



# Martin Haller

## Microsoft Entra ID Defense

# Entra ID: Defense

# How we got here?

- » Goals of attack (monetization)
- » Entra ID: Attack surface
- » Entra ID: Lateral movement & persistence

# Where to start?

- » Actual and future threats
- » Research of others
  - » <https://www.cisa.gov/>
  - » <https://www.purple-knight.com/security-indicators/>
  - » <https://www.pingcastle.com/>
  - » <https://cyberdom.blog/2022/11/09/cloud-misconfiguration-risks-azure/>

# Main ingredients

- » Hardening (attack surface reduction)
- » Monitoring
- » Backup
- » KISS (Keep It Simple, Stupid)
- » Step by step

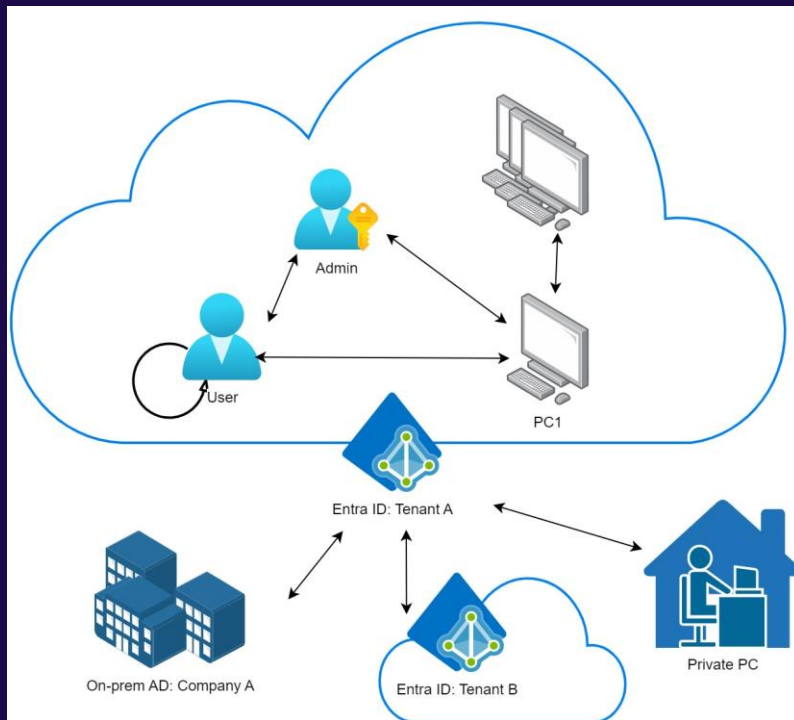
# Context

Company with up to 1.000 seats and small internal IT department.

# Entra ID: Hardening

# Privileged accounts

- » Never use hybrid accounts (synchronized between Entra ID and AD)
- » Separated regular and privileged accounts
- » Protect Azure AD Connect server (?Entra ID Connect?)



<input type="checkbox"/>	Display name ↑	User principal name ↑↓	User type	On-premises sy...
<input type="checkbox"/>	___VMware_Conv_SA___	___VMware_Conv_SA___@...	Member	Yes



# Native apps

- » Microsoft Authenticator (Passwordless, Push, higher security)
- » Microsoft Outlook (Purview, MAM, easier support, more functionality)
- » Microsoft 365 Mobile App

