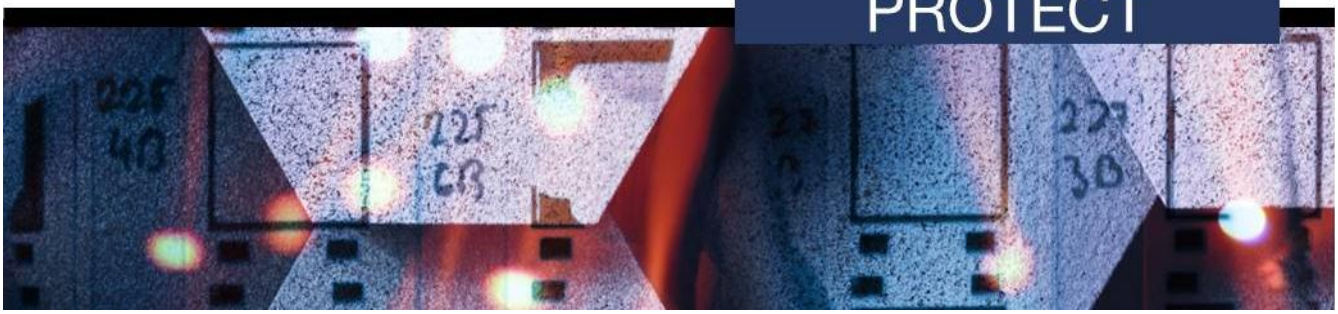

APRIL 2018

Essential Eight Maturity Model

Introduction

1. The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the *Strategies to Mitigate Cyber Security Incidents*, to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies are known as the Essential Eight.

Maturity levels

2. To assist organisations in determining the maturity of their implementation of the Essential Eight, five maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:
    a. Maturity Level Zero: Not aligned with intent of mitigation strategy
    b. Maturity Level One: Partly aligned with intent of mitigation strategy
    c. Maturity Level Two: Mostly aligned with intent of mitigation strategy
    d. Maturity Level Three: Fully aligned with intent of mitigation strategy
    e. Maturity Level Four: For higher risk environments.

What maturity level to aim for

3. As a baseline, organisations should aim to reach Maturity Level Three for each mitigation strategy. However, some organisations are constantly targeted by highly skilled adversaries, or otherwise operate in a higher risk environment. These organisations should aim to reach Maturity Level Four for mitigation strategies designed to assist in mitigating the specific threat vectors that adversaries are known to be using against them.

Further information

4. The *Strategies to Mitigate Cyber Security Incidents*, including supporting publications, can be found at https://www.asd.gov.au/infosec/mitigationstrategies.htm.

Contact details

5. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).

