purple knight

SECURITY ASSESSMENT REPORT

v 4.2.2312.5001 | Community

Note: A typical Active Directory is in a constant state of flux, with hundreds or even thousands of changes made each day.
Purple Knight offers a helpful snapshot of your security posture, but it's no substitution for continuous monitoring of events taking place in your directory.
To learn more about a comprehensive, round-the-clock monitoring of all aspects of AD, click here.

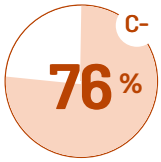
SECURITY POSTURE OVERVIEW

This report summarizes the security assessment results performed in your hybrid identity environment on 19/05/2024 by Semperis' Active Directory security assessment tool, Purple Knight. Depending on the environments selected for evaluation, the report includes the assessment results for an Active Directory forest, an Azure AD tenant, Okta domain, or all.

- Active Directory forest: Purple Knight queried the Active Directory environment and ran a series of security indicator scripts against domains within the selected forest (see Appendix 1 – Domains list for a full list of the domains included in the assessment).
- Azure AD tenant: Purple Knight queried the selected Azure AD tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.
- Okta identity platform: Purple Knight queried the selected Okta domain checking for activities that may indicate unauthorized access attempts, suspicious behavior, or potential threats within the Okta infrastructure.

The report provides an overall security risk score as well as detailed results about each Indicator of Exposure (IOE) found. By uncovering security weaknesses, this assessment report provides valuable insight into the overall security posture across your hybrid identity environment and presents opportunities to minimize the attack surface and stay ahead of the ever-changing threat landscape.

View Appendix 1 - Domains list



AZURE AD

Tenant	**thecybersecuritycrew.au**
Application ID	**c11e6d85-0277-49cb-9811-aadf0ab904e0**
Duration	**00:00:27.7845585**

Indicators

Evaluated	**35**
Not selected	**0**
IOEs found	**18**
Passed	**17**
Failed to run	**0**
Not Relevant	**0**
Canceled	**0**

CRITICAL IOEs FOUND

None

ADDITIONAL IOEs FOUND

NAME	PLATFORM	SEVERITY LEVEL	ACTION
• Application Name and Geographic Location additional contexts are disabled on MFA	Azure AD	Warning	Read More...
• Certificate-Based Authentication Persistence	Azure AD	Warning	Read More...
• Check for guests having permission to invite other guests	Azure AD	Warning	Read More...
• Check for users with weak or no MFA	Azure AD	Warning	Read More...
• Conditional Access Policy that disable admin token persistence	Azure AD	Warning	Read More...
• Conditional Access Policy that does not require a password change from high risk users	Azure AD	Warning	Read More...
• Conditional Access Policy that does not require MFA when sign-in risk has been identified	Azure AD	Warning	Read More...
• MFA not configured for privileged accounts	Azure AD	Warning	Read More...
• More than 5 Global Administrators exist	Azure AD	Warning	Read More...
• Non-admin users can create tenants	Azure AD	Warning	Read More...
• Non-admin users can register custom applications	Azure AD	Warning	Read More...
• Non-synced AAD user that is eligible for a privileged role	Azure AD	Warning	Read More...
• Unrestricted user consent allowed	Azure AD	Warning	Read More...
• Administrative units are not being used	Azure AD	Informational	Read More...
• Check if legacy authentication is allowed	Azure AD	Informational	Read More...
• Custom banned password protection not in use	Azure AD	Informational	Read More...
• Guest users are not restricted	Azure AD	Informational	Read More...
• Users can create security groups	Azure AD	Informational	Read More...

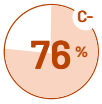
INDICATORS FAILED TO RUN

None

Notes

AZURE AD RESULTS

Categories



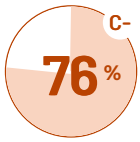
AZURE AD

Azure AD indicators look for common attack vectors that threat actors use to gain access to

Read More ...

CATEGORY

AZURE AD



WEIGHT	EVALUATED	INDICATORS FOUND
7	35	18

Azure AD indicators look for common attack vectors that threat actors use to gain access to the Azure AD environment.

