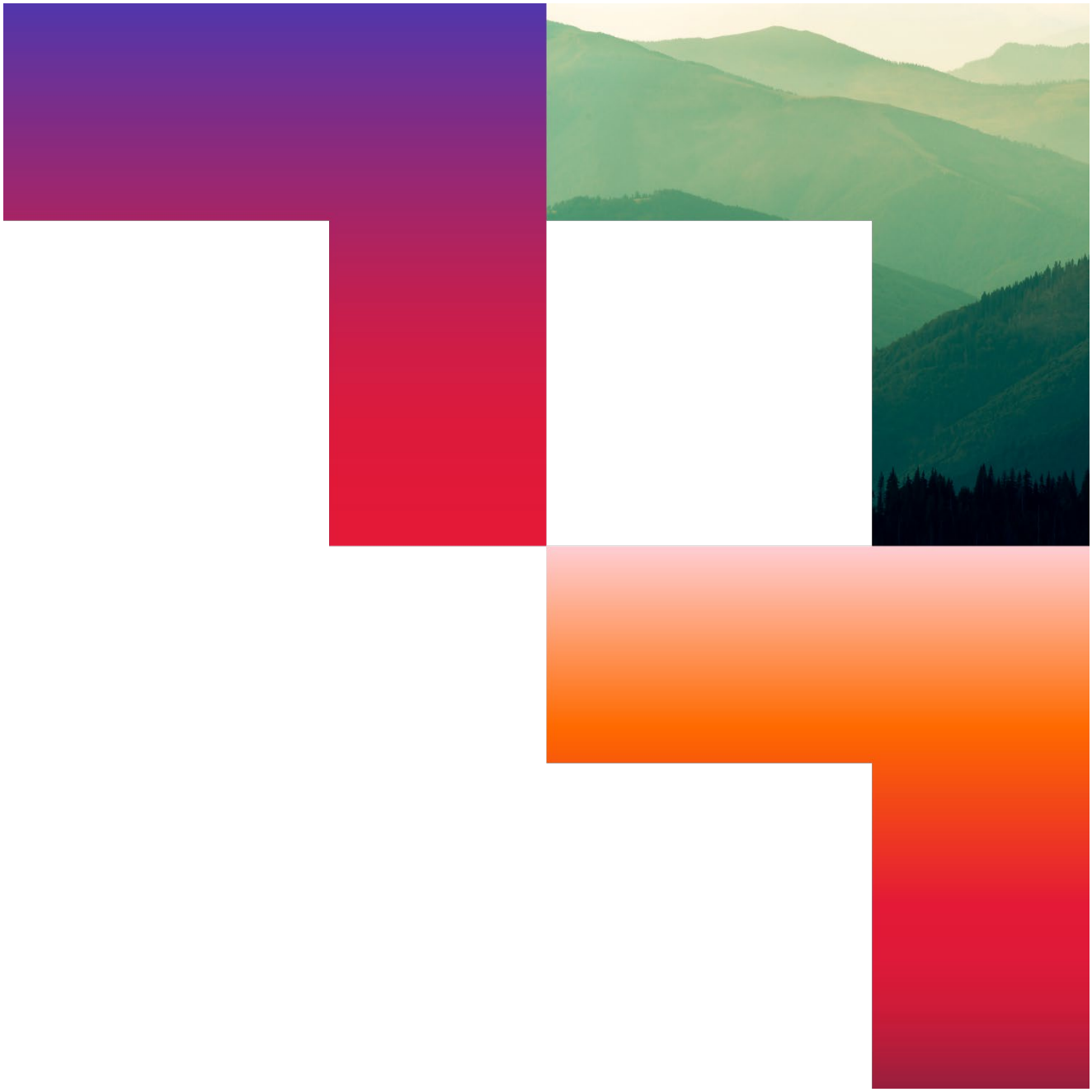


Deception as a Service

Contracting Body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

Our Deception-as-a-Service (DaaS) offering leverages Fortinet Deception technology to detect, divert, and contain malicious activity inside your environment. By deploying decoys, honeytokens, and deceptive assets across your network, we surface attacker behaviours early—before they can cause damage.

All deception alerts are securely integrated into the CGI UK SOC, where analysts validate, investigate, and respond using standardized playbook responses. This provides your organization with an advanced layer of proactive defence that turns your environment into a hostile place for attackers.

Why CGI?

For over 40 years, CGI has supported government and commercial organisations in delivering complex, high-assurance digital services and operating in highly regulated environments. This experience underpins CGI's approach to Responsible AI and AI governance, which combines strategic advisory capability with practical, audit-ready assurance.

CGI brings together in-house expertise across policy development, risk management, data, analytics, digital delivery, assurance and regulation to support the responsible adoption of AI. Our approach recognises that effective AI governance is not achieved through policy alone, but through clear accountability, proportionate controls and demonstrable evidence that risks are understood and managed in practice.

CGI has significant experience working with public sector organisations to establish governance frameworks, maturity models and assurance mechanisms that stand up to board scrutiny, audit and regulatory review. Our Responsible AI Consultancy and AI RMF service builds on this background by providing an end-to-end offering that supports organisations from initial AI strategy and use case identification through to ongoing assurance, maturity assessment and regulatory readiness.

1. Service Description

Our Deception-as-a-Service (DaaS) offering leverages Fortinet Deception technology to detect, divert, and contain malicious activity inside your environment. By deploying decoys, honeytokens, and deceptive assets across your network, we surface attacker behaviours early—before they can cause damage.

All deception alerts are securely integrated into the CGI UK SOC, where analysts validate, investigate, and respond using standardized playbook responses. This provides your organization with an advanced layer of proactive defence that turns your environment into a hostile place for attackers.

Key Objectives

- Early Breach Detection – identify malicious insiders or external attacker's post-compromise.
- Deception Coverage – deploy Fortinet decoys and tokens across endpoints, servers, and cloud environments.
- SOC Integration – route high-fidelity deception alerts directly to the CGI UK SOC for 24/7 monitoring.
- Playbook Responses – ensure consistent, rapid response and investigation actions.
- Reduce Dwell Time – limit attacker lateral movement by triggering early alarms.

Our Approach

Phase	Activities
Design & Deployment	Deploy Fortinet Deception sensors and assets (fake credentials, servers, shares, databases). Tailor deception to your environment.
Integration	Configure alert feeds into CGI UK SOC's SIEM/SOAR for correlation and case management.
Playbook Development	Build and test playbooks covering common scenarios: – Credential theft attempts – Privilege escalation – Lateral movement – Unauthorized data access
Monitoring & Response	CGI UK SOC monitors deception alerts 24/7, validates incidents, and executes playbook responses.
Continuous Tuning	Adjust deception layer and playbooks based on threat intelligence, SOC feedback, and adversary behaviour.
Reporting & Review	Provide monthly service reports, incident summaries, and maturity recommendations.

Deliverables

- Deception Deployment Plan – tailored blueprint for Fortinet Deception across your environment.
- Integrated SOC Alerting – deception alerts directly monitored in CGI UK SOC.
- Playbook Library – standardized workflows for detection, triage, investigation, and response.
- Incident Reports – detailed investigations of triggered deception events.
- Monthly Service Reviews – insights into activity trends, lessons learned, and roadmap recommendations.
- Executive Dashboards – high-level metrics on deception effectiveness and SOC response times.

Benefits to Clients

- High-Fidelity Detection – deception produces near-zero false positives, allowing SOC analysts to focus on real threats.
- Reduced Lateral Movement Risk – attackers engaging with decoys are detected early before reaching critical assets.
- Playbook Consistency – responses are standardized, repeatable, and aligned to best practice.

- 24/7 SOC Coverage – integration with the CGI UK SOC ensures round-the-clock monitoring and response.
- Adaptive Security – deception assets can be tuned and updated to evolve with the threat landscape.
- Deterrence Factor – increases attacker uncertainty, raising the cost of intrusion.
- Regulatory & Assurance Value – demonstrates proactive threat detection capability to stakeholders and auditors.

2. Service constraints

CGI will need to complete a technical assessment prior to you purchasing this service.

3. Service Pricing and Terms and Conditions

3.1. Pricing

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

3.2. Terms and Conditions

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

4. 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:

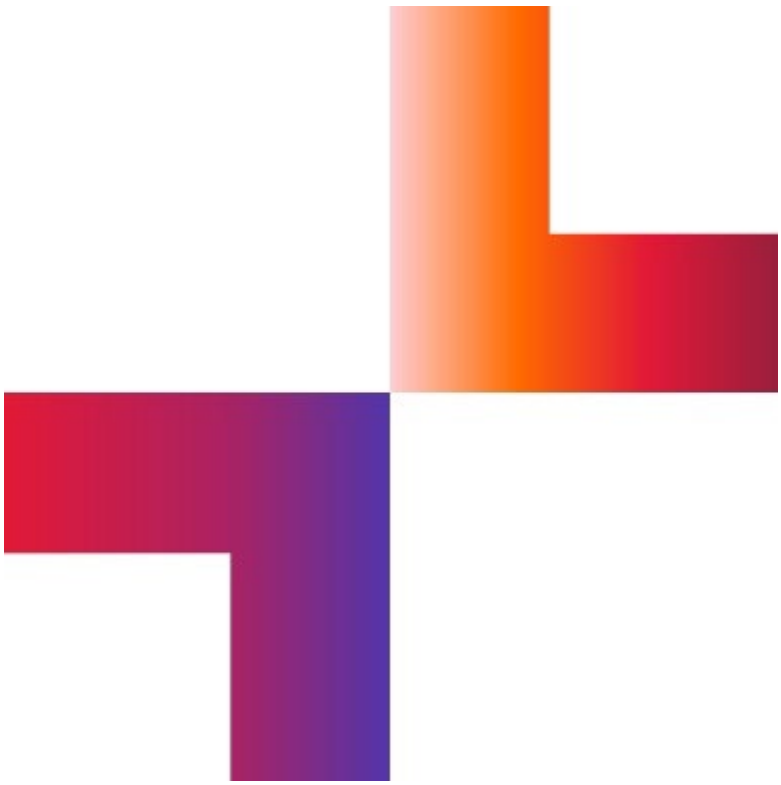
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk