# Example Essential Eight Assessment Test Plan – Maturity Level Three

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mitigation Strategy** | **Test ID** | **Control Description** | **Test Methodology** | **Test Findings** |
| **Patch applications** | ML3-PA-01 | Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | Use a vulnerability scanner to identify the listed applications within the environment and check that they have been patched against a critical vulnerability or known working exploit. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than 48 hours. |  |
| ML3-PA-02 | Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | Use a vulnerability scanner to identify the listed applications within the environment and check that they have been patched against a non-critical vulnerability that has no known working exploits. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than two weeks. |  |
| ML3-PA-03 | Applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed. | Use a vulnerability scanner to identify the listed applications within the environment and check they are still vendor supported. |  |
| **Patch operating systems** | ML3-PO-01 | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers. | Observe a vulnerability scan, or request evidence of previous vulnerability scans, and note the date/time stamp and scope. Check whether the vulnerability scan attempted to identify out-of-date drivers in operating systems. |  |
| ML3-PO-02 | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware. | Observe a vulnerability scan, or request evidence of previous vulnerability scans, and note the date/time stamp and scope. Check whether the vulnerability scan attempted to identify out-of-date firmware for devices. |  |
| ML3-PO-03 | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | Use a vulnerability scanner to check whether operating systems for workstations, non-internet-facing servers and non-internet-facing network devices have been patched against a critical vulnerability or known working exploit. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than 48 hours. |  |
| ML3-PO-04 | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | Use a vulnerability scanner to check whether operating systems for workstations, non-internet-facing servers and non-internet-facing network devices have been patched against a non-critical vulnerability that has no known working exploits. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than one month. |  |
| ML3-PO-05 | Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | Use a vulnerability scanner to check whether drivers for operating systems have been updated to mitigate a critical vulnerability or known working exploit. Determine the date the driver update was installed and compare to when the driver was made available. Check that the gap between is not greater than 48 hours. |  |
| ML3-PO-06 | Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | Use a vulnerability scanner to check whether drivers for operating systems have been updated to mitigate a non-critical vulnerability that has no known working exploits. Determine the date the driver update was installed and compare to when the driver was made available. Check that the gap between is not greater than one month. |  |
| ML3-PO-07 | Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | Use a vulnerability scanner to check whether firmware for devices has been updated to mitigate a critical vulnerability or known working exploit. Determine the date the firmware update was installed and compare to when the firmware was made available. Check that the gap between is not greater than 48 hours. |  |
| ML3-PO-08 | Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | Use a vulnerability scanner to check whether firmware for devices has been updated to mitigate a non-critical vulnerability that has no known working exploits. Determine the date the firmware update was installed and compare to when the firmware was made available. Check that the gap between is not greater than one month. |  |
| ML3-PO-09 | The latest release, or the previous release, of operating systems are used. | Query Active Directory using PowerShell commands or tools such as ADRecon or BloodHound to identify operating system versions within the environment. |  |
| **Multi-factor authentication** | ML3-MF-01 | Multi-factor authentication is used to authenticate users of data repositories. | Verify both a privileged and unprivileged user is presented with a MFA challenge when authenticating to data repositories. |  |
| ML3-MF-02 | Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant. | Verify MFA for customers of online customer services uses either security keys, smart cards or passkeys. |  |
| ML3-MF-03 | Multi-factor authentication used for authenticating users of data repositories is phishing-resistant. | Verify MFA for users of data repositories uses either security keys, smart cards or Windows Hello for Business. |  |
| ML3-MF-04 | Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events. | Verify the organisation has responded to a sign of compromise in a non-internet-facing server trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| ML3-MF-05 | Event logs from workstations are analysed in a timely manner to detect cyber security events. | Verify the organisation has responded to a sign of compromise in a workstation trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| **Restrict administrative privileges** | ML3-RA-01 | Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties. | Review the privileged users of systems, applications and data repositories. Ensure their assigned privileges match their expected duties and role. Query Active Directory using PowerShell commands or tools such as BloodHound and ADRecon to identify users with more privileges than required in their role. Ensure privileged Active Directory groups such as Domain Administrators have limited membership. |  |