SECURITY INDICATOR

Application Name and Geographic Location additional contexts are disabled on MFA

IOE Found

SEVERITY	WEIGHT
Warning	6

Security Frameworks

MITRE ATT&CK

- Initial Access

MITRE D3FEND

- Harden - Multi-factor Authentication

Description

This indicator checks if Application Name and Geographic Location additional contexts are enabled on MFA. Required permissions: Policy.Read.All

Likelihood of Compromise

MFA bombing is a tactic where an attacker spams the user with MFA authentication requests and the user unknowingly or unwillingly accepts the attempt. Enabling the application name and geographic location additional contexts on MFA provides another level of security for a user sign-in. That is, when these additional contexts are enabled, the name of the application and the location based on the IP address where the sign-in originated from are displayed, which helps the user verify that the authentication request is legitimate. https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context

Result

Application name and geographic location additional contexts on MFA are disabled.

Remediation Steps

Enable application name and geographic location on MFA so the users will see on their app the application name attempting to ask for sign-in approval and additionally will receive the location based on the IP address from where the sign-in request was initiated for the sign-in approval request. To enable Application Name additional context on MFA go to -> Azure portal -> Azure Active Directory -> Security -> Authentication methods -> Microsoft Authenticator -> Configure tab, under the configure tab you will see Show application name in push and passwordless notifications, turn the status to Enabled and set to "all users". To enable Geographic location addidtional context on MFA go to -> Azure portal -> Azure Active Directory -> Security -> Authentication methods -> Microsoft Authenticator -> Configure tab, under the configure tab you will see Show geographic location in push and passwordless notifications, turn the status to Enabled and set to "all users". Under the "Basic" tab select all users.

SECURITY INDICATOR

Conditional Access policy with Continuous Access Evaluation disabled

Pass

SEVERITY	WEIGHT
Warning	5

Security Frameworks

MITRE ATT&CK

- Persistence
- Privilege Escalation

Description

This indicator checks for Conditional Access policies that have the Continuous Access Evaluation feature disabled. Required permissions: Policy.Read.All

Likelihood of Compromise

The Continuous Access Evaluation feature allows you to revoke the access token for Microsoft applications and limit the time an attacker has access to company data.

Result

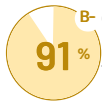
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Certificate-Based Authentication Persistence

IOE Found



SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Persistence
- Privilege Escalation

Description
This indicator assesses the presence of specific Azure AD MS Graph app roles and permissions that, when combined, can enable a user to establish persistence through certificate-based authentication (CBA). The indicator examines the following roles and permissions and their implications for potential persistence through CBA:

The following role/permission assignment allows you to enable CBA in your Azure AD tenant.
- User account assigned the Authentication Policy Administrator role.
- Application with Policy.ReadWrite.AuthenticationMethod permission.

The following permission allows you to add a Root CA once CBA is enabled.
- App with Organization.ReadWrite.All permission.

In addition to the above, the indicator also checks for accounts assigned the following roles and permissions, which should be reviewed to determine if they are required:
- Privileged Role Administrator
- Privileged Authentication Administrator
- RoleManagement.ReadWrite.Directory
- AppRoleAssignement.ReadWrite.All

Likelihood of Compromise
If an attacker is able to gain access to an Account with Authentication Policy Administrator role or an application with a combination of "Policy.ReadWrite.AuthenticationMethod" and "Organization.ReadWrite.All" permissions, they can log into Azure AD as any user, even a Global Administrator

Result
Found 1 principals with at least one of the required permissions to be able to persist using CBA

Name	ID	RoleDefinitionID	Type	ObjecType	Ignored
Demouser8@thecybersecuritycrew.au	87e3ccac-eb37-4c41-8f1c-319cf3b918d5	Privileged Role Administrator	Active	User	False

Showing 1 of 1

Remediation Steps
To mitigate the risk associated with the Certificate-Based Authentication Persistence indicator, it is recommended to review and evaluate the necessity of this permission for each Microsoft Graph app role/permission assignments to ensure they are required. Limit the assignment of the following permission to only trusted apps that genuinely need to add a Root CA once CBA is enabled:
- Authentication Policy Administrator
- Application with Policy.ReadWrite.AuthenticationMethod and Organization.ReadWrite.All permissions.

Remove the roles and permissions from any accounts that do not require them for legitimate operational or administrative purposes:
- Privileged Role Administrator
- Privileged Authentication Administrator
- RoleManagement.ReadWrite.Directory
- AppRoleAssignement.ReadWrite.All

SECURITY INDICATOR

Administrative units are not being used

IOE Found

SEVERITY
Informational

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Lateral Movement

Description
This indicator checks for the existence of administrative units. Administrative units are helpful to limit the scope of a security principle's authority. Required permissions: AdministrativeUnit.Read.All

Likelihood of Compromise
Attackers that compromise an administrator account could have wide-ranging access across resources. By utilizing admninistrative units, it is possible to limit the scope of specific admins and ensure that a single compromise of credentials is constrained and does not affect the entire environment. For more info click here.

