Demystifying the Arcane of Lateral Movement between Azure & On-Prem AD

CYCRAFT

Echo Lee

- Cyber Security Researcher @ Cycraft
- Spoke at CyberSec

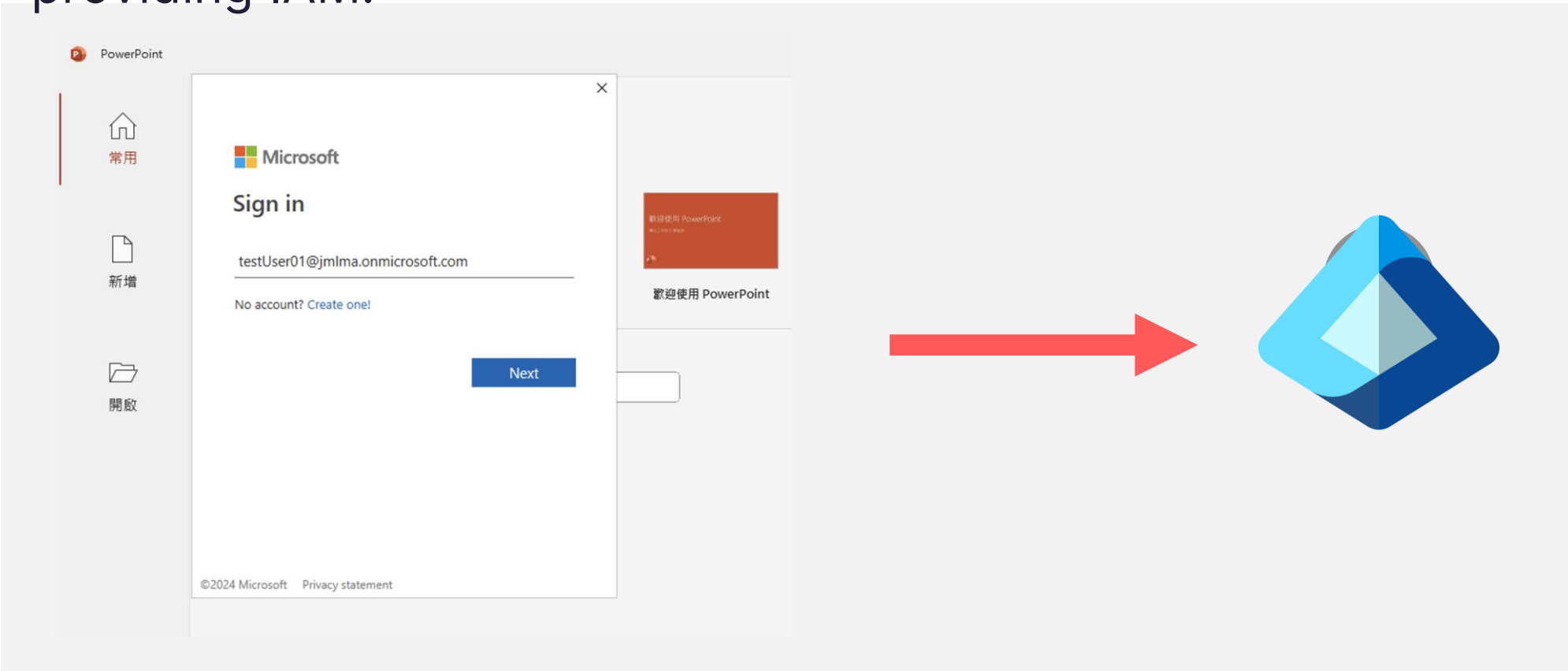
Jimmy Su (Contributor)

- Cyber Security Researcher @ Cycraft
- Spoke at SECCON, CyberSec

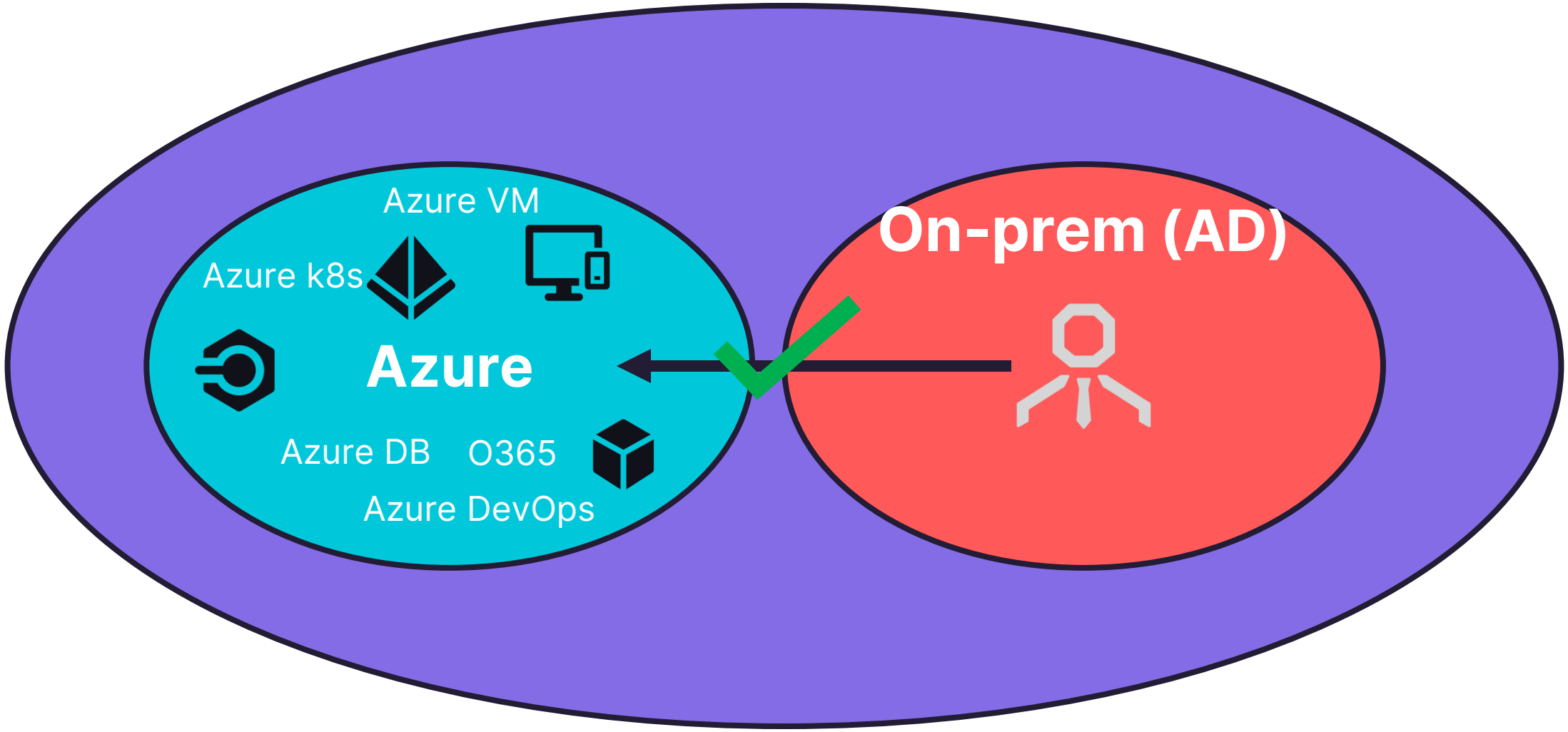
Attacking from On-Prem to Azure

What is Entra ID?

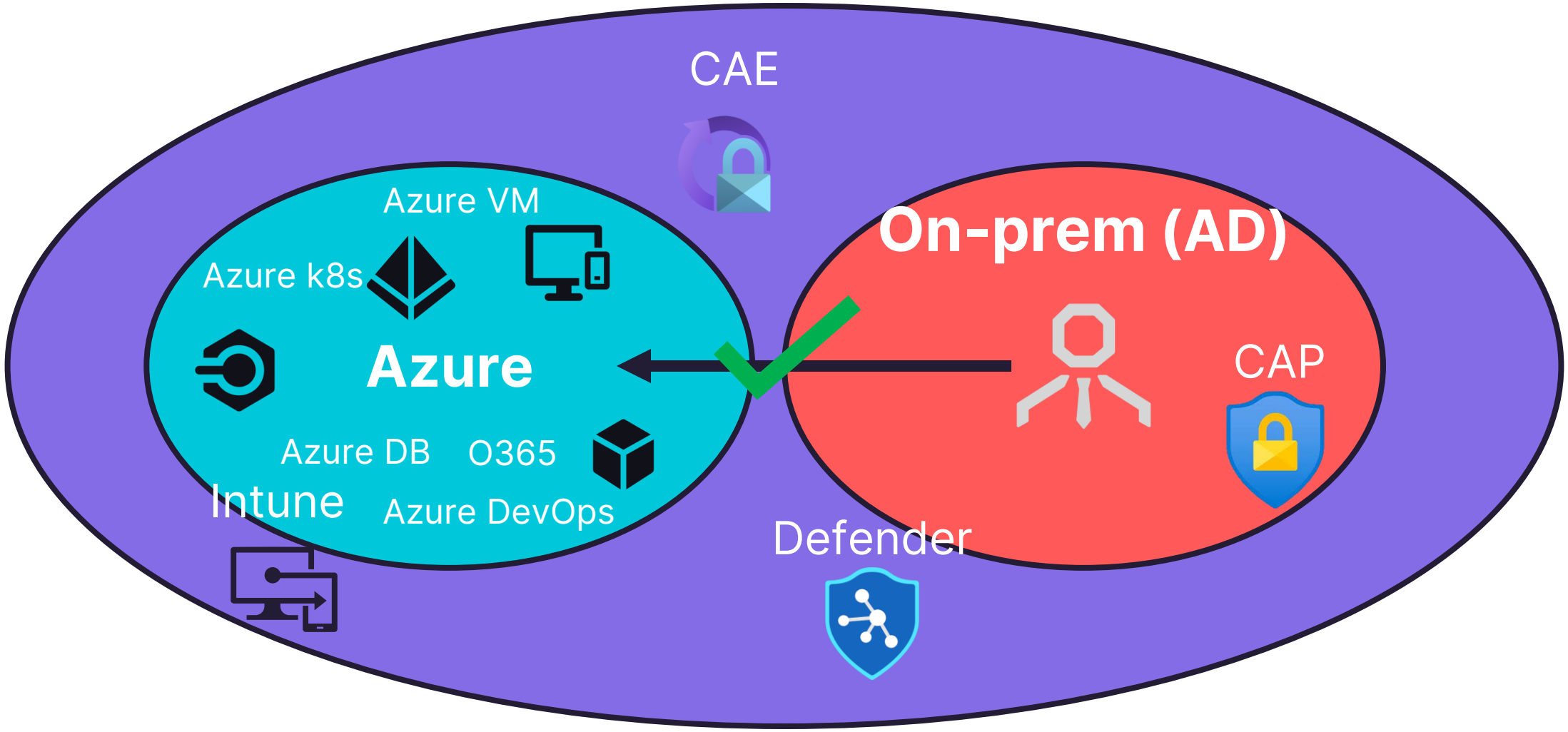
- Entra ID, formerly known as Azure AD, is Azure's resource for providing IAM.



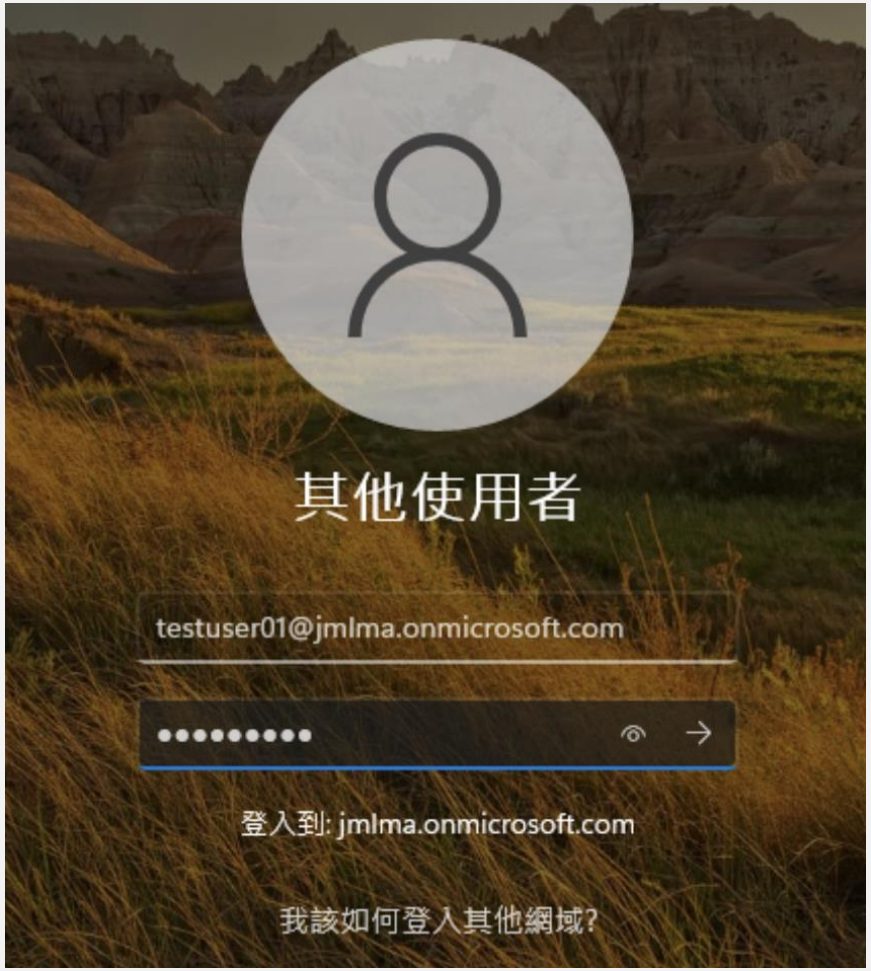
Hybrid Identity



Hybrid Identity

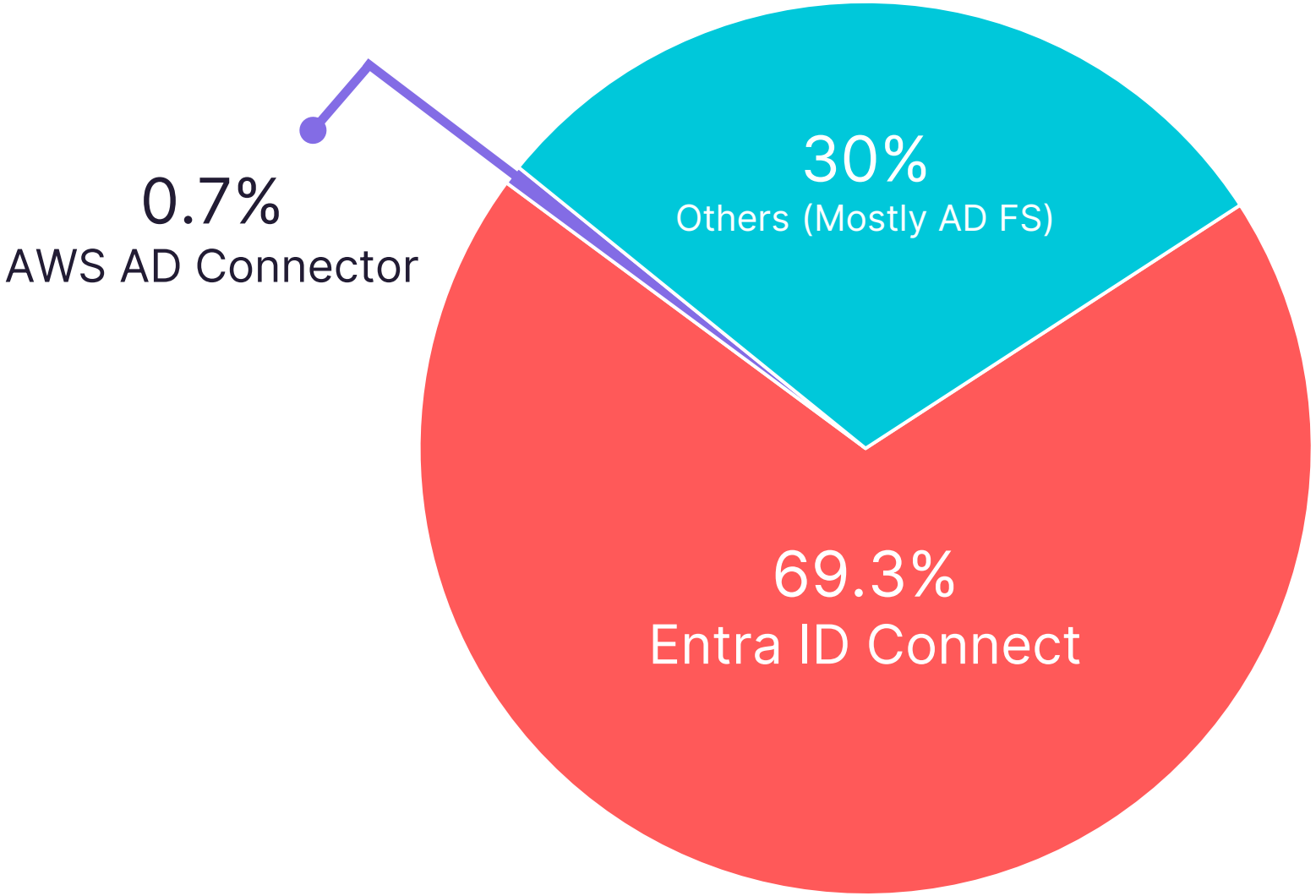


SSO login to cloud resources



After logging on to the local computer SSO to Cloud Resources

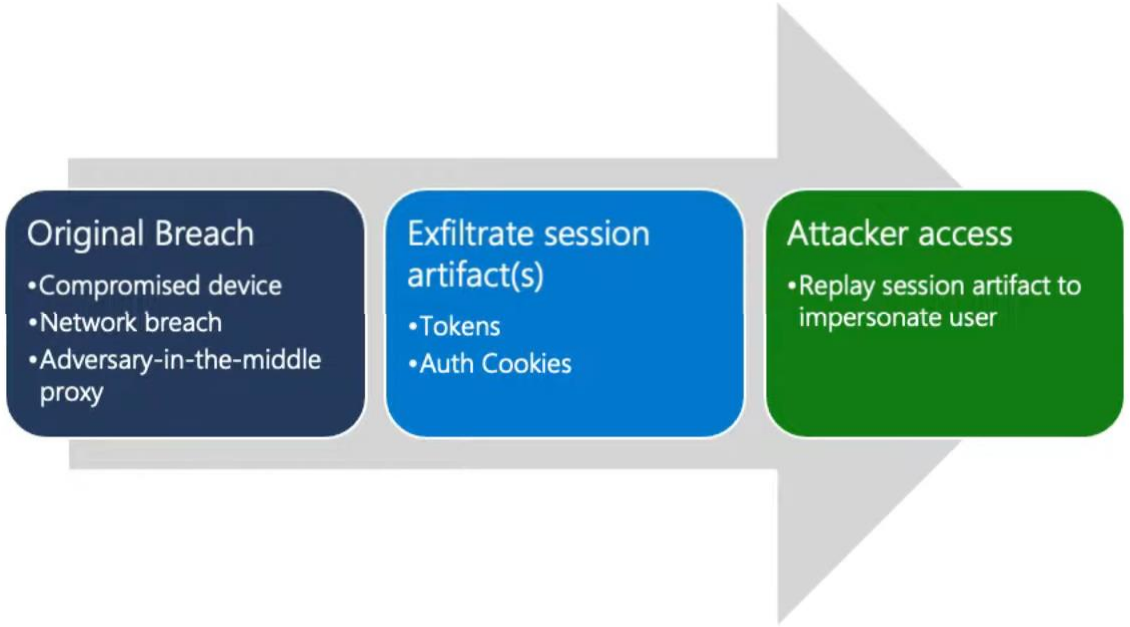
Proportion of Hybrid Identity



As former Facebook CSO Stamos – who admittedly has some skin in the game in his role for Microsoft Security rival SentinelOne – noted on LinkedIn: "AzureAD is overly complex, and lacks a UX that allows for administrators to easily understand the web of security relationships and dependencies that attackers are becoming accustomed to exploiting. In many organizations, AzureAD is deployed in hybrid mode, which combines the vulnerability of cloud (external password sprays) and on-premise (NTLM, mimikatz) identity technologies in a combination that smart attackers utilize to bounce between domains, escalate privilege and establish persistence.

