Maturity Level Three

The focus of this maturity level is malicious actors who are more adaptive and much less reliant on public tools and techniques. These malicious actors are able to exploit the opportunities provided by weaknesses in their target's cyber security posture, such as the existence of older software or inadequate logging and monitoring. Malicious actors do this to not only extend their access once initial access has been gained to a target, but to evade detection and solidify their presence. Malicious actors make swift use of exploits when they become publicly available as well as other tradecraft that can improve their chance of success.

Generally, malicious actors may be more focused on particular targets and, more importantly, are willing and able to invest some effort into circumventing the idiosyncrasies and particular policy and technical controls implemented by their targets. For example, this includes socially engineering a user to not only open a malicious document but also to unknowingly assist in bypassing controls. This can also include circumventing stronger multi-factor authentication by stealing authentication token values to impersonate a user. Once a foothold is gained on a system, malicious actors will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks. Depending on their intent, malicious actors may also destroy all data (including backups).

The guidance below outlines the requirements to be assessed in addition to the requirements of the previous maturity level. In doing so, assessments against Maturity Level Three should focus on the delta between Maturity Level Two and Maturity Level Three.

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	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.
	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Mitigation Strategy	Description
	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.
	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.
	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.
	Online services that are no longer supported by vendors are removed.
	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.
	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.
Patch operating systems	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	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.

Mitigation Strategy	Description
	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.
	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.
	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.
	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.
	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.
	The latest release, or the previous release, of operating systems are used.
	Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.
	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.
	Multi-factor authentication is used to authenticate privileged users of systems.
	Multi-factor authentication is used to authenticate unprivileged users of systems.
	Multi-factor authentication is used to authenticate users of data repositories.
	Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.
	Multi-factor authentication used for authenticating users of online services is phishing-resistant.
	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.

Mitigation Strategy	Description
	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
	Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.
	Successful and unsuccessful multi-factor authentication events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from workstations are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict administrative privileges	Requests for privileged access to systems, applications and data repositories are validated when first requested.
	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.
	Privileged access to systems and applications is disabled after 45 days of inactivity.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
	Secure Admin Workstations are used in the performance of administrative activities.
	Privileged users use separate privileged and unprivileged operating environments.
	Privileged operating environments are not virtualised within unprivileged operating environments.
	Unprivileged user accounts cannot logon to privileged operating environments.
	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
	Just-in-time administration is used for administering systems and applications.
	Administrative activities are conducted through jump servers.

Mitigation Strategy	Description
	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
	Memory integrity functionality is enabled.
	Local Security Authority protection functionality is enabled.
	Credential Guard functionality is enabled.
	Remote Credential Guard functionality is enabled.
	Privileged access events are centrally logged.
	Privileged user account and security group management events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from workstations are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Application control	Application control is implemented on workstations.
	Application control is implemented on internet-facing servers.
	Application control is implemented on non-internet-facing servers.
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
	Application control restricts the execution of drivers to an organisation-approved set.
	Microsoft’s recommended application blocklist is implemented.
	Microsoft’s vulnerable driver blocklist is implemented.
	Application control rulesets are validated on an annual or more frequent basis.
	Allowed and blocked application control events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.

Mitigation Strategy	Description
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from workstations are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict Microsoft Office macros	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
	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.
	Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.
	Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.
	Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.
	Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.
	Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.
	Microsoft Office macros in files originating from the internet are blocked.
	Microsoft Office macro antivirus scanning is enabled.
	Microsoft Office macros are blocked from making Win32 API calls.
	Microsoft Office macro security settings cannot be changed by users.
User application hardening	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Web browser security settings cannot be changed by users.
	Microsoft Office is blocked from creating child processes.
	Microsoft Office is blocked from creating executable content.

Mitigation Strategy	Description
	Microsoft Office is blocked from injecting code into other processes.
	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Office productivity suite security settings cannot be changed by users.
	PDF software is blocked from creating child processes.
	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	PDF software security settings cannot be changed by users.
	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.
	Windows PowerShell 2.0 is disabled or removed.
	PowerShell is configured to use Constrained Language Mode.
	PowerShell module logging, script block logging and transcription events are centrally logged.
	Command line process creation events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from workstations are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.
	Unprivileged user accounts cannot access their own backups.

