CGI's Analyst as a Service

CGI's Analyst as a Service is the deployment of our experts to augment your Security Operations Centre.

Analyst as a Service (AaaS). We provide experienced and highly skilled cyber security analysts, either working alongside your existing Security Operations Centre (SOC) team, or to step in and deliver a fully managed service utilising your existing technology and infrastructure.

Why you need to take action

Cyber-attacks are on the rise. You want to ensure your organisation delivers the highest level of security protection around the clock, but you may not have the resources to do this alone or struggling to recruit in a competitive labour market.

CGI understand that many businesses aspire to run a SOC, but they are often restricted by the costs of finding the experts necessary to protect their business. You are looking for industry-leading external support to boost your existing security infrastructure.

How CGI's AaaS works

Our Analyst As a Service was established in 2017 to address the need of augmenting Security Operations Team.

Our resource pool of highly experienced analysts can be leveraged into your own security operations either full time, evenings and weekends or via an 8x5 provision.

Our analysts maintain knowledge of a large variety of security tools including all of the major SIEM vendors such as Splunk, ArcSight, Qradar, LogPoint, MS Sentinel, AWS Security Hub amongst others. This means with only a short knowledge transfer process our analysts can start analysing and responding to alerts in rapid time.

We work with your business in a supporting role. Our experts enable your team to operate at a much higher level with the added advantage of cross training. We share our extensive experience and enrich your team's capabilities without the need to replace technology, implement new systems or be lumbered with hidden costs. If you decide the service is no longer required, then hand over is simple with no need to decommission systems and avoid costly exit clauses.

Benefits

- Access all the benefits of a larger security team without the additional cost of recruitment.
- Maximise the most of your security stack and resourcing investments.
- Close the operational gap with swift deployment of resources.
- Access cover when you need it – We can augment your team to provide coverage outside of core business hours with our 24x7 service.
- Relieve the burden of increased workload and increasing number of alerts on your team.
- Reduce your recruitment overheads in a vibrant industry where retention of staff is often incredibly challenging.

What connectivity will AaaS require?

AaaS will require secure connectivity into your SIEM. Our experienced project and engineering teams will work with you to organise this as quickly as possible while adhering to all of our strict security controls. Once connected, we will acquaint ourselves with, and start collating your network, logs and rules. Following this, we can complete the onboarding of our analysts and recommend any improvements to your existing monitoring tools.

We will leverage our SOAR technology platform to ensure you benefit from our efficient operations. Another important element of AaaS is that we can work using either on-premise or cloud native tools:

On-Premise	Cloud
Monitoring of alerts using client's own analytics and alerting tools. Reduces cost by leveraging existing tools and speeds up the service onboarding as there are no complex SIEM tools to configure within your environment.	Monitoring of client's AWS GuardDuty/Security Hub or Microsoft Azure Security Centre/Sentinel alerts using built-in cloud security analytics and alerting tools. Reduces cost by leveraging existing cloud tools and speeds up the service onboarding as there are no complex SIEM tools to configure within your environment.

How could AaaS work alongside our own SOC?

A number of our clients work in tandem with our cyber team when deploying AaaS. For example, an education sector partner with an internal SOC has opted to use our out of hours team for cover on a weekday basis. Others prefer weekend cover, while some opt for 24x7x365 cover.

Choose a service level that suits you

Our service is exceptionally flexible when it comes to providing the level of operational cover you need, and our operational security team will assist in evaluating the best option for your organisation.

An initial consultation with your CGI cyber representative is critical to get the requirements in-line with your company's expectations. Typically, these consultations bring up questions around:

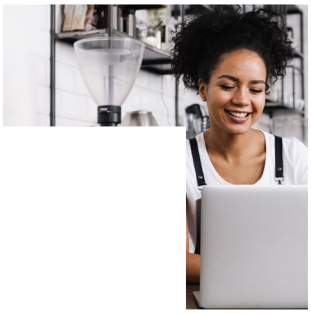
- How could AaaS complement our existing SOC service?
- What is best for our business, weekend cover or an out of hours option?
- Could we benefit from a full 24x7x365 service given the economies of scale CGI could bring?
- I have a set budget, can this be taken into consideration when assessing the service levels?

Whichever option is selected you will receive alerts via email, an incident ticket, a monthly compliance report and an assigned Service Delivery Manager.

Our AaaS can also align to other services provided by our cyber team:

- Cyber Threat Intelligence
- Phishing Defence Service
- Digital Forensics & Incident Response
- Vulnerability Management

We can provide further information about each of the services above upon enquiry.



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 82,000 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