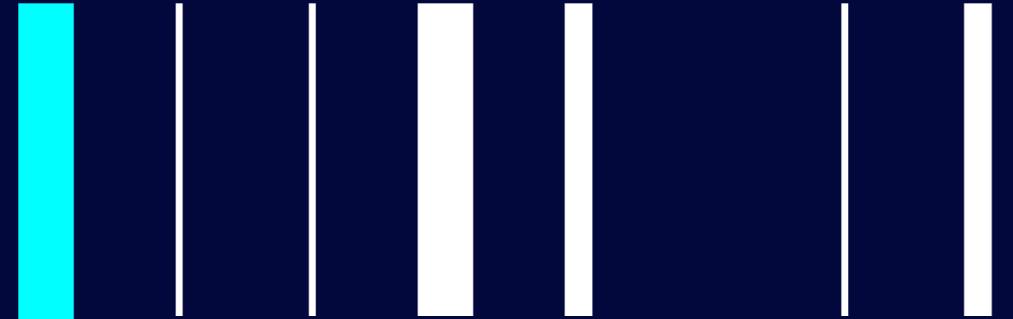
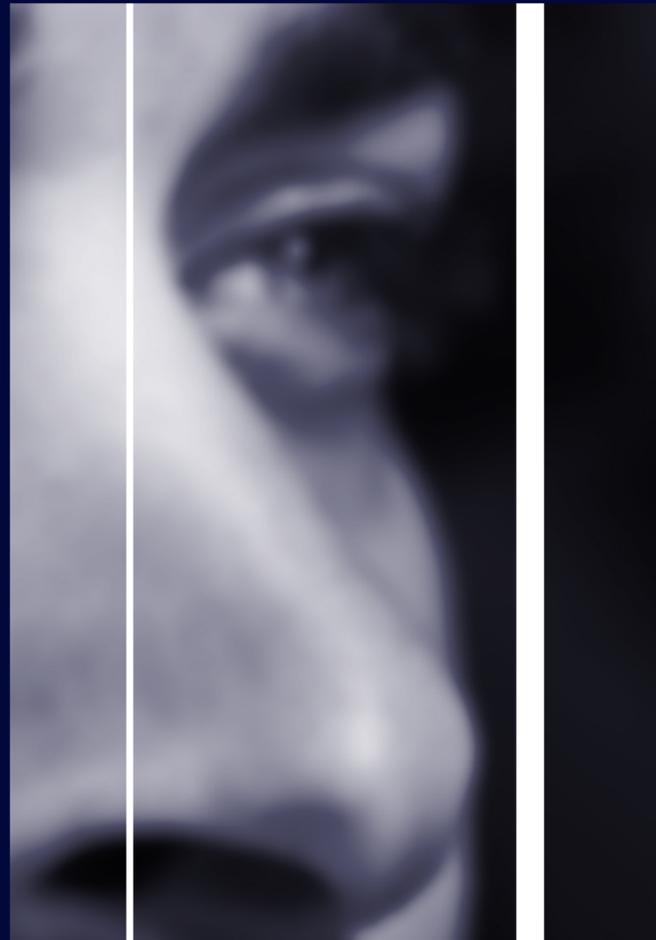
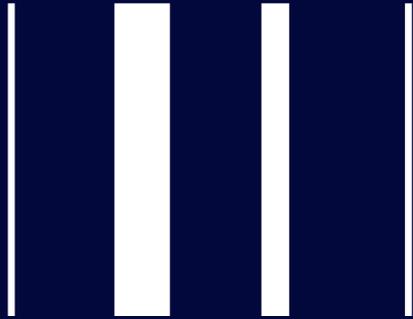
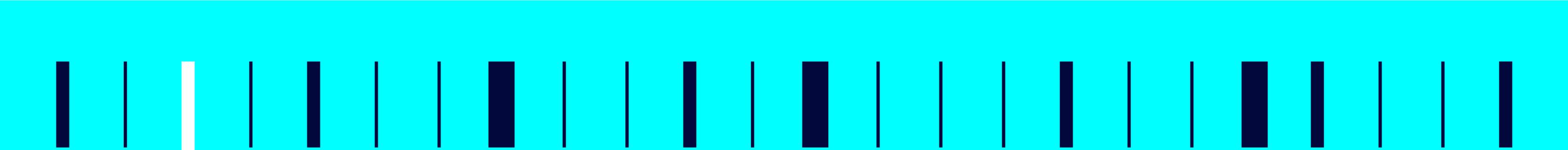


Capita



Cyber
Security
ebook



Contents

- 03 We're all human >**
- 11 Capita Security Testing and Consultancy Services >**
- 13 Why Capita for security testing? >**
- 15 Capita Security Technology Management >**
- 18 Capita Managed Security Services >**
- 21 How does it work? >**
- 22 Why Capita for MSS? >**
- 23 How we make SIEMs cost effective >**

We're all human

Recognising our vulnerability is what makes our cyber security stronger.

