VOLKIS™

Volkis Sample Essential 8 Report

Prepared for ACME Enterprises, 28 April 2022

Table of Contents

Executive summary

This is a sample **Essential 8 Assessment** report from **Volkis**. It has been designed to be similar to the report provided at the end of an assessment performed against the ACSC Essential 8 Maturity Model.

The report includes helpful overviews and charts summarising your compliance with the requirements of the standard. An attached spreadsheet will list the individual requirements in detail, providing evidence, details, and recommendations for how your organisation complies with each requirement.

ACME Enterprises engaged Volkis to perform an assessment against the Essential 8 Cyber Security Maturity Model that is developed and released by the Australian Cyber Security Centre (ACSC). This model comprises 8 technical security controls that the ACSC thinks are appropriate for all organisations in Australia and is backed by the federal government and Australian Signals Directorate.

Currently two controls, “Patch applications” and “Multi-factor authentication” are at the highest maturity level of 3, while “Regular backups”, “Patch operating systems” and “Configure Microsoft Office macro settings” are at maturity level 2. Three controls, “Application control”, “User application hardening” and “Restrict administrative privileges” failed to meet the requirements to reach maturity level 1.

Application control is currently not installed at all in ACME Enterprises. This control will prevent malware from being executed on user devices and servers, providing effective defence against phishing attacks and malicious software packages.

Additional activities will boost compliance with the Essential 8:

- Restricting the execution of applications and other executables to those on an organisation approved list. This will elevate the “Application control” to maturity level 2.
- Follow vendor hardening guidance for Microsoft Office and PDF software, and implementing advertisement blocking in web browsers to meet maturity level 2 of “User application hardening”.

- Restrict the use of privileged accounts, ensuring restrictions are in place as to systems they can access. Remove the ability to access the Internet, email or other web services and implement a review process to remove additional privileges when not required. Following the recommendations in this report will increase “Restrict administrative privileges” to maturity level 2.

Volkis recommends ACME Enterprises aims to meet compliance with a maturity level of 2 across the IT environment. By following the recommendations in this report ACME Enterprises can build resilient and effective security in the organisation.

Overview

ACME Enterprises engaged Volkis to perform an assessment against the Essential 8 Cyber Security Maturity Model that is developed and released by the Australian Cyber Security Centre (ACSC). This model comprises 8 technical security controls that the ACSC thinks are appropriate for all organisations in Australia and is backed by the federal government and Australian Signals Directorate.

Assessment approach

The assessment investigated the IT environment of ACME Enterprises. Information was gathered in the following ways:

- **SOE Review**: A sample laptop was supplied to Volkis. This laptop was reviewed against applicable Essential 8 controls, identifying whether application control is installed, Microsoft Office macros and applications are appropriately configured, and the latest patches have been installed.
- **Penetration testing results**: The results from penetration testing were reviewed for potential compliance issues.
- **Documentation**: The policies, processes, and procedures that were provided to Volkis were reviewed against the standard. The controls described in the provided documentation was assumed to be in place and effective.
- **Workshops**: Volkis consultants performed workshops with ACME Enterprises employees to gather additional information where necessary.

Compliance summary

The below chart shows the maturity levels of each of the Essential 8 controls. Each filled in sector represents a maturity level that has been achieved by ACME Enterprises.

Currently two controls, “Patch applications” and “Multi-factor authentication” are at the highest maturity level of 3, while “Regular backups”, “Patch operating systems” and “Configure Microsoft Office macro settings” are at maturity level 2. Three controls, “Application control”, “User application hardening” and “Restrict administrative privileges” failed to meet the requirements to reach maturity level 1.

