Cyber Adversary Simulation (CyAS): scheme documents now available

Our view of good cyber adversary simulation – and how assured providers can deliver it.

Cyber adversary simulation is one of the most effective ways for organisations to understand how they would fare against a capable cyber attacker. Yet, the quality of services available across the market can vary significantly. To help buyers understand what 'good' looks like, we have published new NCSC guidance based on our experience delivering and overseeing adversary simulation engagements.

Alongside this, as the launch of our new assured Cyber Adversary Simulation (CyAS) scheme draws nearer, we've also published the first set of scheme documents. These explain what we expect of companies wanting to become NCSC-assured providers.

Why adversary simulation matters

Adversary simulation assesses an organisation's defences by safely and systematically testing its ability to prevent, detect and respond to simulated cyber attacks. It is particularly suitable for organisations with mature cyber security processes and technologies, allowing them to put their defences through their paces before they are needed for real.

Adversary simulation should **not,** however, be a tick-box exercise with pass/fail outcomes. A carefully scoped adversary simulation engagement will help organisations understand where their defences are working, where they are not, and what needs to improve. It will also evaluate whether an organisation can identify threats early, triage them quickly and appropriately, and escalate where necessary.

The new guidance also explains how engagements should be planned, controlled, delivered, and reported so that it gives *meaningful* evidence about your cyber resilience while managing the risks of testing live services and sensitive systems.

About the CyAS Scheme

Alongside the guidance, we have shared the first CyAS scheme documents, including the Scheme Standard and the Working Practices Document. These documents give an early and transparent view of the standard we will use to assess applicants, including expectations on companies, key role holders, technical delivery and reporting. As a result, buyers will have a transparent and consistent benchmark for assessing providers, helping them make more informed procurement decisions and giving them greater confidence in the quality of NCSC-assured services.

We have developed the CyAS scheme in partnership with cyber oversight bodies, including regulators and government policy organisations responsible for understanding cyber resilience in their sectors. This collaboration has helped us create a common and widely applicable core standard, while allowing potential customer organisations to define additional, specific requirements where needed.

In contrast to some similar standard industry schemes, our CyAS approach is capability-led. We are **not** expecting providers to simply replay a fixed script of known attacker behaviours. Rather, NCSC-assured CyAS companies will apply an adversarial mindset, use continuous and tailored reconnaissance, and develop bespoke approaches to the objectives agreed with their customer.

Next steps

When the CyAS scheme formally launches in November 2026, buyers will be able to choose from providers assured against the NCSC's CyAS standard. However, the CyAS scheme is currently a 'minimum viable product'; an early version which reflects the scheme as it stands today. We expect to refine the scheme as we learn from early delivery and feedback from partners, buyers and providers.

We'll continue to update the scheme as it develops and will publish more information later this year about the launch for buyers and future opportunities for providers. In the meantime, we encourage organisations to read the new guidance and the CyAS Scheme documents, and use them as the basis for your own work in this area.

As always, we welcome comments and feedback.

Catherine H, Head of Assured Professional Services Schemes

WRITTEN BY

Catherine H

Head of Assured Professional Services Schemes, Industry Assurance, NCSC

PUBLISHED

17 September 2026

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

PART OF BLOG

Events and initiatives NCSC publications