# Today
# Live from Deadwood
# *by*

TEMS SECURITY SERVICES

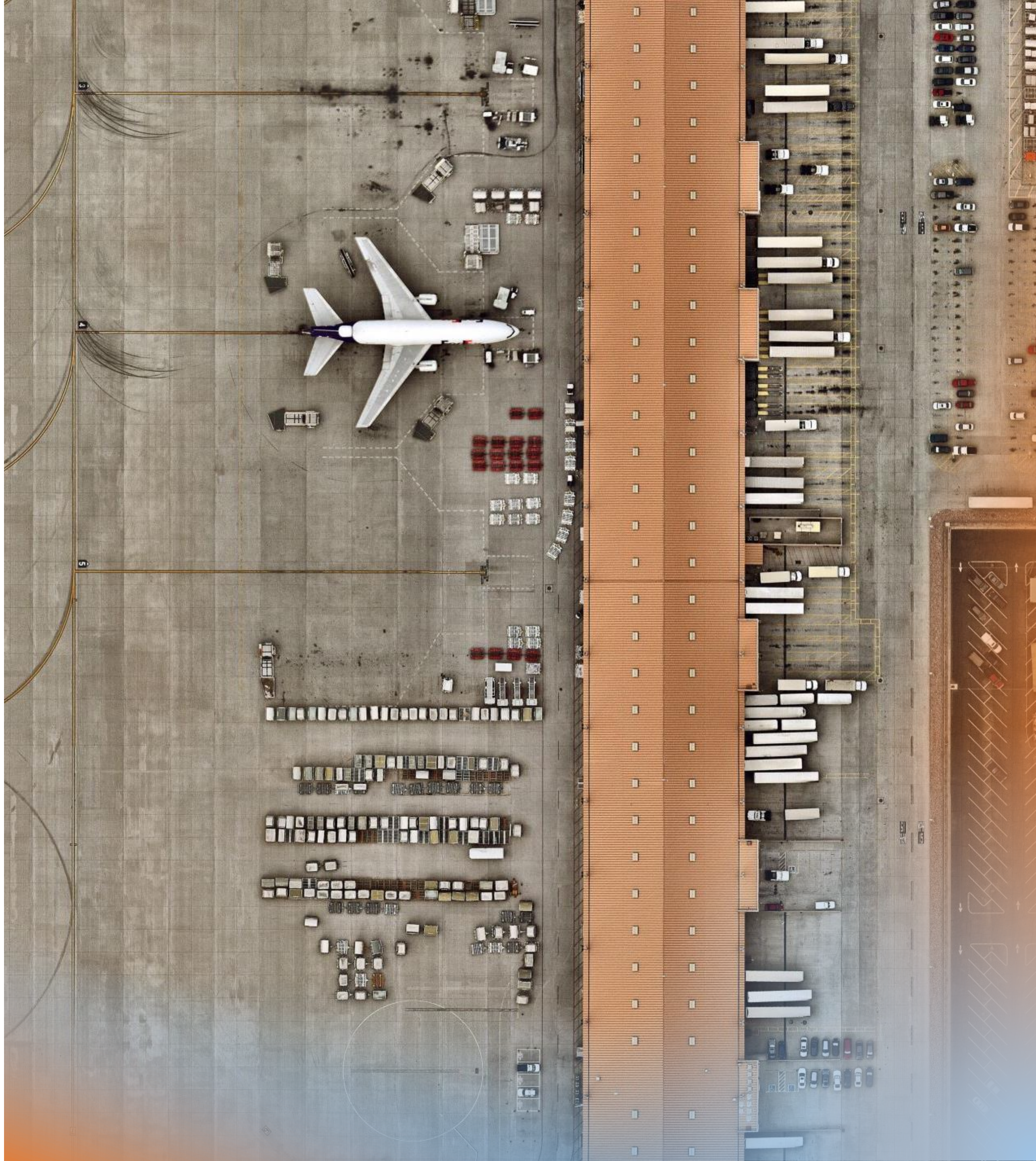
Work smarter
Not harder

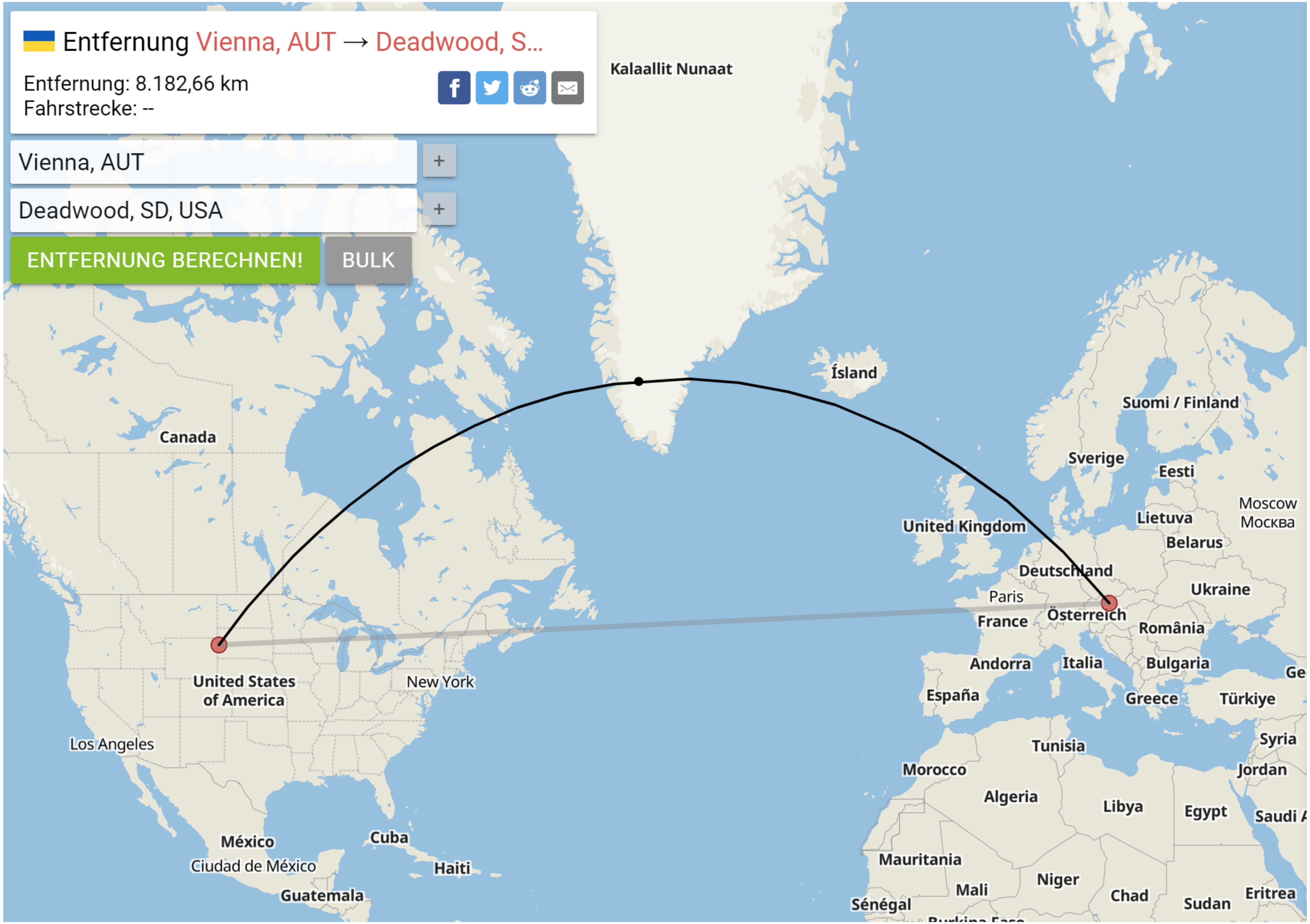
tems security

# Some statistics data

| | |
|---|---|
| • Vienna – Deadwood | 8.182,66 km |
| • Time difference | 8 hours |
| • Population | 1.270 |
| • WildWest Hacking Fest Attendees | 950 |
| • Closest airport (Rapid City) | 67km |
| • Elevation | 1.390 Meter |

- No public transportation from the Airport





Entfernung Vienna, AUT → Deadwood, S...