ref.: https://www.thestack.technology/how-russia-hacked-microsoft-ms-graph/

Token replay attacks

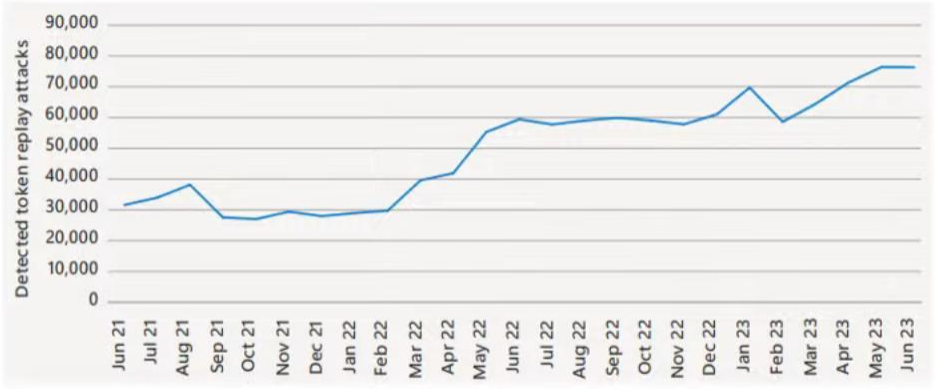


Still relatively rare

- Less than 3% of all identity compromises
- 11 detections per 100k active users (0.01%)

But growing…

- ~75k token replay attacks in June 23
- 100% increase YoY

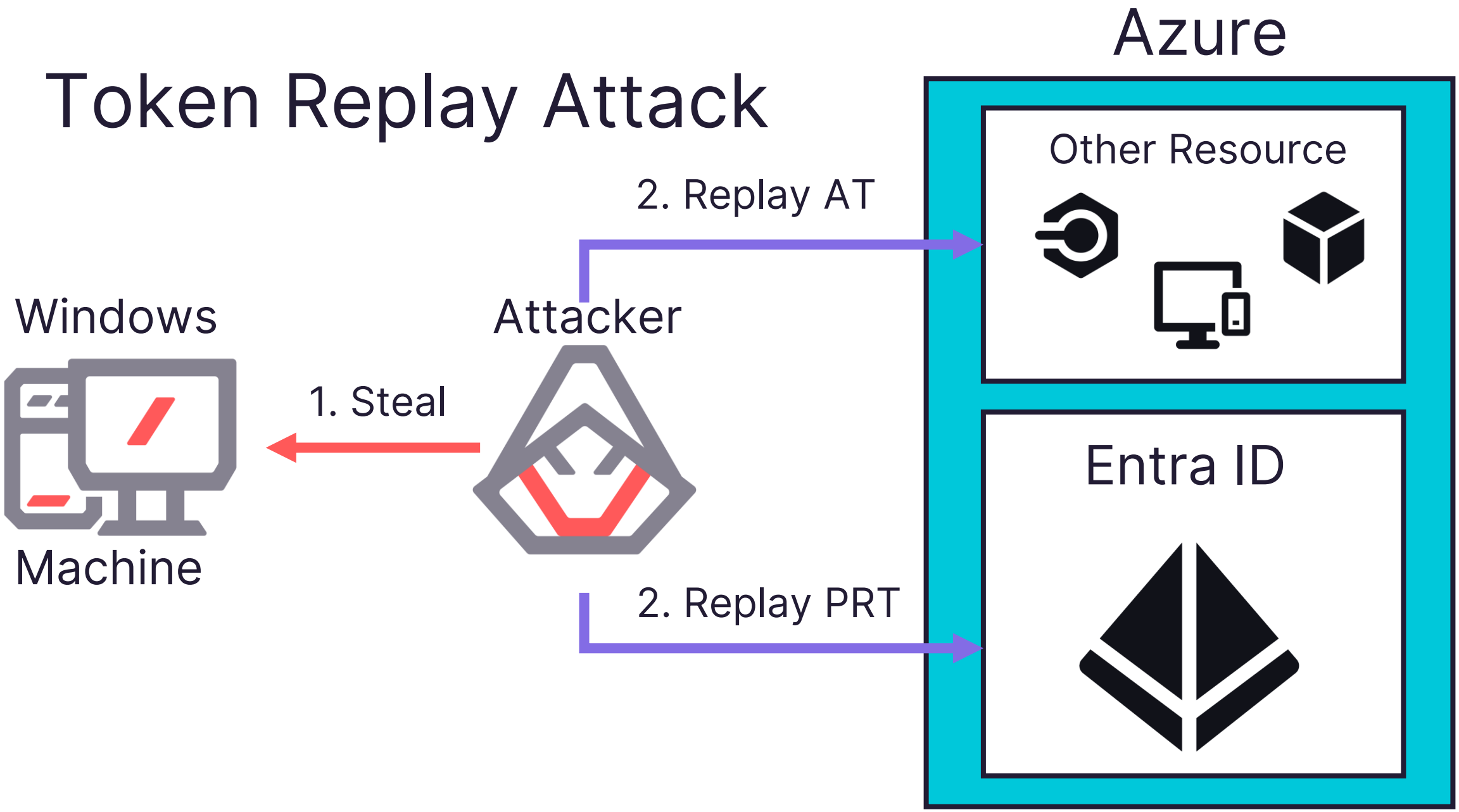


Source : Microsoft Digital Defense Report 2023 (MDDR) | Microsoft Security Insider