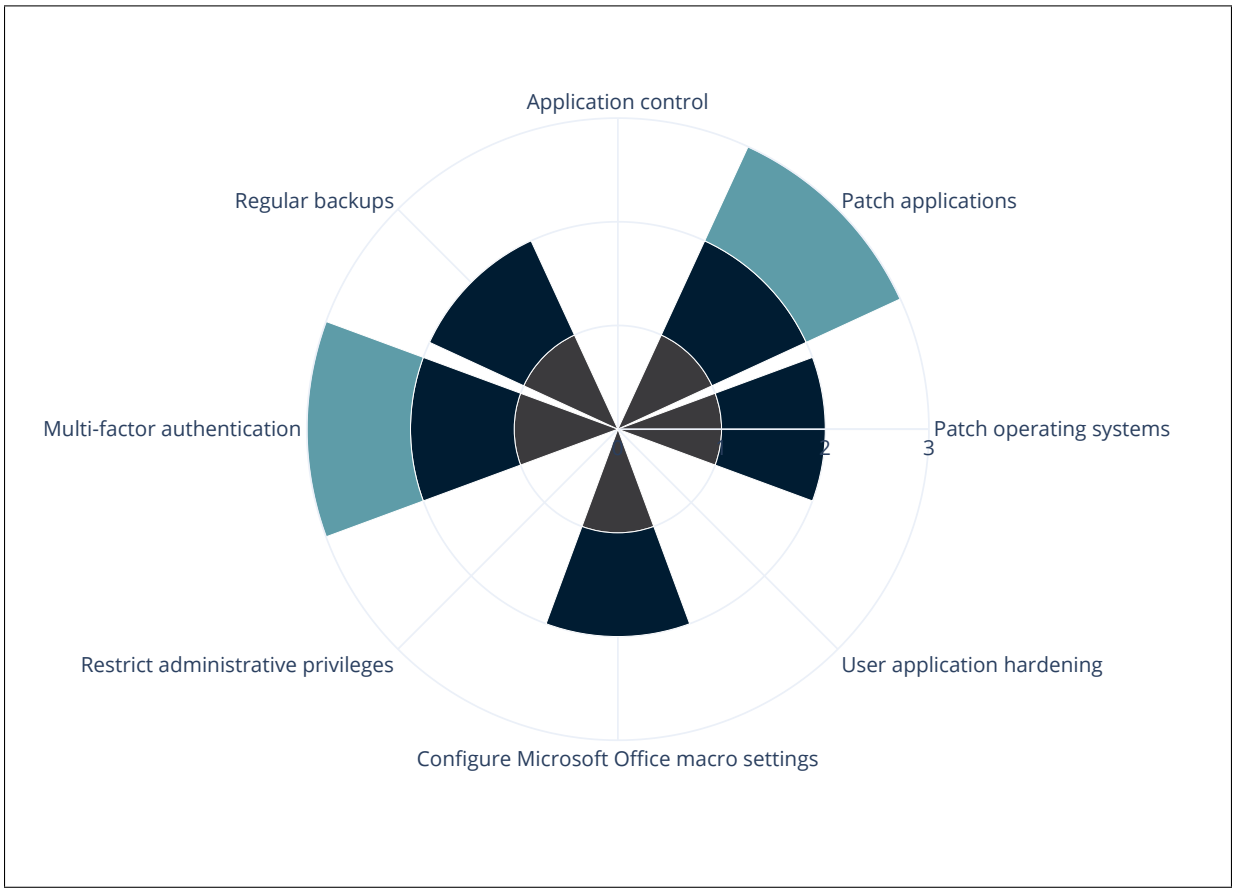


Figure 1: Essential 8 maturity levels

Essential 8 Maturity Model compliance

This section contains details of the controls that comprise the Essential 8 Maturity Model. The eight controls of the Essential 8 are:

- Application control
- Patch applications
- Patch operating systems
- User application hardening
- Configure Microsoft Office macro settings
- Restrict administrative privileges
- Multi-factor authentication
- Regular backups

Each of the eight controls in the Essential 8 has three maturity levels. These levels define not just whether the controls are in place, but how effective they are likely to be at preventing and detecting attacks.

The maturity levels expand on each other. To meet the requirements of maturity level 2, for example, the requirements of maturity level 1 must be fulfilled as well as the additional requirements for maturity level 2. To meet maturity level 3 for all 8 controls of the standard, 92 requirements must be met in total.

Application control

Overview

Application controls systems prevent the execution of unknown applications. It is an effective way of protecting against malware and of limiting the effectiveness of phishing attacks.

There is currently no application control installed in the environment. Due to this, ACME Enterprises do not currently meet the requirements of maturity level 1.

Recommendations

Application control should be implemented on user devices and internally hosted servers. Ideally, the application control suite should:

- Be installed on all workstations and servers.
- Be able to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets, and drivers to an organisation-approved set.
- Log allowed and blocked executions, sending these log events to a centralised logging platform.
- Ensure bypasses in Microsoft's recommended driver and executable block rules are restricted.

When installed, the application control ruleset should be validated on an annual or more frequent basis.

