



A Z U R E
BOOTCAMP SWITZERLAND



How Criminals Breach your Azure Environment

Marco Schmidt & Manuel Meyer



> whoami - Manu



Azure Architect @ GrabX Solutions



Leading your way through the Azure Cloud



Zurich, Switzerland



Organizing community events



manuelmeyer.net



> whoami - Marco



Security Engineer @ GrabX Solutions



Working with customers to protect their cloud environments



Bern, Switzerland



Like to break things



thesecurityguy.ch



> Introduction

- Fictional Scenario of **Attack Kill Chain** in the Cloud
- All techniques are **valid attack techniques** and have been **used by threat actors in the past**
- Scenario has been **simplified** to fit the session
- REMEMBER:

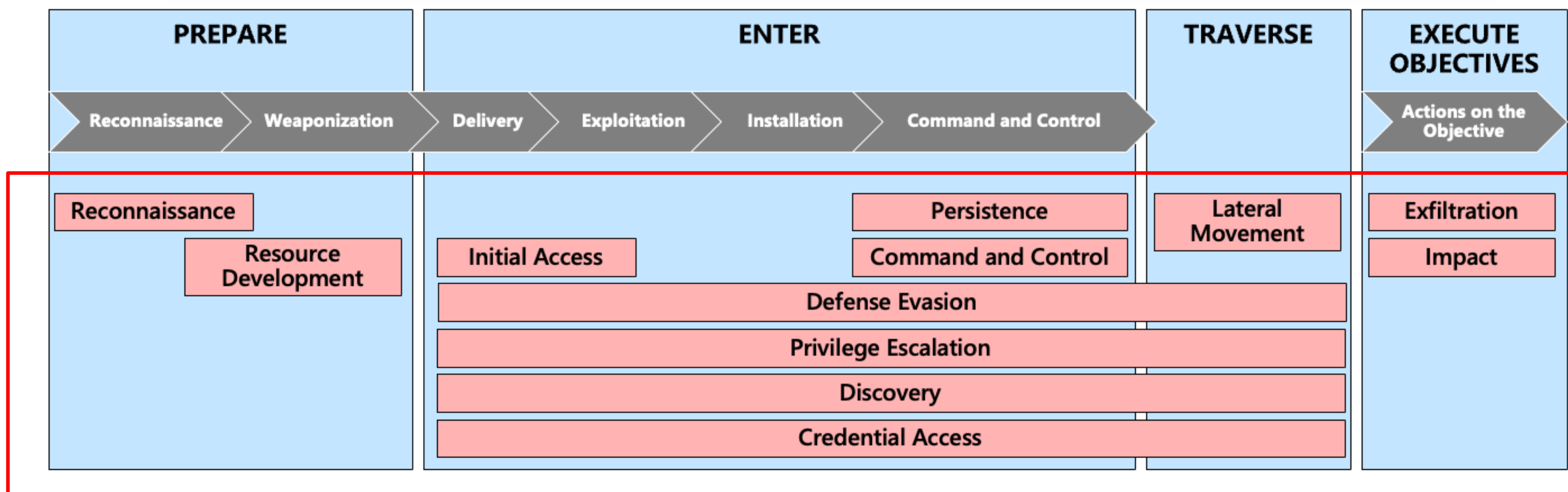
With great power comes great responsibility! 💪



Attack Chain Models

Describe stages of an attack

PETE	Simple model for business leaders and other non-technical stakeholders
MITRE ATT&CK Framework	Detailed model for technical detection coverage assessments and planning
Lockheed Martin Kill Chain	Legacy Reference Model (missing lateral traversal)





-> Find Passwords

-> User Enumeration

-> Password Spray

-> Conditional Access Bypass

-> Abusing Dynamic Groups

-> Abusing VM
Contributor Role

Reconnaissance

➤ Find Passwords

How do Hackers get your Passwords?

- Open Source Intelligence (OSINT)
- Phishing
- Darkweb
- Dumpster Diving
- Password Attacks
- Malware
- Etc.



> Find Passwords

How can you protect against this?

- Use Passkeys
- Entra ID Smart Lockout
- M365 Defender Suite
- User Awareness Training
- **Most important:** Brain.exe



> User Enumeration



Sign in

This username may be incorrect. Make sure that you typed it correctly. Otherwise, contact your admin.

asdf@grabx.ch

No account? [Create one!](#)

[Can't access your account?](#)

Back

Next



Sign-in options



← marco.schmidt@grabx.ch

Enter password

Password

[Sign in with a security key](#)

Sign in

Please sign-in with your GrabX credentials

> User Enumeration

POST ▼ https://login.microsoftonline.com/common/GetCredentialType

Params Authorization ● Headers (10) Body ● Pre-request Script Test

● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● Gra

```
1 {
2   "username": "asdf@grabx.ch"
3 }
```

Body Cookies (4) Headers (14) Test Results

Pretty Raw Preview Visualize JSON ▼ ≡

```
1 {
2   "Username": "asdf@grabx.ch",
3   "Display": "asdf@grabx.ch",
4   "IfExistsResult": 1,
5   "IsUnmanaged": false,
6   "ThrottleStatus": 0,
```

POST ▼ https://login.microsoftonline.com/common/GetCredentialType

Params Authorization ● Headers (10) Body ● Pre-request Script Te

● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● G

```
1 {
2   "username": "marco.schmidt@grabx.ch"
3 }
```

