Protective Monitoring Services

CGI
Experience the commitment®

Cyber attacks are becoming increasingly sophisticated, targeting people, networks and devices. Attackers are finding new ways into organisations by-passing the perimeter security walls and stealing valuable information or disrupting business. Organisations need to be agile, adopt new technologies, operate with customers and suppliers across the world and be confident that they are secure.

THE CHALLENGE

The cyber threat to organisations is increasing as attempts are made to steal, alter, deny or destroy digital property on a daily basis. As the financial rewards grow, the scale, frequency and sophistication has escalated. Small groups, located anywhere in the world, can launch attacks on a huge scale at little cost. Threats can be from foreign states, political activists, organised crime groups, or individuals seeking to disrupt operations for their own gain.

Often, security measures are introduced reactively as organisations grow, merge or adopt new technologies, which can leave data vulnerable to the dynamic threat of cyber attack. An intrusion detection system may protect your network from some attacks, but they need an expert analysing logs for suspicious activity. Network ports may be configured to deny unauthorised devices connection but, unless these are continually monitored, there is no way to detect new unauthorised access.

Organisations are being asked to do more with less. A growing volume and diversity of data must be protected, whilst costs must be reduced. The threat posed to data, will continue to grow, so any protective solutions need to be flexible, scale as requirements change and be at a sustainable price.

Cyber attackers, continually evolve the tools and methods they use. So updating the skills and knowledge of your IT security staff and keeping them within your organisation is a constant challenge.

OUR PROTECTIVE MONITORING SERVICE

As a leading supplier of cyber security services in the UK, Europe and North America, we offer the full range of services to secure your organisation.

Our Protective Monitoring service continually scans an organisation's infrastructure and systems looking for unusual patterns of behaviour. We then provide the insight to detect and act on suspicious events, in real time, 24 hours a day.

The service is provided from one of our Security Operating Centres (SOC), which is a centralised shared service responsible for monitoring the systems, networks and devices for multiple clients. The service can be hosted in the UK or one of our other nine global locations.

A CYBER SECURITY PARTNER YOU CAN TRUST

- The best cyber security supplier in the UK with hundreds of experts
- Ten Security Operations Centres with shared intelligence
- 24 hour, every day monitoring of systems with real-time alerting
- Immediate action on suspicious activity by containment or shutdown
- Supports governance and regulatory compliance
- Dashboard highlighting key areas of vulnerabilities
- Full reporting to support forensics and evidential requirements
- We are developing a secure service enabling utility companies to access information on the energy usage of the 53 million smart meters which will be deployed in the UK from 2015
- As a trusted partner to the Canadian Payments Association, we help ensure that more than $170 billion in transactions a day are cleared through CPA systems safely and securely
- For 27 years we have operated a commercial evaluation facility and regularly test the products and services of over 25 global technology suppliers
- We have ensured that the biggest and, most complex, single infrastructure project in Europe is security accredited for the UK's Ministry of Defence

Our Protective Monitoring service, also referred to as Security Incident and Event Monitoring (SIEM), collects events and logs from a wide variety of network devices, host systems, endpoint systems and applications or software services, normalising and aggregating the data. It provides:

- Intrusion protection service
- Log and secure log management services
- Firewall management
- Security messaging services
- Anti-DoS (Anti-Denial of Service)

Our cyber security specialists use a combination of manual techniques and automated tools to continuously monitor and analyse security events and logs, 24 hours a day. They alert our client to significant security events and, if necessary, initiate the incident management process. They track high severity alerts throughout the process and proactively tune the log and event collection to ensure only the most important events are reported.

CGI's Protective Monitoring service is provided using a scalable, flexible per-device pricing approach. Pricing is based on a client's specific requirements ranging from simple end-point nodes to the most complex, for example, web application firewalls. We can provide the most appropriate service for your requirement by tailoring the mix of devices to you.

Our service enables government and commercial organisations to meet CESG's Good Practice Guide Number 13 (GPG 13) for Protective Monitoring. Although, GPG 13 is targeted at UK government organisations, industry is facing increasing regulation to ensure all commercial organisations are properly protected, for example, those in the critical national infrastructure.

Many clients want a deeper analysis of the cyber threat to their organisation provided by our Advanced Threat Investigation service. Building on the protective monitoring, it identifies new, sophisticated attacks based on the latest threat information in order to allow the deployment of countermeasures.

WHY CGI?

We can provide the capability to protect your organisation around the world. CGI has ten Security Operating Centres providing protective monitoring services and handling more than 74 million cyber events every day.

Our service works a 24 hours by seven day operation with a fail-over site in place. This enables near-constant monitoring of your network to detect intrusions whenever they occur for immediate action. Over hundred clients across the world are supported by CGI cyber security managed services.

Our solutions protect against 43 million sophisticated cyber attack incidents on military and intelligence networks daily. We deploy knowledge held corporately on these engagements to our Protective Monitoring service.

For 27 years we have operated a commercial evaluation facility and regularly test the products and services of over 25 global technology suppliers.

For over 35 years, we have helped secure government and commercial clients and now have over 1,400 security professionals, sharing expertise, the latest research, knowledge, capabilities and solutions.

We offer the full range of support from consultancy, secure solutions to services such as Protective Monitoring and Advanced Threat Investigation.