Service Definition
Cyber Essentials

Introduction

Intertek NTA is a CE+ Certification Body licensed by The IASME Consortium, Cyber Essentials Partner to the National Cyber Security Centre (NCSC). The Cyber Essentials Scheme has been developed by the UK Government in partnership with information security industry experts and sets out to achieve the following:

- To provide a clear statement of the basic controls all organisations should implement to mitigate the risk from common Internet based threats, within the context of the Government's 10 Steps to Cyber Security guideline published in September 2012 as part of the 'Keeping the UK safe in cyber space initiative'.
- To offer a mechanism using the 'assurance framework' by which an organisation can demonstrate to customers, investors, insurers and others that it has taken these essential precautions to protect itself from Internet-based threats.

By implanting or maintaining CE+ you will be protecting its infrastructure against common types of cyber-attack such as exploitation of known vulnerabilities in Internet connected servers and devices using widely available tools and techniques.

Scope

CE+ will cover the basics of cyber security in corporate IT systems. It is important to understand that the certification only provides a snapshot of the cyber security practices at the time of assessment. Maintaining a robust cyber security stance requires additional measures and a proactive approach such as sound risk management, as well as ongoing updates such as patching and malware protection.

The following are defined in scope for the self-assessment questionnaire, external vulnerability assessment and review of internal end user devices (EUDs):

- Firewalls
- Secure configuration
- Security update management
- User access control
- Malware protection

There are currently two levels of certification that can be applied for:

Requires you to complete a self-assessment questionnaire, with responses independently reviewed.

As above plus tests of your internal workstations and mobile devices, and a vulnerability scan of your Internet facing systems performed using a range of approved tools and techniques.

Service Definition
Cyber Essentials

To certify against the CE or CE+ standard you are required to:

- Complete a self-assessment questionnaire ('Willow' version as of 28th April 2025), which will be independently verified by a certification body (Intertek NTA)
- Undertake an external vulnerability test to verify that the systems meet the requirements of the scheme
- Undertake an internal security assessment of end-user devices

Organisations who meet the 'pass' criteria for these stages are issued with the CE+ 'Badge', which can be used to demonstrate to existing and prospective customers and stakeholders that you have been successfully measured against the standard.

Certification Process
Detailed below are the activities you must undertake prior to achieving certification:

1. **Scope Definition** – You must define and document the scope for the assessment in relation to the number of systems that are exposed to the Internet and internal end user devices to be reviewed, with each device being representative of its wider estate, e.g. that there are no significant variances across desktops, laptops and mobile devices in terms of OS and standard-software (browser, Adobe, etc.) versions.
2. **Self-Assessment Questionnaire (SAQ)** – You will receive login credentials to the assessment portal to access a questionnaire which covers the requirements for basic technical protection from cyber-attacks. Upon completion, an authorised signatory of the organisation (board member or equivalent) should sign the questionnaire attesting its accuracy and compliance. The completed questionnaire will then be reviewed by an Intertek NTA CE Assessor. *Note: You must receive a pass on this element before the 'Plus' elements of the scheme (External Vulnerability Assessment and End User Device Assessment) can be progressed.*
3. **External Vulnerability Assessment** – Intertek NTA will conduct a vulnerability test against the public facing infrastructure, including the firewall(s), to ensure there are no public-facing vulnerabilities.
4. **Internal Vulnerability Assessment** – A vulnerability scan will be performed against a sample of your internal infrastructure. This scan will ensure that all applications and software are up-to-date, there are no high risk/critical vulnerabilities, and devices aren't missing any patches.
5. **User Testing** – Intertek NTA will conduct an internal security assessment of end-user devices. This directly tests that individual controls have been implemented correctly and recreates various attack scenarios to determine whether a system compromise using basic capabilities can be achieved. Sample testing of devices is also required to provide assurance as to the consistency of builds provided for review. Testing will include:
    - **Results *Malware Test:***
      Benign malware files will be downloaded onto the sample devices, to ensure that the anti-virus is running, and identifying downloaded payloads before they can have any effect on a system. These are empty files that contain a virus signature, purely designed to trigger the anti-virus. (eicar.org)