Cyber attacks work for one very good reason. People. We are the weak link in the security chain. We create short passwords, allow ourselves to get tricked by scammers and hackers, and we expect experts to take care of our cyber security – but sometimes overlook that they're human too. Hackers target security professionals just as much as users, and it's this knowledge which helps us to keep organisations safe.



Strong cyber security creates secure businesses

Cyber security is no longer a purely defensive mechanism. It's a key component of the digital transformation process that is crucial for enterprises to succeed.

With a strong cyber security strategy based on people, processes and technology, organisations can realise the full benefits of adopting the cloud, enabling their teams to work and collaborate remotely, and engaging securely and safely with customers online.

Cyber security can help businesses mitigate risk, identify weaknesses, contain threats, support compliance and ultimately have a positive impact on the bottom line. It is more than peace of mind; it is a strategic ethos vital in progressing any modern-day business towards achieving its long-term goals.

Keeping your organisation safe is increasingly challenging

Cyber crime now costs UK businesses more than £30bn per year, with some global estimates as high as £4.9 trillion by the early 2020s. In 2018, PwC estimated that the annual average cost to UK firms that fell victim to a cyber attack was £857,000 and rising.

And it's not just the immediate impact of a breach that organisations have to worry about. Under GDPR legislation, fines can be significantly larger than they used to be, and the broader impact on brand and reputation is often even more damaging. To combat these potential costs, cyber security tech spending has seen a huge upsurge in recent years, which is expected to continue well into the next decade. However, organisations frequently struggle to see a return on this investment as most of it goes on technology, which is only one part of the problem.

With so many risks and challenges to contend with, it's easy to see why internal IT teams often feel overwhelmed by the responsibility of keeping a business cyber secure. Especially when they don't have the right people, expertise, governance or processes to cope with ever-increasing cyber security threats and risks. Or struggle to get adequate financing and funding, and are expected to do far more with a lot less.

In that situation, even if the right technology is in place, how can an organisation respond to the information, reports and alerts that their tech provides if they don't know what to do with it? A firewall log can tell you what it blocked, but will never tell you what got through.

So, the people and process risks are as significant as the technical ones, and sometimes even harder to fix. That's why a fresh approach is needed.

