Head Office
Orion House (HQ)
Stone Business Park
Stone
Staffordshire, ST15 0LT
+44 (0)1785 827000

Beacon House
Stone Business Park
Stone
Staffordshire, ST15 0NN
+44 (0)1785 827000

1414 Charlton Court
Gloucester Business Park
Gloucester
Gloucestershire, GL3 4AE
+44 (0)1452 650000

Vulcan House
Calleva Park
Aldermaston
Reading, RG7 8PA
+44 (0)118 981 0673

Kinniside Suite,
Innovation Centre
Westlakes Science & Technology Park
Whitehaven
Cumbria, CA24 3TP
+44 (0)1946 517450

Systems House
Rosebank
The Alba Campus
Livingston
West Lothian
Edinburgh, EH54 7EG
+44 (0)1785 827000

Follow us on LinkedIn and Twitter

www.capula.co.uk

capula
an Imtech company

Cyber Security Offerings

Protecting critical assets from cyber threats

capula
an Imtech company

Protecting critical assets from cyber threats

Today's industrial assets are increasingly reliant on network-connected digital control technology. As those assets become more integrated and interconnected, they also become more vulnerable. Businesses need high levels of availability from their mission-critical industrial platforms. That makes them high value targets for cyber-criminal activity, and the threat environment is evolving rapidly.

With a demonstrable track record and over four decades of experience in the development and support of Industrial Control Systems (ICS) for customers in security-critical sectors, Capula is ideally positioned to help your organisation assess, mitigate and manage the vulnerabilities in its digital infrastructure.

As independent specialists, we have developed strong working partnerships with the UK's leading security organisations. These partnerships enable us to deploy the most sophisticated and proven security assessment tools on the market. We combine those resources with our advanced domain knowledge and expertise to provide you with a greater understanding of the level of maturity of your most critical assets.

We develop high-level action plans with defined metrics that enable you to work towards your desired maturity level. This forms the basis for discussion with your key business stakeholders, helping them to understand the present maturity level of your systems, and to plan for the future at a pace that helps you keep ahead of potential cyber threats.

By investing in Capula technologies and care agreements, you can be sure that the reliability and security of your systems is given the highest priority.

Our services include:

Business maturity audits

In the industrial cyber-security space, the risks are changing all the time, as companies extend, adapt and improve their systems, as new vulnerabilities are identified and as threat strategies evolve. Effective management of security is not one-off exercise. It should form part of a 'business as usual' process to ensure an organisation's overall risk management strategy is clear and well defined.

Using proven assessment tools, our audit identifies the maturity level of individual or combined elements we qualify as 'defensible units' within the business, based on pre-defined controls using a wide range of security standards including ISO 27001, IEC 62443, NIST SP800-53 - Security Controls and many others.

Security consultancy - external assessment

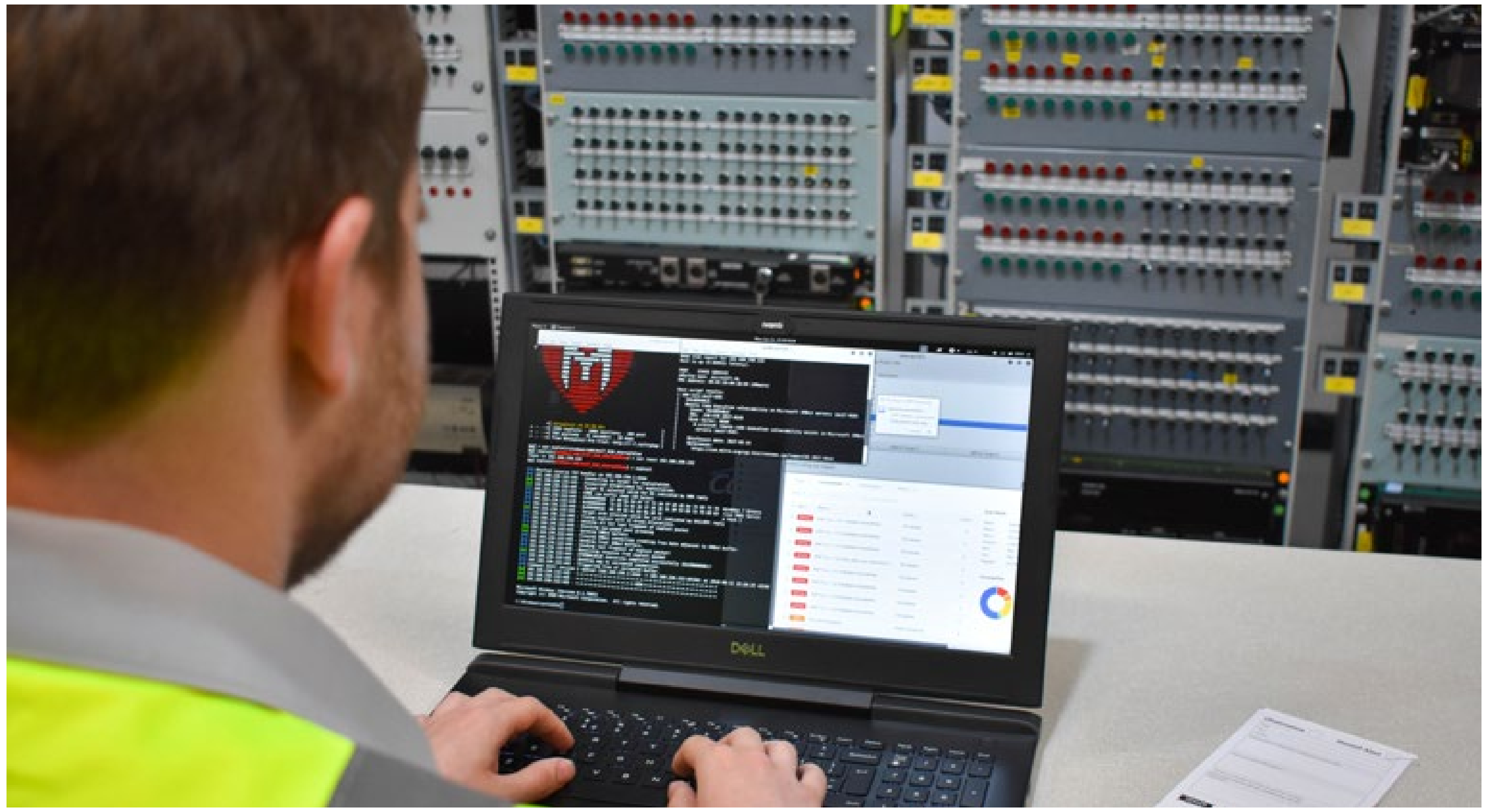
We can conduct a full interactive test that will scan websites, URLs or systems hosted by external third party providers. For all the resources in scope, a baseline assessment is undertaken to reveal information that may be visible to unauthorised actors. This assessment provides an early warning of data breaches that may jeopardise your GDPR[1] and NIS[2] compliance.