- ***Download Test:***
- We will instruct the users to visit a website that is set up with different file types. The user will then download these files, so the assessor can monitor how the system reacts to the file types. The assessor will ensure that none of the files can auto-download from the site, and none of them auto-run upon download.
- ***Email Test:***
- Similar to the download test, a set of various file types will be emailed to the user. This is so the assessor can identify which emails successfully reach the users' inbox, which ones still have their attachments on the emails, and whether those attachments can be run without any prompts appearing on the screen.
- ***Admin Test:***
- This test is to ensure that all users are logged in as a standard user account for their day-to-day activities. The user will be required to run the 'device manager' application. If the user is a standard user, a pop-up will appear on the screen detailing this.
- ***MFA Test:***
- This test is to ensure that all administrators of any cloud services in use have multi-factor authentication (MFA) configured on their account. The assessor will require a cloud administrator to log in, so the MFA code/token request can be observed.

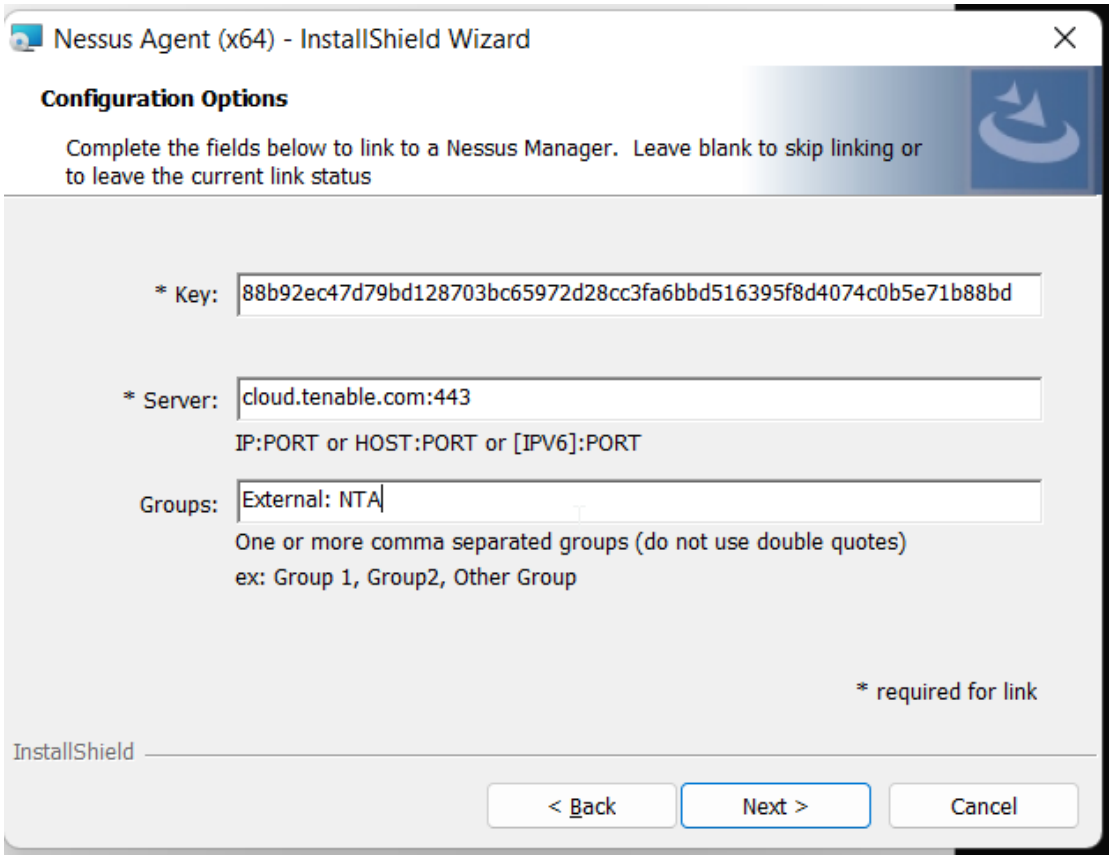
6. **Results** – The results from the SAQ, External Vulnerability Assessment, Internal Vulnerability Assessment and User Testing will be reviewed, and the findings will determine the 'Pass' or 'Fail' status of the organisation.
7. **Certification Award –** If a 'Pass' status is achieved, you will be re-issued with the certificate and badge demonstrating that the requirements of the scheme have been met. If the organisation achieves a 'fail' status, the assessment will need to be repeated once any failing points have been mitigated.