Result
There are ZERO Administrative Units created.

Remediation Steps
Review the organizational structure and consider adding Administrative Units to limit delegation scope.

SECURITY INDICATOR

Conditional Access policies contain private IP addresses

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Initial Access

Description
This indicator checks if any named locations contains private IP addresses which are used on an enabled Conditional Access policy. Required permissions: Policy.Read.All

Likelihood of Compromise
Having private IP addresses in named locations associated with Conditional Access policies could result in an undesired security posture.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Check for guests having permission to invite other guests

IOE Found

F 0 %

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Lateral Movement

Description
This indicator checks for guests that have permission to invite other guests. Required permissions: Policy.Read.All

Likelihood of Compromise
Allowing guests to invite other guests means that invitations can take place outside of any entitlement management in place. For more info click here.

Result
Guests are allowed to send guest invitations.

Remediation Steps
To prevent unauthorized guests from inviting others into the organization, consider updating the "Guest invite settings" to restrict this ability. This can be done through the Azure Active Directory portal. To update the "Guest invite settings" to restrict unauthorized guests from inviting others into the organization, follow these steps:

Navigate to the Azure Active Directory portal (https://portal.azure.com).
Search for and select "Azure Active Directory".
Select "External identities" from the left-hand menu.
Select "Set up external collaboration settings."

In the "Guest invite settings" section, choose the desired setting for "Guest invite restrictions." You can choose to allow only admin roles, any member, or no one to invite guests.
Click "Save" to apply the changes.
For more information, see the Microsoft documentation on configuring external collaboration settings in Azure Active Directory here.

SECURITY INDICATOR

Users or devices inactive for at least 90 days

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Persistence
- Privilege Escalation

Description
This indicator checks for users or devices that have not signed in during the past 90 days. Required permissions: Device.Read.All, User.Read.All

Likelihood of Compromise
If a user or device has been inactive for 90 days or more, it is likely that the account or device is no longer in use and leaves an open gate to the Azure AD tenant.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Check if legacy authentication is allowed

IOE Found

F 0 %

SEVERITY
Informational

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Credential Access

Description
This indicator checks whether legacy authentication is blocked, either via conditional access policies or security defaults. Required permissions: Policy.Read.All

Likelihood of Compromise
Allowing legacy authentication increases the risk that an attacker will logon using previously compromised credentials. For more info click here.

Result
Legacy Authentication is not being blocked.

LegacyAuthenticationMethod
exchangeActiveSync
other

Showing 2 of 2

Remediation Steps
To protect the authentication process, it is recommended to block legacy authentication (i.e. client app types such as exchangeActiveSync and others) for all users via conditional access policies or by enabling security defaults.

SECURITY INDICATOR

Conditional Access policies that contain MFA Trusted IPs

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Defense Evasion

Description
This indicator checks if any enabled Conditional Access policies contain references to MFA Trusted IPs. Required permissions: Policy.Read.All

Likelihood of Compromise
When 'MFA Trusted IPs' is used, Continuous Access Evaluation (CAE) is unable to properly evaluate changes in a user's location. This can lead to a lack of access enforcement and an unstable security posture.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Privileged group contains guest account

Pass

SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

Description
This indicator checks whether any privileged roles have been assigned to guest accounts. Required permissions: User.Read.All, RoleManagement.Read.Directory

Likelihood of Compromise
External attackers covet privileged accounts, as they provide a fast track to an organization's most critical systems. Since guest accounts represent an external entity and do not undergo the same account security as users in your tenant, assigning privileged roles to them poses a heightened risk.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

MFA not configured for privileged accounts

IOE Found

SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Credential Access

Description
This indicator checks that MFA (Multi-Factor Authentication) is enabled for users with administrative rights. Required permissions: RoleManagement.Read.Directory, Reports.Read.All

Likelihood of Compromise
Accounts having privileged access are more valuable targets to attackers. A compromise of a privileged user represents a significant risk. As a result, these accounts require extra protections.

Result
5 privileged user(s) found without MFA configured.