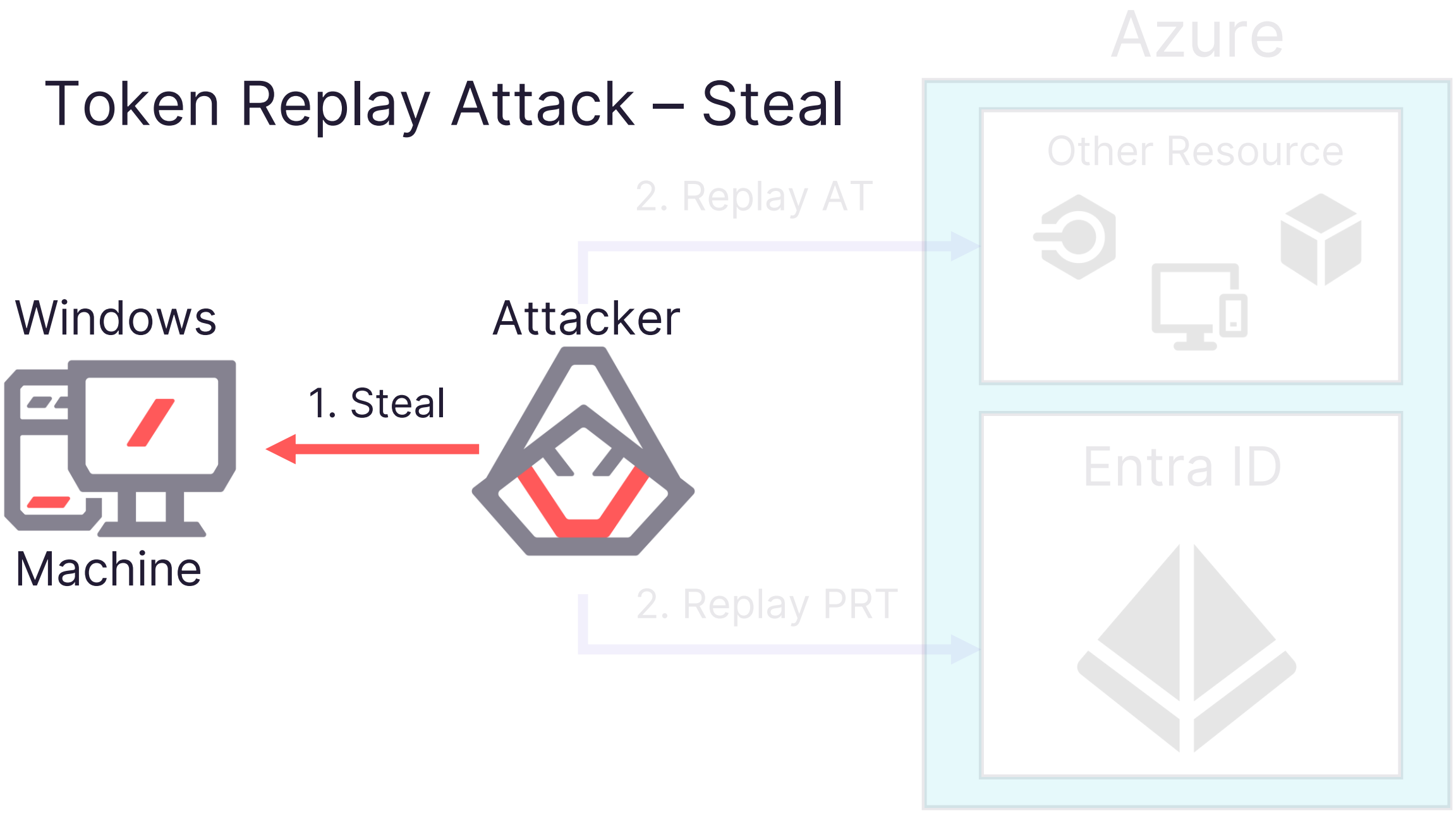
Entra ID Protection data

ref.:https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

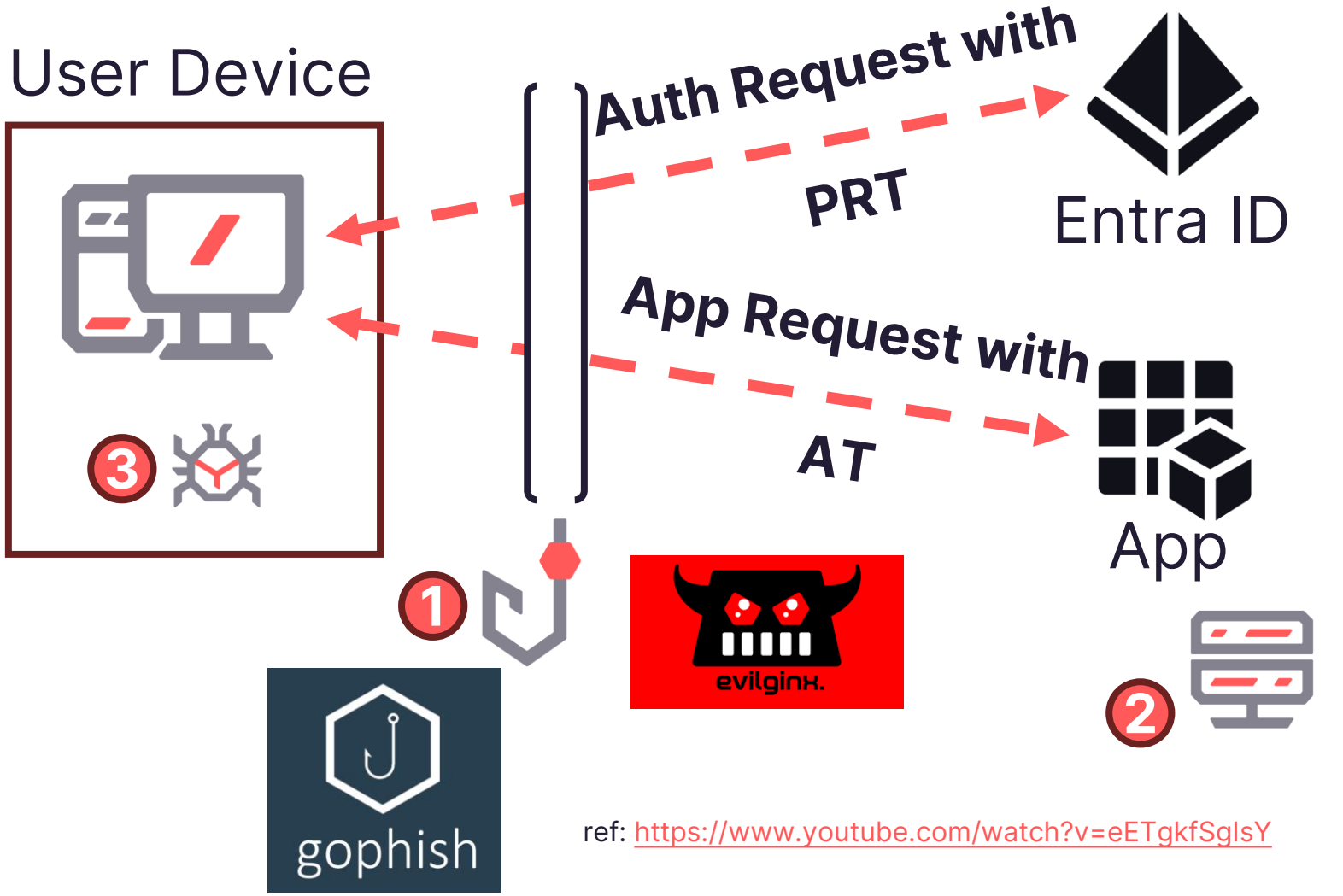
Token Replay Attack



Token Replay Attack – Steal



Token Replay Attack – Steal

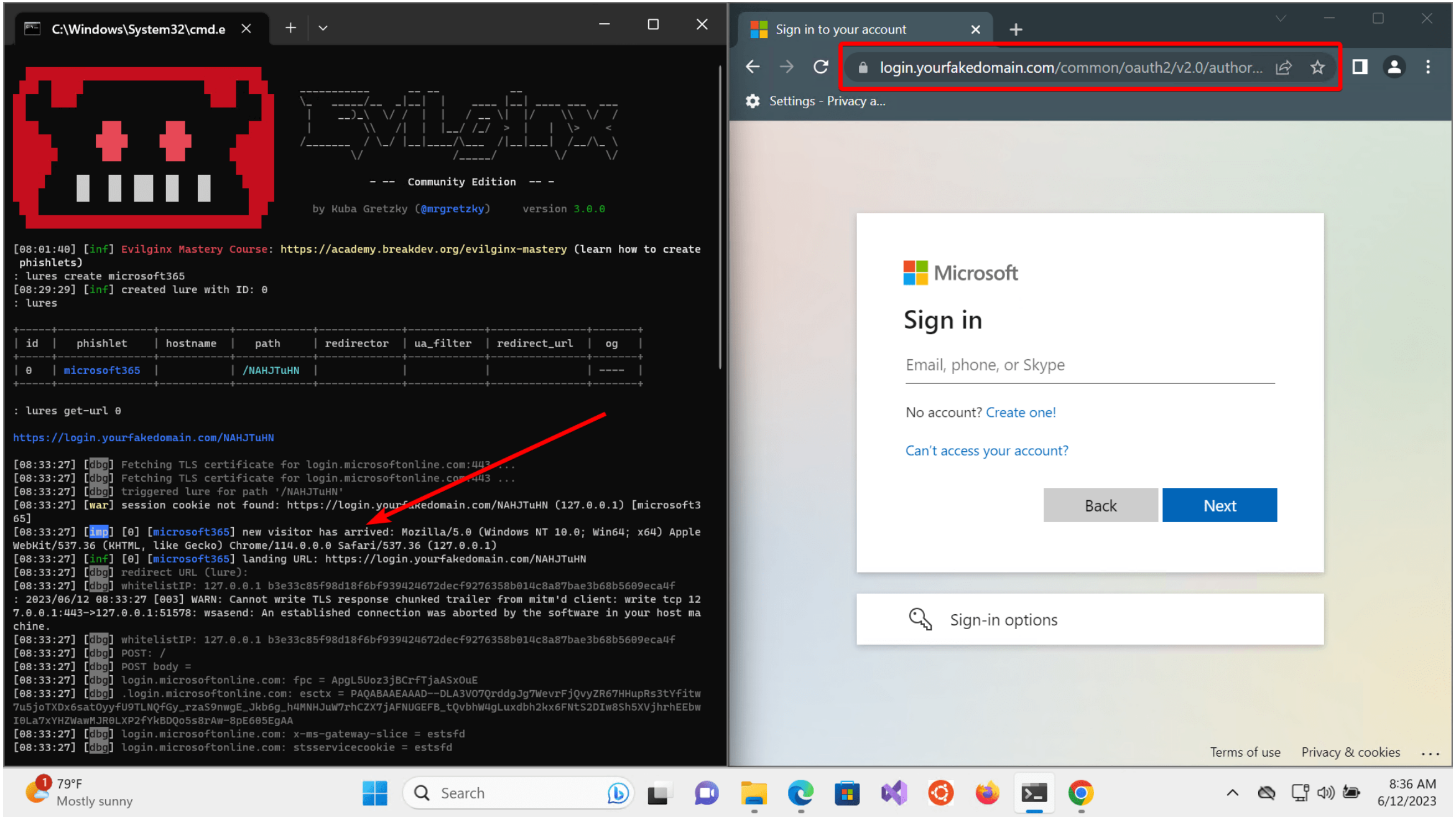


> AiTM

> Extract tokens from breached server logs

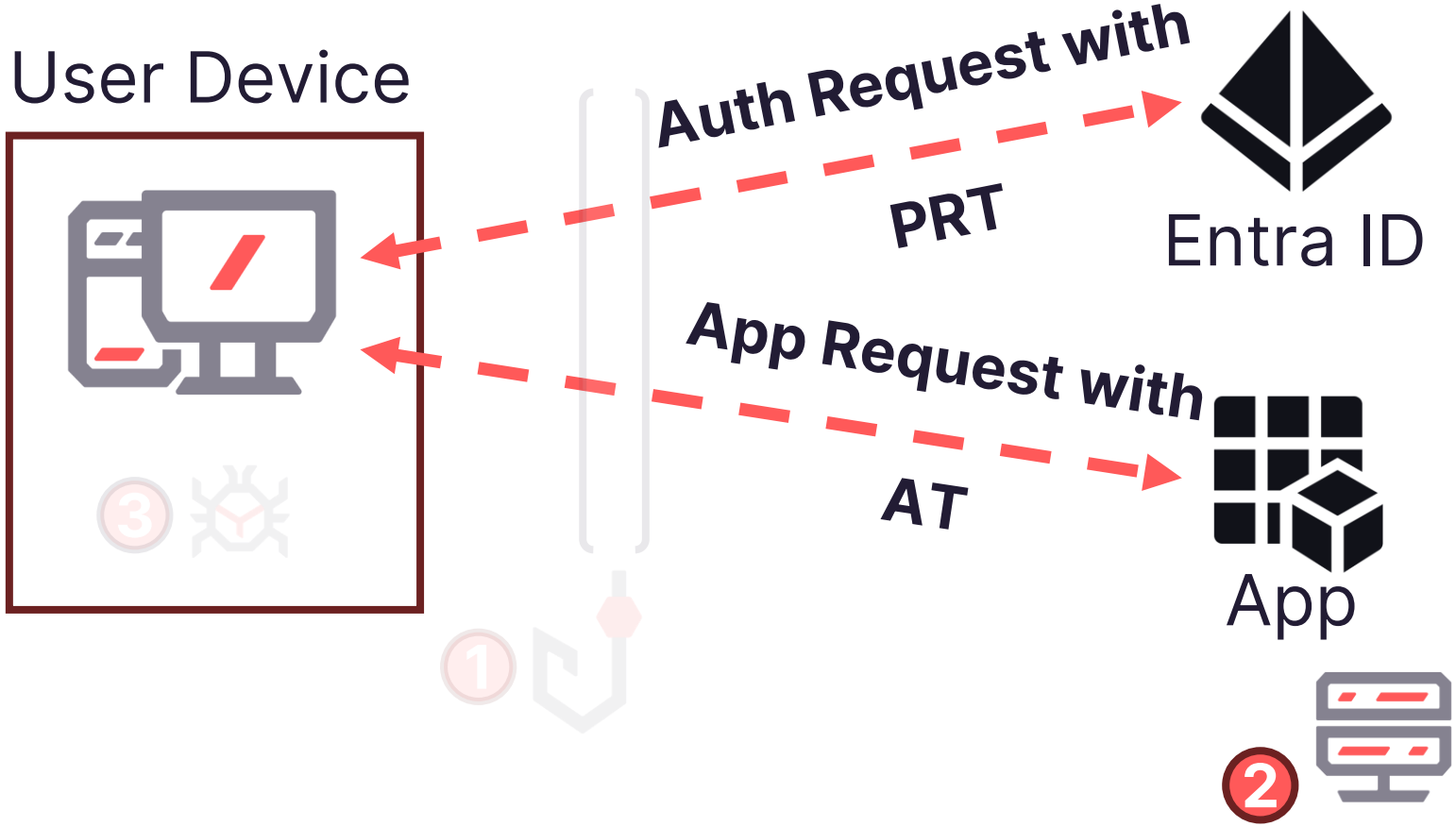
> Software inside device

ref: https://www.youtube.com/watch?v=eETgkfSgIsY



ref: https://janbakker.tech/running-evilginx-3-0-on-windows/

Token Replay Attack – Steal



> AiTM

> **Extract tokens from breached server logs**

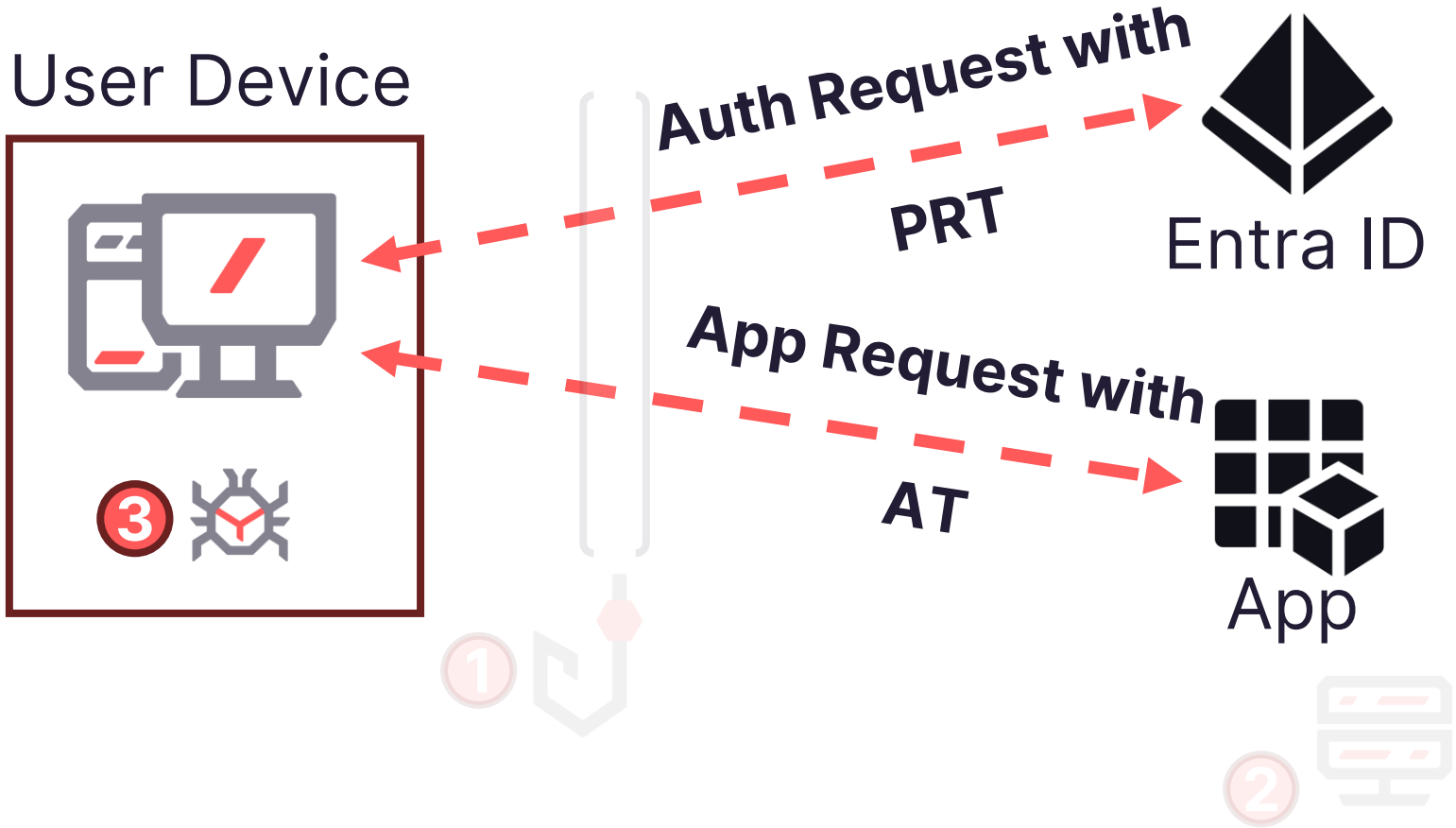
> Software inside device

ref: https://www.youtube.com/watch?v=eETgkfSgIsY

Extract tokens from breached server logs

- Threats that have been patched
  - az cli、Az PowerShell
  - LeakyCLI (CVE-2023-36052)
- Easily misconfigured
  - Hardcore token in pipeline
  - CI/CD Server log

Token Replay Attack – Steal



> AiTM

> Extract tokens from breached server logs

> **Software inside device**

ref: https://www.youtube.com/watch?v=eETgkfSgIsY

Software inside device –

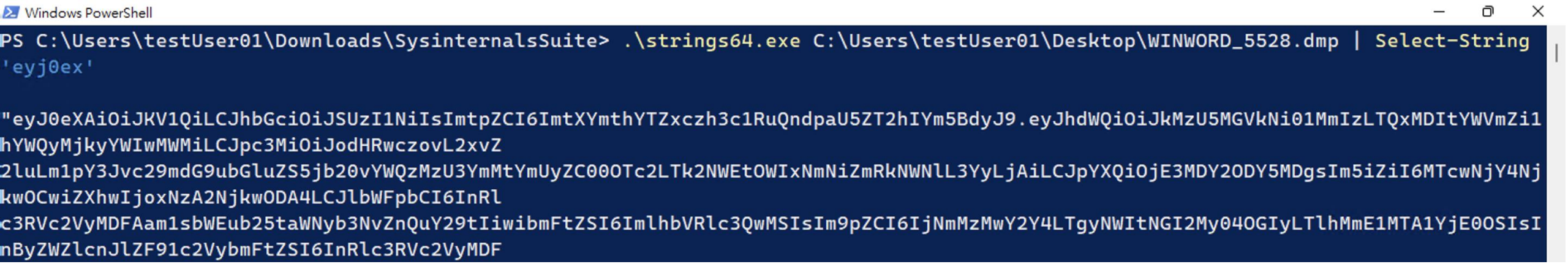
- Unlogged out of Azure Management Tools
  - az cli
  - Az PowerShell
  - ...
- attacker could directly steal the user's Access Token.

Software inside device

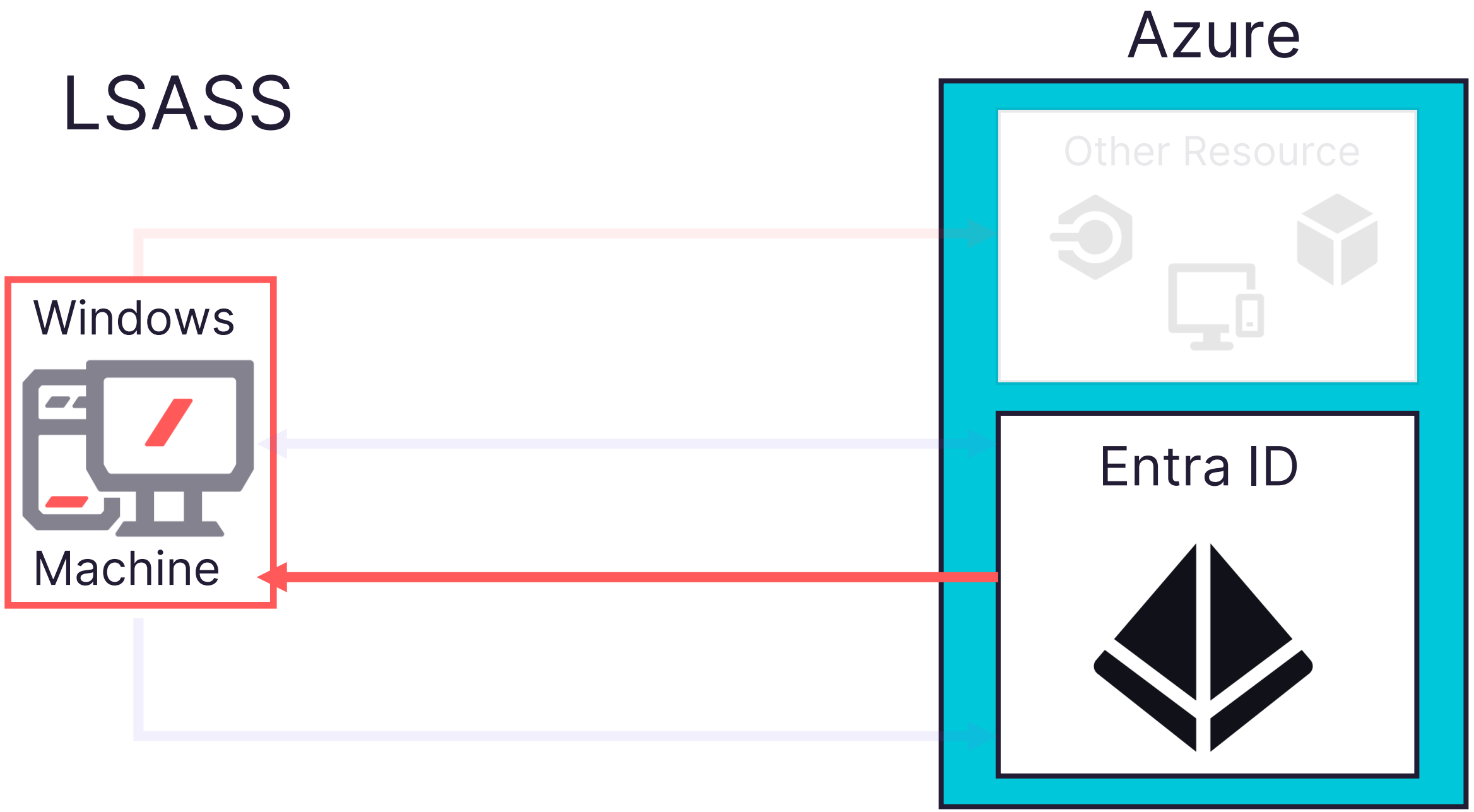
- Access Token (AT)
  - Unlogged out of Azure Management Tools
    - az cli
    - Azure PowerShell Module
  - Office 365
    - Outlook
    - PowerPoint
  - …
- Primary Refresh Token (PRT)
  - LSASS (mimikatz)
  - BrowserCore.exe (ROADToken)

O365 Application

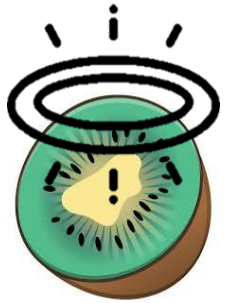
- The Office 365 application memory on your computer stores plaintext Access token



LSASS



LSASS

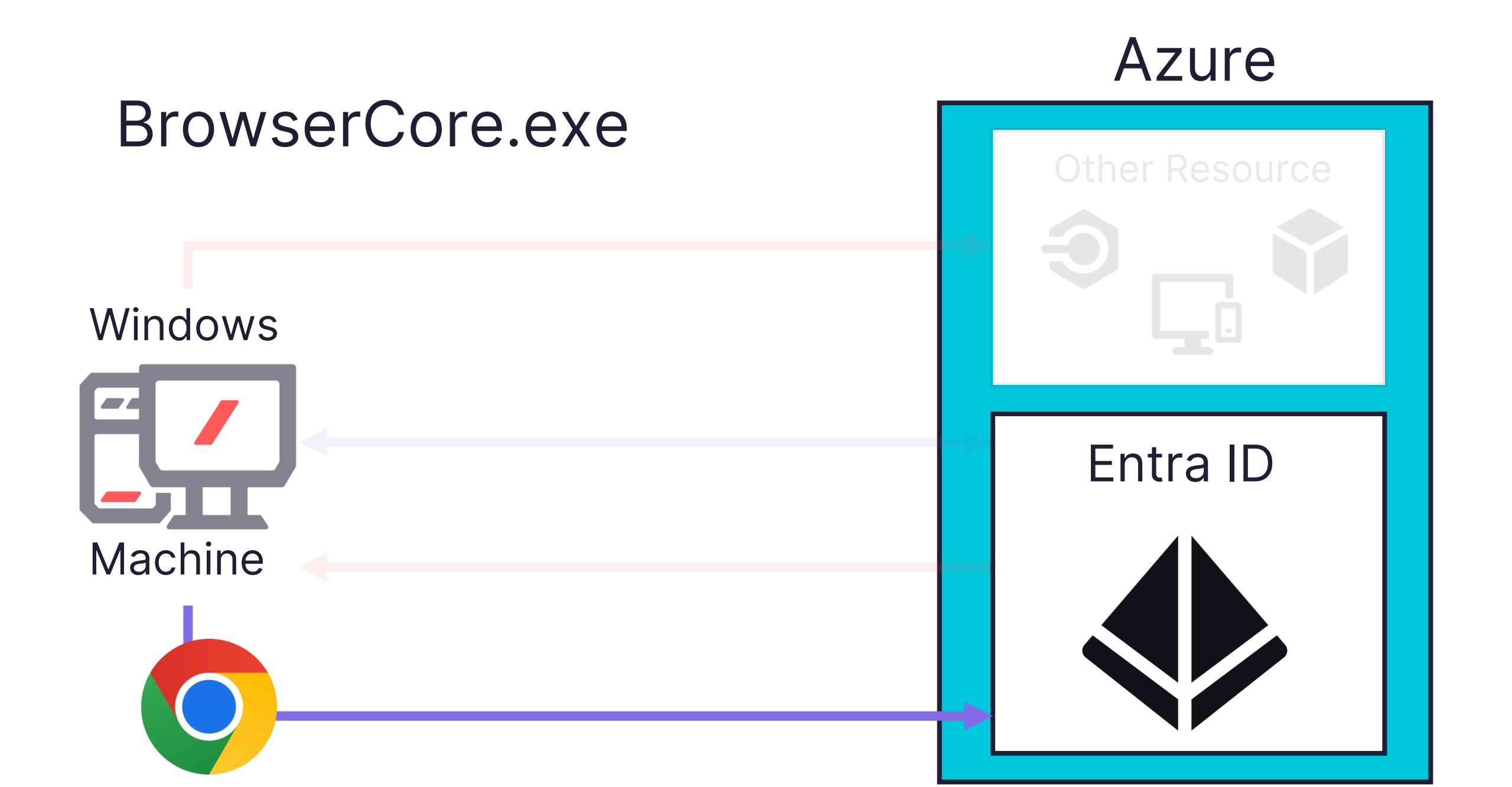


- Microsoft patched the PRT memory location and changed the algorithm in an update, and since then mimikatz can no longer retrieve PRT in an environment with TPM.

