# Example Essential Eight assessment test plan: Maturity Level Two

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mitigation Strategy** | **Test ID** | **Control Description** | **Test Methodology** | **Test Findings** |
| **Patch applications** | ML2-PA-01 | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. | Observe a vulnerability scan, or request evidence of previous vulnerability scans, and note the date/time stamp and scope. Check whether the list of scanned applications includes the list of applications that should have been scanned. |  |
| ML2-PA-02 | Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. | Use a vulnerability scanner to identify the listed applications within the environment. Check the date applications were updated and compare to the dates patches were released. Check that the gap between is not greater than one month. |  |
| **Multi-factor authentication** | ML2-MF-01 | Multi-factor authentication is used to authenticate privileged users of systems. | Verify a privileged user is presented with a MFA challenge when authenticating to their workstation or attempting to raise privileges. |  |
| ML2-MF-02 | Multi-factor authentication is used to authenticate unprivileged users of systems. | Verify an unprivileged user is presented with a MFA challenge when authenticating to their workstation. |  |
| ML2-MF-03 | Multi-factor authentication used for authenticating users of online services is phishing-resistant. | Verify MFA for users of online services (including online customer services) uses either security keys, smart cards or passkeys. |  |
| ML2-MF-04 | Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option. | Verify MFA for customers of online customer services offers the ability to use either security keys, smart cards or passkeys. |  |
| ML2-MF-05 | Multi-factor authentication used for authenticating users of systems is phishing-resistant. | Verify MFA for users of systems uses either security keys, smart cards or Windows Hello for Business. |  |
| ML2-MF-06 | Successful and unsuccessful multi-factor authentication events are centrally logged. | Verify the following event logs are centrally captured.Successful MFA events for the organisation’s online systems.Successful MFA events for administrative access.Unsuccessful MFA events for the organisation’s online systems.Unsuccessful MFA events for administrative access. |  |
| ML2-MF-07 | Event logs are protected from unauthorised modification and deletion. | Verify unauthorised users are unable to modify or delete event logs. |  |
| ML2-MF-08 | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Verify the organisation has responded to a sign of compromise in an internet-facing server trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| ML2-MF-09 | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Verify the organisation has identified a cybersecurity incident through the analysis of cybersecurity events. This evidence will typically exist as email correspondence. |  |
| ML2-MF-10 | Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | Verify that cybersecurity incidents are being reporting internally within the organisation. Identify that such reporting is occurring within a reasonable timeframe. This evidence will typically exist as email correspondence or formal briefing material. |  |
| ML2-MF-11 | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Verify that cybersecurity incidents are being reporting to ASD. Identify that such reporting is occurring within a reasonable timeframe. This evidence will typically exist as incident numbers provided by ASD for all reports submitted via ReportCyber. |  |
| ML2-MF-12 | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Verify that the organisation has an up-to-date cybersecurity incident response plan. It should accurately represent processes and procedures following in response to the last cybersecurity incident experienced by the organisation. |  |
| **Restrict administrative privileges** | ML2-RA-01 | Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated. | Review documented process to disable privileged access after 12 months. Review evidence, such as support tickets, emails, logs or an automated disabling procedure to confirm accounts are disabled after 12 months unless revalidated.Query Active Directory using PowerShell commands or tools such as ADRecon to identify accounts with no expiry dates or an expiration date greater than 12 months.The following PowerShell command returns privileged accounts with no account expiry set.*Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties AccountExpirationDate | Where-Object {$\_.AccountExpirationDate -like ""} | Select @{n='Username'; e={$\_.SamAccountName}}, @{n='Account Expiration Date'; e={$\_.AccountExpirationDate}}, @{n='Enabled'; e={$\_.Enabled}}*The following PowerShell command returns any privileged accounts that have an expiry date greater than 12 months.*Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties AccountExpirationDate | Where-Object {$\_.AccountExpirationDate -gt (Get-Date).AddMonths(12)} | Select @{n='Username'; e={$\_.SamAccountName}}, @{n='Account Expiration Date'; e={$\_.AccountExpirationDate}}, @{n='Enabled'; e={$\_.Enabled}}* |  |