Annual Review
There is a requirement to recertify at least once a year, which requires a repeat of the above process.

Internal Vulnerability Assessment
Tenable agents will need to be installed on each device applicable within the sample. This will include Servers, Desktops, and Laptops.

Tenable agents can be downloaded for each OS type from the link below:
https://www.tenable.com/downloads/nessus-agents?loginAttempted=true

When installing, it is essential the device is installed with the Intertek NTA details as per the image below.



- Key: 88b92ec47d79bd128703bc65972d28cc3fa6bbd516395f8d4074c0b5e71b88bd
- Server: cloud.tenable.com:443
- Groups “External: NTA”

User Testing

The user testing takes approximately 15 minutes per user. This is usually conducted over Teams (or similar video conferencing facility) with a screenshare. The assessor will send the user various test attachments, request them to download test files, test their account permissions, and verify that the anti-malware solution is functioning as expected. Where possible, it would be useful if the owner of each end user device in the sample can be assigned a schedule, where the assessor can send video conferencing invites to the users.

Service Management

You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

Intertek NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, Intertek NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling the test, ensuring reports are sent out in a timely manner, scheduling follow up tests and debriefs etc.

This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

Ordering and Invoicing Process

Once the scope of work and number of units/days required has been agreed between the customer and Intertek NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

Customer Responsibilities

The customer is responsible for the completion of the self-assessment questionnaire and providing details of the systems in scope of assessment. The provision of appropriate information will ensure that delivery meets the requirements of the *Cyber Essentials* standard.

Technical Requirements

Below is some useful information with regards to the IASME rules for certification assessments:

- Applicants must now declare that they have read the "*Cyber-Essentials-Requirements-for-IT-infrastructure-3.1*" document when they submit the self-assessment:
- (https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf)
- Intertek NTA are unable to start the CE+ Assessment until the CE Basic self-assessment has been successfully completed (and passed).
- The self-assessment must be signed off by a board member, otherwise it's an automatic fail.
- Any unsupported operating systems are also an automatic fail.
- Anything more than 2 non-compliant questions will also result in a fail.
- The CE+ element must be completed within 3 months of the date of the CE basic award.
- The definition of a Home Worker has changed to "*Any employee contracted or legally required to work at home for any period of time at the time of the assessment needs to be classed as a home worker for Cyber Essentials*."
- If you do have Home Workers, then their scope boundary (if no VPN is in place) must be a host-based software firewall that meets Cyber Essentials controls.
- Mobile devices:
  - Any company-owned devices that access organisational data and services* are in scope for assessment.
  - In addition to mobile or remote devices owned by the organisation, user-owned (BYOD) devices that access organisational data or services* are in scope.
  - You would need to have some form of policy/process or technical-based control to manage remote access.
  - We have to test a representative sample of devices (both corporate and BYOD if in use). This includes an assessment of access controls, the OS (must be up to date/supported), inbound mail and download tests.

** Organisational service includes any software applications, Cloud applications, Cloud services, User Interactive desktops and Mobile Device management solutions owned or subscribed to by the applicant organisation.*
For example: Web applications, Microsoft Office 365, Google Workspace, Mobile Device Management containers, Citrix Desktop, virtual desktop solutions, IP telephony.

- If there are any failing issues to be remediated then they must be fixed within a maximum of 2 days for the self-assessment and 30 days for the CE+ elements. Beyond these timeframes you will have to wait for a further 30 days before re-taking the assessment (at the applicable cost).