Entfernung: 8.182,66 km
Fahrstrecke: --

Vienna, AUT

Deadwood, SD, USA

# WWHF#2023 / Deadwood SD

tems security

tems
security

# Poll 1:
# How much costs this rental car per day?

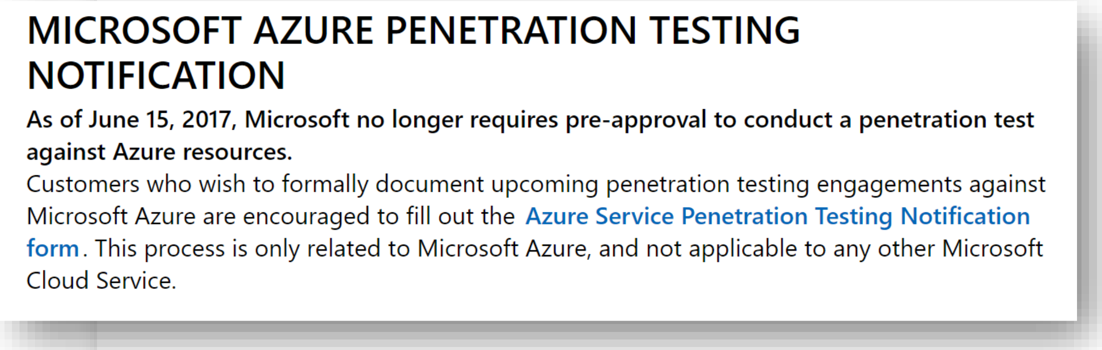
1. US$ 40,00
2. US$ 80,00
3. US$ 120,00
4. US$ 160,00

# Agenda

- All about the Cloud

# General permission by Cloud Provider

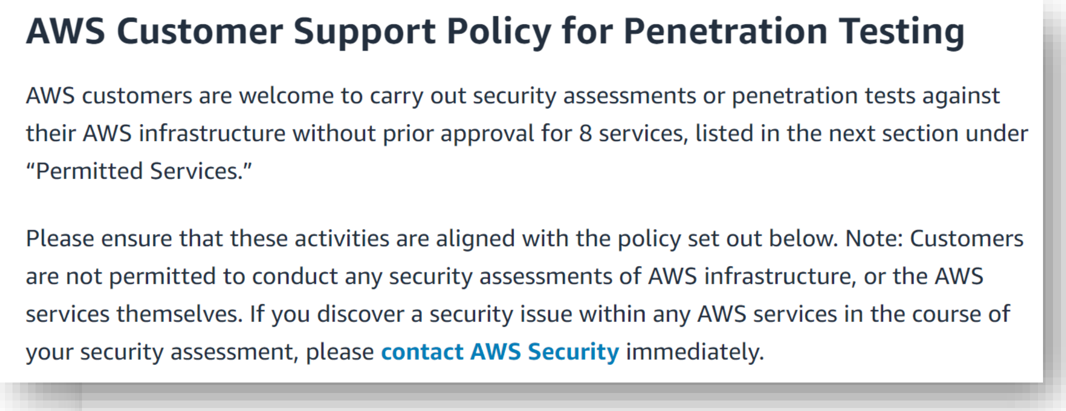
- All three big players are allowed without PTA to Pentest Cloud Services.
- Some dont‘s for Pentester on SaaS Provider:
    - DoS testing
    - Intense fuzzing
    - Phishing the cloud provider’s employees
    - Testing other company’s assets



## MICROSOFT AZURE PENETRATION TESTING NOTIFICATION

**As of June 15, 2017, Microsoft no longer requires pre-approval to conduct a penetration test against Azure resources.**

Customers who wish to formally document upcoming penetration testing engagements against Microsoft Azure are encouraged to fill out the Azure Service Penetration Testing Notification form. This process is only related to Microsoft Azure, and not applicable to any other Microsoft Cloud Service.



## AWS Customer Support Policy for Penetration Testing

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services, listed in the next section under “Permitted Services.”

Please ensure that these activities are aligned with the policy set out below. Note: Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves. If you discover a security issue within any AWS services in the course of your security assessment, please **contact AWS Security** immediately.

# My summary

- Service prinzipis can be setup with certs in Azure
- Great Recon tools outside at this moment (will follow up in Webinar 13)
- Everyone can get your Tenant ID with a single command
- Exploiting Misconfigured Cloud Assets
  - S3 Buckets
  - Elastic Block Store (EBS)
  - Microsoft Azure Storage
  - Google Cloud Platform
- Key Disclosure in Public Repositories
- Teams is unsecure per default

tems
security

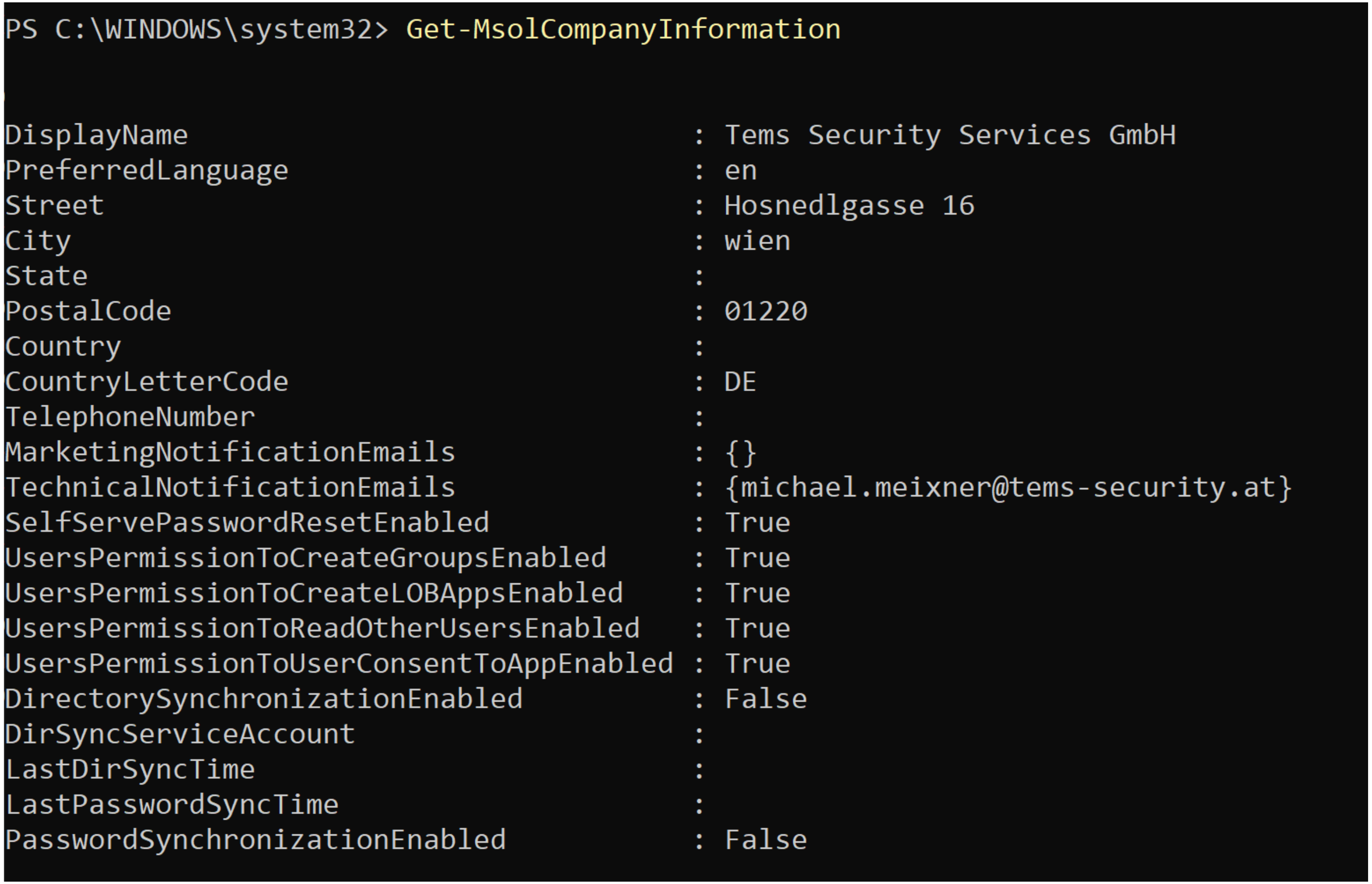
# Entra ID-Passwords

**<u>Everyone can do the follow</u>**

- ✓ If a user cred is valid
- ✓ If MFA is enabled on the account
- ✓ If a tenant doesn't exist
- ✓ If a user doesn't exist
- ✓ If the account is locked
- ✓ If the account is disabled
- ✓ If the password is expired