Summary of control implementation

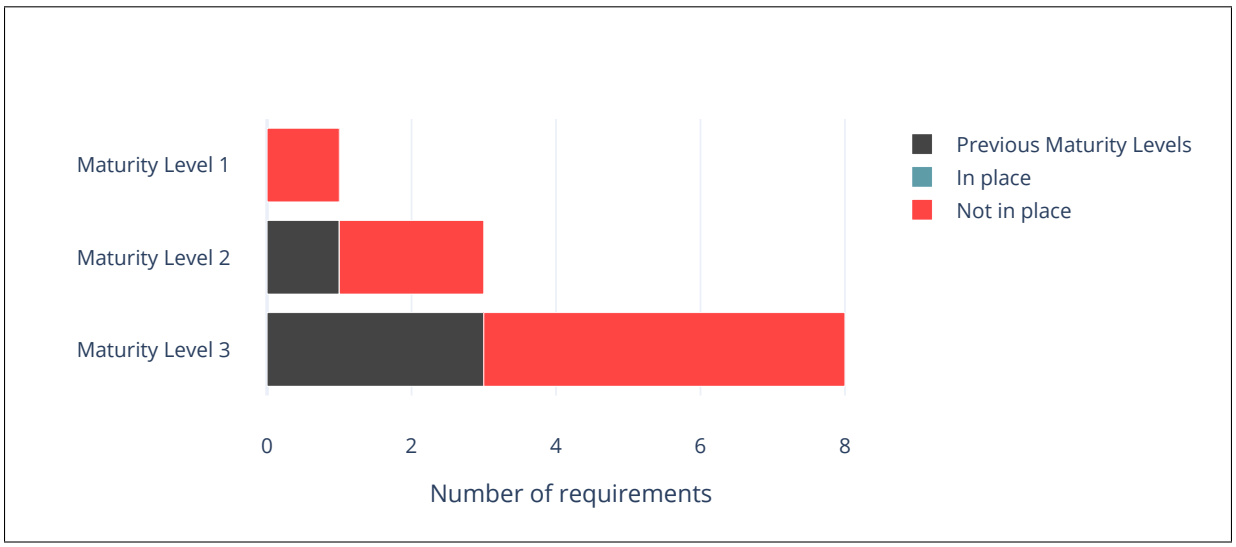


Figure 2: Application control maturity level requirements in place

Application control maturity level requirement status

Maturity Level 1	Maturity Level 2	Maturity Level 3
The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	**Application control is implemented on workstations and internet-facing servers to restrict** the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets **to an organisation-approved set**.	Application control is implemented on workstations **and servers** to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets **and drivers** to an organisation-approved set.
	Allowed and blocked executions on workstations and internet-facing servers are logged.	Allowed and blocked executions on workstations **and servers** are centrally logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected**.
		Microsoft's 'recommended block rules' are implemented.
		Microsoft's 'recommended driver block rules' are implemented.
		Application control rulesets are validated on an annual or more frequent basis.

Patch applications

Overview

Applications are kept up-to-date with the latest patches, predominently using auto-update functions. Applications are updated, and there is vulnerability scanning tool in place that will validate patch levels. This allows ACME Enterprises to verify that applications are up-to-date on user devices.

ACME Enterprises currently meets the requirements for maturity level 3.

Recommendations

No further action is required by ACME Enterprises at this time.

Summary of control implementation

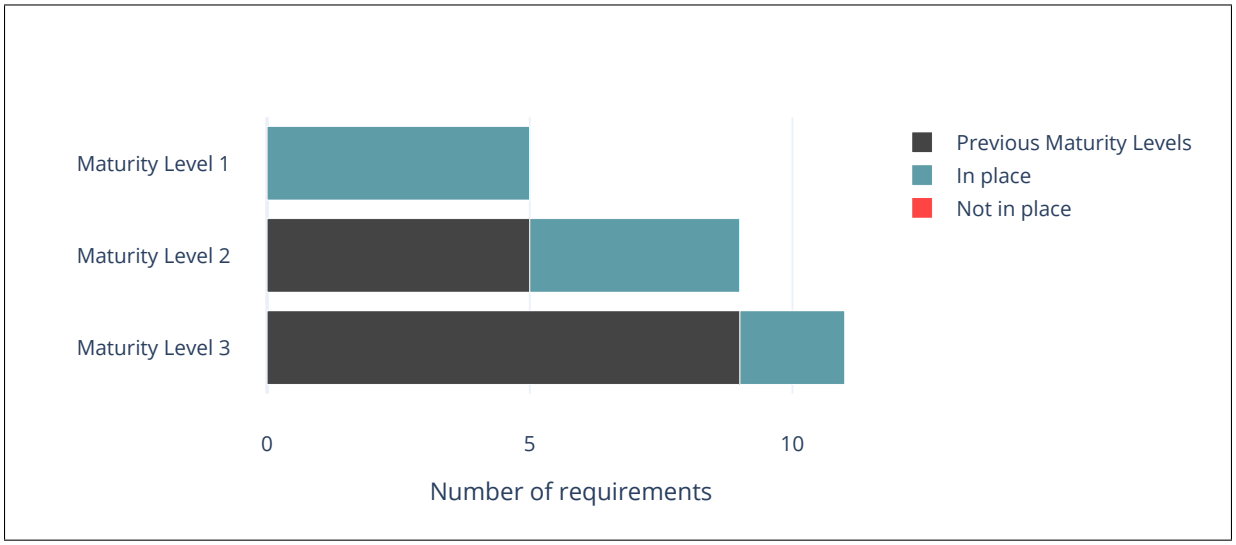


Figure 3: Patch applications maturity level requirements in place

Patch applications maturity level requirement status

Maturity Level 1	Maturity Level 2	Maturity Level 3
Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month.	
A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.	
Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within **two weeks** of release.	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, **or within 48 hours if an exploit exists**.
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	A vulnerability scanner is used at least **weekly** to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	
Internet-facing services, 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** that are no longer supported by vendors are removed.

Configure Microsoft Office macro settings

Overview

Microsoft Office macros are blocked with users unable to change the settings. Additional AV scanning with Microsoft Defender is enabled. This meets the requirements of maturity level 2.

While macros are blocked, the list of trusted publishers is not validated on an annual or more frequent basis. There is also no centralised log management for allowed and blocked macros.

Recommendations

To meet the requirements of maturity level 3, implement the following requirements:

- Implement a process for validating the list of trusted publishers at least annually.
- Consider implementing monitored centralised log management. This should include collecting logs for allowed and blocked office macro executions.