| ML3-RA-02 | Secure Admin Workstations are used in the performance of administrative activities. | Verify that the principles of Secure Admin Workstations are being applied to privileged operating environments. For example, by minimising the attack surface as much as possible by removing unnecessary functionality and hardening configurations through the use of ASD and vendor hardening guides.  Note, this control doesn’t necessary require that dedicated physical devices be used exclusively for privileged operating environments. |  |
| ML3-RA-03 | Just-in-time administration is used for administering systems and applications. | Query Active Directory using PowerShell commands or tools such as ADRecon to identify privileged users and groups. Consider some users may currently have just-in-time access and ensure they are not permanently members of a privileged group.  Review evidence of valid use of this system, such as service requests or support tickets. Look for evidence of this solution being bypassed, such as users in privileged groups for extended periods of time. Ensure the system configuration meets the intent of this control, such as limiting who can receive privileged access. |  |
| ML3-RA-04 | Memory integrity functionality is enabled. | Check the registry setting at *HKLM:\SYSTEM\CurrentControlSet\Control\* *DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity\* and confirm that Enabled is set to 0 or 1.  E8MVT is able to check the registry setting for this control.  *Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity\" | Select-Object -Property Enabled* |  |
| ML3-RA-05 | Local Security Authority protection functionality is enabled. | Check the registry setting at *HKLM:\SYSTEM\CurrentControlSet\Control\LSA\* and confirm that RunAsPPL is set to 1 or 2.  E8MVT is able to check the registry setting for this control.  *Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\LSA\" | Select-Object -Property RunAsPPL* |  |
| ML3-RA-06 | Credential Guard functionality is enabled. | Check the registry setting at *HKLM:\SYSTEM\CurrentControlSet\Control\LSA\* and confirm that LsaCfgFlags is set to 1 or 2.  E8MVT is able to check the registry setting for this control.  *Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\LSA\" | Select-Object -Property lsacfgflags* |  |
| ML3-RA-07 | Remote Credential Guard functionality is enabled. | Check the registry setting at *HKLM:\SYSTEM\CurrentControlSet\Control\LSA\* and confirm that DisableRestrictedAdmin is set to 0.  E8MVT is able to check the registry setting for this control.  *Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\LSA\" | Select-Object -Property DisabledRestrictedAdmin* |  |
| ML3-RA-08 | Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events. | Verify the organisation has responded to a sign of compromise in a non-internet-facing server trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| ML3-RA-09 | Event logs from workstations are analysed in a timely manner to detect cyber security events. | Verify the organisation has responded to a sign of compromise in a workstation trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| **Application control** | ML3-AC-01 | Application control is implemented on non-internet-facing servers. | Check whether an in-built or third-party application control solution has been implemented for non-internet-facing servers. |  |
| ML3-AC-02 | Application control restricts the execution of drivers to an organisation-approved set. | Determine the extent in which the organisation is approving the use of specific drivers in their environment. At a minimum, the organisation may make a risk-based decision to allow all drivers except for those on Microsoft’s vulnerable driver blocklist. |  |
| ML3-AC-03 | Microsoft’s vulnerable driver blocklist is implemented. | Attempt to install a driver that is on the vulnerable driver blocklist. Verify rules for the blocked drivers exist in an application control configuration and that they are enforced. Alternatively, check whether memory integrity has been enabled via the Windows Security app as this will automatically enforce the vulnerable driver blocklist.  E8MVT will retrieve the latest version of the vulnerable driver 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. |  |
| ML3-AC-04 | Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events. | Verify the organisation has responded to a sign of compromise in a non-internet-facing server trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| ML3-AC-05 | Event logs from workstations are analysed in a timely manner to detect cyber security events. | Verify the organisation has responded to a sign of compromise in a workstation trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| **Restrict Microsoft Office macros** | ML3-RM-01 | Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute. | Attempt to execute Microsoft Office macros from untrusted locations (if configured).  OR  Attempt to execute signed and unsigned Microsoft Office macros from untrusted publishers (if configured).  OR  Determine if a sandbox solution is in place and effective for Microsoft Office. Note, Application Guard for Office automatically blocks the execution of Microsoft Office macros rather than running them within a sandboxed environment. |  |
| ML3-RM-02 | Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations. | If digital signatures or Trusted Locations are used by the organisation, verify that a process exists for checking that Microsoft Office macros are free of malicious code. |  |