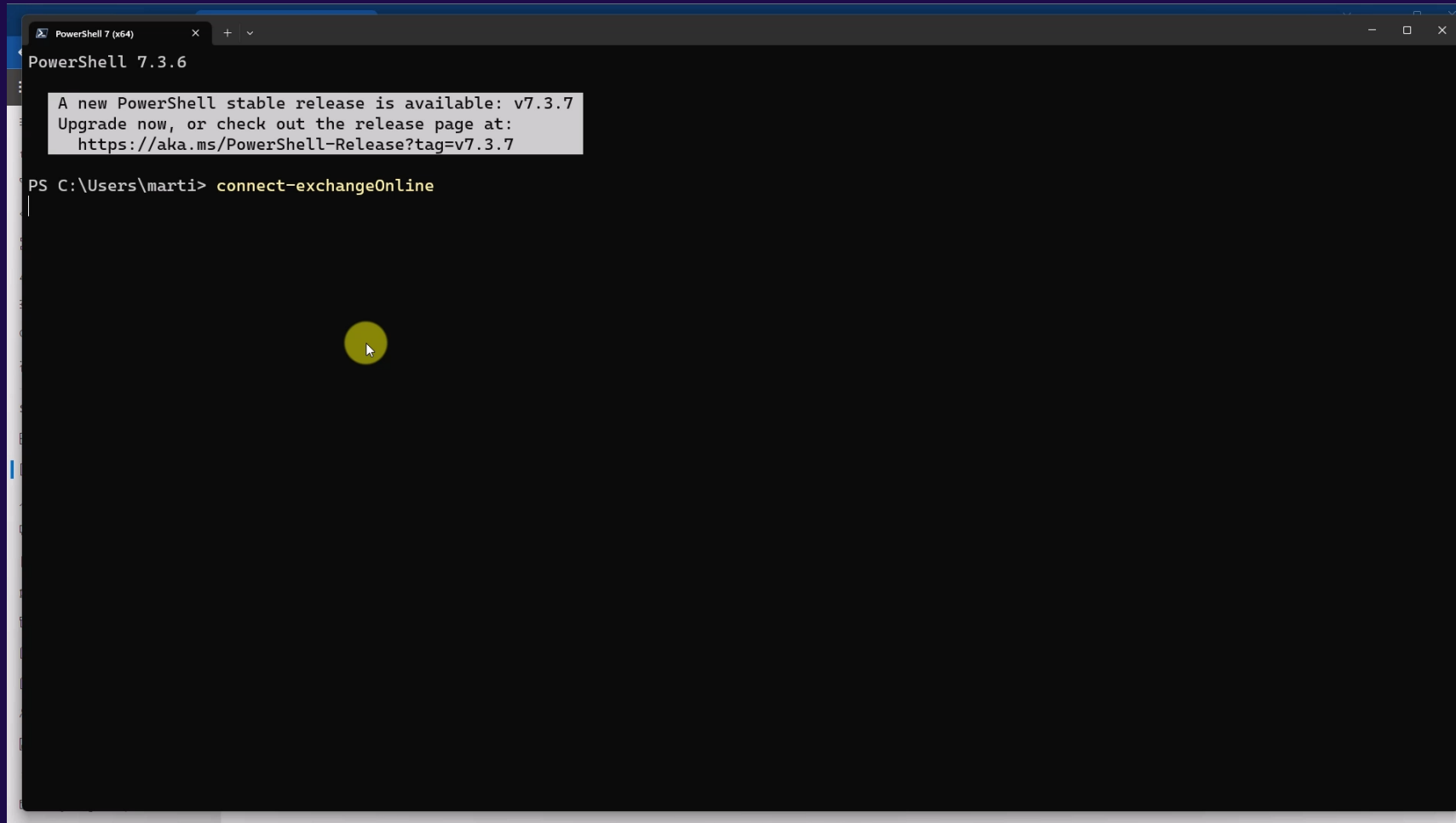
# Easy configuration

- » Limit Entra ID Join
- » Limit App Registration
- » Limit App Consent
- » Limit Group Creation
- » Limit Entra ID portal for users
- » Limit Guests Invitations
- » Limit Guests Visibility

# Other configuration

- » Exchange External Tag
- » Self-serve password reset portal (disable for admins)
- » Authentication methods
- » Unified audit logging

# DEMO: Hardening



# Entra ID: Conditional Access

## Grant ✕

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

- Require multifactor authentication ⓘ
- Require authentication strength ⓘ
- Require device to be marked as compliant ⓘ
- Require Hybrid Microsoft Entra joined device ⓘ
- Require approved client app ⓘ  
[See list of approved client apps](#)
- Require app protection policy ⓘ  
[See list of policy protected client apps](#)
- Require password change ⓘ

For multiple controls

Require all the selected controls

Require one of the selected controls

## Session ✕

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

Use app enforced restrictions ⓘ

**i** This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. [Learn more](#)

- Use Conditional Access App Control ⓘ
- Sign-in frequency ⓘ
- Persistent browser session ⓘ
- Customize continuous access evaluation ⓘ
- Disable resilience defaults ⓘ
- Require token protection for sign-in sessions (Preview) ⓘ

# Conditional Access (CA)

- » Under which conditions you can access apps
- » Security defaults vs. CA
- » Default allow
- » Not everything can be set as requirement
- » All policies are being evaluated
- » Azure App Web Proxy
- » Guest access and MFA
- » How many CA policies is limit?
- » Authentication strength

Multifactor authentication	Built-in	Windows Hello For Business and 16 more
Passwordless MFA	Built-in	Windows Hello For Business and 3 more
Phishing-resistant MFA	Built-in	Windows Hello For Business and 2 more

# Conditional Access - essentials

## » Global rules:

- » Block legacy authentication
- » **Recommended:**
  - » Register Security information: MFA or trusted network
  - » Register or join devices: MFA

## » Privileged users

- » No persistent session, signing frequency
- » **Recommended:** FIDO2, trusted network

## » Users

- » Start: MFA, Hybrid Joined Device or Compliant device
- » **Recommended:** MFA (on company devices WHfB)
- » No persistent session



# Conditional Access – tiering?

- » **Public:** BYOD (MAM)
- » **Restricted:** Enterprise devices (Intune/GPO, EDR)
- » **Confidential:** Subset of Enterprise devices (stricter configuration)
- » **Special:**
  - » VPN: sign-in frequency
  - » RDP



# DEMO: Conditional Access

The screenshot shows the Microsoft Entra admin center interface. The main content area is titled 'Conditional Access | Policies' and displays a list of 6 policies. The policies are as follows:

Policy Name	State	Creation Date	Modified Date
BASE: Block legacy authentication	On	9/24/2023, 4:59:19 PM	9/24/2023, 4:59:46 PM
BASE: Securing security info registration	On	9/24/2023, 5:00:08 PM	9/24/2023, 5:00:56 PM
BASE: Secure device registration or join	On	9/24/2023, 5:03:36 PM	
BASE: Require MFA and sign-in freq for admins	On	9/24/2023, 5:04:50 PM	9/24/2023, 5:05:48 PM
BASE: Require compliant or hybrid Azure AD joined device or multifactor authentication for all users	On	9/24/2023, 5:06:29 PM	9/24/2023, 5:07:15 PM
BASE: No persistent session	On	9/24/2023, 5:07:51 PM	

# Entra ID: Monitoring

# Monitoring - essentials

## » Risky users

### User risk detections

Risk detection	Detection type	Type
Possible attempt to access Primary Refresh Token (PRT)	Offline	Premium
Anomalous user activity	Offline	Premium
User reported suspicious activity	Offline	Premium
Additional risk detected	Real-time or Offline	Nonpremium
Leaked credentials	Offline	Nonpremium
Microsoft Entra threat intelligence	Offline	Nonpremium

Zdroj: <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#additional-risk-detected-sign-in>

# Monitoring

- » Risky users
- » Risky sign-ins

Zdroj: <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#additional-risk-detected-sign-in>

## Sign-in risk detections

Risk detection	Detection type	Type
Atypical travel	Offline	Premium
Anomalous Token	Offline	Premium
Token Issuer Anomaly	Offline	Premium
Malware linked IP address	Offline	Premium <b>This detection has been deprecated.</b>
Suspicious browser	Offline	Premium
Unfamiliar sign-in properties	Real-time	Premium
Malicious IP address	Offline	Premium
Suspicious inbox manipulation rules	Offline	Premium
Password spray	Offline	Premium
Impossible travel	Offline	Premium
New country	Offline	Premium
Activity from anonymous IP address	Offline	Premium
Suspicious inbox forwarding	Offline	Premium
Mass Access to Sensitive Files	Offline	Premium
Verified threat actor IP	Real-time	Premium
Additional risk detected	Real-time or Offline	Nonpremium
Anonymous IP address	Real-time	Nonpremium
Admin confirmed user compromised	Offline	Nonpremium
Microsoft Entra threat intelligence	Real-time or Offline	Nonpremium

# Monitoring - essentials

- » Risky users
- » Risky sign-ins
- » Defender alerts

The screenshot displays the Microsoft 365 Defender interface. At the top, there is a search bar and the text 'Microsoft 365 Defender'. The main heading is 'Incidents'. Below this, there is a section for 'Most recent incidents and alerts' with an 'Export' button. A table lists the incidents:

<input type="checkbox"/>		Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets
<input type="checkbox"/>	>	Executable content from email blocked on one ...	36		Low	Initial access		AAD-PC-947 PATRON-
<input type="checkbox"/>	>	Executable content from email blocked on one ...	35		Low	Initial access		aad-pc-009 PATRON-

# Monitoring - logs

## » Azure AD Audit Log

- » Contains: changes done in Entra ID
- » Retention: Free = 7 days, P1 = 30 days
- » [https://entra.microsoft.com/#view/Microsoft\\_AAD\\_IAM/AuditEventsV2PillsBlade](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuditEventsV2PillsBlade)

## » Azure AD Sign-in Log

- » Contains: sign-ins to M365
- » Retention: Free = 7 days, P1 = 30 days
- » [https://entra.microsoft.com/#view/Microsoft\\_AAD\\_IAM/SignInEventsV3Blade](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/SignInEventsV3Blade)

## » Office 365 Unified Access Log (Microsoft Purview Audit)

- » Not enabled by default.
- » Retention: Free = 90 days ([180 days](#)), E5 = 1 year
- » <https://compliance.microsoft.com/auditlogsearch>

## » Log Analytics / Sentinel

## » [Everything you wanted to know about Security and Audit Logging in Office 365](#)

# DEMO: Sign-in logs

The screenshot displays the Microsoft Entra admin center interface. The left sidebar shows navigation options like Home, Favorites, Identity, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, Monitoring & health, Sign-in logs, Audit logs, Provisioning logs, and Learn & support. The main content area is titled 'Sign-in events' and includes a search bar with filters for 'Date: Last 24 hours', 'Show dates as: Local', and 'Username contains: diego.s@mhlab.cz'. Below the search bar, there are tabs for 'User sign-ins (interactive)', 'User sign-ins (non-interactive)', 'Service principal sign-ins', and 'Managed identity sign-ins'. A table of sign-in events is shown with columns for Date, Request ID, User, Application, Status, and IP address. The table contains four rows of data for user Diego Siciliani. A yellow circle highlights the 'Status' column in the table. On the right, a 'Activity Details: Sign-ins' pane is open, showing 'Basic info' for a specific sign-in event. This pane includes fields for Date, Request ID, Correlation ID, Authentication requirement, Status, Continuous access evaluation, and Additional Details. It also provides a 'Troubleshoot Event' section with a 'Launch the Sign-in Diagnostic' link and a list of steps to follow. The bottom of the pane shows user information such as User, Username, User ID, Sign-in identifier, User type, Cross tenant access type, Application, Application ID, Resource, Resource ID, Resource tenant ID, Home tenant ID, Home tenant name, Client app, and Client credential type.

Date	Request ID	User	Application	Status	IP address
9/24/2023, 5:21:23 PM	ea319dd-0b5f-487c...	Diego Siciliani	Office365 Shell WCS...	Success	95.82.15
9/24/2023, 5:21:23 PM	cc0fbfb-76ee-4394...	Diego Siciliani	Office365 Shell WCS...	Success	95.82.15
9/24/2023, 5:21:23 PM	ca698c0b-c6e3-4121...	Diego Siciliani	Office365 Shell WCS...	Success	95.82.15
9/24/2023, 5:21:18 PM	c98b8ab8-1e7e-423...	Diego Siciliani	OfficeHome	Success	95.82.15

**Activity Details: Sign-ins**

**Basic info** Location Device info Authentication Details Conditional Access Report-only

Date: 9/24/2023, 5:21:18 PM  
Request ID: c98b8ab8-1e7e-4237-a11f-4c5fee322000  
Correlation ID: b1d64528-5b31-4397-91ea-ff4a92fa827  
Authentication requirement: Multifactor authentication  
Status: Success  
Continuous access evaluation: No  
Additional Details: MFA completed in Azure AD

Follow these steps:

Troubleshoot Event: [Launch the Sign-in Diagnostic](#)

1. Review the diagnosis and act on suggested fixes.

User: Diego Siciliani  
Username: diego.s@mhlab.cz  
User ID: 916e4a09-21bd-47d0-b5f3-f3a526931d67  
Sign-in identifier: diego.s@mhlab.cz  
User type: Member  
Cross tenant access type: None  
Application: OfficeHome  
Application ID: 4765445b-32c6-49b0-83e6-1d93765276ca  
Resource: OfficeHome  
Resource ID: 4765445b-32c6-49b0-83e6-1d93765276ca  
Resource tenant ID: 06cc7d68-ad59-4943-958e-c5f5b80baf53  
Home tenant ID: 06cc7d68-ad59-4943-958e-c5f5b80baf53  
Home tenant name:  
Client app: Browser  
Client credential type: None

Další čtení: <https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>



- Protection
- Identity governance
- External Identities
- User experiences
- Hybrid management
- Monitoring & health
- Sign-in logs
- Audit logs**
- Provisioning logs
- Health (Preview)
- Log Analytics
- Diagnostic settings
- Workbooks
- Usage & insights
- Learn & support

Home >

# Audit Logs

Download Export Data Settings Refresh Columns Got feedback?

Date : Last 24 hours Show dates as : Local Service : All Category : All Activity : All Add filters

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated
9/4/2023, 3:55:57 PM	Core Directory	DirectoryManagement	Set Company Inform...	Success		MHLab	adm-lh@
9/4/2023, 3:55:33 PM	Authentication Meth...	ApplicationManage...	Authentication Meth...	Success	NoContent	Authentication Meth...	Lidia Holl
9/4/2023, 3:55:33 PM	Core Directory	Policy	Update policy	Success		Default User Credent...	Azure Cre
9/4/2023, 3:52:08 PM	Core Directory	DirectoryManagement	Set Company Inform...	Success		MHLab	adm-lh@
9/4/2023, 3:52:03 PM	Authentication Meth...	ApplicationManage...	Authentication Meth...	Success	NoContent	Authentication Meth...	Lidia Holl
9/4/2023, 3:52:03 PM	Core Directory	Policy	Update policy	Success		Default User Credent...	Azure Cre
9/4/2023, 3:43:19 PM	Authentication Meth...	ApplicationManage...	Authentication Meth...	Success	NoContent	Authentication Meth...	Lidia Holl
9/4/2023, 3:43:19 PM	Core Directory	Policy	Update policy	Success		Default User Credent...	Azure Cre
9/4/2023, 2:36:35 PM	Core Directory	DirectoryManagement	Set Company Inform...	Success		MHLab	adm-lh@
9/4/2023, 2:36:09 PM	Authentication Meth...	ApplicationManage...	Authentication Meth...	Success	NoContent	Authentication Meth...	Lidia Holl
9/4/2023, 2:36:09 PM	Core Directory	Policy	Update policy	Success		Default User Credent...	Azure Cre
9/4/2023, 2:08:19 PM	Self-service Passwor...	UserManagement	Change password (s...	Success	None	Lidia Holloway (ADM)	adm-lh@
9/4/2023, 2:08:19 PM	Core Directory	UserManagement	Update StsRefreshTo...	Success		adm-lh@mhlab.cz	adm-lh@

# Monitoring – what to search for in logs

- » Privileged groups/roles
- » Break glass admin use
- » GDAP / DAP
- » Consent to apps
- » Application permissions changes
- » Application secrets modification
- » Changes in authentication methods
- » Use of TAP (temporary access password)
- » Changes in trusted CA
- » Changes in PTA (AAD Connect)
- » Cross tenant sync
- » Changes in mail flow
- » Mass changes/deletions
- » Hunting (apps, user agent, not passing MFA, used countries)

# Auditování

- » Configuration revision
- » Not used accounts (guests)
- » Tools:
  - » <https://github.com/cisagov/ScubaGear>
  - » <https://www.pingcastle.com/>
  - » <https://www.purple-knight.com/>

« [+ Add authentication method](#) | [Reset password](#) | [Require re-register multifactor authentication](#) | [Revoke multifactor authentication sessions](#) | [View authentication methods policy](#) | [Got feedback?](#)

**i** Want to switch back to the old user authentication methods experience? [Click here to go back.](#) →

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. [Learn more](#)

Default sign-in method (Preview) ⓘ      Microsoft Authenticator notification ✎

### Usable authentication methods

Authentication method	Detail	
FIDO2 security key	MH - Kensington C	...
FIDO2 security key	MH - YubiKey BIO C	...
Windows Hello for Business		...
Windows Hello for Business	NB-MH2	...
Microsoft Authenticator	iPhone	...
Microsoft Authenticator	iPhone 12 Pro	...
















### Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

### System preferred multifactor authentication method

Feature status	System preferred MFA method
Disabled	N/A

73 devices found

<input type="checkbox"/>	Name <span>↓</span>	Enabled	OS	Version	Join type	Owner	MDM	Compliant	Registered <span>↓</span>	Activity <span>↑</span>
<input type="checkbox"/>	 BLACK	<span>❌</span> No	Windows	10.0.18363.0	Azure AD registered		None	N/A	8/6/2020, 1:41 PM	4/10/2022, 1:
<input type="checkbox"/>	 DESKTOP-G5MP43G	<span>✅</span> Yes	Windows	10.0.19044.1706	Azure AD registered		None	N/A	5/28/2022, 8:54 AM	5/28/2022, 8:
<input type="checkbox"/>	 NUC-2	<span>✅</span> Yes	Windows	10.0.18363.0	Azure AD registered		None	N/A	5/2/2019, 1:09 PM	7/18/2022, 8:
<input type="checkbox"/>	 PC-01	<span>✅</span> Yes	Windows	10.0.19042.1826	Azure AD registered		None	N/A	9/1/2022, 9:34 AM	9/15/2022, 4:
<input type="checkbox"/>	 NUC-7	<span>✅</span> Yes	Windows	10.0.16299.0	Azure AD registered		None	N/A	9/24/2018, 8:28 AM	10/18/2022,
<input type="checkbox"/>	 DESKTOP-H8MNQ6E	<span>✅</span> Yes	Windows	10.0.17134.0	Azure AD registered		None	N/A	11/11/2018, 10:14 AM	11/7/2022, 8:
<input type="checkbox"/>	 DESKTOP-I8T5KIL	<span>✅</span> Yes	Windows	10.0.19044.1586	Azure AD registered		None	N/A	3/15/2022, 2:59 PM	11/30/2022,
<input type="checkbox"/>	 LAPTOP-GEEJOBIS	<span>✅</span> Yes	Windows	10.0.18362.0	Azure AD registered		None	N/A	12/26/2019, 10:07 AM	12/7/2022, 5:
<input type="checkbox"/>	 AAD-WIN11-B	<span>✅</span> Yes	Windows	10.0.22621.963	Azure AD joined		None	<span>❌</span> No	2/15/2023, 3:40 PM	2/15/2023, 3:
<input type="checkbox"/>	 NUC-3	<span>✅</span> Yes	Windows	10.0.16299.0	Azure AD registered		None	N/A	3/27/2018, 1:48 PM	3/20/2023, 1:
<input type="checkbox"/>	 PC-WIN11-B2	<span>✅</span> Yes	Windows	10.0.22621.963	Azure AD joined		Microsoft Intune	<span>❌</span> No	2/15/2023, 4:28 PM	3/28/2023, 3:
<input type="checkbox"/>	 iPhone 11	<span>✅</span> Yes	iOS	16.4.1	Azure AD registered		None	N/A	12/16/2019, 9:30 AM	3/31/2023, 8:
<input type="checkbox"/>	 NUC-1	<span>✅</span> Yes	Windows	10.0.19044.1889	Azure AD registered		None	<span>❌</span> No	9/13/2022, 10:30 AM	4/1/2023, 4:5
<input type="checkbox"/>	 PC-06	<span>❌</span> No	Windows	10.0.19042.867	Azure AD registered		None	N/A	4/1/2021, 8:46 AM	4/4/2023, 8:2
<input type="checkbox"/>	 PC-WIN-11	<span>✅</span> Yes	Windows	10.0.22000.1696	Azure AD joined		Microsoft Intune	N/A	4/4/2023, 10:51 AM	4/4/2023, 10:

# Number of applications in tenant?

Search by application name or object ID + Add filter

188 applications found

Name	↑↓
<b>MI</b> Microsoft Intune API	
<b>MT</b> MS Teams Griffin Assistant	
<b>SW</b> Sway	
<b>MI</b> Microsoft Information Protection API	
<b>MC</b> Microsoft Cloud App Security	

Search by application name or object ID + Add filters

808 applications found

Name	↑↓
<b>SF</b> Skype For Business Entitlement	
<b>FS</b> Fiji Storage Backend	
<b>MA</b> Microsoft Azure Alerts Management	
<b>A</b> AutoCAD Mobile	
<b>MA</b> Microsoft Azure App Service	



Light Mode



# SCuBA M365 Security Baseline Conformance Reports

Tenant Display Name	Tenant Domain Name	Tenant ID	Report Date
MHLab	47pqby.onmicrosoft.com	06cc7d68-ad59-4943-958e-c5f5b80baf53	09/20/2023 03:34:41 Pacific Daylight Time

Baseline Conformance Reports	Details			
<a href="#">Azure Active Directory</a>	3 tests passed	4 warnings	15 tests failed	8 manual checks needed
<a href="#">Microsoft 365 Defender</a>	38 tests passed	16 warnings	25 tests failed	5 manual checks needed
<a href="#">Exchange Online</a>	7 tests passed	2 warnings	5 tests failed	23 manual checks needed
<a href="#">OneDrive for Business</a>	1 tests passed	3 warnings	1 test failed	2 manual checks needed
<a href="#">SharePoint Online</a>	1 tests passed	3 warnings	1 test failed	2 manual checks needed
<a href="#">Microsoft Teams</a>	7 tests passed	5 warnings	4 tests failed	9 manual checks needed

# Azure Active Directory Baseline Report

Note: Conditional Access (CA) Policy exclusions and additional policy conditions may limit a policy's scope more narrowly than desired. Recommend reviewing matching policies against the baseline statement to ensure a match between intent and implementation.

Tenant Display Name	Report Date	Baseline Version	Module Version
MHLab	09/20/2023 03:34:41 Pacific Daylight Time	0.1	0.3.0

## AAD 2.1 Legacy Authentication SHALL be Blocked

Requirement	Result	Criticality	Details
Legacy authentication SHALL be blocked	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. <a href="#">View all CA policies.</a>

## AAD 2.2 High Risk Users SHALL be Blocked

Requirement	Result	Criticality	Details
A notification SHOULD be sent to the administrator when high-risk users are detected	N/A	Should/Not-Implemented	Currently cannot be checked automatically. See Azure Active Directory Secure Configuration Baseline policy 2.2 for instructions on manual check
Users detected as high risk SHALL be blocked	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. <a href="#">View all CA policies.</a>

## AAD 2.3 High Risk Sign-ins SHALL be Blocked

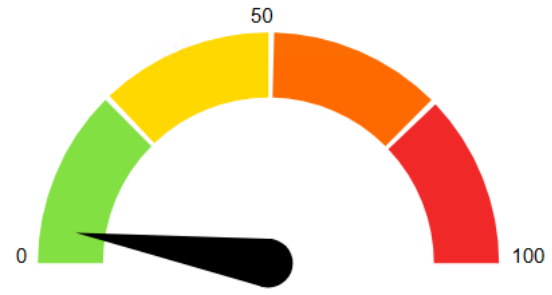
Requirement	Result	Criticality	Details
Sign-ins detected as high risk SHALL be blocked	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. <a href="#">View all CA policies.</a>





This section focuses on the core security indicators.  
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

## Indicators



Domain Risk Level: 5 / 100

It is the score computed based on the rules that matched during the analysis

## Maturity Level

This section represents the maturity score (inspired from [ANSSI](#)).  
This feature is reserved for customers who have [purchased a license](#)

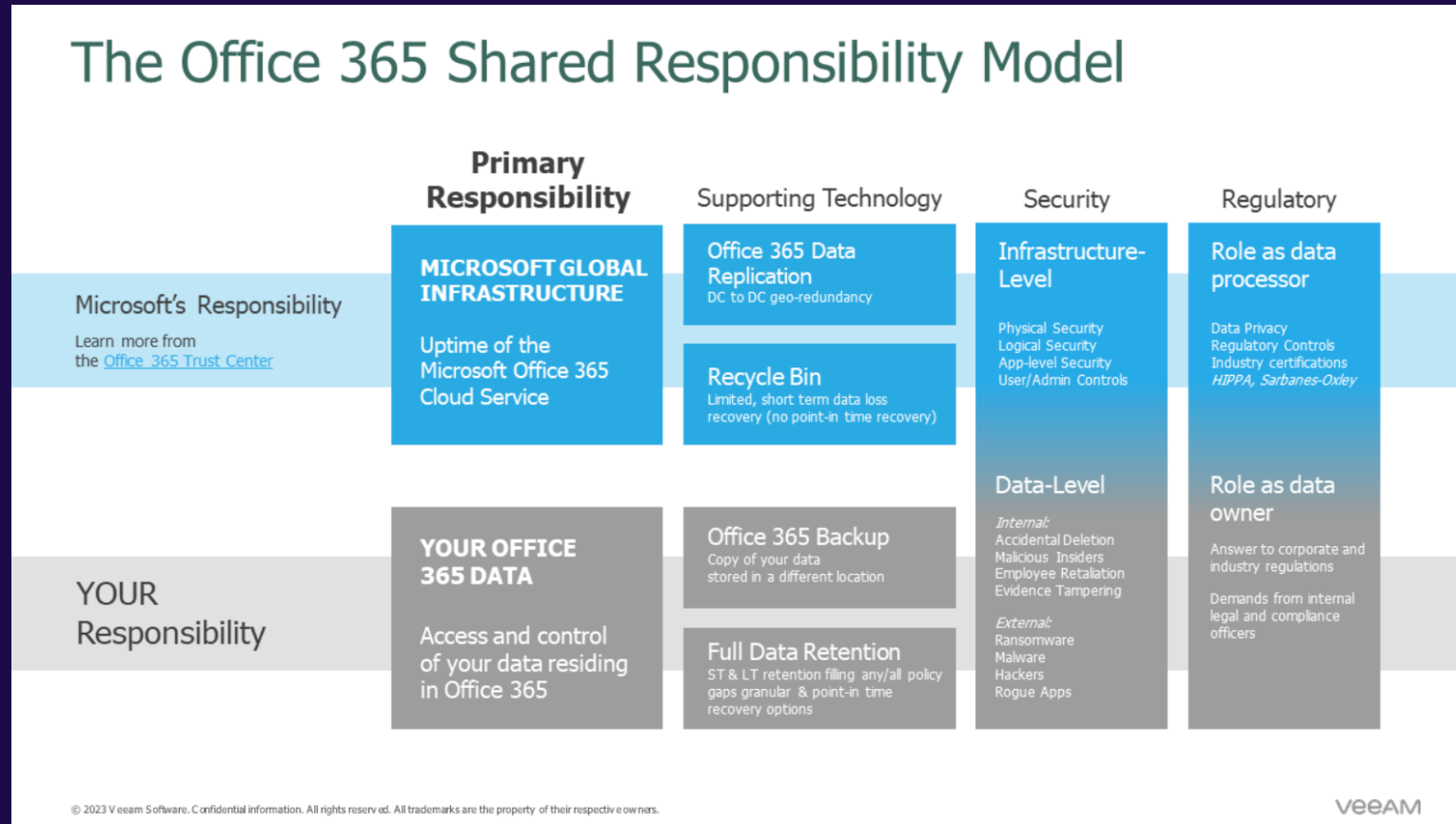
## MITRE ATT&CK®

This section represents an evaluation of the techniques available in the [MITRE ATT&CK®](#)  
This feature is reserved for customers who have [purchased a license](#)

## Rules

# Entra ID: Backup

## » Veeam Backup for Microsoft 365



Zdroj: <https://www.veeam.com/backup-microsoft-office-365.html>

# Entra ID: Implementation

# How to do it?

- » Multitenancy is the challenge?
- » Custom scripts
- » 3rd party tools (MS Lighthouse, N-able, AdminDroid)
- » Auditing tools (PingCastle, Purple Knight, Bloodhound, SCuBA)
- » Licences: Microsoft 365 Business Premium (20,6 EUR/month)
  - » Office Apps,
  - » Exchange, Sharepoint, OneDrive, ?Teams,
  - » Entra ID P1,
  - » Intune,
  - » Defender Business,
  - » Azure Information Protection

# In case of account compromise

- » Disable sign-in
- » Revoke sessions
- » Check authentication methods for the user
- » Reset password
- » Inspect audit logs
- » Enable sign-in

# Keep on working

- » Extending hardening and monitoring
- » Observation of trends in attacks
- » Defender for \*
- » Intune (LAPS, Baselines, Applocker, WHfB)
- » Azure resources

# Summary



# Summary

- » Audit
- » Hardening
- » Monitoring
- » Backup
- » KISS!! Small steps!
- » Keep learning

# Other resources

# Other resources

- » <https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project>
- » <https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model>
- » <https://aadinternals.com/aadkillchain/>
- » <https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project>
- » <https://www.huntress.com/blog/legitimate-apps-as-traitorware-for-persistent-microsoft-365-compromise>
- » <https://github.com/WillOram/AzureAD-incident-response/blob/main/README-OFFENSIVETECHNIQUES.md>
- » [https://github.com/hevnsnt/Awesome\\_Incident\\_Response](https://github.com/hevnsnt/Awesome_Incident_Response)
- » <https://learn.microsoft.com/en-us/security/operations/token-theft-playbook>
- » <https://call4cloud.nl/2021/08/the-battle-between-aadj-and-aadr/>



Thank **<YOU>**