Mitigation Strategy	Description
	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.
	Privileged user accounts (excluding backup administrator accounts) cannot access their own backups.
	Unprivileged user accounts are prevented from modifying and deleting backups.
	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.
	Backup administrator accounts are prevented from modifying and deleting backups during their retention period.

MATURITY LEVEL THREE – DEEP DIVE

Patch applications

Context

At this maturity level, patches, updates or other vendor mitigations should be applied within 48 hours for office productivity suites, web browsers and their extensions, email clients, PDF software, and security products when vulnerabilities are assessed as critical by vendors or when working exploits exist. In addition, all applications that are no longer supported by vendors should be removed from systems.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting an assessment method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
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 the relevant guidance provided in Maturity Level One of this guide but apply 48 hour timeframes when vulnerabilities are assessed as critical by vendors or when working exploits exist.
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 the relevant guidance provided in Maturity Level One of this guide when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
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 the relevant guidance provided in Maturity Level One of this guide and extend it to all applications.

Patch operating systems

Context

At this maturity level, patches, updates or other vendor mitigations should be applied within 48 hours for operating systems of workstations, servers and network devices when vulnerabilities are assessed as critical by vendors or when working exploits exist. In addition, vulnerabilities in drivers and firmware should be mitigated at this maturity level.

Modern operating systems for workstations, servers and network devices often contain security functionality that is not available in earlier releases, even if those earlier releases remain supported by vendors. It is important that an organisation takes advantage of new security functionality in later releases of operating systems to further mitigate malicious actors' activities.

The latest release of Microsoft Windows and Microsoft Server will depend on the servicing branch being used. Further release information is available from Microsoft. Similar information is often available from vendors of other operating systems and network devices.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.	Use the relevant guidance provided in Maturity Level One of this guide but apply vulnerability scanning activities to drivers.
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.	Use the relevant guidance provided in Maturity Level One of this guide but apply vulnerability scanning activities to firmware.
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 the relevant guidance provided in Maturity Level One of this guide but apply 48 hour timeframes when vulnerabilities are assessed as critical by vendors or when working exploits exist.
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 the relevant guidance provided in Maturity Level One of this guide when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
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 the relevant guidance provided in Maturity Level One of this guide and apply 48 hour timeframes when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control	Assessment Guidance (ordered by effectiveness)
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 the relevant guidance provided in Maturity Level One of this guide when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
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 the relevant guidance provided in Maturity Level One of this guide and apply 48 hour timeframes when vulnerabilities are assessed as critical by vendors or when working exploits exist.
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 the relevant guidance provided in Maturity Level One of this guide when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
The latest release, or the previous release, of operating systems are used.	A network-based vulnerability scanner can be used to identify operating systems and their versions. The output of these tools can then be used to check against the latest operating system versions available from vendors.
	For Microsoft Windows workstations and servers, the ‘winver’ command can be run to determine the version of the operating system. Request a screenshot of the output of running this command for servers and workstations (assuming a SOE is used for workstations). For Linux workstations and servers, the ‘cat /etc/os-release’ command can be run to determine the version of the operating system. Request a screenshot of the output of running this command for servers and workstations (assuming a SOE is used for workstations). This version can then be checked against release information for the Linux distribution being used to determine whether it is a supported version or not.

Multi-factor authentication

Context

At this maturity level, users of data repositories should be using phishing-resistant multi-factor authentication. In addition, customers of online customer services should be using phishing-resistant multi-factor authentication, rather than just being offered it as an option.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Multi-factor authentication is used to authenticate users of data repositories.	Request a list of data repositories for the system and associated screenshots of users attempting to access each of these data repositories. The screenshots should show multiple forms of authentication being requested.
Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.	Observe a customer user account authenticating to any of the organisation's online customer services that process, store or communicate sensitive customer data, as well as any third-party online customer services that process, store or communicate sensitive customer data. Check whether they are required to use a phishing-resistant form of multi-factor authentication, such as a security key, smart card or passkey.
Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.	Observe both unprivileged and privileged users authenticating to a data repository. Check whether they are required to use a phishing-resistant form of multi-factor authentication, such as a security key, smart card or passkey.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Event logs from workstations are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).

Restrict administrative privileges

Context

Personnel seeking access to systems, applications and data repositories, especially with privileged access, should have a genuine business requirement to do so. Once a requirement to access a system, application or data repository is established, users should be provided with only the privileges they require to undertake their duties. This can be achieved using role-based access controls.