Body Cookies (4) Headers (14) Test Results

Pretty Raw Preview Visualize JSON ▼ ≡

```
1 {
2   "Username": "marco.schmidt@grabx.ch",
3   "Display": "marco.schmidt@grabx.ch",
4   "IfExistsResult": 0,
5   "IsUnmanaged": false,
6   "ThrottleStatus": 0,
```

> User Enumeration

```
AAInternals 0.9.1
AAInternals 0.9.1 (pwsh)
PS /Users/marco/AzureBootCamp> Get-Content ./users.txt | Invoke-AADIntUserEnumerationAsOutsider

UserName      Exists
-----
asdf@grabx.ch False
marco.schmidt@grabx.ch True

PS /Users/marco/AzureBootCamp>
```

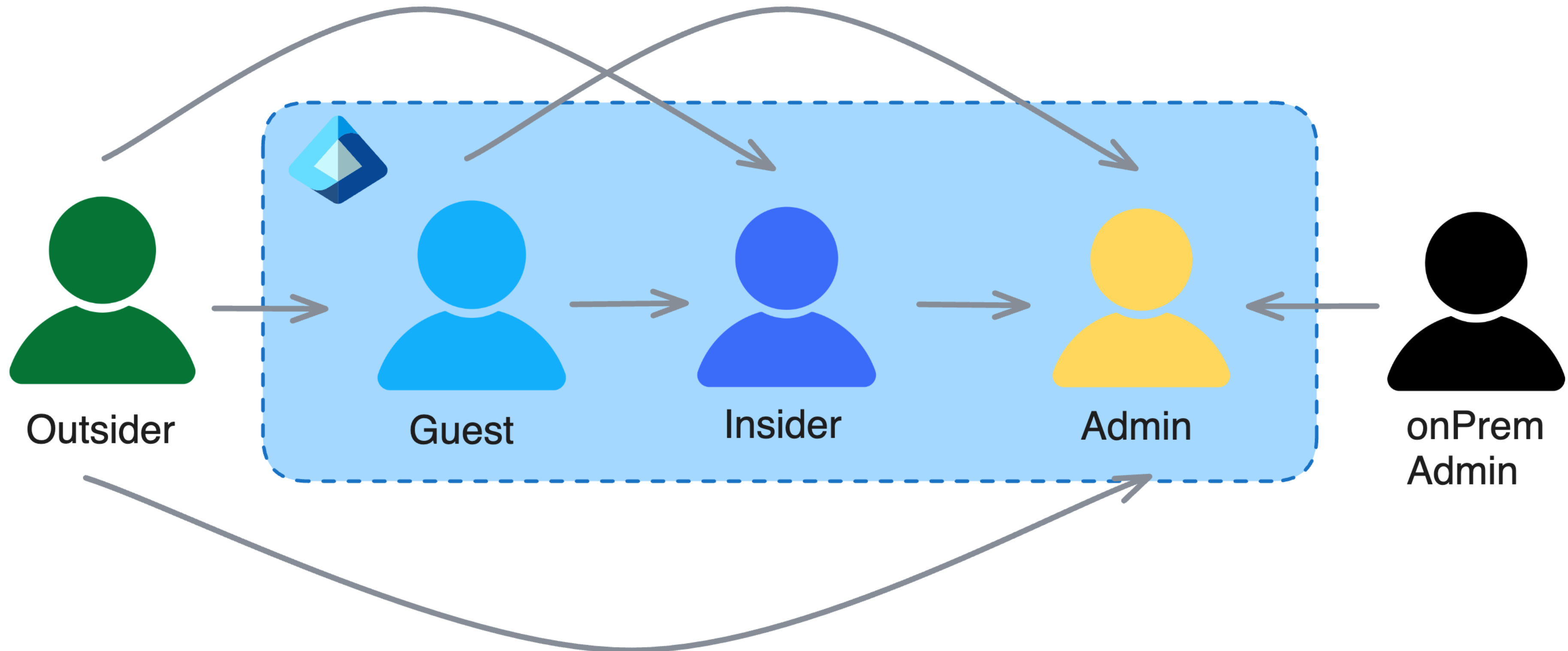

> AADInternals



- First Released in 2018 by Security Researcher Dr. Nestory Syynimaa
- “The ultimate Azure AD / Microsoft 365 hacking and admin toolkit”
- License: Creative Commons

> AADInternals

Kill chain roles





Azure AD and Microsoft 365 kill chain

	Recon	Compromise	Persistence	Actions on Intent
Outsider	Get-AADIntTenantDomains Get-AADIntOpenIDConfiguration Get-AADIntLoginInformation Invoke-AADIntReconAsOutsider Invoke-AADIntUserEnumerationAsOutsider	Invoke-AADIntPhishing		
Guest	Get-AADIntAzureTenants Get-AADIntAzureInformation Get-AADIntSPOSiteUsers Get-AADIntSPOSiteGroups Invoke-AADIntReconAsGuest Invoke-AADIntUserEnumerationAsGuest			
User	Get-AADIntTenantDetails Get-AADIntGlobalAdmins Get-AADIntSyncConfiguration Get-AADIntCompanyInformation Get-AADIntSPOServiceInformation Invoke-AADIntReconAsInsider Invoke-AADIntUserEnumerationAsInsider			New-AADIntBulkPRTToken Join-AADIntDeviceToAzureAD Join-AADIntDeviceToIntune
Admin	Get-AADIntAzureSubscriptions	Grant-AADIntAzureUserAccessAdminRole Set-AADIntAzureRoleAssignment Invoke-AADIntAzureVMScript Register-AADIntPTAAgent Set-UserMFA Set-UserMFAApps	ConvertTo-AADIntBackdoor Set-AADIntPassThroughAuthentication	New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal
On-prem admin		Export-AADIntADESSigningCertificate Get-AADIntSyncCredentials Set-AADIntUserPassword Install-AADIntPTASpy		New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal

> User Enumeration

How can you protect against this?