Essential Eight Maturity Model

APRIL 2018

		Maturity Level Zero Not aligned with intent of mitigation strategy	Maturity Level One Partly aligned with intent of mitigation strategy	Maturity Level Two Mostly aligned with intent of mitigation strategy	Maturity Level Three Fully aligned with intent of mitigation strategy	Maturity Level Four For higher risk environments
MITIGATION STRATEGIES TO PREVENT MALWARE DELIVERY AND EXECUTION						
Application whitelisting	**Workstations**	Application whitelisting is not implemented on all workstations of high-risk users or Whitelisting of executables is not enforced	Application whitelisting is implemented on all workstations of high-risk users Whitelisting of executables is enforced	Application whitelisting is implemented on all workstations of high-risk users Whitelisting of executables and software libraries is enforced	Application whitelisting is implemented on all workstations Whitelisting of executables, software libraries, scripts and installers is enforced	Application whitelisting is implemented on all workstations Whitelisting of executables, software libraries, scripts and installers is enforced using only file hashes
	Servers	Application whitelisting is not implemented on all important servers (e.g. Active Directory, email servers and other servers handling user authentication) or Whitelisting of executables is not enforced	Application whitelisting is implemented on all important servers (e.g. Active Directory, email servers and other servers handling user authentication) Whitelisting of executables is enforced	Application whitelisting is implemented on all important servers (e.g. Active Directory, email servers and other servers handling user authentication) Whitelisting of executables and software libraries is enforced	Application whitelisting is implemented on all important servers (e.g. Active Directory, email servers and other servers handling user authentication) Whitelisting of executables, software libraries, scripts and installers is enforced	Application whitelisting is implemented on all servers Whitelisting of executables, software libraries, scripts and installers is enforced using only file hashes
Patch applications	**Workstations**	Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are not applied or are applied on a greater than monthly basis for any workstation or Non-vendor-supported versions of Adobe Flash, web browsers, Microsoft Office, Java or PDF viewers are used	Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are applied within one month for all workstations Only vendor-supported versions of Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are used	Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are applied within 48 hours for workstations of high-risk users and two weeks for all other workstations Only vendor-supported versions of Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are used	Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are applied and verified within 48 hours for all workstations Only vendor-supported versions of Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are used	Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are applied and verified within 48 hours for all workstations Only the latest vendor-supported versions of Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are used
	Servers	Patches for extreme risk security vulnerabilities in web server software, server applications that store important (sensitive or high-availability) data, and other internet-accessible server applications are not applied or are applied on a greater than monthly basis for any server or Non-vendor-supported versions of web server software, server applications that store important data or other internet-accessible server applications are used	Patches for extreme risk security vulnerabilities in web server software, server applications that store important (sensitive or high-availability) data, and other internet-accessible server applications are applied within one month for all servers Only vendor-supported versions of web server software, server applications that store important data and other internet-accessible server applications are used	Patches for extreme risk security vulnerabilities in web server software, server applications that store important (sensitive or high-availability) data, and other internet-accessible server applications are applied within 48 hours for important servers (e.g. Active Directory, email servers and other servers handling user authentication) and two weeks for all other servers Only vendor-supported versions of web server software, server applications that store important data and other internet-accessible server applications are used	Patches for extreme risk security vulnerabilities in web server software, server applications that store important (sensitive or high-availability) data, and other internet-accessible server applications are applied and verified within 48 hours for all servers Only vendor-supported versions web server software, server applications that store important data and other internet-accessible server applications are used	Patches for extreme risk security vulnerabilities in web server software, server applications that store important (sensitive or high-availability) data, and other internet-accessible server applications are applied and verified within 48 hours for all servers Only the latest vendor-supported versions of web server software, server applications that store important data and other internet-accessible server applications are used
Configure Microsoft Office macro settings	**Workstations**	All Microsoft Office macros can execute without prompting users for approval or Microsoft Office macro settings can be changed by users	Microsoft Office macros can execute, but only after prompting users for approval Microsoft Office macro settings can't be changed by users	Only signed Microsoft Office macros can execute Microsoft Office macros from the Internet are blocked Microsoft Office macro settings can't be changed by users	Only Microsoft Office macros in Trusted Locations with limited write access can execute Microsoft Office macros from the Internet are blocked Microsoft Office macro settings can't be changed by users	Microsoft Office macros are blocked from executing and Trusted Locations are disabled Microsoft Office macro settings can't be changed by users
User application hardening	**Workstations**	Web browsers automatically play Adobe Flash content or Web browser Adobe Flash settings can be changed by users	Web browsers use 'click to play' for Adobe Flash content Web browser Adobe Flash settings can't be changed by users	Web browsers block or don't support Adobe Flash content Web browser Adobe Flash settings can't be changed by users Web browsers block web advertisements and Java from the Internet	Web browsers block or don't support Adobe Flash content Web browser Adobe Flash settings can't be changed by users Web browsers block web advertisements and Java from the Internet Flash and OLE functionality is disabled in Microsoft Office Unneeded features in Microsoft Office, web browsers and PDF viewers are disabled	Web browsers block or don't support Adobe Flash content Web browser Adobe Flash settings can't be changed by users Web browsers block web advertisements and Java from the Internet Adobe Flash is uninstalled from operating systems (i.e. NPAPI, PPAPI and ActiveX files are removed) Flash and OLE functionality is disabled in Microsoft Office Unneeded features in Microsoft Office, web browsers and PDF viewers are disabled Microsoft Office, web browsers and PDF viewers are hardened using ASD and vendor hardening guides