| ML2-RA-02 | Privileged access to systems and applications is disabled after 45 days of inactivity. | Review documented process to disable privileged access after 45 days of inactivity. Review evidence, such as support tickets, emails, logs or an automated disabling procedure to confirm privileged accounts are disabled after 45 days of inactivity.Query Active Directory using PowerShell commands or tools such as ADRecon to identify privileged accounts with a ‘lastlogondate’ greater than 45 days.*Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties LastLogonDate | Where-Object {$\_.LastLogonDate -lt (Get-Date).AddDays(-45) -and$\_.LastLogonDate -ne $null} | Select @{n='Username'; e={$\_.samaccountname}}, @{n='Last Logon Date'; e={$\_.LastLogonDate}}, @{n='Enabled'; e={$\_.enabled}}* |  |
| ML2-RA-03 | Privileged operating environments are not virtualised within unprivileged operating environments. | Confirm with the organisation where the infrastructure for privileged operating environments is hosted. Look for privileged operating environment on unprivileged virtual hosts and typical user workstations. |  |
| ML2-RA-04 | Administrative activities are conducted through jump servers. | Attempt to connect to servers or administrator-only systems from an unprivileged operating environment. |  |
| ML2-RA-05 | Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed. | Run the following PowerShell commands to retrieve the number of devices with LAPS and compare this with the number of devices in Active Directory.Run the following PowerShell command to get number of devices with LAPS.*Get-ADComputer -Filter {ms-Mcs-AdmPwdExpirationTime -like "\*"} -Properties ms-Mcs-AdmPwdExpirationTime | measure*Run the following PowerShell command to get the number of enabled devices in Active Directory.*Get-ADComputer -Filter {Enabled -eq $true} | measure*Observe evidence of a password management or privileged access management solution in use for managing break glass and service account passwords. Ensure generated passwords are unique, unpredictable and meet a minimum length requirement (i.e. 30 characters). Look for accounts with identical passwords.Confirm how passwords are generated for local administrator accounts and how they are managed. If using LAPS for local administrator accounts, check the following group policy setting *Computer Configuration/Administrative Templates/LAPS/Password Settings*.Query Active Directory using PowerShell commands or tools such as ADRecon to identify service accounts with passwords last set more than 12 months ago.Run the following PowerShell command to get service accounts with passwords older than 12 months. Replace SVC\_\* with service account naming convention.*$PassLastSetTimeFrame = (Get-Date).AddMonths(-12)Get-ADUser -Filter "enabled -eq 'true' -and SamAccountName -like 'SVC\_\*'" -Properties pwdlastset | Where-Object{$\_.pwdlastset -like '0' -or ([datetime]::FromFileTime($\_.pwdLastSet) -lt $PassLastSetTimeFrame)} | Select-Object SAMAccountName, @{name ="pwdLastSet"; expression={([datetime]::FromFileTime($\_.pwdLastSet))}}* |  |
| ML2-RA-06 | Privileged access events are centrally logged. | Verify the following event logs are centrally captured.Event ID 4672 is created when an account with special privileges successfully logs in.Event ID 4625 is created when a logon request fails. |  |
| ML2-RA-07 | Privileged account and group management events are centrally logged. | Verify the following event logs are centrally captured.Event ID 4738 is created when a user account is modified in Active Directory.Event ID 4728 is created when a member is added to an Active Directory Security Group.Event ID 4729 is created when a member is removed from an Active Directory Security Group.Event ID 4737 is created when a change is made to an Active Directory Security Group. |  |
| ML2-RA-08 | Event logs are protected from unauthorised modification and deletion. | Verify unauthorised users are unable to modify or delete event logs. |  |
| ML2-RA-09 | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Verify the organisation has responded to a sign of compromise in an internet-facing server trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| ML2-RA-10 | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Verify the organisation has identified a cybersecurity incident through the analysis of cybersecurity events. This evidence will typically exist as email correspondence. |  |
