M365, Azure & DLP Assessment

November 2024

Presented by

WhiteRook Cyber

P: 1300 794 777
E: info@whiterookcyber.com.au
W: whiterookcyber.com.au

Executive Summary

White Rook Cyber performed a Cloud Security Assessment on Test Company's Data Loss Protection (DLP), Azure & Microsoft 365 environments.

The scope includes a deep dive assessment of the DLP implementation as well as Test Company's Azure and Microsoft 365 environments, aligning them with the CIS Microsoft Azure Foundations Benchmark 3.0 and CIS Microsoft 365 Foundations Benchmark 3.1, respectively.

In the assessment of C subscriptions, we discovered one hundred and seventy-two (172) non-compliant recommendations including four (4) critical-risk and fifty-six (56) high-risk findings require prompt attention to mitigate significant vulnerabilities. Additionally, there are forty-five (45) medium-risk and forty (40) low-risk findings, presenting opportunities for further enhancement. Twenty-seven (27) informational findings have been included.

Overall, we have found the Health Index of the external environment to have **significant room for improvement**, **sitting at 54%**; and the **Internal DLP current state to sit at the Planning Stage only**.

Considering these findings, we recommend a strong focus on securing the environment and implementing continuous monitoring and remediation processes to maintain and strengthen compliance. Adhering to the principle of least privilege, having a well-defined incident response plan, and optimising resource usage is vital. Staying updated with Azure and Microsoft 365 updates, maintaining robust documentation and reporting, and fostering a strong security culture among staff will help enhance Test Company's overall cyber security.

By proactively addressing these areas, Test Company can ensure a more secure and resilient Azure and Microsoft 365 environments, safeguarding its data and operations both internally and externally while minimising security risks. We remain committed to working closely with Test Company to further strengthen its environments' security and compliance posture.

If further clarification is required on the contents of this report, please reach out to White Rook Cyber.

We appreciate the opportunity to help improve your security.

Scope of Review

The scope of this assessment encompassed an extensive examination of Test Company's DLP, Azure and Microsoft 365 environments, adhering to the relevant CIS benchmarks.

Microsoft Azure Assessment

The Azure environment was assessed against CIS Microsoft Azure Foundations Benchmark 3.0.

Within the assessment, we delved into the following critical areas, each aligned with the CIS benchmarks:

1. Identity and Access Management: Scrutinising user authentication, access policies, and roles.
2. Security: Assessing the deployment and configuration of Microsoft Defender and Key Vault across various services for threat protection.
3. Storage Accounts: Ensuring the security and access controls of storage accounts, including data encryption and network access.
4. Database Services: Evaluating the security posture of database services such as SQL Server, PostgreSQL, MySQL, and Cosmos DB.
5. Logging and Monitoring: Examining logging configurations, monitoring tools, and alerting mechanisms for proactive threat detection.
6. Networking: Analysing network security, including virtual networks and network access controls.
7. Virtual Machines: Assessing virtual machine configurations, access controls, and network security groups.
8. App Service: Evaluating the security configurations of web applications, including secure ports and role-based access control.
9. Miscellaneous: Evaluating any security configurations that do not fit into the other critical areas.

This comprehensive review provided a detailed assessment of Test Company’s in-scope environments, identifying compliance, risks, and areas for improvement to strengthen the organisation’s security posture. The insights gathered aim to support proactive security measures, regulatory compliance, and effective threat mitigation.

Microsoft 365 Assessment

Test Company’s Microsoft 365 environment was assessed against the CIS Microsoft 365 Foundations Benchmark 3.1. Within the assessment, we evaluated each of the following platforms that make up the Microsoft 365 suite and aligned to the CIS benchmark.

1. Microsoft Teams: Evaluating the security configurations of Microsoft Teams meetings, chats, calls, etc. to assess control efficacy.
2. Microsoft Exchange: Assessing the security configuration and controls of Microsoft Exchange Online.
3. Microsoft Azure: Evaluating Microsoft Azure and Entra against security configurations and controls.
4. Microsoft SharePoint: Evaluating the security and privacy controls and configurations.
5. Microsoft Office 365: Assessing Microsoft Office 365 control and configuration.

This review provided a detailed assessment of Test Company’s Microsoft 365 tenancy, identifying compliance, risks, and areas for improvement.

Microsoft DLP Assessment

Test Company’s Microsoft 365 environment was assessed for DLP implementation and security controls. The following DLP implantation were evaluated:

1. Audit Settings in Microsoft 365 including Alert Policies.
2. Communication Compliance Policies and sensitivity labels as configured within the environment, including current monitoring activities.
3. Use of Microsoft Compliance Manager in its DLP activities.
4. Configuration & use of eDiscovery within the organisation.
5. Information Governance Implementations include use and overview of current of Data Retention Labels and Policies.
6. Information protection including the use of sensitivity labels for critical data and IRM for exchange
7. Records Management and utilisation within the Microsoft Environment
8. Backups of Data and Access Controls around Data.

Reporting Format

The assessment results and recommendation/remediations are provided in several different formats to immediately assist your IT technical department/service team.

- **Encrypted Executive Report (this PDF)**
- **Interactive HTML Reports with Knowledge base article links for further information, and easy to copy PowerShell scripts to assist in remediation efforts.**

Microsoft 365 Cloud Security Assessment Findings

Prepared by

WhiteRook Cyber

Microsoft 365 Security Report

This White Rook Cyber report assesses your compliance posture, highlights risks and recommends remediation steps to ensure compliance with essential data protection and regulatory standards.

Start Date	**: 10/27/2024 20:27:17**
End Date	**: 11/10/2024 20:41:15**
Organization	**: Test Company Pty Ltd**
Stats	**: 137** out of **298** security checks identified possible opportunities for improvement.

Informational	Low	Medium	High	Critical
21	31	28	56	1

54%

Configuration Health Index

The configuration health index is a weighted value representing your configuration. Not all configuration is considered the same. Some configuration is weighted higher than others.

Solutions Summary

✓ **All Solutions**	21	31	28	56	1
Microsoft Teams	0	0	1	8	0
Microsoft Exchange	3	2	17	20	0
Microsoft Azure	16	28	9	21	1
Microsoft Sharepoint	1	0	0	4	0
Microsoft Office 365	1	1	1	3	0

● Informational ● Low ● Medium ● High ● Critical

Microsoft Teams

Medium [8]: CISM Tm 8.2.1 - External access is not restricted in the Teams admin center!

CISM Tm 8.2.1 - External access is not restricted in the Teams admin center!

ID: CISMTm821

Description:

Allowing users to communicate with Skype or Teams users outside of an organization presents a potential security threat as external users can interact with organization users over Skype for Business or Teams. While legitimate, productivity-improving scenarios exist, they are outweighed by the risk of data loss, phishing, and social engineering attacks against organization users via Teams. Therefore, it is recommended to restrict external communications in order to minimize the risk of security incidents.

Remediation:

Use the PowerShell script to disallow External Communication

PowerShell Script:

```
Set-CsTenantFederationConfiguration -AllowTeamsConsumer $false -
AllowPublicUsers $false -AllowFederatedUsers $false
```

Returned Value:

AllowTeamsConsumer: True

AllowPublicUsers: True

AllowFederatedUsers: True

Default Value:

All True

Expected Value:

All False

Impact:

2

Likelihood:

4

Priority:

Low

RiskRating: Medium

References:

[Manage external meetings and chat with people and organizations using Microsoft identities]

High [15]: CISM Tm 8.1.2 - Users can send emails to a channel emailaddress

👎 CISM Tm 8.1.2 - Users can send emails to a channel emailaddress

ID: CISMTm812

Description:

Channel email addresses are not under the tenant's domain and organizations do not have control over the security settings for this email address. An attacker could email channels directly if they discover the channel email address.

Remediation:

Use the PowerShell script to disallow Emails into Channels:

PowerShell Script:

```
Set-CsTeamsClientConfiguration -Identity Global -AllowEmailIntoChannel
$false
```

Returned Value:

True

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

[Restricting channel email messages to approved domains]

High [15]: CISM Tm 8.5.3 - Everyone can bypass the lobby

👎 CISM Tm 8.5.3 - Everyone can bypass the lobby

ID: CISMTm853

Description:

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times.

Remediation:

Use the PowerShell script to disallow External Access

PowerShell Script:

```
Set-CsTeamsMeetingPolicy -Identity Global -AutoAdmittedUsers
"EveryoneInCompanyExcludingGuests"
```

Returned Value:

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ Restricting channel email messages to approved domains

High [15]: CISM Tm 8.6.1 - Users cannot report security concerns in Teams

👎 CISM Tm 8.6.1 - Users cannot report security concerns in Teams

ID: CISMTm861

Description:

Users will be able to more quickly and systematically alert administrators of suspicious malicious messages within Teams. The content of these messages may be sensitive in nature and therefore should be kept within the organization and not shared with Microsoft without first consulting company policy.

Remediation:

Use the PowerShell script to allow users to report security concerns in teams:

PowerShell Script:

```
Set-CsTeamsMessagingPolicy -Identity Global -
AllowSecurityEndUserReporting $true; $usersub = "example@contoso.com";
$params = @{ Identity = "DefaultReportSubmissionPolicy"
EnableReportToMicrosoft = $false ReportChatMessageEnabled = $false
ReportChatMessageToCustomizedAddressEnabled = $true
ReportJunkToCustomizedAddress = $true ReportNotJunkToCustomizedAddress
= $true ReportPhishToCustomizedAddress = $true ReportJunkAddresses =
$usersub ReportNotJunkAddresses = $usersub ReportPhishAddresses =
$usersub }; Set-ReportSubmissionPolicy @params; New-
ReportSubmissionRule -Name DefaultReportSubmissionRule -
ReportSubmissionPolicy DefaultReportSubmissionPolicy -SentTo $usersub
```

Returned Value:

ReportChatMessageEnabled: True

Default Value:

True

Expected Value:

-

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

User reported message settings in Microsoft Teams

High [15]: CISM Tm 8.1.1 - External file sharing in Teams is not enabled for only approved cloud storage services

CISM Tm 8.1.1 - External file sharing in Teams is not enabled for only approved cloud storage services

ID: CISMTm811

Description:

Ensuring that only authorized cloud storage providers are accessible from Teams will help to dissuade the use of non-approved storage providers.

Remediation:

Use the PowerShell script to disallow External File Sharing:

PowerShell Script:

```
Set-CsTeamsClientConfiguration -AllowGoogleDrive $false -AllowShareFile $false -AllowBox $false -AllowDropBox $false -AllowEgnyte $false
```

Returned Value:

AllowDropbox: True

AllowBox: True

AllowEgnyte: True

Default Value:

All True

Expected Value:

All False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

[Manage Skype for Business Online with PowerShell]

High [15]: CISM Tm 8.5.1 - Anonymous users can join a meeting

👎 CISM Tm 8.5.1 - Anonymous users can join a meeting

ID: CISMTm851

Description:

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times

Remediation:

Use the PowerShell script to disallow External Access

PowerShell Script:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToJoinMeeting $false
```

Returned Value:

True

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

Configure Teams meetings with protection for sensitive data

High [15]: CISM Tm 8.5.5 - The meeting chat allows anonymous users

👎 CISM Tm 8.5.5 - The meeting chat allows anonymous users

ID: CISMTm855

Description:

Ensuring that only authorized individuals can read and write chat messages during a meeting reduces the risk that a malicious user can inadvertently show content that is not appropriate or view sensitive information.

Remediation:

Use the PowerShell script to disallow External Access

PowerShell Script:

```
Set-CsTeamsMeetingPolicy -Identity Global -MeetingChatEnabledType
"EnabledExceptAnonymous"
```

Returned Value:

Enabled

Default Value:

Everyone

Expected Value:

EnabledExceptAnonymous

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ Set-CSTeamsMeetingPolicy

High [15]: CISM Tm 8.5.6 - Not only organizers and co-organizers can present, but also other users

👎 CISM Tm 8.5.6 - Not only organizers and co-organizers can present, but also other users

ID: CISMTm856

Description:

Ensuring that only authorized individuals are able to present reduces the risk that a malicious user can inadvertently show content that is not appropriate.

Remediation:

Use the PowerShell script to allow only organizers and co-organizers to present:

PowerShell Script:

```
Set-CsTeamsMeetingPolicy -Identity Global -DesignatedPresenterRoleMode
"OrganizerOnlyUserOverride"
```

Returned Value:

EveryoneUserOverride

Default Value:

Everyone

Expected Value:

OrganizerOnlyUserOverride

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

[Manage who can present and request control in Teams meetings]

High [15]: CISM Tm 8.5.8 - External meeting chat is on

👎 CISM Tm 8.5.8 - External meeting chat is on

ID: CISMTm858

Description:

This meeting policy setting controls whether users can read or write messages in external meeting chats with untrusted organizations. If an external organization is on the list of trusted organizations this setting will be ignored. Restricting access to chat in meetings hosted by external organizations limits the opportunity for an exploit like GIFShell or DarkGate malware from being delivered to users

Remediation:

Use the PowerShell script to disallow External Access

PowerShell Script:

```
Set-CsTeamsMeetingPolicy -Identity Global -
AllowExternalNonTrustedMeetingChat $false
```

Returned Value:

True

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ [Teams settings and policies reference]

Microsoft Exchange

Informational [0]: CSTM-Ex024 - Mailboxes with Internal Forwarding Rules Enabled

👍 CSTM-Ex024 - Mailboxes with Internal Forwarding Rules Enabled

ID: CSTM-Ex024

Description:

The Exchange Online mailboxes listed above have Forwarding rules configured enabled. Attackers commonly create hidden forwarding rules in compromised mailboxes. These rules may be exfiltrating data with or without the user's knowledge.

Remediation:

Use the PowerShell Command to disable the Internal Forward Rules based on the EmailAddress. A list is included about which emailadresses are impacted.

PowerShell Script:

```
Remove-InboxRule -Mailbox  -Identity "Rule Name"
```

Returned Value:

ash

Default Value:

None

Expected Value:

None

Impact:

0

Likelihood:

3

Priority:

Informational

RiskRating: Informational

References:

- Office 365 - List all email forwarding rules (PowerShell)
- Get-Mailbox Commandlet Reference

Informational [0]: CSTM-Ex031 - Microsoft Exchange & Microsoft Office 365 Contains Public Groups

CSTM-Ex031 - Microsoft Exchange & Microsoft Office 365 Contains Public Groups

ID: CSTM-Ex031

Description:

Ensure that only organizationally managed and approved public groups exist.

Remediation:

In the Microsoft 365 Administration portal, go to: Teams&Groups > Select the Public Group > Go To Settings > Set Privacy To Private

PowerShell Script:

```
$publicgroups = Get-UnifiedGroup | ? { $_.AccessType -eq "Public"}
```

Returned Value:

Test Company Pty Ltd All Company All Company Group for Answers in Viva Engage – DO NOT DELETE 24893030400,Public Public Public Public

Test Company Pty Ltd All Company All Company Group for Answers in Viva Engage – DO NOT DELETE 24893030400,Public Public Public Public

Test Company Pty Ltd All Company All Company Group for Answers in Viva Engage – DO NOT DELETE 24893030400,Public Public Public Public

Test Company Pty Ltd All Company All Company Group for Answers in Viva Engage – DO NOT DELETE 24893030400,Public Public Public Public

Default Value:

0

Expected Value:

Approved Public Groups Documented

Impact:

4

Likelihood:

1

Priority:

Informational

RiskRating: Informational

References:

Reference - Get-UnifiedGroup

Group Self-Service

Informational [0]: Tenant Transport Rules

Tenant Transport Rules

ID: CSTM-Ex017

Description:

There are Transport Rules Existing in Microsoft Exchange, please verify if they are not faulty or have any malicious intend

Remediation:

Review Mail Flow rules and validate that all results are expected and no conflicting rules are in place.

PowerShell Script:

```
Remove-TransportRule -Identity ID
```

Returned Value:

1

Default Value:

0

Expected Value:

0

Impact:

4

Likelihood:

1

Priority:

Informational

RiskRating: Informational

References:

[Manage Mail Flow Rules in Exchange Online]

Low [3]: CIS MEx 2.1.6 - Exchange Online Spam Policies are not set to notify administrators

CIS MEx 2.1.6 - Exchange Online Spam Policies are not set to notify administrators

ID: CISMEx216

Description:

A blocked account is a good indication that the account in question has been breached and an attacker is using it to send spam emails to other people.

Remediation:

Run the following PowerShell command

PowerShell Script:

```
$BccEmailAddress = @(""); $NotifyEmailAddress = @(""); Set-HostedOutboundSpamFilterPolicy -Identity Default -BccSuspiciousOutboundAdditionalRecipients $BccEmailAddress -BccSuspiciousOutboundMail $true -NotifyOutboundSpam $true -NotifyOutboundSpamRecipients $NotifyEmailAddress
```

Returned Value:

BccSuspiciousOutboundMail: False

NotifyOutboundSpam: False

Default Value:

BccSuspiciousOutboundMail: False / NotifyOutboundSpam: False

Expected Value:

BccSuspiciousOutboundMail: True / NotifyOutboundSpam: True

Impact:

3

Likelihood:

1

Priority:

High

RiskRating: Low

References:

- Set-HostedOutboundSpamFilterPolicy Function Reference
- Configure Outbound Spam Notification Office 365 Exchange Online

Low [2]: CIS MEx 3.2.2 - Teams DLP Policies Not Enabled and Enforced

CIS MEx 3.2.2 - Teams DLP Policies Not Enabled and Enforced

ID: CISMEx322

Description:

Enabling the default Teams DLP policy rule in Microsoft 365 helps protect an organization's sensitive information by preventing accidental sharing or leakage of that information in Teams conversations and channels.

Remediation:

Use the PowerShell script to create a new DLPCompliancePolicy or review the policies existence and if they are enabled.

PowerShell Script:

```
New-DlpCompliancePolicy -Name "SSN Teams Policy" -Comment "SSN Teams Policy" -TeamsLocation All -Mode Enable
```

Returned Value:

Default Value:

Enable

Expected Value:

Enable

Impact:

2

Likelihood:

1

Priority:

Informational

RiskRating: Low

References:

[Learn about data loss prevention](#)

[Create, test, and tune a DLP policy](#)

Medium [9]: CIS MEx 2.1.9 - Ensure that DKIM is enabled for all Exchange Online Domains

👎 CIS MEx 2.1.9 - Ensure that DKIM is enabled for all Exchange Online Domains

ID: CISMEx219

Description:

By enabling DKIM with Office 365, messages that are sent from Exchange Online will be cryptographically signed. This will allow the receiving email system to validate that the messages were generated by a server that the organization authorized and not being spoofed.

Remediation:

DKIM rollout can be a very involved process, for which there is a complete reference in the 'Use DKIM to validate the outbound email sent from your custom domain' guide in the References section below. This finding refers specifically to enabling the DKIM signing configuration within O365 itself, which can be done using the Set-DkimSigningConfig PowerShell function or the Security and Compliance Center in the O365 administration portal.

PowerShell Script:

```
Set-DkimSigningConfig -Identity < domainName > -Enabled $True
```

Returned Value:

testdomain.com.au

Default Value:

False on all custom domains

Expected Value:

None

Impact:

3

Likelihood:

3

Priority:

High

RiskRating: Medium

References:

- [Use DKIM to validate outbound email sent from your custom domain]
- [DKIM Configuration]
- [DKIM FAQ]
- [Set up DKIM to sign mail from your Microsoft 365 domain]

Medium [9]: CSTM-Ex015 - Exchange Mailboxes with SendOnBehalfOf Delegates Found

👎 CSTM-Ex015 - Exchange Mailboxes with SendOnBehalfOf Delegates Found

ID: CSTM-Ex015

Description:

The Exchange Online mailboxes listed above have delegated SendOnBehalfOf permissions to another account.

Remediation:

This finding refers to individual mailboxes that have SendOnBehalfOf delegated permissions. For these mailboxes, verify that the delegate access is expected, appropriate, and do not violate company policy.

PowerShell Script:

```
Get-Mailbox -ResultSize Unlimited -Properties GrantSendOnBehalfTo |
Set-Mailbox -GrantSendOnBehalfTo @{remove="*"}
```

Returned Value:

4

Default Value:

0

Expected Value:

0

Impact:

3

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

↗ Set-Mailbox Commandlet Reference

↗ Remove Send on Behalf permissions using Powershell

Medium [9]: CSTM-Ex014 - Exchange Mailboxes with SendAs Delegates Found

CSTM-Ex014 - Exchange Mailboxes with SendAs Delegates Found

ID: CSTM-Ex014

Description:

The Exchange Online mailboxes listed above have delegated SendAs Access permissions to another account.

Remediation:

This finding refers to individual mailboxes that have SendAs Access delegated permissions. For these mailboxes, verify that the delegate access is expected, appropriate, and do not violate company policy.

PowerShell Script:

```
Remove-MailboxPermission -Identity mailbox -AccessRights SendAs -Confirm:$false -User user
```

Returned Value:

10

Default Value:

0

Expected Value:

0

Impact:

3

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

Remove-MailboxPermission Commandlet Reference

Medium [9]: CSTM-Ex012 - Risky eDiscovery Case Administrators

👎 CSTM-Ex012 - Risky eDiscovery Case Administrators

ID: CSTM-Ex012

Description:

Microsoft Compliance Center eDiscovery provides a method for organizations to search and export content from Microsoft 365 and Office 365. eDiscovery searches are able to access all sources of information, including users' mailboxes to return the requested content. By default, no users are assigned the eDiscovery Administrator role and users may only access cases and searches that they have created.

Remediation:

Review the list of users who are assigned this role, determine if these assignments are appropriate for the tenant and remove any users who should not hold this role.

PowerShell Script:

```
Remove-eDiscoveryCaseAdmin -User example@contoso.com
```

Returned Value:

Default Value:

No eDiscovery Admins

Expected Value:

No eDiscovery Admins / Approved Users

Impact:

3

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

↗ Get started with Core eDiscovery in Microsoft 365

↗ More information about the eDiscovery Manager role group

Medium [9]: CSTM-Ex009 - iFrames Not Identified as Spam

CSTM-Ex009 - iFrames Not Identified as Spam

ID: CSTM-Ex009

Description:

Cyber adversaries often place HTML iframes in the body of an email as a vector for containing spam templates or other malicious content. the organization does not have Exchange spam/content Filter policies to flag emails containing iframes as spam. It is advisable to create content filter rules to detect iframes in email as spam.

Remediation:

Use the PowerShell Script or the References to create a iFrame Spam policy

PowerShell Script:

```
New-HostedContentFilterPolicy -Name "Example Policy" -
HighConfidenceSpamAction Quarantine -SpamAction Quarantine -
BulkThreshold 6 -MarkAsSpamFramesInHtml On -
MarkAsSpamSpfRecordHardFail On -MarkAsSpamEmptyMessages On -
MarkAsSpamJavaScriptInHtml On
```

Returned Value:

Off

Default Value:

Off

Expected Value:

On

Impact:

3

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

- Configuring Exchange Online Protection, First Steps
- Advanced Spam Filter (ASF) Settings in Exchange Online Protection
- Set-HostedContentFilterPolicy Commandlet Reference

Medium [9]: CSTM-Ex007 - Multiple Policies Not Enabled that are found by the ConfigAnalyzerPolicyRecommendations!

👎 CSTM-Ex007 - Multiple Policies Not Enabled that are found by the ConfigAnalyzerPolicyRecommendations!

ID: CSTM-Ex007

Description:

Anti-Spam, Anti-Phishing and Anti-Malware Policies are recommended to have an existing policy configured to minimize impact from spam and phishing and malware within your organization

Remediation:

Configure the Anti-Spam, Anti-Phishing and Anti-Malware policy according to the recommendations. Please consult the text file for further information.

PowerShell Script:

```
New-AntiPhishPolicy; New-HostedContentFilterPolicy; New-MalwareFilterPolicy
```

Returned Value:

10

Default Value:

> 0

Expected Value:

0

Impact:

3

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

[ConfigAnalyzerPolicyRecommendations.txt]

[Lock, Stock and Office 365 ATP Automation]

Medium [9]: CSTM-Ex005 - External Forwarding and AutoForwarding is not correctly Configured

👎 CSTM-Ex005 - External Forwarding and AutoForwarding is not correctly Configured

ID: CSTM-Ex005

Description:

AllowedOOFType should not match 'External' and AutoForwardEnabled should not match 'True'. External Forwarding should be disabled to avoid information leaks and disclosure. Attackers often create these rules to exfiltrate data from your tenancy, this could be accomplished via access to an end-user account or otherwise.

Remediation:

Use the PowerShell Scripts: Get-TransportRule | Remove-TransportRule Set-RemoteDomain Default -AutoForwardEnabled $false; $rejectMessageText = "{Your Reject Message}" and the PowerShell Script to create a TransportRule that blocks AutoForwarding

PowerShell Script:

```
New-TransportRule -name "Client Rules To External Block" -Priority 0 -
SentToScope NotInOrganization -FromScope InOrganization -
MessageTypeMatches AutoForward -RejectMessageEnhancedStatusCode 5.7.1 -
RejectMessageReasonText $rejectMessageText
```

Returned Value:

AllowedOOFType: External

AutoForwardEnabled: True

Default Value:

AllowedOOFType: External

AutoForwardEnabled: True

Expected Value:

AllowedOOFType: Not External

AutoForwardEnabled: False

Impact:

3

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

↗ [Procedures for mail flow rules in Exchange Server]()

> ↗ Disable automatic forwarding in Office 365 and Exchange Server to prevent information leakage
> ↗ Set-RemoteDomain
> ↗ All you need to know about automatic email forwarding in Exchange Online

Medium [8]: CIS MEx 3.3.1 - No SharePoint Online Data Classification Policies Set!

👎 CIS MEx 3.3.1 - No SharePoint Online Data Classification Policies Set!

ID: CISMEx331

Description:

By categorizing and applying policy-based protection, SharePoint Online Data Classification Policies can help reduce the risk of data loss or exposure, and enable more effective incident response if a breach does occur.

Remediation:

Use the PowerShell script to create a New Label Policy

PowerShell Script:

```
New-LabelPolicy -Name "Example Name" -Labels "Example","Domain"
```

Returned Value:

Default Value:

No Policy

Expected Value:

A Policy

Impact:

2

Likelihood:

4

Priority:

Medium

RiskRating: Medium

References:

↗ [Top sensitivity labels applied to content]()

Medium [8]: CIS MEx 6.5.2 - MailTips is not enabled for end users

👎 CIS MEx 6.5.2 - MailTips is not enabled for end users

ID: CISMEx652

Description:

MailTips assist end users with identifying strange patterns to emails they send. By having this disabled end-users are at risk exfiltrating information or doing malicious things without knowing or without being warned.

Remediation:

Run the PowerShell Command to enable MailTips

PowerShell Script:

```
Set-OrganizationConfig -MailTipsAllTipsEnabled $true -
MailTipsExternalRecipientsTipsEnabled $true -
MailTipsGroupMetricsEnabled $true -MailTipsLargeAudienceThreshold "25"
```

Returned Value:

MailTipsLargeAudienceThreshold:

Default Value:

MailTipsAllTipsEnabled: False

MailTipsExternalRecipientsTipsEnabled: False

MailTipsGroupMetricsEnabled: False

MailTipsLargeAudienceThreshold: 25

Expected Value:

MailTipsAllTipsEnabled: True

MailTipsExternalRecipientsTipsEnabled: True

MailTipsGroupMetricsEnabled: True

MailTipsLargeAudienceThreshold: >25

Impact:

2

Likelihood:

4

Priority:

Medium

RiskRating: Medium

References:

- [MailTips in Exchange Online](#)
- [Set-OrganizationConfig](#)

Medium [8]: Office Message Encryption is Not Enabled

Office Message Encryption is Not Enabled

ID: CSTM-Ex028

Description:

Messages the organization sends using Exchange email may contain confidential information such as employee names, internal IT or security information, and other data vital to the organization's continued operations. If a suitably positioned adversary were to intercept or otherwise obtain the organization's email messages, they may be able to read this sensitive information as O365 emails are not cryptographically secured by default. O365 Message Encryption provides the ability to encrypt email sent through the organization's O365 instance and share encrypted email with any user that is emailed.

Remediation:

Enabling Office Message Encryption can be a significant process that entails enabling the technology, determining which cryptographic key management strategy will be used, and enabling Exchange mail transport rules that will automatically encrypt the organization's email. For many organizations, this process can be simplified by using Microsoft's default cryptographic key management scheme; however, this is a decision that can only be made by someone with contextual knowledge of the organization's constraints. Please follow the detailed guide linked in the References section for more information.

PowerShell Script:

```
$RMSConfig = Get-AipServiceConfiguration; $LicenseUri =
$RMSConfig.LicensingIntranetDistributionPointUrl; Set-IRMConfiguration
-LicensingLocation $LicenseUri; Set-IRMConfiguration -
InternalLicensingEnabled $true -ExternalLicensingEnabled $true -
AzureRMSLicensingEnabled $true
```

Returned Value:

InternalLicensingEnabled: False

AzureRMSLicensingEnabled: False

Default Value:

None

Expected Value:

True

Impact:

4

Likelihood:

2

Priority:

Medium

RiskRating: Medium

References:

↗ [Set up new Message Encryption capabilities]

Medium [7]: CIS MEx 1.3.3 - External sharing of calendars is available!

👎 CIS MEx 1.3.3 - External sharing of calendars is available!

ID: CISMEx133

Description:

Attackers often spend time learning about organizations before launching an attack. Publicly available calendars can help attackers understand organizational relationships and determine when specific users may be more vulnerable to an attack, such as when they are traveling.

Remediation:

Use the PowerShell Script to enable Modern Authentication for Microsoft Exchange Online. You can also check the text file which mailboxes have Calendar Sharing enabled.

PowerShell Script:

```powershell
$Policy = Get-SharingPolicy | Where-Object { $_.Domains -like " *
CalendarSharing*" }; Set-SharingPolicy -Identity $Policy.Name -Enabled
$False
```

Returned Value:

0

Default Value:

True and Every Mailbox

Expected Value:

False and 0 Mailboxes

Impact:

2

Likelihood:

5

Priority:

Medium

RiskRating: Medium

References:

[Share Microsoft 365 calendars with external users]

Medium [6]: CSTM-Ex021 - No Transport Rules to Block Large Attachment

👎 CSTM-Ex021 - No Transport Rules to Block Large Attachment

ID: CSTM-Ex021

Description:

No Exchange Online Transport Rules are in place to block emails with overly large attachments. Emails with overly large attachments may present a security risk for several reasons. Emails the domains receive may have overly large attachments that contain malware, and adversaries sometimes use overly large files in an attempt to bypass anti-malware scanners or otherwise avoid suspicion. An adversary with access to an organizational email account may also use a large attachment to exfiltrate sensitive data from the organization; for example, emailing an encrypted archive file to other adversarial infrastructure using a compromised O365 account. It is often recommended to create a rule that detects and blocks attachments over a certain size for these reasons.

Remediation:

Go to the Exchange Mail Flow rules screen and create a new rule which blocks attachments over a designated size.

PowerShell Script:

```
Get-Mailbox | Set-Mailbox -MaxSendSize 10MB -MaxReceiveSize 10MB; get-
transportconfig | Set-TransportConfig -maxsendsize 15MB -
maxreceivesize 15MB; get-receiveconnector | set-receiveconnector -
maxmessagesize 10MB; get-sendconnector | set-sendconnector -
maxmessagesize 10MB; get-mailbox | Set-Mailbox -Maxsendsize 10MB -
maxreceivesize 10MB; New-TransportRule -Name LargeAttach -
AttachmentSizeOver 10MB -RejectMessageReasonText "Message attachment
size over 10MB - email rejected."
```

Returned Value:

No-Reply Blocking

Default Value:

No Transport Rule

Expected Value:

Configured Transport Rule

Impact:

2

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

↗ [Common Attachment Blocking Scenarios]

Medium [6]: CIS MEx 6.1.2 - Mailbox auditing for E3 users is not enabled!

CIS MEx 6.1.2 - Mailbox auditing for E3 users is not enabled!

ID: CISMEx612

Description:

Whether it is for regulatory compliance or for tracking unauthorized configuration changes in Microsoft 365, enabling mailbox auditing, and ensuring the proper mailbox actions are accounted for allows for Microsoft 365 teams to run security operations, forensics or general investigations on mailbox activities

Remediation:

$AuditAdmin = @("Copy", "Create", "FolderBind", "HardDelete", "MessageBind", "Move", "MoveToDeletedItems", "SendAs", "SendOnBehalf", "SoftDelete", "Update", "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"); $AuditDelegate = @("Create", "FolderBind", "HardDelete", "Move", "MoveToDeletedItems", "SendAs", "SendOnBehalf", "SoftDelete", "Update", "UpdateFolderPermissions", "UpdateInboxRules"); $AdminOwner = @("Create", "HardDelete", "MailboxLogin", "Move", "MoveToDeletedItems", "SoftDelete", "Update", "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"); Then use the PowerShell Script to remediate this issue.

PowerShell Script:

```
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditEnabled True -
AuditLogAgeLimit 180 -AuditAdmin  -AuditDelegate  -AuditOwner
```

Returned Value:

AuditDisabled:

Default Value:

False

Expected Value:

True

Impact:

2

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

[Manage mailbox auditing]

Medium [6]: CIS MEx 6.1.1 - Mailbox auditing is not Enabled for all users

👎 CIS MEx 6.1.1 - Mailbox auditing is not Enabled for all users

ID: CISMEx611

Description:

Enforcing the default ensures auditing was not turned off intentionally or accidentally. Auditing mailbox actions will allow forensics and IR teams to trace various malicious activities that can generate TTPs caused by inbox access and tampering

Remediation:

$AuditAdmin = @("Copy", "Create", "FolderBind", "HardDelete", "MailItemsAccessed", "Move", "MoveToDeletedItems", "SendAs", "SendOnBehalf", "SoftDelete", "Update", "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"); $AuditDelegate = @("Create", "FolderBind", "HardDelete", "Move", "MoveToDeletedItems", "SendAs", "SendOnBehalf", "SoftDelete", "Update", "UpdateFolderPermissions", "UpdateInboxRules"); $AdminOwner = @("Create", "HardDelete", "MailboxLogin", "Move", "MoveToDeletedItems", "SoftDelete", "Update", "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"); Then use the PowerShell Script to remediate this issue.

PowerShell Script:

```
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditEnabled $true -
AuditLogAgeLimit 180 -AuditAdmin $AuditAdmin -AuditDelegate
$AuditDelegate -AuditOwner $AuditOwner; Set-OrganizationConfig -
AuditDisabled $false
```

Returned Value:

AuditDisabled: @{AuditDisabled=False}

Default Value:

False

Expected Value:

True

Impact:

2

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

↗ Manage mailbox auditing

Medium [6]: CIS MEx 3.2.1 - DLP Policy is not enabled!

👎 CIS MEx 3.2.1 - DLP Policy is not enabled!

ID: CISMEx321

Description:

Enabling DLP policies alerts users and administrators that specific types of data should not be exposed, helping to protect the data from accidental exposure.

Remediation:

Use the PowerShell script to configure a New-Dlp Compliance Policy

PowerShell Script:

```
New-DlpPolicy -Name "Contoso PII"" -Template {templatehere}
```

Returned Value:

No DLP Policy Active

Default Value:

No Policy

Expected Value:

A Policy

Impact:

2

Likelihood:

3

Priority:

Informational

RiskRating: Medium

References:

↗ Learn about data loss prevention

Medium [6]: CIS MEx 3.1.1 - Microsoft 365 audit log search is Disabled!

👎 CIS MEx 3.1.1 - Microsoft 365 audit log search is Disabled!

ID: CISMEx311

Description:

Enabling audit log search in the Microsoft Purview compliance portal can help organizations improve their security posture, meet regulatory compliance requirements, respond to security incidents, and gain valuable operational insights.

Remediation:

Use the PowerShell script to enable the AuditLog in Microsoft Exchange

PowerShell Script:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

Returned Value:

False

Default Value:

False

Expected Value:

True

Impact:

2

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

↗ Enable/Disable the Audit Log

Medium [6]: CIS MEx 6.1.3 - Mailbox auditing for E5 users is not enabled!

👎 CIS MEx 6.1.3 - Mailbox auditing for E5 users is not enabled!

ID: CISMEx613

Description:

Whether it is for regulatory compliance or for tracking unauthorized configuration changes in Microsoft 365, enabling mailbox auditing, and ensuring the proper mailbox actions are accounted for allows for Microsoft 365 teams to run security operations, forensics or general investigations on mailbox activities

Remediation:

$AuditAdmin = @("Copy", "Create", "FolderBind", "HardDelete", "MessageBind", "Move", "MoveToDeletedItems", "SendAs", "SendOnBehalf", "SoftDelete", "Update", "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"); $AuditDelegate = @("Create", "FolderBind", "HardDelete", "Move", "MoveToDeletedItems", "SendAs", "SendOnBehalf", "SoftDelete", "Update", "UpdateFolderPermissions", "UpdateInboxRules"); $AdminOwner = @("Create", "HardDelete", "MailboxLogin", "Move", "MoveToDeletedItems", "SoftDelete", "Update", "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"); Then use the PowerShell Script to remediate this issue.

PowerShell Script:

```
$MBX = Get-EXOMailbox -ResultSize Unlimited | Where-Object
{$_.RecipientTypeDetails -eq "UserMailbox" }; $MBX | Set-Mailbox -
AuditEnabled $true -AuditLogAgeLimit 180 -AuditAdmin $AuditAdmin -
AuditDelegate $AuditDelegate -AuditOwner $AuditOwner
```

Returned Value:

file://C:\Out/CISMEx613-MailboxAuditSettingsPerE5User.txt

Default Value:

False

Expected Value:

True

Impact:

2

Likelihood:

3

Priority:

Medium

RiskRating: Medium

References:

↗ Manage mailbox auditing

High [15]: CIS MEx 2.4.2 - Priority accounts do not have 'Strict protection' presets applied

👎 CIS MEx 2.4.2 - Priority accounts do not have 'Strict protection' presets applied

ID: CISMEx242

Description:

Enabling priority account protection for users in Microsoft 365 is necessary to enhance security for accounts with access to sensitive data and high privileges, such as CEOs, CISOs, CFOs, and IT admins. These priority accounts are often targeted by spear phishing or whaling attacks and require stronger protection to prevent account compromise. To address this, Microsoft 365 and Microsoft Defender for Office 365 offer several key features that provide extra security, including the identification of incidents and alerts involving priority accounts and the use of built-in custom protections designed specifically for them.

Remediation:

Use the PowerShell Script to enable PriorityAccountProtection

PowerShell Script:

```
Enable-EOPProtectionPolicyRule -Identity "Strict Preset Security
Policy"; Enable-ATPProtectionPolicyRule -Identity "Strict Preset
Security Policy"
```

Returned Value:

No Strict AntiPhishPolicy Available No Strict MalwareFilterPolicy Available No Strict HostedContentFilterPolicy Available No Strict SafeAttachmentPolicy Available No Strict SafeLinksPolicy Available No Strict EOPProtectionPolicy Available No Strict ATPProtectionPolicy Available

Default Value:

True

Expected Value:

True

Impact:

3

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

- [Preset security policies in EOP and Microsoft Defender for Office 365]
- [Recommended settings for EOP and Microsoft Defender for Office 365 security]

Security recommendations for priority accounts in Microsoft 365

High [15]: CIS MEx 2.1.4 - Safe Attachments Not Enabled

CIS MEx 2.1.4 - Safe Attachments Not Enabled

ID: CISMEx214

Description:

Enabling Safe Attachments policy helps protect against malware threats in email attachments by analyzing suspicious attachments in a secure, cloud-based environment before they are delivered to the user's inbox. This provides an additional layer of security and can prevent new or unseen types of malware from infiltrating the organization's network.

Remediation:

Run the following PowerShell command:

PowerShell Script:

```
$domains = Get-AcceptedDomain; New-SafeAttachmentPolicy -Name "Safe Attachment Policy" -Enable $true -Redirect $false -RedirectAddress $ITSupportEmail New-SafeAttachmentRule -Name "Safe Attachment Rule" -SafeAttachmentPolicy "Safe Attachment Policy" -RecipientDomainIs $domains[0]
```

Returned Value:

No SafeAttachmentPolicy Found!

Default Value:

False

Expected Value:

True

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

Deploy ATP with PowerShell

High [15]: CIS MEx 2.1.7 - Anti-Phishing policy not has been created

CIS MEx 2.1.7 - Anti-Phishing policy not has been created

ID: CISMEx217

Description:

Protects users from phishing attacks (like impersonation and spoofing), and uses safety tips to warn users about potentially harmful messages.

Remediation:

Rune the following command to create a new AntiPhishPolicy

PowerShell Script:

```
$domains = Get-AcceptedDomain; New-AntiPhishPolicy -Name "AntiPhish
Policy" -Enabled $true -EnableOrganizationDomainsProtection $true -
EnableSimilarUsersSafetyTips $true -EnableSimilarDomainsSafetyTips
$true -EnableUnusualCharactersSafetyTips $true -
AuthenticationFailAction Quarantine -
EnableMailboxIntelligenceProtection $true -
MailboxIntelligenceProtectionAction movetoJMF -PhishThresholdLevel 2 -
TargetedUserProtectionAction movetoJMF -
EnableTargetedDomainsProtection $true -TargetedDomainProtectionAction
MovetoJMF -EnableAntispoofEnforcement $true New-AntiPhishRule -Name
"AntiPhish Rule" -AntiPhishPolicy "AntiPhish Policy" -
RecipientDomainIs $domains[0]
```

Returned Value:

PhishThresholdLevel:

Default Value:

No Policy

Expected Value:

A Policy

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

[Securing Your Office 365 Tenants. Part 2]

↗ Configure anti-phishing policies

High [15]: CIS MEx 6.5.3 - Additional storage providers are not restricted in Outlook on the Web

👎 CIS MEx 6.5.3 - Additional storage providers are not restricted in Outlook on the Web

ID: CISMEx653

Description:

By default additional storage providers are allowed in Office on the Web (such as Box, Dropbox, Facebook, Google Drive, OneDrive Personal, etc.). This could lead to information leakage and additional risk of infection from organizational non-trusted storage providers. Restricting this will inherently reduce risk as it will narrow opportunities for infection and data leakage.

Remediation:

Use the PowerShell Script to remediate this issue. You can check with the PowerShell command: **Get-OwaMailboxPolicy | Format-Table Name, AdditionalStorageProvidersAvailable** if the remediation has been successful!

PowerShell Script:

```
Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -
AdditionalStorageProvidersAvailable $false
```

Returned Value:

OwaMailboxPolicy-Default: AdditionalStorageProvidersAvailable: True

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

[3rd party cloud storage services supported by Office apps]

High [12]: CSTM-Ex027 - MailboxPlans Have Legacy Protocols Enabled

👎 CSTM-Ex027 - MailboxPlans Have Legacy Protocols Enabled

ID: CSTM-Ex027

Description:

For Exchange Online, Microsoft provides many protocols for end users to connect to their mailbox. We have IMAP, POP, ActiveSync, ECP, MAPI, OWA and more. Typically, we want to block less secure protocols like IMAP4 and POP3 so that users will not use these to connect a mailbox to.

Remediation:

Execute the PowerShell command to disable the legacy protocols

PowerShell Script:

```
New-AuthenticationPolicy -Name "Block Legacy Authentication"; Get-
CASMailboxPlan -Filter {SmtpClientAuthenticationDisabled -eq "false" }
| Set-CASMailboxPlan -ActiveSyncEnabled: $false -PopEnabled: $false -
ImapEnabled: $false -MAPIEnabled: $false; Get-CASMailbox -Filter
{SmtpClientAuthenticationDisabled -eq "true"} | Select-Object @{n =
"Identity"; e = {$_.primarysmtpaddress}} | Set-CASMailbox -
ActiveSyncEnabled: $false -PopEnabled: $false -ImapEnabled: $false -
MAPIEnabled: $false
```

Returned Value:

108 Affected Objects Identified.

Default Value:

ActiveSyncEnabled,PopEnabled,ImapEnabled,EwsEnabled,MapiEnabled = True

Expected Value:

ActiveSyncEnabled,PopEnabled,ImapEnabled,EwsEnabled,MapiEnabled = False

Impact:

4

Likelihood:

3

Priority:

High

RiskRating: High

References:

- ↗ How to: Block legacy authentication access to Azure AD with Conditional Access
- ↗ How To Block Legacy Authentication Office 365

↗ Block Legacy Authentication now, and do not wait for Microsoft

High [12]: CSTM-Ex025 - Exchange Mailboxes with POP Enabled

CSTM-Ex025 - Exchange Mailboxes with POP Enabled

ID: CSTM-Ex025

Description:

The Exchange Online mailboxes listed have POP enabled. POP is a method of accessing an Exchange Online mailbox. Cyber adversaries have used POP as a workaround for subtly conducting password spraying attacks or other credential-related attacks, because POP is a form of legacy authentication generally not subject to the restraints of Multi-Factor Authentication and other modern authentication safeguards. For these reasons it is recommended that POP be disabled where possible.

Remediation:

This finding refers to individual mailboxes that have POP enabled. For these mailboxes, POP authentication can be disabled using the Set-CASMailbox commandlet. A list of affected email addresses is included in this report. Key stakeholders should be polled prior to making this change, as there is a chance POP is used within the organization for legacy applications or service accounts.

PowerShell Script:

```
Get-CASMailboxPlan -Filter {PopEnabled -eq "true" } | Set-
CASMailboxPlan -ImapEnabled $false; Get-CASMailbox -Filter
{ImapEnabled -eq "true"} | Select-Object @{n = "Identity"; e =
{$_.primarysmtpaddress}} | Set-CASMailbox -PopEnabled $false
```

Returned Value:

18 Affected Objects Identified.

Default Value:

True

Expected Value:

False

Impact:

4

Likelihood:

3

Priority:

High

RiskRating: High

References:

Configure mailbox access (POP3 and IMAP)

- Set-CASMailbox Commandlet Reference
- Federal Bureau of Investigation Business Email Compromise Mitigation Recommendations
- How to disable POP and IMAP for all Mailboxes in Office 365

High [12]: CSTM-Ex029 - Outlook Web Application Offline Mode Enabled

👎 CSTM-Ex029 - Outlook Web Application Offline Mode Enabled

ID: CSTM-Ex029

Description:

One of the oft-overlooked features of web mail, known as OWA, is the offline mode feature. This feature leaves an unencrypted copy of the last 500 emails on your device for easy access while you are not connected.

Remediation:

Use the PowerShell Script to disable AllowOfflineOn for all computers

PowerShell Script:

```
Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -AllowOfflineOn NoComputers
```

Returned Value:

OwaMailboxPolicy-Default

AllowOfflineOn: AllComputers

Default Value:

No restrictions

Expected Value:

NoComputers are allowed to AllowOfflineOn

Impact:

3

Likelihood:

4

Priority:

Medium

RiskRating: High

References:

- [Disable offline access in Outlook on the Web at a global level]
- [Office 365 - Have You Evaluated These Exchange Online Features?]

High [12]: CSTM-Ex030 - Multiple Weak Protocols in Outlook Web Application Enabled

👎 CSTM-Ex030 - Multiple Weak Protocols in Outlook Web Application Enabled

ID: CSTM-Ex030

Description:

Some protocols could lead to information exposure towards public areas. Consider disabling the settings to harden Microsoft Exchange Security.

Remediation:

Use the PowerShell Script to disable AllowOfflineOn for all computers

PowerShell Script:

```
Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -
ActiveSyncIntegrationEnabled $false -
AdditionalStorageProvidersAvailable $false -BoxAttachmentsEnabled
$false -DisableFacebook $true -DropboxAttachmentsEnabled $false -
GoogleDriveAttachmentsEnabled $false -LinkedInEnabled $false -
OneDriveAttachmentsEnabled $true -OutlookBetaToggleEnabled $true -
ReportJunkEmailEnabled $true -SilverlightEnabled $false
```

Returned Value:

ActiveSyncIntegrationEnabled True

SilverlightEnabled True

FacebookEnabled True

LinkedInEnabled True

Default Value:

Weak Protocols Are Enabled

Expected Value:

Weak Protocols Are Disabled

Impact:

4

Likelihood:

3

Priority:

Medium

RiskRating: High

References:

↗ [Reference - Set-OwaMailboxPolicy]()

↗ [OWA Mailbox Policy Configuration - With PowerShell!]()

High [12]: CSTM-Ex023 - Exchange Mailboxes with IMAP Enabled

CSTM-Ex023 - Exchange Mailboxes with IMAP Enabled

ID: CSTM-Ex023

Description:

The Exchange Online mailboxes listed above have IMAP Authentication enabled. IMAP Authentication is a method of authenticating to an Exchange Online mailbox. Cyber adversaries have used IMAP authentication as a workaround for subtly conducting password spraying attacks or other credential-related attacks, because IMAP authentication is a form of legacy authentication generally not subject to the restraints of Multi-Factor Authentication and other modern authentication safeguards. For these reasons it is recommended that IMAP Authentication be disabled where possible.

Remediation:

Use the PowerShell Command to disable Mailboxes with IMAP Check with Get-CasMailbox -ResultSize unlimited -Filter PopEnabled -eq $false -and ImapEnabled -eq $false

PowerShell Script:

```
Get-CASMailboxPlan -Filter {ImapEnabled -eq "true" } | set-
CASMailboxPlan -ImapEnabled $false; Get-CASMailbox -Filter
{ImapEnabled -eq "true"} | Select-Object @{n = "Identity"; e =
{$_.primarysmtpaddress}} | Set-CASMailbox -ImapEnabled $false
```

Returned Value:

18 Affected Objects Identified.

Default Value:

True

Expected Value:

False

Impact:

4

Likelihood:

3

Priority:

High

RiskRating: High

References:

- Configure mailbox access (POP3 and IMAP)
- Set-CASMailbox Commandlet Reference
- Federal Bureau of Investigation Business Email Compromise Mitigation Recommendations

↗ How to disable POP and IMAP for all Mailboxes in Office 365

High [12]: CIS MEx 2.1.3 - Notifications for internal users sending malware is Disabled

CIS MEx 2.1.3 - Notifications for internal users sending malware is Disabled

ID: CISMEx213

Description:

This setting alerts administrators that an internal user sent a message that contained malware. This may indicate an account or machine compromise, that would need to be investigated.

Remediation:

Configure a MalwareFilterPolicy by using the PowerShellScript

PowerShell Script:

```
Set-MalwareFilterPolicy -Identity "Malware Filter Policy Name" -Action
DeleteMessage -EnableInternalSenderAdminNotifications $true -
InternalSenderAdminAddress "admin@yourdomain.com"
```

Returned Value:

Default: has EnableInternalSenderAdminNotifications on False and as addresses

Default Value:

EnableInternalSenderAdminNotifications: False

Expected Value:

True, with a configured mailbox or distribution list address

Impact:

3

Likelihood:

4

Priority:

High

RiskRating: High

References:

[Configuring Exchange Online Protection]

[Set-MalwareFilterPolicy Commandlet Reference Example 1]

High [12]: CSTM-Ex032 - SMTP Authentication not Globally Disabled

👎 CSTM-Ex032 - SMTP Authentication not Globally Disabled

ID: CSTM-Ex032

Description:

SMTP Authentication is a method of authenticating to an Exchange Online mailbox to deliver email. Cyber adversaries have used SMTP authentication as a workaround for subtly conducting password spraying attacks or other credential-related attacks and bypassing multi-factor authentication protection because legacy authentication methods such as SMTP do not support MFA. There are two ways of disabling SMTP, globally and granularly on a per-user-mailbox level. It is recommended that SMTP Authentication be globally disabled if possible. Note that this may disrupt the functionality of legacy or other applications that require it or continued operations.

Remediation:

Use the PowerShell to create a new SafeLinksPolicy to disable and enable all recommended settings!

PowerShell Script:

```
Set-TransportConfig -SmtpClientAuthenticationDisabled $true
```

Returned Value:

SmtpClientAuthenticationDisabled: False

Default Value:

True

Expected Value:

True

Impact:

4

Likelihood:

3

Priority:

High

RiskRating: High

References:

↗ [Enable or disable authenticated client SMTP submission (SMTP AUTH) in Exchange Online]()

↗ [Set-CASMailbox Commandlet Reference]()

High [12]: CSTM-Ex016 - Exchange Mailboxes with Forwarding Rules to External Recipients

CSTM-Ex016 - Exchange Mailboxes with Forwarding Rules to External Recipients

ID: CSTM-Ex016

Description:

Email forwarding can be useful but can also pose a security risk due to the potential disclosure of information. Attackers might use this information to attack your organization or partners. The mailboxes returned in this finding all forward mail to external recipients.

Remediation:

This finding refers to individual mailboxes that have forwarding rules enabled to external recipients. For these mailboxes, verify that the forwarding rules do not violate company policy, are expected, and allowed. Remediation can be accomplished by running the PowerShell command. A list of affected email addresses is included in this report. You can use the references as well to remediate this issue

PowerShell Script:

```
Get-Mailbox -ResultSize Unlimited | Where {($_.ForwardingAddress -ne
$Null) -or ($_.ForwardingsmtpAddress -ne $Null)} | Set-Mailbox -
ForwardingAddress $null -ForwardingSmtpAddress $null -
DeliverToMailboxAndForward $false; Get-RemoteDomain | Set-RemoteDomain
-AutoForwardEnabled $false
```

Returned Value:

2

Default Value:

0

Expected Value:

0

Impact:

4

Likelihood:

3

Priority:

High

RiskRating: High

References:

- Office 365 - List all email forwarding rules (PowerShell)
- Get-Mailbox Commandlet Reference
- Remove forwarding from Office 365 Mailboxes with Powershell

↗ DISABLE FORWARDING IN OWA WITH POWERSHELL

High [12]: CSTM-Ex013 - Exchange Mailboxes with FullAccess Delegates Found

CSTM-Ex013 - Exchange Mailboxes with FullAccess Delegates Found

ID: CSTM-Ex013

Description:

The Exchange Online mailboxes listed above have delegated Full Access permissions to another account.

Remediation:

This finding refers to individual mailboxes that have Full Access delegated permissions. For these mailboxes, verify that the delegate access is expected, appropriate, and do not violate company policy.

PowerShell Script:

```
Remove-MailboxPermission -Identity mailbox -AccessRights FullAccess -
Confirm:$false -User user
```

Returned Value:

9

Default Value:

0

Expected Value:

0

Impact:

4

Likelihood:

3

Priority:

High

RiskRating: High

References:

[Remove-MailboxPermission Commandlet Reference]

High [12]: CSTM-Ex004 - Exchange does not have a Authentication Policy Enabled

CSTM-Ex004 - Exchange does not have a Authentication Policy Enabled

ID: CSTM-Ex004

Description:

Exchange Online faces a lot of attacks, attack vectors and malicious actors. Having BasicAuthenitcation not disabled leaves the M365 vulnerable for brute force attacks and weak security of accounts

Remediation:

Use the PowerShell script to set the Authentication Policy

PowerShell Script:

```
Set-AuthenticationPolicy -Identity "" -AllowBasicAuthActiveSync:$False
-AllowBasicAuthAutodiscover:$False -AllowBasicAuthImap:$False -
AllowBasicAuthMapi:$False -AllowBasicAuthOfflineAddressBook:$False -
AllowBasicAuthOutlookService:$False -AllowBasicAuthPop:$False -
AllowBasicAuthReportingWebServices:$False -AllowBasicAuthRest:$False -
AllowBasicAuthRpc:$False -AllowBasicAuthSmtp:$False -
AllowBasicAuthWebServices:$False -
AllowBasicAuthPowershell:$FalsengWebServices $False -AllowBasicAuthRpc
$False -AllowBasicAuthSmtp $False -AllowBasicAuthWebServices $False -
AllowBasicAuthPowershell $False
```

Returned Value:

No Authentication Policy Found!

Default Value:

No Authentication Policy

Expected Value:

An Authentication Policy

Impact:

4

Likelihood:

3

Priority:

Medium

RiskRating: High

References:

[PowerShell and Exchange Online Security]

High [12]: CIS MEx 2.1.1 - Safe Links for Office Applications is not Enabled!

👎 CIS MEx 2.1.1 - Safe Links for Office Applications is not Enabled!

ID: CISMEx211

Description:

Enabling Safe Links policy for Office applications allows URL's that exist inside of Office documents and email applications opened by Office, Office Online and Office mobile to be processed against Defender for Office time-of-click verification and rewritten if required. Safe Links for Office applications extends phishing protection to documents and emails that contain hyperlinks, even after they have been delivered to a user.

Remediation:

Use the PowerShell Script to create and apply the policy within your organization.

PowerShell Script:

```
$params = @{ Name = "CIS SafeLinks Policy" EnableSafeLinksForEmail =
$true EnableSafeLinksForTeams = $true EnableSafeLinksForOffice = $true
TrackClicks = $true AllowClickThrough = $false ScanUrls = $true
EnableForInternalSenders = $true DeliverMessageAfterScan = $true
DisableUrlRewrite = $false }; New-SafeLinksPolicy @params ; New-
SafeLinksRule -Name "CIS SafeLinks" -SafeLinksPolicy "CIS SafeLinks
Policy" -RecipientDomainIs (Get-AcceptedDomain).Name -Priority 0
```

Returned Value:

Subscription is not Active. Thus SafeLinks is not working

Default Value:

Undefined

Expected Value:

EnableSafeLinksForEmail: True EnableSafeLinksForTeams: True EnableSafeLinksForOffice: True TrackClicks: True AllowClickThrough: False ScanUrls: True EnableForInternalSenders: True DeliverMessageAfterScan: True DisableUrlRewrite: False

Impact:

3

Likelihood:

4

Priority:

High

RiskRating: High

References:

SafeLinks Policy Configuration

> ↗ Preset Security Policies

High [12]: CSTM-Ex018 - Dangerous Attachment Extensions are Not Filtered

CSTM-Ex018 - Dangerous Attachment Extensions are Not Filtered

ID: CSTM-Ex018

Description:

Email is a primary vector of exploitation. It is common for attackers to send malicious file attachments designed to mimic legitimate business files. A list of historically malicious extensions that should be blocked/filtered from O365 emails is checked against the Tenant's malware filters to determine if these file types are being blocked. The file extensions listed herein are on this list of dangerous file extensions, but no O365 Malware Filter Policy is configured to filter them. Creating filters for these file types may decrease the risk of malware spreading within the organization through phishing or lateral phishing. The common malicious attachments defined in O365 at the time this document was authored are: xll, wll, rtf, reg, ws, wsf, vb, wsc, wsh, msh, msh1, msh2, mshxml, msh1xml, msh2xml, ps1, ps1xml, ps2, ps2xml, psc1, psc2, pif, msi, gadget, application, com, cpl, msc, hta, msp, bat, cmd, js, jse, scf, lnk, inf, dotm, xlsm, xltm, xlam, pptm, potm, ppam, ppsm, sldm

Remediation:

This finding refers to individual mailboxes that have Full Access delegated permissions. For these mailboxes, verify that the delegate access is expected, appropriate, and do not violate company policy.

PowerShell Script:

```
Set-MalwareFilterPolicy Default -FileTypes ade,adp,cpl,app,bas,asx,bat,chm,cmd,com,crt,csh,dotm,exe,fxp,hlp,hta,inf,ins,isp,js,jse,ksh,lnk,mda,mdb,mde,mdt,mdw,mdz,msc,msi,msp,mst,ops,pcd,pif,prf,prg,ps1,ps11,ps11xml,ps1xml,ps2,ps2xml,psc1,psc2,reg,scf,scr,sct,shb,shs,url,vb,vbe,vbs,wsc,wsf,wsh,xnk,ace,ani,docm,jar,asp,cer,der,dll,dos,gadget,Hta,Inf,Ins,Isp,Its,Jse,Ksh,Lnk,mad,maf,mag,mam,maq,mar,mas,mat,mau,mav,maw,msh,msh1,msh1xml,msh2,msh2xml,mshxml,obj,os2,plg,pst,rar,tmp,vsmacros,vsw,vxd,w16,ws,apk,appx,cab,iso,library,lib,msix,mhtml,msixbundle,terminal,plugin,font,command,bundle -EnableFileFilter $true
```

Returned Value:

90

Default Value:

0

Expected Value:

0

Impact:

3

Likelihood:

4

Priority:

High

RiskRating: High

References:

↗ 50+ File Extensions That Are Potentially Dangerous on Windows

↗ Set-MalwareFilterPolicy

High [10]: CIS MEx 1.3.6 - CustomerLockbox Feature is disabled

CIS MEx 1.3.6 - CustomerLockbox Feature is disabled

ID: CISMEx136

Description:

Customer Lockbox is a security feature that provides an additional layer of control and transparency to customer data in Microsoft 365. It offers an approval process for Microsoft support personnel to access organization data and creates an audited trail to meet compliance requirements. Enabling this feature protects organizational data against data spillage and exfiltration.

Remediation:

Use the PowerShell script to enable CustomerLockBox for your Exchange Tenant

PowerShell Script:

```
Set-OrganizationConfig -CustomerLockBoxEnabled $true
```

Returned Value:

CustomerLockBoxEnabled: False

Default Value:

False

Expected Value:

True

Impact:

2

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

[Customer Lockbox Overview]

High [10]: CIS MEx 6.3.1 - Users can Install Outlook Add-ins

CIS MEx 6.3.1 - Users can Install Outlook Add-ins

ID: CISMEx631

Description:

Attackers commonly use vulnerable and custom-built add-ins to access data in user applications. While allowing users to install add-ins by themselves does allow them to easily acquire useful add-ins that integrate with Microsoft applications, it can represent a risk if not used and monitored carefully.

Remediation:

Use the Tenable Reference and use the PowerShell template within the article.

PowerShell Script:

```
New-RoleAssignmentPolicy -Name "Example" -Roles $revisedRoles
```

Returned Value:

Policy contains My Custom Apps!

Policy contains My Marketplace Apps!

Default Value:

Users can Install Outlook Add-Ins

Expected Value:

Users cannot Install Outlook Add-Ins

Impact:

2

Likelihood:

5

Priority:

High

RiskRating: High

References:

[Specify the administrators and users who can install and manage add-ins for Outlook in Exchange Online]

[Role assignment policies in Exchange Online]

High [10]: CIS MEx 6.2.3 - Email from external senders cannot be identified

👎 CIS MEx 6.2.3 - Email from external senders cannot be identified

ID: CISMEx623

Description:

Tagging emails from external senders helps to inform end users about the origin of the email. This can allow them to proceed with more caution and make informed decisions when it comes to identifying spam or phishing emails.

Remediation:

Use the PowerShell script to enable CustomerLockBox for your Exchange Tenant

PowerShell Script:

```
Set-ExternalInOutlook -Enabled $true
```

Returned Value:

250ca08f-eeb3-4252-b9a5-f26f540404d1: False

Default Value:

False

Expected Value:

True

Impact:

2

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

↗ [Native external sender callouts on email in Outlook]()

High [10]: CIS MEx 2.1.5 - Safe Attachments for Office Applications is not Enabled!

CIS MEx 2.1.5 - Safe Attachments for Office Applications is not Enabled!

ID: CISMEx215

Description:

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams protects organizations from inadvertently sharing malicious files. When a malicious file is detected, that file is blocked so that no one can open, copy, move, or share it until further actions are taken by the organization's security team.

Remediation:

Use the PowerShell Script to create and apply the policy within your organization.

PowerShell Script:

```
Set-AtpPolicyForO365 -EnableATPForSPOTeamsODB $true -EnableSafeDocs
$true -AllowSafeDocsOpen $false
```

Returned Value:

ATP Policy is not working!

Default Value:

Undefined

Expected Value:

EnableATPForSPOTeamsODB: True EnableSafeDocs: True AllowSafeDocsOpen: False

Impact:

2

Likelihood:

5

Priority:

High

RiskRating: High

References:

[Deploy ATP with PowerShell]

Microsoft Azure

Informational [0]: CIS Az 7.3 - OS and Data disks are not encrypted with Customer Managed Keys (CMK)

CIS Az 7.3 - OS and Data disks are not encrypted with Customer Managed Keys (CMK)

ID: CISAz73

Description:

Encrypting the IaaS VM's OS disk (boot volume) and Data disks (non-boot volume) ensures that the entire content is fully unrecoverable without a key, thus protecting the volume from unwanted reads. PMK (Platform Managed Keys) are enabled by default in Azure-managed disks and allow encryption at rest. CMK is recommended because it gives the customer the option to control which specific keys are used for the encryption and decryption of the disk. The customer can then change keys and increase security by disabling them instead of relying on the PMK key that remains unchanging. There is also the option to increase security further by using automatically rotating keys so that access to disk is ensured to be limited. Organizations should evaluate what their security requirements are, however, for the data stored on the disk. For high-risk data using CMK is a must, as it provides extra steps of security. If the data is low risk, PMK is enabled by default and provides sufficient data security.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName
$vmName -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $KeyVaultResourceId;
```

Returned Value:

cloud-ct-base_OsDisk_1_bfbf6b887ee44479b7d06c8904a4e942 testcompany-vpn_OsDisk_1_6fb6cc26136241c5b0ac53ad8c5f2bfd

Default Value:

By default, Azure disks are encrypted using SSE with PMK.

Expected Value:

VMs with an Managed Disk.

