Introducing Active Cyber Defence 2.0

ACD 2.0 aims to build the next generation of services in partnership with industry and academia.

Ollie Whitehouse, Jonathon Ellison

As the National Cyber Security Centre, we aim to provide a cohesive suite of services that help organisations protect themselves against cyber threats. Some of these services are directly provided by us, where we are uniquely placed to do so, while others are delivered by industry partners with NCSC assurance. We constantly review the services we deliver and look to divest to industry where and when appropriate. Next month, you will hear more about our direction of travel for those services delivered through industry.

Active Cyber Defence (ACD) has gained widespread recognition and been adopted as a concept by many countries. Why? Because it effectively increases national cyber resilience on a large scale, while imposing significant costs on adversaries.

> *Active Cyber Defence (ACD) seeks to reduce the harm from commodity cyber attacks by providing tools and services that protect from a range of attacks.*

This protection comes in many forms: from addressing security vulnerability, to actively detecting and disrupting attacks.

Most of the current services began life back in 2017. While they have evolved since then, the range of services on offer has been broadly consistent. Meanwhile, the cyber capabilities of those we serve – and the set of capabilities on offer from the private sector – have evolved. This defensive change has combined with an evolution in the threat.

It's important that the UK's National Cyber Security Centre focuses its efforts where we can make a uniquely valuable contribution – where we see a gap in the commercial market, or where being part of GCHQ presents a unique opportunity to drive up resilience at scale. In light of this changing context, and using our experience from providing the existing ACD services, we are assessing

new delivery models and partners and are seeking to build a next generation suite of services under ACD 2.0.

Given the modern threat, the contemporary internet and a host of other factors, what should we be delivering? Where is the cyber defence edge to be had? Where can we add unique value? Having mainly targeted the original ACD services at the public sector, is it time to broaden our reach?

In pursuit of this goal, we have set these principles for ACD 2.0:

- The NCSC will only deliver solutions where the market is not able to – whether that's due to our unique position in government, scaling abilities, capabilities or authorities
- The NCSC will look to divest most of our new successful services within 3 years – to another part of government or the private sector to run on an enduring basis

We want ACD 2.0 to be a partnership; across the NCSC, across the cyber security community in government, and crucially also with industry and academia. Combined with our unique organisation, we can have a disproportionate impact on cyber resilience at scale.

Get involved - how to work with us

As we embark on ACD 2.0, our first step is to look at our attack surface management suite - currently that's Web Check, Mail Check and Early Warning.

We've learned a lot from running these services and are keen to build on that by running experiments alongside industry providers. We have experiments we want to run, but we're also keen to hear from you if you have ideas.

Our hypothesis remains that helping organisations know and reduce their attack surface and related vulnerability is one of the most efficient ways to drive up external resilience.

If you have an attack surface management product, or ideas for other experiments we should run in future, and would like to work with the NCSC, please get in touch with us.

Ollie Whitehouse, Chief Technology Officer (CTO), NCSC
Jonathon Ellison, NCSC Director of National Resilience

WRITTEN BY

Ollie Whitehouse
Chief Technology Officer (CTO), NCSC

WRITTEN BY

Jonathon Ellison
NCSC Director of National Resilience

PUBLISHED

2 August 2024

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals

PART OF BLOG

Events and initiatives