| ML2-RA-11 | Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | Verify that cybersecurity incidents are being reporting internally within the organisation. Identify that such reporting is occurring within a reasonable timeframe. This evidence will typically exist as email correspondence or formal briefing material. |  |
| ML2-RA-12 | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Verify that cybersecurity incidents are being reporting to ASD. Identify that such reporting is occurring within a reasonable timeframe. This evidence will typically exist as incident numbers provided by ASD for all reports submitted via ReportCyber. |  |
| ML2-RA-13 | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Verify that the organisation has an up-to-date cybersecurity incident response plan. It should accurately represent processes and procedures following in response to the last cybersecurity incident experienced by the organisation. |  |
| **Application control** | ML2-AC-01 | Application control is implemented on internet-facing servers. | Check whether an in-built or third-party application control solution has been implemented for internet-facing servers. |  |
| ML2-AC-02 | Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients. | If a path-based approach is used for application control, check that it covers all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients. Note, hash-based and publisher-based approaches are system-wide and automatically meet the intent of this control. |  |
| ML2-AC-03 | Microsoft’s recommended application blocklist is implemented. | Attempt to run a binary that is on the recommended application blocklist such as mshta.exe, wmic.exe or wscript.exe.E8MVT will retrieve the latest version of the blocklist from Microsoft. It will compare each of the rules against those configured on the system and return a failed result if any do not match. This will not consider any rules that are determined to be necessary for business purposes and are risk managed. |  |
| ML2-AC-04 | Application control rulesets are validated on an annual or more frequent basis. | Check that the organisation has a process for reviewing the list of allowed applications on an annual or more frequent basis.Check that there is evidence that the organisation has enacted the annual application list review within the last 12 months. |  |
| ML2-AC-05 | Allowed and blocked application control events are centrally logged. | Verify allowed and blocked application control event logs are centrally captured. |  |
| ML2-AC-06 | Event logs are protected from unauthorised modification and deletion. | Verify unauthorised users are unable to modify or delete event logs. |  |
| ML2-AC-07 | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Verify the organisation has responded to a sign of compromise in an internet-facing server trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| ML2-AC-08 | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Verify the organisation has identified a cybersecurity incident through the analysis of cybersecurity events. This evidence will typically exist as email correspondence. |  |
| ML2-AC-09 | Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | Verify that cybersecurity incidents are being reporting internally within the organisation. Identify that such reporting is occurring within a reasonable timeframe. This evidence will typically exist as email correspondence or formal briefing material. |  |
| ML2-AC-10 | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Verify that cybersecurity incidents are being reporting to ASD. Identify that such reporting is occurring within a reasonable timeframe. This evidence will typically exist as incident numbers provided by ASD for all reports submitted via ReportCyber. |  |
| ML2-AC-11 | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Verify that the organisation has an up-to-date cybersecurity incident response plan. It should accurately represent processes and procedures following in response to the last cybersecurity incident experienced by the organisation. |  |
| **Restrict Microsoft Office macros** | ML2-RM-01 | Microsoft Office macros are blocked from making Win32 API calls. | Open a file that contains a Microsoft Office macro that makes a Win32 API call. Do this for all installed Microsoft Office applications. E8MVT can assist with this test. |  |
| **User application hardening** | ML2-AH-01 | Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Use the Microsoft Policy Analyzer to validate the effective state of the system against the Microsoft Edge security baseline.Determine if Google Chrome is configured via group policy settings and if the configured settings are in line with the *Chrome Browser Enterprise Security Configuration Guide* provided by Google at https://support.google.com/chrome/a/answer/9710898?hl=en.In the absence of official Firefox hardening guidance from Mozilla, confirm what hardening has been performed by the organisation. |  |