UserName	MFARegistered	Ignored
david@thecybersecuritycrew.au	False	False
kevin@thecybersecuritycrew.au	False	False
neil@thecybersecuritycrew.au	False	False
svc-automation@thecybersecuritycrew.au	False	False
targetuser1@thecybersecuritycrew.onmicrosoft.com	False	False

Showing 5 of 5

Remediation Steps
It is recommended to configure MFA for privileged user(s).

SECURITY INDICATOR

Check for risky API permissions granted to application service principals

Pass

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

Description
This indicator checks if one of the following risky application roles have been assigned for API permissions: RoleManagement.ReadWrite.Directory that can directly promote to Global Admin, and AppRoleAssignment.ReadWrite.All that can grant SELF above role, thus allowing promotion to Global Admin. Required permissions: Application.Read.All

Likelihood of Compromise
A malicious application administrator could use these permissions to grant administrative privileges to themself or another.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Check for users with weak or no MFA

IOE Found

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Initial Access
- Lateral Movement

Description
This indicator checks all users for MFA registration as well as which additional methods are configured. SMS and Voice are considered less secure than mobile applications and FIDO

Likelihood of Compromise
Due to the lack of uniform security measures put in place within mobile networks, SMS and voice cannot be relied upon to provide adequate security. A malicious user can vish/smish codes and trick users into providing authentication.

Result
Out of 19 users, 14 (74%) either aren't registered for MFA or are using weak MFA methods.

UserPrincipalName	MFARegistered	AuthMethods	Ignored
Demouser1@thecybersecuritycrew.au	False	N/A	False
Demouser2@thecybersecuritycrew.au	False	N/A	False
Demouser4@thecybersecuritycrew.au	False	N/A	False
Demouser5@thecybersecuritycrew.au	False	N/A	False
Demouser6@thecybersecuritycrew.au	False	N/A	False
Demouser7@thecybersecuritycrew.au	False	N/A	False
Demouser9@thecybersecuritycrew.au	False	N/A	False
neilr.sec_gmail.com#EXT#@thecybersecuritycrew.onmicrosoft.com	False	N/A	False
puneeth@thecybersecuritycrew.au	False	N/A	False

Showing 9 of 9

Remediation Steps
It is recommended to avoid using SMS or Voice as MFA methods.

SECURITY INDICATOR

Security defaults not enabled

Pass

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Initial Access
- Credential Access

Description
This indicator checks whether security defaults are enabled when there are no conditional access policies configured. Required permissions: Policy.Read.All

Likelihood of Compromise
As attackers constantly attempt to compromise cloud environments, it is important to maintain the highest possible security baseline for authentication. To protect the authentication process and privileged actions, security defaults are recommended for tenants that have no conditional access policies configured. Security defaults will require MFA, block legacy authentication, and require additional authentication when accessing the Azure portal, Azure Powershell, or the Azure CLI.

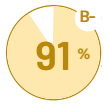
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Non-synced AAD user that is eligible for a privileged role

IOE Found



SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

Description
This indicator checks for Azure AD users that are eligible for a high-privilege role and have the proxyAddress attribute, but are not synchronized with an AD account. For more information see the following Semperis blog entry. Required permissions: User.Read.All, RoleManagement.Read.Directory, Directory.Read.All

Likelihood of Compromise
An attacker might use SMTP matching to synchronize controlled AD users with AAD users that are eligible for high-privilege roles. This process overwrites the AAD password and could result in privilege escalation over AAD.

Result
Found 1 users not sychronized with on-prem which are eligible to high privilege role assignment.

displayName	UPN	ProxyAddresses	Roles	Ignored
Demouser8	Demouser8@thecybersecuritycrew.au	SMTP:Demouser8@thecybersecuritycrew.au	User administrator	False

Showing 1 of 1

Remediation Steps
Read more about this potential attack and follow the remediation steps in the Semperis blog entry.

SECURITY INDICATOR

Unrestricted user consent allowed

IOE Found

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Persistence
- Lateral Movement

Description
This indicator checks if users are allowed to add applications from unverified publishers. Required permissions: Policy.Read.All

Likelihood of Compromise
When users are allowed to consent to any 3rd party applications, there is considerable risk that an allowed app will take intrusive or risky actions.

Result
Users are allowed to consent to risky 3rd party apps.

Remediation Steps
To protect the confidentiality of company data and improve security posture, it is recommended that users not have the ability to consent to all 3rd party apps. The best practice is to allow user consent only for applications that have been published by a verified publisher and have administrators approve all other consent requests via the admin consent workflow.