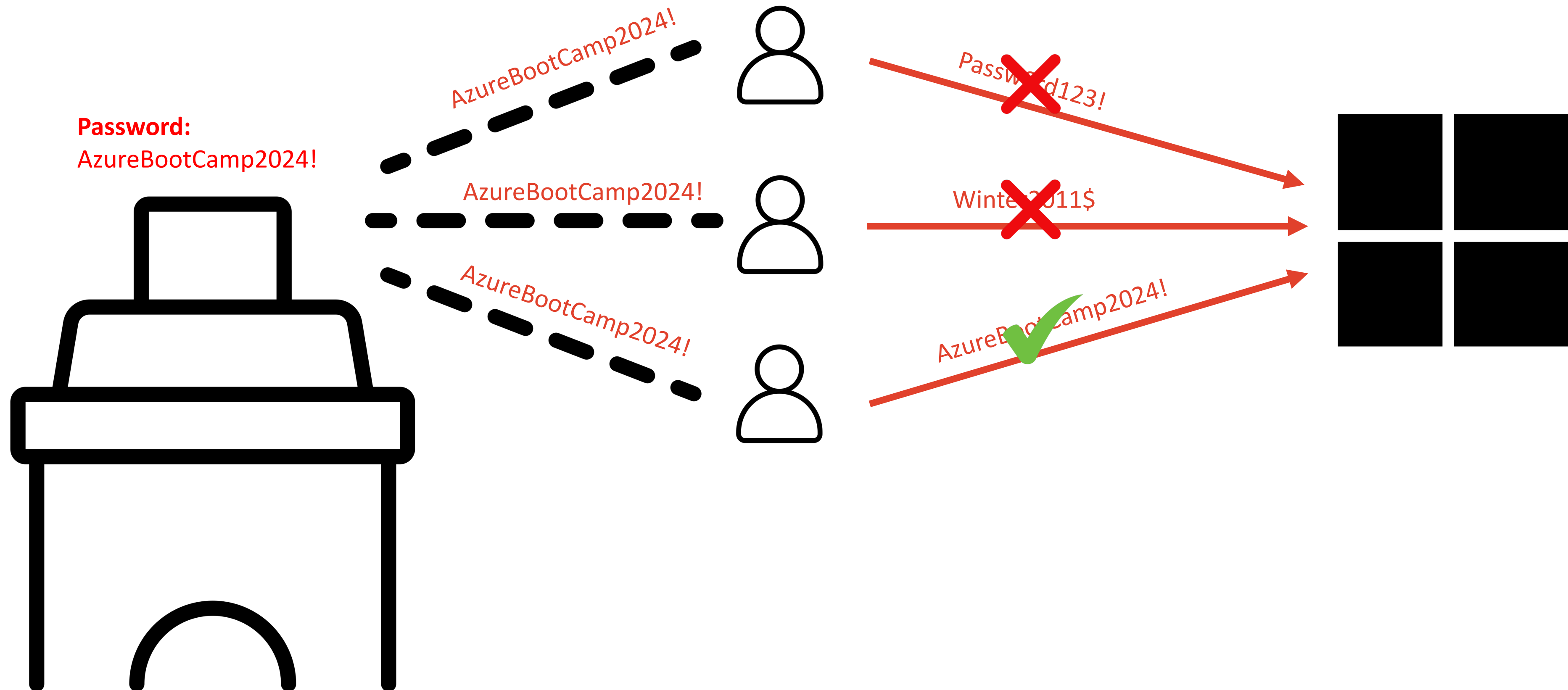
- You can't





Result: Enumerated existing users

> Password Spray



Password Spray

- API Endpoint:
<https://login.microsoft.com/common/oauth/token>
- API Responses:
 - AADSTS50034 -> User doesn't exist
 - AADSTS50126 -> Invalid password
 - AADSTS50076 or AADSTS50079 -> MFA response
 - AADSTS50057 -> Disabled account
 - AADSTS50055 -> Password expired.

MSOLSpray

- Uses Entra ID Error Codes to find out information about accounts
- Can find out if account has MFA enabled without triggering notifications
- Can use FireProx to rotate source IPs and avoid detection and lockout
- First released in 2020 by Penetration Tester Beau Bullock (MIT License).

> MSOLSpray

```
pwsh
pwsh #1
PS /Users/marco/AzureBootCamp> Invoke-MSOLSpray -Userlist ./users.txt -Password AzureBootCamp2024!
[*] There are 3 total users to spray.
[*] Now spraying Microsoft Online.
[*] Current date and time: 11/11/2024 11:11:11
[*] SUCCESS! test3@██████████.onmicrosoft.com : AzureBootCamp2024! - NOTE: The user's password is expired.
PS /Users/marco/AzureBootCamp> 
```

> Password Spray

How can you protect against this?