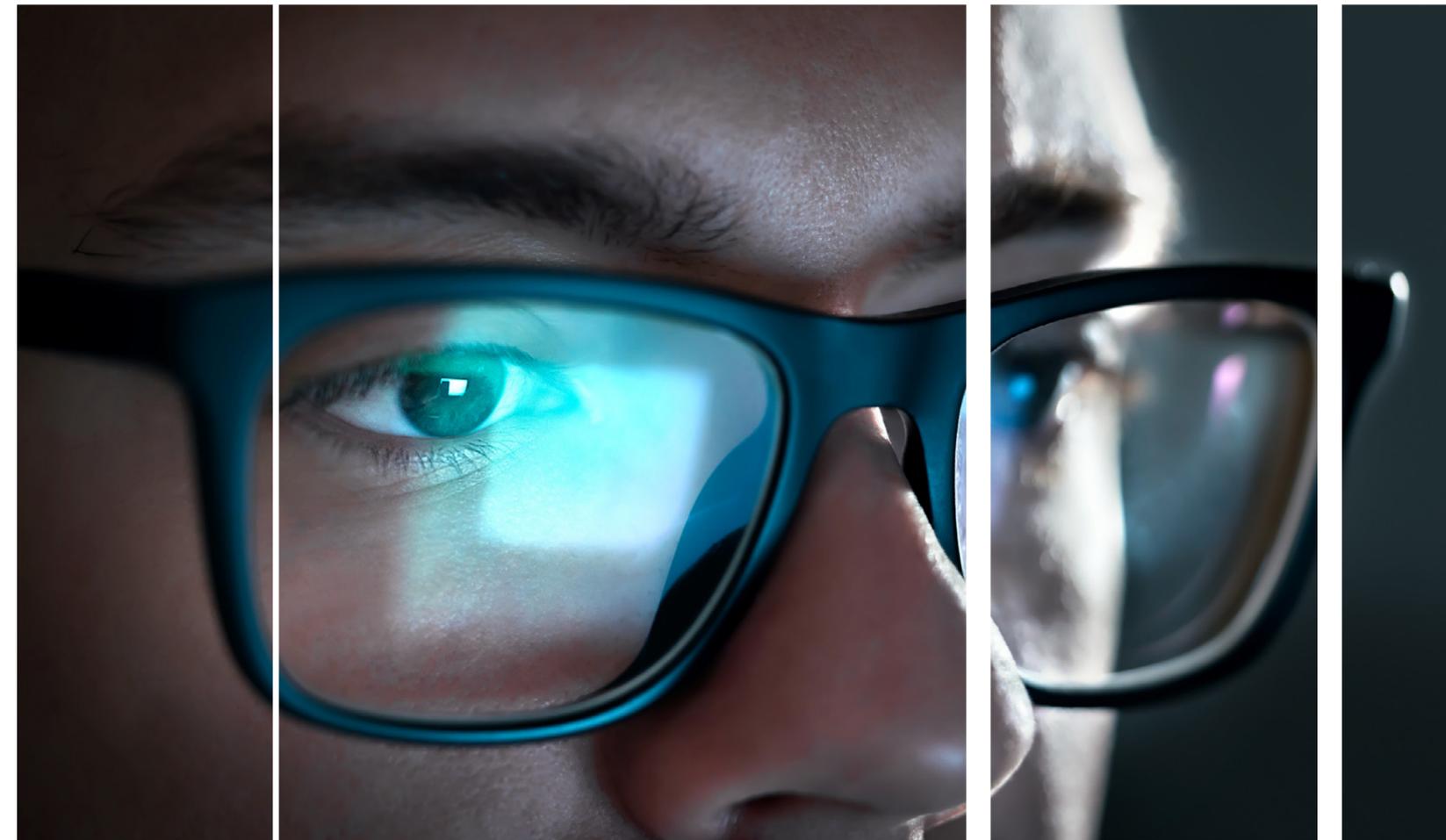
We recognise that people are one of the biggest threats, which is why we put as much emphasis on understanding them as we do processes and technology.

A human-focused cyber security service

When enterprises fail to achieve real value from their cyber security technology investments, it's usually because they don't have the people, technology and processes in place.

Capita is the ideal partner to provide a holistic security solution that addresses both technology and people, with the advisory capability to ensure that the solution is properly put together to meet each customer's specific needs: we ensure our customers can protect their network, staff and customer data online, and significantly reduce the threat posed by cyber attacks.

We also help our customers plan for unexpected digital or physical events, by helping them spot the gaps created by human vulnerability and giving them the resilience they need to keep their businesses going and to recover rapidly.



Why Capita for Cyber Security?

We can bring your teams up to speed

We recognise that security experts are human. Sometimes they are forced to over-rely on technology like anti-malware software and standard endpoint protection. That means we look closer for the gaps that threats can slip through. We also look after thousands of business processes for hundreds of organisations across the public and private sectors, so really understand where those gaps are likely to be.

We offer an exhaustive testing capability

We support our cyber security portfolio with a wide range of penetration testing, software testing, compliance, governance and threat analysis services that can help you understand the threats specific to your organisation and protect you against them.

We work quickly

We provide the right solutions to reduce risk, in line with our client's agenda to ensure faster, tighter fixes. We don't supply what you don't need! Our teams are exceptionally experienced at searching for security gaps, and work with market-leading tools designed and optimised to identify them rapidly.



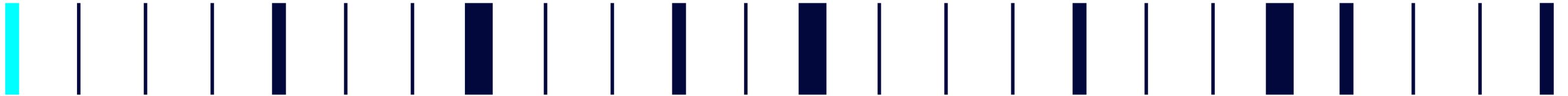
We help you to address the key questions relating to security that all organisations face these days. Issues such as:

1 Am I secure?

Given human nature, nothing can ever be entirely secure. Sometimes, excessive security can even inhibit business efficiency. But too many organisations are still in the dark about where they really stand.