		Maturity Level Zero Not aligned with intent of mitigation strategy	Maturity Level One Partly aligned with intent of mitigation strategy	Maturity Level Two Mostly aligned with intent of mitigation strategy	Maturity Level Three Fully aligned with intent of mitigation strategy	Maturity Level Four For higher risk environments
MITIGATION STRATEGIES TO LIMIT THE EXTENT OF CYBER SECURITY INCIDENTS						
Restrict administrative privileges	**Workstations and servers**	Requirements for privileged accounts are not validated or Privileged accounts are capable of reading emails and web browsing	Requirements for privileged accounts are validated initially All privileged accounts are restricted from reading emails and web browsing using policy controls	Requirements for privileged accounts are validated initially and on an annual or more frequent basis All privileged accounts are restricted from reading emails and web browsing using policy controls	Requirements for privileged accounts are validated initially and on an annual or more frequent basis Duties-based restrictions on privileged accounts are applied All privileged accounts are blocked from reading emails and web browsing using technical controls	Requirements for privileged accounts are validated initially and on a monthly or more frequent basis, or before they are required for a task and revoked immediately afterwards Duties-based restrictions on privileged accounts are applied All privileged accounts are blocked from reading emails and web browsing using technical controls
Patch operating systems	**Workstations**	Patches for extreme risk security vulnerabilities in operating systems are not applied or are applied on a greater than monthly basis for any workstation or A non-vendor-supported operating system version is used	Patches for extreme risk security vulnerabilities in operating systems are applied within one month for all workstations Only vendor-supported operating system versions are used	Patches for extreme risk security vulnerabilities in operating systems are applied within 48 hours for workstations of high-risk users and two weeks for all other workstations Only vendor-supported operating system versions are used	Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all workstations Only vendor-supported operating system versions are used	Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all workstations Only the latest vendor-supported operating system version is used
	Servers	Patches for extreme risk security vulnerabilities in operating systems are not applied or are applied on a greater than monthly basis for any server or network device or A non-vendor-supported operating system version is used	Patches for extreme risk security vulnerabilities in operating systems are applied within one month for all servers and network devices Only vendor-supported operating system versions are used	Patches for extreme risk security vulnerabilities in operating systems are applied within 48 hours for important servers (e.g. Active Directory, email servers and other servers handling user authentication) and two weeks for all other servers and network devices Only vendor-supported operating system versions are used	Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all servers and network devices Only vendor-supported operating system versions are used	Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all servers and network devices Only the latest vendor-supported operating system version is used
Multi-factor authentication	**Workstations and servers**	Multi-factor authentication is not implemented for all users using remote access solutions (e.g. VPNs, remote desktops, corporate webmail)	Multi-factor authentication is implemented for all users using remote access solutions (e.g. VPNs, remote desktops, corporate webmail) In addition to passphrases, only U2F security keys, physical OTP tokens, biometrics, smartcards, mobile apps, SMS messages, emails, voice calls and/or software certificates are used for multi-factor authentication	Multi-factor authentication is implemented for all users using remote access solutions (e.g. VPNs, remote desktops, corporate webmail) Multi-factor authentication is implemented for all users performing privileged actions In addition to passphrases, only U2F security keys, physical OTP tokens, biometrics, smartcards, mobile apps, SMS messages, emails and/or voice calls are used for multi-factor authentication	Multi-factor authentication is implemented for all users using remote access solutions (e.g. VPNs, remote desktops, corporate webmail) Multi-factor authentication is implemented for all users performing privileged actions Multi-factor authentication is implemented for all users accessing important (sensitive or high-availability) data repositories In addition to passphrases, only U2F security keys, physical OTP tokens, biometrics and/or smartcards are used for multi-factor authentication	Multi-factor authentication is implemented for all users using remote access solutions (e.g. VPNs, remote desktops, corporate webmail) Multi-factor authentication is implemented for all users performing privileged actions Multi-factor authentication is implemented for all users accessing important (sensitive or high-availability) data repositories In addition to passphrases, only U2F security keys and/or physical OTP tokens are used for multi-factor authentication
MITIGATION STRATEGIES TO RECOVER DATA AND SYSTEM AVAILABILITY						
Daily backups	**Workstations and servers**	Backups of important new/changed data, software and configuration settings are either not performed or performed less often than monthly or Backups are stored for less than one month or Full recovery of backups has not been tested	Backups of important new/changed data, software and configuration settings are performed monthly Backups are stored for between one to three months Full recovery of backups has been tested	Backups of important new/changed data, software and configuration settings are performed weekly Backups are stored offline or otherwise disconnected from computers and networks, or online but in a non-rewritable and non-erasable manner Backups are stored for between one to three months Full recovery of backups has been tested Partial recovery of backups is tested on an annual or more frequent basis	Backups of important new/changed data, software and configuration settings are performed daily Backups are stored offline or otherwise disconnected from computers and networks, or online but in a non-rewritable and non-erasable manner Backups are stored for three months or greater Full recovery of backups has been tested Full recovery of backups has been tested after each fundamental IT infrastructure change Partial recovery of backups is tested on an annual or more frequent basis	Backups of important new/changed data, software and configuration settings are performed daily or continuously Backups are stored offline or otherwise disconnected from computers and networks, or online but in a non-rewritable and non-erasable manner Backups are stored at multiple geographically-dispersed locations Backups are stored for three months or greater Full recovery of backups has been tested Full recovery of backups has been tested after each fundamental IT infrastructure change Full recovery of backups is tested on an annual or more frequent basis