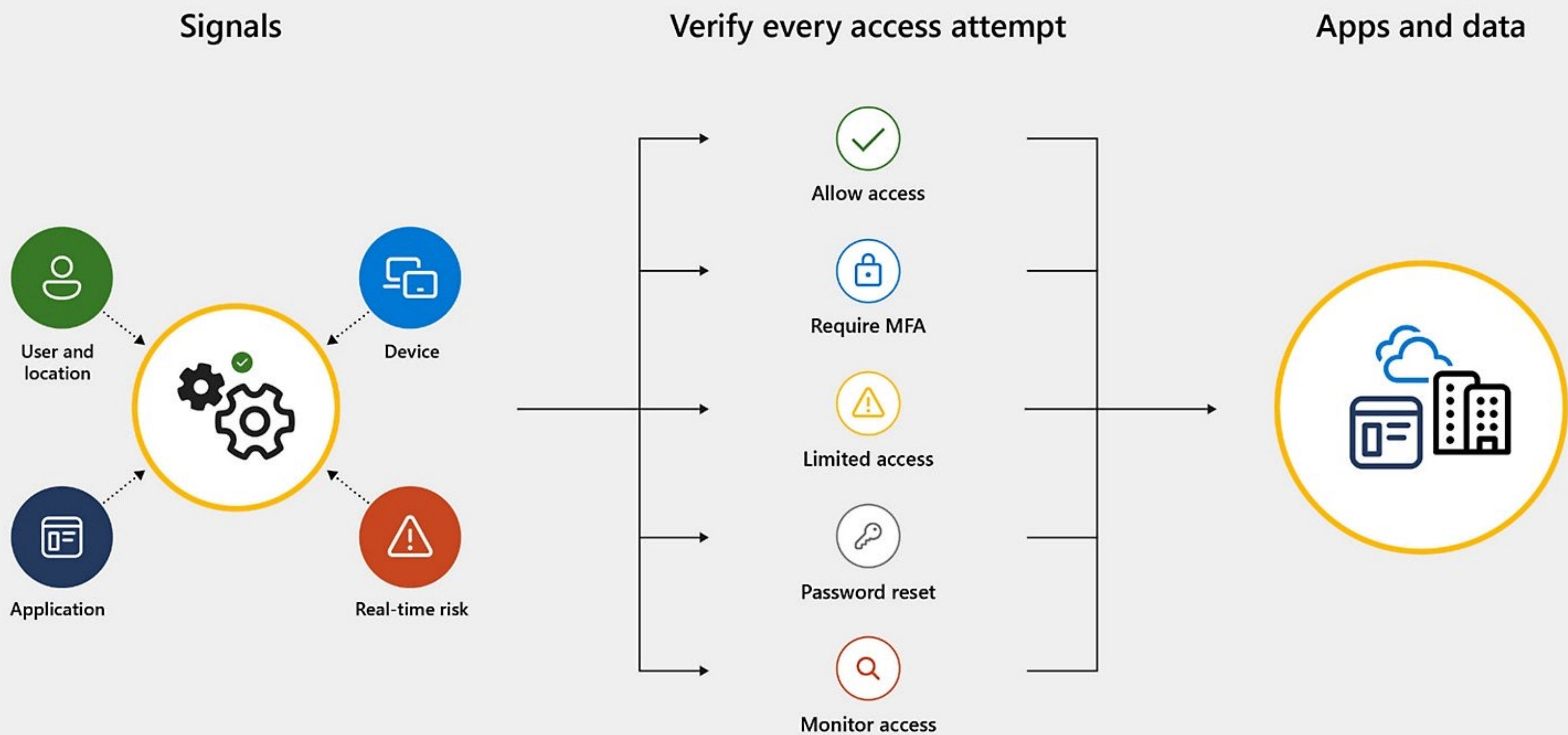
- Make users use strong Passwords
- Use Passwordless Authentication.





Result: Found password for Initial Access

Conditional Access Bypass

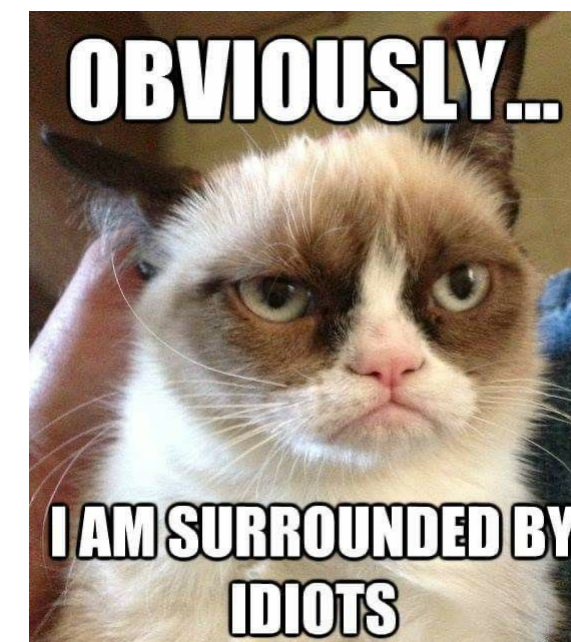


➤ Conditional Access Bypass

- Common Attack Vectors:
 - Location
 - Exclusion Group Abuse
 - Device Platform
 - MITM Attacks (e.g. with Evilginx)
 - MFA Bombing
 - Social Engineering
 - Etc.