Capita can help you ensure that you understand your current security posture, and whether it is consistent with your overall appetite for risk as an organisation.

We can provide guidance on simple baselines like National Cyber Security Centre (NCSC) Cyber Essentials and more demanding frameworks like NIST and ISO27001. We can also provide more specific compliance guidance in areas like GDPR or PCI-DSS if needed.



2 Enabling the workforce

Employees need to be trusted to do their jobs. But the fact that most accidents and data breaches are caused by human error means that, as well as being your greatest assets, your people are also your greatest source of risk.

We'll help to train your team, and show you how embracing new trends like cloud apps and BYOD (Bring Your Own Device) can protect them from phishing, fake websites and malware attacks that compromise their devices and user accounts.

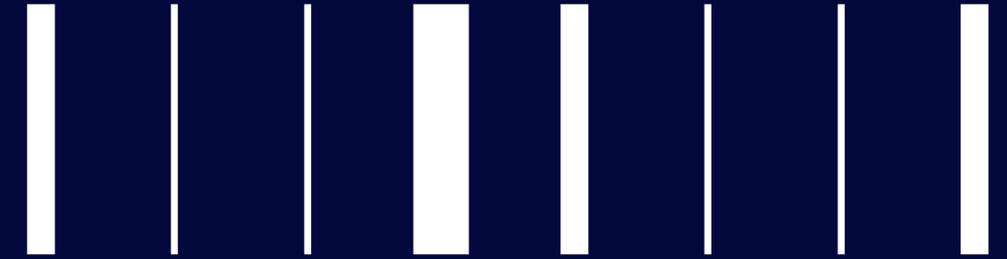
3 Protecting Key Data Assets

The regime is becoming stricter and more punitive. GDPR can result in significant fines for organisations that do not take adequate measures to protect their customers' personal data. But when assets can reside in the cloud or in a hybrid environment, it can be hard to determine where the perimeter even is, let alone how to secure it.

Our security solutions are designed for a variety of different environments. So whether you're in a cloud, on-premises or hybrid environment, we can help ensure that your data is secure.

Capita can help you understand how to achieve this balance, with a technology-agnostic approach geared to finding the right solutions for your business.

Capita Security Testing and Consultancy Services



Many organisations may be at risk of attack, perhaps unwittingly. Because they lack internal expertise and therefore don't know the strength and maturity of their cyber security estate.

Regular security tests can help reduce external and internal (human error or malicious saboteurs) threats. But they don't supply a full or detailed picture of potential vulnerabilities.

With the biggest source of risk in an organisation being people, assessing the risk they're currently exposed to and determining acceptable levels of risk can be challenging for businesses.

Capita's Security Testing and Consultancy practice work together to deliver a total picture of the cyber security status that organisations need.

We can design a bespoke approach to identifying security needs that fits your business, budgets and levels of security awareness.

We use advanced scanning techniques that combine process assessment and vulnerability identification to give a complete end-to-end view.

We can alternatively apply these techniques independently for faster results.

Our capabilities can be split into three main areas: a) implementation, support and audit using industry best practice standards, b) security testing and technical assessment, and c) threat prevention.

Three steps to the clearest view of your security level

1 Assessing your needs

We offer our capabilities as discrete, stand-alone services, such as Internal Audits and Web Application Penetration Testing, or we can combine them as a powerful integrated solution.

2 Determining your security maturity

Using the industry-recognised Axelos Resilia tool enables us to map security maturity directly to your organisation's IT delivery lifecycle. This means that areas of process vulnerability can be rapidly identified and remediated.

3 Finding your weak spots

We provide a detailed assessment of your network's vulnerability in a number of different ways. These include vulnerability scans to identify general gaps and areas of weakness across a wide estate, or something more targeted like penetration testing and red-team exercises, which validate the protection around more critical assets.

Why Capita for security testing?

We support our cyber security portfolio with a wide range of in-depth professional solutions.