| ML3-RM-03 | Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations. | If Trusted Locations are used by the organisation, verify that a process exists for controlling write access to these locations.  Trusted Locations for each Microsoft Office application can be obtained from the registry at *HKCU:\software\microsoft\office\<version>\<product>\security\trusted locations*.  The following PowerShell command can be used to obtain a list of Trusted Locations.  *Get-ItemProperty -Path "HKCU:\SOFTWARE\policies\microsoft\office\<version>\<product>\security\trusted locations"*  As a standard user attempt to write a file to each of these locations.  E8MVT will find configured Trusted Locations and attempt to write a file to each location. |  |
| ML3-RM-04 | Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View. | Attempt to execute Microsoft Office macros in a Microsoft Office file signed by an untrusted publisher.  Check the *trustbar* value is set to 1 at the following registry location.  *HKCU:\Software\Microsoft\Office\16.0\Common\TrustCenter\*  Check the following registry entry for each Microsoft Office application to confirm that the TCID19092 value has been set.  *HKCU\SOFTWARE\Policies\Microsoft\office\<version>\<product>\disabledcmdbaritemslist*  The following PowerShell commands can also be used.  *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\Common\TrustCenter\" | Select-Object -Property trustbar*  *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\<version>\<product>\" | Select-Object -Property disabledcmdbaritemslist*  For example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\word\" | Select-Object -Property disabledcmdbaritemslist* |  |
| ML3-RM-05 | Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View. | If digital signatures are used by the organisation, verify that only V3 signatures are supported.  The following PowerShell command be used to confirm this.  *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\VBA\security\" | Select-Object -Property onlytrustvbasignaturev3* |  |
| ML3-RM-06 | Microsoft Office’s list of trusted publishers is validated on an annual or more frequent basis. | If digital signatures are used by the organisation, verify that a process is in place to regularly review this list to allow/remove trusted publishers. Request evidence of an annual validation having taken place.  Ideally, the organisation should re-sign all approved Microsoft Office macros obtained from external parties, after appropriate checks have taken place, and only list certificates they control within the trusted publishers list. |  |
| **User application hardening** | ML3-AH-01 | .NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed. | Select the ‘Turn Windows Features on or off’ option from the Control Panel and confirm that *.NET Framework (includes .NET 2.0 and 3.0)* is not selected.  Check the registry keys below for the existence of older .NET Frameworks.  E8MVT will check this location to determine if older .NET Framework versions exist on the system.  *Get-ChildItem -Path "HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP"*  *Get-ChildItem -Path "HKLM:\Software\Microsoft\.NETFramework\Policy\"* |  |
| ML3-AH-02 | Windows PowerShell 2.0 is disabled or removed. | Select the ‘Turn Windows Features on or off’ option from the Control Panel and confirm that *Windows PowerShell 2.0* is not selected.  Run the following PowerShell command *Get-ChildItem "HKLM:\SOFTWARE\Microsoft" -Recurse -Include PowerShellEngine* and confirm that version 2.0 is not found in the results.  The PowerShell command $PSVersionTable will display a list of supported PowerShell versions. Ensure that 2.0 and below is not part of this list. The command *$PSVersionTable.PSVersion.Major* can be used to confirm the running version.  E8MVT will check the described registry key to locate old PowerShell versions.  *Get-ChildItem "HKLM:\SOFTWARE\Microsoft\Powershell" -Recurse -Include PowerShellEngine*  Enter *powershell -Version 2* into a PowerShell prompt to check if the system can be downgraded. |  |
| ML3-AH-03 | PowerShell is configured to use Constrained Language Mode. | Run *$ExecutionContext.SessionState.LanguageMode* in PowerShell to check if Constrained Language Mode is configured. If Constrained Language Mode is configured this should return ‘ConstrainedLanguage’.  E8MVT will not run if the system is configured for Constrained Language Mode. |  |
| ML3-AH-04 | Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events. | Verify the organisation has responded to a sign of compromise in a non-internet-facing server trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| ML3-AH-05 | Event logs from workstations are analysed in a timely manner to detect cyber security events. | Verify the organisation has responded to a sign of compromise in a workstation trigged by monitoring activities. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments. |  |
| **Regular backups** | ML3-RB-01 | Unprivileged accounts cannot access their own backups. | Verify access controls restrict unprivileged users from accessing backups. |  |
| ML3-RB-02 | Privileged accounts (excluding backup administrator accounts) cannot access their own backups. | Verify access controls restrict privileged users (excluding backup administrator accounts) from accessing backups. |  |
| ML3-RB-03 | Backup administrator accounts are prevented from modifying and deleting backups during their retention period. | Verify access controls restrict the modification and deletion of backups during their retention period to only break glass accounts. |  |