➤ Conditional Access Bypass

- Common Attack Vectors:
 - Avoid Conditional Access completely by getting access to an excluded user!
 - Who is typically excluded?
 - BreakGlass Admins
 - Lazy Admins
 - Service Accounts
 - Angry Complaining Users



➤ Conditional Access Bypass

- Common Attack Vectors:
 - Location
 - Exclusion Group Abuse
 - Device Platform
 - MITM Attacks (e.g. with Evilginx)
 - MFA Bombing
 - Social Engineering
 - Etc.



Require MFA for all users

Conditional Access policy

 Delete  View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Require MFA for all users

Assignments

Users

[Specific users included](#)

Target resources

[All cloud apps](#)

Conditions

[1 condition selected](#)

Access controls

Grant

[1 control selected](#)

Session

Enable policy

Report-only **On** Off

Save

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk

[Not configured](#)

Sign-in risk

[Not configured](#)

Device platforms

[5 included](#)

Locations

[Not configured](#)

Client apps

[Not configured](#)

Filter for devices

[Not configured](#)

Device platforms



Apply policy to selected device platforms. [Learn more](#)

Configure

Yes

No

Include

Exclude

☐ Any device

☒ Select device platforms

☒ Android

☐ iOS

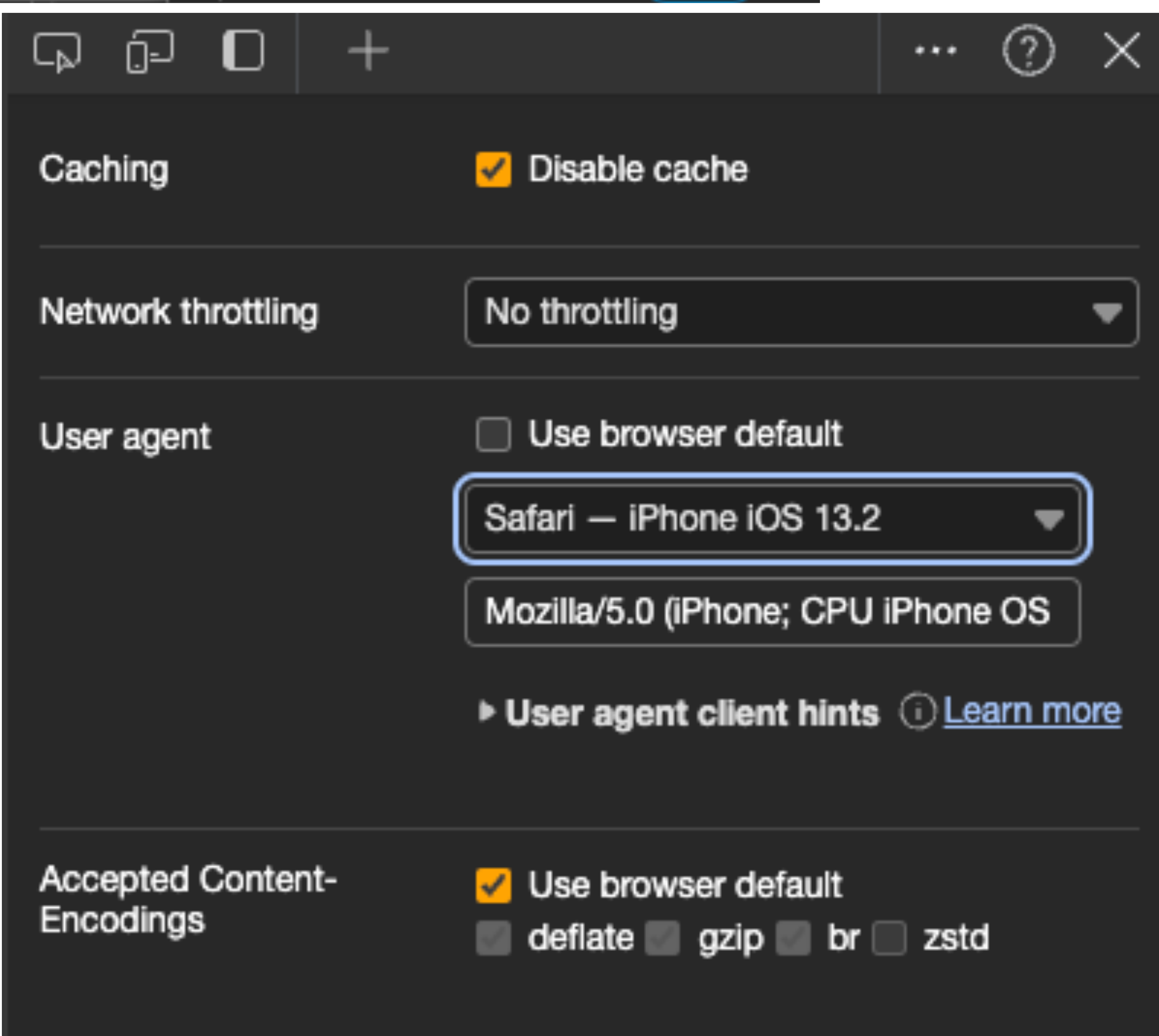
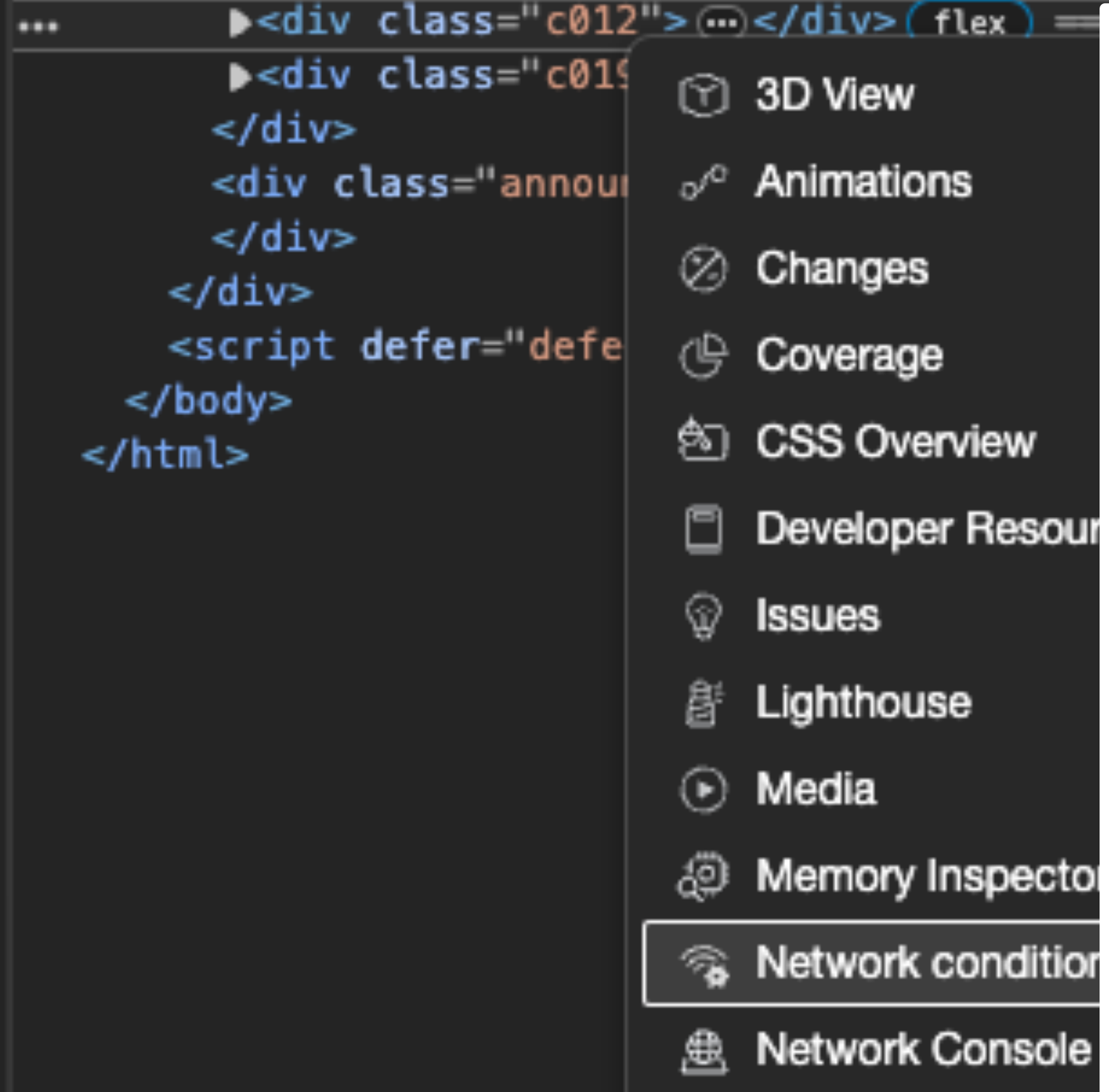
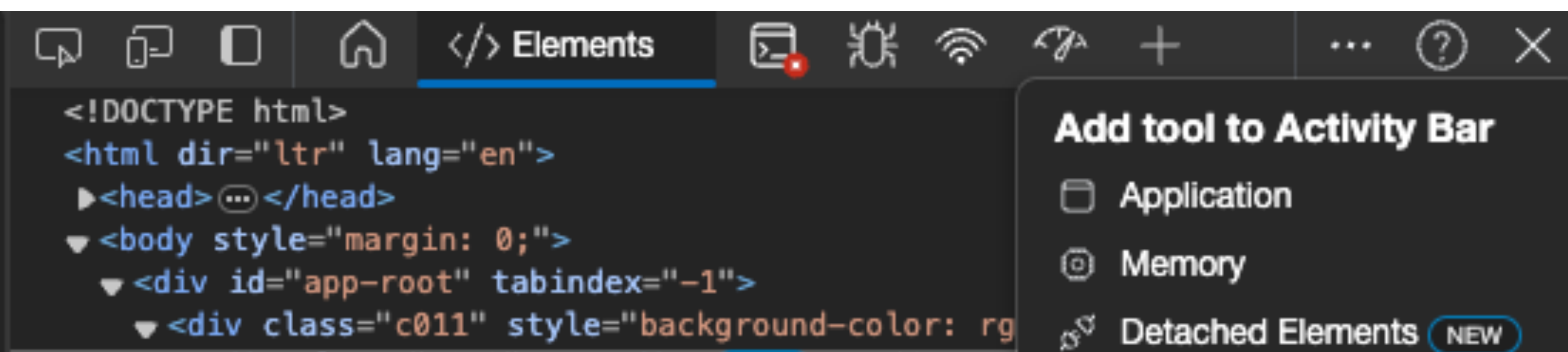
☒ Windows Phone

☒ Windows

☒ macOS

☒ Linux

Done



Conditional Access Bypass

How can you protect against this?