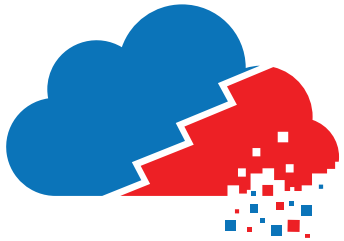
```
Signature with key:
eyJhbGciOiJIUzI1NiIsICJjdHgiOiJIVWttRkFrb2VcL1VFQTlsOHoxdXJKV0R6MlhvcFJYOTUifQ.eyJyZWZyZXNoX3Rva2VuIjo
hVYktDZHBjVXlGYllKLVJPN3JFb2M3cWpodG9CZElzblY2TVdtSTJUczNBTlkuQVFBQkFBQUFBQUFHVl9idjIxb1FRNFJPcWgwXzEt
IOVZKX2N2QVlKVUx1d1RWWTYxaFlZX1FzQWdxUXVib2hwRmk4a0FWNENZUDZfYkl0czJDTWVnOHM4clk5VDRHY3FxaFFkeVRsT1hIV
NzVsMjhhMlUzWGRNemNaVVhMZ2xPYTVqNldvWUl2VDExaXVwY0xKbW9tNU1DcUNuUC1pdWdpemdweEdsZk55Qm9YR0UzVFB2a29hZE
DRCYUNUNktrUXVtYkx0XzZBbmlTYjlGTFZqbDFDbjFzMGEwSzZ0WHlwRGpqMmpSNkdLdkY2RTMtd1FacTNzQkF3UnRyOHZqT0dNMXF
RsVVRudUwxdXZmVzRYSFNZdS0wRXFtaHdKUVBFQUFnR3c3ajMwdmtScDA5bWlyd2NnQXM2MWJSdWFYbFRKM0VqenBrc3kydE9IcURV
teENDZ0RvLXVueHhiLXpjRHBmYnQ3eUpHUlJSOGVhWk4wZWRHaERnUWVxVkVER0g0b2Q4dlRMMkxzYjRyZ3h4NEt5NUpzYUs1V3lBW
Q0Y5RE5GOWlXXzRqNXF3dm5Xb1FpQWVkTEpfTVp1VDJpR3htSXN5NkE0Q2tZTWJNLW9JVDFJNUo0NGxllVc1bXdrakJMNmFDM1J5ZF
WdKNWU5M2dRVmJJcUN2N2NUTW9UdW9RUlZZQmx3TUIydlcxWW02anNBVExBRVlKSkliLXZhT1d1T3kwemdHTVBqRzBobWtUOWE1dGt
VPUTY3YVNGQ2QzeUIwSTFDZkU4dzJpZVg0V0U4RmZKM1FhVFdWNkpDTzNTQ0Q1RnZCc2xZVWdiaFl5UUR4blN5Fh5OTEyaVRIcW5X
6b3JqZGtMclNqSHVFaFlaZHNyUWQzX0FGNWFHZ0l1RzA4R2U5blBjUjViYlY3UHhSRGR0MGhrc1FLUVNqMFlEbDZrWTA3bFRENWNKV
WjFIand2NXdRRzRBVHFZRmd5eHgwUkRsekVBMmhIdWZIS0JOUXB3ME9taW9FeWpQOUV3M216VVlFbm1GdXVwZU50ZjVld04xcVk5SH
0JLS1dpV0RyWU1UOXBJM2tnNzdBUGZJR2REbjItcDJhcGpEdFBGbDljRWtPS3ljcDB4VS1ST3JkY1MtS2Z1M0JxTjY2VU5NQ1JFTTR
ExNmo4VktXUFFOOUMyNXJGZmFQN1ZxeDNZalRMY24xenlpUWlVc0tHRjdVLTdQTjJHZElUZmpmTXBQRjdvUlpHVXVDeURGcGNkSDJf
qUGR0R1hPalNJUWdSN3ptRGFTbXdEVE9DejJidGN6MXNxUlB4SFFINGR3WFBOQnNWYXNqRGZXb2paLTNKR3I2b0VyaG5sY0tlMk1lY
Sks1MWxYMkFpT2U4MXFMelJKdHdqMmJTeHMwa0NwUWg0aGdkWmtNRUY5SWN1akRob0psdENNVDRldzZpODJmTkNaTEhMVWFvUlg1cm
3hqUVg4S3dlMEZOdWE5eTYzLWxCT3Fwd3Q2M211MHphYVRPRnFQZmlZSEhHQzA2d3pjSlk3eHRndUcyeXltVVNBYkIySDIwRzdiRy1
SyYUZPNmJyUTVabmJDcjJrbzVBOGVEQk15ZVRPOFpHYVVEaW9mOVhSdmVkSzhnQUEiLCAiaXNfcHJpbWFyeSI6InRydWUiLCAiaWF0
```

ref: https://cloud.hacktricks.xyz/pentesting-cloud/azure-security/az-lateral-movement-cloud-on-prem/pass-the-prt

BrowserCore.exe



BrowserCore.exe



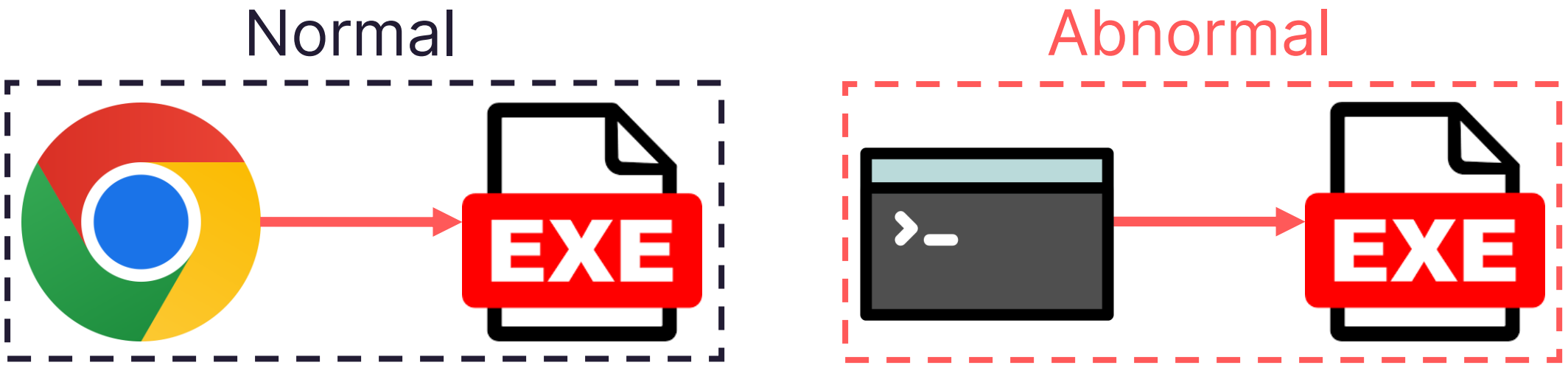
- Simulate how BrowserCore.exe communicates with Azure to get PRT through ROADToken.

```
PS C:\Users\yubi\Desktop> .\ROADToken.exe AQABAAAAAAB2UyzwtQEKR7-rWbgdcBZI2ISVwAlvcRIt1ge79PVA7sEpm_0rPkvztsBzCkJv0DCHWF
AutTVY9GBekAzXWsQkwDLgSGWhLB6-U-BSDOsNGSAA
Using nonce AQABAAAAAAB2UyzwtQEKR7-rWbgdcBZI2ISVwAlvcRIt1ge79PVA7sEpm_0rPkvztsBzCkJv0DCHWFAutTVY9GBekAzXWsQkwDLgSGWhLB6-
U-BSDOsNGSAA supplied on command line
,         { "response": [{ "name": "x-ms-RefreshTokenCredential", "data": "eyJhbGciOiJIUzI1NiIsICJjdHgiOiJKMlZUWlNCTjhJV
Dd5Yk1iWnQ0WXR4T3VWXC9MYzQrV2sifQ.eyJyZWZyZXNoX3Rva2VuIjoiMC5BQUFBal9LSFluOVBJa09XVWFocGZZX2h2SWM3cWpodG9CZElzblY2TVdtST
JUdDBBSDguQWdBQkFBQUFBQUIyVXl6d3RRRUtSNy1yV2JnZGNCWklBUURzX3dJQTlQOTVhRUdRa3hSVlZKS1dOSE9RbmlBOEd2eVNtM1VCR0UtYm5wN2wzRX
JnYktHbVVlT3VQTjNDRVB3Y0JUaXBBZmdwbG1nMUk1MkRUVE02U0M0YW1qejRLTmtuY1NaMUJyUmFtNHh2X0Q0amNEY1RBWTVSWUFiN3haQy11aHk4Y2lMVX
NFSzE0TmxEcmppdWpkQVFKLTNZSm12dnJqdTV6Q0djOXJsZDJ6bWYzMG8xNHVkYnhlQjhjNW5sbFFSRVBjZHdRMFY2c2dWSnE5VHYwanZnZnRGbFhBX0kxYX
```

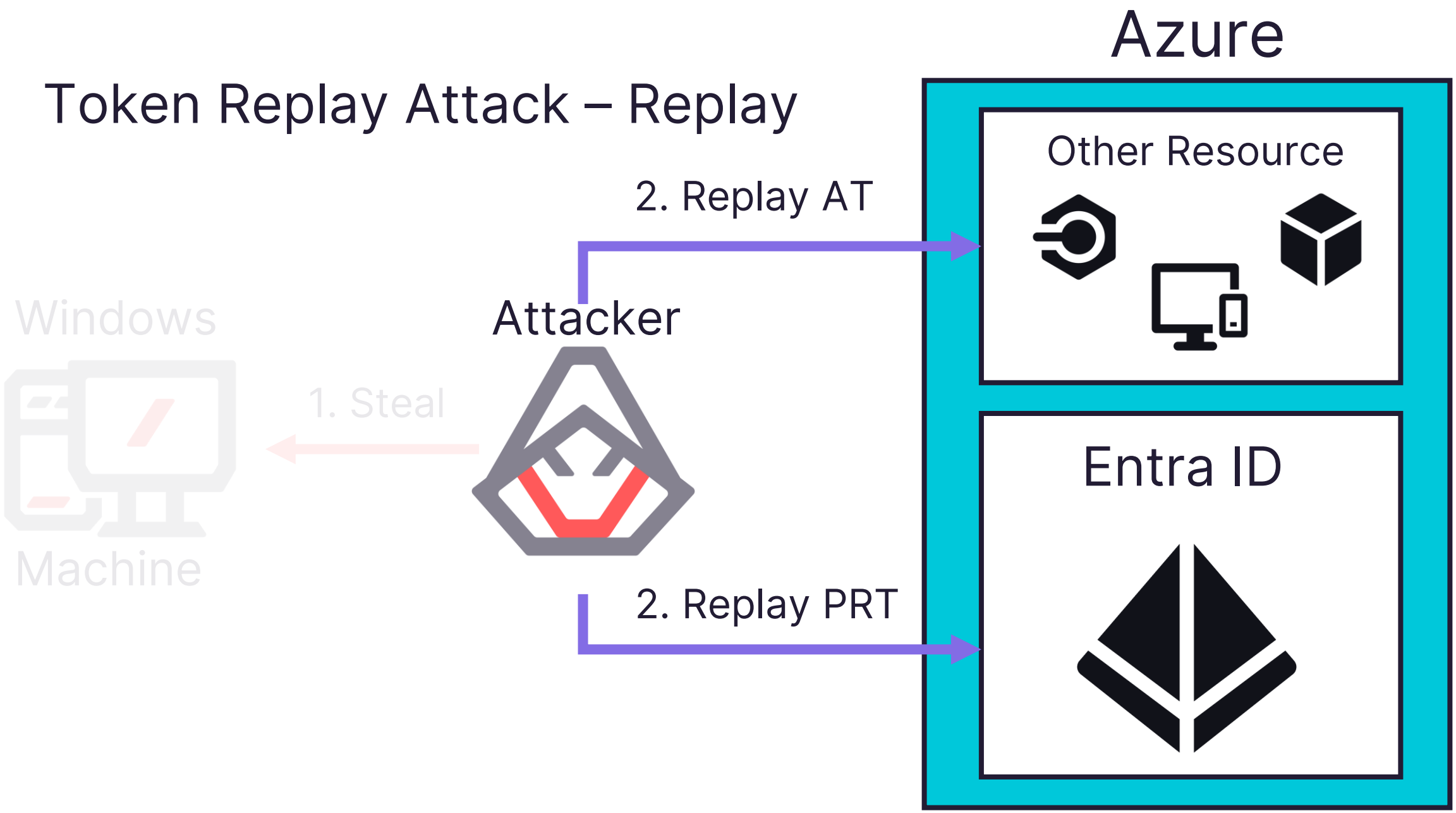
ref: https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/

BrowserCore.exe – Detection

- BrowserCore.exe is usually executed by Chrome



Token Replay Attack – Replay

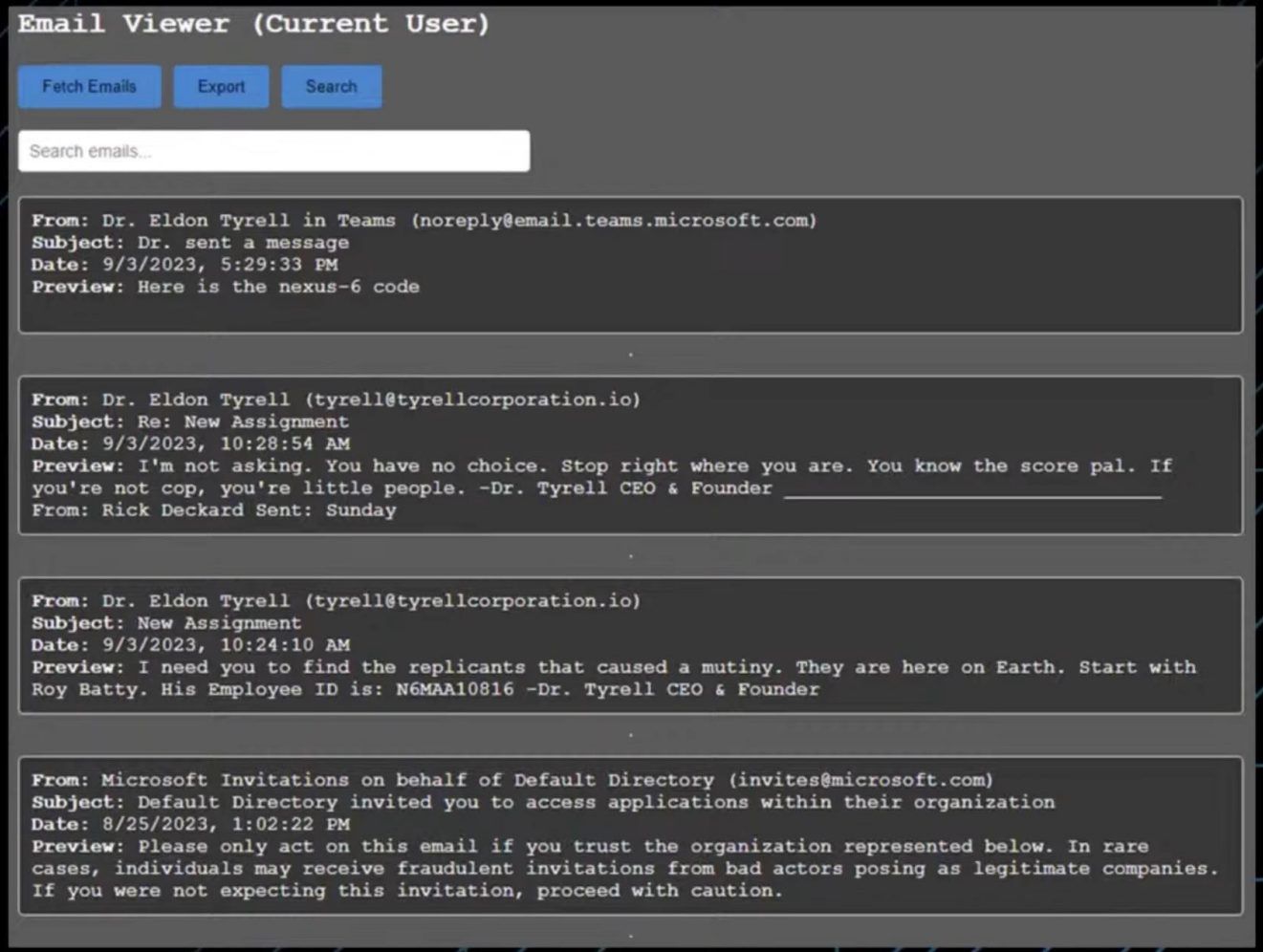


Token Replay Attack – Replay

- Access Token (AT)
  - AADInternals
  - ROADTools
  - Graph Runner
  - TokenTactics v2
- Primary Refresh Token (PRT)
  - Azure Portal
  - AADInternals
  - ROADTools
  - Graph Runner
  - TokenTactics v2

GUI

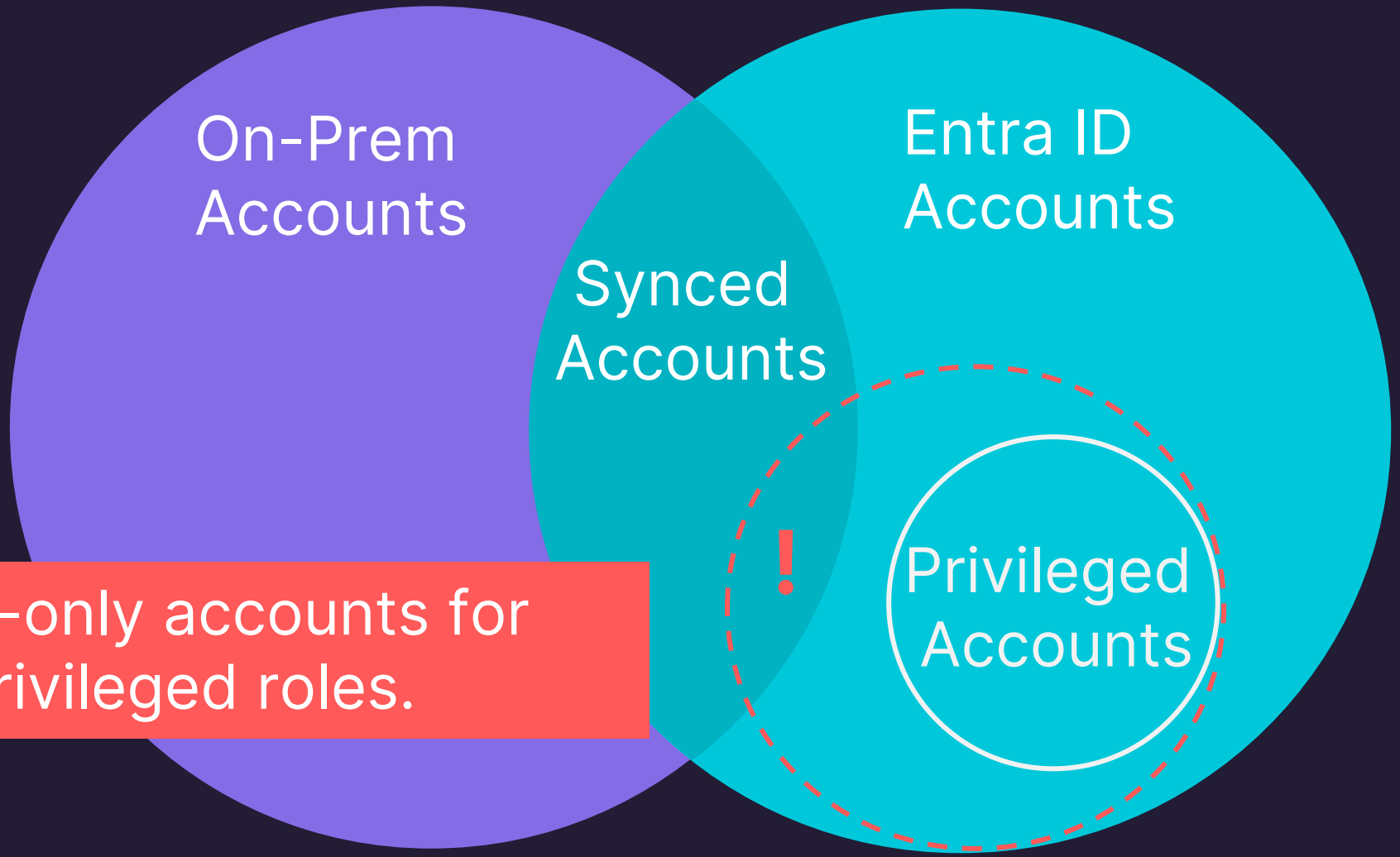
- Send custom API requests
- Enumerate users/groups
- Read/search/send email
- Read shared email
- Read/send Teams msgs
- Access SharePoint and OneDrive files



And to be able to just take that access token and throw

Azure to On-Prem

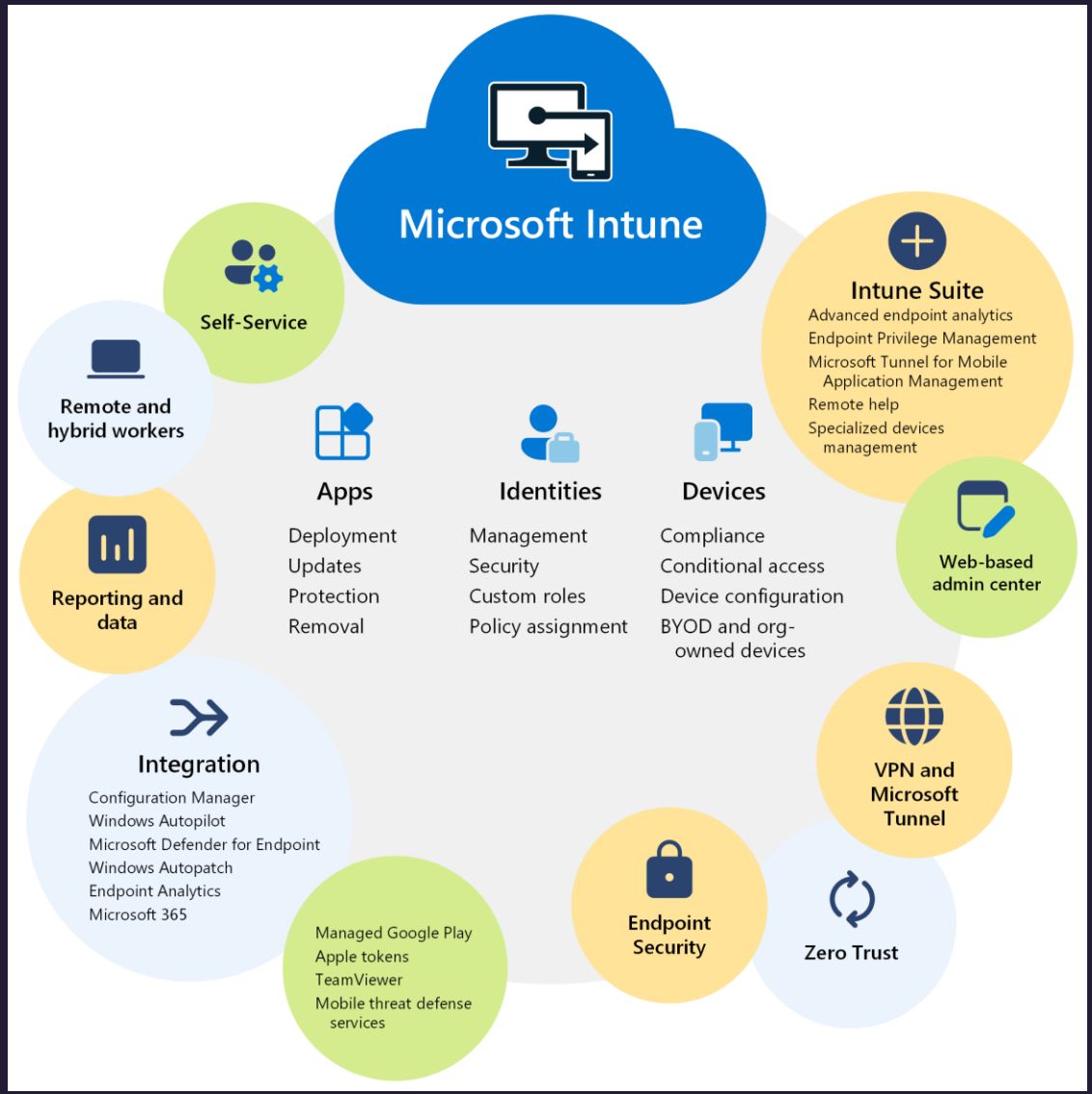
Secure synchronization settings



Use cloud-only accounts for Entra ID privileged roles.

