CYBER ESSENTIALS CERTIFICATION

KEY BENEFITS & DELIVERABLES

- **Business enabler:** Holding a Cyber Essentials or Cyber Essesntials Plus certification is a requirement when bidding for government contracts
- **Reduces Risk:** It is estimated that by implementing the Cyber Essentials criteria the risk of success of internet-based attacks is reduced by 80%
- **Increases Efficiency:** Key processes integrated within Cyber Essentials improves the organisation's business efficiencies
- **Reduces Costs:** Cyber insurance premiums are reduced for Cyber Essentials certificate holders
- **Improves Reputation**: Partners, suppliers and vendors prefer to do business with organisations that are certified by independent authorities as following industry-recommended best practises regarding data privicy and protection

SERVICE DESCRIPTION

The National Cyber Security Centre recognises that commercially sensitive information is an attractive target for cyber criminals and state-sponsored or afliated threat actors. The NSCS has created the Cyber Essentials framework to provide guidelines for businesses to protect their valuable information assets. Both the government and major businesses have now made the the CE certification a condition of doing business.

The Cyber Essentials scheme focuses on five essential mitigation controls: boundary firewalls and internet gateways, secure configuration, access control, malware protection & patch management. It encourages organisations and business leaders to consider their cybersecurity measures, take ownership of their cyber risks and build mitigating controls into their overall corporate risk management regime.

The first level of Cyber Essentials scheme is the Cyber Essentials Certification. Obtaining this certification demonstrates key competencies that an organisation has in place to ensure good practices are followed when dealing with data security and processes.

A self-assessment questionnaire is required to be completed and then returned to be reviewed by our security teams. A Certified Assessor will check the questionnaire responses and measure them against the guidelines laid out in the Cyber Essentials Scheme.

The Cyber Essentials Plus certif cation process includes the completion of a self-assessment questionnaire as well as an external vulnerability assessment against internet facing infrastructure. Further review of internal standard workstation types & company-issued mobile devices also falls within the scope of Cyber Essential Plus.

Once all criteria are met, our accreditation division will process and issue the relevant certification.

KEY TECHNICAL COMPONENTS

Cyber Essentials and Cyber Essentials Plus

- Self-Assessment Questionnaire reviewed by certified accreditation professionals
- External Vulnerability Scan

Cyber Essentials Plus only

Internal Workstation Review

- Each standard workstation type in your organisation is assessed against a number of criteria aimed at assessing the five key control areas, and how these have been applied to your internal user devices

Mobile Device Review

- If your organisation offers mobile devices to users, these will be reviewed for effective patch-management and access controls

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com