SECURITY INDICATOR

Custom banned password protection not in use

IOE Found

SEVERITY
Informational

WEIGHT
2

Security Frameworks
MITRE ATT&CK

- Credential Access
- Initial Access

MITRE D3FEND

- Harden - Strong Password Policy

Description
This indicator checks if custom banned password protection is enabled. To improve security, a custom banned password list allows you to add specific strings that are used to validate user passwords and block weak password terms.

Required permissions:
Directory.Read.All

Likelihood of Compromise
Attackers often use password guessing attacks to take control over user accounts. Organizations that do not use custom banned password protection to block weak passwords are more susceptible to password guessing attacks.

Result
Custom banned passwords not in use.

Remediation Steps
Enable **Enforce custom list** in Entra ID, populate the **Custom banned password list** and then routinely verify if the list requires any additions or changes.

The configuration for custom banned passwords can be found in the Microsoft Entra admin center (direct link).

To browse to the settings in the Microsoft Entra admin center, expand the **Protection** menu on the left, select **Authentication methods**, and then **Password protection**. On the right of the blade you want to ensure **Enforce custom list** is set to **Yes**, and that **Custom banned password list** is populated with banned words.

For further reference on using and maintaining custom banned passwords, see Password protection in Microsoft Entra ID | Microsoft Learn.

SECURITY INDICATOR

Conditional Access Policy that disable admin token persistence

IOE Found

F 0 %

SEVERITY
Warning

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Credential Access

Description
This indicator looks for Conditional Access policies that disable token persistence for users with admin roles and have a sign-in frequency that is less than or equal to 9 hours. Required permissions: Policy.Read.All

Likelihood of Compromise
When an admin login his token cached on the client and he is now vulnerable for a Primary Refresh Token related attacks.

Result
No Conditional Access policies are configured to disable admin token persistence with a sign-in frequency set to 9 or less hours.

Remediation Steps
Create a new Conditional Access Policy - 1. Under "Assignments" select "Users and Groups" a. Under "Include" select "Select users and groups" b. Select "Directory roles" and add the following roles: Global Administrator, Application Administrator, Authentication Administrator, Billing Administrator, Cloud Application Administrator, Conditional Access Administrator, Exchange Administrator, Helpdesk Administrator, Password Administrator, Privileged Authentication Administrator, Security Administrator, SharePoint Administrator, User Administrator, Authentication Policy Administrator, External Identity Provider Administrator, Privileged Role Administrator. You can select more roles if necessary, but the roles listed above are mandatory. 2. Under "Cloud apps or actions" select "All cloud apps". 3. Under "Session" select the following : a. Check "Sign-in frequency" and select "Periodic reauthentication". In the first field, enter a value of 9 and in the second field, select "Hours". b. Check "Persistent browser session" and select "Never persistent".

SECURITY INDICATOR

AAD Connect sync account password reset

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

Description
This indicator checks if there have been any password resets against stale (i.e. not logged on within 3 days) AAD Connect 'Sync_*' accounts. Required permissions: AuditLog.Read.All, Directory.Read.All, User.Read.All, RoleManagement.Read.Directory

Likelihood of Compromise
An attacker may reset the password of a stale AAD synchronization account in order to elevate privileges or take other privileged actions.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Guest users are not restricted

IOE Found

F 0 %

SEVERITY
Informational

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Reconnaissance

Description
This indicator checks if guest users are restricted in the tenant. This option blocks guest users from performing enumeration of users and groups. Required permissions: Policy.Read.All

Likelihood of Compromise
Attackers may use unrestricted guest users to perform enumeration of users and groups in the tenant.

Result
Guest users are not restricted in this tenant.

Remediation Steps
Restrict guest users by going to User settings -> Manage external collaboration settings -> Guest user access is restricted to properties and memberships of their own directory objects (most restrictive).

SECURITY INDICATOR

Guest accounts that were inactive for more than 30 days

Pass

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Persistence
- Privilege Escalation

Description
This indicator checks for Guest accounts that have not signed in, using an interactive or non-interactive sign in, during the past 30 days. Required permissions: User.Read.All, AuditLog.Read.All

Likelihood of Compromise
Inactive Guest accounts leave an open gate to your tenant and should be addressed.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

MFA bombing attack occurred in the past day

Pass

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Initial Access

MITRE D3FEND

- Harden - Multi-factor Authentication

Description
This indicator detects MFA bombing attempts on privileged accounts by monitoring login activity to identify unusual patterns of login activity of more than 5 failed MFA attempts within the last day. Note that this indicator will not detect activity of users using passwordless authentication. Required permissions: AuditLog.Read.All, Directory.Read.All, RoleManagement.Read.All

Likelihood of Compromise
MFA bombing is a tactic where an attacker spams the user with MFA requests and the user unknowingly or unwillingly accepts the request. MFA bombing attacks can be successful in certain cases, particularly if the system's MFA protections are not configured properly or are not robust enough to withstand a high volume of login attempts.