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

↗ Overview of managed disk encryption options
↗ Use asset inventory to manage your resources security posture
↗ Azure data security and encryption best practices
↗ Azure PowerShell - Enable customer-managed keys with server-side encryption - managed disks
↗ Server-side encryption of Azure Disk Storage

Informational [0]: CIS Az 9.8 - 'HTTP Version' is not the Latest, if Used to Run the Web App

CIS Az 9.8 - 'HTTP Version' is not the Latest, if Used to Run the Web App

ID: CISAz98

Description:

Newer versions may contain security enhancements and additional functionality. Using the latest version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected. HTTP 2.0 has additional performance improvements on the head-of-line blocking problem of old HTTP version, header compression, and prioritization of requests. HTTP 2.0 no longer supports HTTP 1.1's chunked transfer encoding mechanism, as it provides its own, more efficient, mechanisms for data streaming.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Set-AzWebApp -ResourceGroupName  -Name  -Http20Enabled $true
```

Returned Value:

testcompany-zabbix.azurewebsites.net testcompany-grafana.azurewebsites.net testcompany-pgadmin.azurewebsites.net testcompany-cms.azurewebsites.net

Default Value:

Disabled

Expected Value:

Enabled

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[Configure an App Service app]

Informational [0]: CIS Az 9.6 - 'Python version' is not the Latest, If Used to Run the Web App

👍 CIS Az 9.6 - 'Python version' is not the Latest, If Used to Run the Web App

ID: CISAz96

Description:

Newer versions may contain security enhancements and additional functionality. Using the latest software version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Set-AzWebApp -AssignIdentity $True -ResourceGroupName  -Name
```

Returned Value:

testcompany-zabbix.azurewebsites.net testcompany-grafana.azurewebsites.net testcompany-pgadmin.azurewebsites.net analytics-store.azurewebsites.net testcompanywebapp.azurewebsites.net testcompany-cms.azurewebsites.net testcompany.azurewebsites.net orcaremediation-aaa4382d-7c6b-58.azurewebsites.net

Default Value:

By default, this is per-user's choice

Expected Value:

Latest version available online

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

↗ [Configure an App Service app]()

Informational [0]: CIS Az 7.7 - Some VHDs / OS / Data Disks are not Encrypted

CIS Az 7.7 - Some VHDs / OS / Data Disks are not Encrypted

ID: CISAz77

Description:

While it is recommended to use Managed Disks which are encrypted by default, 'legacy' VHDs may exist for a variety of reasons and may need to remain in VHD format. VHDs are not encrypted by default, so this recommendation intends to address the security of these disks. In these niche cases, VHDs should be encrypted using the procedures in this recommendation to encrypt and protect the data content.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
New-AzKeyvault -name  -ResourceGroupName  -Location  -
EnabledForDiskEncryption; $KeyVault = Get-AzKeyVault -VaultName  -
ResourceGroupName ; Set-AzVMDiskEncryptionExtension -ResourceGroupName
 -VMName  -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -
DiskEncryptionKeyVaultId $KeyVault.ResourceId
```

Returned Value:

cloud-ct-base testcompany-vpn

Default Value:

NO Encryption

Expected Value:

Encryption

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[Create a managed disk from a VHD file in a storage account in same or different subscription with PowerShell]

Informational [0]: CIS Az 8.1 - Expiration Date is not set for all Keys in RBAC Key Vaults

CIS Az 8.1 - Expiration Date is not set for all Keys in RBAC Key Vaults

ID: CISAz81

Description:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The exp (expiration date) attribute identifies the expiration date on or after which the key MUST NOT be used for encryption of new data, wrapping of new keys, and signing. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration date for all keys to help enforce the key rotation. This ensures that the keys cannot be used beyond their assigned lifetimes

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Set-AzKeyVaultKeyAttribute -VaultName  -Name  -Expires
```

Returned Value:

testcompany-keyvault1

Default Value:

No Expiration

Expected Value:

An Expiration Date + Time

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[Azure Key Vault basic concepts]

Informational [0]: CIS Az 9.5 - 'PHP version' is not the Latest, If Used to Run the Web App

CIS Az 9.5 - 'PHP version' is not the Latest, If Used to Run the Web App

ID: CISAz95

Description:

Newer versions may contain security enhancements and additional functionality. Using the latest software version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Set-AzWebApp -AssignIdentity $True -ResourceGroupName  -Name
```

Returned Value:

testcompany-zabbix.azurewebsites.net testcompany-grafana.azurewebsites.net testcompany-pgadmin.azurewebsites.net analytics-store.azurewebsites.net testcompanywebapp.azurewebsites.net testcompany-cms.azurewebsites.net testcompany.azurewebsites.net orcaremediation-aaa4382d-7c6b-58.azurewebsites.net

Default Value:

By default, this is per-user's choice

Expected Value:

Latest version available online

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[Configure an App Service app]

Informational [0]: CIS Az 9.4 - Register with Entra ID is not enabled on App Service

CIS Az 9.4 - Register with Entra ID is not enabled on App Service

ID: CISAz94

Description:

App Service provides a highly scalable, self-patching web hosting service in Azure. It also provides a managed identity for apps, which is a turn-key solution for securing access to Azure SQL Database and other Azure services.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Set-AzWebApp -AssignIdentity $True -ResourceGroupName  -Name
```

Returned Value:

testcompany-zabbix.azurewebsites.net testcompany-grafana.azurewebsites.net testcompany-pgadmin.azurewebsites.net testcompany-cms.azurewebsites.net

Default Value:

By default, Managed service identity via Entra ID is disabled.

Expected Value:

Enabled

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[Tutorial: Connect to SQL Database from .NET App Service without secrets using a managed identity]()

Informational [0]: CIS Az 8.8 - Private Endpoints are not Used for Azure Key Vault

CIS Az 8.8 - Private Endpoints are not Used for Azure Key Vault

ID: CISAz88

Description:

Once set up, Automatic Private Key Rotation removes the need for manual administration when keys expire at intervals determined by your organization's policy. The recommended key lifetime is 2 years. Your organization should determine its own key expiration policy.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Update-AzKeyVault -ResourceGroupName  -VaultName  -
EnableRbacAuthorization $True
```

Returned Value:

testcompany-keyvault1 yolotoonnx0425418561

Default Value:

By default, Automatic Key Rotation is not enabled.

Expected Value:

Automatic Key Rotation is enabled.

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[Configure cryptographic key auto-rotation in Azure Key Vault]

Informational [0]: CIS Az 8.3 - Expiration Date is not set for all Secrets in RBAC Key Vaults

CIS Az 8.3 - Expiration Date is not set for all Secrets in RBAC Key Vaults

ID: CISAz83

Description:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The exp (expiration date) attribute identifies the expiration date on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration date for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Set-AzKeyVaultSecretAttribute -VaultName  -Name  -Expires
```

Returned Value:

testcompany-keyvault1

Default Value:

No Expiration

Expected Value:

An Expiration Date + Time

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

Azure Key Vault basic concepts

Informational [0]: CIS Az 8.4 - Expiration Date is not set for all Secrets in Non-RBAC Key Vaults

CIS Az 8.4 - Expiration Date is not set for all Secrets in Non-RBAC Key Vaults

ID: CISAz84

Description:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The exp (expiration date) attribute identifies the expiration date on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration date for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Set-AzKeyVaultSecretAttribute -VaultName  -Name  -Expires
```

Returned Value:

testcompany-keyvault1

Default Value:

No Expiration

Expected Value:

An Expiration Date + Time

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[Azure Key Vault basic concepts]

Informational [0]: CIS Az 8.7 - Private Endpoints are not Used for Azure Key Vault

CIS Az 8.7 - Private Endpoints are not Used for Azure Key Vault

ID: CISAz87

Description:

Private endpoints will keep network requests to Azure Key Vault limited to the endpoints attached to the resources that are whitelisted to communicate with each other. Assigning the Key Vault to a network without an endpoint will allow other resources on that network to view all traffic from the Key Vault to its destination. In spite of the complexity in configuration, this is recommended for high security secrets.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Update-AzKeyVault -ResourceGroupName  -VaultName  -
EnableRbacAuthorization $True
```

Returned Value:

testcompany-keyvault1 yolotoonnx0425418561

Default Value:

By default, Private Endpoints are not enabled for any services within Azure.

Expected Value:

Private Endpoints are enabled for any services within Azure.

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

- [What is a private endpoint?]()
- [Use private endpoints for Azure Storage]()
- [Integrate Key Vault with Azure Private Link]()
- [Tutorial: Connect to a storage account using an Azure Private Endpoint]()

Informational [0]: CIS Az 7.1 - An Azure Bastion Host Does not Exist

CIS Az 7.1 - An Azure Bastion Host Does not Exist

ID: CISAz71

Description:

The Azure Bastion service allows organizations a more secure means of accessing Azure Virtual Machines over the Internet without assigning public IP addresses to those Virtual Machines. The Azure Bastion service provides Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Virtual Machines using TLS within a web browser, thus preventing organizations from opening up 3389/TCP and 22/TCP to the Internet on Azure Virtual Machines. Additional benefits of the Bastion service includes Multi-Factor Authentication, Conditional Access Policies, and any other hardening measures configured within Azure Active Directory using a central point of access

Remediation:

No PowerShell Script Available

PowerShell Script:

```
New-AzBastion -ResourceGroupName  -Name  -PublicIpAddress $publicip -
VirtualNetwork $virtualNet -Sku "Standard" -ScaleUnit
```

Returned Value:

testcompany-core testcompany-wireguard-vpn_group testcompanyWebsite Analytics-Jets SecurityCentre NetworkWatcherRG securitycentre analytics-jets VisualStudioOnline-1793A15812F14BCCAC37AF9F1E6105DC testcompany-CORE jenolantimedelayoccupanc testcompany-WIREGUARD-VPN_GROUP testcompany-pgadmin_group testcompanywebsite benedict1-rg DefaultResourceGroup-eastus2 Orca-Remediation

Default Value:

By default, the Azure Bastion service is not configured.

Expected Value:

the Azure Bastion service is configured.

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[What is Azure Bastion?]

Informational [0]: CIS Az 7.5 - Check if Approved Extensions Are Installed

CIS Az 7.5 - Check if Approved Extensions Are Installed

ID: CISAz75

Description:

Azure virtual machine extensions are small applications that provide post-deployment configuration and automation tasks on Azure virtual machines. These extensions run with administrative privileges and could potentially access anything on a virtual machine. The Azure Portal and community provide several such extensions. Each organization should carefully evaluate these extensions and ensure that only those that are approved for use are actually implemented.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Remove-AzVMExtension -ResourceGroupName  -Name  -VMName
```

Returned Value:

cloud-ct-base: AADSSHLoginForLinux cloud-ct-base: AzurePerformanceDiagnosticsLinux cloud-ct-base: AzurePolicyforLinux cloud-ct-base: OmsAgentForLinux testcompany-vpn: AADSSHLoginForLinux testcompany-vpn: AzurePolicyforLinux testcompany-vpn: OmsAgentForLinux

Default Value:

By default, no extensions are added to the virtual machines.

Expected Value:

Only approved Extensions

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[Virtual machine extensions and features for Windows]()

Informational [0]: CIS Az 8.5 - Some Key Vaults are not Recoverable

👍 CIS Az 8.5 - Some Key Vaults are not Recoverable

ID: CISAz85

Description:

There could be scenarios where users accidentally run delete/purge commands on Key Vault or an attacker/malicious user deliberately does so in order to cause disruption. Deleting or purging a Key Vault leads to immediate data loss, as keys encrypting data and secrets/certificates allowing access/services will become non-accessible. There is a Key Vault property that plays a role in permanent unavailability of a Key Vault: enablePurgeProtection: Setting this parameter to 'true' for a Key Vault ensures that even if Key Vault is deleted, Key Vault itself or its objects remain recoverable for the next 90 days. Key Vault/objects can either be recovered or purged (permanent deletion) during those 90 days. If no action is taken, the key vault and its objects will subsequently be purged. Enabling the enablePurgeProtection parameter on Key Vaults ensures that Key Vaults and their objects cannot be deleted/purged permanently.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Update-AzKeyVault -VaultName  -EnablePurgeProtection
```

Returned Value:

testcompany-keyvault1 yolotoonnx0425418561

Default Value:

enableSoftDelete: null enablePurgeProtection: null

Expected Value:

enableSoftDelete: true enablePurgeProtection: true

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

↗ [Azure Key Vault soft-delete overview]

Informational [0]: CIS MAz 2.4.3 - Unable to verify if Microsoft Defender for Cloud Apps is enabled and configured

CIS MAz 2.4.3 - Unable to verify if Microsoft Defender for Cloud Apps is enabled and configured

ID: CISMAz243

Description:

Security teams can receive notifications of triggered alerts for atypical or suspicious activities, see how the organization's data in Microsoft 365 is accessed and used, suspend user accounts exhibiting suspicious activity, and require users to log back in to Microsoft 365 apps after an alert has been triggered

Remediation:

The implementation of Microsoft Defender for Cloud App MUST be done manually, because there is no automatic script available at this moment.

PowerShell Script:

```
https://learn.microsoft.com/en-us/defender-cloud-apps/get-started
```

Returned Value:

Default Value:

No Microsoft Defender for Cloud Apps active

Expected Value:

Microsoft Defender for Cloud Apps active

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

- Microsoft Defender for Cloud Apps - Get Started
- Microsoft Defender for Cloud Apps - Policies

Informational [0]: CIS Az 8.6 - Role Based Access Control for Azure Key is not Enabled

CIS Az 8.6 - Role Based Access Control for Azure Key is not Enabled

ID: CISAz86

Description:

The new RBAC permissions model for Key Vaults enables a much finer grained access control for key vault secrets, keys, certificates, etc., than the vault access policy. This in turn will permit the use of privileged identity management over these roles, thus securing the key vaults with JIT Access management.

Remediation:

No PowerShell Script Available

PowerShell Script:

```
Update-AzKeyVault -ResourceGroupName  -VaultName  -
EnableRbacAuthorization $True
```

Returned Value:

yolotoonnx0425418561

Default Value:

EnableRbacAuthorization: False

Expected Value:

EnableRbacAuthorization: True

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

[What is Azure role-based access control (Azure RBAC)?]

Low [4]: CIS Az 1.1.1 - Security Defaults is disabled in Microsoft Entra ID

CIS Az 1.1.1 - Security Defaults is disabled in Microsoft Entra ID

ID: CISAz11

Description:

Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks.

Remediation:

Use the PowerShell Script to enable Security Defaults on Microsoft Azure Active Directory

PowerShell Script:

```
$body = $body = (@{"isEnabled"="true"} | ConvertTo-Json) ;Invoke-MgGraphRequest -Method PATCH https://graph.microsoft.com/beta/policies/identitySecurityDefaultsEnforcementPolicy -Body $body
```

Returned Value:

SecureDefaultsState.isEnabled: False

Default Value:

True for tenants created later than 2019, False for tenants created before 2019

Expected Value:

True

Impact:

4

Likelihood:

1

Priority:

Medium

RiskRating: Low

References:

[Security defaults in Microsoft Entra ID]

[Introducing security defaults]

[IM-2: Protect identity and authentication systems]

Low [4]: CISMAz 5.1.3.1 - No dynamic group for guest users is created!

CISMAz 5.1.3.1 - No dynamic group for guest users is created!

ID: CISMAz5131

Description:

Dynamic Groups allow for an automated method to assign group membership. Guest user accounts will be automatically added to this group and through this existing conditional access rules, access controls and other security measures will ensure that new guest accounts are restricted in the same manner as existing guest accounts.

Remediation:

Use the PowerShell Script to create a Dynamic Group for Guests

PowerShell Script:

```
$params = @{ DisplayName = "Dynamic Test Group"  MailNickname =
"DynGuestUsers"  MailEnabled = $false SecurityEnabled = $true
GroupTypes = "DynamicMembership"  MembershipRule = "(user.userType -eq
"Guest")" MembershipRuleProcessingState = "On"}; New-MgGroup @params
```

Returned Value:

0

Default Value:

0

Expected Value:

At least 1

Impact:

4

Likelihood:

1

Priority:

Medium

RiskRating: Low

References:

- Create or update a dynamic group in Microsoft Entra ID
- Dynamic membership rules for groups in Microsoft Entra ID
- Create dynamic groups in Microsoft Entra B2B collaboration

Low [3]: CIS Az 1.5 - Number of methods required to reset a password is not set to 2 or more methods

CIS Az 1.5 - Number of methods required to reset a password is not set to 2 or more methods

ID: CISAz150

Description:

A Self-service Password Reset (SSPR) through Azure Multi-factor Authentication (MFA) ensures the user's identity is confirmed using two separate methods of identification. With multiple methods set, an attacker would have to compromise both methods before they could maliciously reset a user's password.

Remediation:

Manually change the value from 1 to 2 in the Azure Portal. There is no script available at this moment unfortunately.

PowerShell Script:

```
https://portal.azure.com/#view/Microsoft_AAD_IAM/PasswordResetMenuBlade
/~/AuthenticationMethods
```

Returned Value:

1

Default Value:

2

Expected Value:

2

Impact:

3

Likelihood:

1

Priority:

High

RiskRating: Low

References:

- [Tutorial: Enable users to unlock their account or reset passwords using Microsoft Entra self-service password reset]
- [Combined security information registration for Microsoft Entra overview]
- [IM-6: Use strong authentication controls]
- [Password reset registration]
- [Plan a Microsoft Entra self-service password reset deployment]
- [What authentication and verification methods are available in Microsoft Entra ID?]

Low [2]: CIS Az 3.7 - 'Public access level' is enabled for some storage accounts

CIS Az 3.7 - 'Public access level' is enabled for some storage accounts

ID: CISAz37

Description:

The default configuration for a storage account permits a user with appropriate permissions to configure public (anonymous) access to containers and blobs in a storage account. Keep in mind that public access to a container is always turned off by default and must be explicitly configured to permit anonymous requests. It grants read□only access to these resources without sharing the account key, and without requiring a shared access signature. It is recommended not to provide anonymous access to blob containers until, and unless, it is strongly desired. A shared access signature token or Azure AD RBAC should be used for providing controlled and timed access to blob containers. If no anonymous access is needed on any container in the storage account, it’s recommended to set allowBlobPublicAccess false at the account level, which forbids any container to accept anonymous access in the future.

Remediation:

You can change the settings in the URL written in PowerShellScript.

PowerShell Script:

```
Set-AzStorageAccount -ResourceGroupName  -Name  -PublicNetworkAccess
Disabled
```

Returned Value:

Default Value:

Enabled

Expected Value:

Disabled

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Configure anonymous read access for containers and blobs
- Assign an Azure role for access to blob data
- Remediate anonymous read access to blob data (classic deployments)
- Remediate anonymous read access to blob data (Azure Resource Manager deployments)

Low [2]: CIS Az 3.17 - Some Azure Storage Accounts have their 'Allow Blob Anonymous Access' set to Enabled

CIS Az 3.17 - Some Azure Storage Accounts have their 'Allow Blob Anonymous Access' set to Enabled

ID: CISAz317

Description:

If 'Allow Blob Anonymous Access' is enabled, blobs can be accessed by adding the blob name to the URL to see the contents. An attacker can enumerate a blob using methods, such as brute force, and access them. Exfiltration of data by brute force enumeration of items from a storage account may occur if this setting is set to 'Enabled

Remediation:

You can change the settings in the by executing the written PowerShellScript.

PowerShell Script:

```
Set-AzStorageAccount -ResourceGroupName  -Name  -
allowCrossTenantReplication $false
```

Returned Value:

orcaremediationaaa4382d testcompanyfunctions jenolantimedelayoc8c092e

Default Value:

Disabled

Expected Value:

Disabled

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- [Remediate anonymous read access to blob data (Azure Resource Manager deployments)]()
- [Remediate anonymous read access to blob data (classic deployments)]()

Low [2]: CIS Az 3.16 - 'Cross Tenant Replication' is enabled

CIS Az 3.16 - 'Cross Tenant Replication' is enabled

ID: CISAz316

Description:

Disabling Cross Tenant Replication minimizes the risk of unauthorized data access and ensures that data governance policies are strictly adhered to. This control is especially critical for organizations with stringent data security and privacy requirements, as it prevents the accidental sharing of sensitive information.

Remediation:

You can change the settings in the by executing the written PowerShellScript.

PowerShell Script:

```
Set-AzStorageAccount -ResourceGroupName  -Name  -
allowCrossTenantReplication $false
```

Returned Value:

orcaremediationaaa4382d testcompanyaz testcompanyfunctions jenolantimedelayoc8c092e

Default Value:

Enabled on accounts before Dec 15 2023, else disabled

Expected Value:

Disabled

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

[Prevent object replication across Microsoft Entra tenants]

Low [2]: CIS Az 3.15 - The Minimum TLS version for some storage accounts is not set to minimum Version 1.2

CIS Az 3.15 - The Minimum TLS version for some storage accounts is not set to minimum Version 1.2

ID: CISAz315

Description:

TLS 1.0 has known vulnerabilities and has been replaced by later versions of the TLS protocol. Continued use of this legacy protocol affects the security of data in transit.

Remediation:

You can change the settings in the by executing the written PowerShellScript.

PowerShell Script:

```
Set-AzStorageAccount -ResourceGroupName  -Name  -MinimumTlsVersion
TLS1_2
```

Returned Value:

orcaremediationaaa4382d testcompanycoreperfdiag880 jenolantimedelayoc8c092e

Default Value:

TLS1_2 if created via portal. Else TLS1_0

Expected Value:

TLS1_2

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

[Enforce a minimum required version of Transport Layer Security (TLS) for requests to a storage account]

Low [2]: CIS Az 3.4 - Setting Some Storage Account Access Keys are not Periodically Regenerated

👍 CIS Az 3.4 - Setting Some Storage Account Access Keys are not Periodically Regenerated

ID: CISAz34

Description:

When a storage account is created, Azure generates two 512-bit storage access keys which are used for authentication when the storage account is accessed. Rotating these keys periodically ensures that any inadvertent access or exposure does not result from the compromise of these keys.

Remediation:

You can change the settings in the URL written in PowerShellScript.

PowerShell Script:

```
Get-AzStorageAccount | Set-AzStorageAccount -Name
$_.StorageAccountName -KeyExpirationPeriodInDay 90
```

Returned Value:

orcaremediationaaa4382d yolotoonnx2724207365 testcompanyaz testcompanycoreperfdiag880 testcompanyfunctions jenolantimedelayoc8c092e

Default Value:

null

Expected Value:

90

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- [Create a storage account]
- [PCI DSS Key Rotation Requirements]
- [NIST 800-57 Rev. 5 - Recommendation for Key Management]

Low [2]: CIS Az 3.3 - Setting 'Enable key rotation reminders' is not enabled for each Storage Account

👍 CIS Az 3.3 - Setting 'Enable key rotation reminders' is not enabled for each Storage Account

ID: CISAz33

Description:

Reminders such as those generated by this recommendation will help maintain a regular and healthy cadence for activities which improve the overall efficacy of a security program. Cryptographic key rotation periods will vary depending on your organization's security requirements and the type of data which is being stored in the Storage Account. For example, PCI DSS mandates that cryptographic keys be replaced or rotated 'regularly,'and advises that keys for static data stores be rotated every 'few months.'For the purposes of this recommendation, 90 days will prescribed for the reminder. Review and adjustment of the 90 day period is recommended, and may even be necessary. Your organization's security requirements should dictate the appropriate setting

Remediation:

You can change the settings in the URL written in PowerShellScript.

PowerShell Script:

```
Get-AzStorageAccount | Set-AzStorageAccount -Name
$_.StorageAccountName -KeyExpirationPeriodInDay 90
```

Returned Value:

orcaremediationaaa4382d yolotoonnx2724207365 testcompanyaz testcompanycoreperfdiag880 testcompanyfunctions jenolantimedelayoc8c092e

Default Value:

Null

Expected Value:

KeyExpirationPeriodInDay: 90

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- [Create a storage account]()
- [PCI DSS Key Rotation Requirements]()

↗ NIST 800-57 Rev. 5 - Recommendation for Key Management

Low [2]: CIS Az 3.11 - Soft Delete is not Enabled for some Azure Containers and Blob Storage

👍 CIS Az 3.11 - Soft Delete is not Enabled for some Azure Containers and Blob Storage

ID: CISAz311

Description:

Containers and Blob Storage data can be incorrectly deleted. An attacker/malicious user may do this deliberately in order to cause disruption. Deleting an Azure Storage blob causes immediate data loss. Enabling this configuration for Azure storage ensures that even if blobs/data were deleted from the storage account, Blobs/data objects are recoverable for a particular time which is set in the 'Retention policies,' ranging from 7 days to 365 days

Remediation:

You can change the settings in the by executing the written PowerShellScript.