Summary of control implementation

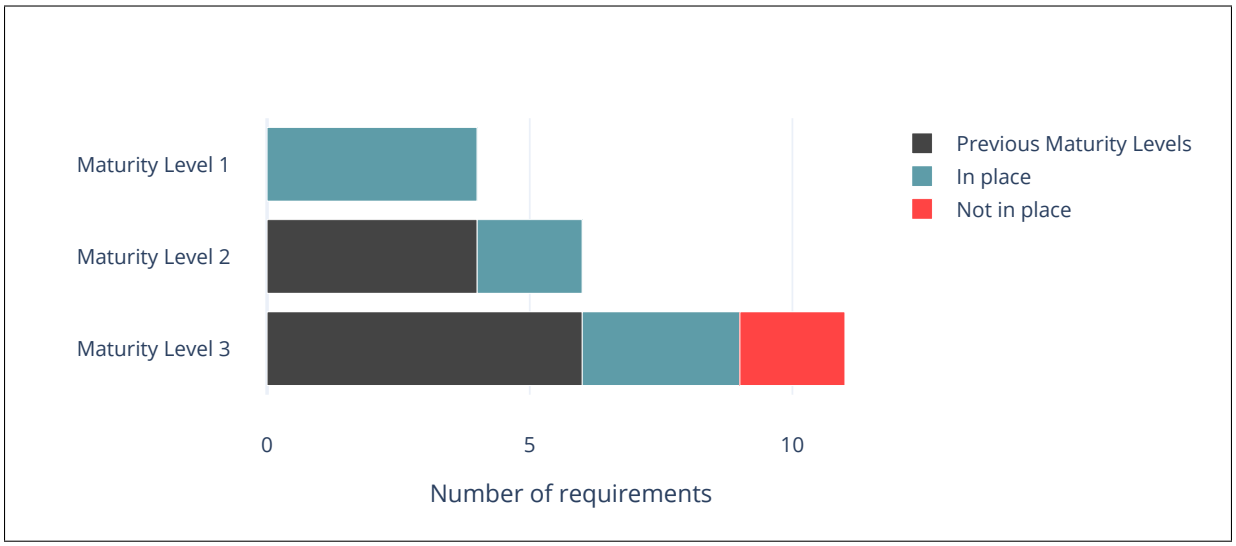


Figure 4: Configure Microsoft Office macro settings maturity level requirements in place

Configure Microsoft Office macro settings maturity level requirement status

Maturity Level 1	Maturity Level 2	Maturity Level 3
Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Microsoft Office macros are blocked from making Win32 API calls.	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 in files originating from the internet are blocked.		Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.
Microsoft Office macro antivirus scanning is enabled.		Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.
Microsoft Office macro security settings cannot be changed by users.		Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.
	Allowed and blocked Microsoft Office macro executions are logged.	Allowed and blocked Microsoft Office macro executions are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected**.

User application hardening

Overview

User hardening policies are applied using Microsoft Intune, Attack Surface Reduction, and group policy settings. This includes blocking Java and Internet Explorer 11 from processing data from the internet, applying security policies to Microsoft Office, PDF, and Powershell, and ensuring web browser settings cannot be changed by users.

There is currently no web advertisement blocker installed for users, meaning that ACME Enterprises does not currently meet the requirements for Maturity Level 1.

While these security settings are applied, additional settings that are present in ACSC and vendor hardening guides were not enabled.

Internet Explorer 11 is still present on user devices, however this browser will be considered “end-of-life” on 15th of June 2022.

Powershell script executions were logged, however Powershell 2.0 was still accessible and Powershell Constrained Language Mode was not set.

Recommendations

To improve the security of ACME Enterprises and meet maturity level 3, implement the following controls:

- Implement web advertisement blocking on user devices.
- Follow ACSC and vendor hardening guides when configuring user devices.
- Disable PowerShell 2.0 and Internet Explorer 11.
- Consider implementing monitored centralised log management. This should collect logs for PowerShell script executions allowing potentially malicious executions to be identified.

Summary of control implementation

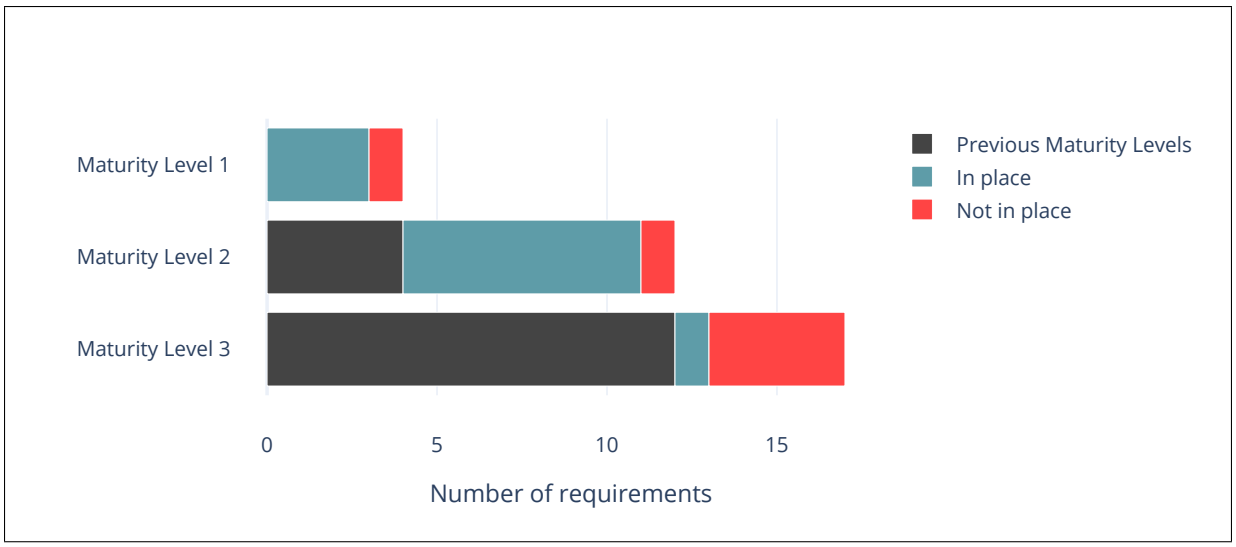


Figure 5: User application hardening maturity level requirements in place

User application hardening maturity level requirement status

Maturity Level 1	Maturity Level 2	Maturity Level 3
Web browsers do not process Java from the internet.	Microsoft Office is blocked from creating child processes.	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.
Web browsers do not process web advertisements from the internet.	Microsoft Office is blocked from creating executable content. Microsoft Office is blocked from injecting code into other processes. Microsoft Office is configured to prevent activation of OLE packages. PDF software is blocked from creating child processes.	Windows PowerShell 2.0 is disabled or removed. PowerShell is configured to use Constrained Language Mode.
	ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.	
Internet Explorer 11 does not process content from the internet.		Internet Explorer 11 is **disabled or removed**.
Web browser security settings cannot be changed by users.	Web browser, **Microsoft Office and PDF software** security settings cannot be changed by users.	
	Blocked PowerShell script executions are logged.	Blocked PowerShell script executions are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected**.

Restrict administrative privileges

Overview

The misuse of administrative privileges is the primary way to expand access in an organisation's network, leveraging user access to gain control over the entire environment. Restricting administrative privileges raises the bar for attackers, preventing them from obtaining the higher level of access.

Currently there are only two accounts in the "Domain Administrators" group and users do not have local administrator access over their own devices. There are sensible restrictions in place for the use of privileged accounts.

The privileged users have separate privileged accounts from their day-to-day accounts, limiting the scope for compromise with phishing and internet based attacks. This is not enforced, however, with technical controls by completely blocking access to unprivileged operating environments, internet, email, and web services. This prevents ACME Enterprises from meeting the requirements of maturity level 1.

Automated routines are not yet in place for disabling unused or inactive accounts, however manual processes exist for this function. Jump boxes are unnecessary for the environment due to the use of cloud hosting and software-as-a-service.

Recommendations

Further restrictions can be put in place for administrative privileges. This includes:

- Restricting privileged accounts from accessing unprivileged operating environments, the internet, email, and web services.
- Implementing automatic processes for disabling accounts after 45 days of inactivity, and disabling accounts annually unless the accounts are revalidated.
- Using a system such as Local Administrator Password Solution (LAPS) to ensure local administrator account passwords are securely set and managed.
- Enabling Windows Defender Credential Guard and Remote Credential Guard.
- Using just-in-time administration.
- Implementing centralised log management for logging and monitoring the use of privileged accounts.

Summary of control implementation

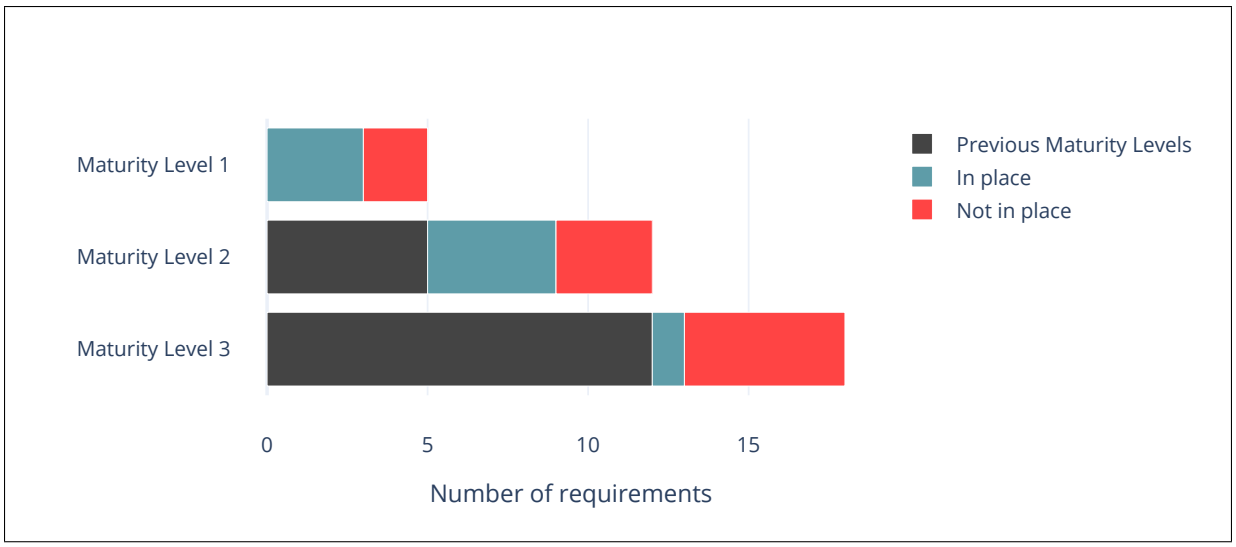


Figure 6: Restrict administrative privileges maturity level requirements in place