* MSOLSpray is your tool for that

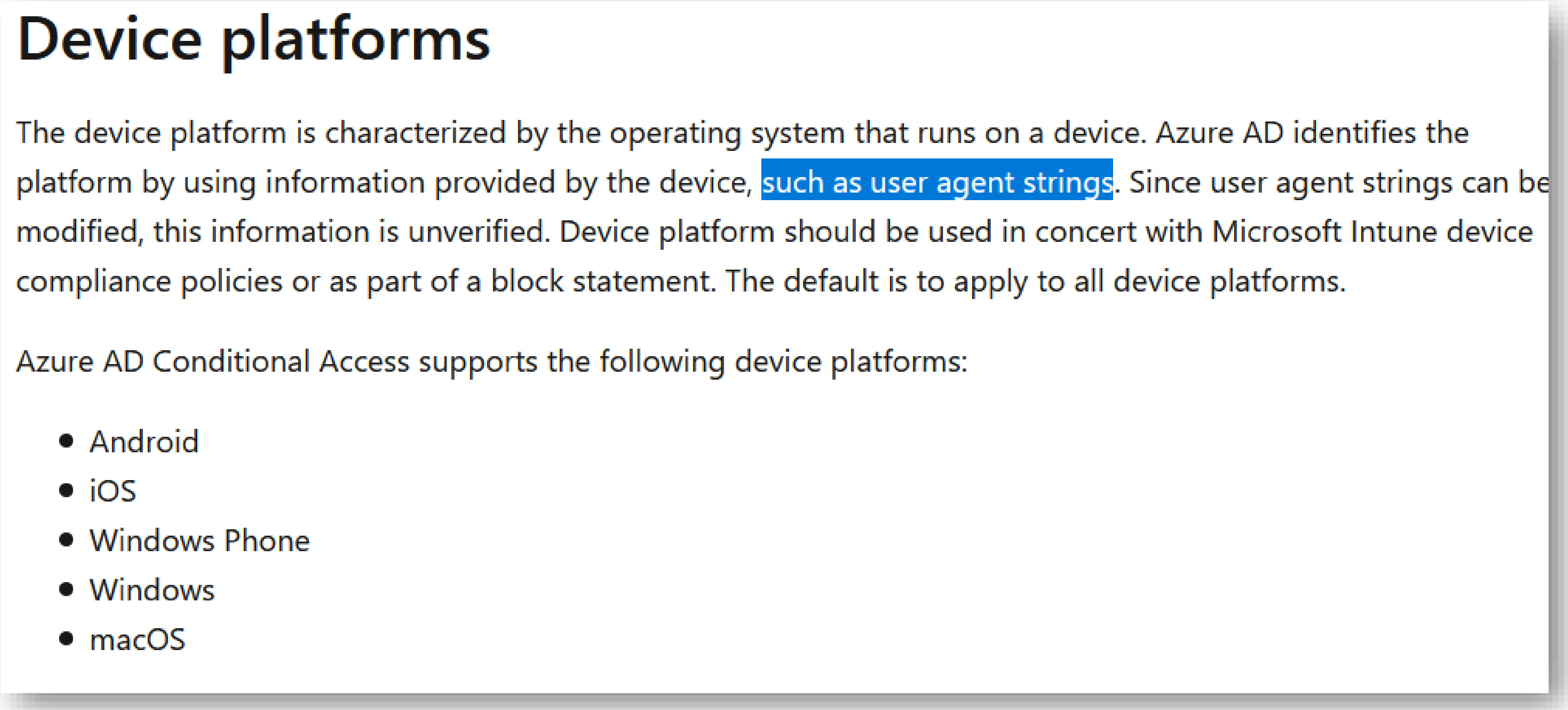
# Recon: Global Azure Information



```
PS C:\WINDOWS\system32> Get-MsolCompanyInformation


DisplayName                              : Tems Security Services GmbH
PreferredLanguage                        : en
Street                                   : Hosnedlgasse 16
City                                     : wien
State                                    :
PostalCode                               : 01220
Country                                  :
CountryLetterCode                        : DE
TelephoneNumber                          :
MarketingNotificationEmails              : {}
TechnicalNotificationEmails              : {michael.meixner@tems-security.at}
SelfServePasswordResetEnabled            : True
UsersPermissionToCreateGroupsEnabled     : True
UsersPermissionToCreateLOBAppsEnabled    : True
UsersPermissionToReadOtherUsersEnabled   : True
UsersPermissionToUserConsentToAppEnabled : True
DirectorySynchronizationEnabled          : False
DirSyncServiceAccount                    :
LastDirSyncTime                          :
LastPasswordSyncTime                     :
PasswordSynchronizationEnabled           : False
```

# One of the Conditional Access Pitfall



## Device platforms

The device platform is characterized by the operating system that runs on a device. Azure AD identifies the platform by using information provided by the device, such as user agent strings. Since user agent strings can be modified, this information is unverified. Device platform should be used in concert with Microsoft Intune device compliance policies or as part of a block statement. The default is to apply to all device platforms.

Azure AD Conditional Access supports the following device platforms:

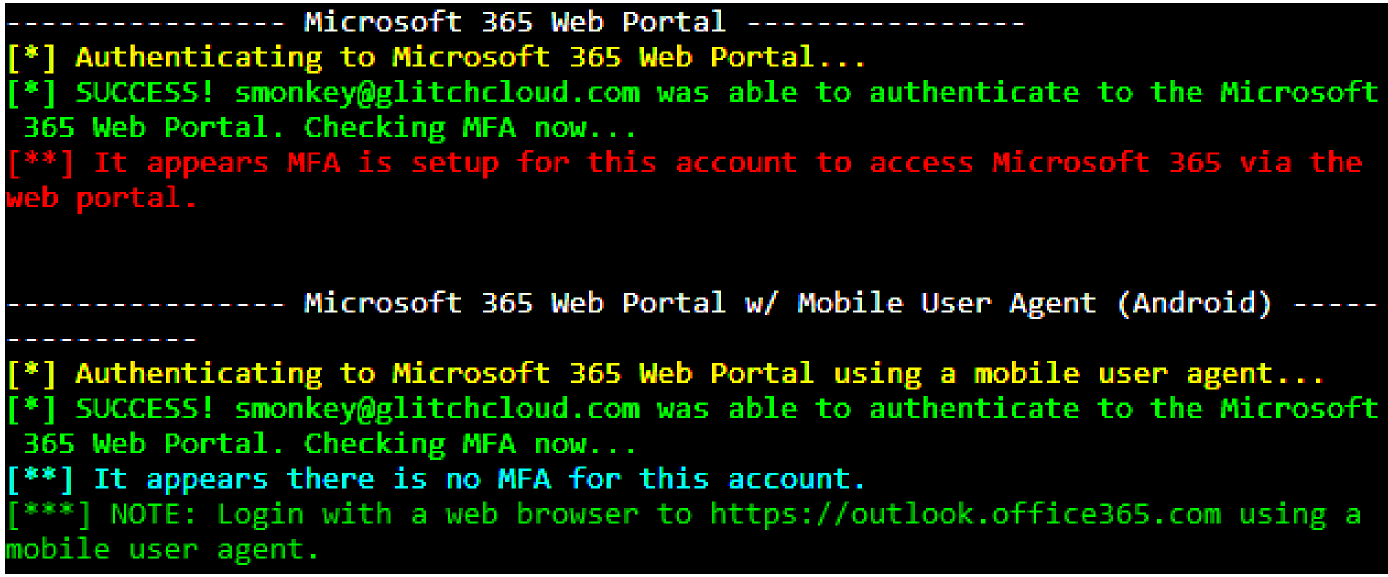
- Android
- iOS
- Windows Phone
- Windows
- macOS

# Second Conditional Access Pitfall (authenticated)

Tools will help to find inconsistencies in Microsoft MFA deployments, only with valid username and password

- Microsoft Graph API
- Azure Service Management API
- Microsoft 365 Exchange Web Services
- Microsoft 365 Web Portal
- Microsoft 365 Web Portal Using a Mobile User Agent
- Microsoft 365 Active Sync
- ADFS

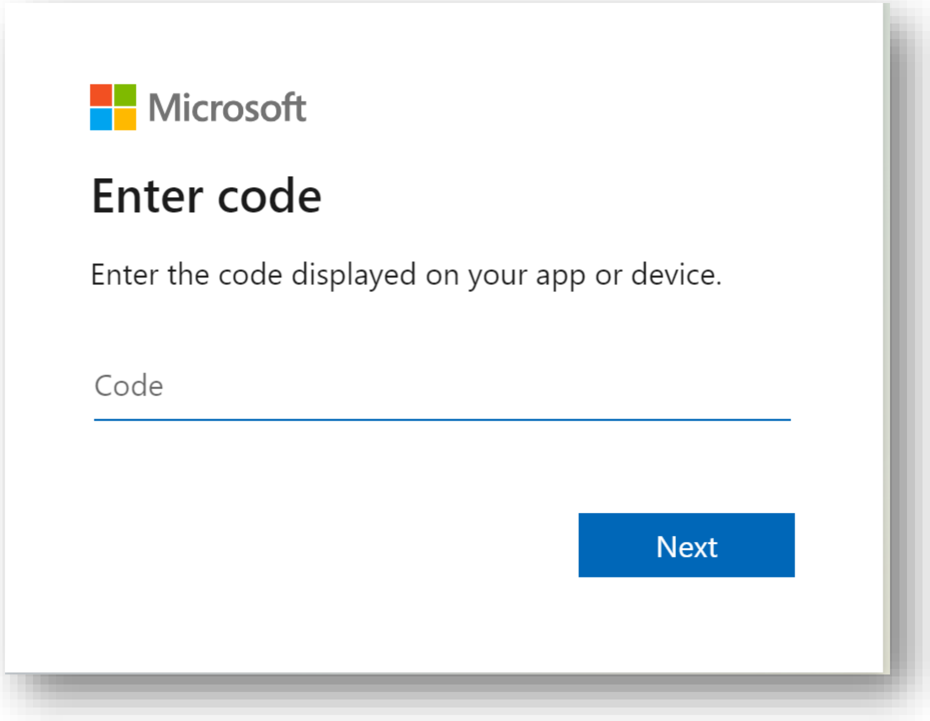
**Username & Password from Leaked dataset**



```
---------------- Microsoft 365 Web Portal ----------------
[*] Authenticating to Microsoft 365 Web Portal...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft
 365 Web Portal. Checking MFA now...
[**] It appears MFA is setup for this account to access Microsoft 365 via the
web portal.


---------------- Microsoft 365 Web Portal w/ Mobile User Agent (Android) -----
-----------
[*] Authenticating to Microsoft 365 Web Portal using a mobile user agent...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft
 365 Web Portal. Checking MFA now...
[**] It appears there is no MFA for this account.
[***] NOTE: Login with a web browser to https://outlook.office365.com using a
mobile user agent.
```

# Device Code Phishing

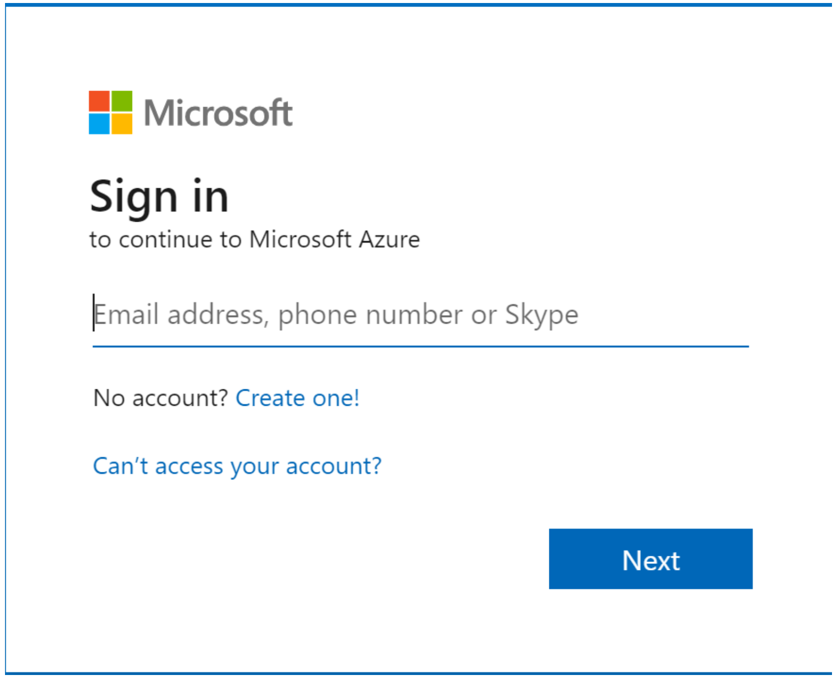


Microsoft

Enter code

Enter the code displayed on your app or device.

Code



Microsoft

Sign in

to continue to Microsoft Azure

Email address, phone number or Skype

No account? Create one!

Can’t access your account?

Access token = 1h (not possible to revoke this token)

Refresh token = 90 days (Admin or User can revoke this token)

# Steal Tokens (1/2)

Google JSON Tokens and credentials.db

Azure Cloud Service Packages (.cspkg)

Azure Publish Settings files (.publishsettings)

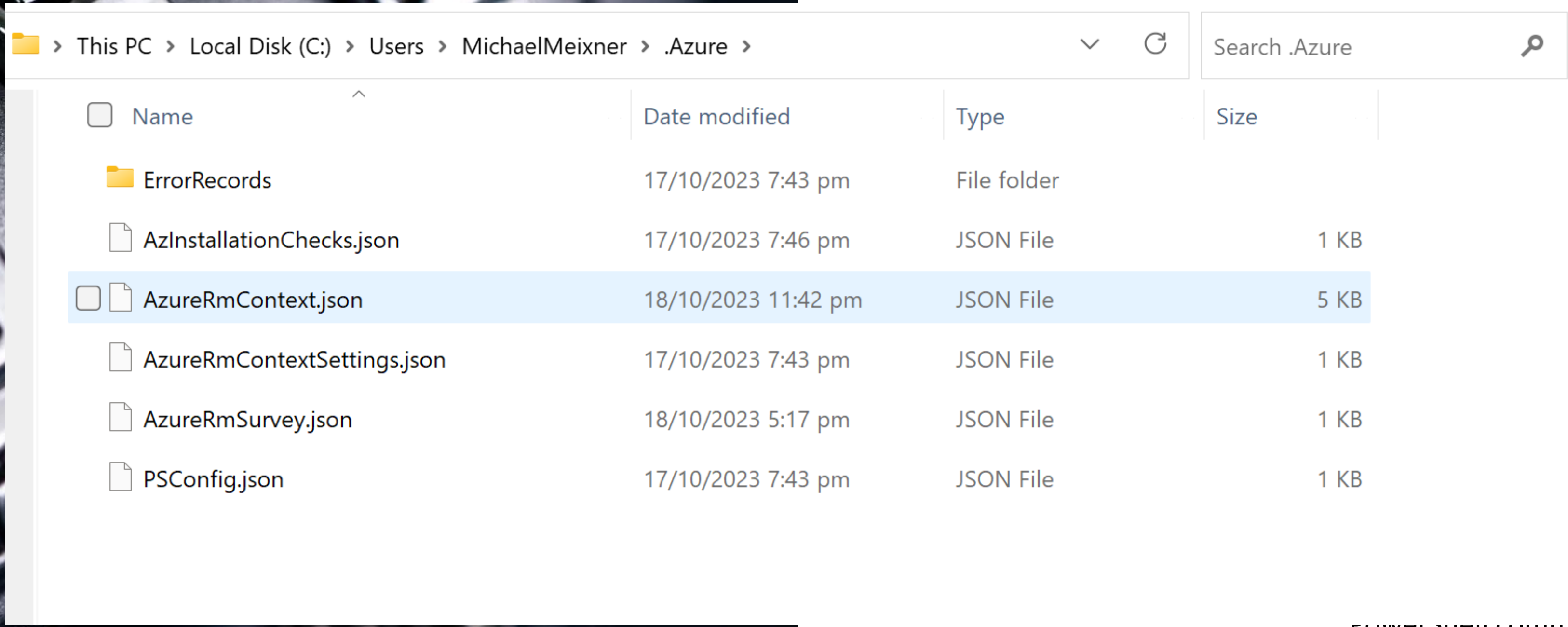
Developers often use storage explorers to easily upload and download files to Azure

Storage Explorers store credentials on disk (Windows Credential Manager) and then use them to authenticate to services such as Azure

Web Config and App Config files

tems security

# Steal Tokens (2/2)


This PC › Local Disk (C:) › Users › MichaelMeixner › .Azure ›
Search .Azure

| □ Name | Date modified | Type | Size |
|---|---|---|---|
| ErrorRecords | 17/10/2023 7:43 pm | File folder | |
| AzInstallationChecks.json | 17/10/2023 7:46 pm | JSON File | 1 KB |
| □ AzureRmContext.json | 18/10/2023 11:42 pm | JSON File | 5 KB |
| AzureRmContextSettings.json | 17/10/2023 7:43 pm | JSON File | 1 KB |
| AzureRmSurvey.json | 18/10/2023 5:17 pm | JSON File | 1 KB |
| PSConfig.json | 17/10/2023 7:43 pm | JSON File | 1 KB |

context files (.json)

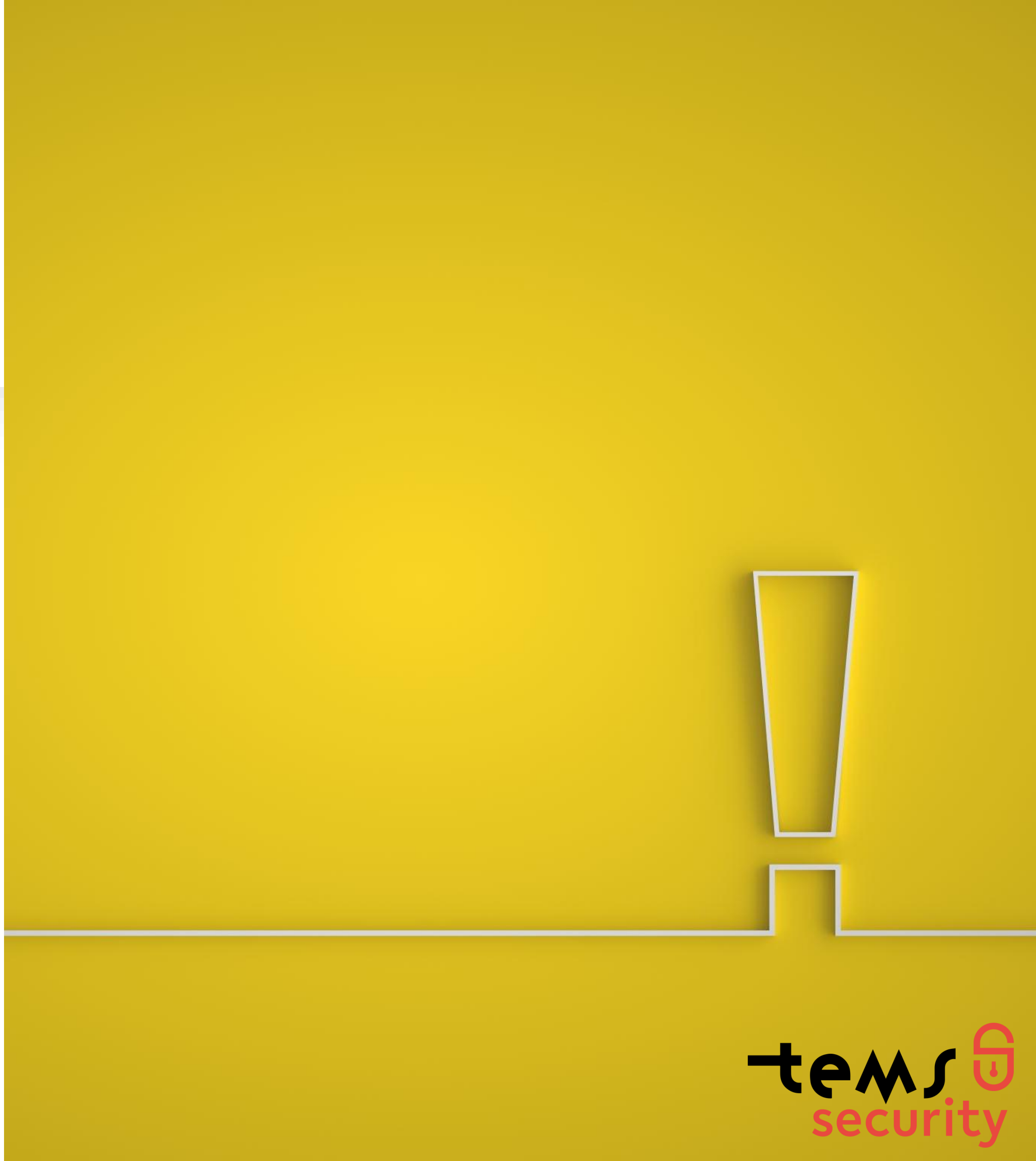
ızure\
s

PowerShell command
history is here

%USERPROFILE%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt

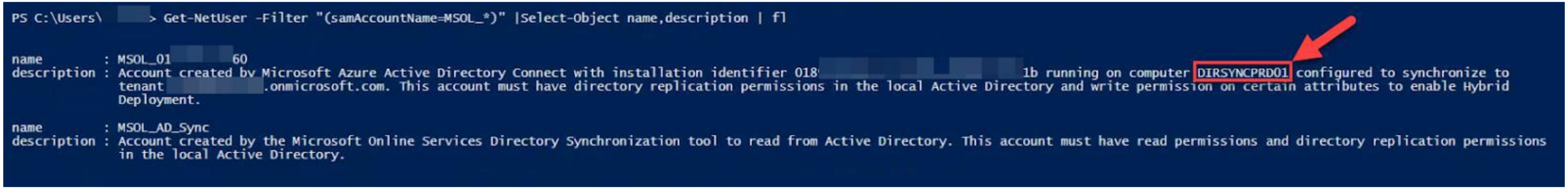
# Hybrid Entra ID Joined Devices

- **Global Administrators** and **Intune Administrators** can execute PowerShell scripts on Hybrid-joined systems
- Use Microsoft’s Endpoint Manager to execute
- Scripts get executed on reboot or hourly when a sync occurs



# ADConnect DCSync

## AAD Connector is a hidden DC and must be protected as your DC too



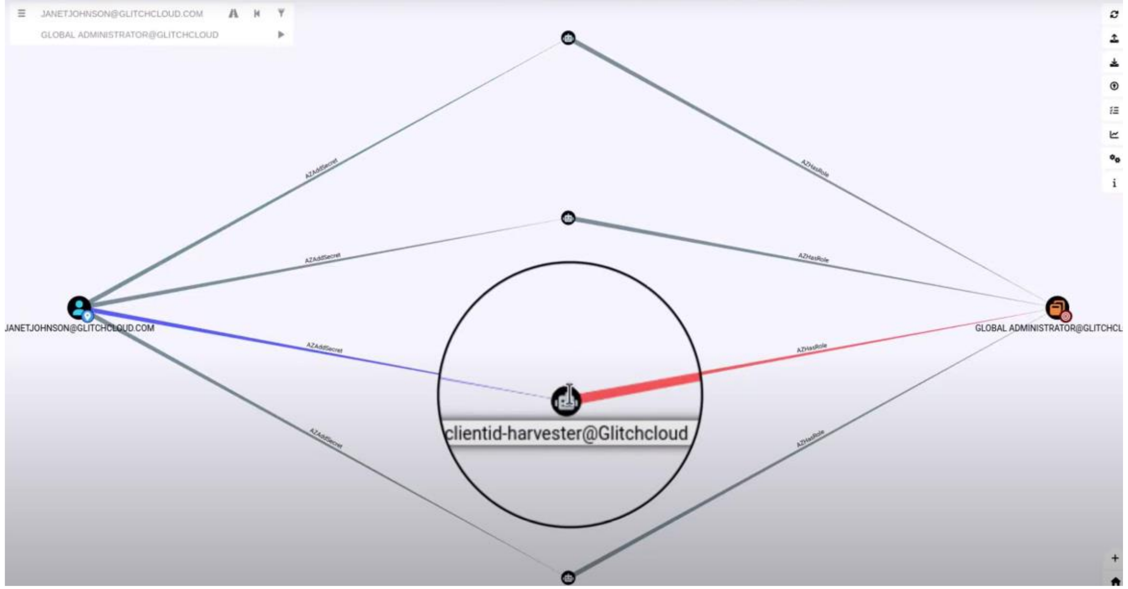
```
PS C:\Users\[redacted]> Get-NetUser -Filter "(samAccountName=MSOL_*)" |Select-Object name,description | fl

name        : MSOL_01[redacted]60
description : Account created bv Microsoft Azure Active Directory Connect with installation identifier 018[redacted]1b running on computer DIRSYNCPRD01 configured to synchronize to
              tenant [redacted].onmicrosoft.com. This account must have directory replication permissions in the local Active Directory and write permission on certain attributes to enable Hybrid
              Deployment.

name        : MSOL_AD_Sync
description : Account created by the Microsoft Online Services Directory Synchronization tool to read from Active Directory. This account must have read permissions and directory replication permissions
              in the local Active Directory.
```

```
Get-NetUser -Filter "(samAccountName=MSOL_*)" |Select-Object name,description | fl
```

# Bloodhound for Azure



JANETJOHNSON@GLITCHCLOUD.COM

GLOBAL ADMINISTRATOR@GLITCHCLOUD

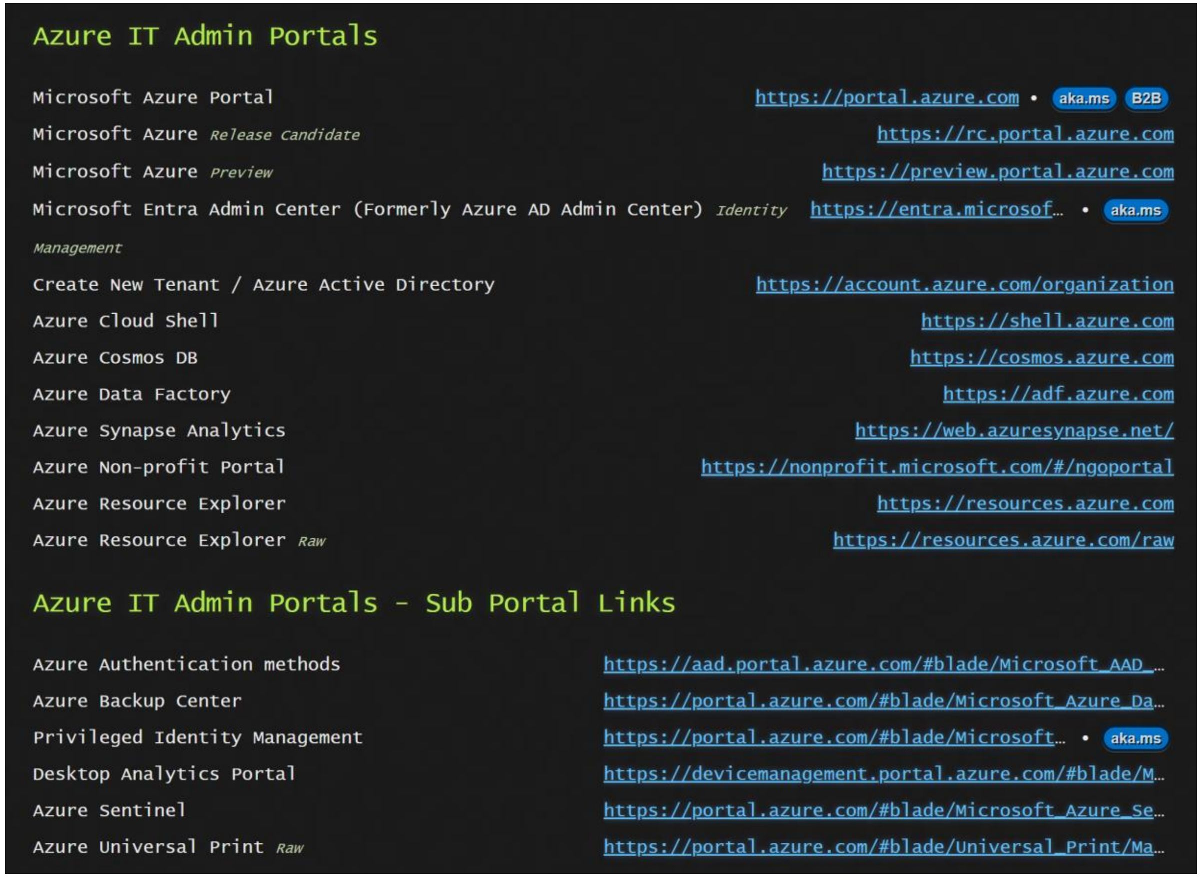
AZAddSecret
AZHasRole
AZAddSecret
AZHasRole
JANETJOHNSON@GLITCHCLOUD.COM
GLOBAL ADMINISTRATOR@GLITCHCL
AZAddSecret
AZHasRole
clientid-harvester@Glitchcloud
AZAddSecret
AZHasRole

https://github.com/BloodHoundAD/AzureHound

# Entra ID from Hacker point of view (authenticated)

- Clone Groups – (example Administrators)
- Dump Condition access polices
- Dump Dynamic Group Schema
- Users can create APPs per Default
- Find Mailboxes with through settings
- All Users are allowed to create Security Groups in Entire ID
- Block Azure ID access block you only on the GUI but not from the Powershell
- Pillage (plündern)
  - Teams Messages, Teams-Chat, Teams-Files
  - E-Mails
  - SharePoint
- Search for all UserAttributes
- Full Search for Onedrive & Sharepoint with Graph API
- Download files which are blocked to download
- Read Email with touching the Read/unread function in Outlook