PowerShell Script:

```
Set-AzStorageAccount -ResourceGroupName  -Name  -Bypass AzureServices
```

Returned Value:

orcaremediationaaa4382d yolotoonnx2724207365 testcompanyaz testcompanycoreperfdiag880 testcompanyfunctions jenolantimedelayoc8c092e

Default Value:

Disabled

Expected Value:

Enabled

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- [Use private endpoints for Azure Storage]
- [What is Azure Virtual Network?]
- [Quickstart: Create a private endpoint by using the Azure portal]
- [Quickstart: Create a private endpoint by using the Azure CLI]
- [Tutorial: Connect to a storage account using an Azure Private Endpoint]

Low [2]: CIS Az 5.1.3 - Some storage accounts containing containers with activity logs are not encrypted with Customer Managed Keys (CMK)

👍 CIS Az 5.1.3 - Some storage accounts containing containers with activity logs are not encrypted with Customer Managed Keys (CMK)

ID: CISAz513

Description:

Configuring the storage account with the activity log export container to use CMKs provides additional confidentiality controls on log data, as a given user must have read permission on the corresponding storage account and must be granted decrypt permission by the CMK.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
Set-AzStorageAccount
```

Returned Value:

Default Value:

KeySource: Microsoft.Storage

Expected Value:

KeySource: Microsoft.Keyvault

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

↗ [Managing legacy log profiles]()

Low [2]: CIS Az 3.12 - Some Storage for Critical Data is not Encrypted with Customer Managed Keys

CIS Az 3.12 - Some Storage for Critical Data is not Encrypted with Customer Managed Keys

ID: CISAz312

Description:

By default, data in the storage account is encrypted using Microsoft Managed Keys at rest. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted. If you want to control and manage this encryption key yourself, however, you can specify a customer-managed key. That key is used to protect and control access to the key that encrypts your data. You can also choose to automatically update the key version used for Azure Storage encryption whenever a new version is available in the associated Key Vault.

Remediation:

You can change the settings in the by executing the written PowerShellScript.

PowerShell Script:

```
Set-AzStorageAccount -ResourceGroupName  -Name  -Bypass AzureServices
```

Returned Value:

orcaremediationaaa4382d yolotoonnx2724207365 testcompanyaz testcompanycoreperfdiag880 testcompanyfunctions jenolantimedelayoc8c092e

Default Value:

Encryption: Microsoft Managed Keys

Expected Value:

Encryption: Customer Managed Keys

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- [Azure Storage encryption for data at rest]
- [Protect data at rest]
- [About Azure Storage service-side encryption]

Low [2]: CIS Az 5.2.1 - Activity Log Alert do not exist for Create Policy Assignment

CIS Az 5.2.1 - Activity Log Alert do not exist for Create Policy Assignment

ID: CISAz521

Description:

Monitoring for create policy assignment events gives insight into changes done in 'Azure policy - assignments' and can reduce the time it takes to detect unsolicited changes.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Authorization/policyAssignments/write

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Classic alerts in Azure Monitor to retire in June 2019
- Create or edit an activity log, service health, or resource health alert rule
- Create or edit a log search alert rule

Low [2]: CIS Az 5.2.10 - Activity Log Alert does not exist for Delete Public IP Address rules

CIS Az 5.2.10 - Activity Log Alert does not exist for Delete Public IP Address rules

ID: CISAz5210

Description:

Monitoring for Delete Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Network/publicIPAddresses/delete

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Classic alerts in Azure Monitor to retire in June 2019
- Create or edit an activity log, service health, or resource health alert rule
- Create or edit a log search alert rule

Low [2]: CIS Az 5.2.2 - Activity Log Alert does not exist for Delete Policy Assignment

CIS Az 5.2.2 - Activity Log Alert does not exist for Delete Policy Assignment

ID: CISAz522

Description:

Monitoring for create policy assignment events gives insight into changes done in 'Azure policy - assignments' and can reduce the time it takes to detect unsolicited changes.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Authorization/policyAssignments/delete

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Classic alerts in Azure Monitor to retire in June 2019
- Create or edit an activity log, service health, or resource health alert rule
- Create or edit a log search alert rule

Low [2]: CIS Az 5.2.3 - Activity Log Alert does not exist for Create or Update Network Security Groups

👍 CIS Az 5.2.3 - Activity Log Alert does not exist for Create or Update Network Security Groups

ID: CISAz523

Description:

Monitoring for Create or Update Network Security Group events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Network/networkSecurityGroups/write

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- ↗ Classic alerts in Azure Monitor to retire in June 2019
- ↗ Create or edit an activity log, service health, or resource health alert rule
- ↗ Create or edit a log search alert rule

Low [2]: CIS Az 5.2.4 - Activity Log Alert does not exist for Delete Network Security Groups

CIS Az 5.2.4 - Activity Log Alert does not exist for Delete Network Security Groups

ID: CISAz524

Description:

Monitoring for Create or Update Network Security Group events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Network/networkSecurityGroups/delete

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Classic alerts in Azure Monitor to retire in June 2019
- Create or edit an activity log, service health, or resource health alert rule
- Create or edit a log search alert rule

Low [2]: CIS Az 5.2.5 - Activity Log Alert does not exist for Create or Update Security Solutions

👍 CIS Az 5.2.5 - Activity Log Alert does not exist for Create or Update Security Solutions

ID: CISAz525

Description:

Monitoring for Create or Update Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Security/securitySolutions/write

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- ↗ [Classic alerts in Azure Monitor to retire in June 2019]()
- ↗ [Create or edit an activity log, service health, or resource health alert rule]()
- ↗ [Create or edit a log search alert rule]()

Low [2]: CIS Az 3.8 - Some Default Network Access Rules for Storage Accounts are not Set to Deny

CIS Az 3.8 - Some Default Network Access Rules for Storage Accounts are not Set to Deny

ID: CISAz38

Description:

Storage accounts should be configured to deny access to traffic from all networks (including internet traffic). Access can be granted to traffic from specific Azure Virtual networks, allowing a secure network boundary for specific applications to be built.Access can also be granted to public internet IP address ranges to enable connections from specific internet or on-premises clients. When network rules are configured, only applications from allowed networks can access a storage account. When calling from an allowed network, applications continue to require proper authorization (a valid access key or SAS token) to access the storage account.

Remediation:

You can change the settings in the URL written in PowerShellScript.

PowerShell Script:

```
Set-AzStorageAccount -ResourceGroupName  -Name  -NetworkRuleSet Deny
```

Returned Value:

Default Value:

Allow

Expected Value:

Deny

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

[Configure Azure Storage firewalls and virtual networks]

Low [2]: CIS Az 2.2.1 - Ensure That Microsoft Defender for IoT Hub Is Set To 'On'

👍 CIS Az 2.2.1 - Ensure That Microsoft Defender for IoT Hub Is Set To 'On'

ID: CISAz221

Description:

IoT devices are very rarely patched and can be potential attack vectors for enterprise networks. Updating their network configuration to use a central security hub allows for detection of these breaches

Remediation:

You can change the settings in the URL written in PowerShellScript.

PowerShell Script:

```
https://portal.azure.com/#view/Microsoft_Azure_SubscriptionManagement/ManageSubscriptionPoliciesBlade
```

Returned Value:

Unable to audit...

Default Value:

Off

Expected Value:

On

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

↗ Defender EASM Overview

↗ Create a Defender EASM Azure resource

Low [2]: CIS Az 5.4 - Azure Monitor Resource Logging is not Enabled for All Services that Support it

👍 CIS Az 5.4 - Azure Monitor Resource Logging is not Enabled for All Services that Support it

ID: CISAz54

Description:

A lack of monitoring reduces the visibility into the data plane, and therefore an organization's ability to detect reconnaissance, authorization attempts or other malicious activity. Unlike Activity Logs, Resource Logs are not enabled by default. Specifically, without monitoring it would be impossible to tell which entities had accessed a data store that was breached. In addition, alerts for failed attempts to access APIs for Web Services or Databases are only possible when logging is enabled.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzApplicationInsights
```

Returned Value:

Diagnostic Settings not configured for resource: cloud-ct-base-nsg Diagnostic Settings not configured for resource: testcompany-vpn-nsg Diagnostic Settings not configured for resource: testcompany-cms Diagnostic Settings not configured for resource: testcompany-grafana Diagnostic Settings not configured for resource: analytics.testdomain.com.au-testcompany-grafana Diagnostic Settings not configured for resource: cloud-ct-base/AADSSHLoginForLinux Diagnostic Settings not configured for resource: testcompanywebapp Diagnostic Settings not configured for resource: vault-lnkvf6yr Diagnostic Settings not configured for resource: testcompany-postgres Diagnostic Settings not configured for resource: LPR-Hub Diagnostic Settings not configured for resource: DefaultWorkspace-c292b24b-4160-4fc3-a417-c42d1f729f58-EAU Diagnostic Settings not configured for resource: NetworkWatcher_australiaeast Diagnostic Settings not configured for resource: SecurityCenterFree(DefaultWorkspace-c292b24b-4160-4fc3-a417-c42d1f729f58-EAU) Diagnostic Settings not configured for resource: Security(DefaultWorkspace-c292b24b-4160-4fc3-a417-c42d1f729f58-EAU) Diagnostic Settings not configured for resource: SQLVulnerabilityAssessment(DefaultWorkspace-c292b24b-4160-4fc3-a417-c42d1f729f58-EAU) Diagnostic Settings not configured for resource: SQLAdvancedThreatProtection(DefaultWorkspace-c292b24b-4160-4fc3-a417-c42d1f729f58-EAU) Diagnostic Settings not configured for resource: ct.testdomain.com.au-testcompanydash Diagnostic Settings not configured for resource: hugh_rg_Linux_australiacentral-AustraliaCentralwebspace-Linux-220906010648 Diagnostic Settings not configured for resource: CTTier1 Diagnostic Settings not configured for resource: privatelink.azureiotcentral.com/7ifhakasvfdby Diagnostic Settings not configured for resource:

> testcompany-iotcentral Diagnostic Settings not configured for resource: transport-nsw Diagnostic Settings not configured for resource: Failure Anomalies - testcompany-analytics-storer Diagnostic Settings not configured for resource: workspacetestcompanycore83d2 Diagnostic Settings not configured for resource: testcompany-vnet-firewall-mgt-ip Diagnostic Settings not configured for resource: testcompany-postgres.private.postgres.database.azure.com/7ifhakasvfdby Diagnostic Settings not configured for resource: testcompany-iotcentral Diagnostic Settings not configured for resource: testcompany-eventshub Diagnostic Settings not configured for resource: privatelink.servicebus.windows.net Diagnostic Settings not configured for resource: testcompanyaz Diagnostic Settings not configured for resource: cloud-ct-base Diagnostic Settings not configured for resource: testcompany-vnet-firewall-basic-policy Diagnostic Settings not configured for resource: functions Diagnostic Settings not configured for resource: privatelink.azurewebsites.net/7ifhakasvfdby Diagnostic Settings not configured for resource: Failure Anomalies - testcompany-functions Diagnostic Settings not configured for resource: cloud-ct-base Diagnostic Settings not configured for resource: testcompany-analytics-storer Diagnostic Settings not configured for resource: privatelink.azure-devices.net Diagnostic Settings not configured for resource: analytics-store Diagnostic Settings not configured for resource: cloud-ct-base_OsDisk_1_bfbf6b887ee44479b7d06c8904a4e942 Diagnostic Settings not configured for resource: ct.testdomain.com.au-testcompanywebapp Diagnostic Settings not configured for resource: Failure Anomalies - analytics-storer Diagnostic Settings not configured for resource: Failure Anomalies - analytics-store Diagnostic Settings not configured for resource: workspace-EAU-c292b24b-4160-4fc3-a417-c42d1f729f58-conduci-b2fd Diagnostic Settings not configured for resource: cloud-ct-base/OmsAgentForLinux Diagnostic Settings not configured for resource: jenolantimedelayoc8c092e Diagnostic Settings not configured for resource: testcompany-core-vnet-ip Diagnostic Settings not configured for resource: functions-nic Diagnostic Settings not configured for resource: Failure Anomalies - jenolantimedelayoccupanc Diagnostic Settings not configured for resource: jenolantimedelayoccupanc Diagnostic Settings not configured for resource: testcompanyfunctions Diagnostic Settings not configured for resource: transport-nsw-private-endpoint Diagnostic Settings not configured for resource: privatelink.azure-devices-provisioning.net/7ifhakasvfdby Diagnostic Settings not configured for resource: testcompany-core-vpn-ip-2 Diagnostic Settings not configured for resource: privatelink.servicebus.windows.net/7ifhakasvfdby Diagnostic Settings not configured for resource: privatelink.azurewebsites.net Diagnostic Settings not configured for resource: transport-nsw-private-endpoint-nic Diagnostic Settings not configured for resource: testcompany-iotcentral-nic Diagnostic Settings not configured for resource: eventhub-private-endpoint Diagnostic Settings not configured for resource: testcompany-analytics-function Diagnostic Settings not configured for resource: vm-address-publicIpAddress Diagnostic Settings not configured for resource: privatelink.azure-devices-provisioning.net Diagnostic Settings not configured for resource: analytics-storer Diagnostic Settings not configured for resource: testcompany-functions Diagnostic Settings not configured for resource: privatelink.azureiotcentral.com Diagnostic Settings not configured for resource: ASP-JenolanTimedelayOccupancy-75d8 Diagnostic Settings not configured for resource:

testcompany-keyvault1 Diagnostic Settings not configured for resource: cloud-ct-base/AzurePolicyforLinux Diagnostic Settings not configured for resource: privatelink.azure-devices.net/7ifhakasvfdby Diagnostic Settings not configured for resource: api.testdomain.com.au-analytics-store Diagnostic Settings not configured for resource: testcompany-core-vpn-ip-3 Diagnostic Settings not configured for resource: testcompany-postgres.private.postgres.database.azure.com Diagnostic Settings not configured for resource: Failure Anomalies - testcompany-analytics-function Diagnostic Settings not configured for resource: Application Insights Smart Detection Diagnostic Settings not configured for resource: testcompanycoreperfdiag880 Diagnostic Settings not configured for resource: ASP-testcompanyWebsite-a3d3 Diagnostic Settings not configured for resource: testcompany-core-vnet Diagnostic Settings not configured for resource: testcompany-vpn617_z1 Diagnostic Settings not configured for resource: testcompany-vpn Diagnostic Settings not configured for resource: cloud-ct-base352 Diagnostic Settings not configured for resource: testcompany-vpn_OsDisk_1_6fb6cc26136241c5b0ac53ad8c5f2bfd Diagnostic Settings not configured for resource: testcompany-vpn_key Diagnostic Settings not configured for resource: cloud-ct-base/AzurePerformanceDiagnosticsLinux Diagnostic Settings not configured for resource: testcompany-vpn/OmsAgentForLinux Diagnostic Settings not configured for resource: testcompany-vpn/AzurePolicyforLinux Diagnostic Settings not configured for resource: eventhub-private-endpoint.nic.9f082858-9ac7-43f4-b42c-5409442a906d Diagnostic Settings not configured for resource: testcompanyWebsitePlan Diagnostic Settings not configured for resource: testcompany-core-vpn-ip-1 Diagnostic Settings not configured for resource: testcompany Diagnostic Settings not configured for resource: testcompany-zabbix Diagnostic Settings not configured for resource: sentry.testdomain.com.au-testcompany-zabbix Diagnostic Settings not configured for resource: nexus.testdomain.com.au-testcompany-cms Diagnostic Settings not configured for resource: testcompany-iothub Diagnostic Settings not configured for resource: testcompany-iothub-dps Diagnostic Settings not configured for resource: testcompany-vpn/AADSSHLoginForLinux Diagnostic Settings not configured for resource: 14df1c96-d7b9-41fc-9bb0-64cbf1d2620f-dashboard Diagnostic Settings not configured for resource: workspace-EAU-c292b24b-4160-4fc3-a417-c42d1f729f58-conduci-9ff5 Diagnostic Settings not configured for resource: testcompany-pgadmin Diagnostic Settings not configured for resource: Failure Anomalies - testcompany-pgadmin Diagnostic Settings not configured for resource: conduicve-pgadmin Diagnostic Settings not configured for resource: Failure Anomalies - conduicve-pgadmin Diagnostic Settings not configured for resource: testcompany-pgadmin Diagnostic Settings not configured for resource: testcompanyWebsite-AustraliaEastwebspace-Linux-240903025725 Diagnostic Settings not configured for resource: yolotoonnx2724207365 Diagnostic Settings not configured for resource: DefaultWorkspace-eastus2 Diagnostic Settings not configured for resource: yolotoonnx3331197126 Diagnostic Settings not configured for resource: yolo_to_onnx Diagnostic Settings not configured for resource: Failure Anomalies - yolotoonnx3331197126 Diagnostic Settings not configured for resource: OrcaRemediation-aaa4382d-7c6b-58 Diagnostic Settings not configured for resource: orcaremediationaaa4382d Diagnostic Settings not configured for resource: EastUSLinuxDynamicPlan Diagnostic Settings not configured for resource: OrcaRemediationaaa4382d-7c6b-58 Diagnostic Settings not configured for resource: Failure Anomalies - OrcaRemediation-aaa4382d-7c6b-58

Default Value:

Application Insights are not enabled by default.

Expected Value:

Enabled

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- ↗ Monitor Azure resources with Azure Monitor
- ↗ Supported categories for Azure Monitor resource logs
- ↗ Stream Azure Monitor activity log data
- ↗ Azure Key Vault logging
- ↗ Sources of monitoring data for Azure Monitor and their data collection methods
- ↗ Common and service-specific schemas for Azure resource logs
- ↗ Diagnostic logs - Azure Content Delivery Network

Low [2]: CIS Az 5.2.7 - Activity Log Alert does not exist for Create and Update SQL Server Firewall Rules

CIS Az 5.2.7 - Activity Log Alert does not exist for Create and Update SQL Server Firewall Rules

ID: CISAz527

Description:

Monitoring for Create or Update SQL Server Firewall Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Sql/servers/firewallRules/write

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Classic alerts in Azure Monitor to retire in June 2019
- Create or edit an activity log, service health, or resource health alert rule
- Create or edit a log search alert rule

Low [2]: CIS Az 5.2.8 - Activity Log Alert does not exist for Delete SQL Server Firewall Rules

CIS Az 5.2.8 - Activity Log Alert does not exist for Delete SQL Server Firewall Rules

ID: CISAz528

Description:

Monitoring for Delete SQL Server Firewall Rule events gives insight into SQL network access changes and may reduce the time it takes to detect suspicious activity.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Sql/servers/firewallRules/delete

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Classic alerts in Azure Monitor to retire in June 2019
- Create or edit an activity log, service health, or resource health alert rule
- Create or edit a log search alert rule

Low [2]: CIS Az 5.2.9 - Activity Log Alert does not exist for Create or Update Public IP Address rules

👍 CIS Az 5.2.9 - Activity Log Alert does not exist for Create or Update Public IP Address rules

ID: CISAz529

Description:

Monitoring for Create or Update Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Network/publicIPAddresses/write

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Classic alerts in Azure Monitor to retire in June 2019
- Create or edit an activity log, service health, or resource health alert rule
- Create or edit a log search alert rule

Low [2]: CIS Az 5.2.6 - Activity Log Alert does not exist for Delete Security Solutions

CIS Az 5.2.6 - Activity Log Alert does not exist for Delete Security Solutions

ID: CISAz526

Description:

Monitoring for Create or Update Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

Remediation:

Use the PowerShell Script to remediate the issue.

PowerShell Script:

```
New-AzActivityLogAlert
```

Returned Value:

Azure subscription 1

Default Value:

By default, no monitoring alerts are created.

Expected Value:

an Activity Log Alert Rule for Microsoft.Security/securitySolutions/delete

Impact:

2

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- Classic alerts in Azure Monitor to retire in June 2019
- Create or edit an activity log, service health, or resource health alert rule
- Create or edit a log search alert rule

Low [1]: CIS Az 2.1.12 - Microsoft Defender Recommendation for 'Apply system updates' status is not equal to 'Completed'

CIS Az 2.1.12 - Microsoft Defender Recommendation for 'Apply system updates' status is not equal to 'Completed'

ID: CISAz2112

Description:

Enabling Microsoft Defender allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Remediation:

Use the powershell command and replace SubScriptionName with the corresponding subscription which has a Free Pricing Tier at the moment.

PowerShell Script:

```
Register-AzResourceProvider -ProviderNamespace
"Microsoft.PolicyInsights";
```

Returned Value:

Policy not created!

Default Value:

By default, patches are not automatically deployed

Expected Value:

Patches are automatically deployed

Impact:

1

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- PV-6: Rapidly and automatically remediate vulnerabilities
- Microsoft Defender for Cloud pricing
- Enable vulnerability scanning with the integrated Qualys scanner

Low [1]: CIS Az 2.1.x - Multiple Defender Subscriptions Not Compliant

👍 CIS Az 2.1.x - Multiple Defender Subscriptions Not Compliant

ID: CISAz21x

Description:

Enabling Microsoft Defender allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Remediation:

Use the powershell command and replace SubScriptionName with the corresponding subscription which has a Free Pricing Tier at the moment.

PowerShell Script:

```
Set-AzSecurityPricing -Name "" -PricingTier "Standard"
```

Returned Value:

ContainerRegistry has a Free subscription

Default Value:

By default, Microsoft Defender plan is off (None) or set to Free

Expected Value:

Standard

Impact:

1

Likelihood:

1

Priority:

Low

RiskRating: Low

References:

- [PV-6: Rapidly and automatically remediate vulnerabilities]
- [Azure Pricing]
- [IM-2: Protect identity and authentication systems]

Low [1]: CIS Az 2.1.17 - Setting: All users with the following roles is not set to Owner

👍 CIS Az 2.1.17 - Setting: All users with the following roles is not set to Owner

ID: CISAz2117

Description:

Enabling security alert emails to subscription owners ensures that they receive security alert emails from Microsoft. This ensures that they are aware of any potential security issues and can mitigate the risk in a timely fashion.

Remediation:

You can change the settings in the URL written in PowerShellScript.

PowerShell Script:

```
https://portal.azure.com/#view/Microsoft_Azure_SubscriptionManagement/ManageSubscriptionPoliciesBlade
```

Returned Value:

Owner AccountAdmin ServiceAdmin

Default Value:

Owner

Expected Value:

Owner

Impact:

1

Likelihood:

1

Priority:

Medium

RiskRating: Low

References:

[Quickstart: Configure email notifications for security alerts]

Medium [9]: CIS MAz 5.2.4.1 - Self Service Password Reset is not set to be enabled for all users

👎 CIS MAz 5.2.4.1 - Self Service Password Reset is not set to be enabled for all users

ID: CISMAz5241

Description:

Users will no longer need to engage the helpdesk for password resets, and the password reset mechanism will automatically block common, easily guessable passwords.

Remediation:

Manually change the value from 0 (None) or 1 (Selected) to 2 (All) in the Azure Portal. There is no script available at this moment unfortunately.