Restrict administrative privileges maturity level requirement status

Maturity Level 1	Maturity Level 2	Maturity Level 3
Requests for privileged access to systems and applications are validated when first requested.	Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.	Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.
Privileged users use separate privileged and unprivileged operating environments.	Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	Just-in-time administration is used for administering systems and applications.
Unprivileged accounts cannot logon to privileged operating environments	Privileged operating environments are not virtualised within unprivileged operating environments.	Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.
Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Administrative activities are conducted through jump servers.	
	Credentials for local administrator accounts and service accounts are unique, unpredictable and managed.	
Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services		**Privileged accounts** are prevented from accessing the internet, email and web services.
	Use of privileged access is logged.	Use of privileged access is **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected**.

Continued on next page

Maturity Level 1	Maturity Level 2	Maturity Level 3
	Changes to privileged accounts and groups are logged.	Changes to privileged accounts and groups are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected**.

Patch operating systems

Overview

The latest operating system patches were installed on the supplied device. Although patches were installed, and a vulnerability scanning tools that validate patch levels is in use, ACME Enterprises does not install updates on servers or devices within 48 hours if an exploit is known.

Delays in updating software with known exploits prevents ACME Enterprises from reaching maturity level 3.

Recommendations

Consider updating the current patch management programme to require patches are applied to servers or devices within 48 hours should an exploit exist.

Summary of control implementation

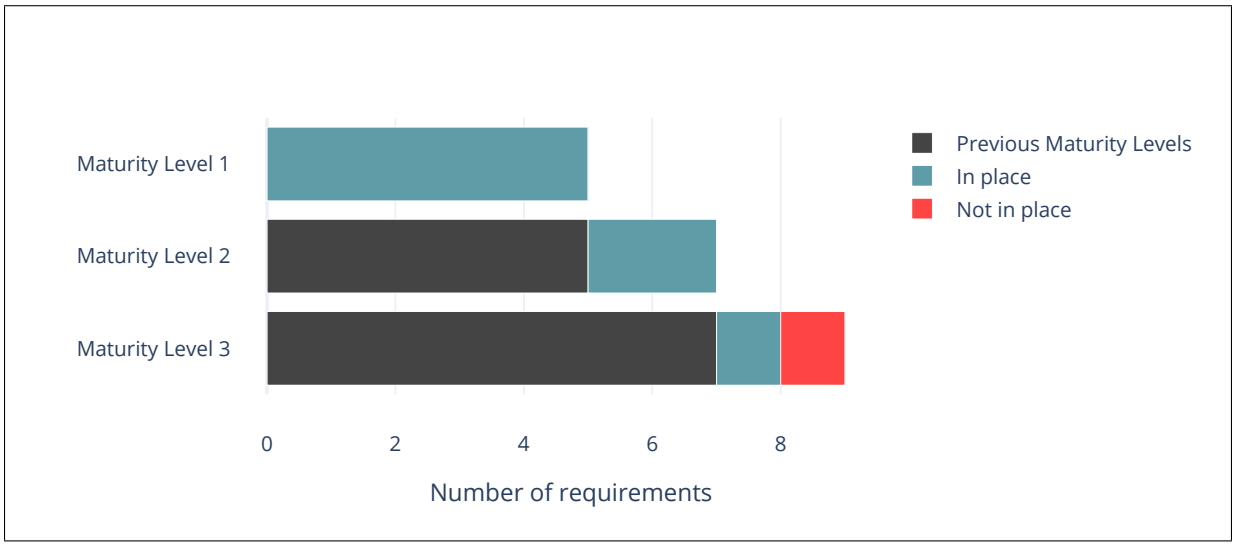


Figure 7: Patch operating systems maturity level requirements in place

Patch operating systems maturity level requirement status

Maturity Level 1	Maturity Level 2	Maturity Level 3
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.		The latest release, or the previous release, of operating systems are used for workstations, servers and network devices.
A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services.		
Operating systems that are no longer supported by vendors are replaced.		
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within **two weeks** of release.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, **or within 48 hours if an exploit exists**.
A vulnerability scanner is used at least fortnightly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices.	A vulnerability scanner is used at least **weekly** to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices.	

Multi-factor authentication

Overview

Multi-factor authentication (MFA) is in place on all major services including Microsoft 365. MFA is enabled on all accounts and centralised log management implemented. This meets the requirements of maturity level 3.

Recommendations

No further action is required by ACME Enterprises at this time.