While lower maturity levels required the use of privileged operating environments for administrative activities, they did not require Secure Admin Workstations (SAWs) to be implemented for such environments. However, at this maturity level, a concerted effort should be made to apply the principles associated with SAWs to such environments to ensure that their attack surface is reduced as much as possible. This includes hardening operating systems, including removing all unnecessary functionality. Note, this does not necessarily require separate physical machines to be used for privileged operating environments.

Just-in-time (JIT) privileged access management (PAM) is an extension of role-based access control in which privileged users are only granted the access required to perform their duties immediately before that access is required and for only as long as it is required.

Within an active user session, credentials are cached within the Local Security Authority System Service process to allow for access to network resources without users having to repeatedly enter their credentials. Local Security Authority protection functionality and Credential Guard are designed to assist in protecting this process. Remote Credential Guard provides a similar functionality for remote access. In addition, memory integrity helps protect the overall integrity of systems.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	**Assessment Guidance (ordered by effectiveness)**
Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.	Discuss the approach that the organisation has taken to restrict privileged users to only what is required for them to undertake their duties. Often this will involve identifying several different roles, developing policies for those roles and assigning privileged users to one or more of those roles depending on their duties. A system administrator should be able to demonstrate the different user groups and policies or access controls that apply to each. This can confirmed via an RSoP report.
Secure Admin Workstations are used in the performance of administrative activities.	Consider the extent to which the principles associated with SAWs have been applied to privileged operating environments. This includes whether ASD hardening guidance and vendor hardening guidance for operating systems has been applied. Furthermore, determine if a concerted effort has been made to reduce the attack surface of such environments as much as possible. Note, this does not necessarily require separate physical machines to be used for privileged operating environments.
Just-in-time administration is used for administering systems and applications.	The implementation of JIT PAM is a complex activity that forms the basis for restricting administrative privileges at this maturity level. Given the complex nature of JIT PAM, it will become apparent from discussions with system administrators as to whether a JIT PAM approach has been adopted or not. In doing so, it may be worthwhile observing the process of a system administrator requesting and being granted JIT access.

Control	Assessment Guidance (ordered by effectiveness)
Memory integrity functionality is enabled.	Within the RSoP report, look for the 'Turn On Virtualization Based Security' setting at 'Computer Configuration\Policies\Administrative Templates\System\Device Guard\'. It should be enabled with a value of 'Virtualization Based Protection of Code Integrity: Enabled with UEFI lock'.
Local Security Authority protection functionality is enabled.	Within the RSoP report, look for the 'Configure LSASS to run as a protected process' setting at 'Computer Configuration\Policies\Administrative Templates\System\Local Security Authority\'. It should be enabled with a value of 'Configure LSA to run as a protected process: Enabled with UEFI lock'.
Credential Guard functionality is enabled.	Within the RSoP report, look for the 'Turn On Virtualization Based Security' setting at 'Computer Configuration\Policies\Administrative Templates\System\Device Guard\'. It should be enabled with a value of 'Credential Guard Configuration: Enabled with UEFI lock'.
Remote Credential Guard functionality is enabled.	Within the RSoP report, look for the 'Restrict delegation of credentials to remote servers' setting at 'Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\'. It should be enabled with a value of 'Use the following restricted mode: Require Remote Credential Guard'.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Event logs from workstations are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).

Application control

Context

At this maturity level, a requirement is introduced relating to the use of application control for non-internet-facing servers. In addition, the scope of application control implementations is expanded to include drivers. Note, while Microsoft AppLocker does not currently support the control of drivers, Windows Defender Application Control does. However, Microsoft AppLocker can be used if Microsoft's vulnerable driver blocklist is also enforced via Microsoft Window's memory integrity functionality, assuming an organisation is willing to accept the risk of all other drivers being able to execute.

Microsoft maintains a list of vulnerable drivers that have been discovered by security researchers. Implementing Microsoft's vulnerable driver blocklist can help to provide protection from malicious actors that would have sought to use these against an otherwise robust application control implementation in order to gain access to a system.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Application control is implemented on non-internet-facing servers.	Check whether an application control solution has been implemented on non-internet-facing servers.
Application control restricts the execution of drivers to an organisation-approved set.	Depending on the application control solution, controlling the execution of drivers may or may not be supported. Request a copy of application control rulesets to check for the inclusion of drivers.
Microsoft's vulnerable driver blocklist is implemented.	Check whether memory integrity has been enabled via the Windows Security app as this will automatically enforce Microsoft's vulnerable driver blocklist.
	Depending on the application control solution, controlling the execution of drivers may or may not be supported. Request a copy of application control rulesets to check for drivers. If driver rules are included, check whether Microsoft's vulnerable driver blocklist has been specified.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Event logs from workstations are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).