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/PasswordResetMenuBlade/~/Properties
```

Returned Value:

0

Default Value:

0

Expected Value:

2

Impact:

3

Likelihood:

3

Priority:

High

RiskRating: Medium

References:

- Let users reset their own passwords
- Tutorial: Enable users to unlock their account or reset passwords using Microsoft Entra self-service password reset
- Enable combined security information registration in Microsoft Entra ID

Medium [8]: CSTM-Az001 - The Security Defaults are not enabled on Azure Active Directory Tenant

CSTM-Az001 - The Security Defaults are not enabled on Azure Active Directory Tenant

ID: CSTM-Az001

Description:

Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks.

Remediation:

Use the PowerShell Script to enable Security Defaults on Microsoft Azure Active Directory

PowerShell Script:

```
$body = $body = (@{"isEnabled"="true"} | ConvertTo-Json) ;Invoke-MgGraphRequest -Method PATCH https://graph.microsoft.com/beta/policies/identitySecurityDefaultsEnforcementPolicy -Body $body
```

Returned Value:

False

Default Value:

True for tenants >2019, False for tenants <2019

Expected Value:

True

Impact:

4

Likelihood:

2

Priority:

Medium

RiskRating: Medium

References:

- [Security defaults in Azure AD]
- [Introducing security defaults]
- [IM-2: Protect identity and authentication systems]

Medium [6]: CISMAz 5.1.5.2 - User consent to apps accessing company data on their behalf is allowed!

👎 CISMAz 5.1.5.2 - User consent to apps accessing company data on their behalf is allowed!

ID: CISMAz5152

Description:

Attackers commonly use custom applications to trick users into granting them access to company data. Disabling future user consent operations setting mitigates this risk, and helps to reduce the threat-surface. If user consent is disabled previous consent grants will still be honored but all future consent operations must be performed by an administrator.

Remediation:

Use the PowerShell Script disable user consent for Non-Admin Users.

PowerShell Script:

```
$params = @{ defaultUserRolePermissions = @{
permissionGrantPoliciesAssigned = @() } }; Update-
MgPolicyAuthorizationPolicy -BodyParameter $params
```

Returned Value:

ManagePermissionGrantsForSelf.microsoft-user-default-legacy ManagePermissionGrantsForOwnedResource.microsoft-dynamically-managed-permissions-for-team ManagePermissionGrantsForOwnedResource.microsoft-dynamically-managed-permissions-for-chat

Default Value:

Null

Expected Value:

Null

Impact:

3

Likelihood:

2

Priority:

Medium

RiskRating: Medium

References:

↗ [Configure how users consent to applications]

Medium [5]: CIS MAz 5.1.2.6 - LinkedIn Account Connections is enabled!

CIS MAz 5.1.2.6 - LinkedIn Account Connections is enabled!

ID: CISMAz5126

Description:

Disabling LinkedIn integration prevents potential phishing attacks and risk scenarios where an external party could accidentally disclose sensitive information.

Remediation:

Change the value to 1 (No) to disable LinkedIn

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings/menuId/UserSettings
```

Returned Value:

enableLinkedInAppFamily: 0

Default Value:

0

Expected Value:

1

Impact:

1

Likelihood:

5

Priority:

Medium

RiskRating: Medium

References:

[Integrate LinkedIn account connections in Microsoft Entra ID]

[LinkedIn account connections data sharing and consent]

Medium [5]: CIS Az 1.6 - No Custom Bad Password List is set to 'Enforce' for your Organization

CIS Az 1.6 - No Custom Bad Password List is set to 'Enforce' for your Organization

ID: CISAz160

Description:

Enabling this gives your organization further customization on what secure passwords are allowed. Setting a bad password list enables your organization to fine-tune its password policy further, depending on your needs. Removing easy-to-guess passwords increases the security of access to your Azure resources

Remediation:

Manually enable Enforce custom list and set it to True. There is no script available at this moment unfortunately.

PowerShell Script:

```
https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtection
```

Returned Value:

CustomBannedPasswords: False PolicyMode: 0

Default Value:

False + No List

Expected Value:

True + List with passwords

Impact:

1

Likelihood:

5

Priority:

Medium

RiskRating: Medium

References:

- [Combined password policy and check for weak passwords in Microsoft Entra ID]
- [Eliminate bad passwords using Microsoft Entra Password Protection]
- [AzureAD PowerShell Module]
- [Password Guidance]
- [Tutorial: Configure custom banned passwords for Microsoft Entra password protection]
- [IM-6: Use strong authentication controls]

Medium [5]: CISM MAz 5.2.3.2 - No Custom Bad Password List is used within your organization

👎 CISM MAz 5.2.3.2 - No Custom Bad Password List is used within your organization

ID: CISMAz5232

Description:

Creating a new password can be difficult regardless of one's technical background. It is common to look around one's environment for suggestions when building a password, however, this may include picking words specific to the organization as inspiration for a password. An adversary may employ what is called a 'mangler' to create permutations of these specific words in an attempt to crack passwords or hashes making it easier to reach their goal.

Remediation:

Manually enable Enforce custom list and set it to True. There is no script available at this moment unfortunately.

PowerShell Script:

```
https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsM
enuBlade/~/PasswordProtection
```

Returned Value:

CustomBannedPasswords: False PolicyMode: 0

Default Value:

False + No List

Expected Value:

True + List with passwords

Impact:

1

Likelihood:

5

Priority:

Medium

RiskRating: Medium

References:

↗ [Tutorial: Configure custom banned passwords for Microsoft Entra password protection]()

↗ [Eliminate bad passwords using Microsoft Entra Password Protection]()

Medium [5]: CIS Az 1.17 - Restrict user ability to access groups features in the Access Pane is Set to 'No'

👎 CIS Az 1.17 - Restrict user ability to access groups features in the Access Pane is Set to 'No'

ID: CISAz1170

Description:

Self-service group management enables users to create and manage security groups or Office 365 groups in Microsoft Entra ID. Unless a business requires this day-to-day delegation for some users, self-service group management should be disabled.

Remediation:

Change the Value to False to restrict non-admin users from accessing sensitive data. There is no automatic script available at this moment unfortunately.

PowerShell Script:

```
https://portal.azure.com/#view/Microsoft_AAD_IAM/GroupsManagementMenuBlade/~/General
```

Returned Value:

Restrict user ability to access groups features in the Access Panel is Set to : True

Default Value:

True

Expected Value:

False

Impact:

1

Likelihood:

5

Priority:

Medium

RiskRating: Medium

References:

- [Set up self-service group management in Microsoft Entra ID]
- [PA-1: Separate and limit highly privileged/administrative users]
- [GS-2: Define and implement enterprise segmentation/separation of duties strategygment]
- [GS-6: Define and implement identity and privileged access strategy]

Medium [4]: CIS Az 1.1.4 - Allow users to remember multi-factor authentication on devices they trust is Enabled

CIS Az 1.1.4 - Allow users to remember multi-factor authentication on devices they trust is Enabled

ID: CISAz14

Description:

Remembering Multi-Factor Authentication (MFA) for devices and browsers allows users to have the option to bypass MFA for a set number of days after performing a successful sign-in using MFA. This can enhance usability by minimizing the number of times a user may need to perform two-step verification on the same device. However, if an account or device is compromised, remembering MFA for trusted devices may affect security. Hence, it is recommended that users not be allowed to bypass MFA.

Remediation:

Check via the link

PowerShell Script:

```
https://account.activedirectory.windowsazure.com/UserManagement/MfaSettings.aspx
```

Returned Value:

Check the value here: https://account.activedirectory.windowsazure.com/UserManagement/MfaSettings.aspx

Default Value:

Disabled

Expected Value:

Disabled

Impact:

4

Likelihood:

1

Priority:

Medium

RiskRating: Medium

References:

- [Configure Microsoft Entra multifactor authentication settings]
- [IM-6: Use strong authentication controls]

Medium [12]: CIS Az 1.10 - User consent for applications is not set to: 'Do not allow user consent'

👎 CIS Az 1.10 - User consent for applications is not set to: 'Do not allow user consent'

ID: CISAz110

Description:

If Microsoft Entra ID is running as an identity provider for third-party applications, permissions and consent should be limited to administrators or pre-approved. Malicious applications may attempt to exfiltrate data or abuse privileged user accounts

Remediation:

Goto: https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings or Use the PowerShell Command

PowerShell Script:

```
Import-Module Microsoft.Graph.Identity.SignIns; $params =
@{DefaultUserRolePermissions = @{PermissionGrantPoliciesAssigned =
@()}}; Update-MgPolicyAuthorizationPolicy -BodyParameter $params
```

Returned Value:

ManagePermissionGrantsForSelf.microsoft-user-default-legacy ManagePermissionGrantsForOwnedResource.microsoft-dynamically-managed-permissions-for-team ManagePermissionGrantsForOwnedResource.microsoft-dynamically-managed-permissions-for-chat

Default Value:

Allow user consent for apps

Expected Value:

Do not allow user consent or Allow user consent for apps from verified publishers, for selected permissions

Impact:

3

Likelihood:

4

Priority:

High

RiskRating: Medium

References:

- Admin Consent for Permissions in Azure Active Directory
- Configure how users consent to applications
- PA-1: Separate and limit highly privileged/administrative users

> ↗ GS-2: Define and implement enterprise segmentation/separation of duties strategy
> ↗ GS-6: Define and implement identity and privileged access strategy

High [8.2]: CIS MAz 5.2.2.5 - Phishing-resistant MFA strength must be required for Administrators

CIS MAz 5.2.2.5 - Phishing-resistant MFA strength must be required for Administrators

ID: CISMAz5225

Description:

Sophisticated attacks targeting MFA are more prevalent as the use of it becomes more widespread. These 3 methods are considered phishing-resistant as they remove passwords from the login workflow. It also ensures that public/private key exchange can only happen between the devices and a registered provider which prevents login to fake or phishing websites..

Remediation:

Configure the policy at the ConditionalAccess Blade below in the PowerShell Script. There is a Policy Template available which you can create if there is no such policy created beforehand.

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies
```

Returned Value:

No Policy Configured!

Default Value:

No Policy

Expected Value:

Impact:

2

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

- [Passwordless authentication options for Microsoft Entra ID]
- [Enable passwordless security key sign-in]
- [Conditional Access authentication strength]
- [How To: Configure the Microsoft Entra multifactor authentication registration policy]

High [8.2]: CIS MAz 5.2.2.3 - No Conditional Access policies to block legacy authentication

CIS MAz 5.2.2.3 - No Conditional Access policies to block legacy authentication

ID: CISMAz5223

Description:

Legacy authentication protocols do not support multi-factor authentication. These protocols are often used by attackers because of this deficiency. Blocking legacy authentication makes it harder for attackers to gain access.

Remediation:

Configure the policy at the ConditionalAccess Blade below in the PowerShell Script. There is a Policy Template available which you can create if there is no such policy created beforehand.

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies
```

Returned Value:

No Conditional Access Policy (Correctly) Configured to block Legacy Authentication

Default Value:

No Policy

Expected Value:

A Policy

Impact:

5

Likelihood:

2

Priority:

High

RiskRating: High

References:

- [Disable Basic authentication in Exchange Online]
- [How to set up a multifunction device or application to send emails using Microsoft 365 or Office 365]
- [Deprecation of Basic authentication in Exchange Online]

High [15]: CIS MAz 5.1.2.1 - Some User Accounts do not have MFA enabled

CIS MAz 5.1.2.1 - Some User Accounts do not have MFA enabled

ID: CISMAz5121

Description:

Both security defaults and conditional access with security defaults turned off are not compatible with per-user multi-factor authentication (MFA), which can lead to undesirable user authentication states. The CIS Microsoft 365 Benchmark explicitly employs Conditional Access for MFA as an enhancement over security defaults and as a replacement for the outdated per-user MFA. To ensure a consistent authentication state disable per-user MFA on all accounts.

Remediation:

Please enable MFA for all users through the Admin Portal. You can also use the legacy script by Adminroid

PowerShell Script:

```
https://admindroid.sharepoint.com/:u:/s/external/EVzUDxQqxWdLj91v3mhAipsBt0GqNmUK5b4jFXPr181Svw?e=OOcfQn&isSPOFile=1
```

Returned Value:

9

Default Value:

Disabled

Expected Value:

All Users have MFA Enabled

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

- [Enable per-user Microsoft Entra multifactor authentication to secure sign-in events]
- [Set up multifactor authentication for Microsoft 365]

High [15]: CIS Az 1.1.3 - Multi-Factor Auth Status is 'Disabled' for some non-privileged Users

CIS Az 1.1.3 - Multi-Factor Auth Status is 'Disabled' for some non-privileged Users

ID: CISAz13

Description:

Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk

Remediation:

Please enable MFA for all users through the Admin Portal. You can also use the legacy script by Adminroid

PowerShell Script:

```
https://admindroid.sharepoint.com/:u:/s/external/EVzUDxQqxWdLj91v3mhAip
sBt0GqNmUK5b4jFXPr181Svw?e=OOcfQn&isSPOFile=1
```

Returned Value:

9 Users have MFA Disabled

Default Value:

All Users have no MFA Enabled

Expected Value:

All Users have MFA Enabled

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

- How it works: Microsoft Entra multifactor authentication
- Enable per-user Microsoft Entra multifactor authentication to secure sign-in events
- IM-6: Use strong authentication controls

High [15]: CIS Az 1.18 - Users can create security groups in Azure portals, API or PowerShell

👎 CIS Az 1.18 - Users can create security groups in Azure portals, API or PowerShell

ID: CISAz1180

Description:

When creating security groups is enabled, all users in the directory are allowed to create new security groups and add members to those groups. Unless a business requires this day-to-day delegation, security group creation should be restricted to administrators only.

Remediation:

Use the Powershell Script to modify the policy to disallow Tenant Creation by unauthorized users

PowerShell Script:

```
$RolePermissions = @{};
$RolePermissions["AllowedToCreateSecurityGroups"] = $False; Update-
MgPolicyAuthorizationPolicy -AuthorizationPolicyId
"authorizationPolicy" -DefaultUserRolePermissions $RolePermissions
```

Returned Value:

AllowedToCreateSecurityGroups: True

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

- ↗ Set up self-service group management in Microsoft Entra ID
- ↗ PA-1: Separate and limit highly privileged/administrative users
- ↗ GS-2: Define and implement enterprise segmentation/separation of duties strategygment
- ↗ GS-6: Define and implement identity and privileged access strategy

High [15]: CIS Az 1.14 - Guest users access restrictions is not set to 'Guest user access is restricted to properties and memberships of their own directory objects'

CIS Az 1.14 - Guest users access restrictions is not set to 'Guest user access is restricted to properties and memberships of their own directory objects'

ID: CISAz1140

Description:

Limiting guest access ensures that guest accounts do not have permission for certain directory tasks, such as enumerating users, groups or other directory resources, and cannot be assigned to administrative roles in your directory. Guest access has three levels of restriction. 1. Guest users have the same access as members (most inclusive) 2. Guest users have limited access to properties and memberships of directory objects 3. Guest user access is restricted to properties and memberships of their own directory objects The recommended option is the 3rd, most restrictive: 'Guest user access is restricted to their own directory object'

Remediation:

Use the PowerShell Script to mitigate this issue:

PowerShell Script:

```
Update-MgPolicyAuthorizationPolicy -GuestUserRoleId "2af84b1e-32c8-42b7-82bc-daa82404023b"
```

Returned Value:

10dae51f-b6af-4016-8d66-8c2a99b929b3

Default Value:

10dae51f-b6af-4016-8d66-8c2a99b929b3

Expected Value:

2af84b1e-32c8-42b7-82bc-daa82404023b

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

- Member and guest users
- PA-3: Manage lifecycle of identities and entitlements
- GS-2: Define and implement enterprise segmentation/separation of duties strategy
- GS-6: Define and implement identity and privileged access strategy

↗ Restrict guest access permissions in Microsoft Entra ID

High [15]: CIS Az 1.13 - Users Can Register Applications Is Set to 'Yes'

👎 CIS Az 1.13 - Users Can Register Applications Is Set to 'Yes'

ID: CISAz1130

Description:

It is recommended to only allow an administrator to register custom-developed applications. This ensures that the application undergoes a formal security review and approval process prior to exposing Microsoft Entra ID data. Certain users like developers or other high-request users may also be delegated permissions to prevent them from waiting on an administrative user. Your organization should review your policies and decide your needs.

Remediation:

Use the PowerShell Script to enable Security Defaults on Microsoft Entra ID

PowerShell Script:

```
Import-Module Microsoft.Graph.Identity.SignIns; $params =
@{AllowedToCreateApps = $false}; Update-MgPolicyAuthorizationPolicy -
BodyParameter $params
```

Returned Value:

True

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

- [Restrict who can create applications]
- [Who has permission to add applications to my Azure AD instance?]
- [GS-1: Align organization roles, responsibilities and accountabilities]
- [PA-1: Separate and limit highly privileged/administrative users]
- [Managing user consent for applications using Office 365 APIs]
- [Admin Consent for Permissions in Azure Active Directory]

High [15]: CIS Az 1.9 - Notify all admins when other admins reset their password?' is set to 'No'

👎 CIS Az 1.9 - Notify all admins when other admins reset their password?' is set to 'No'

ID: CISAz190

Description:

Global Administrator accounts are sensitive. Any password reset activity notification, when sent to all Global Administrators, ensures that all Global administrators can passively confirm if such a reset is a common pattern within their group. For example, if all Global Administrators change their password every 30 days, any password reset activity before that may require administrator(s) to evaluate any unusual activity and confirm its origin.

Remediation:

Change the value manually. There is no automatic script available at this moment unfortunately.

PowerShell Script:

```
https://portal.azure.com/#view/Microsoft_AAD_IAM/PasswordResetMenuBlade
/~/Notifications
```

Returned Value:

Notify all admins when other admins reset their password? is set to: False

Default Value:

False

Expected Value:

True

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

- Notifications
- Plan a Microsoft Entra self-service password reset deployment
- GS-6: Define and implement identity and privileged access strategy
- PA-1: Separate and limit highly privileged/administrative users
- Set up notifications and customizations

High [15]: CIS MAz 5.2.3.1 - Microsoft Authenticator is not configured to protect against MFA fatigue

CIS MAz 5.2.3.1 - Microsoft Authenticator is not configured to protect against MFA fatigue

ID: CISMAz5231

Description:

As the use of strong authentication has become more widespread, attackers have started to exploit the tendency of users to experience 'MFA fatigue.' This occurs when users are repeatedly asked to provide additional forms of identification, leading them to eventually approve requests without fully verifying the source. To counteract this, number matching can be employed to ensure the security of the authentication process. With this method, users are prompted to confirm a number displayed on their original device and enter it into the device being used for MFA. Additionally, other information such as geolocation and application details are displayed to enhance the end user's awareness. Among these 3 options, number matching provides the strongest net security gain.

Remediation:

Navigate to Microsoft Entra and select Microsoft Authenticator. Review the settings and set it to all_users and enable the first 3 options in the Configure section.

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AdminAuthMethods
```

Returned Value:

displayAppInformationRequiredState: default targetid: all_users
displayLocationInformationRequiredState: default targetid: all_users

Default Value:

Enabled for tenants >2022, Disabled for tenants <2022

Expected Value:

From 2023 if not manually assigned it would be enabled if Microsoft manages the setting.

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

[Protecting authentication methods in Microsoft Entra ID]
[Defend your users from MFA fatigue attacks]

> How number matching works in multifactor authentication push notifications for Authenticator - Authentication methods policy

High [12]: CSTM-Az011 - Account Lockout Protection not optimally configured

CSTM-Az011 - Account Lockout Protection not optimally configured

ID: CSTM-Az011

Description:

MFA fraud alerts are used to alert the admins when the multi-factor authentication request is initiated without the users' concern. In MFA fraud alerting, the users notify the admins by reporting fraudulent activity that occurred in their accounts.

Remediation:

Manually enable the checkboxes to enable Account Lockout Protection and FraudAlerts for your organization

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/MultifactorAuthenticationMenuBlade/~/AccountLockout/fromProviders~/false
```

Returned Value:

accountLockoutDurationMinutes: blockForFraud: enableFraudAlert: fraudCode: There are no fraudNotificationEmailAddresses smsTimeoutSeconds:

Default Value:

accountLockoutDurationMinutes:5/accountLockoutResetMinutes:1/accountLockoutThreshold:5/blockForFraud:False/enableFraudAlert:False/fraudCode:null/defaultBypassTimespan:300/pinAttempts:null/smstimeoutseconds:null

Expected Value:

accountLockoutDurationMinutes:5/accountLockoutResetMinutes:1/accountLockoutThreshold:5/blockForFraud:False/enableFraudAlert:True/fraudCode:0/defaultBypassTimespan:300/pinAttempts:3/smstimeoutseconds:300

Impact:

3

Likelihood:

4

Priority:

High

RiskRating: High

References:

[Configure MFA Fraud Alerts in Azure AD : An Alarm for Security Emergency]

High [12]: CIS Az 1.11 - User consent for applications is not set to: 'Do not allow user consent' or 'Allow for Verified Publishers'

CIS Az 1.11 - User consent for applications is not set to: 'Do not allow user consent' or 'Allow for Verified Publishers'

ID: CISAz1110

Description:

If Microsoft Entra ID is running as an identity provider for third-party applications, permissions and consent should be limited to administrators or pre-approved. Malicious applications may attempt to exfiltrate data or abuse privileged user accounts.

Remediation:

Goto: https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings or Use the PowerShell Command

PowerShell Script:

```
Import-Module Microsoft.Graph.Identity.SignIns; $params = @{DefaultUserRolePermissions = @{PermissionGrantPoliciesAssigned = @()}}; Update-MgPolicyAuthorizationPolicy -BodyParameter $params
```

Returned Value:

ManagePermissionGrantsForSelf.microsoft-user-default-legacy ManagePermissionGrantsForOwnedResource.microsoft-dynamically-managed-permissions-for-team ManagePermissionGrantsForOwnedResource.microsoft-dynamically-managed-permissions-for-chat

Default Value:

Allow user consent for apps

Expected Value:

Do not allow user consent or Allow user consent for apps from verified publishers, for selected permissions

Impact:

3

Likelihood:

4

Priority:

High

RiskRating: High

References:

- Configure how users consent to applications
- PA-1: Separate and limit highly privileged/administrative users
- GS-2: Define and implement enterprise segmentation/separation of duties strategy

> ↗ GS-6: Define and implement identity and privileged access strategy

High [10]: CIS MAz 5.1.2.3 - Non-Admin Users can create new tenants!

👎 CIS MAz 5.1.2.3 - Non-Admin Users can create new tenants!

ID: CISMAz5123

Description:

Restricting tenant creation prevents unauthorized or uncontrolled deployment of resources and ensures that the organization retains control over its infrastructure. User generation of shadow IT could lead to multiple, disjointed environments that can make it difficult for IT to manage and secure the organization's data, especially if other users in the organization began using these tenants for business purposes under the misunderstanding that they were secured by the organization's security team.

