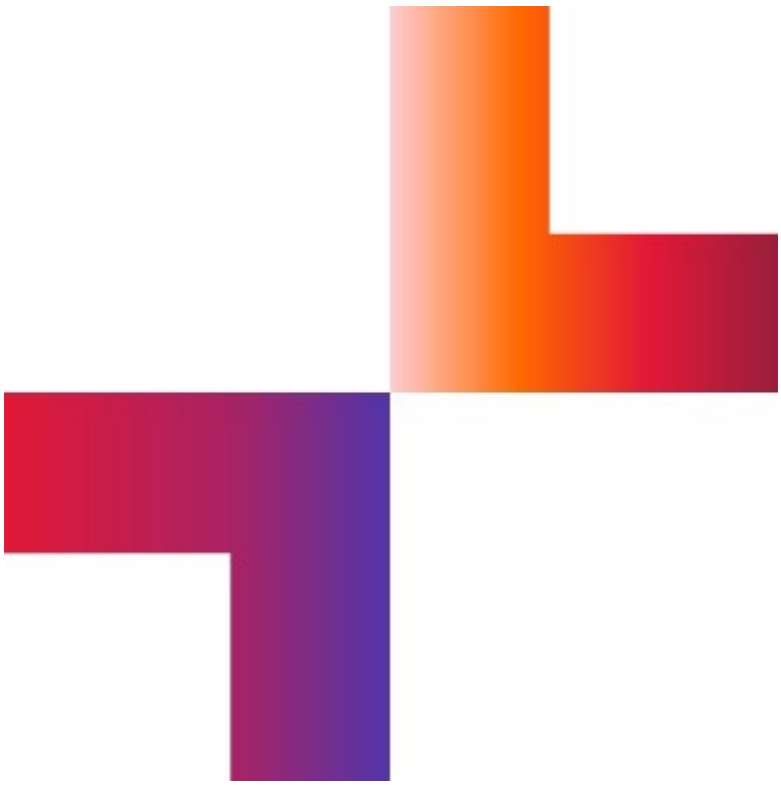
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk