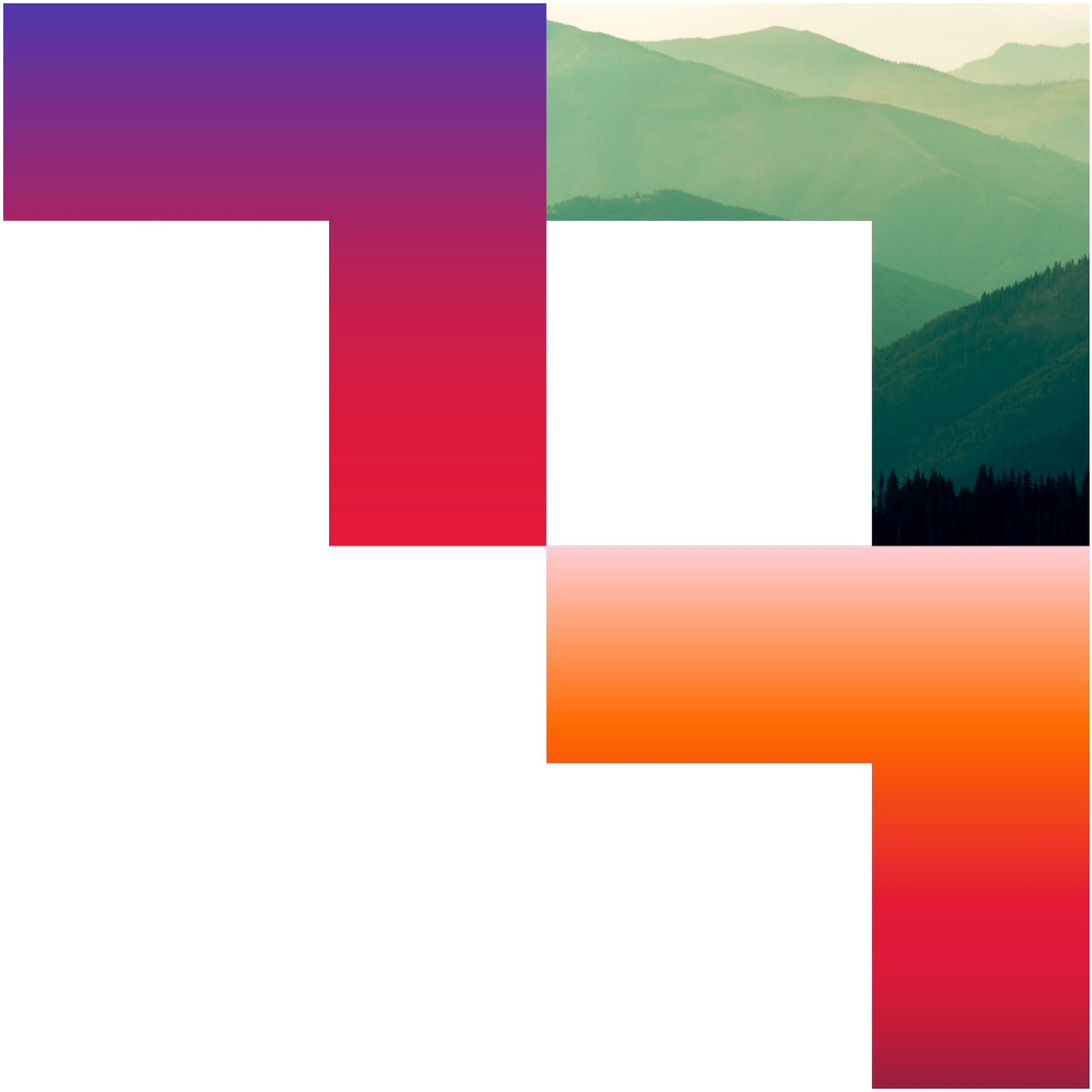


# Cyber Threat Intelligence (CTI) Services

## Contracting body

30 Jan 2026

Issue 1.0

# Table of contents

# Service Definition overview

Cyber Threat Intelligence is the knowledge of your adversaries and their motivations, intentions and methods that is collected, analysed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise.

# Why CGI?

With 50 years of experience across government and commercial sectors, CGI is proud to operate 10 global SOCs with a portfolio of over 150 clients, for which we fully manage their security services. With a key focus on the UK, we have specifically created cyber-security centres in South Wales and Berkshire to be centres of excellence for the security services that CGI delivers to our UK clients. These form part of CGI's global pool of cyber-security resources and our network of 10 additional Cyber Security Centres of Excellence, with whom our UK-based resources share best practice and innovation on a regular and continuous basis.

**Cyber Consultants**

We have over 260 qualified cyber experts in our Cyber Consultants practice. In Cyber, we maintain a depth of employee experience, ranging from Cyber graduates, to CISOs with over 20 years' experience within Cyber Security.

Our Security Operation Centre hosts a number of specialist Teams, including Cyber Threat Intelligence (CTI), Phishing and Digital Forensic and Crest accredited Incident Response (DFIR) Teams, all of which are 100% UK-based, and hold SC or DV clearance.

**Certifications**

- We are a founding member of the Cyber Security Information Sharing Partnership (CiSP).
- We are a member of the Microsoft Intelligent Security Association (MISA). Membership is obtained by invitation only and held by approximately 300 companies globally. Our partnership with Microsoft allows us to access the right resources and take intelligence feeds that are not available via any other programme.
- We have been a Microsoft Gold Certified Partner for Security Solutions since 2003.
- Accredited for ISO 27001 - Information Security Management Standard.
- Accredited List X - UK Government site security scheme for suppliers required to hold sensitive information.
- Cyber Essentials Plus Certification.
- Defence Cyber Certification - Level 0.

# 1. Service Description

## 1.1. Why you need to take action.

Cyber criminals have scaled up their attacks, resulting in a significant rise in ransomware attacks, data thefts and supply chain compromises. Without Cyber Threat Intelligence, enterprises are unable to understand who may be targeting them and the tactics, techniques, and procedures they use. This lack of knowledge limits defenders in mitigating the risks to the organisation. This makes it difficult to prioritise vulnerability management, and to know where to focus their limited budgets for maximum impact.

Our CTI service gives you insight into:

- Cyber criminals
- Hacktivists
- State-sponsored attackers
- Insider threats
- Accidental / malicious external data loss
- Mentions of your organisation on the dark web
- Threat detection prioritisation
- Cyber-attack trends against your industries.

Without a comprehensive security strategy, organisations leave themselves vulnerable to attacks that could cost millions to recover from and seriously impact their brand.

## 1.2. How does our CTI service work?

At CGI, intelligence is drawn from a comprehensive range of both open and closed sources. This includes intelligence reports from cyber security vendors, raw data, malware signatures, leaked credentials, mentions on a paste sites & code repository, logo abuse detections and detections of registered domains associated to your trademark and company. With threat actors setting up watering hole attacks using fake websites utilising company associated domains and logos, we can conduct takedown requests on your behalf to reduce risk.

Our highly skilled threat intelligence analysts assess the information gathered and turn it into intelligence that can be trusted. We provide daily landscape reports, monthly client-specific industry reports, and ad-hoc threat intelligence monitoring and alerts, with refined reporting specific to your organisation. All our intelligence products provide insights that allow you to take action to mitigate the risk and are aligned to the MITRE ATT&CK framework, as advised by the NCSC.

We integrate our service with your existing security tools and infrastructure. Our Cyber Threat Intelligence envelops your IT security posture providing a defensive force multiplier to your operational or network security teams. We can provide ingestible data feeds that provide intelligence straight into security tools such as SIEM, IDS and firewalls maximising their capabilities to identify threats, bolstering your automated security response. What is more, we can start delivering threat intelligence services in as little as seven days, so you can rapidly understand your organisation’s threat landscape and take immediate action.

## 1.3. Benefits

- Predict, identify, and rapidly mitigate cyber-attacks with insights and intelligence that reach far beyond your own network defences.
- Improve your threat detection with better visibility of threats explicitly targeting your sector, infrastructure, and digital assets.
- Apply constant monitoring using advanced threat intelligence platform tools, so no attack goes unnoticed or unaddressed.
- Achieve in-depth understanding of new global risks, informed by a world-wide network of threat intelligence expertise, and stay one step ahead of attackers.

- Enable strategic decision making by understanding the Advanced Persistent Threats (APTs) that are affecting your organisation, allowing you to make strategic decisions to mitigate the cyber threat.
- Ensure your security posture is proactive not reactive and improve decision making during and after a cyber-intrusion.
- Support regulations such as GDPR, PCI DSS and HIPAA by providing intelligence and insights to strengthen security posture whilst demonstrating compliance.

## 1.4. What's included?

- Daily threat landscape report.
- Monitoring of external data sources including:
- Dark web, including ransomware extortion site mentions
- Code repositories
- Pastebins
- Messaging platforms
- Social media
- Logo abuse
- Supplier mentions by threat actors
- Industry peer mentions by threat actors
- Monthly client threat report
- Technology stack monitoring
- IP address monitoring
- Brand monitoring
- Malware analysis
- Malicious website takedown
- Alerting (emerging threat reports).

## 1.5. Optional Services

- Corporate digital footprint analysis
- Corporate VIP protective monitoring
- Service integration with Managed Detection and Response service
- Phishing campaign service
- Phishing triage service.

# 2. Data backup and restore

CGI can carry out backup and restore activities in accordance with any specific requirements and in compliance with the Information Assurance Backup / Restore policies as defined in ISO 27001; any information that has been processed as part of an engagement will be stored securely. Where applicable, this information can then be restored from an appropriate back-up, should the need arise.

# 3. Service Continuity

CGI will agree appropriate service continuity in accordance with any specific requirements, and any conditions that need to be met.

# 4. Onboarding and Offboarding

## 4.1. Onboarding

For Specialist Cloud Services, CGI will engage directly with the client to ensure the full scope of the requirements is understood and agreed in advance of any engagement. We will work with senior stakeholders to define the necessary business outcomes and ensure the services are aligned accordingly.

For all services, CGI understands the client's requirements and make on-boarding specific to these needs, using the experience, lessons learnt and methodology from many years of public sector transition experience, we can quickly align to client joiners, movers and leavers policies and ensure that we have appropriately cleared staff for every engagement.

## 4.2. Offboarding

Off-boarding is instigated by a client request or after expiration of the service agreement.

### 4.2.1. Access to data upon exit

Deletion of any virtual machine image and data will occur in line with the service agreement. Any required data will be made available using appropriate media, in line with the data security classification. After client notification that data has been successfully recovered, CGI will purge and destroy client data from any computer or storage device or media that remains part of CGI's estate, with the exception of any data related to a data retention agreement between a client and CGI.

# 5. Service constraints

CGI will work with you to define and tailor the services to meet your specific requirements. During this definition period, detailed responsibilities will be agreed across the service delivery. Examples of common general constraints are listed below:

- Share the existing internal sponsorship and governance for Information Assurance.
- Assign or appoint a suitably skilled and empowered person to act as the receiving client.
- Provide appropriate access to its policies, processes and standards for the Information Assurance service and other suppliers.
- Provide timely information relating to its business plans, goals and projects.

As a main feature of any Service will necessitate an on-going dialogue with client representatives, the most important responsibility of the Contracting Body is to ensure the timely availability of individuals for fact-finding interviews.

# 6. Service levels

The overall accountability for the relationship with the client lies with CGI’s Executive Sponsor and CGI Account Manager and they will provide strategic governance to the service working closely with the client's Senior Executive team or nominated delivery / engagement contact. The purpose of this team is to ensure that the relationship is collaborative, the service is delivering, as agreed, the governance model is working, and best practice is being applied.