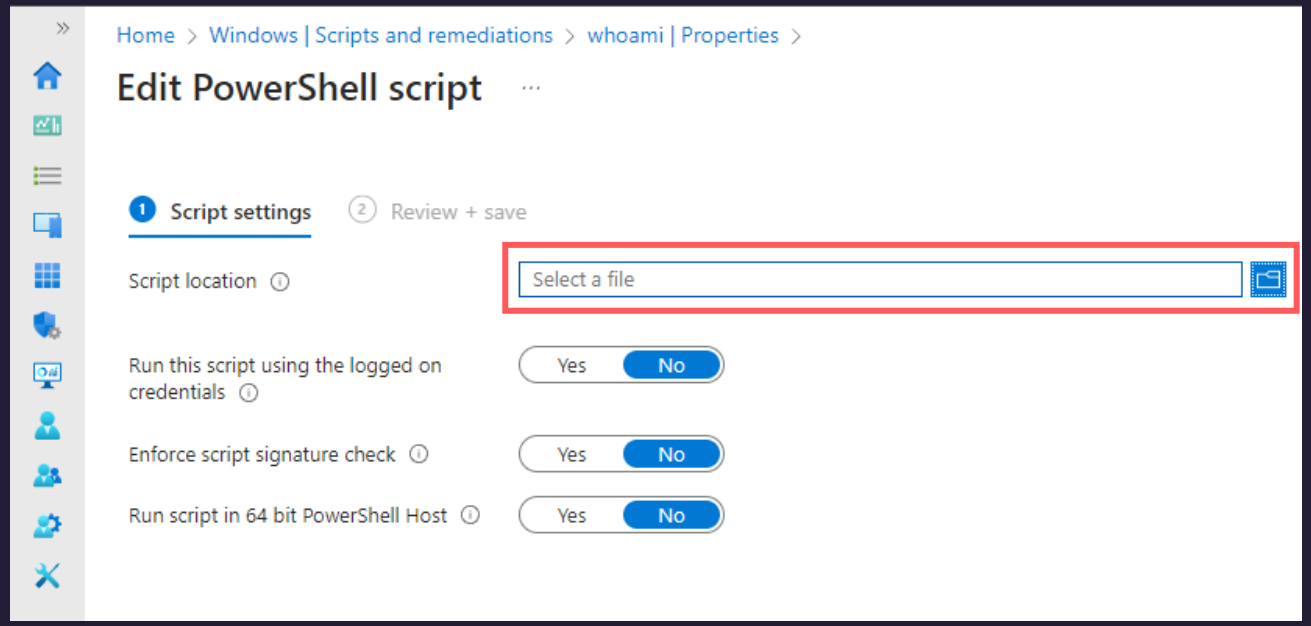
Microsoft Intune

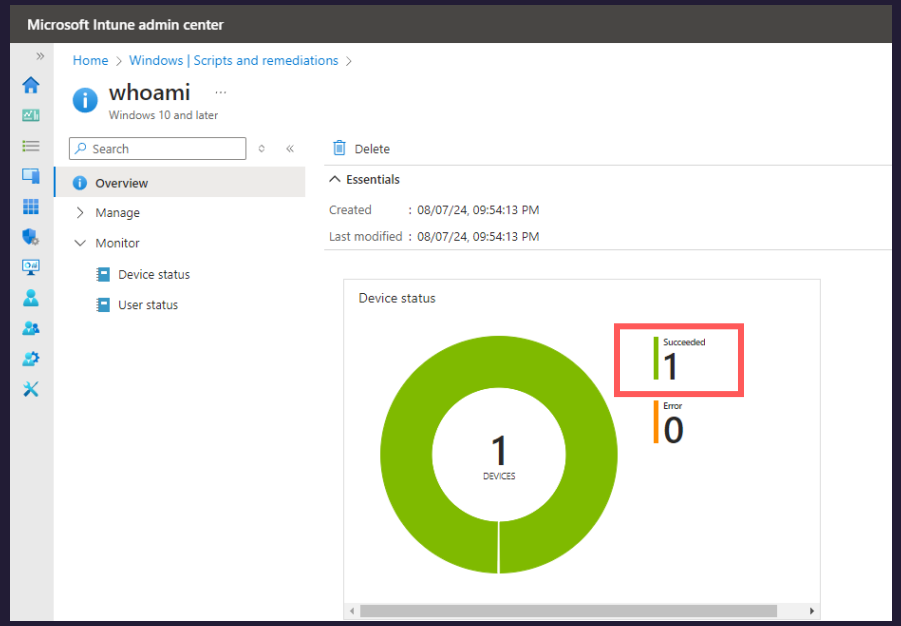
- Endpoint Management Solution
  - Windows, macOS, Android, iOS …
- Simplify app management
  - app management
- Automates policy deployment
  - Device configuration
  - Compliance
  - Conditional access



Execute Scripts on Endpoint Device

- Prerequisites
  - Windows 10/11 devices or macOS 12.0 or later
  - Entra ID-joined or Hybrid-joined
  - Microsoft Intune Plan





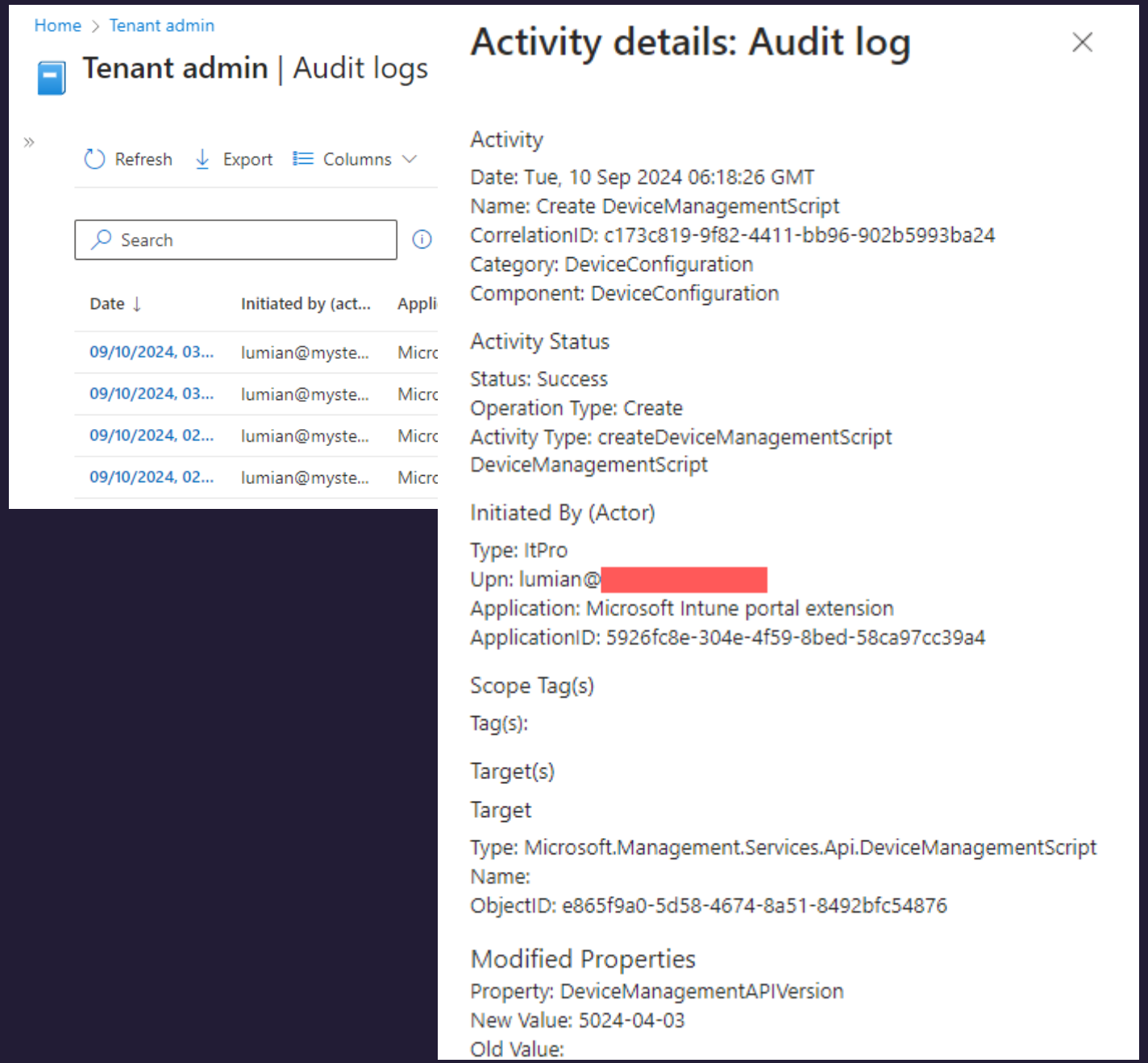
Death from Above: Lateral Movement from Azure to On-Prem AD

Required roles or permission

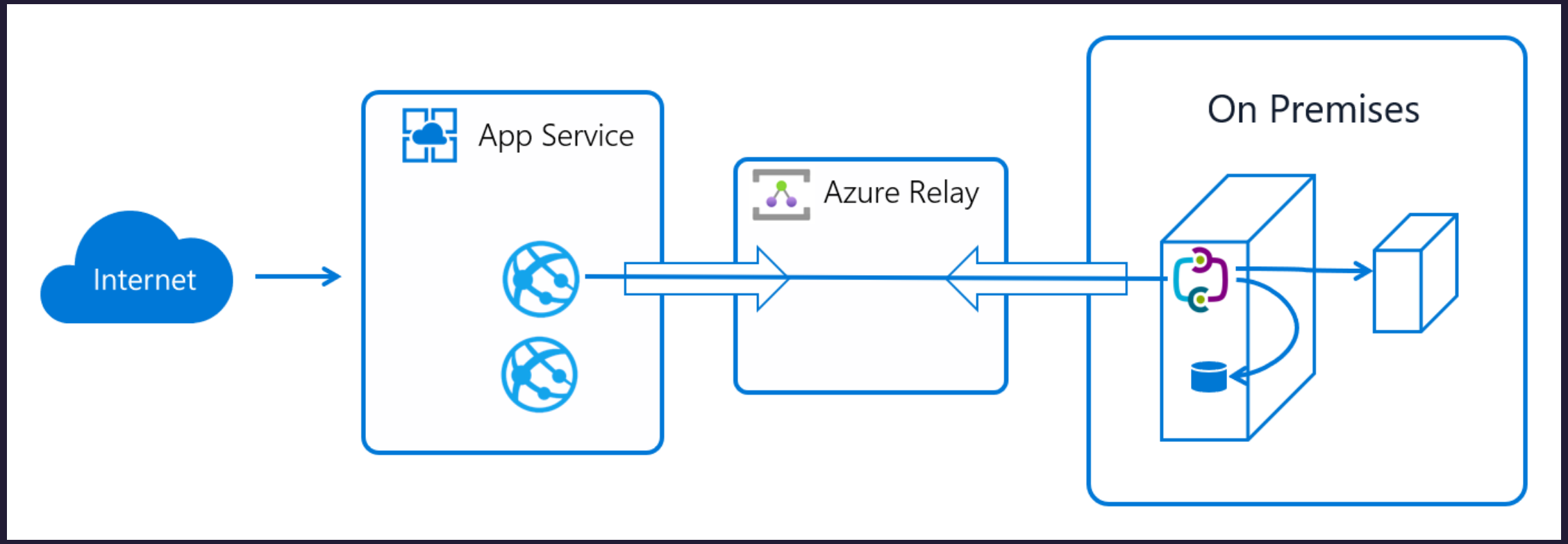
- Entra ID Role Action
  - microsoft.intune/allEntities/allTasks
    (Could Not be assigned to the Custom roles)
- Entra ID Built-in Roles
  - Global Administrator
  - Intune Service Administrator
- Microsoft Graph permission
  - DeviceManagementConfiguration.ReadWrite.All

Detection

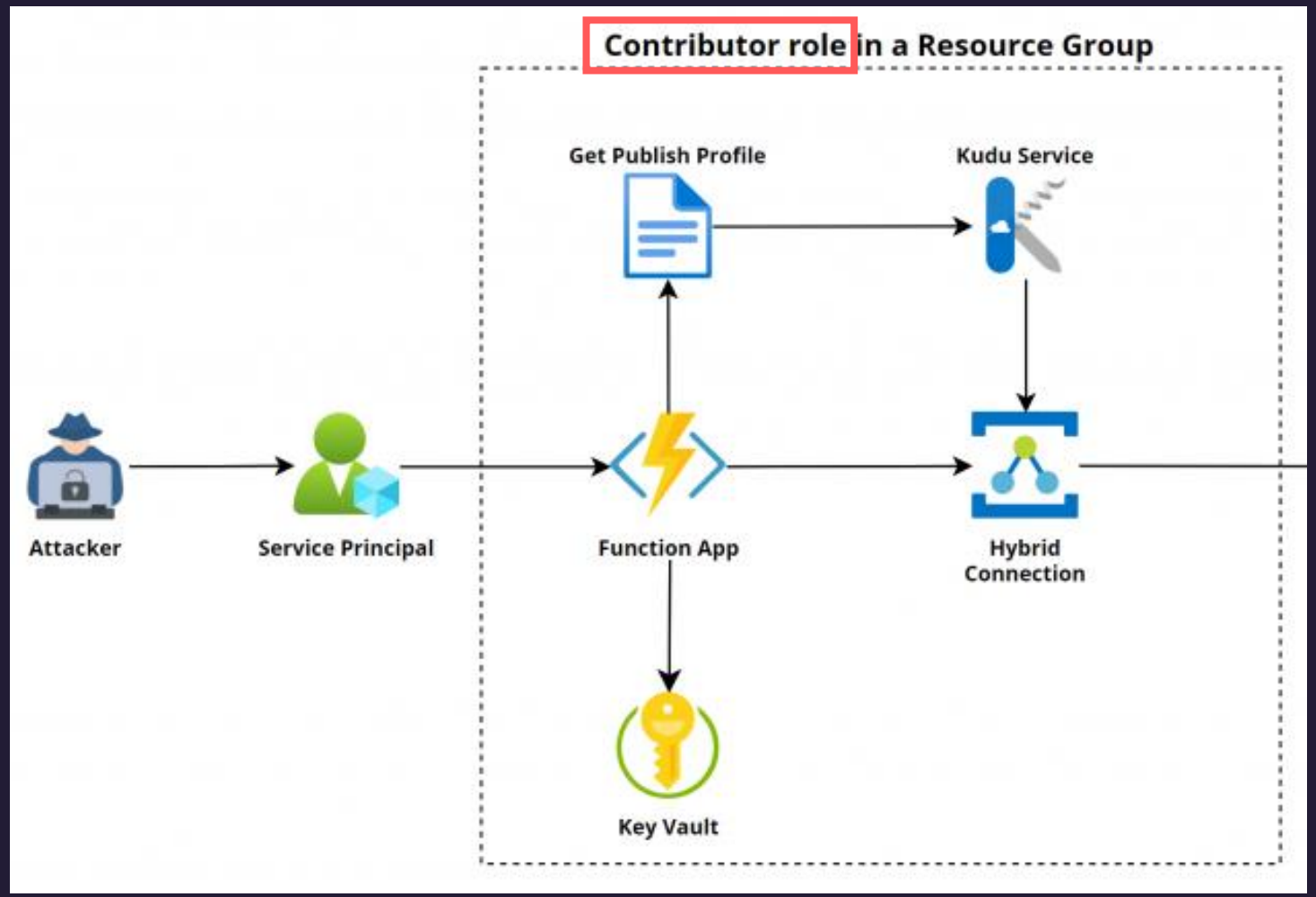
- Intune admin center
  - Script Evidence
    - Could be Removed
  - Audit logs
    - Lack of detail
- Host Forensics
  - Logfile
    - Script Content
  - Registry
    - Execute Result