# https://msportals.io/

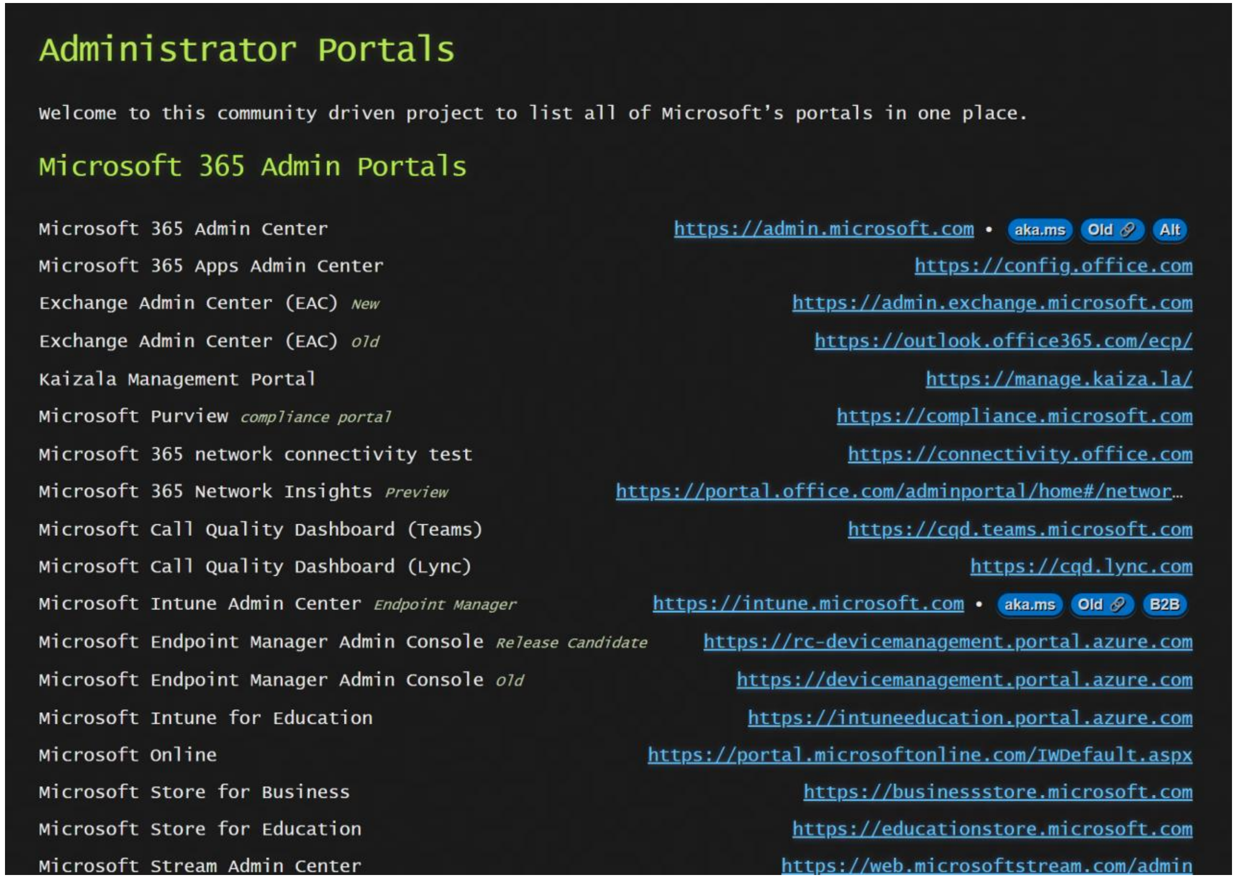


## Azure IT Admin Portals

| | |
|---|---|
| Microsoft Azure Portal | https://portal.azure.com • aka.ms B2B |
| Microsoft Azure *Release Candidate* | https://rc.portal.azure.com |
| Microsoft Azure *Preview* | https://preview.portal.azure.com |
| Microsoft Entra Admin Center (Formerly Azure AD Admin Center) *Identity Management* | https://entra.microsof… • aka.ms |
| Create New Tenant / Azure Active Directory | https://account.azure.com/organization |
| Azure Cloud Shell | https://shell.azure.com |
| Azure Cosmos DB | https://cosmos.azure.com |
| Azure Data Factory | https://adf.azure.com |
| Azure Synapse Analytics | https://web.azuresynapse.net/ |
| Azure Non-profit Portal | https://nonprofit.microsoft.com/#/ngoportal |
| Azure Resource Explorer | https://resources.azure.com |
| Azure Resource Explorer *Raw* | https://resources.azure.com/raw |

## Azure IT Admin Portals - Sub Portal Links

| | |
|---|---|
| Azure Authentication methods | https://aad.portal.azure.com/#blade/Microsoft_AAD_… |
| Azure Backup Center | https://portal.azure.com/#blade/Microsoft_Azure_Da… |
| Privileged Identity Management | https://portal.azure.com/#blade/Microsoft… • aka.ms |
| Desktop Analytics Portal | https://devicemanagement.portal.azure.com/#blade/M… |
| Azure Sentinel | https://portal.azure.com/#blade/Microsoft_Azure_Se… |
| Azure Universal Print *Raw* | https://portal.azure.com/#blade/Universal_Print/Ma… |



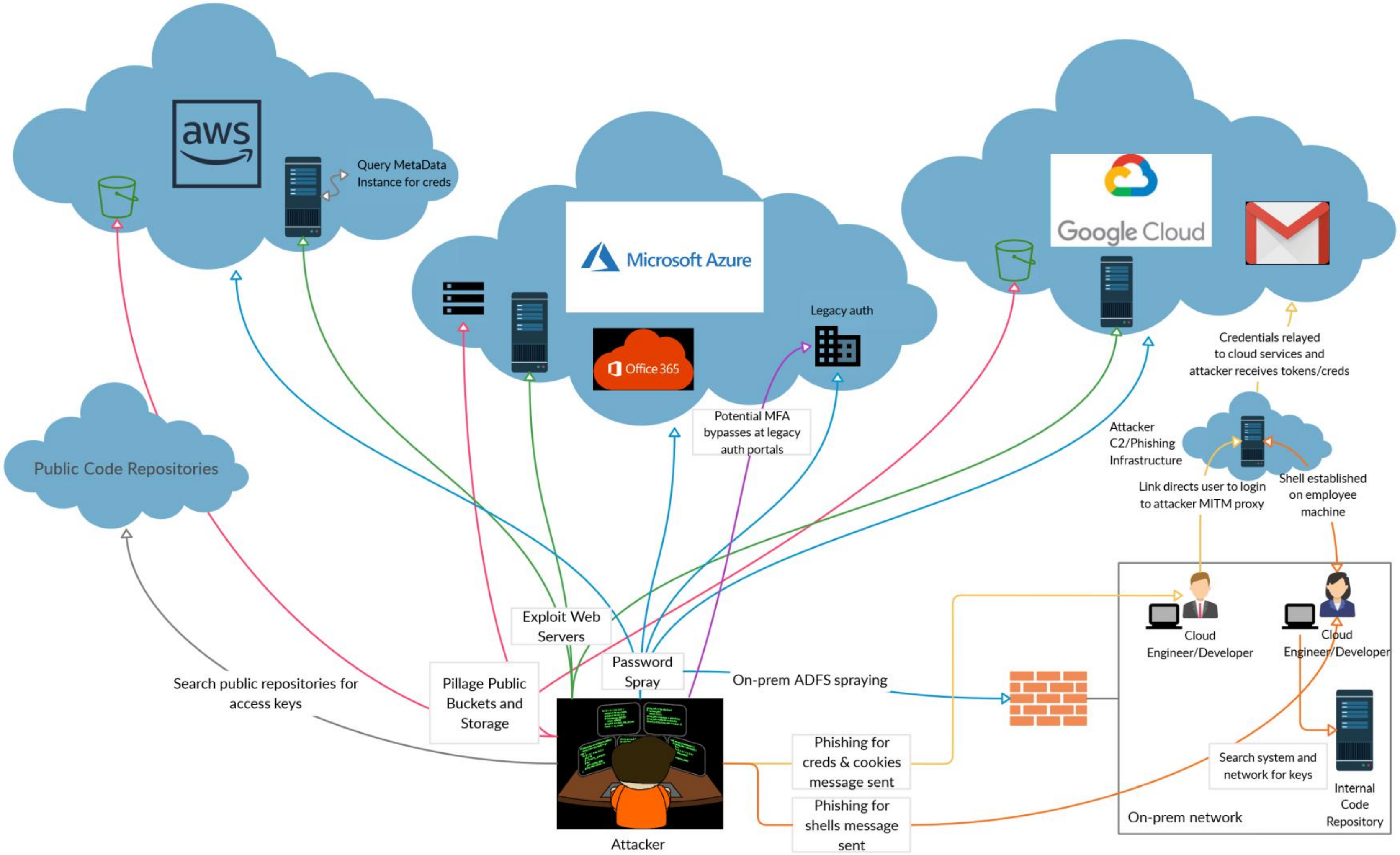
## Administrator Portals

Welcome to this community driven project to list all of Microsoft's portals in one place.

## Microsoft 365 Admin Portals

| | |
|---|---|
| Microsoft 365 Admin Center | https://admin.microsoft.com • aka.ms Old 🔗 Alt |
| Microsoft 365 Apps Admin Center | https://config.office.com |
| Exchange Admin Center (EAC) *New* | https://admin.exchange.microsoft.com |
| Exchange Admin Center (EAC) *old* | https://outlook.office365.com/ecp/ |
| Kaizala Management Portal | https://manage.kaiza.la/ |
| Microsoft Purview *compliance portal* | https://compliance.microsoft.com |
| Microsoft 365 network connectivity test | https://connectivity.office.com |
| Microsoft 365 Network Insights *Preview* | https://portal.office.com/adminportal/home#/networ… |
| Microsoft Call Quality Dashboard (Teams) | https://cqd.teams.microsoft.com |
| Microsoft Call Quality Dashboard (Lync) | https://cqd.lync.com |
| Microsoft Intune Admin Center *Endpoint Manager* | https://intune.microsoft.com • aka.ms Old 🔗 B2B |
| Microsoft Endpoint Manager Admin Console *Release Candidate* | https://rc-devicemanagement.portal.azure.com |
| Microsoft Endpoint Manager Admin Console *old* | https://devicemanagement.portal.azure.com |
| Microsoft Intune for Education | https://intuneeducation.portal.azure.com |
| Microsoft Online | https://portal.microsoftonline.com/IWDefault.aspx |
| Microsoft Store for Business | https://businessstore.microsoft.com |
| Microsoft Store for Education | https://educationstore.microsoft.com |
| Microsoft Stream Admin Center | https://web.microsoftstream.com/admin |

# Modern Attack (you are blind without logging!)


aws
Query MetaData Instance for creds
Microsoft Azure
Office 365
Legacy auth
Google Cloud
Public Code Repositories
Potential MFA bypasses at legacy auth portals
Credentials relayed to cloud services and attacker receives tokens/creds
Attacker C2/Phishing Infrastructure
Link directs user to login to attacker MITM proxy
Shell established on employee machine
Exploit Web Servers
Password Spray
On-prem ADFS spraying
Search public repositories for access keys
Pillage Public Buckets and Storage
Phishing for creds & cookies message sent
Phishing for shells message sent
Attacker
Cloud Engineer/Developer
Cloud Engineer/Developer
Search system and network for keys
Internal Code Repository
On-prem network

tems security

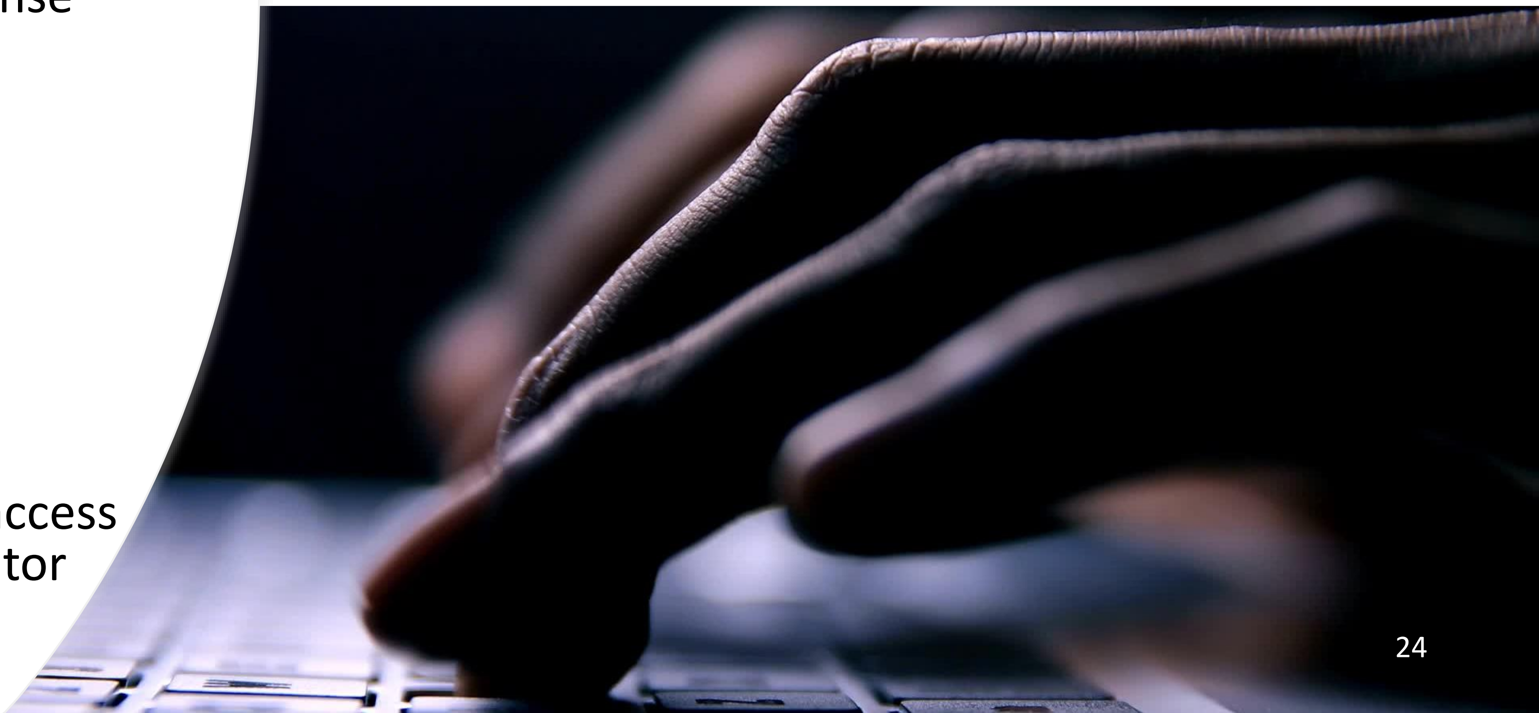
# Entra ID - Event Logging

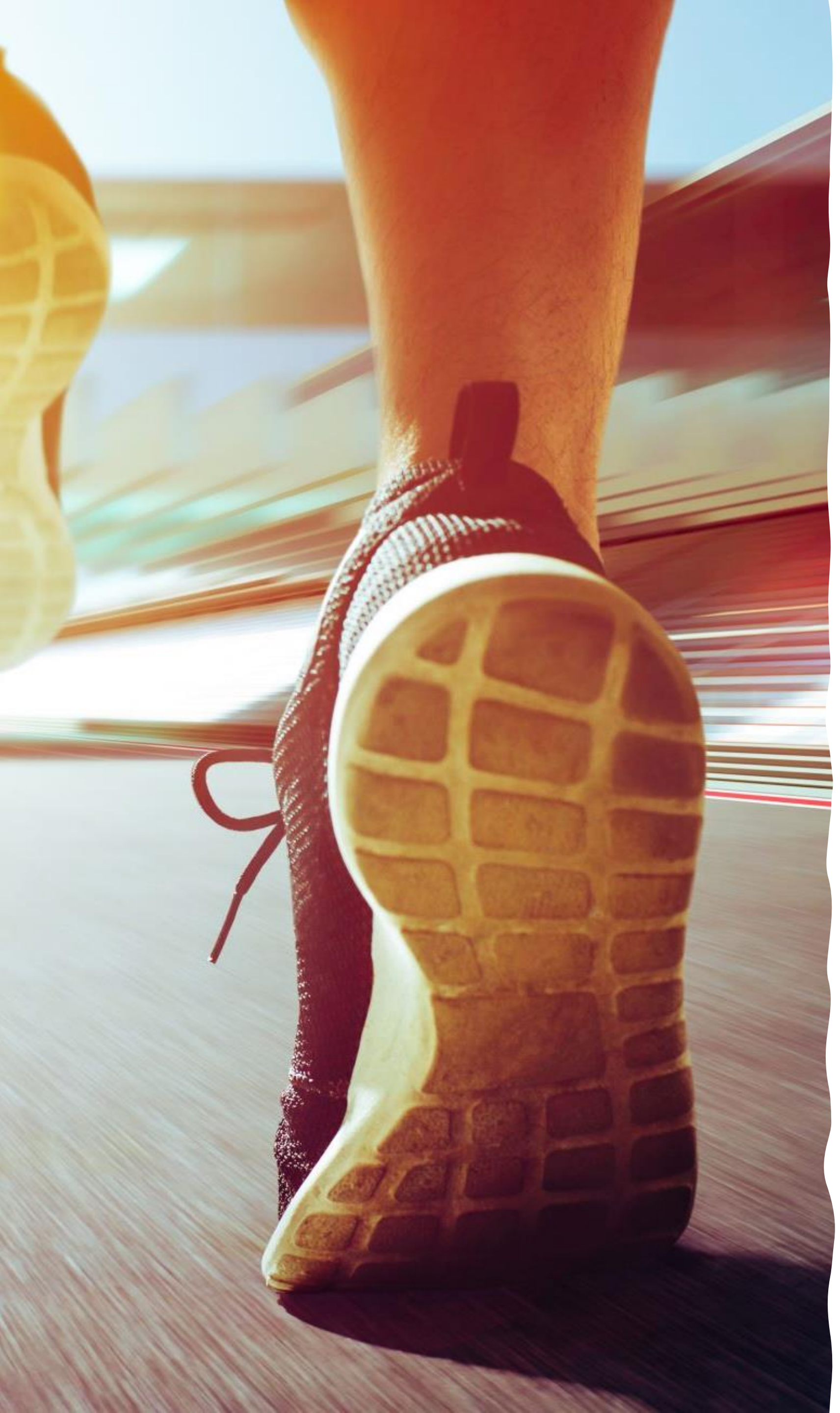
- Every Global Administrator must be familiar with all different Loggings in O365
  - Sign-in logs
  - Apps
  - Risk Users
  - …..

Will be huge topic at 13. Webinar (all about logging in Entra ID)

# Summary

- ✓ With a Guest account a good hacker can gain to Global Administrator within some days (*without Entra ID Hardening)*.
- ✓ If you gain hacked and you have O365 in sync you do have two issue (on-Prem, Azure)
  - ✓ With Azure you do have even more headache to get the hacker out of your tenant!
    You should adapt your Incident Response Plan for Entra ID
- ✓ Hacker are working on *„how to hack the incident response team“*
- ✓ If the Hacker are on your O365 Tenant no communication is secure before clean-up!
- ✓ Better you spend some time to hardening your Entra ID before it is too late.
- ✓ If you are using Cloud Services with have access to your local environments you must monitor that as well.





# Next Webinar

November
22nd 2023
09:00am

12. Webinar
All about MS CA-Services
by Stephan Emich

tems
security

# Get in contact with us

Philip Berger
Managing Director
☎ +43(664) 343 8644
✉ Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director
☎ +43(664) 1453328
✉ Michael.meixner@tems-security.at