Remediation:

Change the value to False (Yes) to restrict non-admins from creating tenants! Or use the PowerShell script to restrict non-admins.

PowerShell Script:

```
$params = @{ DefaultUserRolePermissions = @{ AllowedToCreateTenants = $false } }; Update-MgBetaPolicyAuthorizationPolicy -AuthorizationPolicyId "authorizationPolicy" -BodyParameter $params
```

Returned Value:

allowedToCreateTenants: True

Default Value:

AllowedToCreateTenants: True

Expected Value:

AllowedToCreateTenants: False

Impact:

2

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

[Restrict member users default permissions]

High [10]: CIS MAz 5.1.2.4 - Access to the Azure AD administration portal is not restricted!

👎 CIS MAz 5.1.2.4 - Access to the Azure AD administration portal is not restricted!

ID: CISMAz5124

Description:

The Azure AD administrative (AAD) portal contains sensitive data and permission settings, which are still enforced based on the user's role. However, an end user may inadvertently change properties or account settings that could result in increased administrative overhead. Additionally, a compromised end user account could be used by a malicious attacker as a means to gather additional information and escalate an attack.

Remediation:

Change the value to True (Yes) to restrict access to the AD portal

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings/menuId/UserSettings
```

Returned Value:

restrictNonAdminUsers: False

Default Value:

restrictNonAdminUsers: False

Expected Value:

restrictNonAdminUsers: True

Impact:

2

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ Restrict member users default permissions

High [10]: CIS MAz 5.2.2.4 - Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users

CIS MAz 5.2.2.4 - Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users

ID: CISMAz5224

Description:

Forcing a time out for MFA will help ensure that sessions are not kept alive for an indefinite period of time, ensuring that browser sessions are not persistent will help in prevention of drive-by attacks in web browsers, this also prevents creation and saving of session cookies leaving nothing for an attacker to take.

Remediation:

You can navigate to the Entry Portal and the Conditional Access blade to configure the policy.

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies
```

Returned Value:

No Policy Configured!

Default Value:

No Policy

Expected Value:

presistentBrowserMode: never and isEnabled: true | signInFrequencyValue: between 4 and 24 and timevalue: hours | clientAppTypes: All | applicationsIncludeApplications: All | grantControls.builtInControls: mfa

Impact:

2

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

[Configure adaptive session lifetime policies]

High [10]: CIS MAz 5.2.2.8 - Ensure Microsoft Azure Management is limited to administrative roles

👎 CIS MAz 5.2.2.8 - Ensure Microsoft Azure Management is limited to administrative roles

ID: CISMAz5228

Description:

Blocking sign-in to Azure Management applications and portals enhances security of sensitive data by restricting access to privileged users. This mitigates potential exposure due to administrative errors or software vulnerabilities, as well as acting as a defense in depth measure against security breaches.

Remediation:

Unfortunately we cannot accurately detect if correctly configured. If you have a existing policy. Please verify if the settings are configured correctly.

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies
```

Returned Value:

Could not verify is policy exists!

Default Value:

No Policy and Non-administrators can access the Azure AD administration portal

Expected Value:

A Correctly Configured Policy Non-administrators cannot access the Azure AD administration portal

Impact:

2

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ [Conditional Access: Cloud apps, actions, and authentication context]

High [10]: CIS MAz 5.2.2.7 - Verify if you have an Azure AD Identity Protection sign-in risk policy enabled

👎 CIS MAz 5.2.2.7 - Verify if you have an Azure AD Identity Protection sign-in risk policy enabled

ID: CISMAz5227

Description:

Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication.

Remediation:

Unfortunately we cannot accurately detect if a sign-in risk policy is enabled. If you have a sign-in risk policy. Please verify if the settings are configured correctly.

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies
```

Returned Value:

No Conditional Access Policy Configured!

Default Value:

No Policy

Expected Value:

A Correctly Configured Policy

Impact:

2

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ How To: Give risk feedback in Azure AD Identity Protection

↗ What are risk detections?

High [10]: CIS MAz 5.2.2.6 - Verify if you have an Azure AD Identity Proteciton user risk policy enabled

CIS MAz 5.2.2.6 - Verify if you have an Azure AD Identity Proteciton user risk policy enabled

ID: CISMAz5226

Description:

With the user risk policy turned on, Azure AD detects the probability that a user account has been compromised. Administrators can configure a user risk conditional access policy to automatically respond to a specific user risk level.

Remediation:

Unfortunately we cannot accurately detect if a user risk risk policy is enabled. If you have a user risk policy. Please verify if the settings are configured correctly.

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies
```

Returned Value:

No Conditional Access Policy Configured!

Default Value:

No Policy

Expected Value:

A Correctly Configured Policy

Impact:

2

Likelihood:

5

Priority:

High

RiskRating: High

References:

- [How To: Give risk feedback in Azure AD Identity Protection]
- [What are risk detections?]

High [10]: CIS Az 1.15 - Guest invite restrictions is not set to 'Only users assigned to specific admin roles can invite guest users'

CIS Az 1.15 - Guest invite restrictions is not set to 'Only users assigned to specific admin roles can invite guest users'

ID: CISAz1150

Description:

Restricting invitations to users with specific administrator roles ensures that only authorized accounts have access to cloud resources. This helps to maintain 'Need to Know' permissions and prevents inadvertent access to data. By default the setting Guest invite restrictions is set to Anyone in the organization can invite guest users including guests and non-admins. This would allow anyone within the organization to invite guests and non-admins to the tenant, posing a security risk.

Remediation:

Use the PowerShell Script to mitigate this issue:

PowerShell Script:

```
Update-MgPolicyAuthorizationPolicy -AllowInvitesFrom
"adminsAndGuestInviters"
```

Returned Value:

everyone

Default Value:

everyone

Expected Value:

adminsAndGuestInviters

Impact:

2

Likelihood:

5

Priority:

Informational

RiskRating: High

References:

- [Configure external collaboration settings]()
- [PA-3: Manage lifecycle of identities and entitlements]()
- [GS-2: Define and implement enterprise segmentation/separation of duties strategy]()
- [GS-6: Define and implement identity and privileged access strategy]()

High [10]: CIS Az 1.16 - 'Restrict access to Azure AD administration portal is set to 'No'

CIS Az 1.16 - 'Restrict access to Azure AD administration portal is set to 'No'

ID: CISAz1160

Description:

The Microsoft Entra ID administrative portal has sensitive data and permission settings. All non-administrators should be prohibited from accessing any Entra ID data in the administration portal to avoid exposure

Remediation:

Change the Value to True to restrict non-admin users from accessing sensitive data. There is no automatic script available at this moment unfortunately.

PowerShell Script:

```
https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings
```

Returned Value:

Restrict access to Azure AD administration portal is set to:

Default Value:

False

Expected Value:

True

Impact:

2

Likelihood:

5

Priority:

High

RiskRating: High

References:

- [The Azure AD portal strikes back]
- [Microsoft Entra built-in roles]
- [GS-2: Define and implement enterprise segmentation/separation of duties strategygment]
- [GS-6: Define and implement identity and privileged access strategy]
- [PA-1: Separate and limit highly privileged/administrative users]

High [10]: CIS MAz 5.1.2.2 - Third party integrated applications are allowed!

CIS MAz 5.1.2.2 - Third party integrated applications are allowed!

ID: CISMAz5122

Description:

Third party integrated applications connection to services should be disabled, unless there is a very clear value and robust security controls are in place. While there are legitimate uses, attackers can grant access from breached accounts to third party applications to exfiltrate data from your tenancy without having to maintain the breached account.

Remediation:

Manually change it here: https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/AdminConsentSettings

PowerShell Script:

```
https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings/menuId/UserSettings
```

Returned Value:

AllowedToCreateApps: True

Default Value:

AllowedToCreateApps: True

Expected Value:

AllowedToCreateApps: False

Impact:

2

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

[How and why applications are added to Microsoft Entra ID]

High [10]: CIS Az 1.3 - Restrict non-admin users from creating tenants is set to No

👎 CIS Az 1.3 - Restrict non-admin users from creating tenants is set to No

ID: CISAz130

Description:

It is recommended to only allow an administrator to create new tenants. This prevent users from creating new Azure AD or Azure AD B2C tenants and ensures that only authorized users are able to do so.

Remediation:

Use the Powershell Script to modify the policy to disallow Tenant Creation by unauthorized users

PowerShell Script:

```
$RolePermissions = @{}; $RolePermissions["allowedToCreateTenants"] =
$False; Update-MgPolicyAuthorizationPolicy -AuthorizationPolicyId
"authorizationPolicy" -DefaultUserRolePermissions $RolePermissions
```

Returned Value:

True

Default Value:

True

Expected Value:

False

Impact:

2

Likelihood:

5

Priority:

Medium

RiskRating: High

References:

- What are the default user permissions in Microsoft Entra ID?
- Tenant Creator
- Disable Microsoft 365 User Tenant Creation in Azure AD

Critical [20]: CIS Az 1.1.2 - Multi-Factor Auth Status is 'Disabled' for some privileged Users

CIS Az 1.1.2 - Multi-Factor Auth Status is 'Disabled' for some privileged Users

ID: CISAz12

Description:

Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Remediation:

Please enable MFA for all Admin users through the Admin Portal. You can also use the legacy script by Adminroid

PowerShell Script:

```
https://admindroid.sharepoint.com/:u:/s/external/EVzUDxQqxWdLj91v3mhAip
sBt0GqNmUK5b4jFXPr181Svw?e=OOcfQn&isSPOFile=1
```

Returned Value:

1 Admins have MFA Disabled

Default Value:

All Admins have no MFA Enabled

Expected Value:

All Admins have MFA Enabled

Impact:

4

Likelihood:

5

Priority:

Critical

RiskRating: Critical

References:

- How it works: Microsoft Entra multifactor authentication
- Azure Active Directory Premium MFA Attributes via Graph API?
- IM-6: Use strong authentication controls

Microsoft Sharepoint

Informational [0]: CIS MSp 7.2.8 - Ensure external sharing is restricted by security group!

CIS MSp 7.2.8 - Ensure external sharing is restricted by security group!

ID: CISMSp728

Description:

Organizations wishing to create tighter security controls for external sharing can set this to enforce role-based access control by using security groups already defined in Microsoft Entra.

Remediation:

Use the link to access the sharepoint settings and change the setting there

PowerShell Script:

```
https://contoso-
admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/sharing
```

Returned Value:

Cannot Verify!

Default Value:

Unchecked

Expected Value:

Checked

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

Allow only members in specific security groups to share SharePoint and OneDrive files and folders externally

High [15]: CIS MSp 7.2.1 - Modern Authentication for Microsoft Sharepoint is disabled!

CIS MSp 7.2.1 - Modern Authentication for Microsoft Sharepoint is disabled!

ID: CISMSp721

Description:

Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by SharePoint applications. Requiring modern authentication for SharePoint applications ensures strong authentication mechanisms are used when establishing sessions between these applications, SharePoint, and connecting users.

Remediation:

Use the PowerShell Script to enable Modern Authentication for Microsoft Exchange Online.

PowerShell Script:

```
Set-SPOTenant -LegacyAuthProtocolsEnabled $false -
LegacyBrowserAuthProtocolsEnabled $false
```

Returned Value:

LegacyAuthProtocolsEnabled: True
LegacyBrowserAuthProtocolsEnabled: True

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

[Reference - Set-SPOTenant]

High [15]: CIS MSp 7.2.10 - Reauthentication with verification code is not restricted!

👎 CIS MSp 7.2.10 - Reauthentication with verification code is not restricted!

ID: CISMSp7210

Description:

By increasing the frequency of times guests need to reauthenticate this ensures guest user access to data is not prolonged beyond an acceptable amount of time.

Remediation:

Use the PowerShell Script to enable this setting:

PowerShell Script:

```
Set-SPOTenant -EmailAttestationRequired $true -
EmailAttestationReAuthDays 15
```

Returned Value:

EmailAttestationRequired: False

Default Value:

False and 30

Expected Value:

True and 15

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

- ↗ Secure external sharing recipient experience
- ↗ Manage sharing settings for SharePoint and OneDrive in Microsoft 365
- ↗ Email one-time passcode authentication

High [15]: CIS MSp 7.2.2 - SharePoint and OneDrive integration with Azure AD B2B is not enabled!

👎 CIS MSp 7.2.2 - SharePoint and OneDrive integration with Azure AD B2B is not enabled!

ID: CISMSp722

Description:

External users assigned guest accounts will be subject to Azure AD access policies, such as multi-factor authentication. This provides a way to manage guest identities and control access to SharePoint and OneDrive resources. Without this integration, files can be shared without account registration, making it more challenging to audit and manage who has access to the organization's data.

Remediation:

Use the PowerShell Script to enable Modern Authentication for Microsoft Exchange Online.

PowerShell Script:

```
Set-SPOTenant -EnableAzureADB2BIntegration $true
```

Returned Value:

EnableAzureADB2BIntegration: False

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

- SharePoint and OneDrive integration with Microsoft Entra B2B
- B2B collaboration overview

High [15]: CIS MSp 7.2.9 - Guest access to a site or OneDrive does not expire automatically

👎 CIS MSp 7.2.9 - Guest access to a site or OneDrive does not expire automatically

ID: CISMSp729

Description:

This setting ensures that guests who no longer need access to the site or link no longer have access after a set period of time. Allowing guest access for an indefinite amount of time could lead to loss of data confidentiality and oversight.

Remediation:

Use the PowerShell Script to enable this setting:

PowerShell Script:

```
Set-SPOTenant -ExternalUserExpireInDays 30 -
ExternalUserExpirationRequired $True
```

Returned Value:

ExternalUserExpirationRequired: False

Default Value:

60 and false

Expected Value:

30 and true

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ [Manage sharing settings for SharePoint and OneDrive in Microsoft 365]()

↗ [Managing SharePoint Online Security: A Team Effort]()

Microsoft Office 365

Informational [0]: CIS MOff 1.2.1 - Public Microsoft 365 Groups Found!

CIS MOff 1.2.1 - Public Microsoft 365 Groups Found!

ID: CISMOff121

Description:

Ensure that only organizationally managed and approved public groups exist. When a group has a 'public' privacy, users may access data related to this group.

Remediation:

Remove or make specific groups private

PowerShell Script:

```
-
```

Returned Value:

4

Default Value:

0 Public Groups

Expected Value:

0 Public Groups

Impact:

0

Likelihood:

0

Priority:

Informational

RiskRating: Informational

References:

- Groups Self-Service Management
- Compare Groups

Low [3]: CIS MOff 1.3.8 - Sways can be shared with people outside of your organization

👍 CIS MOff 1.3.8 - Sways can be shared with people outside of your organization

ID: CISMOff138

Description:

Disable external sharing of Sway documents that can contain sensitive information to prevent accidental or arbitrary data leak.

Remediation:

Manually uncheck at Sway Setting in the Admin Portal. The respective setting: 'Let people in your organization share their sways with people outside your organization'

PowerShell Script:

```
https://admin.microsoft.com/Adminportal/Home#/Settings/Services/:/Settings/L1/Sway
```

Returned Value:

ExternalSharingEnabled: True

Default Value:

True

Expected Value:

False

Impact:

3

Likelihood:

1

Priority:

Informational

RiskRating: Low

References:

- [Administrator settings for Microsoft Forms]
- [Review and unblock forms or users detected and blocked for potential phishing]

Medium [8]: CIS MOff 1.3.2 - 'Idle Session Timeout' for unmanaged devices is not set to 3 hours or less!

👎 CIS MOff 1.3.2 - 'Idle Session Timeout' for unmanaged devices is not set to 3 hours or less!

ID: CISMOff132

Description:

Ending idle sessions through an automatic process can help protect sensitive company data, and will add another layer of security for end users who work on unmanaged devices that can potentially be accessed by the public. Unauthorized individuals onsite or remotely can take advantage of systems left unattended over time. Automatic timing out of sessions makes this more difficult.

Remediation:

Manually change the value to 3 hour or less and enable the checkbox if not done in the portal.

PowerShell Script:

```
https://admin.microsoft.com/Adminportal/Home#/Settings/SecurityPrivacy
```

Returned Value:

TimeoutString: Never TimeoutValue: 0

Default Value:

TimeoutString: Never TimeoutValue: 0

Expected Value:

TimeoutString: NOT Never TimeoutValue: <180

Impact:

2

Likelihood:

4

Priority:

Medium

RiskRating: Medium

References:

[Idle session timeout for Microsoft 365](#)

High [15]: CIS MOff 1.3.4 - User owned apps and services are not restricted

👎 CIS MOff 1.3.4 - User owned apps and services are not restricted

ID: CISMOff134

Description:

Attackers commonly use vulnerable and custom-built add-ins to access data in user applications. While allowing users to install add-ins by themselves does allow them to easily acquire useful add-ins that integrate with Microsoft applications, it can represent a risk if not used and monitored carefully. Disable future user's ability to install add-ins in Microsoft Word, Excel, or PowerPoint helps reduce your threat-surface and mitigate this risk.

Remediation:

Manually uncheck at User owned apps and services the first two options so all 3 checkboxes are unchecked.

PowerShell Script:

```
https://admin.microsoft.com/Adminportal/Home#/Settings/Services/:/Settings/L1/Store
```

Returned Value:

iwpurchaseallowed: True iwpurchasefeatureenabled: True

Default Value:

iwpurchaseallowed: True / iwpurchasefeatureenabled: True

Expected Value:

iwpurchaseallowed: False / iwpurchasefeatureenabled: False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ [Microsoft Admin Portal]

High [15]: CIS MOff 1.3.7 - 'third-party storage services' are not restricted in 'Microsoft 365 on the web'

👎 CIS MOff 1.3.7 - 'third-party storage services' are not restricted in 'Microsoft 365 on the web'

ID: CISMOff137

Description:

By using external storage services an organization may increases the risk of data breaches and unauthorized access to confidential information. Additionally, third-party services may not adhere to the same security standards as the organization, making it difficult to maintain data privacy and security.

Remediation:

Manually uncheck the box 'Let users open files stored in third-party storage services in Microsoft 365 on the web'. The URL is given in PowerShellScript.

PowerShell Script:

```
https://admin.microsoft.com/Adminportal/Home#/Settings/Services/:/Settings/L1/OfficeOnline
```

Returned Value:

Enabled: True

Default Value:

Enabled: True

Expected Value:

Enabled: False

Impact:

3

Likelihood:

5

Priority:

High

RiskRating: High

References:

↗ [Enable or disable third-party storage services]

High [12]: CIS MOff 1.1.2 - Less than 2 emergency access accounts have been defined

CIS MOff 1.1.2 - Less than 2 emergency access accounts have been defined

ID: CISMOff112

Description:

In various situations, an organization may require the use of a break glass account to gain emergency access. In the event of losing access to administrative functions, an organization may experience a significant loss in its ability to provide support, lose insight into its security posture, and potentially suffer financial losses.

Remediation:

Create an extra Global Admin Account if you only have one.

PowerShell Script:

```
https://admin.microsoft.com/
```

Returned Value:

3

Default Value:

1

Expected Value:

2

Impact:

4

Likelihood:

3

Priority:

High

RiskRating: High

References:

- [Manage emergency access accounts in Microsoft Entra ID]
- [Securing privileged access for hybrid and cloud deployments in Microsoft Entra ID]

Microsoft Azure Security Assessment Findings

Prepared by

WhiteRook Cyber

Azure Security Inspection Report

This White Rook Cyber report assesses your compliance posture, highlights risks and recommends remediation steps to ensure compliance with essential data protection and regulatory standards.

Prepared for organization:
Test Company

Subscription Information:
Subscription Name: **Azure subscription 1** Subscription ID: **c292b24b-4160-4fc3-a417-c42d1f729f58**.

Stats:
12 out of **33** executed security checks identified possible opportunities for improvement in subscription **Azure subscription 1**.

Findings Summary

ID	Finding Name	Risk
1	Azure Management Not Restricted by Conditional Access Policies	Critical
2	Logging Not Enabled on Key Vaults	Critical
3	Storage Account Access Keys Not Rotated	Critical
4	Purge Protection Not Enabled on Azure Key Vaults	Medium
5	Storage Accounts Allow Public Access	Medium
6	Virtual Machines with Extensions	Medium
7	Storage Accounts Minimum TLS Version Less Than TLSv1.2	Low
8	Non-Default Network Security Group Firewall Rules Found	Informational
9	RBAC Roles Assigned at Subscription Scope	Informational
10	Soft Delete Retention Less than 90 Days	Informational
11	Virtual Machine Disks not Encrypted	Informational
12	Virtual Machine Disks not Encrypted with Customer Managed Keys	Informational

Critical [1]: Azure Management Not Restricted by Conditional Access Policies

👎 Azure Management Not Restricted by Conditional Access Policies

Affected Azure Objects:
● Tenant is not licensed for Conditional Access.

Finding:
No Conditional Access policies were found that restrict access to Azure Management. This leaves the Tenant extremely vulnerable to various attacks.

Potential Severity: Critical

Assessed Severity:

Remediation:
Consider creating Conditional Access policies or re-enabling Secure Defaults. If the Tenant is not licensed for Conditional Access, consider enabling Secure Defaults.

References:
↗ What is Conditional Access in Azure Active Directory?
↗ Common Conditional Access Policies
↗ Adopt a Zero Trust approach
↗ Common Conditional Access policy: Require MFA for Azure management

Critical [2]: Logging Not Enabled on Key Vaults

👎 Logging Not Enabled on Key Vaults

Affected Azure Objects:
● Cluster Name: TestCompany-keyvault1, Location: australiaeast
● Cluster Name: yolotoonnx0425418561, Location: eastus2

Finding:
Logging is not enabled on the identified Key Vaults. Logging should be enabled on all Key Vaults to track access and changes to keys, secrets, and certificates.

Potential Severity: Critical

Assessed Severity:

Remediation:
Select Key Vault from the Azure Portal⟶click on "Diagnostic settings" under Monitoring⟶select "Add diagnostic setting"⟶select the log types and destination details of your choice and select "Save".

References:
↗ Best practices for using Azure Key Vault
↗ Azure Key Vault logging
↗ Enable Key Vault logging

Critical [3]: Storage Account Access Keys Not Rotated

👎 Storage Account Access Keys Not Rotated

Affected Azure Objects:

- C:\out\Azure_report\TestCompany\Subscription_1\log
- C:\out\Azure_report\TestCompany\Subscription_1\log\ErrorLog.log

Finding:

When you create a storage account, Azure generates two 512-bit storage account access keys for that account. These keys can be used to authorize access to data in your storage account via Shared Key authorization. Your storage account access keys are similar to a root password for your storage account. Always be careful to protect your access keys. Use Azure Key Vault to manage and rotate your keys securely. Avoid distributing access keys to other users, hard-coding them, or saving them anywhere in plain text that is accessible to others.

Potential Severity: Critical

Assessed Severity:

Remediation:

Microsoft recommends that you use Azure Key Vault to manage your access keys, and that you regularly rotate and regenerate your keys. Using Azure Key Vault makes it easy to rotate your keys without interruption to your applications. You can also manually rotate your keys using any of the methods linked below. All keys can be immediately rotated using the following PowerShell command: $storageAccounts = Get-AzStorageAccount; foreach ($sa in $storageAccounts){$keys = Get-AzStorageAccountKey -Name $sa.StorageAccountName -ResourceGroupName $sa.ResourceGroupName; foreach ($key in $keys){New-AzStorageAccountKey -ResourceGroupName $sa.ResourceGroupName -Name $sa.StorageAccountName -KeyName $key.KeyName}}

References:

↗ Manage storage account access keys
↗ Manage storage account keys with Key Vault and Azure PowerShell
↗ Manage storage account keys with Key Vault and the Azure CLI

Medium [4]: Purge Protection Not Enabled on Azure Key Vaults

👎 Purge Protection Not Enabled on Azure Key Vaults

Affected Azure Objects:
- Cluster Name: TestCompany-keyvault1, Location: australiaeast
- Cluster Name: yolotoonnx0425418561, Location: eastus2

Finding:
Purge Protection for key vaults is not enabled. Purge protection is an optional Key Vault behavior and is not enabled by default. Purge protection can only be enabled once soft delete is enabled. It can be turned on via CLI or PowerShell. Purge protection is recommended when using keys for encryption to prevent data loss. Most Azure services that integrate with Azure Key Vault, such as Storage, require purge protection to prevent data loss. When purge protection is on, a vault or an object in the deleted state cannot be purged until the retention period has passed. Soft-deleted vaults and objects can still be recovered, ensuring that the retention policy will be followed. The default retention period is 90 days, but it is possible to set the retention policy interval to a value from 7 to 90 days through the Azure portal. Once the retention policy interval is set and saved it cannot be changed for that vault.

Potential Severity: Medium

Assessed Severity:

Remediation:
Select Key Vault from the Azure Portal→click on "Properties" tab→select the radio button corresponding to "Enable soft delete"→enter a retention period in days. The recommended configuration for Soft Delete Retention is 90 days.

References:
↗ Purge protection
↗ Azure Key Vault soft-delete overview

Medium [5]: Storage Accounts Allow Public Access

👎 Storage Accounts Allow Public Access

Affected Azure Objects:

- Storage Account: TestCompanyfunctions, Resource Group: TestCompany-core
- Storage Account: jenolantimedelayoc8c092e, Resource Group: jenolantimedelayoccupanc
- Storage Account: orcaremediationaaa4382d, Resource Group: Orca-Remediation

Finding:
Public access is configured for the identified storage accounts. This non-default configuration, if explicitly configured, can allow for anonymous, public read access to a container and its blobs.

Potential Severity: Medium

Assessed Severity:

Remediation:
Disable public access for storage accounts, unless it is a business requirement. If public access is required, monitor anonymous requests using Azure Metrics Explorer. To change access levels: Go to "Storage Accounts"→select the affected storage account, select Containers under "Data Storage"→select the resources and select "change access level" at the top of the page→change the Public access level drop down to "Private (no anonymous access)" Alternatively, the following PowerShell commands can be run on each of the affected blobs: Set-AzStorageAccount -ResourceGroupName "$ResourceGroupName" -Name "$StorageAccountName" -AllowBlobPublicAccess $false

References:
↗ Configure anonymous public read access for containers and blobs

Medium [6]: Virtual Machines with Extensions

👎 Virtual Machines with Extensions

Affected Azure Objects:
● Virtual Machine: cloud-ct-base, Extensions: AADSSHLoginForLinux,AzurePerformanceDiagnosticsLinux,AzurePolicyforLinux,OmsAgentForLinux
● Virtual Machine: TestCompany-vpn, Extensions: AADSSHLoginForLinux,AzurePolicyforLinux,OmsAgentForLinux

Finding:
The listed virtual machines were found to have Virtual Machine Extensions installed. Installed extensions may allow for misconfigurations, data leakage, or unintended access to the resources they are installed on.

Potential Severity: Medium

Assessed Severity:

Remediation:
Navigate to the identified virtual machines individually → select "Extensions" and review the installed extensions. Remove any unapproved extensions, or extensions no longer in use, by selecting "Uninstall" on the desired extension.

References:
↗ Azure virtual machine extensions and features
↗ Microsoft Azure VMs Hijacked in Cloud Cyberattack

Low [7]: Storage Accounts Minimum TLS Version Less Than TLSv1.2

👍 Storage Accounts Minimum TLS Version Less Than TLSv1.2

Affected Azure Objects:
● Storage Account: TestCompanycoreperfdiag880, Resource Group: TestCompany-core, Current TLS Setting: TLS1_0
● Storage Account: jenolantimedelayoc8c092e, Resource Group: jenolantimedelayoccupanc, Current TLS Setting: TLS1_0
● Storage Account: orcaremediationaaa4382d, Resource Group: Orca-Remediation, Current TLS Setting: TLS1_0

Finding:
The identified Storage Accounts have configurations that allow insecure TLS versions. TLS 1.0 and 1.1 are susceptible to downgrade attacks and other vulnerabilities. All Storage Accounts should accept at a minimum TLS version 1.2.

Potential Severity: Low

Assessed Severity:

Remediation:
Go to storage accounts⟶select the affected storage account⟶under the "Minimum TLS version", select Version 1.2, and save.

References:
↗ Enforce a minimum required version of Transport Layer Security (TLS) for requests to a storage account

Informational [8]: Non-Default Network Security Group Firewall Rules Found

Non-Default Network Security Group Firewall Rules Found

Affected Azure Objects:

- Resource: cloud-ct-base-nsg; Non-default Firewall Rules: Name: MicrosoftDefenderForCloud-JITRule_1350811658_9CCEFA6447AD40739C83CA28D3DEB0E4; Access: Deny; Direction: Inbound; SourcePorts: *; DestinationPorts: 22; SourceIP: *; DestinationIP: 10.0.4.68 Name: AllowVnet; Access: Allow; Direction: Inbound; SourcePorts: *; DestinationPorts: *; SourceIP: VirtualNetwork; DestinationIP: 10.0.4.68 Name: AllowMyIpAddressCustomAnyInbound; Access: Allow; Direction: Inbound; SourcePorts: *; DestinationPorts: *; SourceIP: 180.150.44.30 49.3.105.164; DestinationIP: 10.0.4.68 Name: AllowCidrBlockCustom8080Inbound; Access: Allow; Direction: Inbound; SourcePorts: *; DestinationPorts: *; SourceIP: 106.71.18.208; DestinationIP: *
- Resource: TestCompany-vpn-nsg; Non-default Firewall Rules: Name: MicrosoftDefenderForCloud-JITRule_-710473118_BEF2C30549714984B07F2C86AE7A1824; Access: Deny; Direction: Inbound; SourcePorts: *; DestinationPorts: 22; SourceIP: *; DestinationIP: 10.0.4.73 Name: AllowWireguardPort; Access: Allow; Direction: Inbound; SourcePorts: *; DestinationPorts: 51194; SourceIP: *; DestinationIP: * Name: Allow10051ForActiveAgents; Access: Allow; Direction: Inbound; SourcePorts: *; DestinationPorts: 10051; SourceIP: *; DestinationIP: * Name: Allow10050ForPassiveAgents; Access: Allow; Direction: Inbound; SourcePorts: *; DestinationPorts: 10050; SourceIP: *; DestinationIP: *

Finding:

Non-default Network Security Group (NSG) firewall rules were found. As NSG rules are generally simple Block/Allow rules, there is potential for the rules to be misconfigured, overly permissive, or no longer necessary.

Potential Severity: Informational

Assessed Severity:

Remediation:

Review the results of this finding and determine if the rules are expected and appropriate. To remediate, go to Subscriptions→select the identified subscription→select the identified Resource Group → select the identified resource → select "Networking" under the Settings heading → select the identified rule and choose whether to change the configuration or delete the rule.

References:

- Network security groups
- How network security groups filter network traffic
- Azure Firewall vs NSG

Informational [9]: RBAC Roles Assigned at Subscription Scope

👍 RBAC Roles Assigned at Subscription Scope

Affected Azure Objects:
● 5029 affected objects identified. See supplemental document *All_Resource_RBAC_Assignment.csv* for additional details.

Finding:
All members of Azure Role-based Access Control (RBAC) roles assigned to the individual resources were exported. Permissions of role members assigned at the subscription scope are inherited by all resources and resource groups by default. Inherited and explicit permissions are identified in the output.

Potential Severity: Informational

Assessed Severity:

Remediation:
Review existing assignments and action as necessary.

References:
↗ Remove Azure role assignments
↗ What is Azure role-based access control (Azure RBAC)?

Informational [10]: Soft Delete Retention Less than 90 Days

👍 Soft Delete Retention Less than 90 Days

Affected Azure Objects:
- Cluster Name: yolotoonnx0425418561, Location: eastus2, Soft Delete Retention Period:

Finding:
Soft delete retention is set for less than 90 days. Soft delete allows you to recover an accidentally deleted key vault for a specified amount of time. This prevents any accidental loss of secrets, certificates, and keys in the key vault.

Potential Severity: Informational

Assessed Severity:

Remediation:
Select Key Vault from the Azure Portal→click on "Properties" tab→select the radio button corresponding to "Enable soft delete"→enter a retention period in days. The recommended configuration for Soft Delete Retention is 90 days, unless superseded by policy or regulatory requirements.

References:
↗ Soft-delete will be enabled on all key vaults
↗ Azure Key Vault soft-delete overview

Informational [11]: Virtual Machine Disks not Encrypted

👍 Virtual Machine Disks not Encrypted

Affected Azure Objects:
● OS Volume and Data Volumes on VM cloud-ct-base are not encrypted.
● OS Volume and Data Volumes on VM TestCompany-vpn are not encrypted.

Finding:
List of Virtual machines with unencrypted disks and/or volumes.

Potential Severity: Informational

Assessed Severity:

Remediation:
Navigate to the identified virtual machines individually → select "Disks" → select "Encryption" → select the disk(s) to encrypt → select or configure an Azure Key Vault to manage the disks encryption keys.

References:
↗ Configure email notifications for security alerts
↗ Create and configure a key vault for Azure Disk Encryption on a Windows VM

Informational [12]: Virtual Machine Disks not Encrypted with Customer Managed Keys

👍 Virtual Machine Disks not Encrypted with Customer Managed Keys

Affected Azure Objects:
● Disk cloud-ct-base_OsDisk_1_bfbf6b887ee44479b7d06c8904a4e942 on VM cloud-ct-base using encryption type EncryptionAtRestWithPlatformKey
● Disk TestCompany-vpn_OsDisk_1_6fb6cc26136241c5b0ac53ad8c5f2bfd on VM TestCompany-vpn using encryption type EncryptionAtRestWithPlatformKey

Finding:
List of Azure disk encryption types on all current VM's

Potential Severity: Informational

Assessed Severity:

Remediation:
Navigate to the identified virtual machines individually → select "Disks" → select "Encryption" → select the disk(s) to encrypt → select or configure an Azure Key Vault to manage the disks encryption keys.

References:
↗ [Configure email notifications for security alerts]

Data Loss Prevention Assessment Findings

Prepared by

WhiteRook Cyber

WhiteRook Cyber

DLP Assessment

DLP Assessment

White Rook Cyber assesses your compliance posture, highlights risks and recommends remediation steps to ensure compliance with essential data protection and regulatory standards.

Prepared for organization: **Conducive Technology Pty Ltd**

Tenant Name: **conducivetech.onmicrosoft.com**

Note: The following report is customized for following geolocation(s): Australia

Solutions Summary

All Solutions	1	14	8
Compliance Manager			
Compliance Manager	1	0	0
Discovery & Response			
Audit	0	1	1
eDiscovery	0	2	0
Insider Risk			
Communication Compliance	0	2	1
Insider Risk Management	0	2	0
Microsoft Information Governance			
Information Governance	0	2	0
Records Management	0	2	0
Microsoft Information Protection			
Information Protection	0	3	0

● Recommendation ● Improvement ● OK

Note: There was an issue in fetching Data Loss Prevention, Information Protection information. Insufficient Licensing Error.

Audit

Improvement Enable Auditing in Office 365

👎 Your organization should enable auditing for your Office 365 tenant

Your organization should enable auditing for your Office 365 tenant. When audit log search in the Security & Compliance Center is turned on, user and admin activity from your organization is recorded in the audit log and retained for 90 days, and up to one year depending on the license assigned to users.

Configuration	Setting	Status
Auditing in Office 365	Disabled	☒ **Improvement** Remediation Available

↗ Advanced Audit

↗ Compliance Center - Audit Log search

↗ Compliance Manager - Audit Actions

↗ How to search Audit Log

Remediation Script

OK Configure Alert Policies

Your organization has configured alert policies

Your organization should configure alert policies to send notifications on activities that are indicators of a potential security issue or data breach. Office 365 provides built-in alert policies that are turned on by default.

Alert Policy	Severity	Email notifications	Status
Suspicious connector activity	High	TenantAdmins	✓ Ok
Reply-all storm detected	High	TenantAdmins	✓ Ok
User restricted from sharing forms and collecting responses	High	TenantAdmins	✓ Ok
Potential Nation-State Activity	High	TenantAdmins	✓ Ok
Priority accounts' mail flow is unhealthy	High	TenantAdmins	✓ Ok
User restricted from sending email	High	TenantAdmins	✓ Ok
Form blocked due to potential phishing attempt	High	TenantAdmins	✓ Ok
Suspicious Email Forwarding Activity	High	TenantAdmins	✓ Ok
Messages have been delayed	High	TenantAdmins	✓ Ok
Tenant restricted from sending unprovisioned email	High	TenantAdmins	✓ Ok
Tenant restricted from sending email	High	TenantAdmins	✓ Ok
Failed exact data match upload	High	TenantAdmins	✓ Ok
Form flagged and confirmed as phishing	High	TenantAdmins	✓ Ok
Suspicious tenant sending patterns observed	High	TenantAdmins	✓ Ok

↗ Compliance Manager - Audit Actions

↗ Learn more about alert policies

↗ Security & Compliance Console : Alert Policies

↗ Turn on audit log search

Communication Compliance

Improvement Remediate Corporate Policy Violation

Your organization needs to remediate corporate policy violations

Your organization should use communication compliance to scan internal and external communications for policy matches so they can be examined by designated reviewers. Reviewers can investigate scanned communications and take appropriate remediation actions.

Communication Compliance Remediation	Items pending Review	Status
Communication Compliance Policy Matches	No communication Policy defined	⊗ Improvement

↗ Communication compliance in Microsoft 365

↗ Compliance Center - Communication Compliance

↗ Compliance Manager - CC Actions

Improvement Monitor Communications for Offensive or Threatening Language

👎 Your organization should define policies to monitor internal communications

Your organization should use communication compliance to monitor internal communication for offensive and threatening language. You can create a policy that uses pretrained classifier to detect content containing profanities or language that might be considered threatening or harrassment.

Policy	Policy Status	Status
No Active Policy Defined	No Active Policy Defined	✖ **Improvement**

↗ Communication compliance in Microsoft 365

↗ Compliance Center - Communication Compliance

↗ Compliance Manager - CC Actions

OK Enable Communication Compliance in O365

Your organization has enabled Communication Compliance in O365

Your organization should use communication compliance to scan internal and external communications for policy matches so they can be examined by designated reviewers.

Role	Role Groups (Having 1 or more members)	Status
Supervisory Review Administrator	SupervisoryReview	✓ Ok
Case Management	OrganizationManagement, ComplianceAdministrator, eDiscoveryManager, InsiderRiskManagement, InsiderRiskManagementAdmins, InsiderRiskManagementAnalysts, InsiderRiskManagementInvestigators, CommunicationComplianceInvestigators, CommunicationCompliance, PrivacyManagement, PrivacyManagementAdministrators, PrivacyManagementAnalysts, PrivacyManagementInvestigators, SubjectRightsRequestAdministrators, DataSecurityManagement, CommunicationComplianceAdministrators, CommunicationComplianceAnalysts, CommunicationComplianceViewers	✓ Ok
Compliance Administrator	OrganizationManagement, ComplianceAdministrator, ComplianceDataAdministrator	✓ Ok

Communication compliance in Microsoft 365

Compliance Center - Communication Compliance

Compliance Manager - CC Actions

Compliance Manager

Recommendation Use Compliance Manager to manage your compliance posture

Your organization should use Compliance Manager to manage your compliance posture

Compliance Manager is an end-to-end solution in the Microsoft 365 compliance center for managing and tracking compliance activities. It simplifies compliance and helps reduce risk. Compliance Manager translates complex regulatory requirements to specific controls and through compliance score, provides a quantifiable measure of compliance. It offers intuitive compliance management, a vast library of scalable assessments, and built-in automation. Its a great place to begin your compliance journey because it gives you an initial assessment of your compliance posture the first time you visit.

Compliance Manager Quickstart Guide

Learn more about Compliance Manager

Visit Compliance Manager

eDiscovery

Improvement Use Advanced eDiscovery Cases to Support Legal Investigations

Your organization needs to review (or set up) Advanced eDiscovery cases

Your organization should use Advanced eDiscovery to manage the end-to-end workflow to preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations.

Case Name	Case Status	Status
No eDiscovery cases found		✖ Improvement

↗ Compliance Center - Advanced eDiscovery ↗ eDiscovery in Microsoft 365 ↗ Get started with Advanced eDiscovery

Improvement Use Core eDiscovery Cases to Support Legal Investigations

Your organization needs to review (or set up) Core eDiscovery cases

Your organization should use Core eDiscovery cases to identify, hold, and export content found in Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, and Skype for Business conversations, and Yammer teams.

Case Name	Case Status	Status
No eDiscovery cases found		✖ Improvement

↗ Compliance Center - Core eDiscovery ↗ eDiscovery in Microsoft 365 ↗ Get started with Core eDiscovery

Information Governance

Improvement Use Data Retention Labels and Policies

Your organization should use retention policies by publishing a retention label

Your organization should apply retention labels to content when it matches specific conditions (such as containing specific keywords or types of sensitive information).

Retention Policies	Labels	Remarks	Status
No active policy or label defined		**Affected workloads:** Exchange, SharePoint, OneDrive	✖ **Improvement**

↗ Compliance Center - Information Governance

↗ Compliance Manager - IG Actions

↗ Learn More Overview of retention labels

↗ Overview of retention policies

Improvement Auto-Apply Retention Labels

Your organization should use auto-apply retention policies

Your organization should automatically apply retention labels to content when it matches specific conditions (such as containing specific keywords or types of sensitive information). Microsoft recommends that automatic labeling be implemented to decrease reliance on users for correct classification.

Retention Policies	Labels	Remarks	Status
No active policy or label defined		**Affected workloads:** Exchange, SharePoint, OneDrive	✖ Improvement

Compliance Center - Information Governance

Compliance Manager - IG Actions

Learn More Overview of retention labels

Overview of retention policies

Information Protection

Improvement Use IRM for Exchange Online

Your organization should enable IRM for Exchange Online

Your organization should enable and use Azure Information Protection for Exchange Online. This configuration lets Exchange provide protection solutions, such as mail flow rules, data loss prevention policies that contain sets of conditions to filter email messages and take actions, and protection rules for Outlook clients.

IRM Configuration	Setting	Status
AzureRMSLicensingEnabled	False	✖ Improvement

Compliance Center - Information Protection

Compliance Manager - IP Actions

How to configure applications for Azure Rights Management

Improvement Auto-apply client side sensitivity labels

Your organization should use client side sensitivity labels

Your organization should automatically apply client side sensitivity labels based on sensitive information types or other criteria. Microsoft recommends that automatic labeling be implemented to decrease reliance on users for correct classification.

Labels	Remarks	Status
No Auto Apply Policy		✖ Improvement

Compliance Center - Information Protection

Compliance Manager - IP Actions

How to apply a sensitivity label to content automatically

Overview of sensitivity labels

Improvement Create Sensitivity Labels for Sensitive or Critical Data

Your organization should be using sensitivity labels to classify your information

Your organization should use sensitivity labels and policies to classify your information in SharePoint Online, OneDrive for Business, and Exchange Online. This helps categorize your most important data and effectively protect it from illicit access; it can also make it easier to investigate discovered breaches.

Label Policy	Labels	Remarks	Status
No Active Policy defined	No Active Policy defined		✖ Improvement

↗ Compliance Center - Information Protection

↗ Compliance Manager - IP Actions

↗ How to configure classifications for your Microsoft 365 environment

↗ Overview of sensitivity labels

Insider Risk Management

Improvement Create customized or use default insider risk management policies for departing employee data theft

Your organization should set up IRM policies for departing employee data theft

Your organization should create an insider risk management policy to detect, investigate, and take action on departing employee data theft. Insider risk management in Microsoft 365 leverages an HR connector and selected indicators to alert you of any user activity related to data theft among departing employees.

Policy	User Groups	Status
No active policy defined		✖ Improvement

[Compliance Center - Insider Risk Management]

[Getting started with Insider risk management]

[Insider risk management policies]

Improvement Create customized or use default insider risk management policies for data leaks

Your organization should set up IRM policies for data leaks

Microsoft recommends that your organization create an insider risk management policy to detect, investigate, and take action on data leaks. Data leaks can include accidental oversharing of information outside your organization or data theft with malicious intent.

Policy	User Groups	Status
No active policy defined		❌ Improvement

[Compliance Center - Insider Risk Management](#)

[Getting started with Insider risk management](#)

[Insider risk management policies](#)

Records Management

Improvement Declare Data as Records by Creating & Publishing a Record Label

👎 Your organization should use record labels to declare data as records

Your organization should use records management to manage regulatory, legal, and business-critical records across corporate data. By using retention labels to declare records, you can implement a single, consistent records-management strategy across all of Office 365.

Policy Name	Labels	Remarks	Status
No record label policy defined		**Affected workloads:** Exchange, SharePoint, OneDrive	✖ Improvement

↗ Compliance Center - Records Management

↗ Compliance Manager - RM Actions

↗ Overview of Records

↗ Records management in Microsoft 365

Improvement Automatically Apply Record Labels

Your organization should use auto apply record label policies

Your organization should use records management to manage regulatory, legal, and business-critical records across corporate data. You can automatically apply record labels to content that matches certain conditions.

Policy Name	Labels	Remarks	Status
No record label policy defined		**Affected workloads:** Exchange, SharePoint, OneDrive	✖ Improvement

↗ Compliance Center - Records Management

↗ Compliance Manager - RM Actions

↗ Overview of Records

↗ Records management in Microsoft 365