Hybrid Connection



Cloud penetration Situation

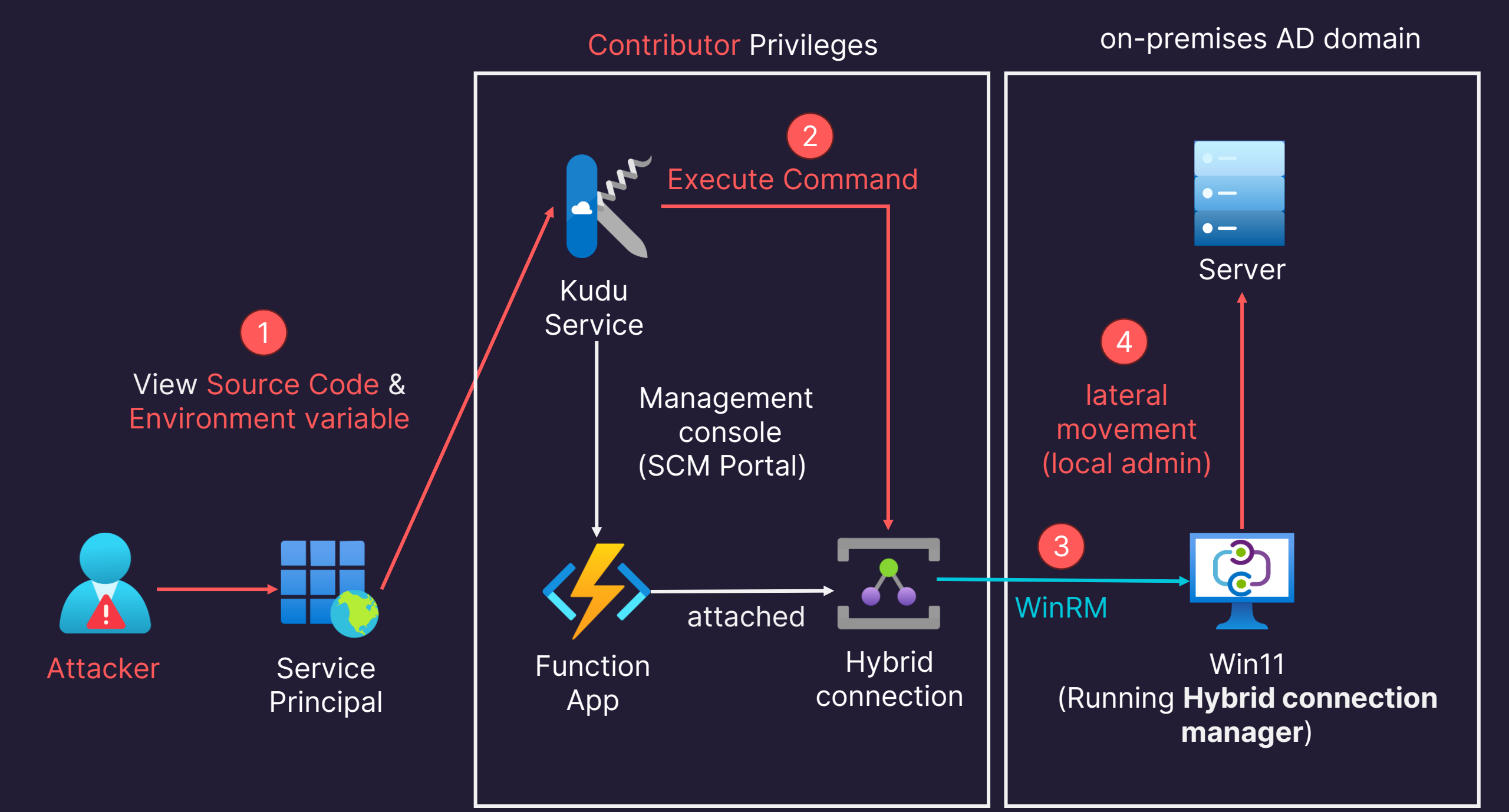



```
PS C:\> Get-AzResource

Name              : onpremsecretstore
ResourceGroupName : LAB
ResourceType      : Microsoft.KeyVault/vaults
Location          : eastus
ResourceId        : /subscriptions/bfc8dc69-69ff-444b-93
                    ault/vaults/onpremsecretstore
Tags              :

Name              : onpremlab
ResourceGroupName : LAB
ResourceType      : Microsoft.Relay/namespaces
Location          : eastus
ResourceId        : /subscriptions/bfc8dc69-69ff-444b-93
                    y/namespaces/onpremlab
Tags              :

Name              : laba47a
ResourceGroupName : LAB
ResourceType      : Microsoft.Storage/storageAccounts
Location          : eastus
ResourceId        : /subscriptions/bfc8dc69-69ff-444b-93
                    age/storageAccounts/laba47a
Tags              :

Name              : ASP-LAB-b1c3
ResourceGroupName : LAB
ResourceType      : Microsoft.Web/serverFarms
Location          : eastus
ResourceId        : /subscriptions/bfc8dc69-69ff-444b-93
                    serverFarms/ASP-LAB-b1c3
Tags              :

Name              : hybrid-func
ResourceGroupName : LAB
ResourceType      : Microsoft.Web/sites
Location          : eastus
ResourceId        : /subscriptions/bfc8dc69-69ff-444b-93
                    sites/hybrid-func
```

Azure Resource

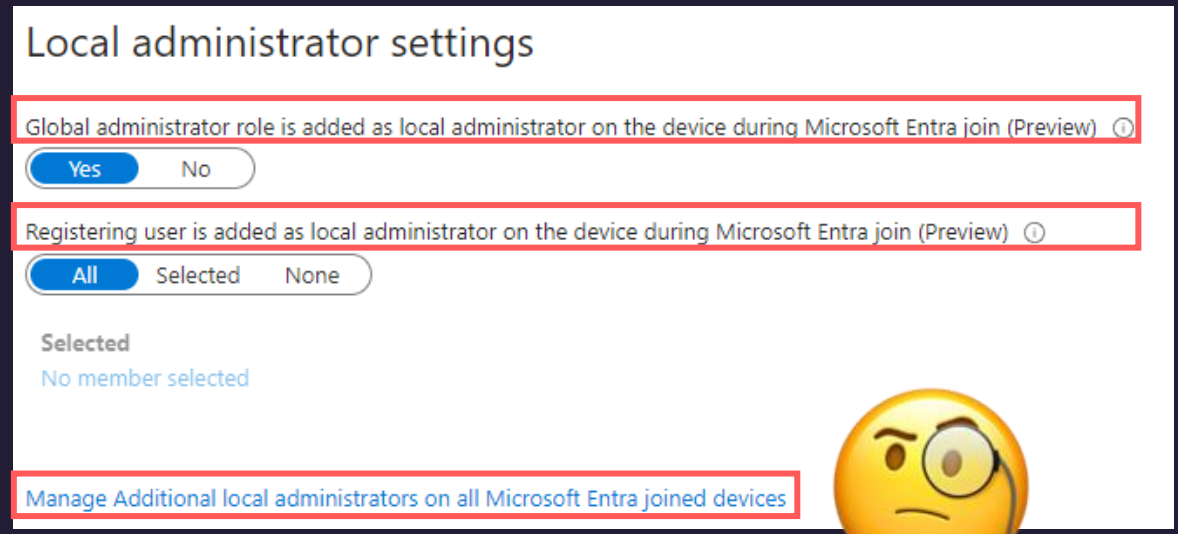
Function Apps (Lambda in AWS) are
serverless computing services provided by Azure Cloud.

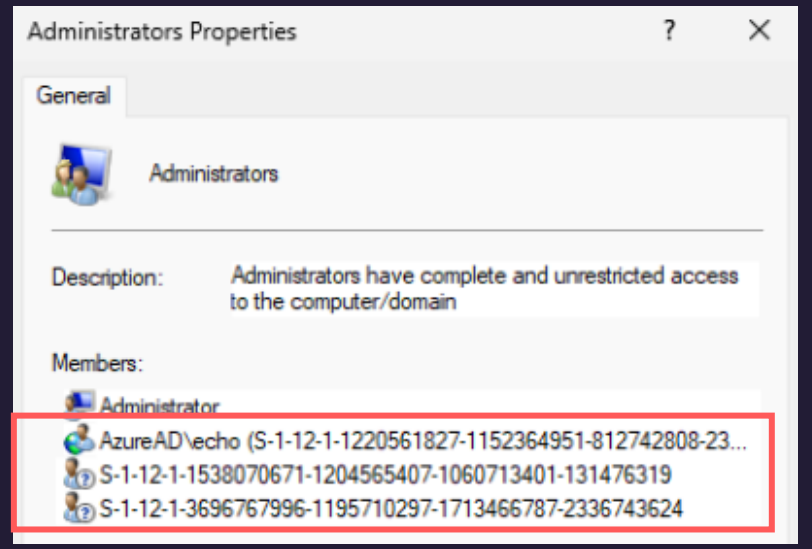
Kudu is the engine behind some features of some Computing Services.
Kudu gives you information about your App Service app, such as:
Environment variables & Run commands in the Kudu console
Need to be Owner or Contributor to access


Contributor Privileges
on-premises AD domain
1
View Source Code &
Environment variable
Attacker
Service
Principal
2
Execute Command
Kudu
Service
Management
console
(SCM Portal)
Function
App
attached
Hybrid
connection
3
WinRM
4
lateral
movement
(local admin)
Server
Win11
(Running **Hybrid connection manager**)

Manage local admin group on Entra joined devices

- During the device registration as Entra-joined these Identities are added to the local admin group by default:
  - Global Administrator
  - Microsoft Entra Joined Device Local Administrator
  - The user performing the Microsoft Entra join





CYCRAFT

Manage Additional local administrators on all Microsoft Entra joined devices

- How it Works:
  - Assign User Microsoft Entra Joined Device Local Administrator Role
  - Should this be free?
- The Microsoft Document is out of date

Manage the Microsoft Entra Joined Device Local Administrator role

You can manage the Microsoft Entra Joined Device Local Administrator role from **Device settings**.

1. Sign in to the Microsoft Entra admin center as at least a Privileged Role Administrator.
2. Browse to **Identity** > **Devices** > **All devices** > **Device settings**.
3. Select **Manage Additional local administrators on all Microsoft Entra joined devices**.
4. Select **Add assignments** then choose the other administrators you want to add and select **Add**.

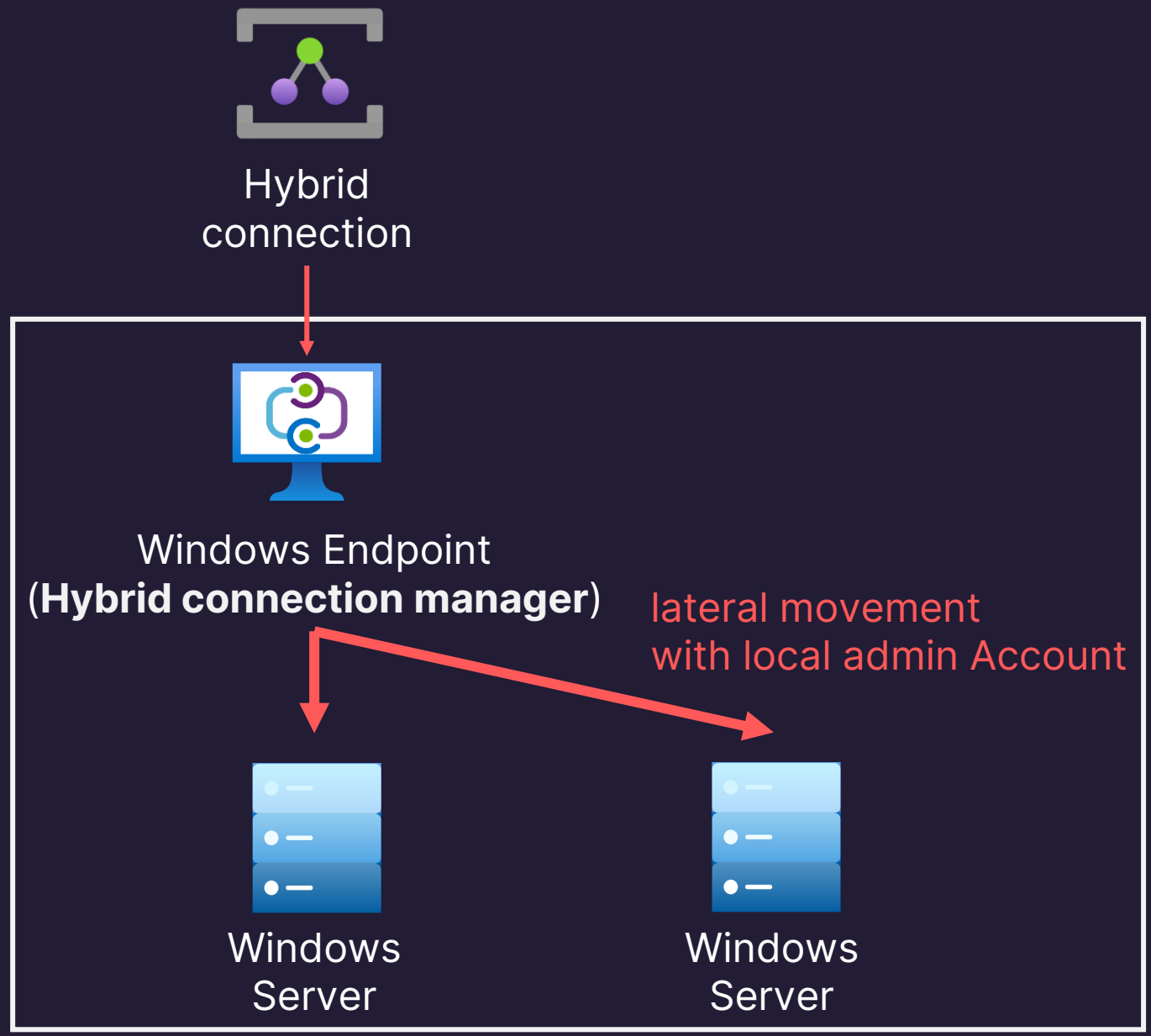
To modify the Microsoft Entra Joined Device Local Administrator role, configure **Additional local administrators on all Microsoft Entra joined devices**.

Note

This option requires Microsoft Entra ID P1 or P2 licenses.

Attack Scenario

- Prerequisites
  - Attacker Get Access to an endpoint Server
  - Most Entra joined Devices are in the same intranet
- Attacker Required roles:
  - Global Administrator
  - Microsoft Entra Joined Device Local Administrator

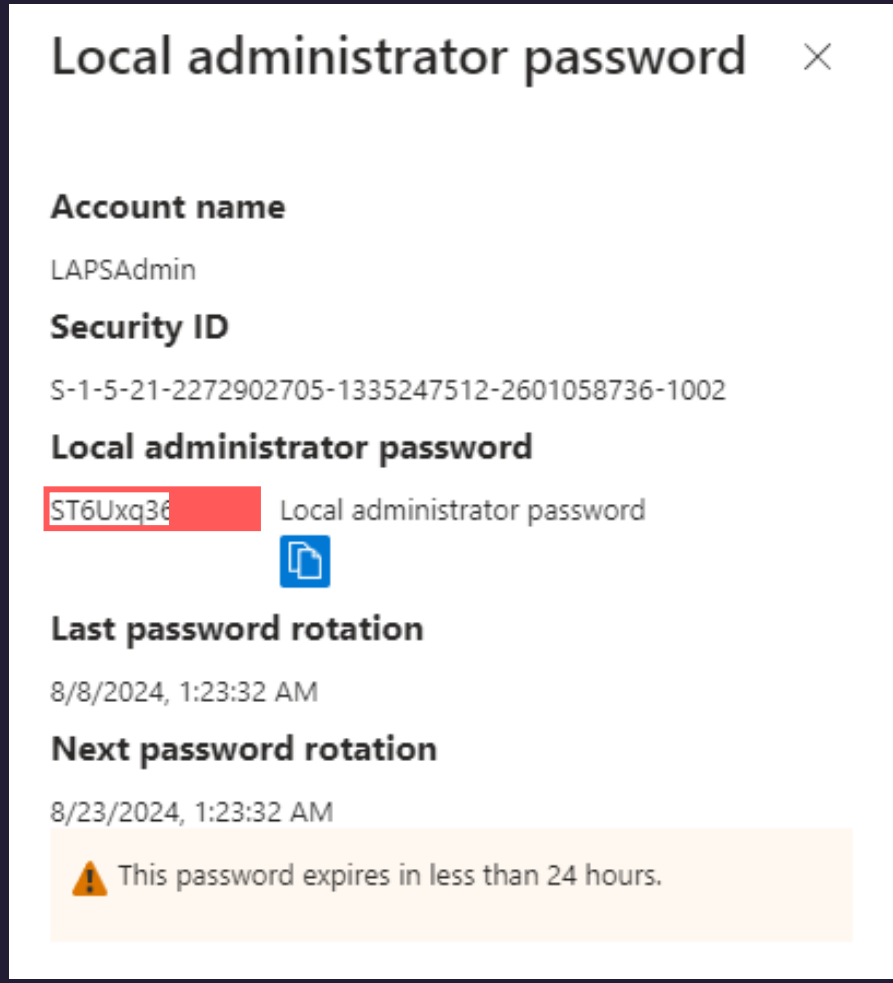


Local Administrator Password Solution

- Legacy Microsoft LAPS
  - solution to manage the local Administrator account passwords on domain-joined computers
  - Back up local administrator account passwords to Windows AD
  - Mitigate any lateral traversal attacks
- Windows LAPS vs. legacy Microsoft LAPS
  - Back up local administrator account passwords to Entra ID for Entra-joined & Hybrid-joined devices

Obtain Password from Entra ID

- Prerequisites
  - Windows 10/11 devices
  - Entra joined / Hybrid-joined
- The preferred deployment policy is to use Intune with the Windows LAPS CSP.

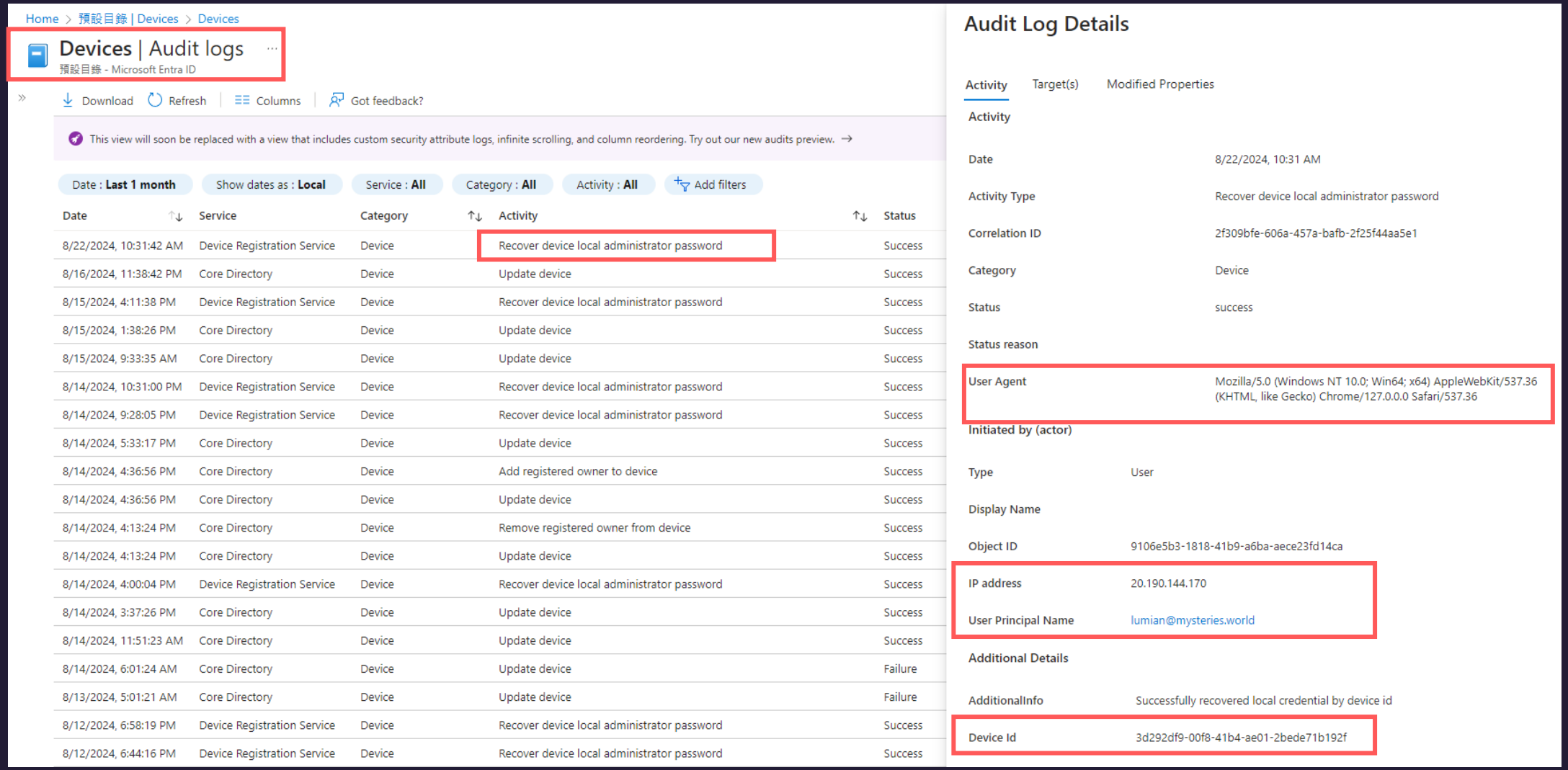


Step-by-Step Guide: Enabling Windows LAPS in Entra ID (Azure Active Directory)

Required roles or permission

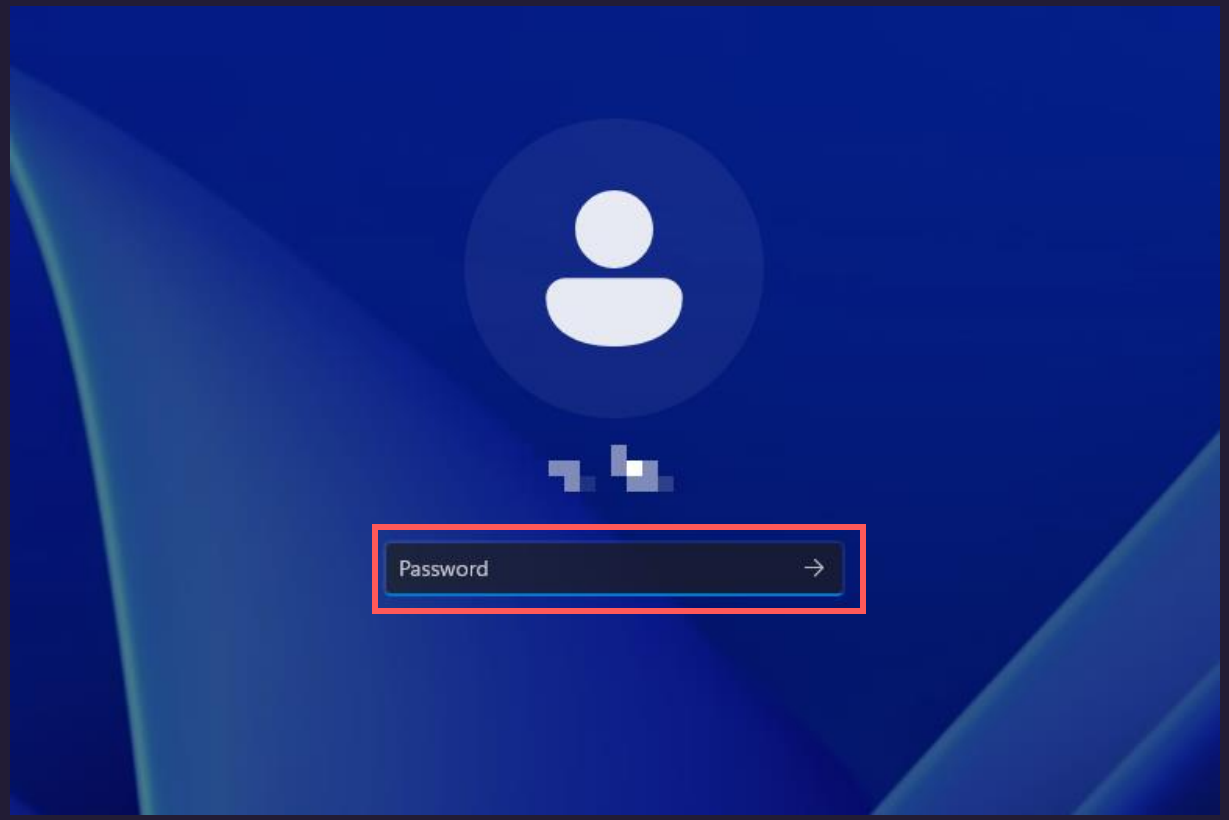
- Entra ID Role Action
  - microsoft.directory/deviceLocalCredentials/password/read
    (Could be assigned to the Custom roles)
- Entra ID Built-in Roles
  - Global Administrator
  - Intune Service Administrator
  - Cloud Device Administrator
- Microsoft Graph permission
  - DeviceLocalCredential.Read.All

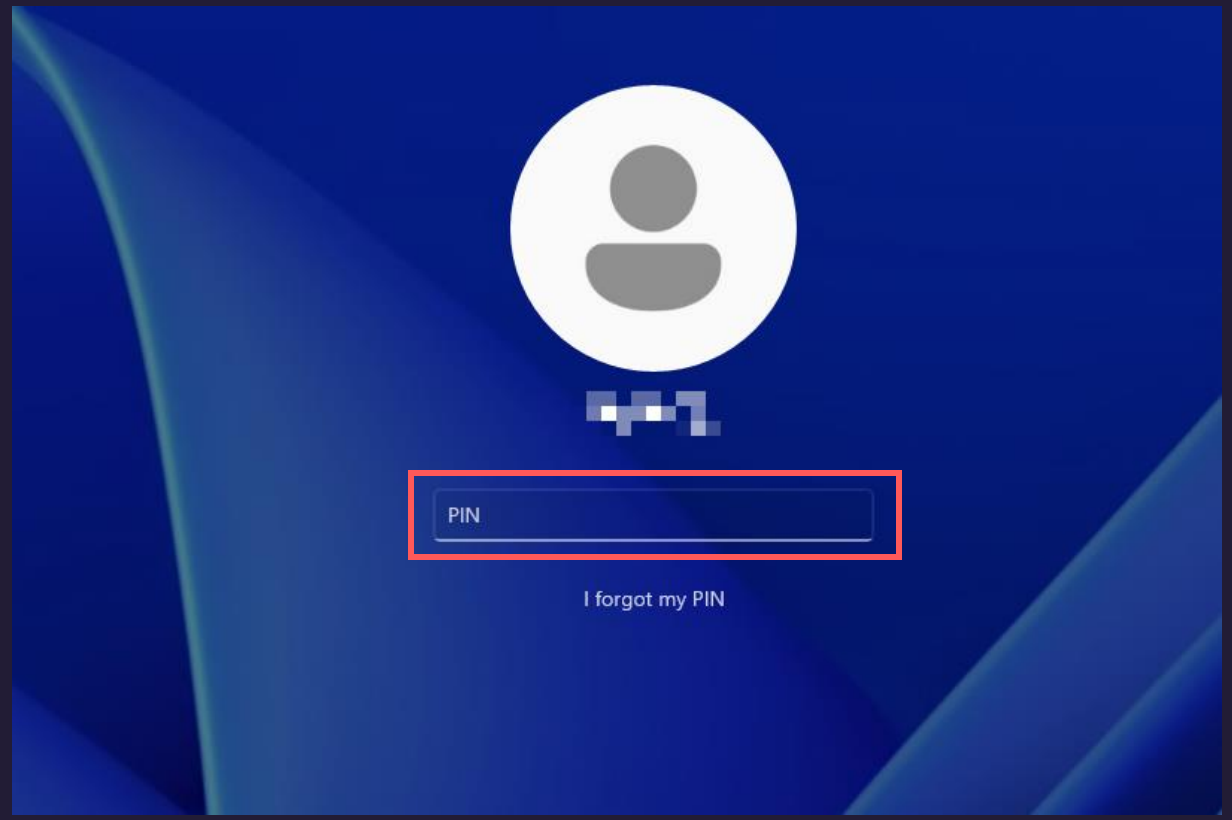
Detection



Enable Windows LAPS with Azure AD

What’s the difference

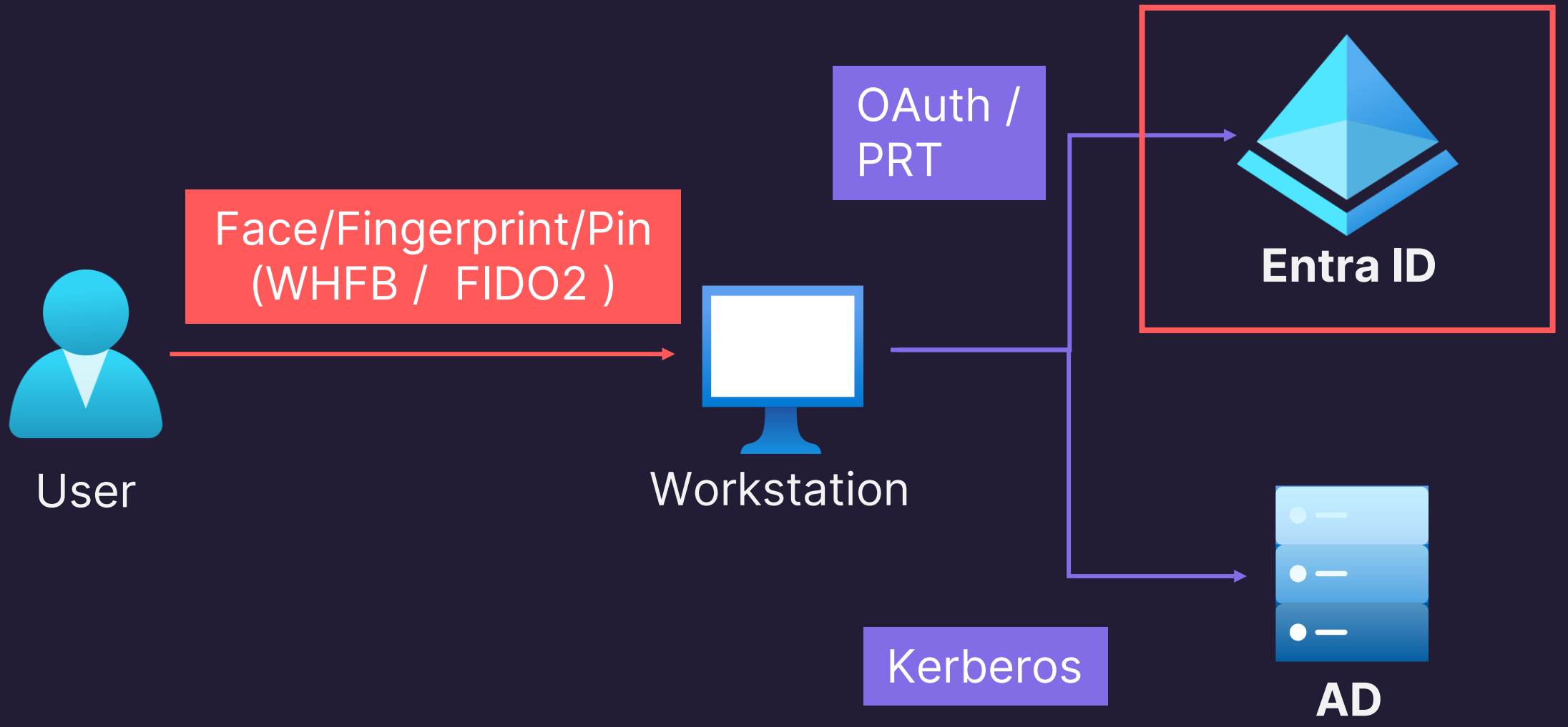




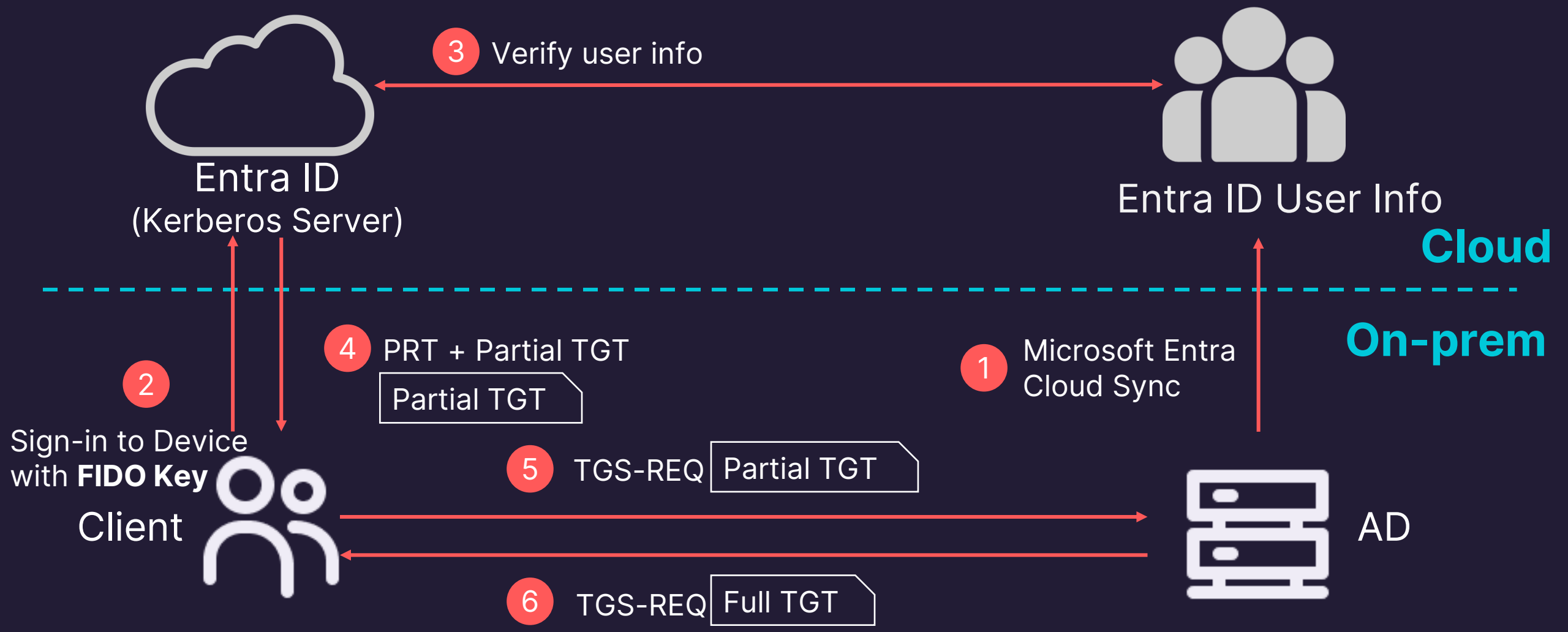
Cloud Kerberos Trust

- In Hybrid-joined using Windows Hello (for Business)
  - Cloud Kerberos Trust is setup by default
- on-premises / Cloud SSO for Passwordless authentication without PKI

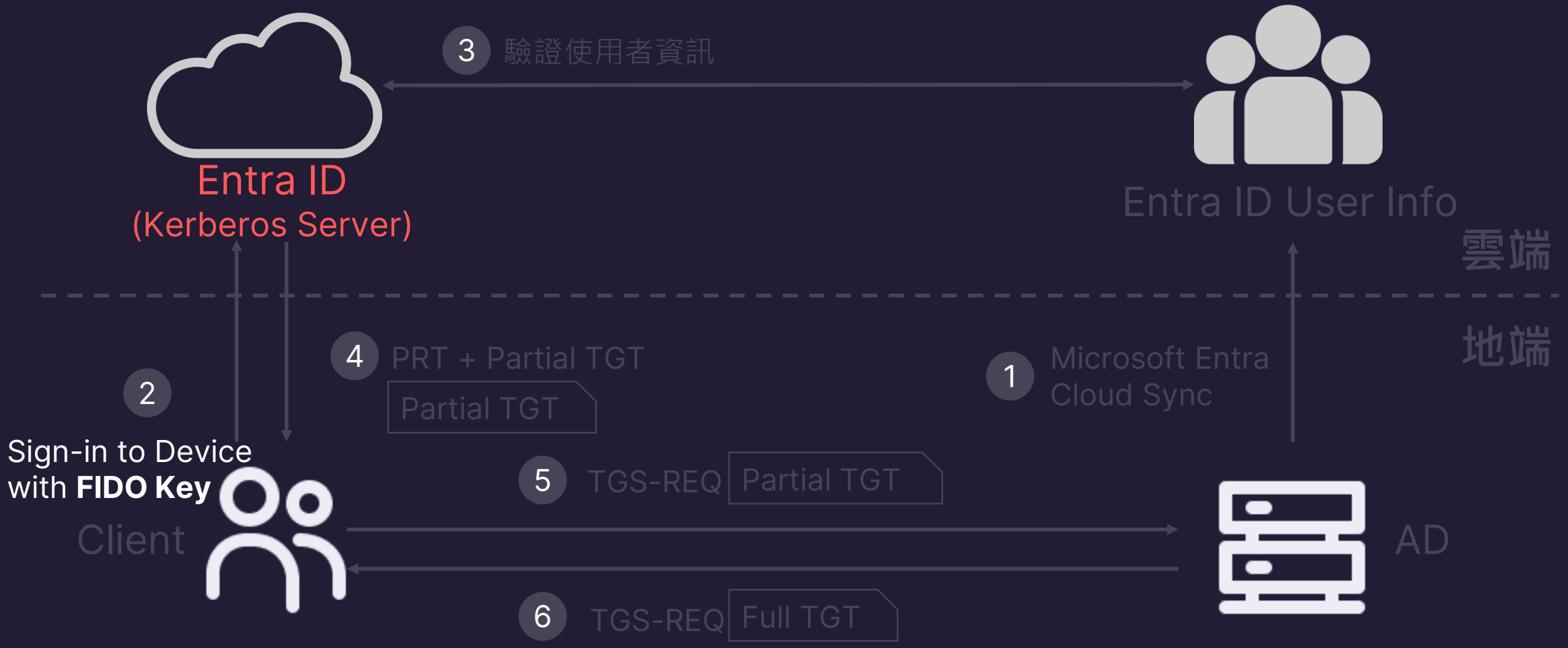
Passwordless Authentication



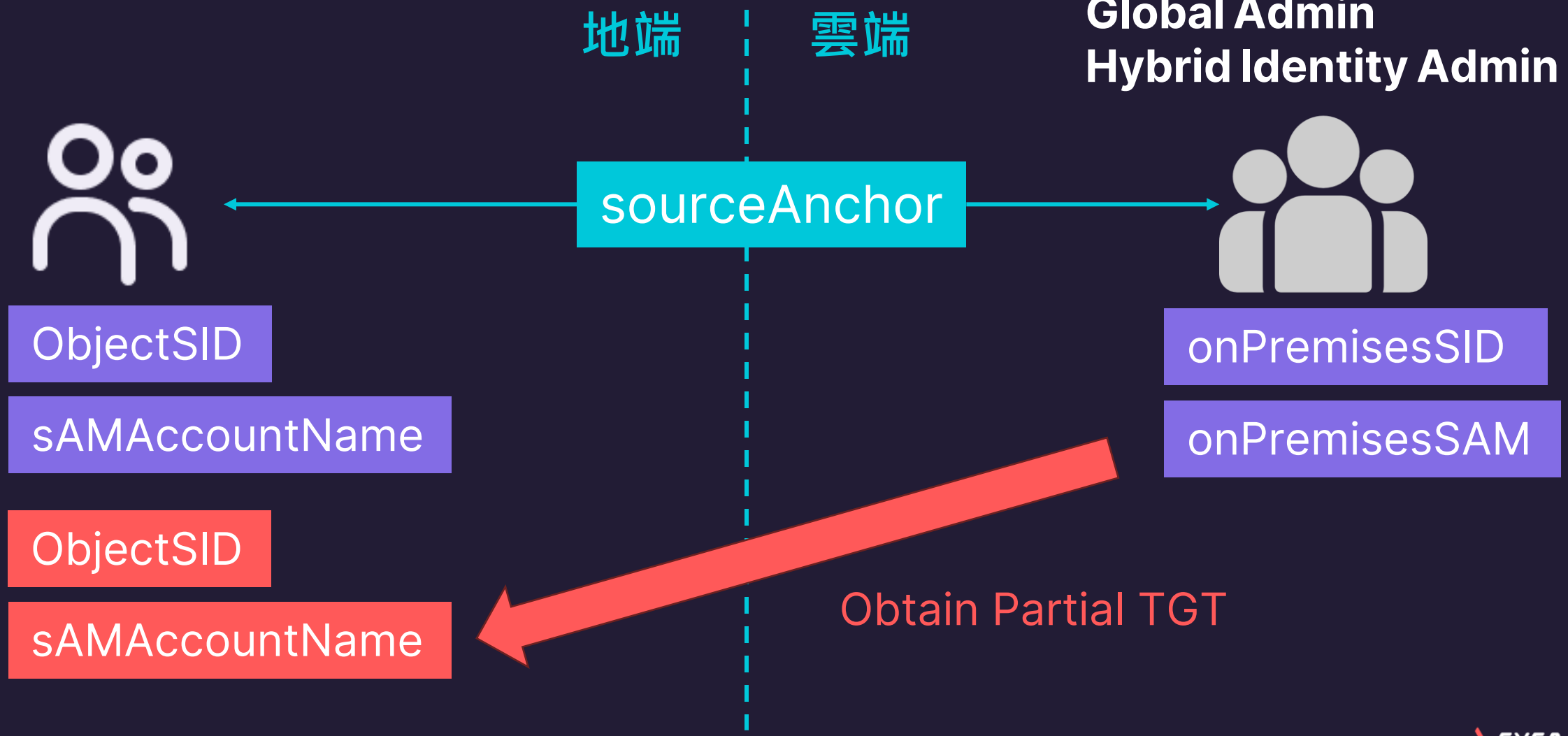
Passwordless Authentication 流程



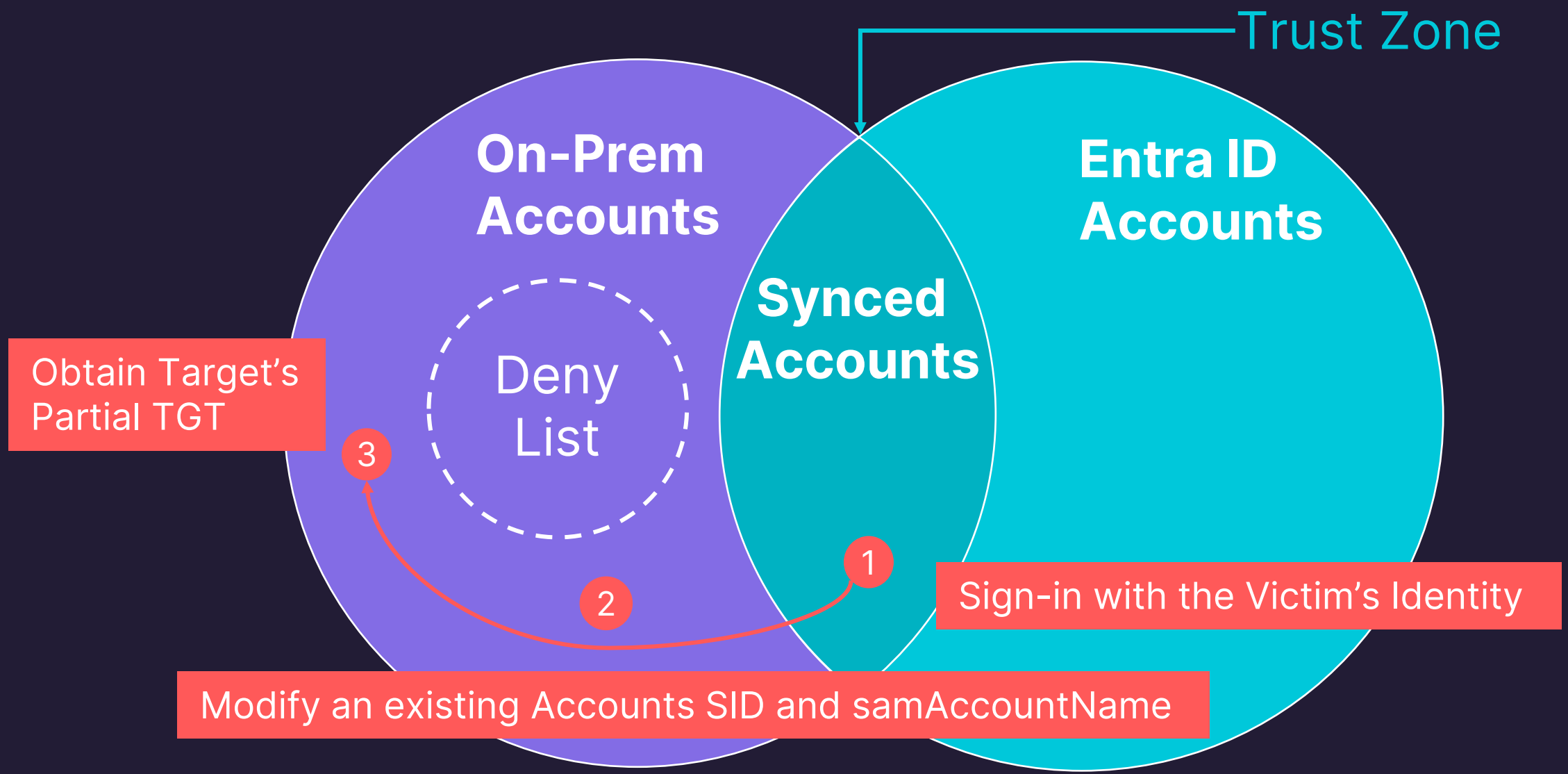
攻擊者視角


3 驗證使用者資訊
Entra ID
(Kerberos Server)
Entra ID User Info
雲端
地端
4 PRT + Partial TGT
Partial TGT
2
1 Microsoft Entra
Cloud Sync
Sign-in to Device
with FIDO Key
Client
5 TGS-REQ Partial TGT
AD
6 TGS-REQ Full TGT

Syncing between On-Prem / Cloud



Violate Cloud Kerberos Trust



CYCRAFT

Entra ID Kerberos Server Password Replication Policy

- Allow:
  - Domain User
- Deny: (優先)
  - Domain Admins
  - Schema Admins
  - Enterprise Admins
  - Account Operators
  - ...

- What's missing?
- The AAD connect service account (MSOL_XXXXXX) with DCSYNC privileges (always there)

Abuse of Cloud Kerberos Trust

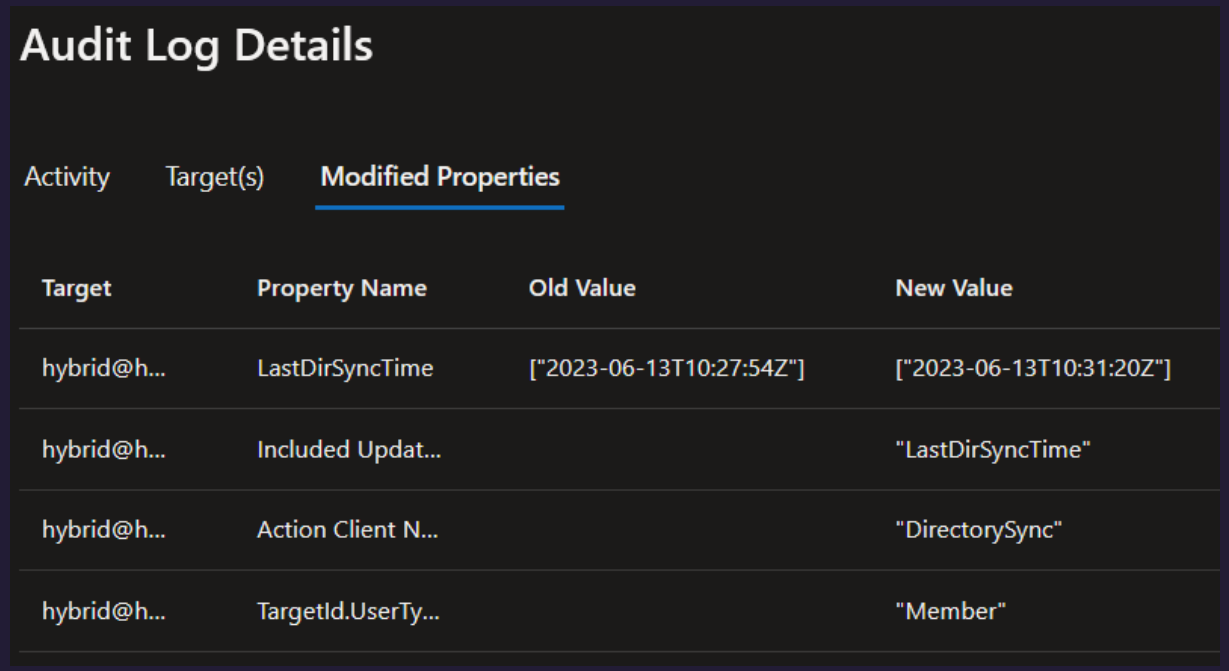
- Prerequisites
  - Windows Hello For Business
  - Hybrid-joined
- On-prem
  - Hybrid (Sync) account which we can modify & authenticate
- Entra ID Roles
  - Global Admin
  - Hybrid Identity Admin
- Target
  - On-Prem Account that is in the Allow List, but not in the Deny List.
  - Hybrid (Sync) accounts could be the targets
    - onPremisesSID, onPremisesSAM cannot be the same, so attackers need to change them first

Notes

- To allow local services that do not support Kerberos to use FIDO2, support a field with long-term secrets (NTLM) in the Kerberos Extended Protocol. Attackers can extract NTLM from Full-TGT after acquiring it, which can be used to increase the durability of the attack.
- Reference:
  - The Kerberos Key List Attack: The return of the Read Only Domain Controllers

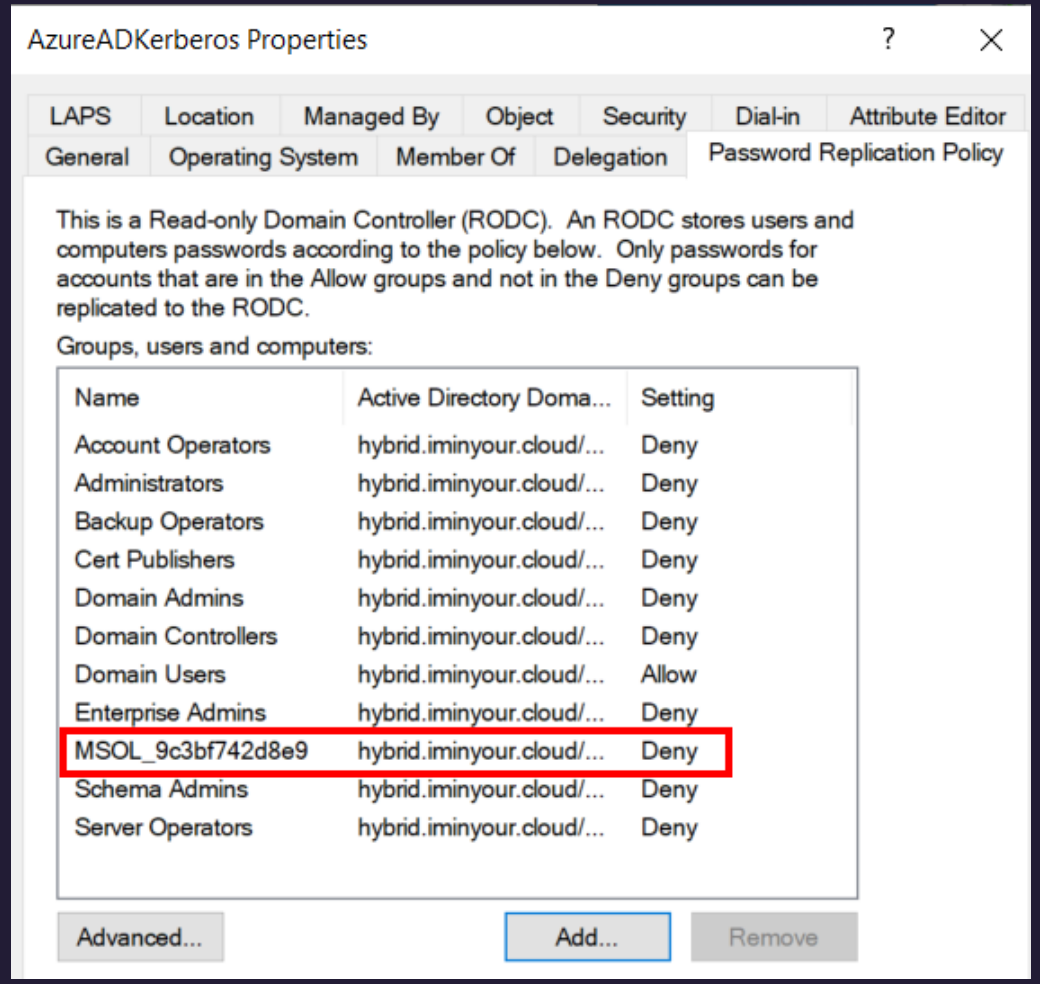
Detection

- Bad News
  - You won't see onPremisesSID,onPremises SAM changed, you'll only see the abnormal synchronization time.
- Good News
  - Synchronization is not normally performed by normal users, but by a dedicated synchronization account, Sync_XXXXX.



Prevention

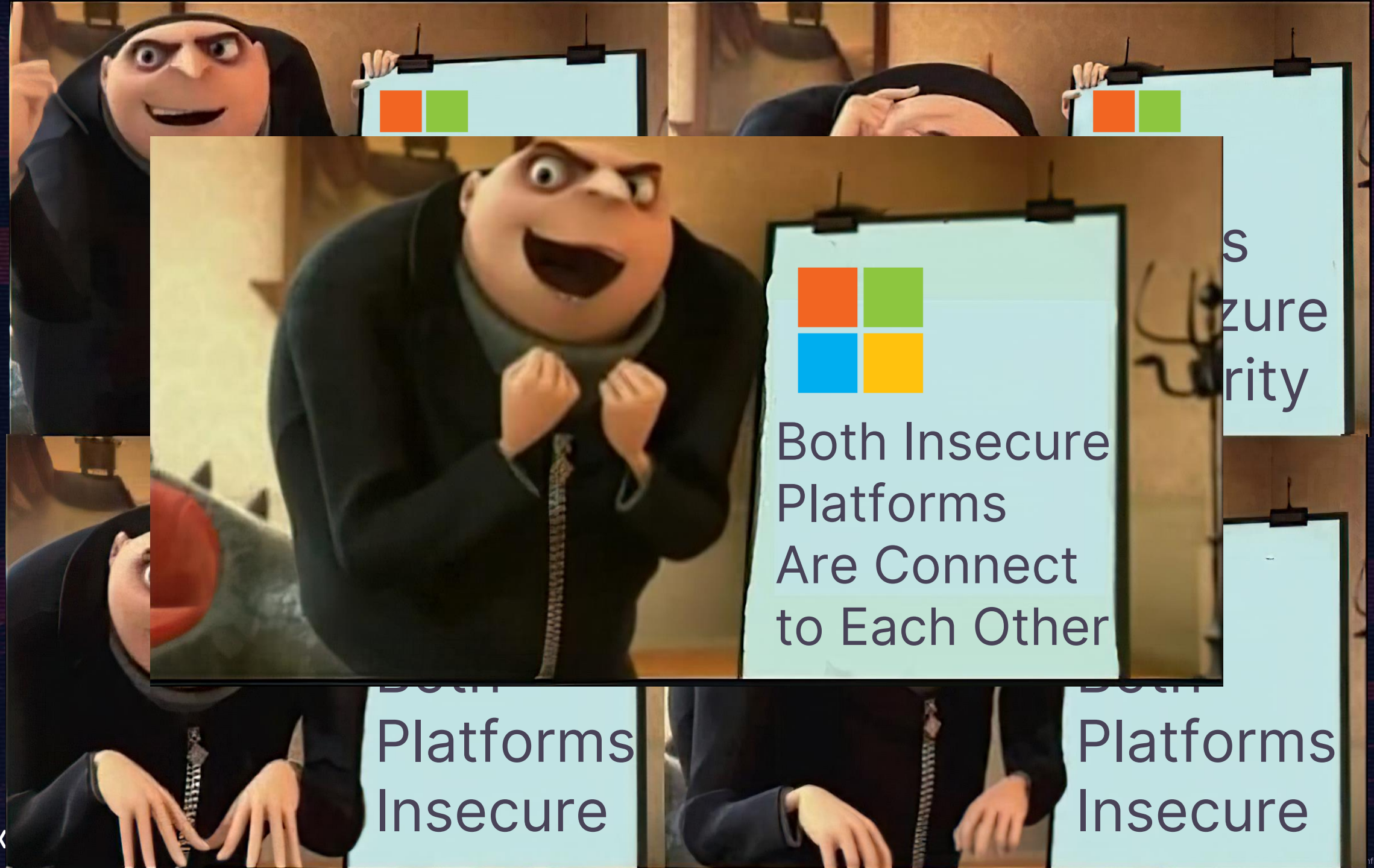
- It's not enough to put MSOL_XXXX into the DENY LIST.
- Based on our experience the number of unintended administrators is 5.8 times the number of administrators, unless these accounts are put on the DENY LIST or the control relationship is eliminated, this attack can be eliminated!



Obtaining Domain Admin from Azure AD by abusing Cloud Kerberos Trust

	Prerequisites	Must been in intranet	Entra ID Role	Azure Role	**Obtain Content**
Windows LAPS	Entra-joined Hybrid-joined	✓	Global Admin Intune Admin	✗	local system administrator password
Microsoft Intune	✗	✗	Global Admin Intune Admin Cloud Device Admin	✗	Execute scripts with system privileges
Cloud Kerberos Trust	Hybrid-joined WHFB	✓	Global Admin Hybrid Identity Admin	✗	User Plain text Password
Hybrid Connection	✗	✗	Global Admin	Owner contributor	Cloud to Intranet Direct Connection
Manage local admin group	Entra-joined	✓	Global Admin Microsoft Entra Joined Device Local Admin	✗	local system administrator password


Ignore Windows Security
Focus on Azure Security
Both Platforms Insecure
Both Platforms Insecure


Both Insecure
Platforms
Are Connect
to Each Other
Platforms
Insecure
Platforms
Insecure

Action

CYCRAFT

Thanks!

EVERYTHING
STARTS
FROM
SECURITY