- Keep exclusion list as short as possible
- Create Block Rules to prevent access in unwanted scenarios
- Pay attention to conditions
- Use CA gap analyzer workbook



CA gap analyzer

Prereqs:

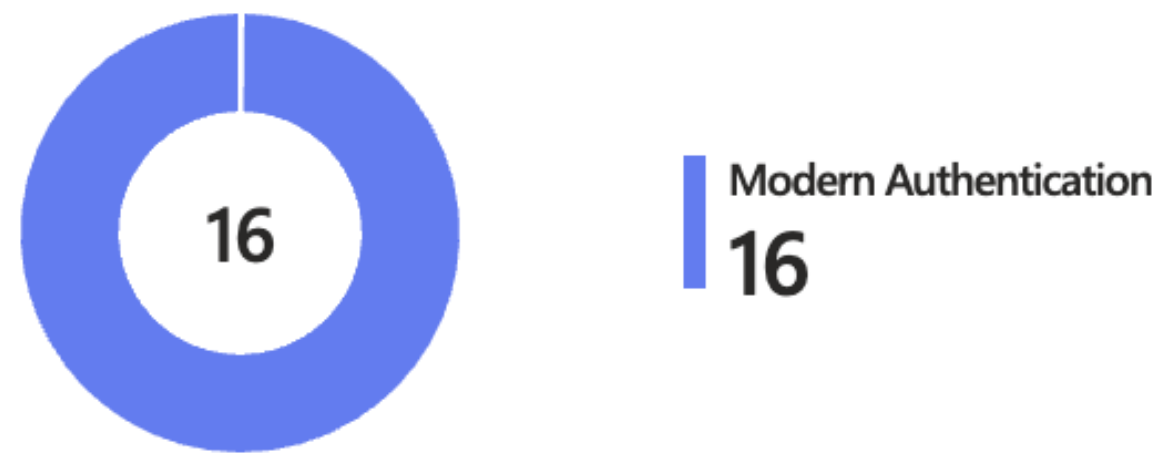
- Microsoft Entra Premium P1
- Log Analytics Workspace
- Role for Azure Monitor and Entra ID

Legacy Authentication

Microsoft recommends blocking sign-ins using legacy authentication

Click [here](#) to learn more about legacy authentication

Users Signing-In Using Legacy vs. Modern Authentication

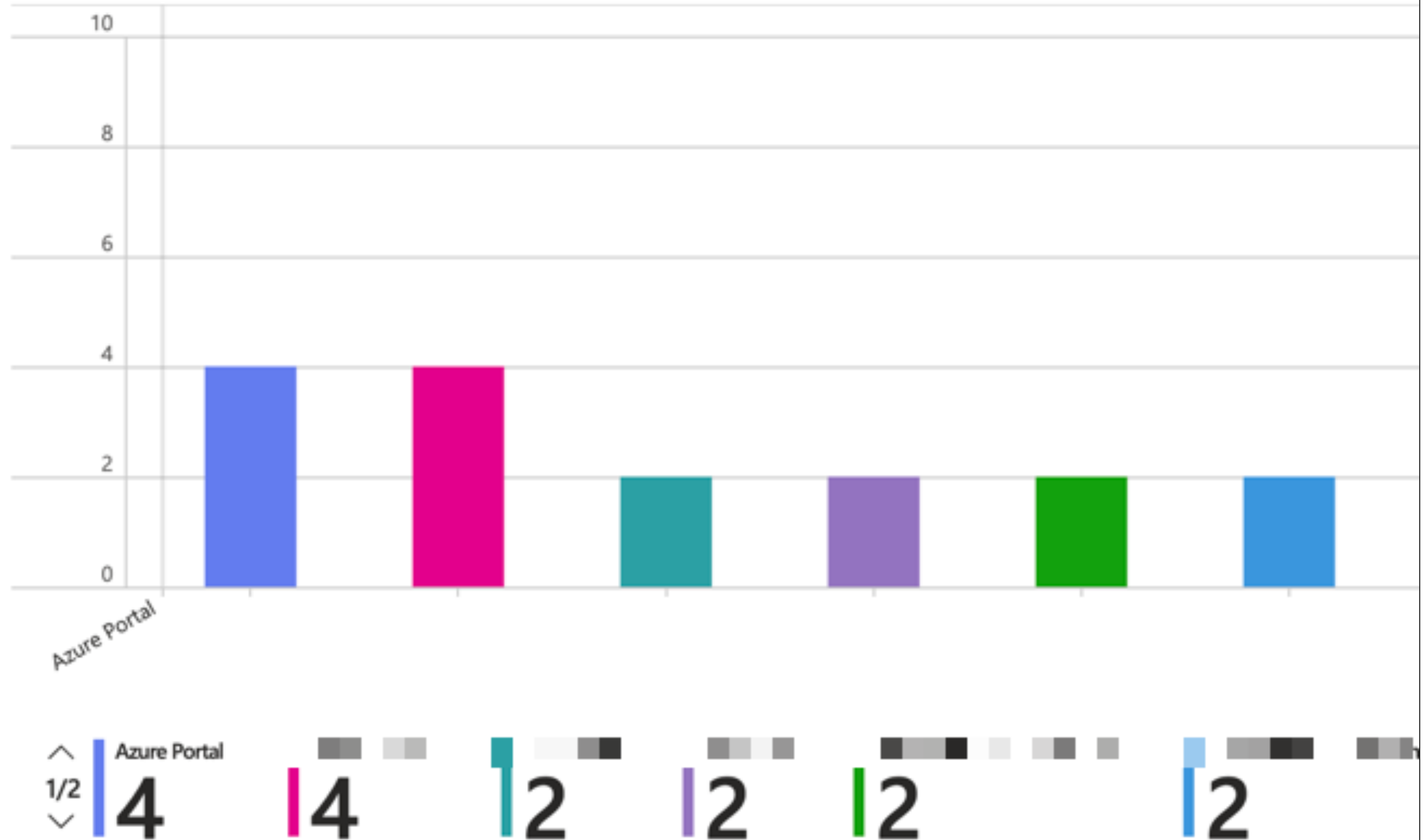


Users Using Legacy Authentication by Application

✓ No applications allowing legacy authentication sign-ins for the selected time range

