Cyber Essentials Plus Assessment Report

Assessment of:	Fitech UK Limited
Assessed by (Certification Body)	Bulletproof
Assessed by (Assessor name)	Saagar Shah
Assessed by (Lead Assessor name)	Saagar Shah
Date of assessment visit	22/04/2022
Date of report:	2022-04-25

Cyber Essentials Plus certification can only be issued by a licensed Certification Body.

You can confirm the authenticity of this report by contacting IASME Consortium

+44 (0)3300 882752

1. About this report

Cyber Essentials Plus is the audited version of the Cyber Essentials information security standard. Cyber Essentials requires organisations to have a number of technical and procedural controls in place to improve their information security in order to mitigate common internet-borne cyber attacks. Cyber Essentials Plus is a series of tests that provide a further level of assurance that these technical controls have been successfully implemented within an organisation.

This report is a record of the Cyber Essentials Plus audit of Fitech UK Limited against the Cyber Essentials standard that has been carried out by Saagar Shah of the Certifying Body Bulletproof.

Cyber Essentials provides assurance that a number of key information security controls are in place within an organisation. For further assurance, the IASME information security standard provides a broader set of controls that enable good information security governance across an organisation.

1.1. Summary of findings

The organization has a good group policy and a brilliant antivirus in place. It also has a very well configured firewall in place that protects against all threats. The number of browser are also limited which reduces risk and all user accounts are locked down which protects the users from any malware attacks or phishing attempts. All devices have segregated accounts. Cloud systems are secure and have MFA enabled.

The assessor has concluded that Fitech UK Limited has passed the required tests and should be awarded the Cyber Essentials Plus certification.

If a test has not been passed successfully, the assessor has provided feedback within the relevant section.

1.2. Evidence of activities

In carrying out the audit, the assessor will have carried out a number of technical tests and have seen documentary evidence. This evidence forms the basis for the assessor’s recommendations and where appropriate has been included in this report.

2. Scope

Location:
Kemp House, 152-160 City Road, LONDON, EC1V 2NX

Certain items will be out of scope for the Cyber Essentials Plus assessment. Notable exceptions are listed below:

Website - Externally Hosted

3. External Testing

3.1. Test 1 – Remote vulnerability assessment

This test was awarded PASS by the assessor.

The test did not identify any vulnerabilities that were scored 7 or higher on CVSS v3 during the testing of the external IP addresses.

4. Internal testing

A suitable sample set of devices was selected as follows:

2 Apple MacOS Monterey

1 Android 12

4.1. Test 2 – Review of device patching

This test was awarded PASS by the assessor.

No vulnerabilities were identified for the tested devices that were scored 7 or higher on CVSS v3 and that met the parameters listed in the Cyber Essentials Plus guidance.

4.2. Test 3 – Review of malware protection

This test was awarded PASS by the assessor.

It was identified that Fitech UK Limited is using the following methods of malware protection in their organisation:

- A - Anti-malware software
- B - Limiting installation of applications to an approved set

A - Anti-malware software

Anti-malware software is correctly installed and configured on all devices that rely on this method

B - Limiting installation of applications to an approved set

This method of anti-malware protection is correctly configured on all devices that rely on it.

4.3. Test 4 – Review of protection against malware sent by email

This test was awarded PASS by the assessor.

The standard set of test files was sent to each End User Device in the sample set via email.

All of the malware test files were successfully blocked by the End User Devices.

All of the non-malware test files prompted a suitable warning or opportunity to cancel before opening for all End User Devices.

4.4. Test 5 – Review of protection against malware delivered through a website

This test was awarded PASS by the assessor.

The standard set of test files was attempted to be accessed via a website on all End User Devices within the sample set.

All of the malware test files were successfully blocked by the End User Devices.

All of the non-malware test files prompted a suitable warning or opportunity to cancel before opening for all End User Devices.

4.5. Test 6 – Review of Multi Factor Authentication Configuration

This test was awarded PASS by the assessor.

All cloud services that provide a method of authentication were confirmed to have MFA enabled and configured for standard users and administrators within the sample set.

4.6. Test 7 – Configuration of Account Separation

This test was awarded PASS by the assessor.

The assessor has confirmed that account separation is in place and that when attempting to run an administrative task by a standard user on the sampled devices, credentials to a separate administrator account were requested.

CYBER
ESSENTIALS
PLUS

CERTIFICATE OF ASSURANCE

Fitech UK Limited

Kemp House, 152-160 City Road, LONDON, EC1V 2NX

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR : Saagar Shah

CERTIFICATE NUMBER : IASME-CEP-008957

DATE OF CERTIFICATION : 2022-04-25

PROFILE VERSION : Evendine

RECERTIFICATION DUE : 2023-04-25

SCOPE : Whole Organisation

CERTIFICATION MARK

CYBER
ESSENTIALS
CERTIFIED
PLUS

CERTIFICATION BODY

BULLET
PROOF

CYBER ESSENTIALS PARTNER

IASME
CONSORTIUM

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.