Restrict Microsoft Office macros

Context

Disabling the use of Microsoft Office macros represents an optimal security outcome, however, some users will have a demonstrated business requirement for their use. In such situations, additional controls should be implemented to make the use of Microsoft Office macros as secure as possible. This may include either running Microsoft Office macros from within a sandboxed environment, from an appropriately controlled Trusted Location or ensuring they are digitally signed by a trusted publisher using V3 signatures.

As Microsoft Office allows any files that are opened from a Trusted Location to bypass security checks, it is critical that only trusted users can write to or modify content in these locations. Under no circumstances should Trusted Locations be specified within a user's profile, such as their desktop or documents folders.

If the 'Disable all macros except digitally signed macros' setting is used, this will allow any Microsoft Office macro signed by a trusted publisher to execute without prompting the user for permission. However, any Microsoft Office macro that is digitally signed by an untrusted publisher will ask users to decide whether they would like to allow the Microsoft Office macro to execute via the Message Bar or Backstage View. While this prompt can be disabled using a group policy setting, the removal of the option to enable Microsoft Office macros via the Backstage View requires the implementation of an undocumented graphical user interface setting.

When implementing a digitally signed Microsoft Office macro approach, an organisation may identify a list of trusted publishers but fail to review and validate the list on a regular basis for its correctness and ongoing suitability. This can create issues when a vendor's code-signing certificate is compromised. Ideally, an organisation should acquire their own code-signing certificate and re-sign any Microsoft Office macros they trust using V3 signatures, even if already signed by a third party. While introducing additional overhead, this mitigates the risk of potentially trusting compromised third-party code-signing certificates.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	**Assessment Guidance (ordered by effectiveness)**
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.	Within the RSoP report, look for the 'VBA Macro Notification Settings' setting at 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Application Settings\Security\Trust Center\'. It should be enabled and configured to 'Disable all macros without notification' (if Trusted Locations are used) or 'Disable all macros except digitally signed macros' (if digitally signed Microsoft Office macros are used). Note, an organisation may choose to use a combination of Trusted Locations and digitally signed Microsoft Office macros. However, if only digitally signed Microsoft Office macros are used then Trusted Locations should be disabled.
	Within each Microsoft Office application, request a screenshot showing Trust Center macro settings (File – Options – Trust Center – Trust Center Settings – Macro Settings). In addition, request a screenshot showing Trust Center trusted

Control	Assessment Guidance (ordered by effectiveness)
	publisher settings (File – Options – Trust Center – Trust Center Settings – Trusted Publishers). For the assessment of Microsoft Office macro security, identify what setting is selected for 'macro settings'. The setting should either be set to 'Disable all macros without notification' (if Trusted Locations are used) or 'Disable all macros except digitally signed macros' (if digitally signed Microsoft Office macros are used). For the assessment of Trusted Locations, check whether the 'Disable all trusted locations' option has been checked or not. If it has not, then Trusted Locations are enabled and should be individually assessed for their suitability.
Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.	Identify users that are responsible for the management of Microsoft Office macros. Discuss with them the processes and procedures that are used to check whether Microsoft Office macros are free of malicious code before they are either digitally signed to placed within Trusted Locations.
Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.	For each Trusted Location that is specified, review the effective file system permissions for that location. If able to, review file system permissions themselves rather than requesting a screenshot. Check the total number of users who are in user groups that have the relevant file system permissions to make changes to content in Trusted Locations.
Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.	Within the RSoP report, look for the 'Disable all Trust Bar notifications for security issues' setting at 'User Configuration\Policies\Administration Templates\Microsoft Office 2016\Security Settings\'. It should be enabled. In addition, look for the 'Disable commands' setting at 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Disable Items in User Interface\Custom\'. It should be enabled with a value of 'Enter a command bar ID to disable: 19092'.
Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.	Within the RSoP report, look for the 'Only trust VBA macros that use V3 signatures' setting at 'User Configuration\Policies\Administration Templates\Microsoft Office 2016\Security Settings\Trust Centre\'. It should be enabled.
Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.	For the assessment of trusted publishers, check which publishers are listed. Ideally, this should only be a code-signing certificate belonging to the organisation. Alternatively, if external vendors' code-signing certificates are listed, discuss how often these are reviewed

Control	Assessment Guidance (ordered by effectiveness)
	and validated, including what mechanisms are used to identify when/if these need to be removed due to compromise by malicious actors as part of cyber supply chain attacks.

