CYBER
ESSENTIALS

Cyber Essentials 2023 Workshop

Neil Furminger - Cyber Essentials Manager

CYBER ESSENTIALS

National Cyber Security Centre

IASME CONSORTIUM

Delivery Partner

in association with National Cyber Security Centre

Cyber Essentials

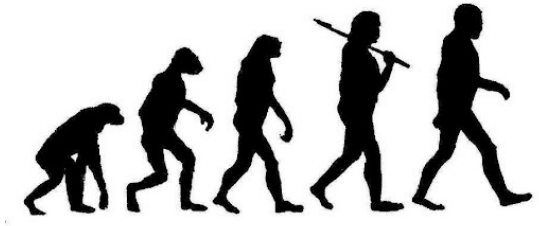
CYBER ESSENTIALS

Cyber Essentials Workshop

- Clarification on level of device detail required
- Discuss the April 2023 changes
- This is your session to ask about any aspects of the scheme
- Common areas of discussion.
  - Scope
  - Unsupported operating systems
  - Unsupported Software
  - BYOD
  - Cloud services and MFA

Cyber Essentials Changes

- Clarification on level of device detail
- Grace periods extended to April 2023.
- Clarification surrounding firmware support.
- Clarification on third party devices in scope.
- Updates to Device Unlocking
- Update to Malware Protection
- Guidance on Zero Trust and Asset Management.



CYBER ESSENTIALS

Level of detail required for User Devices

- ‘Cyber Essentials will require that all applicants list their laptops, desktops, servers, computers, tablets and mobile phones, with details of the make and operating system. However, when it comes to firewalls and routers, the applicant will only be asked to list make and model, but not the specific version of the firmware. By asking for the make and model on these devices, the Assessor will be able to determine if the devices are still receiving security updates to the firmware.’

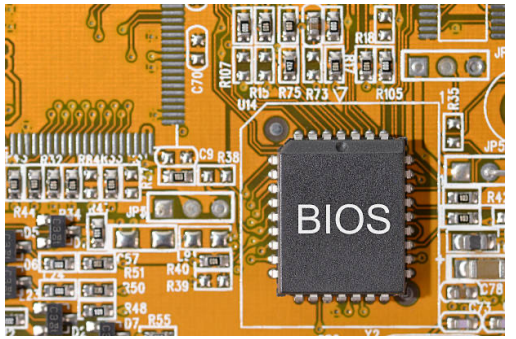
- This applies with immediate effect.
- Blogs and question set include this statement

CYBER ESSENTIALS

Grace Periods Extended Until April 2023

- Thin Clients will need to be listed in the assessment and supported. (A2.4.1)
- All Cloud Services must have MFA to all standard user accounts. (A7.17)
  - A7.17 Has MFA been applied to all users of your cloud services.
- Unsupported software such as applications will need to be removed from scope by placing into their own sub-set. (A6.7).
  - Unsupported OS would still lead to an Auto Fail which has always been the case

CYBER ESSENTIALS



Firmware Clarification

- For Cyber Essentials all software must be supported.
- Firmware has always been included within the definition of software.
- Definition changed to ‘firewall and router firmware’.
- Reason - Threats to Operating Systems are more prevalent within the scheme.
- Router and Firewall Make and Model details required in order for assessor to check the device is still supported and receiving firmware updates.

CYBER ESSENTIALS

Cyber Essentials Third Party Devices

- Issue - Third party devices difficult to understand when to include in scope
- If a third party manages devices on behalf of the applicant, the applicant must understand how the controls are applied.
- To help applicants clarify when a devices in scope a table has been included in the requirements document.
- All user access accounts and accounts accessing cloud services administered/owned by the applicant are in-scope of the assessment.

CYBER ESSENTIALS

Device Scoping table

	Applicant Organisation Owned	Third Party Organisation Owned	BYOD
Employee	✓	N/A	✓
Volunteer	✓	N/A	✓
Trustee	✓	N/A	✓
University Research Assistant	✓	N/A	✓
Student	✓	N/A	✗
MSP Administrator	✓	✗	✗
Third Party Contractor	✓	✗	✗
Customer	✓	✗	✗

✓ Brought into scope

✗ Out of scope

CYBER ESSENTIALS

Device Unlocking Update

- Brute force requirements for device unlocking need to be applied when available the vendor allows the configuration to altered
- When the vendor does not allow configuration in line with the CE Requirements, the applicant should use the vendor defaults.

CYBER ESSENTIALS

Malware Protection Update

- Anti Malware-Software no longer needs to be signature-based.
  - Change has been made to account for the Next Gen solutions.
- Removal of Sandboxing option
- Changes to CE +
  - Tests will now contain manual steps.
  - Request for feedback was sent to all CE+ Assessors

CYBER ESSENTIALS

Zero Trust Guidance

- Information will be included about Zero Trust and Cyber Essentials.
- Implementing the Cyber Essentials controls as they stand will not prevent an organization from adopting Zero Trust.
- NCSC guidance to zero trust has been linked in the requirements document.
- Mapping exercise wascarried out by the CE Technical Working group and NCSC SMEs
- Conclusion there is a correlation between CE and NCSC Zero Trust model

CYBER ESSENTIALS

Asset Management Guidance

- Asset Management not a specific control but is considered to underpin all five technical controls within the scheme.
- Link to NCSC asset management guidance has been included.
- This addition is based on a trend being observed by the NCSC and IASME when engaging with organisations.
- In order to apply the CE controls you must understand which devices they must be applied to.

CYBER ESSENTIALS

Question set changes

- Question set to match V3.1 requirements is called Montpellier
- Question Set language usage has been changed
- Applicant guidance articles have been linked to the start of each section
  - Article for all 5 controls and scope
- The requirements document has changed the order of controls to match the question set

CYBER ESSENTIALS

Question set changes

- A1.7 has been moved to Scope section
  - Same question but new number A2.7.1
- MFA question A7.14 to A7.16
  - A7.14 and A7.15 Information only
  - A7.16 and A7.17 marked for compliance
- Additional option has been added to multiple choice questions
  - New option is ‘None of the above’ and an explanation is required
  - None of the above should be marked with an ‘non-compliance’
- A1.8 has been updated, more detail required at the request of NCSC

CYBER ESSENTIALS

Time lines

- Documents Published – 23rd January 2023
  - V3.1 CE requirements
- Question Set Published - 6th February 2023
  - New Question Set – Montpellier
- Go Live - 24th April 2023
- V3.1 CE requirements language change
  - This is based on feedback received by the NCSC
  - The technical controls still remain the same.
  - Question Set will also reflect the change in language style.

CYBER ESSENTIALS

Latest NCSC Blogs

- Debunking some Myths
  - https://www.ncsc.gov.uk/blog-post/reviewing-the-cyber-essentials-update-2022
- Grace Period Extension
  - https://www.ncsc.gov.uk/information/cyber-essentials-technical-controls-grace-period-update
- Update blog - 23rd January
  - https://www.ncsc.gov.uk/information/cyber-essentials-technical-requirements-updated-for-april-2023

Thank-you

neil.furminger@iasme.co.uk