Result

No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Number Matching Enabled in MFA

Pass

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Initial Access

MITRE D3FEND

- Harden - Multi-factor Authentication

Description
This indicator checks if number matching is enabled on MFA Microsoft Authentication

Likelihood of Compromise
When number matching is not enabled on MFA, users are prone to MFA bombing attacks. MFA bombing is a tactic where an attacker spams the user with MFA requests and the user unknowingly or unwillingly accepts the request.

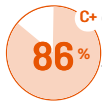
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

More than 5 Global Administrators exist

IOE Found



SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

Description
This indicator checks for the presence of 5 or more Global Administrators. Required permissions: RoleManagement.Read.Directory, PrivilegedAccess.Read.AzureAD, Directory.Read.All

Likelihood of Compromise
Global Administrators control your Azure AD environment have access to all administrative features and have full control of Azure AD; therefore, if even of them is compromised your entire AAD is compromised. Because of that it's best to keep the attack surface low.

Result
Found 6 Global Administrators in Azure AD

AzureUPN	AzureID	AssignmentType	Ignored
sayasmito@thecybersecuritycrew.au	8754dfd4-06f4-4c03-bd59-2aada5906c66	Active	False
kevin@thecybersecuritycrew.au	494c2bab-2143-4d5e-869f-66af06c76b49	Active	False
lachy@thecybersecuritycrew.au	22eef5d8-d8f0-4c9a-b866-04a89f9ce176	Active	False
neil@thecybersecuritycrew.au	073fd85d-ad8b-4d46-99a0-0eacdaaa4575	Active	False
david@thecybersecuritycrew.au	aadbf45b-729a-4ee5-848a-79c40ab7cbac	Active	False
svc-automation@thecybersecuritycrew.au	b3305858-e759-4e3c-bf09-df2bb8292233	Active	False

Showing 6 of 6

Remediation Steps
As a best practice, Microsoft recommends assigning the Global Administrator role to no more than five people in the organization.

Microsoft also recommends that you keep two "break glass" accounts that are permanently assigned the Global Administrator role. The "break glass" account's password are divided into at least two parts. Ensure that the "break glass" accounts do not use the same MFA mechanism as a normal administrator.

SECURITY INDICATOR

Conditional Access Policy does not require MFA on privileged accounts Pass

SEVERITY
Warning

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Credential Access

Description
This indicator checks whether Conditional Access policies require mutli-factor authentication (MFA) for privileged accounts. Required permissions: Policy.Read.All

Likelihood of Compromise
Attackers might take advantage of compromised privileged accounts to compromise the entire tenant. Requiring MFA on privileged accounts strengthens the tenant security to ensure privileged accounts identify themselves by having to provide more than their username and password.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Conditional Access Policy that does not require MFA when sign-in risk has been identified IOE Found

SEVERITY
Warning

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Credential Access

Description
This indicator checks whether a conditional access policy exists that requires MFA if the authentication request risk is medium or high as determined by the Azure AD Identity Protection sign-in risk API. Required permissions: Policy.Read.All

Likelihood of Compromise
A high or medium sign-in risk represents a high or medium probability that an authentication request wasn't authorized by the identity owner. Sign-in risk is identified by Azure.

Result
There are no Conditional Access Policies configured to require MFA if sign-in risk is detected to be medium or high.

Remediation Steps
To protect the authentication process, it is recommended to require MFA if the sign-in risk is detected to be medium or high through conditional access policies. Follow this documentation by Microsoft to add this conditional access policy

SECURITY INDICATOR

Conditional Access Policy that does not require a password change from high risk users IOE Found

SEVERITY
Warning

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Credential Access

Description

This indicator checks whether a conditional access policy exists that requires password change from users determined to be high risk by the Azure AD Identity Protection user risk API. Required permissions: Policy.Read.All

Likelihood of Compromise
A high user risk represents a high probability of an account having being compromised, as identified by Azure.

Result
There isn't a Conditional Access Policy configured that requires a password change for high risk users.