User application hardening

Context

.NET Framework 3.5 (including .NET 2.0 and 3.0) is often targeted by malicious actors due to its lack of security functionality when compared to newer versions of the .NET Framework. Within Microsoft Windows, there are two separate features relating to the .NET Framework, '.NET Framework 3.5 (includes .NET 2.0 and .NET 3.0)' and '.NET Framework 4.8 Advanced Services'.

Microsoft ended support for Windows PowerShell 2.0 in late 2017. At that time, Microsoft noted that Windows PowerShell 2.0 lacked the security functionality of Windows PowerShell 5.0 and higher.

Constrained Language Mode for PowerShell is designed to prevent PowerShell users (which may include malicious actors) from running tools that exploit PowerShell or load Component Object Model objects, libraries and classes into a PowerShell session.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.	Request a screenshot of the 'Windows Features' that are installed. For Microsoft Windows 11, this can be accessed via (Settings – Apps – Optional features – More Windows features). For Microsoft Windows 10, this can be accessed via (Settings – Apps & features – Programs and Features – Turn Windows features on or off). Check which of the .NET Frameworks are installed by checking for a tick or black square. Note, enabling .NET Framework 3.5 will automatically enable PowerShell 2.0.
Windows PowerShell 2.0 is disabled or removed.	Request a screenshot of the 'Windows Features' that are installed.

Control	Assessment Guidance (ordered by effectiveness)
	For Microsoft Windows 11, this can be accessed via (Settings – Apps – Optional features – More Windows features). For Microsoft Windows 10, this can be accessed via (Settings – Apps & features – Programs and Features – Turn Windows features on or off). Check if legacy versions of PowerShell are installed by checking for a tick or black square against 'Windows PowerShell 2.0'. To check if a downgrade to PowerShell 2.0 is available, run the following PowerShell command: *Get-WindowsOptionalFeature -online* | *Where-Object {$_.FeatureName -match "PowerShellv2"}*
PowerShell is configured to use Constrained Language Mode.	Request a screenshot of the output of running the following PowerShell command: *$ExecutionContext.SessionState.LanguageMode*. If Constrained Language Mode is enabled, the output will be 'ConstrainedLanguage'. Otherwise, the output will be 'FullLanguage'.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Event logs from workstations are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).

Regular backups

Context

At this maturity level, only a subset of privileged user accounts (i.e. backup administrator accounts) should be able to access backups. The increasing level of control over which user accounts can access backups, and to what extent, progressively limits the damage that may be caused by a ransomware attack.

In addition, at this maturity level, all user accounts (except for break glass accounts) should not be able to modify and delete backups.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	**Assessment Guidance (ordered by effectiveness)**
Unprivileged user accounts cannot access their own backups.	Use the guidance provided in Maturity Level One of this guide but apply the more restrictive access control requirements. Specifically, unprivileged user accounts should no longer be able to access their own backups.
Privileged user accounts (excluding backup administrator accounts) cannot access their own backups.	Use the guidance provided in Maturity Level One of this guide but apply the more restrictive access control requirements. Specifically, privileged user accounts (excluding backup administrator accounts) should no longer be able to access their own backups. Active Directory queries and tools such as BloodHound can help to identify privileged user accounts including backup administrator accounts.
Backup administrator accounts are prevented from modifying and deleting backups during their retention period.	Use the guidance provided in Maturity Level One of this guide but apply the more restrictive access control requirements. Specifically, backup administrator accounts should no longer be able to modify and delete backups during their retention period, but may do so after the retention period has been exceeded. The modification and deletion of backups during their retention period, should such activities be required, need to be restricted to break glass accounts. Active Directory queries and tools such as BloodHound can help to identify privileged user accounts (including backup administrator accounts) and break glass accounts.