Summary of control implementation

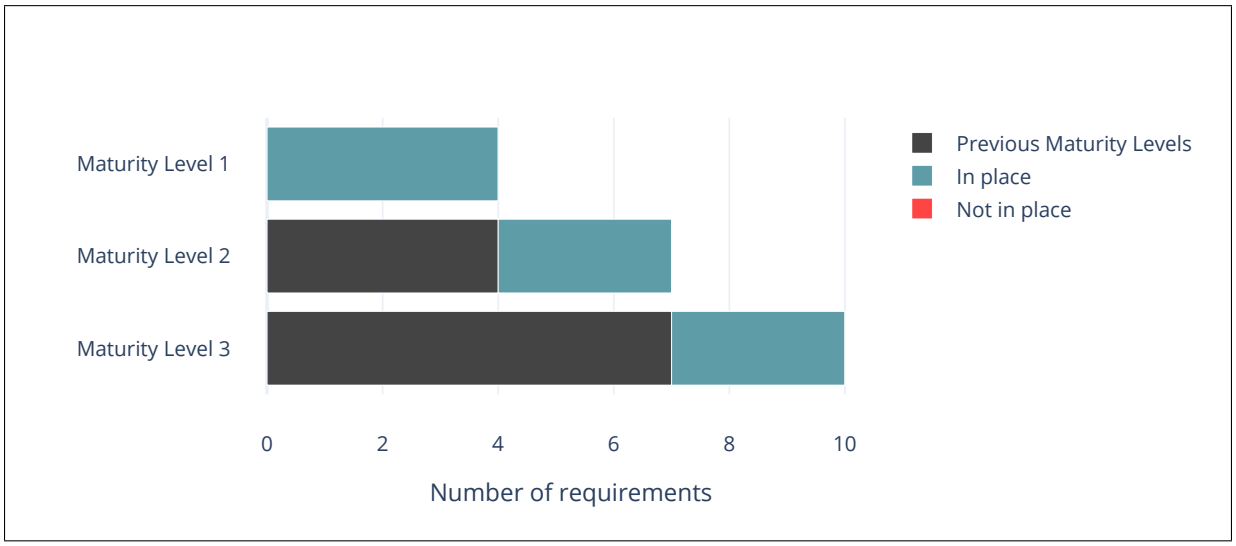


Figure 8: Multi-factor authentication maturity level requirements in place

Multi-factor authentication maturity level requirement status

Maturity Level 1	Maturity Level 2	Maturity Level 3
Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.	Multi-factor authentication is used to authenticate privileged users of systems.	Multi-factor authentication is used to authenticate users accessing important 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 **is verifier impersonation resistant and** uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

Continued on next page

Maturity Level 1	Maturity Level 2	Maturity Level 3
	Successful and unsuccessful multi-factor authentications are logged.	Successful and unsuccessful multi-factor authentications are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected**.

Regular backups

Overview

Backups are in place using Veritas NetBackup. These backups have been tested, and cannot be accessed by unprivileged users. They cover user devices and Microsoft 365 accounts.

Currently privileged users can modify and delete backups. While this prevents ACME Enterprises from reaching Maturity Level 3, this control may not be appropriate for the organisation.

Recommendations

Consider limiting the deletion and modification of backups to break glass accounts.

Summary of control implementation

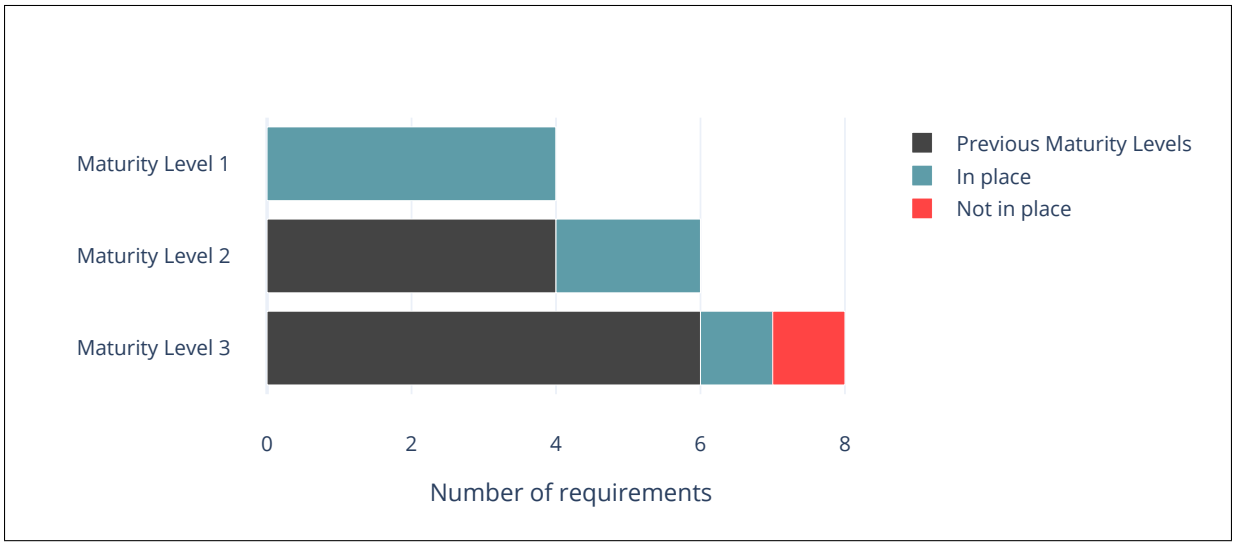


Figure 9: Regular backups maturity level requirements in place

Regular backups maturity level requirement status

Maturity Level 1	Maturity Level 2	Maturity Level 3
Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements. Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.		
Unprivileged accounts can only access their own backups.	Unprivileged accounts, **and privileged accounts (excluding backup administrators)**, can only access their own backups.	Unprivileged accounts, and privileged accounts (excluding backup administrators), **cannot access backups**.
Unprivileged accounts are prevented from modifying or deleting backups.	Unprivileged accounts, **and privileged accounts (excluding backup administrators)**, are prevented from modifying or deleting backups.	Unprivileged accounts, and privileged accounts (excluding backup **break glass accounts**), are prevented from modifying or deleting backups.