Remediation Steps
To protect the authentication process, it is recommended to require a password change for high risk users through conditional access policies or security defaults. Follow this documentation by Microsoft to add this conditional access policy

SECURITY INDICATOR

AAD custom Roles with risky permissions

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Credential Access

Description
This indicator checks if a custom role has permissions that can be abused by an attacker that possess them. Read more in the blog here

Likelihood of Compromise
Custom roles with risky permissions can be abused by attackers in various ways depending on the specific permission that was granted. Potentially, custom roles can be used to gain access to sensitive information or perform malicious actions. Read more in the blog here

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Security questions are in use

Pass

A+ 100%

SEVERITY
Informational

WEIGHT
2

Security Frameworks
MITRE ATT&CK

- Credential Access
- Initial Access

MITRE D3FEND

- Harden - Strong Password Policy

Description
This indicator checks if security questions are in use. Required permissions: Reports.Read.All

Likelihood of Compromise
Using security questions as the only method of confirming someone's identity when resetting a password is less secure and makes it easier for an attacker to perform password guessing attacks.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Guest invites not accepted in last 30 day

Pass

A+ 100%

SEVERITY
Informational

WEIGHT
2

Security Frameworks
MITRE ATT&CK

- Persistence
- Initial Access

Description
This indicator checks for Guest invites that were not accepted within 30 days of the invitation. Required permissions: User.Read.All

Likelihood of Compromise
Stale Guest invitations pose a security risk and should be addressed. Stale Guest invitations have been the cause of multiple attacks. One such attack was due to an Azure AD tenant that was prone to an invite hijacking attack, which has now have been fixed by Microsoft.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Suspicious Directory Synchronization Accounts role member

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

Description
This indicator checks for users that are assigned the Directory Synchronization Accounts role that are not the default Azure AD Connect users. Required permissions: User.Read.All,RoleManagement.Read.Directory

Likelihood of Compromise
The Directory Synchronization Accounts role allows users to perform directory synchronization tasks.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Users are not using their privileged roles

Pass

A+ 100%

SEVERITY
Informational

WEIGHT
2

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Harden - User Account Permissions

Description
This indicator checks for users who have not activated their role for over 30 days. Please note: For users eligible via group membership, audit log retention may prevent gathering an accurate 'EligibleSince' date. Required permissions:RoleEligibilitySchedule.Read.Directory, GroupMember.Read.All, Directory.Read.All

Likelihood of Compromise
Granting excessive privileges to users who do not actually need them significantly raises the likelihood of a successful attack. Moreover, dormant or inactive user accounts create an ideal environment for attackers to operate covertly and avoid detection.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Users can create security groups

IOE Found

F 0 %

SEVERITY
Informational

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Persistence
- Privilege Escalation

MITRE D3FEND

- Model - Access Modeling

Description
This indicator checks if normal users can create security groups. Required permissions: Policy.Read.All

Likelihood of Compromise
Users should not be allowed to create security groups. This is enabled by default in Azure AD and should be disabled.

Result
Any user can create security groups

Remediation Steps
To enhance security practices, it is advisable to disable the feature that allows users to create security groups in Azure AD. Follow these steps to disable the setting:

Open the Azure Active Directory portal.
Navigate to the "Groups" section.
Access the "General" settings associated with groups.
Locate the option labeled "Users can create security groups in Azure portals, API, or PowerShell."
Switch the option to "No" to deactivate users' ability to create security groups.
It is important to note that if users require the ability to create security groups, they should be assigned a valid role that grants them the necessary permissions. Disabling this option does not impact the ability to create Microsoft 365 (M365) groups, which possess distinct permissions and functionalities.
Implementing this change contributes to a more secure and organized Azure AD environment, reducing the potential risks associated with unauthorized group creations and potential security vulnerabilities.

SECURITY INDICATOR

Non-admin users can create tenants

IOE Found

F 0 %

SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Initial Access
- Persistence
- Privilege Escalation

MITRE D3FEND

- Model - Access Modeling

Description
This indicator checks for an authorization policy that enables non-admin users to create Azure AD tenants. Required permissions: Policy.Read.All

Likelihood of Compromise
Badly configured Azure AD tenants that are linked to users from the parent (organization) tenant, may be compromised more easily and won't be well monitored and secured.

Result
Non-admin users are able to create Azure AD tenants

Remediation Steps
To ensure better security practices, it is highly recommended to disable the setting that allows non-admin users to create Azure AD tenants. Follow these steps to restrict non-admin users from creating tenants:

Navigate to the Azure Active Directory portal.
Navigate to the "User settings" section.
Find the "Tenant creation" option.
Select "Yes" from the available options to disable users' ability to create Azure AD tenants.
By following these steps, you restrict the creation of Azure AD tenants to the global administrator or tenant creator roles. This helps to ensure tighter control over tenant creation and reduces the risk of unauthorized access or potential security vulnerabilities.

SECURITY INDICATOR

Non-admin users can register custom applications

IOE Found

SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Persistence
- Privilege Escalation

Description
This indicator checks if there exists an authorization policy that enables non-admin users to register custom applications. Required permissions: Policy.Read.All

Likelihood of Compromise
Allowing users to register custom-developed enterprise applications may be used by attackers to register nefarious applications. This can be leveraged, for example, to promote a user to give the attacker's application permissions, or an admin to give it higher permissions only admins can grant.

Result
Every user can register an application

Remediation Steps
It is recommended to disable this setting by going to AAD -> User settings -> App Registrations:Users can register application applications -> and select "No" from the options.

Notes

Appendix 2 - Scoring method

How do we determine the tests' score

The risk scores included in this report reveal the security posture of the Active Directory environment that was assessed. Risk scores are represented by percentage and letter grade. It is recommended to aim for the highest score possible; a 100% (A+) risk score indicates that there were no Indicators of Exposure (IOEs) found for the security indicators that were assessed. The following explanation is intended to help you understand the scoring methodology and factors used to calculate the risk scores presented in this report.

Risk scores:

The Security Assessment report provides the following risk scores:

- Security Indicator risk score: Each individual security indicator evaluated is assigned a score according to its internal logic and the relative number of results found. The individual security indicator score is assigned a weight (value between 1-10) according to the risk of the IOE found and the likelihood of compromise. This weighted score, together with a general factor of the industry risk, affects the score assigned to the relevant category.
- Category risk score:The security indicators included in the tool cover a range of categories that represent different aspects of Active Directory security posture. The category risk score is based on the test results and severity of each individual security indicator that was evaluated within the relevant category.
- Overall risk score: The overall risk score is derived from a weighted average of all indicator results, which are aggregated according to their respective severity levels.

NOTE: When calculating the risk scores, only security indicators and categories included in the assessment are included (e.g., security indicators that passed and resulting in IOEs found). Security indicators that were not selected, cancelled, or failed to run are not taken into account. For an accurate assessment, it is recommended that you include all security indicators and all domains in the selected forest.

Scoring methods/factors:

Letter grading: Each score is assigned a suitable letter grade according to the following table:

A+ 100	A 99	A- 98	B+ 96-97	B 93-95
B- 90-92	C+ 86-89	C 81-85	C- 75-80	D+ 67-74
D 58-66	D- 44-57	F 0-43		

Risk factors: To determine the risk level of a particular security indicator, the following factors are taken into consideration:

- Severity (Informational, Warning, Critical)
- Likelihood of compromise
- The DREAD Threat Probability Matrix

DREAD Threat Probability Matrix

DREAD		High(3)	Medium(2)	Low(1)
Damage potential	How bad would the attack be?	Significant damage: The attacker can subvert the security system and gain full trust authorization.	Moderate damage: The attacker can access/leak sensitive information.	Minimal damage: The attacker can only access/leak trivial information.
Reproducibility	How easy would it be to recreate the attack?	The attack can be consistently reproduced and does not require a specific timing window.	The attack can be reproduced, but only within a specific timing window and in a particular sequence.	The attack is very difficult to reproduce, even with knowledge of the security weakness/vulnerability.
Exploitability	How easy would it be to launch the attack?	A novice programmer could perform the attack with minimal effort.	Requires a skilled programmer to launch the attack and be able to repeat the steps.	Requires an extremely skilled programmer with in-depth knowledge to launch an attack.
Affected users	How many users would be impacted?	A large percentage or all users are impacted; default configuration and key customers are impacted.	A moderate percentage of users are impacted; non-default configuration is impacted.	A very small percentage of users are impacted; anonymous users are affected
Discoverability	How easy would it be for the attacker to discover this exposure?	Easily discovered. Published information explains the vulnerability and attack technique. The vulnerability is found in commonly used features and is very noticeable.	Would require some effort to discover and successfully exploit. The vulnerability is found in a seldomly-used part of the product and only a few users should discover it	Hard to discover. The issue is obscure, and it is unlikely that users would discover a way to cause damage.

Notes