# 7. Hosting options and locations

CGI has a network of 27 offices across the United Kingdom and Northern Ireland, with our UK members having the capability to deliver as hybrid-workers. Through our engagements we also understand that for some clients it is essential that our members are physically present on their sites, our distributed network of offices makes

this possible. Whatever your requirements are the options for hosting and locations will be agreed at contract negotiations.

# 8. Security

CGI has invested significant resources to develop an Enterprise Security Management Framework (ESMF) based on recognized industry standards and applicable regulations or legislation such as ISO 27001, ISO27701, NIST, COBIT, CIS, CCPA and GDPR to name but a few. This framework is used across the global organisation to protect information assets, technologies, facilities, and CGI members, including the data managed across the business, and is supported by CGI's security and privacy policies, standards and controls (Security Baseline) which are implemented through our processes, practices, services, solutions and our interactions with any third parties working on behalf of CGI.

Across the CGI business, the technical and organisational measures are defined using a risk-based approach. This considers the nature, scope, context and purposes of processing as well as the risk to the rights and freedoms of natural persons, where CGI is acting as either the data controller or data processor. This ensures a level of security and privacy appropriate to the risk, in situations where CGI holds responsibility and accountability for personal data processing.

CGI's ESMF Security Baseline is the minimum-security standard for all CGI offerings (including cloud-based services) to be applied by both CGI and clients. In some cases, CGI Security or Data Privacy may wish to add additional controls e.g. where sensitive personal data is involved. Where CGI or our clients agree to strengthen the level of security or privacy to consider specific requirements (risks, regulatory requirements, etc.) these additional security or protective measures will be defined within the CGI contracted services, particularly where CGI may be acting as data processor on behalf of a client.

# 9. Service Pricing and Terms and Conditions

## 9.1. Pricing

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

## 9.2. Terms and Conditions

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

# 10. 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:

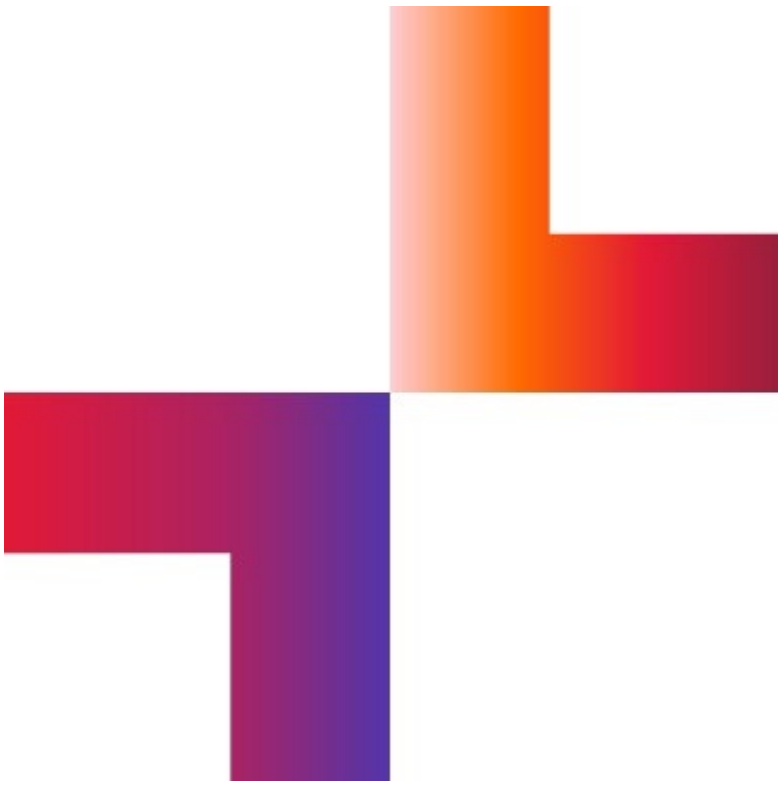
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk