CGI's Protective Monitoring Service

A protective cyber security monitoring service continually analyses an organisation's infrastructure and systems looking for malicious behaviour. It then provides the insight to detect and act on suspicious events, in real time, 24 hours a day.

Our Protective Monitoring Service collects and centrally aggregates security event logs from a wide variety of sources. It triages events in real-time and identifies malicious activities and attack patterns based upon specific customised criteria, appropriate to your environment.

We operate from two UK Cyber defence centres, monitoring, alerting and responding to threats 24x7 all year round for a range of Government and industry clients, using our expertise, technology and skills to deliver cyber security protection.

Benefits

- Transfers responsibility for cyber security monitoring to a managed security service provider with over 40 years of experience in managing risk efficiently and effectively.
- Avoids the cyber security skills gap and any worries about recruiting, training and retaining staff, with access to over 1,700 cyber security professionals operating within 10 global security operation centres (SOCs).
- Takes care of all your day-to-day monitoring requirements.
- Delivers industry-standard protective monitoring via SIEM technology and adheres to Government mandated Protective Monitoring standards such as NCSC, MITRE ATT&CK and GPG13.
- Provides robust security with all data stored and processed on shore in the UK.
- Offers a cost-effective way to free up internal resources to other projects and focus more on your core business activities.
- Customise your service to fit your budget with flexible and scalable 'per-device' pricing and a choice of coverage, from core business hours to 24x7x365.

Why you need to take action

The cyber threat landscape continues to evolve with new, innovative and varied attack methods adapting to their chosen targets environments and driving the threat world into new areas. The risks to your organisation from cyber security incidents is real, and attacks regularly cause significant damage to the performance and reputation of many organisations.

Protective monitoring helps you identify issues and rectify them before they do serious damage to your organisation. It overlays and augments traditional defences with critical sources of information, improving network visibility and security.

How CGI's Protective Monitoring Service works

There are **three primary elements** to our Protective Monitoring Service:

1 Collecting the data

Our Protective Monitoring Service collects event data and logs from the technology in your environment such as network devices, host systems, cloud logs, databases, endpoint systems and applications or software services regardless of whether they are running on-premise or in the cloud. As a minimum, we retain these logs for 180 days so we can look back if required to support any investigations. Our analysts normalise and aggregate this data to enable rapid correlation.

2 Connecting the dots

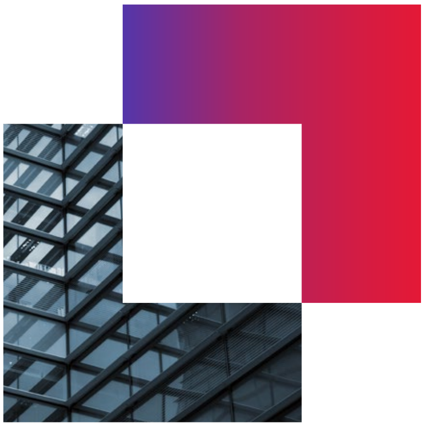
The correlation and enrichment processes are carried out in real-time using our SIEM platform and tooling to ingest the data and detect threat patterns, configuration issues and cyber security incidents.

3 Triage

Our security analysts respond to alerts in accordance with CERT best practice by triaging the event, identifying assets involved and performing additional searching for related logs to validate the threat or to establish a false alarm. If the threat is validated, we'll raise an incident ticket to your CERT team with information about the incident, with containment and/or eradication advice.

We will use a filtering process to reduce the false alarm rates and to allow our analysts to monitor the 'real' threats to your business. We will work with you to create a continuous improvement plan for your Protective Monitoring Service. This will include developing use cases to focus on alerts of real interest, using industry knowledge and our own deep knowledge of current threats to mitigate future threats.

Your Service Delivery Manager will provide regular reports that detail all relevant activity and common threats, giving you peace of mind that your organisation is protected from attackers.



We operate from two UK Cyber defence centres, monitoring, alerting and responding to threats 24x7 all year round for a range of Government and industry clients, using our expertise, technology and skills to deliver cyber security protection.

What to expect from onboarding

We recognise that, by working with us, you are trusting an external company with the responsibility of monitoring your network and protecting your data. Your CGI contact will be there throughout the process to provide the reassurances you need while we prove that we are a trusted and highly regarded managed service provider.

We have a proven service transition methodology that is part of our managed service solution. It makes sure we deliver your service on schedule and with minimum disruption.

Your onboarding team will include representatives from our technical design and engineering teams who will run an initial workshop to define the scope of your monitoring and connectivity. After the workshop, two key members of the team will continue to work with you through to go-live on your Protective Monitoring Service:

- Your Project Manager will take responsibility for the effective coordination of all transition services from design, build, test through to cutover to the service team. They will be on hand to support you throughout the transition phase.
- Your Service Delivery Manager will take responsibility for all service delivery and our customer account relationship with you throughout the life of your contract with us.

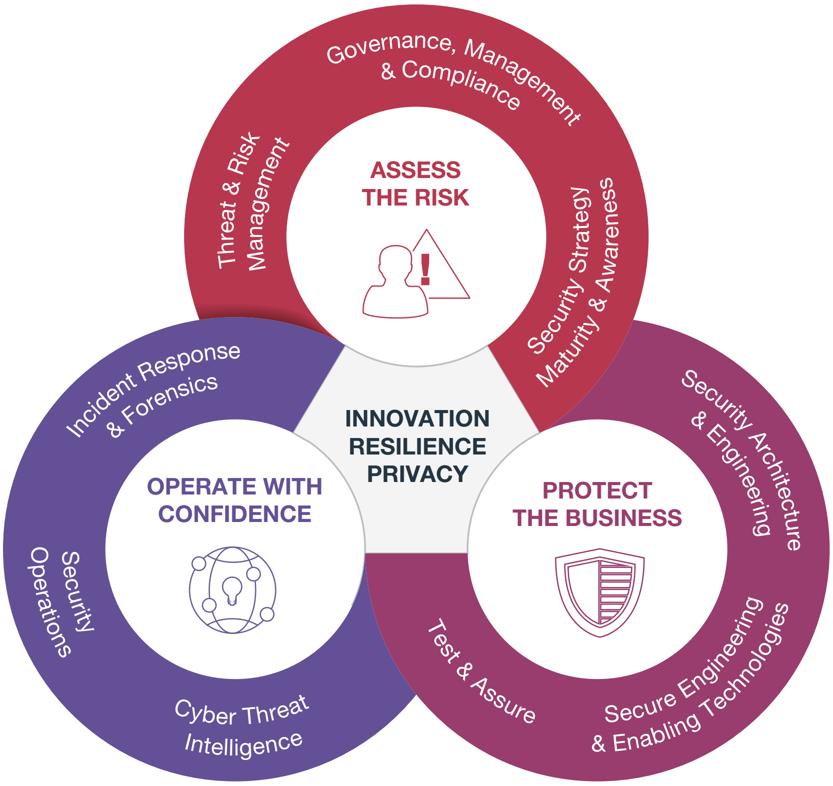
> "CGI's responsiveness demonstrated their commitment to supporting the business and continuing to drive service improvements for us at a time of significant upheaval. The long-standing relationship we have with CGI meant that we had a trusted partner who has helped us ensure our IT systems are flexible and agile enough to manage in unprecedented times."

Andy Feldon
IT Director at Taylor Wimpey

Why CGI

We have a long-standing and highly regarded reputation in IT and business consulting. We offer cyber threat protection monitoring and other managed services across a wide range of sectors including commercial, education, financial, insurance, central government and critical national infrastructure. Individual reference points are available upon request.

We help businesses and government clients to assess risks, protect their business and operate with confidence in the digital world. Over 80% of our team of 1,700 cyber security professionals have government clearances. We operate from 10 Security Operations Centres globally to deliver cyber security services that are tested and proven in some of the world's most sensitive and complex environments.



Governance, Management & Compliance
Threat & Risk Management
ASSESS THE RISK
Security Strategy Maturity & Awareness
Incident Response & Forensics
INNOVATION RESILIENCE PRIVACY
Security Architecture & Engineering
OPERATE WITH CONFIDENCE
PROTECT THE BUSINESS
Security Operations
Test & Assure
Secure Engineering & Enabling Technologies
Cyber Threat Intelligence

We have a proven service transition methodology that is part of our managed service solution. It makes sure we deliver your service on schedule and with minimum disruption.

Choose a service level that suits you

Your initial consultation with one of our cyber representatives will help you decide what level of service will best match your requirements and organisation's expectations.

Baseline

Device count: 0-50

- Data retention for standard log sources for 180 days.
- Monitoring and alerting, plus email and ticket alerting during core business hours.
- Standard executive monthly report.
- NCSC standard use case library.

Enhanced

Device count: 51- 250

- Data retention for standard log sources for 180 days plus two custom log sources.
- Monitoring and alerting, plus email and ticket (plus P1 verbal) alerting during core business hours with option for 24x7 cover.
- Custom executive monthly report.
- NCSC standard use case library and five custom use cases.

Advanced

Device count: 250+

All the features of the Enhanced +

- 10 custom use cases are included in addition to the NCSC use case library.

We help businesses and Government clients to assess risks, protect their business and operate with confidence in the digital world.

Protective Monitoring can also integrate with other services we provide:

- **Cyber Threat Intelligence** – this feeds current, industry specific threat vectors into your Protective Monitoring Service.
- **Anti-Phishing Service** – lockdown one saw a 30,000% increase in phishing attacks making it the number one threat to UK industry. Protect your business from these emails with our Anti-Phishing service.
- **Digital Forensics and Incident Response** – breaches do happen, and including our retainer-based option into your Protective Monitoring Service gives you rapid access to our DFIR team.
- **Vulnerability Management** – improve your security posture by improving visibility into your exposure to known vulnerabilities. This supports developing a more mature, integrated security posture.

Make an enquiry

If you know who your contact point is within CGI, then simply reach out to discuss the options best suited to your requirement.

For general enquiries, please email: cyber.enquiry.uk@cgi.com

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 77,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information
Visit cgi.com/uk/cyber-security
Email us at cyber.enquiry.uk@cgi.com