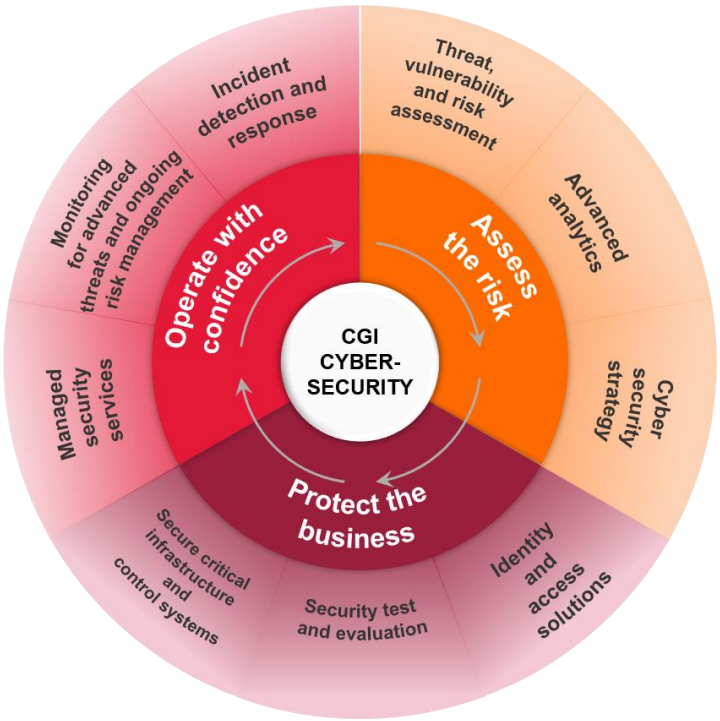
CYBERSECURITY

Penetration Testing Services

Experience the commitment®

Organizations depend on business and IT systems to operate effectively and competitively in this digital age. These systems are frequently updated and even a small change can introduce new vulnerabilities

At the same time, IoT devices such as cameras, sensors and PLCs are often left unattended and unpatched. While organizations are investing significant effort and money to ensure that the systems run efficiently with the necessary security controls, they do not always test to check if the security controls are implemented correctly or are sufficient. Left to chance, vulnerabilities will only be discovered once security has been breached, leaving the organization open to potential regulatory fines, financial loss, reputational damage or theft of business critical information or intellectual property.



OUR APPROACH

CGI understands the need to be agile, introduce new systems, technologies and new ways of working to be competitive and improve efficiency. With the growing utilization of IoT (Internet of Things) devices and cloudification of services, it is particularly crucial that network devices comply with best practices regarding security controls, data transport and IT governance.

A CYBERSECURITY PARTNER YOU CAN TRUST

- We have over 1700 cybersecurity experts providing in-depth knowledge and best practices.
- We design mission-critical solutions to some of the world's most demanding clients. Among these the European SatNav system, Galileo and the UK Police National Database.
- Over a hundred clients across the world are supported by CGI's cybersecurity managed services.
- We handle 75 million cyberattacks on military and intelligence installations on a daily basis.
- Within the insurance sector, we provide AON with risk-analysis and cyber insurance claims.
- 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.
- Every new Volvo car includes a unique authentication certificate provided by us that enables secure access to Volvo online services.

cgi.dk

CGI's penetration testing services (sometimes referred to as "ethical hacking") maximizes risk reduction, while minimizing any disruption to the business. We evaluate systems by subjecting them to external Internet attacks and/or by considering insider threats. Using our penetration testing services regularly helps our clients stay one step ahead of potential attackers, enabling their IT systems to grow with their business, while keeping the enterprise secure. Our approach to penetration testing provides a thorough, quality service with the flexibility necessary to test a wide range of IT systems.

The primary objectives of our penetration testing services are:

- To demonstrate, to the highest level of assurance possible, that a system or device is either susceptible or not susceptible to particular security weaknesses
- To provide clear recommendations for vulnerability mitigation that are straightforward to implement and tailored to the required functionality of the system being tested
- To help our clients ensure that their IT systems and IoT devices are not the weakest link in their security infrastructure

CGI EXPERTISE

Our team holds qualifications from CREST and Offensive Security, for network, web application and IoT testing. We offer seven broad areas of testing, which are normally combined to provide the optimal balance of testing.

- **Internal testing** is carried out while connected directly or close to the network under test, on either 'full knowledge' or 'zero knowledge' engagements. The purpose is to demonstrate that an IT system has been configured in a manner that makes it as secure as possible.
- **Internet testing** takes a "zero knowledge" (black box) approach and is often used to understand what target information attackers can discover from the Internet and other public domain resources.
- **Remote testing** is conducted from external networks to which the IT system is connected. There is generally some sort of perimeter security, for example, a firewall or filtering router that is designed to limit the access available from a given external network to the IT system under test.
- **Web application testing** ensures that an application has been configured securely so that attackers cannot gain unauthorized access to it or its data; users cannot access data for which they are not authorized; and there are no vulnerabilities that users can leverage to gain access to services outside of their restricted operating environment.
- **Wireless testing** is carried out to discover and identify the perimeter of a client's wireless network in order to pinpoint from where potential attacks could be undertaken.
- **Product testing** aims to ensure that applications developed in-house and by third-parties are aligned with current best security practices.

ABOUT CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. Operating in hundreds of locations across the globe, CGI delivers an end-to-end portfolio of capabilities, from IT and business consulting to systems integration, outsourcing services and intellectual property solutions. CGI works with clients through a local relationship model complemented by a global delivery network to help clients digitally transform their organizations and accelerate results.

Can your company's IT systems resist a hacker attack? Do you want to know it?

At CGI, we have some of the best Ethical Hackers you will ever meet.

With the highest certification available, they know the hacker's methods and tools - and use them only for your benefit.

The test consists of a pre-agreed attack on your application.

Afterwards you receive a personal feedback and a report, so you get an idea of your company's vulnerability.

Get in touch and learn more.

For more information about CGI, visit cgi.dk, or email us at cgi.dk@cgi.com.

cgi.dk/cybersecurity