Our services include penetration testing, software testing, compliance, governance and threat analysis. They've been specifically designed to help you understand human vulnerability and the risk that external security threats pose, and to enable you to respond quickly.

We partner with Qualys and other market leading organisations in the cyber security field, enabling us to offer the appropriate technology on an individual basis and embed our solutions in ways that deliver the best results for customers.

We offer fast, quality assessment, enabling our customers to rapidly identify risks and therefore remediate earlier and more effectively.

We provide aligned consultancy and security testing. We use our broad industry experience to add perspective and context to our customers' cyber security issues, and to deliver stronger defences.

What we offer, at a glance

- **Network security**
- **User education and awareness**
- **Malware prevention**
- **Controls on removable media**
- **Secure configuration**
- **The management of user privileges**
- **Incident management**
- **Monitoring**
- **Home and mobile working**

Capita Security Technology Management

Capita has the people, experience and expertise to help ensure you get the most out of your investments in technology in a number of areas.

We can assist with licence management issues, help to install and configure, or even manage the entire lifecycle of the solution, in a broad range of security technology areas.



Cloud security services

With ever-greater reliance on mobile workers and flexible working practices, it's vital that security protections and policy enforcement are consistent across a number of different environments. Capita can ensure that cloud security services blend seamlessly with traditional on-premises solutions.



Cloud and Hybrid Hosting Security

Capita can deploy managed security technology in the cloud, on the customer premises or in our private cloud environment and manage everything centrally with the same robust management tools and processes.

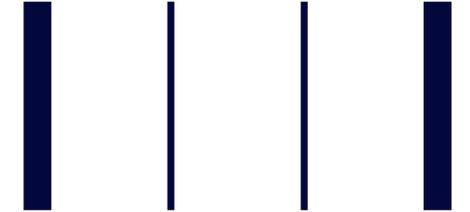
Whatever kind of environment you run, whether cloud-native, hybrid or legacy on-premises, we can provide a flexible, comprehensive solution to encompass your requirements.



Web and email filtering

Malware attached to emails or embedded in websites is still a major threat, and cloud-based proxies have become the de facto standard for addressing these issues.

But moving these services to the cloud does not remove the need for technical management: onboarding, troubleshooting and policy management are all challenges that stay with you when services move to the cloud. Our experienced technical staff can help manage these issues for you and ensure you get the best use and maximum return from these services.





Boundary protection and firewalls

The capabilities of the modern firewall have evolved from simple network/traffic segmentation to the full unified threat management stack, with a number of features that used to be the domain of separate systems like Intrusion Detection/Prevention, Anti-Malware, Web filtering and Sandboxing, now all being delivered from a single device.

It is also possible to run these multi-faceted devices in a range of different environments: as a physical appliance, or as a virtual machine in either a public or private cloud environment.

Capita has the skills and capability to manage a full range of functionality, across all the leading firewall vendors: Checkpoint, Cisco, Palo Alto, Fortinet and others.

Endpoint protection

As businesses adapt to more flexible working practices, securing the endpoint is taking on an ever-greater importance.

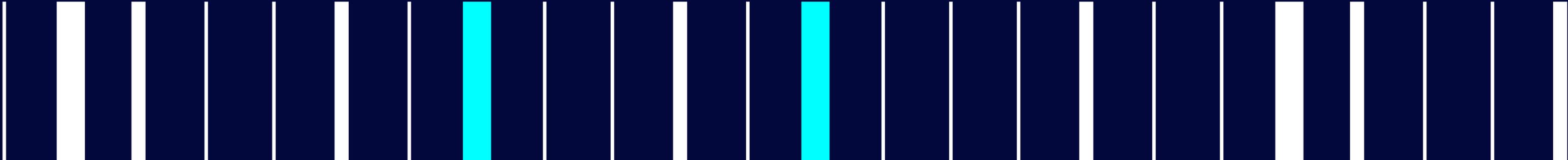
Capita can support solutions from leading vendors such as McAfee, Symantec, Sophos, Ivanti and Microsoft to provide a wide range of endpoint management and endpoint protection functionality such as anti-malware, policy enforcement, patch management encryption and more.



e-safety for education

Schools face the unique challenge of managing safeguarding requirements in the context of budget challenges, so need cost-effective solutions for managing risk in their IT environments. Capita has worked with education partners like C2k to develop specific solutions for the education sector that help solve many of these challenges.