Appendices

Appendix A: Detailed assessment results

Detailed assessment results is provided in the attached spreadsheet:

`Appendix A - Worksheet Base.xlsx`

Appendix B: Document control

Document information

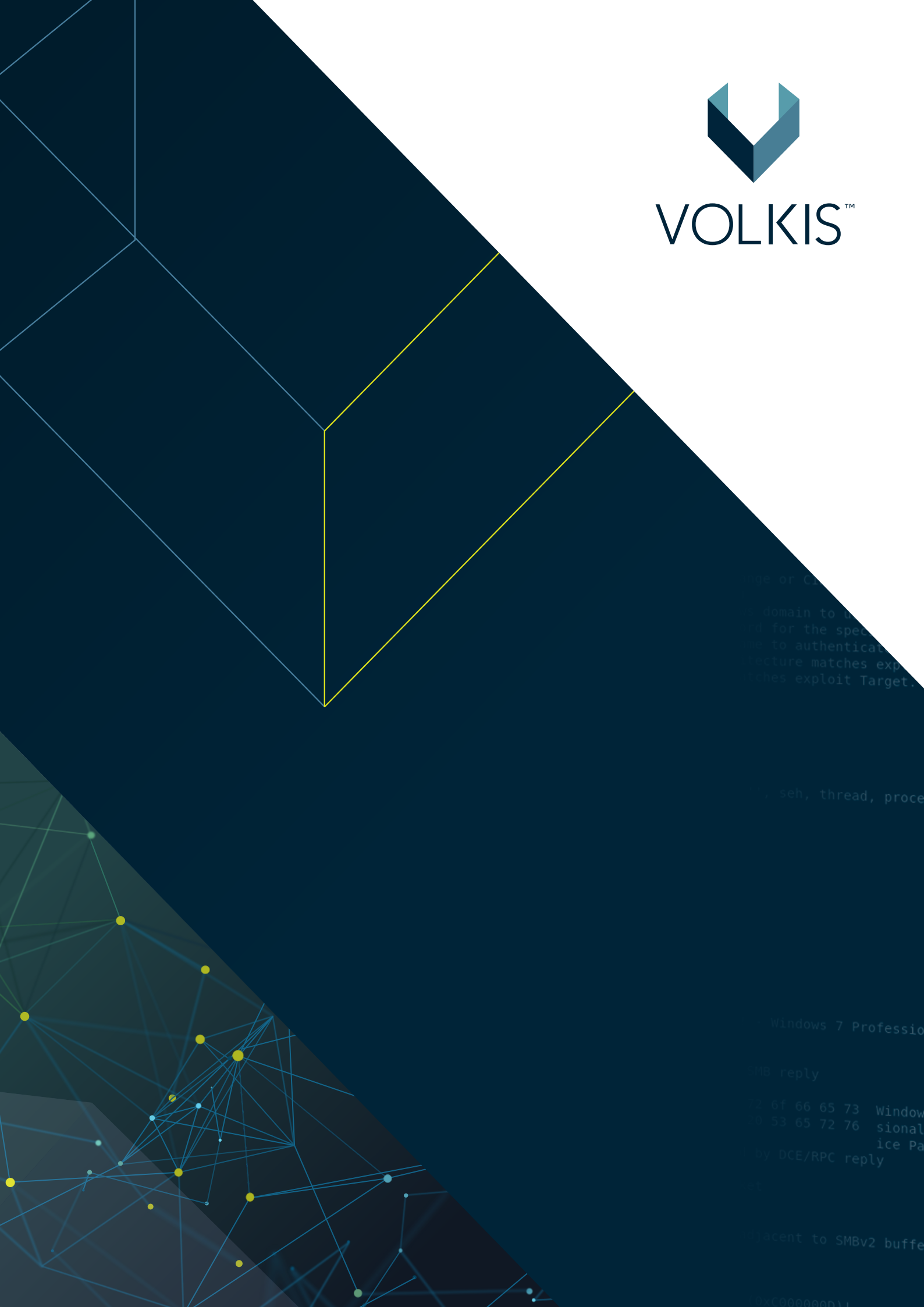
Client	ACME Enterprises
Document name	Volkis Sample Essential 8 Report
Document version	1.0

Document changes

Version	Date	Name	Changes
1.0	2022-04-28	Volkis	April 2022 sample report

Document contributors

Name	Role	Phone number	Email address
Volkis			info@volkis.com.au


VOLKIS™