Cyber Essentials Plus

autodata

Become Cyber Essentials Plus certified to verify that your organisation safeguards against common cyber threats

What is Cyber Essentials

Cyber Essentials is a simple but effective Government-backed scheme that helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security and data protection.

The National Cyber Security Centre or NCSC (part of GCHQ) launched the scheme in June 2014 to enable organisations to gain one of two Cyber Essentials badges. Since October 2014, the UK Government has required all suppliers bidding for government contracts to be certified against the Cyber Essentials scheme.

The basic Cyber Essentials certification verifies that an organisation meets the requirements outlined under five specific technical control themes:

- **FIREWALLS**
- **SECURE CONFIGURATION**
- **USER ACCESS CONTROL**
- **MALWARE PROTECTION**
- **PATCH MANAGEMENT**

Cyber Essentials / Cyber Essentials Plus

Cyber Essentials is a self-assessment certification that requires a questionnaire to be completed and submitted to a certified member of one of the NCSC's Accreditation Bodies. All Autodata's assessments are certified by CREST.

Cyber Essentials Plus additionally requires that we carry out an independent **External Vulnerability Assessment** of your infrastructure.

All organisations holding valid Cyber Essentials certifications are publicly listed on the NCSC's certificate-search database, making it easy to identify whether you are Cyber Essentials Plus certified or not:

https://www.cyberessentials.ncsc.gov.uk/cert-search

External Vulnerability Assessment

Our External Vulnerability Assessment directly tests the controls in place on your network perimeter and highlights any obvious vulnerabilities via:

- A full TCP port scan for all IP addresses within specified ranges
- Scanning for known common UDP services for all IP addresses within specified ranges
- Basic web application scanning for common vulnerabilities performed from an unauthenticated user perspective
- Testing of inbound email binaries and payloads using a remote test account and desktop/laptop to send multiple emails containing one of the test files detailed by the certificating body
- A test from a website page with URLs linking to a set of test binaries
- Authenticated vulnerability scan of hosts using an approved industry-standard workstation build review tool to perform an administrator-level level scan including local checks for each host within a sample set. This stage also includes a patch check for operating system updates and common applications, and a check of any antivirus solutions in use

On completion of the External Vulnerability Assessment we deliver:

- A report listing all identified risks scored using the CVSSv2 standard covering all five Cyber Essentials technical control themes
- Recommendations to further comply with the Government standard
- Your **Cyber Essentials Plus** Certificate and badge

256-260 Old Street, London, UK, EC1V 9DD
t. +44 (0) 207 749 7949 | e. salesteam@autodata.co.uk | www.autodata.co.uk