Capita Managed Security Services



The secret to effective security management is understanding that businesses are run by people, and that people make mistakes.

So no matter how good their protection is, no organisation is entirely invulnerable.

Human error means that breaches will happen. And while it remains important to do everything possible to prevent them, it's equally important to have the expertise in place to be able to spot them when they happen – and that is often where the key challenge is.

Sophisticated modern threat actors are stealthy and know how to evade detection. The traditional answer to this challenge is a Security Incident and Event Management (SIEM) system.

Such a system will pull together event data from a wide array of different sources: siloed logs, alerts, threat feeds, network flows, user activity and the like, and analyse it for indications that the environment has been compromised in some way.

However, SIEM alone is not the answer. Simply putting log data in one place and running a static set of use cases, criteria and thresholds against it can generate a lot of noise that will tie up IT resource, and fail to make anything more secure.



To make a SIEM effective, it needs to be combined with the following:

- Manual analysis of event data and alerts – reviewed by qualified Security Operations Centre (SOC) staff who can distinguish genuine threats from false positives.
- Additional sources of threat intel to inform the review and analysis of threat data.
- Background research by the security team into new and emerging threats which feeds back into regular revisions, SIEM use-cases and thresholds.
- Tuning and refining of SIEM configuration throughout the life of the service to reduce false positives.
- Regular reviews of system performance and alerts generated within the period.

Without these services, a SIEM can become an expensive waste of time. But it can be hard for organisations to recruit and retain the skilled staff needed to carry out such processes.

Capita's managed security services can provide this effective management of the SIEM and remove the burden of running your own SOC internally.

Our purpose-built facilities are UK based, and staffed by certified cyber security professionals employing a variety of market-leading solutions. They are dedicated to finding the cyber 'needle in a haystack' that presages the early stage of a cyber attack.

Capita's Belfast SOC is the most recent, state-of-the-art addition, and the only one of its kind in Northern Ireland. Together with GB and India, this multi-location approach provides a degree of service resilience beyond most organisations' reach and offers our customers the ability to be monitored 24/7/365.

**175
days**

The average time to detect a cyber-attack in EMEA last year. In comparison, our SOCs spot threats in real time as they develop.

Each SOC is tapped into pre-public threat intelligence from the NCSC – a degree of foresight otherwise unattainable for most of our clients.



How does it work?

Our SOC employs IBM QRadar, an acknowledged (by Gartner and Forrester) market leader in the SIEM field which gathers security intelligence from throughout a client's estate, and currently supports more than 500 product integrations.

Each SOC has the flexibility to install and manage a range of QRadar deployment options, which can be hosted in the cloud, Capita data centres or client premises.

This comprehensive, end-to-end platform generates a real-time view of vulnerability across a client's entire estate, supporting it with a global network, advanced AI and behaviour analytics.

Why Capita for MSS?

- Our SOCs are purpose built, highly secure and use the most experienced cyber security talent.
- We are a full-spectrum Managed Service Provider, and don't rely on other MSPs to respond to incidents.
- Our network of multiple SOCs enables 24/7/365 monitoring and an exceptional degree of resilience.
- We bring our clients the skills and capabilities of highly experienced cyber security professionals that are otherwise hard to find, expensive to employ, and difficult to retain.
- We provide real-time identification of security incidents and prioritisation of those with the biggest business impact, enabling the fastest and most effective response.
- Our SIEM service also allows you to collate the forensic evidence often needed for regulatory or compliance purposes.

How we make SIEMs cost effective

SIEMs are traditionally expensive, usually because they are poorly optimised and unfocused. We work with our customers to configure and calibrate the system so it concentrates on their top priorities. Coupled with a range of deployment models, this helps us manage costs for our customers.

Initially, solutions can be deployed to monitor only high-risk areas of the estate – further reducing costs – and scaled up to the entire estate if needed later, and when value is realised.



Why Capita?

-  Over 160 organisations protected by Capita Cybersecurity services.
-  AXELOS our joint venture with the Home Office, sets global standards for cyber resilience.
-  Our access to vendor threat Intel such as IBM X-Force and Palo Alto Unit 42.
-  Government-level security vetting.
-  CREST, CHECK and Tiger Scheme accredited security testing teams.

If you have any questions, or would like to find out more about how we can help your cyber security needs, please visit our website on the link below:

[Find out more](#)

 Capita