| ML2-AH-02 | Microsoft Office is blocked from creating child processes. | Open a file that contains a Microsoft Office macro that will create a child process. Confirm it is unable to do this. Check the ASR rule ‘d4f940ab-401b-4efc-aadc-ad5f3c50688a’ is configured in block mode, or another solution is in place to prevent creation of child processes.Running E8MVT will confirm if the ASR rule to prevent creation of child processes is enabled, or if child process creation has been blocked through a PowerShell command. Running E8MVT will execute the following test that opens a file containing a Microsoft Office macro that creates a child process.*$ASR\_Rules = Get-MPPreference | Select -ExpandProperty AttackSurfaceReductionRules\_Ids $match = $falseForeach($rules in $ASR\_Rules) {If ($rules -match "d4f940ab-401b-4efc-aadc-ad5f3c50688a") {$match = $true}}If($match -eq $true) {Write-Output("Block all Office applications from creating child processes (d4f940ab-401b-4efc-aadc-ad5f3c50688a) is enabled")} else {Write-Output("Block all Office applications from creating child processes (d4f940ab-401b-4efc-aadc-ad5f3c50688a) is not present or disabled")}* |  |
| ML2-AH-03 | Microsoft Office is blocked from creating executable content. | Open a file that contains a Microsoft Office macro that will create executable content. Confirm it is unable to do this. Check the ASR rule ‘3b576869-a4ec-4529-8536-b80a7769e899’ is configured in block mode, or another solution is in place to prevent creation of executable content.Running E8MVT will confirm if the ASR rule to creation of executable content is enabled. Running E8MVT will execute the following test that opens a file containing a Microsoft Office macro that creates executable content.*$ASR\_Rules = Get-MPPreference | Select -ExpandProperty AttackSurfaceReductionRules\_Ids $match = $falseForeach($rules in $ASR\_Rules) {If ($rules -match "3b576869-a4ec-4529-8536-b80a7769e899") {$match = $true}}If($match -eq $true) {Write-Output("Block Office applications from creating executable content (3b576869-a4ec-4529-8536-b80a7769e899) is enabled")} else {Write-Output("Block Office applications from creating executable content (3b576869-a4ec-4529-8536-b80a7769e899) is not present or disabled")}* |  |
| ML2-AH-04 | Microsoft Office is blocked from injecting code into other processes. | Open a file that contains a Microsoft Office macro that will inject code into another process. Confirm it is unable to do this. Check the ASR rule ‘75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84’ is configured in block mode, or another solution is in place to prevent code injection.Running E8MVT will confirm if the ASR rule to prevent injection of code into other processes is enabled. Running E8MVT will execute the following test that opens a file containing a Microsoft Office macro that will attempt to inject code into the explorer.exe process.*$ASR\_Rules = Get-MPPreference | Select -ExpandProperty AttackSurfaceReductionRules\_Ids $match = $falseForeach($rules in $ASR\_Rules) {If ($rules -match "75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84") {$match = $true}}If($match -eq $true) {Write-Output("Block Office applications from injecting code into other processes (75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84) is enabled")} else {Write-Output("Block Office applications from injecting code into other processes (75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84) is not present or disabled")}* |  |
| ML2-AH-05 | Microsoft Office is configured to prevent activation of Object Linking and Embedding packages. | Open a file that contains an OLE object. Check the PackagerPrompt registry key within the Trust Center settings is set to 2. E8MVT will check the required registry key.Alternatively, the following PowerShell command can be used.*Get-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\office\16.0\<application>\security\" | Select-Object -Property PackagerPrompt*For example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\office\16.0\excel\security\" | Select-Object -Property PackagerPrompt* |  |
| ML2-AH-06 | Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Use the Microsoft Policy Analyzer to validate the effective state of the system against the Microsoft Office security baseline.For other office productivity suites, determine if suitable vendor hardening guidance is available. Alternatively, confirm what hardening has been performed by the organisation. |  |
| ML2-AH-07 | Office productivity suite security settings cannot be changed by users. | Attempt to modify security settings in Microsoft Office applications. For example, check that the vbawarnings registry key is configured via policy and that a user is unable to change the Microsoft Office macro settings within the Trust Center options. E8MVT will check the required registry key.Alternatively, the following PowerShell command can be used.*Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\<application>\security\" | Select-Object -Property vbawarnings*Example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\" | Select-Object -Property vbawarnings* |  |