Number of Users Signing In to Applications with Conditional Access Policies

Microsoft recommends that each sign-in to an application has a Conditional Access Policy applied to it.



High Risk Sign-In Events Bypassing Conditional Access Policies

Microsoft recommends blocking all high risk sign-in events, including sign-ins where the user account is known to be compromised.

Select a user for additional information



✓ No risky sign-ins without CA policies applied in this time frame

Users With No Conditional Access Coverage by Location



Switzerland

151

France

1

United States

1

CA gap analyzer

Preview Features:

- Named Locations with no Conditional Access Coverage
- Sign-ins from IPv6 addresses not assigned to a Named Location



Result: Bypassed Conditional Access Policies

> Demo Time



Hey Brokie Losers. Drop me a follow if you want to get rich! Sign up today at:

[@MadCashInc](#)



12:30 PM · May 16, 2024 · [Twitter for iPhone](#)

249m Retweets 98778bn Likes



Alex Wilber
bigwilby



> Entra ID Guest Accounts – Default

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☒ Guest users have limited access to properties and memberships of directory objects
- ☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- ☒ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ☐ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ☐ Only users assigned to specific admin roles can invite guest users
- ☐ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes

No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

Yes

No

Collaboration restrictions

⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. [Learn more.](#)

- ☒ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☐ Allow invitations only to the specified domains (most restrictive)

Guest user access

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

Collaboration restrictions

⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked.

- ☒ Allow invitations to be sent to any domain (most inclusive) <- **Default**
- ☐ Deny invitations to the specified domains
- ☐ Allow invitations only to the specified domains (most restrictive) <- **Recommended**

➤ Abusing Dynamic Groups

- Scenario:
 - Company has outsourced Azure VM Management to another company
 - The name of this fictional company is: VMGenius.io
 - All users are invited as Guest Users.

> Abusing Dynamic Groups

VMGenius-Users | Dynamic membership rules

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Applications

Licenses

Azure role assignments

Dynamic membership rules

<< Save Discard Got feedback?

Configure Rules

Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
And	<Choose a Property>	<Choose an Operator>	Add a value

+ Add expression

+ Get custom extension properties

Some items could not be displayed in the rule builder. [Learn more](#)

Rule syntax

user.userPrincipalName -contains "vmgenius.io"

Group has Virtual Machine Contributor Role

> Abusing Dynamic Groups

Rule syntax

```
user.userName -contains "vmgenius.io"
```

Group has Virtual Machine Contributor Role

> Abusing Dynamic Groups

Basic info



vmGenius

vmgenius.io@gxscmaoutlook.onmicrosoft.com

Member

> Abusing Dynamic Groups

How can you protect against this?

- Don't allow all users to invite guest accounts
- Don't base dynamic group membership rules on user-controlled attributes
- Be aware that even non-user controlled attributes could be changed somehow (e.g. from Entra ID Cloud Sync)
- Be careful when designing dynamic group membership rules.





Result: Escalation to privileged role

➤ **Abusing VM Contributor Role**

- It is a privileged Role
- It can execute Scripts on VM with SYSTEM Privileges
- Abusing Examples:
 - Extract NTLM Hashes from VMs
 - Install Malware on Systems
 - Extract Information from File Servers
 - Elevate Privileges from Cloud-only to onPrem
- RL Example:
 - TA UNC3944 uses Serial Console to deploy remote management software





-> Find Passwords

-> User Enumeration

-> Password Spray

-> Conditional Access Bypass

-> Abusing Dynamic Groups

-> Abusing VM
Contributor Role

➤ Conclusion

- Be careful when exposing information publicly
- Use built-in protection features from Microsoft
- Look at configurations from an attackers perspective
- Keep an eye on you CA Policies and Dynamic Groups
- Don't be lazy! (at least in Cyber Security 😊)

Description	Link
GitHub of Beau Bullock (Azure Pentesting Tools)	https://github.com/dafthack
MicroBurst Toolkit for Attacking Azure	https://github.com/NetSPI/MicroBurst
Website of AADInternals	https://aadinternals.com
Hands-on Azure Pentesting Training	https://cloudbreach.io/breachingazure
Microsoft Penetration Testing Rules of Engagement	https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement
VM Contributor Role Abuse RL Example	https://www.csoonline.com/article/575297/attacker-uses-the-azure-serial-console-to-gain-access-to-microsoft-vm.html
Video about Passkeys from John Savill	PASSKEYS - What they are, why we want them and how to use them! (youtube.com)



Marco Schmidt
marco@thesecurityguy.ch
thesecurityguy.ch



Manuel Meyer
blog@manuelmeyer.net
manuelmeyer.net