

Advanced Threat Investigation

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

A cyber attacker can strike at any time or place in your organisation or within your supply chain. The attacks are constantly evolving and using new techniques, altering the way they infiltrate corporate networks. Protective Monitoring services can only detect known threats and alert you to network intrusions after they have happened. Criminals are often inside an organisation's network, undetected, for many months.

So, leading organisations also collect information on their network activity to forensically establish the kinds of threats they are facing and to predict likely sources of attack and develop mitigation strategies. Highly skilled analysts are needed for this threat analysis and the demand and cost of these scarce skills is rising sharply. Being up-to-date with the latest forensic investigation techniques to stay ahead of the cyber attackers is also a huge challenge.

Clients are asking questions such as:

"How do I know the attackers are not already in my network?"

"Does my protective monitoring service detect insider cyber theft?"

"Do I conduct timely and effective forensic examinations for signs of compromise and illegal activity?"

OUR ADVANCED CYBER THREAT INVESTIGATION SERVICE

Our Advanced Threat Investigation service is provided from our Cyber Centre by our highly skilled and experienced cyber security analysts. They review the latest cyber threat information from multiple sources. Using automated tools and expert analysis, they detect, investigate and respond to sophisticated advanced threats to protect an organisation.

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 Advanced Threat Investigation (ATI) service provides specialist threat based analytics services to augment traditional Protective Monitoring activities such as those provided by our ten Security Operations Centres (SOCs).

We can provide ATI as an easy to implement extension to your existing Protective Monitoring capability or as a separate standalone capability.



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
- Over hundred clients across the world are supported by CGI's cyber security managed services
- 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
- We are reviewing the cyber security preparedness of an important element of the UK energy industry
- 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
- We are one of the founding members of the CESG CHECK scheme which ensures our penetration testing is within UK government guidelines
- 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

We provide a comprehensive set of analytic capabilities that can be scaled to the type of organisation and the threats faced. Our ATI service draws on multiple information sources, tools and security systems to provide a combination of automated analysis and expert insight to detect and respond to advanced network threats. The service allows you to:

- Analyse and track threats to your organisation
- Monitor a range of network and endpoint systems, through volume analytics and skilled manual analysis
- Identify, analyse and trace advanced malware activity
- Keep up-to-date with the increasing sophistication of cyber threats by providing access to in-depth information and security expertise
- Draw on lessons learned from threats impacting government and commercial organisations to provide early warning on new threats
- Continue to operate by monitoring for sophisticated attempts to breach your network and thus reduce the impact of a cyber attack
- Digital forensics of incidents, clean-up and containment

Through our Protective Monitoring service we work closely with security organisations to help defend against intrusion attempts against our client's networks. The ATI service goes a step further and provides investigative capabilities before and after an attack has occurred. We provide proactive support against cyber threats by combining techniques such as data mining, network behavioral analysis, malware and packet analysis with information collected through digital forensics and threat intelligence monitoring.

Our analysts have a deep understanding of the kinds of threats, and network and system vulnerabilities, that organisations are facing, obtained from open and community sources as well as CGI's own research and experience. This knowledge is continually refreshed to protect against the very latest types of cyber attacks.

Our ATI service is provided as an extension of our Protective Monitoring service. We can set up the service within a few weeks, without disruption to existing activity. We can find the advanced attacks that get past standard protection methods. So, you can be confident that your organisation is protected from cyber attack.

WHY CGI?

We can provide the deep expertise to keep you ahead of the attackers and protect your organisation. For over 35 years, we have helped secure government and commercial clients and delivered some of the most complex technology projects and services. For 27 years we have operated a commercial evaluation facility and regularly test the products and services of over 25 global technology suppliers.

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

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

ABOUT CGI

With over 68,000 professionals in 40 countries, CGI fosters local accountability for client success while bringing global delivery capabilities to clients' front doors.

Founded in 1976, CGI applies a disciplined delivery approach that has achieved an industry-leading track record of on-time, on-budget projects.

CGI has a global team of cyber security experts, who work with governments and commercial clients, ensuring their business critical systems and services are effective and secure.

CGI is one of the few providers worldwide with three accredited security certification facilities - located in the UK, Canada and the U.S. Our ten Security Operations Centres continuously identify and deploy the best solutions to maintain a state-of-the-art infrastructure, handling over 74 million cyber events a day.

Our high-quality business consulting, systems integration and outsourcing services help clients leverage current investments while adopting new technology and business strategies that achieve top and bottom line results.

As a demonstration of our commitment, our average client satisfaction score for the past 10 years has measured consistently higher than 9 out of 10.

For more information about CGI, visit : www.cgi-group.co.uk/cybersecurity or email us at cybersecurity@cgi.com

CODE: 49 0914