| ML2-AH-08 | PDF software is blocked from creating child processes. | Check the ASR rule ‘7674BA52-37EB-4A4F-A9A1-F0F9A1619A2C’ is configured in block mode.Alternatively, Adobe Reader can be tested by opening the application, selecting Open from the File menu, selecting ‘All Files (\*.\*)’ from the dropdown menu in the corner, browsing to the system32 folder and selecting calc.exe to open.Running E8MVT will confirm via the following test if the ASR rule to prevent creation of child processes is enabled.*$ASR\_Rules = Get-MPPreference | Select -ExpandProperty AttackSurfaceReductionRules\_Ids $match = $falseForeach($rules in $ASR\_Rules) {If ($rules -match "7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c") {$match = $true}} If($match = $true) {Write-Output("Block Adobe Reader from creating child processes (7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c) is enabled")} else {Write-Output("Block Adobe Reader from creating child processes (7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c) is not present or disabled")}* |  |
| ML2-AH-09 | PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Determine the PDF software in use and if the vendor provides hardening guidance for that product. Follow the guidance to determine if the product has been hardened.Adobe Acrobat and Adobe Reader hardening guidance can be found at https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html. |  |
| ML2-AH-10 | PDF software security settings cannot be changed by users. | Attempt to modify security settings within allowed PDF readers. For example, by disabling sandbox protections in Adobe Reader. |  |
| ML2-AH-11 | PowerShell module logging, script block logging and transcription events are centrally logged. | E8MVT is able to check the registry settings for this control.Alternatively, within the RSoP report, look for the *Turn on Module Logging*, *Turn on PowerShell Script Block Logging* and *Turn on PowerShell Transcription* settings at *Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell*. They should all be enabled. In addition, module logging should ideally be configured to log all modules (i.e. ‘\*’), although an organisation may tailor this setting.Finally, determine if these event logs are being centrally stored. |  |
| ML2-AH-12 | Command line process creation events are centrally logged. | E8MVT is able to check the registry settings for this control.Alternatively, within the RSoP report, look for the *Audit Process Creation* setting at *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\*. It should be enabled with a value of *Success*. In addition, look for the *Include command line in process creation events* setting at *Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation*. It should be enabled.Finally, determine if these event logs are being centrally stored. |  |
| ML2-AH-13 | Event logs are protected from unauthorised modification and deletion. | Verify unauthorised users are unable to modify or delete event logs. |  |
| ML2-AH-14 | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Verify the organisation has responded to a sign of compromise in an internet-facing server trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| ML2-AH-15 | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Verify the organisation has identified a cybersecurity incident through the analysis of cybersecurity events. This evidence will typically exist as email correspondence. |  |
| ML2-AH-16 | Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | Verify that cybersecurity incidents are being reporting internally within the organisation. Identify that such reporting is occurring within a reasonable timeframe. This evidence will typically exist as email correspondence or formal briefing material. |  |
| ML2-AH-17 | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Verify that cybersecurity incidents are being reporting to ASD. Identify that such reporting is occurring within a reasonable timeframe. This evidence will typically exist as incident numbers provided by ASD for all reports submitted via ReportCyber. |  |
| ML2-AH-18 | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Verify that the organisation has an up-to-date cybersecurity incident response plan. It should accurately represent processes and procedures following in response to the last cybersecurity incident experienced by the organisation. |  |
| **Regular backups** | ML2-RB-01 | Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts. | Verify access controls restrict the access of backups to the owner of the backup and backup administrator accounts. |  |
| ML2-RB-02 | Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups. | Verify access controls restrict the modification and deletion of backups to backup administrator accounts. |  |