Our specialist tools can also identify hidden weaknesses in internet-connected systems that may provide opportunities for criminal access. Additionally, we can evaluate weaknesses in personnel by testing end-user awareness of email-borne threats. We can also undertake searches of the dark web for critical business data which may have been leaked, providing your organisation with early warning alerts similar to a perimeter burglar alarm to further assist with regulatory compliance.

Our enhanced scanning offering uses the highest performance scanning tools, with the same technology that tests the most security-sensitive websites used by the payment card industry.

Security consultancy - on-site security assessment

We can undertake full IT health assessments on your internal infrastructure. Working with your IT professionals, we test more aspects of your infrastructure and provide more detailed, actionable recommendations than is possible with "blind" external assessment approaches. The assessment will review your wired and wireless network infrastructure, your IT assets, and provide a report on any weaknesses identified. It will audit the effectiveness of your software patch management, the strength of passwords and of perimeter defences against malware infection.



Full penetration test

This assessment can be operated as a 'red team' test where nothing is provided, and we will detail what we can find as an outsider. We can undertake a full penetration test on all your systems, networks, websites or web applications. Using trained and certified ethical hackers or 'Tiger' team members, you can be assured that the items in scope will be rigorously tested for vulnerabilities.

We can further undertake a full review of your perimeter defences, try to gain access to your site as an adversary and use detailed social engineering skills to obtain access to restricted areas. If required, our teams can pose as trusted insiders, contacting staff for information or professing to be support agents to gain access to hardware as part of an ongoing maintenance agreement. Perhaps you are interested to know what happens to USB devices that are found on your premises and who may be curious enough to plug them in?

Cyber Essentials & Cyber Essentials Plus

We can help your organisation, system or defined process become certified for Cyber Essentials or Cyber Essentials Plus, a requirement for any organisation bidding for UK government contracts that involve the handling of sensitive information. Our trained assessors and security consultants can undertake pre assessment work to ensure that you are ready for your Cyber Essentials certification, or, if you feel that you are already compliant, we can process your assessment against the current framework. This government-backed scheme provides assurance to your stakeholders and customers that you have robust process in place and are fully committed to the ongoing management of cyber-security issues.

Offline patch management services

Our offline patch management service is tailored according to your unique requirements. It may include a full system analysis to confirm all systems are operational, functional and fully patched. Full operating system patching and reporting may be included, whether required for a fully connected, partially connected or an isolated system. Anti-malware signature updates for a chosen vendor can also be implemented, as well as USB port control and 'sheep dip' validations that check content ensuring only trusted data is imported into a secure engineering environment.

How Capula can help you

Capula has been designing, installing and supporting ICS running on Windows, UNIX, Linux and derivatives for over 40 years. Our engineers are skilled in supporting computer hardware from modern devices to legacy systems. Our approach is to review the risks and assess the impact before making changes to a critical running system which may compromise availability. We offer a bespoke approach to dealing with the latest challenges, to ensure that systems are fully patched, secured and that processes are not jeopardised during security maintenance cycles.

We offer this package as part of a one off consultation, works programme or part of a service contract. Contact us on supportadmin@capula.co.uk, or call 01785 827300 to find out more.

For more information about protecting your ICS download our Tip Sheet.

[1] General Data Protection Regulation
[2] Network and Information Systems Regulations 2018